

SYNGRESS
SHINDERBOOKS

1 YEAR UPGRADE
BUYER PROTECTION PLAN



SCENE OF THE

Cybercrime

Computer Forensics Handbook
TOMO I

Bring Cybercriminals to Justice

- Protect Your Business, Home, Employees, and Family from Becoming Targets
- Learn Techniques for Collecting and Preserving Digital Evidence
- Hundreds of CyberLaw Reviews, On the Scene Sidebars, and CyberStats

Debra Littlejohn Shinder
Ed Tittel Technical Reviewer

Prólogo

Este libro, más que ningún otro que haya escrito hasta este punto de mi vida, fue una labor de amor. Me permitió combinar el conocimiento y la experiencia de dos carreras (más de una década en la policía y casi otra década en el campo de la computación, conformando casi 20 años de trabajo con computadoras como aficionada). Cuando era una oficial activa de la policía, el crimen cibernético era un área especialmente esotérica - los investigadores de agencias pequeñas y medianas raramente se tropezaban con un caso que involucrara evidencia digital, y el término *crimen cibernético* no se escuchaba en la mayoría de los círculos policiales.

Hoy día, todo eso ha cambiado. De hecho, toda nuestra forma de vida ha cambiado durante las dos últimas décadas y muchos de esos cambios se le pueden atribuir directamente a la Internet. Conocí a mi esposo en la Net en 1994, cuando todavía era una policía y él practicaba la medicina. Hemos transitado un largo camino desde entonces, nene.

En la actualidad, ambos hacemos nuestras vidas en línea, como autores, asesores, y proveedores de capacitación en línea. El 90% de nuestro negocio se desarrolla a través de la Internet. Muchas de nuestras amistades comenzaron en el mundo virtual y utilizamos el correo electrónico para mantenernos en contacto con miembros de la familia que se encuentran en lugares lejanos con los que, probablemente, no pudiésemos tener contacto si no fuera de esta manera. Hay muchos afuera a los que les caemos bien, cuyas vidas en el “mundo real” están inevitablemente entrelazadas con el tiempo que pasamos en el bajo mundo del ciberespacio. Es inevitable, supongo, que los miembros del mismo elemento antisocial de la sociedad con los que lidié como oficial de policía, encuentren también sus mecanismos para entrar en la Net.

Mientras más profundizaba en las complejidades de las computadoras y las redes en mi afán de desarrollar mi nueva profesión, más recordaba el momento en que me percaté de que la comercialización y el uso generalizado de la Internet proporcionaba oportunidades para los estafadores, ladrones, pornógrafos de niños, comerciantes de drogas y personalidades abusivas que conforman los cuadros de la “clientela” de los oficiales de la policía. Todavía una gran parte del mundo policial parece estar atrasado cuando de tecnología se trata. A finales de los años 1990 existían aún muchas agencias en el país donde los policías hacían sus reportes de forma manual y las secretarías de los policías eran las únicas en la oficina que tenían computadoras, las que usaban sólo como procesadores de texto de calidad superior.

Cuando aparecieron los crímenes por ordenador, los criminales llevaban una gran ventaja. Pero la comunidad de los agentes del orden en el siglo XX parece haber despertado finalmente ante el hecho de que la resistencia es inútil y que las computadoras llegaron para quedarse. He observado a mis ex colegas policías resistiéndose a entender este Mundo Feliz donde la única “herramienta tangible del crimen” pueden ser series etéreas de bits y bytes, donde se pueden cometer delitos por “control remoto” desde cientos o miles de millas de distancia y donde las reglas de la evidencia han sido reemplazadas por la naturaleza de la comunicación digital. También comencé a darme cuenta, cuando el crimen

cibernético devino tema candente del momento, de que muchos de mis compañeros profesionales de la Informática conocen mucho sobre programación y administración de redes, pero entienden muy poco sobre leyes. Frecuentando grupos de noticias técnicas y enviándolas a listas de correos de policías exclusivamente, noté que existía un patrón: la falta de información y comunicación entre los agentes del orden y los especialistas en informática era obviamente grande. Cuando oía percepciones erróneas repetidas de ambos lados, percepciones erróneas que hacían imposible combinar los talentos y esfuerzos de la policía y los profesionales de la informática en contra de los criminales ciberneticos, me quedé pensando: alguien debería escribir un libro. Y eso hice.

Mi objetivo al escribir este libro es alcanzar una audiencia dual. Espero darles a otros expertos técnicos la posibilidad de echarle una miradita al mundo de la ley y el orden, un ambiente bien estructurado donde la “letra de la ley” es primordial y los procedimientos deben seguirse de cerca, no sea que una investigación se contamine y toda la evidencia recopilada termine siendo inútil. También espero darles a los agentes del orden una idea de algunos de los aspectos técnicos sobre cómo se cometen los crímenes ciberneticos -y cómo se puede emplear la tecnología para localizar y construir un caso en contra de los criminales que los cometen. Quiero proporcionarles un mapa de carreteras que puedan usar aquellos que se encuentran a ambos lados de la mesa para orientarse en el panorama legal y técnico, de modo que juntos podamos entender, prevenir, detectar y enjuiciar satisfactoriamente la conducta criminal que representa una amenaza para la comunidad en línea como la que puede representar un crimen “tradicional” para los vecindarios en donde vivimos.

El primer Capítulo “Enfrentando el Problema del Crimen Cibernetico” brinda una amplia perspectiva general sobre el crimen cibernetico: qué es (y qué no), las formas en que se diferencia de otros tipos de crímenes (y las formas en que no) y cómo podemos dividir el amplio concepto de “crimen cibernetico” en categorías que lo hagan más manejable para analizar, legislar, hacer cumplir e, idealmente, prevenir. Aquí es donde encontrará estadísticas y definiciones formales, así como una breve introducción a algunos de los tópicos que serán tratados más detalladamente en capítulos posteriores, tales como cuestiones jurisdiccionales y la naturaleza de la ley local, estatal, nacional e internacional que regula el comportamiento en línea. El capítulo concluye con una propuesta para formar luchadores en contra del crimen cibernetico a todos los niveles (no sólo profesionales de las tecnologías y agentes de la policía, sino también miembros de otras partes del sistema de justicia penal, legisladores y la comunidad en general) y explica cómo un esfuerzo conjunto es el único modo en que seremos capaces de restarle un “byte” significativo al crimen cibernetico.

El Capítulo 2 “Resumiendo la Historia del Crimen Cibernetico” retrocede para tomar una perspectiva histórica. El crimen cibernetico no “apareció” de la noche a la mañana, pero no hay duda de que proporcionalmente hay más actividad criminal en línea hoy que en los primeros años de la Internet. Este capítulo intenta analizar las razones del aumento de la tasa criminal en este “sitio” llamado ciberespacio, siguiendo de cerca el tremendo crecimiento de la Net desde sus orígenes en los años 1960 hasta su encarnación actual como una fuerza sociológica y comercial muy importante que abarca todo el mundo. Observamos cómo ambas, la tecnología en sí y la estructura demográfica de la Internet, han cambiado con el paso de los años, y cómo eso (junto al gran número de personas que se

conectan cada año) han contribuido al problema del crimen. Este capítulo aborda además las formas en las cuales el advenimiento de nuevas tecnologías le facilita la vida a los criminales, no sólo a nosotros.

El Capítulo 3 “Comprendiendo a las Personas en la Escena” rompe momentáneamente con la concentración en cuestiones tecnológicas y legales para explorar el elemento humano del crimen cibernético. Aquí ahondamos en el fascinante nuevo campo de la *psicología cibernética*, el estudio de la conducta humana en el ciberespacio. Primero analizamos a los criminales cibernéticos: motivaciones comunes, tipos de personalidades y las diferencias entre aquellos que cometen diferentes tipos de crímenes cibernéticos. Observamos el arte y la ciencia de crear perfiles criminales y cómo se puede aplicar esto a los infractores de la ley en línea. Pero no nos detenemos aquí. Los criminales no son los únicos en la escena del crimen cibernético a quien los investigadores necesitan comprender. Analizamos también cómo aplicar los principios de la victimología a aquellos que son presas de los criminales cibernéticos y cómo un entendimiento de esos principios puede ayudar a predecir la conducta de los criminales, contribuir al arresto de los mismos, a la vez que ayuda a impedir que otros sean víctimas en el futuro. Posteriormente nos concentramos en el investigador del crimen cibernético. Aquí aprenderá acerca de las características que contribuyen a ser un buen detective cibernético y las aptitudes requeridas para realizar este trabajo. Finalmente, analizamos brevemente el papel desempeñado por ejecutivos y gerentes de compañías en los casos de crímenes cibernéticos que involucran redes corporativas, y cómo el personal directivo puede brindar un importante servicio actuando como enlace entre los agentes de la ley y el personal informático.

El Capítulo 4 “Comprendiendo los Principios Básicos de la Computación” lo sumerge primeramente en los detalles técnicos de cómo funcionan las computadoras. Le brindamos un curso de “pista rápida” (o para algunos lectores un resumen) sobre los principios básicos del hardware de las computadoras, explicando el lenguaje binario usado por las máquinas para procesar la información y comunicarse con otra, y describimos cómo funciona el software, en especial el sistema operativo, como “intermediario” entre el usuario y la máquina. Cada sección de este capítulo incluye un subtítulo titulado “Por qué le Concierno Esto al Investigador”, el cual explica la significación de la información al conducir una investigación criminal.

El Capítulo 5, titulado “Comprendiendo los Principios Básicos de la Interconexión” es una continuación natural de la información del capítulo precedente. Aquí nos concentramos en las comunicaciones de redes, describiendo cómo funcionan y presentándole los componentes del hardware y del software que hacen esto posible. Usted aprende acerca de la función del hardware de interconexión (concentradores, conmutadores, enrutadores y más) y se informa acerca del software del servidor y del cliente, de los sistemas de ficheros de la red y los protocolos. Finalmente, nos centramos aún más en la suite de protocolo TCP/IP que forma la base de las comunicaciones en Internet y en la mayoría de las grandes redes de la actualidad. Usted aprenderá sobre direccionamiento, enrutamiento y resolución de nombres y cómo se pueden usar las utilidades del TCP/IP para obtener información acerca de la red. Una vez más, brindamos las secciones “Por qué le Concierno Esto al Investigador” para relacionar los detalles técnicos con el trabajo de un luchador contra el crimen cibernético.

El Capítulo 6 “Comprendiendo los Ataques y las Intrusiones en la Red” aborda un tipo específico de crimen cibernético - el tipo que generalmente es cometido por criminales con mayores habilidades técnicas (aunque aprenderá cómo los “script kiddies”, con aptitudes y conocimientos limitados, pueden emprender también estos ataques usando herramientas proporcionadas por hackers más sofisticados). Este capítulo examina las actividades que realiza un hacker antes de la intrusión en lo que ella o él se prepara para atacar, y después continúa con los métodos que utilizan los hackers para conseguir entrar en las redes y/o derribarlas. Incluimos una sección sobre el crackeo de contraseñas y analizamos los diferentes tipos de explotaciones técnicas que usan las características de aplicaciones comunes, sistemas operativos y protocolos para crear la Negación de Servicio y otros trastornos en la red.

A lo largo del libro, ofrecemos varias notas breves para complementar el texto principal. Además de las notas explicativas, incluimos lo siguiente:

Estadísticas Cibernéticas: Estas notas breves brindan información estadística sobre el tópico en cuestión.

Deteniendo el crimen: Estas notas breves brindan información sobre las herramientas y técnicas que se pueden usar para prevenir o detectar los crímenes cibernéticos.

Reseña de la Ley Cibernética: Estas notas breves abordan aspectos legales del asunto analizado en el texto, incluyendo estatutos afines y citas de leyes relacionadas con el caso.

En la escena: Estos son acontecimientos reales de investigadores de crímenes cibernéticos y consejos basados en la experiencia en este campo.

Encontrará una gran cantidad de citas de otras fuentes a medida que avance con el texto. Este libro fue hecho con la intención de que sirva como un manual de referencia, y yo quería crear algo que se pudiera usar como un texto para cursos introductorios sobre crímenes cibernéticos (incluyendo aquellos que planeo dar), pero además quería que fuera ameno e interesante, no un libro de texto con un estilo académico árido. Traté de ser específica en los conceptos. Quiero que los lectores capten la “idea general”, no sólo el modo de implementar varias soluciones de seguridad y cómo usar varias técnicas forenses. Las leyes y las técnicas cambiarán con el paso de los años, pero los conceptos que conforman la base de la lucha contra el crimen cibernético seguirán siendo los mismos.

Debido a la naturaleza dinámica de la World Wide Web (www.), algunos de los recursos en línea aquí citados podrían haber desaparecido o haber sido reubicados en el momento en que Usted lea este libro. Infórmenos, por favor, si hay algún vínculo discontinuado y trataremos de encontrar nuevas fuentes para la misma información, o al menos similar, y las pondremos en nuestro sitio Web www.sceneofcybercrime.com o en el sitio Web de nuestra Editorial www.syngress.com/solutions. Me puede escribir a la siguiente dirección electrónica: debshinder@sceneofcybercrime.com.

Finalmente, quería que este fuera un libro *amistoso*, un libro que pudiera ser disfrutado por “gente sencilla” interesada en la ciencia forense aplicada a la computación y el crimen cibernético, así como también por los profesionales de los campos policial y tecnológico.

Espero haberlo logrado. Mi deseo es que Usted lo disfrute tanto al leerlo como yo lo hice al escribirlo y que lo ayude a reflexionar acerca de la constante naturaleza evolutiva de las leyes y la tecnología - de la misma forma en que me obligó a pensar (una y otra vez) en muchas de mis propias ideas acerca de “cómo funcionan las cosas” cuando las llevé a palabras.

Índice

Prólogo	1
Capítulo 1 Enfrentando el Problema del Crimen Cibernético con la Cabeza bien Puesta	16
Definiendo el Crimen Cibernético	
Clasificando por Categorías el Crimen Cibernético	
Combatiendo el Crimen Cibernético	
Capítulo 2 Repasando la Historia del Crimen Cibernético	59
Explorando la criminalidad en los tiempos de las computadoras como estaciones de trabajo individuales	
Comprendiendo a los primeros phreakers, hackers y crackers	
Cómo los servicios en línea facilitaron el crimen cibernético	
Introduciendo la ARPANet: El oeste salvaje de la interconexión	
Observando el incremento de los crímenes a partir de la comercialización de la Internet	
Actualizando la historia del crimen cibernético	
Capítulo 3 Comprendiendo a las Personas en la Escena	100
Comprendiendo a los Criminales del Ciberespacio	
Comprendiendo a las Víctimas del Ciberespacio	
Comprendiendo a los Investigadores del Ciberespacio	
Capítulo 4 Comprendiendo los Principios Básicos de la Computación	149
Comprendiendo el Hardware de la Computadora	
Comprendiendo el Lenguaje de la Máquina	
Comprendiendo los Sistemas Operativos de la Computadora	
Capítulo 5 Comprendiendo los Principios Básicos de la Interconexión	199
Comprendiendo Cómo las Computadoras se Comunican en una Red	
Comprendiendo los Protocolos TCP/IP Utilizados en Internet	
Capítulo 6 Comprendiendo las Intrusiones y los Ataques a Redes	273
Comprendiendo las intrusiones y los ataques a redes	
Reconociendo las actividades preataque	
Comprendiendo el crackeo de contraseñas	
Comprendiendo las explotaciones técnicas	
Atacando con troyanos, virus y gusanos	
Hackeando para no especialistas en tecnologías	
Desplegando un equipo de respuesta a incidentes	

SYNGRESS
LIBROS DE SHINDER

**1 AÑO DE PERFECCIONAMIENTO
PLAN DE PROTECCION AL CONSUMIDOR**

LA ESCENA DEL CRIMEN CIBERNÉTICO
Manual para Forenses de la Computación

Llevando a los Criminales Cibernéticos a la Justicia

- **Proteja su negocio, su casa, sus empleados y su familia de convertirse en blancos fáciles**
- **Aprenda técnicas para recopilar y preservar la evidencia digital**
- **Cientos de reseñas sobre la Ley Cibernética, anécdotas En la Escena y estadísticas cibernéticas**

Debra Littlejohn Zinder
Ed Tittel Revisor Técnico

solutions@syngress.com

Con más de 1,500.000 copias publicadas de nuestras guías de estudio de MCSE, MCSD, CompTIA y Cisco, continuamos buscando vías más eficaces de satisfacer las necesidades de información de nuestros lectores. Una forma en la que lo hacemos es escuchando.

Lectores como Usted nos han dicho que quieren un servicio en Internet que extienda y realce el valor de nuestros libros. Basados en las reacciones de nuestros lectores y en nuestro propio plan estratégico, hemos creado un sitio Web que esperamos supere Sus expectativas.

Solutions@syngress.com es una fuente de tesoros interactiva de útil información que se centra en los tópicos de nuestros libros y las tecnologías afines. El sitio ofrece los siguientes atractivos:

- Un año de garantía contra obsolescencia del contenido debido a actualizaciones del producto por parte del vendedor. Usted puede acceder a actualizaciones en línea para cualquier capítulo afectado.
- Formularios de dudas del consumidor “Pregúntale al autor” que le permiten enviar preguntas a nuestros autores y editores.
- Correos mensuales exclusivos en los que nuestros expertos dan respuestas a dudas de los lectores y explicaciones claras sobre complejas materias.
- Vínculos regularmente actualizados a sitios especialmente seleccionados por nuestros editores para brindarle a los lectores la deseada información adicional confiable sobre temas claves.

Lo mejor de todo, el libro que Usted está ahora sosteniendo, es la clave para este increíble sitio. Sólo vaya a **www.syngress.com/solutions** y déjelo a mano al registrarse para verificar su adquisición.

Gracias por darnos la oportunidad de satisfacer Sus necesidades. Y asegúrese de hacernos saber si hay algo más que podamos hacer para ayudarle a alcanzar el valor máximo de su inversión. Estamos escuchando.

[www. syngress.com/solutions](http://www.syngress.com/solutions)

SYNGRESS®

SYNGRESS®

**1 AÑO DE PERFECCIONAMIENTO
PLAN DE PROTECCION AL CONSUMIDOR**

LA ESCENA DEL CRIMEN CIBERNÉTICO
Manual para Forenses de la Computación

Debra Littlejohn Zinder
Ed Tittel
Editor Técnico

La Compañía Editorial Syngress, el o los autores y cualquier persona o empresa involucrada en la redacción, edición o producción (en conjunto “creadores”) de este libro (“The Work”) no garantizan o aseguran los resultados a obtener del mismo.

No existe garantía alguna, explícita o implícita, con respecto a “The Work” o su contenido. Éste se vende COMO ES y SIN GARANTÍA. Usted puede tener otros derechos legales, los que varían de estado a estado.

Los creadores no serán, en ningún caso, responsables de Sus perjuicios, incluyendo pérdida de ganancias, ahorros desperdiciados u otros daños que puedan surgir como consecuencia de “The Work” o su contenido. Debido a que algunos estados no permiten la exclusión o limitación de responsabilidad en caso de perjuicios resultantes o incidentales, la limitación anterior podría no aplicar en Su caso.

Usted debe tener siempre especial cuidado, incluyendo copias de seguridad y otras precauciones apropiadas, al trabajar con computadoras, redes, datos y ficheros.

Syngress Media®, Syngress®, “Career Advancement Trough Skill Enhancement®”, “Ask the Author UPDATE®”, son marcas registradas de la Compañía Editorial Syngress. “Mission Critical™”, “Hack Proofing®”, y “The Only Way to Stop a Hacker is to Think Like One™” son marcas de la Compañía Editorial Syngress. Las marcas y los nombres de productos mencionados en este libro son marcas de fábrica o de servicio de sus respectivas compañías.

Clave	Número de serie
001	JG9H7GYV83
002	R2UV7T5CVF
003	HJ9HFSCX3A
004	9MB76N679Y
005	U8NLT5R33S
006	X5L7NC4ES6
007	G8D4EB42AK
008	9BKMvc6RD7
009	SGWKP7V6FH
010	5BVfJm39Z

PUBLICADO POR:
Compañía Editorial Syngress
800 Hingham Street
Rockland, MA 02370

La Escena del Crimen Cibernético: Manual para Forenses de la Computación.

Copyright © 2002 por la Compañía Editorial Syngress. Todos los derechos reservados. Impreso en los Estados Unidos de América. Con excepción de lo permitido en la Ley de Derechos de Reproducción de 1976, parte alguna de esta publicación podrá ser reproducida o distribuida en forma alguna y por motivo alguno, o almacenada en una base de datos o sistema de recuperación de datos sin previa autorización por escrito del editor, con la excepción de que los listados del programa pueden ser introducidos, almacenados y ejecutados en un sistema computarizado, pero no pueden ser reproducidos para publicación.

Impreso en los Estados Unidos de América
1 2 3 4 5 6 7 8 9 0

Número del Libro por el Standard Internacional: 1-931836-65-5

Editor técnico: Ed Tittel Diseñador de portada: Michael Kavish

Editor de adquisiciones: Andrew Williams

Editora del desarrollo: Kate Glennon

Diseño de página y arte por: Ediciones personales

Editora de copias: Marlene Bordwell

Índice: Claire A. Splan

Distribuido por Publishers Group West en los Estados Unidos y por Jaguar Book Group Jaguar en Canadá.

Reconocimientos

Nos gustaría reconocer a las siguientes personas por su amabilidad y apoyo para hacer posible este libro.

Richard Kristof y Duncan Anderson de Global Knowledge (Consultores en gestión del conocimiento) por darnos, tan generosamente, acceso a los mejores cursos de la industria de la informática, instructores y facilidades de capacitación.

Ralph Troupe, Rhonda St. John y el equipo de Callisma por su invaluable perspicacia en el desafío de diseñar, utilizar y mantener redes de empresas de clase mundial.

Karen Cross, Lance Tilford, Meaghan Cunningham, Kim Wylie, Harry Kirchner, Kevin Votel, Kent Anderson, Frida Yara, Bill Getz, Jon Mayes, John Mesjak, Peg O'Donnell, Sandra Patterson, Betty Redmond, Roy Remer, Ron Shapiro, Patricia Kelly, Andrea Tetrick, Jennifer Pascal, Doug Reil y David Dahl de Publishers Group West por compartir su increíble experiencia y pericia en el campo del marketing.

Jacquie Shanahan, AnHelen Lindeholm, David Burton, Febea Marinetti y Rosie Moss de Elsevier Science por hacer realidad que nuestra visión permanezca en la mira mundial.

Annabel Dent y Paul Barry de Elsevier Science /Harcourt Australia por toda su ayuda.

David Buckland, Wendi Wong, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan y Joseph Chan de Transquest Publishers por el entusiasmo con el que recibieron nuestros libros.

Kwon Sung June de Acorn Publishing por su apoyo.

Jackie Gross, Gayle Voycey, Alexia Penny, Anik Robitaille, Craig Siddall, Marlene Morrow, Iolanda Miller, Jane Mackay y Marie Skelly de Jackie Gross & Asociados por toda su ayuda y entusiasmo representando nuestro producto en Canadá.

Lois Fraser, Connie McMenemy, Shannon Russell y el resto de los buenos amigos de Jaguar Book Group por su ayuda en la distribución de libros Syngress en Canadá.

¡Una especial bienvenida a la gente de Woodslane en Australia! Gracias a David Scott y a todos allí pues comenzamos vendiendo títulos Syngress a través de Woodslane en Australia, Nueva Zelanda, Papúa Nueva Guinea, Fiji Tonga, Islas Salomón y las Islas Cook.

Reconocimientos de la Autora y Dedicatorias

Puede o no hacer falta un pueblo para educar a un niño, pero estoy segura de que hace falta una red entera de personas, a través del tiempo y del globo, para llevar a cabo un libro como este. Un autor, como un padre, siente una cierta sensación de propiedad sobre el producto final, pero no hubiese podido hacerlo sola y estoy contenta de no haber tenido que hacerlo.

Este libro es la culminación de tres vocaciones aisladas pero a la vez ligadas a las que me he dedicado durante mi vida: el trabajo policial, la interconexión de computadoras y la escritura. Dicen que al final, la última debería ser la primera y esto fue y es verdad en mi caso. Ser una escritora profesional fue una de mis primeras aspiraciones. Tiempo atrás, cuando estaba en 8vo. Grado, garabateé mi primera (mal escrita pero en cierto modo completa) novela de 300 páginas en un cuaderno de notas y se la presté a mis amigos como si fuera una biblioteca de una sola persona. Continué escribiendo y edité mis periódicos del preuniversitario y de la universidad, y es con los profesores y amigos quienes alentaron mis ambiciones entonces, con los que tengo mi primera deuda de gratitud: Bobbie Ferguson, Michael Britton y Barbara Gifford Brown, dondequiera que estén ahora, gracias.

Nunca desistí de aquel sueño, pero el tipo de escritura que hacía antes no pagaba mis cuentas, así que seguí los pasos de mi padre hacia el trabajo gubernamental y terminé enamorándome de la labor policial y siguiendo aquel sendero durante la tercera década de mi vida. Sin mi experiencia como oficial de la policía e instructora de la Academia de Policías, éste sólo sería otro libro técnico, así que quiero agradecer a algunos de los que hicieron todo eso posible: Larry Beckett, Sarah Whitaker, Danny Price, Marty Imvalle, Mike Walker, Patt Scheckel-Hollingsworth, Lin Kirk Jones y Neal Wilson.

Disfruté ser una policía, pero a medida que fui envejeciendo, descubrí que había otra cosa que disfrutaba mucho más aún -y, era, además, más fácil para el cuerpo y mejor pagado. Durante mucho tiempo he sido una aficionada de la computación (mi vieja VIC-20 y la Commodore 64 todavía están aquí en un estante alto en el closet) y tras conocer a mi esposo en línea, juntos montamos nuestra red en la casa y estudiamos juntos para convertirnos en MCSE. Él estaba tan cansado de la medicina como yo del trabajo policial y cuando llegó el momento de buscar una nueva carrera que pudiéramos compartir, la solución fue obvia. El mundo de la tecnología nos atrajo. Prestamos servicio de asesoramiento por un tiempo y después comenzamos a enseñar. Hubo muchos que nos ayudaron en el camino: Cash Traylor, Johnnie e Irene en Eastfield, Thomas Lee y todos los de la lista Saluki, David (gato negro) Smith y la pandilla de DigitalThink, Donna Gang de Technology Partners y todos nuestros estudiantes en los programas de MCSE.

A pesar de todo, escribir era aún mi pasión secreta. Cuando llegó la oportunidad de escribir libros técnicos, parecía que mi vida se había completado. Por darme esa oportunidad, tengo que agradecerle a la gente de Syngress y a Dave Dusthimer de Cisco Press. Muchas personas contribuyeron al éxito de mi carrera como escritora y a la de Tom, en especial, Julie, Maribeth, Kitty, Carl, nuestros editores técnicos y más que todo, los lectores que compraron los libros.

Lo que nos trajo a este libro. Tuve una gran cantidad de aportaciones y ayuda de muchos rincones, las que le añadieron valor e hicieron más fácil y entretenida la redacción: Andrew Williams que lo hizo posible; James Michael Stewart, quien, sin sus contribuciones a los capítulos 8 y 9, este libro no se hubiese terminado en tiempo; el editor técnico Tittel y la editora de desarrollo Kate Glennon, cuyos comentarios y preguntas me mantuvieron alerta. También quiero agradecerle a David Rhoades de Maven Security por la información acerca de las “click kiddies” y a todos los oficiales de la policía que compartieron sus experiencias y su pericia en el campo del crimen cibernético, en especial, Wes Edens, Glen Klinkhart, Dave Pettinari, Troy Lawrence, Bryan Blake, Dean Scoville, Robert Bell, Bud Levin y Robert S. Baldygo, James Rogers, Bob Foy, Michael J. West, Tom Burns e Ira Wilsker.

Finalmente (y lo primero debería ser lo último) hubo muchos amigos y miembros de la familia que me dieron aliento a través del camino. Este libro está dedicado a Tom (mi esposo, mi mejor amigo, mi socio, quien también escribió parte de la sección sobre resolución de nombres en el capítulo 5), Kris y Kniki (los dos mejores chicos del mundo), mamá, papá (a quienes aún extraño cada día), Jeff Tharp (uno de los pocos amigos que realmente sí se mantuvo en contacto después de mudarse lejos), todos los Piglets (en especial Bob, Lash, Dee, Robert, Shawn, el socio, el rey de las hamburguesas, el jefe Al, MikeO y la “señora V, dondequiera que estés”), la pandilla del MarketChat, los contadores de historias, los escritores parlanchines y todos los roedores de tallas inusuales que aparecen en la CBP y listas afines.

-Debra Littlejohn Shinder

Autora

Debra Littlejohn Zinder es una ex-sargento de policía e instructora de Academia de Policías devenida profesional de las tecnologías de la información. Ella y su esposo, el Dr. Thomas W. Zinder, han brindado servicios de asesoría de redes a empresas y municipalidades; han dirigido cursos de capacitación en universidades y centros de capacitación técnica, y han expuesto en seminarios alrededor del país. Deb se especializa en redes y seguridad. Ella y Tom han escrito numerosos libros, incluyendo el best seller *Configurando el ISA Server 2000* (Editorial Syngress, NLSI: 1-928994-29-6) y Deb es la única autora de *Fundamentos de Redes de Computadoras*. Ella es además la autora de más de 100 artículos de publicaciones impresas y revistas electrónicas tales como *TechProGuild*, *CNET*, *8Wire* y *Cramsession*; es miembro del Consejo Editorial de la Revista *Police Crisis Negotiations* y del Consejo Asesor del Centro de Capacitación de Justicia Penal de la Universidad de Eastfield.

Editor Técnico y Contribuyente

Ed Tittel es un veterano con 20 años de trabajo en la industria de la computación, quien ha laborado como programador, ingeniero de sistemas, gerente técnico, escritor, asesor y entrenador. Un contribuyente a más de 100 libros de computación. Ed creó las series *Exam Cram* de guías para la certificación. Además escribe para numerosos sitios Web y revistas acerca de temas de certificación, incluyendo *InformIT.com*, las revistas *Certification* e *IT Contractor* y sitios de búsqueda de información técnica (www.searchsecurity.com, www.searchnetworking.com, www.searchWin2000.com, www.searchWebManagement.com). Cuando no está ocupado escribiendo, investigando o enseñando, le gusta jugar billar, consumir el vaso ocasional de vino tinto y pasear a su perro labrador Blackie.

Contribuyentes

James Michael Stewart (MCSE, CCNA, CISSP, TICSa, analista de seguridad CIW) es un escritor, investigador y entrenador, que se especializó en tópicos de certificación relacionados con las redes y la seguridad. Un contribuyente a más de 75 libros. Lo más reciente ha sido su contribución a títulos que abordan tópicos sobre CISSP, TICSa, Windows 2000 y Windows XP. Dos veces al año también imparte clases para NetWorld + Interop, donde ofrece cursos sobre seguridad, optimización y ajuste del rendimiento de Windows. En su tiempo libre, Michael es un ferviente hacedor de trabajos manuales tales como albañilería y carpintería, esquiador acuático, viajero del mundo y un patón (fundamentalmente en el paso doble).

Michael Cross (MCSE, MCP+I, CNA, Network+) es un especialista en Internet y un programador del Servicio de Policía Regional del Niágara que ha prestado servicio además como administrador de redes del mismo. Michael lleva a cabo exámenes forenses en computadoras involucradas en investigaciones criminales y ha consultado y ayudado en casos lidiando con delitos de Internet o crímenes por ordenador. Es responsable del diseño y mantenimiento del sitio Web del servicio de policía antes mencionado www.nrps.com y de dos versiones de su Intranet (una usada por las estaciones de trabajo y otra con acceso a través de las patrullas). Él programa aplicaciones usadas por varias unidades del Servicio de Policía; ha sido responsable de la seguridad y administración de las redes y continua ayudando en este aspecto. Michael es parte de un equipo de especialistas de la Informática que brinda apoyo a una base de usuarios de más de 800 usuarios civiles y uniformados. Su teoría es que cuando los usuarios portan armas, Usted tiende a estar más motivado a resolver sus problemas.

Antes de trabajar para el Servicio de Policía Regional del Niágara, Michael trabajó como instructor en universidades privadas y escuelas técnicas en Londres, Ontario, Canadá. Fue durante el período en el que fue reclutado como escritor de la Editorial Syngress y se convirtió en un miembro regular del equipo de redacción. Es además dueño de KnightWare, una compañía que diseña páginas Web y brinda otros servicios. Actualmente reside en Saint Catharines, Ontario, Canadá, con su encantadora esposa Jennifer.

Enfrentando el Problema del Crimen Cibernético con la Cabeza bien Puesta

Tópicos que investigaremos en este capítulo:

- **Definiendo el crimen cibernético**
- **Clasificando el crimen cibernético por categorías**
- **Combatiendo el crimen cibernético**

- ✓ **Resumen**
- ✓ **Preguntas Realizadas con Frecuencia**
- ✓ **Referencias**

Introducción

Hoy día vivimos y trabajamos en un mundo de conectividad global. Podemos intercambiar una conversación casual o realizar transacciones monetarias de varios millones de dólares con personas de otras partes del planeta de forma rápida y económica. La proliferación de computadoras personales, el fácil acceso a Internet y un mercado en auge para nuevos dispositivos de comunicación afines han cambiado la manera en que pasamos nuestro tiempo libre y hacemos negocios.

Las formas en que los criminales cometen crímenes también están cambiando. La accesibilidad digital universal crea nuevas oportunidades para los inescrupulosos. Ambas partes, los negocios y los consumidores, han perdido millones de dólares a causa de criminales con habilidades técnicas para la computación. Peor, las computadoras y las redes se pueden usar para acosar víctimas o prepararles violentos ataques – incluso para coordinar y llevar a cabo actividades terroristas que constituyen una amenaza para todos nosotros. Desafortunadamente, en muchos casos, las agencias policiales han estado a la zaga de estos criminales, careciendo de la tecnología y del personal capacitado para encarar esta nueva y creciente amenaza, que ha sido certeramente clasificada como *crimen cibernético*.

Hasta hace muy poco, muchos profesionales de la informática carecían de conciencia e interés en el fenómeno del crimen cibernético. En muchos casos, los oficiales de la policía no contaban con las herramientas necesarias para enfrentar el problema; las viejas leyes no se correspondían en lo absoluto con los crímenes que se estaban cometiendo, las nuevas no estaban para nada al nivel de la realidad de los acontecimientos, y sólo había unos pocos precedentes de tribunales por los cuales guiarse. Además, los debates sobre cuestiones privadas obstaculizaban la capacidad de los agentes del orden para recopilar la evidencia necesaria a fin de enjuiciar estos nuevos casos. Finalmente, había una cierta antipatía - o, al menos, desconfianza - entre los dos jugadores más importantes de cualquier lucha efectiva contra el crimen cibernético: los agentes del orden y los profesionales de la computación. Sin embargo, una estrecha cooperación entre ambas partes es crucial si queremos controlar el problema del crimen cibernético y hacer de Internet un “lugar” seguro para todos sus usuarios.

Los agentes del orden entienden el modo de pensar de los criminales y conocen los principios básicos de la recopilación de evidencias y del enjuiciamiento de los infractores. El personal informático entiende a las computadoras y las redes, cómo funcionan y cómo rastrear información en ellas. Cada parte tiene la mitad de la clave para derrotar al criminal cibernético. El objetivo de este libro es juntar ambos elementos, demostrar que ambos pueden y deben trabajar en conjunto en aras de defenderse, apresar y enjuiciar a aquellas personas que usan la tecnología moderna para acosar a individuos, organizaciones, negocios y a la sociedad.

Cuantificando la Crisis

Crimen cibernético: Suena exótico, al material con que están hechas las novelas futuristas de ciencia ficción. Sin embargo, los oficiales de la policía, los administradores de redes y

otros que lidian con el crimen y/o el ciberespacio están descubriendo que el futuro es ahora y que el crimen cibernético es un gran y creciente problema. Por ejemplo:

- De acuerdo con el *Internet Fraud Complaint Center, IFCC* (Centro de Quejas de Fraudes Electrónicos), una asociación entre el Buró Federal de Investigación (FBI) y el *National White Collar Crime Center* (Centro Nacional contra los Delitos de Cuello Blanco), entre mayo del 2000 y mayo del 2001, su primer año de operación, el sitio Web del *IFCC* recibió 30,503 quejas de fraude electrónico. (El reporte se puede descargar íntegramente en formato PDF desde www1.ifccfbi.gov/strategy/IFCC_Annual_Report.pdf.)
- De acuerdo con el *Sondeo sobre Seguridad y Crimen por Ordenador* realizado en el 2001 por el *Computer Security Institute* (Instituto para la Seguridad Electrónica) conjuntamente con el *Computer Intrusion Squad* (Escuadrón de Intrusiones en Cómputo del FBI), 186 agencias gubernamentales y sociedades anónimas encuestadas reportaron pérdidas financieras de un total de más de 3,5 millones de dólares, debido principalmente al robo de información propietaria y al fraude financiero (véase www.gocsi.com/press/20020407.html).
- De acuerdo con el *Cybersnitch Voluntary Online Crime Reporting System* (Sistema de Reportes Voluntarios de Crímenes en Línea Cybersnitch), los crímenes relacionados con Internet comprenden desde la falsificación de escritorios hasta la pornografía infantil e incluyen crímenes potencialmente violentos tales como el acoso electrónico y amenazas terroristas. (Una lista completa de crímenes cibernéticos reportados está disponible en www.cybersnitch.net/csinfo/csdatabase.asp).
- De acuerdo con la Consultora *Meridien Research*, según reportes de epaynews.com (www.epaynews.com/statistics/fraud.html), el costo del fraude en Internet se espera alcance la suma de entre 5 y 15 billones de dólares para el año 2005.

Aunque casi nadie tiene el potencial para ser afectado por el crimen cibernético, dos grupos de personas deben lidiar con este fenómeno cada vez con más frecuencia:

- Los profesionales de la informática, quienes son, la mayoría de las veces, los responsables de crear la primera línea de defensa y de descubrir el crimen cibernético cuando ocurre.
- Los profesionales de la ley y el orden, quienes son los responsables de lidiar con toda una serie de cuestiones legales, jurisdiccionales y prácticas en sus intentos de imponer justicia a los criminales cibernéticos.

Estadísticas cibernéticas.....

Registrando el Récord de Explosión Poblacional en Línea

Los Sondeos Nua de Internet mostraron que a partir de febrero del año 2002 aproximadamente 544 millones de personas en todo el mundo se conectaron a Internet. A medida que aumente el número de personas conectadas en el mundo, se expandirán las

oportunidades de que los criminales usen la Net para violar la ley, y el crimen cibernético afectará cada vez a mayor cantidad de personas.

A pesar de que es imperativo para el éxito de cualquier guerra contra el crimen cibernético que estos dos grupos trabajen en conjunto, ellos, a menudo, se siguen enfrentando porque ninguno tiene un entendimiento real de lo que hace el otro o del alcance de sus propios roles en el proceso de lucha contra el crimen cibernético.

Definiendo el Crimen Cibernético

Puede que Usted no encuentre en su diccionario el término *crimen cibernético* (irónicamente no aparece siquiera en el *Diccionario Mundial Encarta de 2001* de Microsoft, un diccionario electrónico, como puede ver en la figura 1.1). Sin embargo, una búsqueda en la Web de estas palabras, utilizando el popular motor de búsqueda Google, revela más de 140,000 resultados.

Probablemente no sepamos oficialmente qué es el crimen cibernético, pero todos están hablando de ello. Aún sin una definición en el diccionario, legisladores y agentes del orden de todas partes del mundo parecen creer del crimen cibernético que “lo reconocen cuando lo ven”, como dijera el juez de la Corte Suprema de los Estados Unidos Potter Stewart cuando habló de obscenidad en 1964. Se han aprobado en todas las jurisdicciones leyes que encaran el crimen en línea y aquellos que redactan y hacen cumplir las leyes, tras un lento comienzo, están entrando en acción para enfrentar el problema.

Los departamentos de policías de los Estados Unidos y del resto del mundo están creando unidades contra los crímenes por ordenador, y el crimen cibernético constituye una gran proporción de los delitos investigados por esas unidades. La *National Cybercrime Training Partnership NCTP* (Asociación Nacional de Entrenamiento contra el Crimen Cibernético) reúne agencias de policía locales, estatales y federales. La *International Association of Chiefs of Police IACP* (Asociación Internacional de Jefes de Policía) auspicia una conferencia anual de capacitación para el Manejo de la Información Policial que centra su atención en la seguridad informática y el crimen cibernético. La Unión Europea ha creado un cuerpo llamado el Forum del Crimen cibernético, y un número de estados europeos ha suscrito el Tratado sobre el crimen cibernético del Consejo de la Convención Europea, el cual intenta estandarizar las leyes europeas en lo concerniente al crimen en Internet.

Figura 1.1 El término *crimen cibernético* no aparece en la mayoría de los diccionarios, incluyendo el diccionario electrónico Encarta de Microsoft.



Cada organización y los autores de cada disposición legislativa tienen sus propias ideas de lo que es el crimen cibernético –y de lo que no es. Estas definiciones pueden variar poco o mucho. Para analizar de forma efectiva el crimen cibernético en este libro, sin embargo, necesitamos una definición básica. Con este fin comenzamos con una definición amplia, general y después definimos los delitos de los criminales cibernéticos de forma específica.

Yendo de lo General a lo Específico

El crimen cibernético se puede definir generalmente como una subcategoría del crimen por ordenador. El término se refiere a los delitos criminales cometidos mediante el uso de Internet u otra red de computadoras como un componente del crimen. Las computadoras y redes pueden estar involucradas en crímenes de muchas formas diferentes:

- La computadora o la red pueden ser la herramienta del crimen (usada para cometer el crimen)
- La computadora o la red pueden ser el blanco del crimen (la “víctima”)
- La computadora o la red pueden ser usadas con propósitos incidentales relacionados con el crimen (por ejemplo, para guardar registros de ventas de drogas ilegales)

Para que las leyes puedan hacerse cumplir, deben ser específicas. Resulta útil dar una definición general para ser usada en el análisis, pero los delitos criminales consisten en actos específicos u omisiones, conjuntamente con un estado mental culpable especificado.

En muchos casos, disposiciones legislativas específicas contienen definiciones de términos. Esto es necesario para evitar confusiones, discusiones y litigios sobre la aplicabilidad de una ley o regulación. Esas definiciones deben ser lo más minuciosas posible, pero los legisladores no siempre hacen un buen trabajo al definir términos (y, a veces, ni siquiera los

definen, dejando que los agentes del orden adivinen hasta que los tribunales finalmente toman una decisión).

Una de las críticas más grandes al Tratado Europeo es por sus definiciones demasiado generales. Por ejemplo, la definición del término *proveedor de servicio* es tan vaga que se pudiera aplicar a cualquiera que monte una red de dos computadoras en la casa, y la definición de *datos electrónicos*, debido a que se refiere a cualquier representación de hechos, información o conceptos de cualquier tipo apropiados para ser procesados en un sistema computarizado, abarcaría casi todas las formas posibles de comunicación, incluyendo los documentos escritos a mano y la expresión oral (la cuales se pueden procesar a través de un software de reconocimiento de escritura y discurso). Así mismo, el Departamento de Justicia de los Estados Unidos (DoJ) ha sido criticado por una definición de *crimen cibernético* que especifica “cualquier violación de la ley penal que involucre el conocimiento de la tecnología de la computación para su perpetración, investigación o procesamiento” (reportado en el Boletín del FBI: *FBI Law Enforcement Bulletin*, de Agosto de 2002). Con una definición como esa, virtualmente cualquier crimen se podría clasificar como un crimen por ordenador, simplemente porque un detective examine una base de datos de una computadora como parte de una investigación que esté llevando a cabo.

Estos ejemplos ilustran la dificultad de crear definiciones utilizables para el crimen cibernético y términos afines. Más adelante, en este capítulo, desarrollaremos nuestra propia definición básica de crimen cibernético para los propósitos de este libro.

Comprendiendo la Importancia de las Cuestiones Jurisdiccionales

Otro factor que dificulta llegar a una definición completa de crimen cibernético es el dilema jurisdiccional. Las leyes en diferentes jurisdicciones definen los términos de forma diferente y es importante para los oficiales de la policía que investigan el crimen cibernético, así como para los administradores de redes que quieren involucrarse en el enjuiciamiento de los crímenes cibernéticos que se han cometido en contra de sus redes, familiarizarse con las leyes aplicables. En el caso de la mayoría de los crímenes en los Estados Unidos, eso significa empaparse de las ordenanzas locales y de los estatutos del estado relacionados con el delito. Generalmente, el comportamiento criminal es una cuestión de la jurisdicción en la cual ocurre. Por ejemplo, si alguien lo asalta, Usted presentaría los cargos ante la policía local de la ciudad o del condado donde tuvo lugar en realidad dicho asalto.

Como los crímenes cibernéticos ocurren frecuentemente en el “espacio” virtual que llamamos ciberespacio, resulta más difícil saber cuáles son las leyes que aplican. En muchos casos, el victimario y la víctima están a cientos o miles de millas de distancia y podría darse el caso de que el victimario no haya puesto jamás un pie en el mismo estado o incluso en el mismo país. Debido a que las leyes pueden diferir drásticamente en diferentes jurisdicciones geográficas, un acto fuera de la ley en un lugar podría resultar legal en otro.

¿Qué podría hacer Usted si alguien en California, donde existen leyes liberales en relación con la obscenidad, pusiera a disposición de una persona en Tennessee fotos pornográficas

en Internet, donde los estándares de la comunidad que prevalecen – en los cuales se basan las leyes del Estado- son mucho más conservadores? ¿Qué estado tiene la jurisdicción? ¿Puede Usted enjuiciar exitosamente a alguien bajo la ley estatal por cometer un delito en un estado donde esa persona nunca ha estado? De hecho, este fue el tema de un caso que marcó un hito, los Estados Unidos contra Thomas y Thomas (véase la “Reseña de la Ley Cibernética” en esta sección).

Reseña de la Ley Cibernética....

Los Estados Unidos contra Thomas y Thomas

Robert y Carleen Thomas, residentes en California, fueron juzgados por violación de las leyes de obscenidad en Tennessee cuando un oficial de la policía de Memphis descargó materiales explícitamente sexuales de su Servicio de Boletín Electrónico de California (BBS) hacia una computadora en Tennessee. Esta fue la primera vez que los fiscales presentaron cargos en un caso de obscenidad en el lugar donde el material fue *descargado* en vez de en el lugar en donde ocurrió. Los acusados fueron condenados y apelaron. La Corte de Apelaciones confirmó la condena y las sentencias. La Corte Suprema de los Estados Unidos rechazó su apelación.

Incluso si el acto cometido es ilegal más allá de las jurisdicciones, puede que no encuentre quien lo quiera procesar debido a la pesadilla geográfica que significaría hacerlo (véase “En la escena” en esta sección para tener un ejemplo de la experiencia de un oficial de la policía).

Analizaremos las cuestiones jurisdiccionales mucho más profundo y detalladamente en el Capítulo 11, “Construyendo el caso de crimen cibernético”.

En la escena...

Experiencias de la Vida Real

*De Wes Edens,
Investigador Penal y Experto Forense de Computadoras*

Aquí les presentamos cómo el típico caso multi-jurisdiccional le complica la vida a un detective de la policía en activo. Póngase en el lugar de este detective: Bob Smith, quien vive en su jurisdicción en Oklahoma, reporta que ha tenido compras fraudulentas a la cuenta de su tarjeta de crédito. Además, le han informado que se han abierto dos cuentas utilizando su información vía Internet en dos bancos: Netbank, sito en Georgia y en el Wingspan, que fue recientemente comprado por Bank One.

El (los) sospechoso (s) solicitaron un préstamo para comprar un auto en Dallas, Texas. Como resultado, los sospechosos cambiaron la dirección de Bob en su perfil de crédito por 123 Somewhere Street, Dallas. Esta dirección no existe.

En el curso de su investigación, Usted contacta al Netbank (Georgia) y ellos le informan que no conservan las direcciones IP de las personas que abren cuentas en línea. Usted obtiene una copia de la solicitud de crédito en línea. Esta contiene toda la información del

saldo de Bob Smith, pero ahora la dirección es 321 Elsewhere Street, Dallas, dirección que tampoco existe.

Usted contacta a todas las compañías donde se realizaron las compras con las tarjetas de crédito falsas de Bob. La mitad no le hablará a menos que tenga documentos oficiales y la otra mitad dice que los documentos tienen que provenir de un Tribunal del estado donde ellos radican, no donde radica Usted. Ahora tiene que encontrar departamentos de policía en 5 estados diferentes dispuestos a ayudarlo a generar documentos de tribunales para obtener los registros. Como Usted no ha presentado cargos y la víctima (y probablemente el sospechoso) no viven en la jurisdicción de ellos, la mayoría de esas organizaciones estarán renuentes a involucrarse.

Usted obtiene los documentos de la mitad de las compañías. De 10, sólo una en realidad tiene una dirección IP. Es una cuenta AOL (American Online), lo que significa que pudieron tener acceso a ella desde cualquier lugar del mundo, complicando aún más la pesadilla jurisdiccional, pero Usted insiste. Consigue una orden para AOL, solicitando la información del suscriptor para esa dirección IP en aquel momento. Tres semanas después, AOL le informa que ellos conservan los registros sólo por 21 días, así que no tuvo suerte porque la fecha y la hora IP que estaba buscando ocurrió dos meses atrás.

Usted hace un resumen de los 15 números telefónicos usados para realizar las diversas solicitudes y cuentas sospechosas. Los 15 son diferentes. Tres de ellos de Dallas, dos de Fort Worth y los restantes están desconectados o son números al azar de pueblos del sur de Texas. No existe una conexión aparente entre ninguno de estos números. Usted obtiene las direcciones utilizadas para la entrega de los artículos comprados. Todas las direcciones son diferentes, tres en Dallas, dos en Fort Worth. Varias son rentas pagadas semanalmente o “albergues para vagabundos” donde la gente entra y sale como en una Terminal de ómnibus. Un par son entregas por correo. Usted notifica esos registros sólo para encontrar que toda la información que contienen es falsa.

Decide visitar a su jefe y le explica que necesita viajar a otro estado por algunos días para resolver este robo de 1500USD. Él escucha atentamente hasta que Usted comienza a mencionar ir a Georgia, Maryland y Texas. Entonces le dice que tiene además tres casos de este tipo que involucran otros nueve estados y que probablemente tendrá que ir también a todos esos lugares. Lo puede sentir reírse mientras atraviesa la puerta.

Usted decide visitar a la Fiscal del Distrito sólo por el hecho de hacerlo. Explica el caso hasta el momento y ella pregunta: ¿Qué delito se cometió aquí? (Su respuesta: “Bueno, ninguno que pueda dar por sentado.”) ¿El sospechoso vive aquí? (Probablemente no). ¿Podemos demostrar que tuvo lugar aquí algún intercambio de dinero o contacto físico entre el sospechoso y la víctima? (No, en realidad no). ¿Tiene alguna idea de dónde se encuentra el sospechoso? (Probablemente en Texas). ¿Alguna de las compras se hizo en Oklahoma? (No). ¿Por qué está llevando a cabo esta investigación? (Porque la víctima está parada en mi oficina).

La Fiscal del Distrito le dice que la víctima tiene que reportar este crimen antes las autoridades de Texas. Usted le da a la víctima una lista de siete agencias diferentes en

Texas, una en Georgia y otra en Maryland. Le dice que tiene que entrar en contacto con ellos. Él lo llama tres días más tarde y le dice que ellos quieren que vaya a cada lugar para llenar el reporte del delito y que él no puede darse el lujo de tomar dos semanas libres y viajar 2000 millas para reportar que es una víctima. Usted le sugiere llamar al FBI, aún cuando bien en lo profundo sabe que no van a tomar un caso de fraude de 1500USD.

Usted abandona el caso y toma los otros tres casos de robo de identidad que estaban sobre su escritorio mientras hilaba la rueca en este. Se da cuenta de que los tres fueron cometidos íntegramente a través de Internet y, como el primero, involucran una multitud de estados.

Diferenciando Crímenes que Usan la Net de Aquellos que Dependen de la Net

En muchos casos, los crímenes que llamaríamos crímenes cibernéticos según nuestra definición general, son realmente “los mismos de antes”, excepto que una red de computadoras está involucrada de alguna forma. O sea, una persona podría usar la Internet para ejecutar un esquema piramidal o una carta en cadena, buscar clientes para servicios de prostitución, hacer apuestas para juegos ilegales, o descargar fotos pornográficas de menores. Todos estos actos ya se califican como criminales en ciertas jurisdicciones y se podrían cometer sin el uso de una red de computadoras. El aspecto “cibernético” no es un elemento necesario del delito, sólo proporciona los medios para cometer el crimen. La red de computadoras le da a los criminales una nueva forma de cometer los mismos crímenes de antes. Los estatutos existentes que prohíben estos actos se pueden aplicar tanto a las personas que usen una computadora para cometerlos como a aquellos que los cometan sin el uso de una computadora o red.

En otros casos, el crimen es único y surgió con el advenimiento de la Internet. El acceso no autorizado es un ejemplo. Aunque pudiera asemejarse al allanamiento de morada de una casa o un negocio, los elementos que componen el acceso electrónico no autorizado y el allanamiento de morada físico son diferentes. Según la definición legal, el allanamiento de morada generalmente requiere una entrada física a un local, un elemento que no está presente en la versión del crimen en el ciberespacio. Por consiguiente, se deberán redactar nuevos estatutos prohibiendo este comportamiento específico.

Reseña de la Ley Cibernética...

Robo de Propiedad Intangible

El robo de propiedad intangible, como, por ejemplo, datos electrónicos, representa un problema dentro de los estatutos de muchas jurisdicciones estadounidenses dedicados al robo tradicional. Una definición legal común de robo es “la apropiación ilegal de la propiedad de otro sin el consentimiento efectivo del propietario con la intención de privar al dueño de su propiedad”. (Esta definición fue tomada del Código Penal de Texas, Sección 31.03).

Esta definición funciona bien con la propiedad tangible. Si yo me robo su collar de diamantes o su nueva laptop Dell, está clara mi intención de privarlo a Usted del uso de su propiedad. Sin embargo, yo puedo “robarme” los registros financieros de su compañía o

los primeros cuatro capítulos de la gran novela Americana que Usted está escribiendo *sin* privarlo para nada de la propiedad o de su uso.

Si fuese procesada en virtud del estatuto sobre robo, mi abogado defensor podría argumentar que el último elemento del delito no estaba presente.

Esta es la razón por la que se deben redactar nuevos estatutos para cubrir el robo de propiedades intangibles o intelectuales, las que no son objetos que puedan estar en poder de sólo una persona a la vez.

Las leyes de propiedad intelectual “tradicionales” (derechos de reproducción, marcas registradas, y otras por el estilo) son leyes civiles que no se enjuician en tribunales penales más que en virtud de leyes recientes especiales que contemplan tipos de propiedad intelectual definidos solamente de forma muy limitada tales como los softwares y la música. Algunas leyes federales prohíben el robo de datos, pero el FBI y agencias federales tienen jurisdicción sólo en ciertas circunstancias, tales como cuando los datos son robados de las computadoras del gobierno federal o cuando estos constituyen un secreto comercial. En la mayoría de los casos, depende del estado si se procesa. Los estados no pueden presentar cargos en virtud de la ley federal, sólo en virtud de los estatutos de sus estados. Hasta hace muy poco, muchos estados no tenían estatutos que abarcaran el robo de datos porque los estatutos para el robo tradicional no lo contemplaban y ellos no tenían estatutos para el “robo de propiedad intelectual”.

Recopilando Datos Estadísticos sobre el Crimen Cibernético

Otro problema para definir adecuadamente el crimen cibernético es la escasez de datos estadísticos concretos sobre estos delitos. Al comienzo de este capítulo, brindamos alguna información estadística recopilada por agencias formadas para lidiar con las cuestiones del crimen cibernético. Sin embargo, el reporte de crímenes a estas agencias es voluntario. Esto significa que las cifras son casi seguro mucho menores que la ocurrencia real de crímenes relacionados con redes. Esto se debe no sólo al número desconocido de crímenes cibernéticos no reportados (tal como sucede con todos los crímenes), sino a que muchos o la mayoría de los que se reportan a la policía, no se reportan a las agencias que recopilan estas estadísticas.

De hecho, actualmente resulta prácticamente imposible contabilizar de manera certera el número de crímenes cibernéticos reportados a la policía. Para comprender porqué esto es cierto, echémosle una mirada a cómo se reportan y recopilan los datos de crímenes en los Estados Unidos.

Comprendiendo el Sistema de Reporte de Crímenes

Las agencias locales reguladoras del orden – departamentos municipales de policía y oficinas del sheriff del condado – son responsables de llevar, individualmente, las estadísticas de los reportes de crímenes archivados por sus agencias, los delitos que ellos

En un esfuerzo por proporcionar estadísticas del crimen a nivel nacional, el FBI opera el programa uniforme de reporte de crímenes (*Uniform Crime Reporting UCR*). Las agencias locales reguladoras del orden completan un reporte mensual que es enviado al FBI. Esta información se consolida y expide en forma de reportes, documentando las estadísticas “oficiales” del crimen a nivel nacional. El programa se implementó desde los años 60; más de 18,000 agencias suministran datos, ya sea directamente o a través de sus sistemas estatales de reporte. Estas estadísticas se pusieron a disposición de los medios de comunicación y aparecen en el sitio Web del FBI como se muestra en la figura 1.2.

The screenshot shows a web browser window displaying the FBI's Uniform Crime Reports page. The browser's address bar shows "http://www.fbi.gov/ucr/lcr.htm". The page features the FBI seal and the title "Federal Bureau of Investigation www.fbi.gov". A navigation menu includes links like HOME, UCR TOPS, PRIVATE NOTES & LINKS, CONTACT US, SITE MAP, and SEARCH. The main heading is "Uniform Crime Reports". Under the heading "Crime in the United States", there is a list of links: Information regarding the tabulation of crime statistics, CUIS Preliminary Report, 2001, 2000, 1999, 1998, 1997, 1996, 1995, and 1994. On the left side, there are two vertical menus: one for "UCR OFFICE" listing various regional offices and another for "PRESS ROOM" with links to press releases, news tips, and contact information.

27

Clasificando por Categorías los Crímenes para el Sistema Nacional de Reportes

El NIBRS reúne más detalles sobre más categorías de crímenes que el UCR que ofrece sólo resúmenes de varias categorías de crímenes. Aún así, el grupo A con 22 categorías de delitos y el grupo B con 11 para los cuales el NIBRS recopila datos no incluye ninguna categoría que identifique un delito como un crimen cibernético. (Véase las “Estadísticas Cibernéticas” en esta sección para apreciar una lista de las categorías del NIBRS).

Estadísticas Cibernéticas

Categorías de Crímenes del NIBRS

Según el Manual del UCR (Edición del NIBRS, páginas 1-2), los delitos se dividen en los siguientes grupos de categorías. Para los delitos del grupo A se recopiló una gran cantidad de datos, mientras que para los del grupo B sólo se recopilaron datos de arrestos.

Categorías de delitos del Grupo A

1. Incendiarismo
2. Agresión (con agravantes, simple y agresión por intimidación)
3. Soborno
4. Robo / Allanamiento de morada
5. Falsificación
6. Destrucción/Daños/Vandalismo de Propiedad
7. Drogas/Delitos relacionados con narcóticos (incluyendo violaciones al equipamiento de drogas)
8. Desfalco
9. Extorsión/Chantaje
10. Fraude
11. Delitos relacionados con los juegos de azar
12. Homicidio
13. Secuestro/Rapto
14. Robo (excluyendo el robo de vehículos motorizados)
15. Robo de vehículos motorizados
16. Pornografía/Obscenidad
17. Relacionados con la prostitución
18. Atraco
19. Delitos sexuales (forzosos)
20. Delitos sexuales (no forzosos)
21. Robo de propiedad (excluyendo el hurto)
22. Violaciones de las leyes sobre el uso de armas

Categorías de delitos del Grupo B

1. Cheques sin fondos
2. Toque de queda/Merodear con fines delictivos/Vagancia

3. Conducta revoltosa
4. Conducir bajo la influencia del alcohol
5. Embriaguez
6. Delitos familiares (no violentos)
7. Violaciones de las leyes sobre el consumo de bebidas alcohólicas
8. Voyeurismo (“mirón”)
9. Fugitivo
10. Entrada sin autorización en propiedad ajena
11. Demás delitos

Como puede ver en la lista de categorías de delitos del NIBRS mostradas en la tabla, una agencia local que reporte un crimen cibernético no encontrará una categoría estándar que lo comprenda (por ejemplo, una estafa en línea que le pida a las personas enviar dinero a una “organización benéfica” con falsas pretensiones se clasificaría con el delito de fraude, mientras que acceder a los ficheros de una computadora a través de Internet y robar secretos comerciales se clasificaría como robo) o se colocaría en la categoría de Demás Delitos. Ni modo, ninguna información en los reportes nacionales de crímenes generada a partir de estos datos indica que estos delitos sean crímenes cibernéticos.

Las agencias que lidian con el crimen cibernético deben formularse sus propias categorías específicas de crimen cibernético para llevar las estadísticas internas a fin de determinar con exactitud los tipos de crímenes cibernéticos que ocurren en sus jurisdicciones. Las agencias que cuentan con oficiales con habilidades técnicas o que tienen especialistas informáticos serán capaces de hacerlo sin ayuda externa. En muchos casos, sin embargo, el personal de estas agencias locales del orden no tienen la pericia técnica para comprender las diferencias entre los diversos crímenes relacionados con redes. Los oficiales de la policía podrían entender el concepto de “hackeo”, por ejemplo, pero no serían capaces de diferenciar entre un hacker que accede de forma no autorizada a una red y uno que perturba las operaciones de la red lanzando un ataque de denegación de servicio (DoS) contra ella.

Aquí es donde los profesionales de la informática pueden trabajar con los agentes del orden para ayudar a definir de forma más clara y específica los elementos de un delito de modo que pueda ser investigado y enjuiciado adecuadamente. Las agencias podrían necesitar contratar en calidad de asesores a especialistas en seguridad informática externos y/o los oficiales podrían necesitar recibir una capacitación especializada para comprender los elementos técnicos involucrados en varios crímenes cibernéticos.

En el capítulo 11 analizaremos en detalles la relación entre los profesionales de la informática y los agentes del orden conjuntamente con más especificaciones acerca de cómo ambos pueden trabajar unidos.

Hacia una Definición Básica de Crimen Cibernético

¿Por qué es tan importante para nosotros crear una definición estándar de crimen cibernético? A menos que todos usemos las mismas definiciones - o al menos unas

substancialmente similares- resultará imposible para el personal informático, los usuarios, las víctimas, los oficiales de la policía, detectives, fiscales y jueces analizar el delito inteligentemente. Por esa razón también, seguirá siendo imposible recopilar estadísticas significativas que se puedan emplear para analizar los patrones y las tendencias criminales.

El análisis de los crímenes le permite a las agencias asignar recursos de modo más efectivo y planear sus propias estrategias para responder ante estos problemas. Resulta difícil para los jefes de agencias justificar la necesidad de un presupuesto adicional para (personal especializado, capacitación, equipos, etc.) ante los Comité de Gastos y las organizaciones gubernamentales sin datos concretos que avalen sus solicitudes. También son necesarios datos estadísticos elocuentes y definiciones estándares para educar al público sobre la amenaza que representa el crimen cibernético e involucrar a las comunidades en la lucha contra el mismo. El análisis del crimen es la base de su prevención; comprender los tipos de crímenes que están ocurriendo, dónde y cuándo y quién está involucrado es necesario a fin de crear planes de prevención efectivos.

Aún cuando no tenemos una definición estándar que invocar, vamos a ver cómo definen el crimen cibernético algunas de las autoridades más prominentes.

Estatutos Estatales y Federales de los Estados Unidos

Ya hemos mencionado la poco vasta definición de crimen por ordenador adoptada por el Departamento de Justicia de los Estados Unidos. Cada agencia federal (y las fuerzas especiales de estas agencias) tienen sus propias definiciones. Por ejemplo, el *National Computer Intrusion Squad, NCCS* (Escuadrón Nacional de Intrusiones en Cómputo) del FBI, que está encargado de investigar las violaciones a la *Computer Fraud and Abuse Act* (Ley sobre Fraude y Abuso Electrónicos), relaciona categorías específicas de crímenes relacionados con redes y computadoras que ellos investigan:

- Intrusiones a la red de telefonía conmutada pública (PSTN)
- Intrusiones a la red central de computadoras
- Violaciones a la integridad de la red
- Violaciones de privacidad
- Espionaje industrial/corporativo
- Piratería de softwares
- Otros crímenes en los que las computadoras juegan un papel primordial en la comisión del delito

El título 18 del Código de los Estados Unidos en el Capítulo 47, Sección 1030, define un número de actividades fraudulentas y relacionadas con el fraude que pueden ser procesadas bajo la Ley Federal en relación con computadoras. En su mayoría se trata de crímenes que involucran datos protegidos por la Ley Federal (tales como información de seguridad nacional), o que involucran a agencias gubernamentales, al sistema bancario/financiero o a computadoras “protegidas”, interestatales o del comercio internacional. Definir y procesar

crímenes que no estén contemplados en estas categorías es, por lo general, competencia de cada estado.

La mayoría de los estados de los Estados Unidos tienen leyes para el crimen por ordenador. Estos estatutos son generalmente impuestos por la policía local y estatal y podrían contener sus propias definiciones de términos. Por ejemplo, la sección de Crímenes por Ordenador del Código Penal de Texas define sólo un delito, la Violación de la Seguridad Electrónica (Código Penal de Texas, Sección 33.02) como “el acceso consciente a una computadora, red de computadoras o sistema computarizado sin el consentimiento efectivo del propietario”. La clasificación y el grado de penalidad del delito se incrementa de acuerdo con la suma en dólares de la pérdida que haya sufrido el dueño del sistema o el beneficio que haya obtenido el infractor.

El Código Penal de California (Sección 502), por otra parte, define una lista de 8 actos que constituyen crímenes por ordenador, incluyendo alteración, daño, cancelación o por el contrario, el uso de datos electrónicos para ejecutar un esquema con el fin de estafar; engaño, extorsión, control indebido u obtención de dinero, propiedad o datos; uso de los servicios electrónicos sin permiso; perturbación de servicios electrónicos; ayuda a otra persona a acceder ilegalmente a una computadora; o introducción de contaminantes (tales como virus) en un sistema o una red.

Por consiguiente, la definición de crimen por ordenador según la ley estatal difiere en dependencia del estado. Una vez más, la cuestión jurisdiccional saca su fea cabeza. Si la naturaleza multi-jurisdiccional del crimen cibernético no nos permite tan siquiera definirlo, ¿cómo esperamos procesarlo de un modo efectivo?

Ley Internacional: Definición de Crimen Cibernético de las Naciones Unidas

El crimen cibernético sobrepasa no sólo los límites estatales, sino también nacionales. Quizás deberíamos observar a organizaciones internacionales para dar una definición estándar del crimen.

En el Décimo Congreso de las Naciones Unidas sobre la Prevención del Crimen y el Tratamiento de los Infractores, en un taller dedicado al tema de los crímenes relacionados con redes computarizadas, el crimen cibernético se dividió en dos categorías y se definió como:

- a) Crimen cibernético en un sentido limitado (crimen por ordenador): cualquier comportamiento ilegal dirigido por medio de operaciones electrónicas que tienen como blanco la seguridad de sistemas computarizados y los datos procesados por ellos.
- b) Crimen cibernético en un sentido más amplio (crimen relacionado con computadoras): cualquier comportamiento ilegal cometido por medio de o en relación con un sistema computarizado o una red, incluyendo crímenes como posesión ilegal (y) ofrecimiento o distribución de información por medio de un sistema computarizado o una red.

Por supuesto, estas definiciones se complican con el hecho de que un acto puede ser ilegal en una nación , pero no en otra.

El documento continúa para dar más ejemplos concretos, incluyendo:

- Acceso no autorizado
- Daños a datos o programas de computación
- Sabotaje electrónico
- Intercepción no autorizada de las comunicaciones
- Espionaje electrónico

Estas definiciones, aunque no completamente definitivas, sí nos dan un buen punto de partida - uno que tiene algún reconocimiento y alguna aceptación internacionales - para determinar lo que queremos decir con el término *crimen cibernético*.

Los profesionales de la informática necesitan buenas definiciones de crimen cibernético para saber cuándo (y qué) reportar a la policía, pero las agencias establecedoras del orden *deben* tener definiciones legales de crímenes específicos a fin de culpar a un criminal por un delito. El primer paso para definir específicamente cada crimen cibernético es clasificar todos los actos que se puedan considerar crímenes cibernéticos en categorías organizadas.

Clasificando por Categorías el Crimen Cibernético

Como los intentos por definirlo muestran, **crimen cibernético** es un término tan amplio y abarcador que resulta inútil en cualquiera que no sea una discusión muy general. Desde luego, si usted llamara a la policía para reportar que hubo un robo en su casa, no empezaría diciendo que ha sido víctima de un “crimen de propiedad”. Para que la policía pueda identificar al criminal o presentar cargos contra esa persona una vez identificada, tiene que conocer el acto específico que se cometió.

Clasificar los crímenes como crímenes de propiedad, crímenes contra personas, delitos de armas, mala conducta oficial, etc. resulta muy útil en cuanto nos ayuda a organizar, por grupos, los actos específicos afines. De esa forma, se pueden recopilar estadísticas generales y las agencias reguladoras del orden pueden formar unidades especiales para lidiar con tipos afines de crímenes. Además, los oficiales se pueden especializar y por consiguiente, volverse más expertos en las categorías de crímenes.

Del mismo modo resulta útil definir las categorías del crimen cibernético y entonces ubicar actos (delitos) específicos dentro de esas categorías. Primeramente debemos darnos cuenta de que los crímenes cibernéticos, en dependencia de su naturaleza, se pueden ubicar dentro de categorías existentes, usadas ya para identificar diferentes tipos de crímenes. Por ejemplo, muchos crímenes cibernéticos (tales como la malversación de fondos utilizando tecnología computarizada) se podrían clasificar como *crímenes de cuello blanco*, generalmente definidos como crímenes no violentos cometidos en el curso de actividades comerciales, por lo general (aunque no siempre), motivados por una ganancia monetaria y que con frecuencia involucran robo, estafa o fraude. Por otra parte, los pornógrafos de

niños en Internet se clasifican generalmente como delincuentes sexuales (pedófilos) y se consideran criminales violentos o potencialmente violentos.

Este traspaso a otras categorías y los muy diversos actos que constituyen crímenes cibernéticos dificultan desglosar el crimen cibernético en sus propias categorías limitadas. Sin embargo, la mayoría de las agencias que lidian con él prefieren hacerlo de este modo pues además los ayuda a identificar el tipo de sospechoso que están buscando. (El perfil de una persona que opera un sitio de pornografía infantil en Internet es diferente al de un hacker que entra en los sistemas computarizados de otros, el que a su vez es diferente al de una persona que usa el correo electrónico para ejecutar un esquema de carta en cadena).

Analizaremos en detalles los tipos de criminales cibernéticos y sus características comunes en el Capítulo 3, “Comprendiendo a las Personas en la Escena”.

Creando Categorías de Crímenes Cibernéticos

Existen muchas maneras en las que podemos clasificar por categorías a los diferentes crímenes cibernéticos. Podemos comenzar dividiéndolos en dos categorías muy amplias: una, aquellos crímenes cometidos por criminales violentos o potencialmente violentos y dos, los crímenes no violentos.

Categorías de Crímenes Cibernéticos Violentos o Potencialmente Violentos

Los crímenes violentos o potencialmente violentos que usan redes de computadoras son de la mayor prioridad por razones obvias. Estos delitos representan un peligro físico para alguna persona o algunas personas. Los tipos de crímenes cibernéticos violentos o potencialmente violentos incluyen:

- Terrorismo cibernético
- Asalto por amenaza
- Acecho cibernético
- Pornografía infantil

El Departamento de Estado de los Estados Unidos define el terrorismo como “violencia premeditada motivada por cuestiones políticas, perpetrada contra objetivos civiles por grupos subnacionales o agentes clandestinos”. El *terrorismo cibernético* se refiere al terrorismo cometido, planeado o coordinado en el ciberespacio – o sea, a través de redes de computadoras.

Esta categoría incluye el uso del correo electrónico para las comunicaciones entre los conspiradores, con el que se transmite la información que será usada en actividades violentas, así como el reclutamiento de miembros del grupo terrorista mediante sitios Web. Más ambiciosamente, podría incluir el sabotaje a sistemas computarizados de control de

tráfico aéreo para ocasionar accidentes o choques entre los aviones; la infiltración en sistemas computarizados para el tratamiento del agua a fin de causar la contaminación de la misma; el hackeo a las bases de datos de hospitales y el cambio o cancelación de información que podría traer como resultado un tratamiento incorrecto y peligroso del paciente o de los pacientes; o perturbaciones en la red eléctrica que podrían ocasionar la desaparición del aire acondicionado en el verano y la calefacción en el invierno o causar la muerte a personas dependientes de respiradores artificiales en residencias privadas si no tienen una planta generadora.

El asalto por amenaza se puede cometer a través del correo electrónico. Este tipo de crimen cibernético trata de hacer que las personas teman por sus vidas o de amenazar la vida de sus seres más queridos (un delito que algunas veces lo llaman *amenaza terrorista*). Podría también incluir amenazas de bombas enviadas a agencias gubernamentales o comerciales.

El acecho cibernético es una forma de acoso electrónico que muchas veces involucra amenazas físicas explícitas o implícitas que provocan temor en la víctima y que podrían intensificarse hasta convertirse en un acecho y un comportamiento violento en la vida real.

La pornografía infantil involucra un número de aspectos: las personas que crean materiales pornográficos utilizando a menores, aquellos que distribuyen esos materiales y quienes acceden a ellos. Si se usan computadoras y redes para alguna de estas actividades, la pornografía infantil deviene un crimen cibernético.

Reseña sobre la Ley Cibernética....

Leyes Nacionales sobre Pornografía Infantil

En los Estados Unidos constituye un crimen federal (18 USC 2251 y 2252) anunciar o acoger conscientemente la pornografía infantil. La "*Child Pornography Prevention Act* " (Ley de Prevención de Pornografía Infantil (CAPA) de 1996 expandió la definición de *pornografía infantil* a cualquier representación visual de una conducta explícitamente sexual cuya producción involucre el uso de un menor tomando parte de un comportamiento explícitamente sexual, aún si la representación visual sólo *parece* ser la de un menor tomando parte de tal conducta o es anunciado o presentado para dar la impresión de que es un menor tomando parte de tal conducta. La Free Speech Coalition entabló una demanda por tener la ley revocada como inconstitucional y una Corte de Apelación Federal sí revocó el estatuto. En Octubre de 2001, la Corte Suprema oyó las versiones sobre la constitucionalidad de la CPPA en el caso *Ashcroft v. La Free Speech Coalition*. En Abril de 2002, la Corte Suprema estableció que las disposiciones de la USC 2256 que prohíben la "pornografía infantil virtual" (imágenes generadas en computadoras de niños manteniendo una conducta sexual) son demasiado generales e inconstitucionales.

En el Reino Unido, en virtud de la Ley de Protección de Niños (1978) y la Sección 160 de la Ley de Justicia Criminal de 1988, constituye un delito criminal que una persona posea una fotografía o una "seudo fotografía" de un niño que se considere indecente. El término *seudo fotografía* se define como una imagen hecha por gráficos de computadora o de otra forma que parezca ser una fotografía. Generalmente es una fotografía creada mediante un

software de manipulación de gráficos como el Adobe Photoshop para superponer la cabeza de un niño sobre un cuerpo diferente (el mismo tipo de “pornografía infantil virtual” abordada por la Corte Suprema de los Estados Unidos en su decisión de Abril de 2002).

La mayoría de los países tienen leyes dirigidas a la pornografía infantil. Para tener una sinopsis de las leyes nacionales compiladas por la INTERPOL (Organización Policial contra el Crimen Internacional), véase el sitio Web de la INTERPOL sobre los delitos sexuales contra niños: www.interpol.int/Public/Children/SexualAbuse/NationalLaws.

La pornografía infantil se considera generalmente un crimen violento, aún si algunas de las personas involucradas no han tenido contacto físico con niños. Es así porque para producir materiales pornográficos es necesario el abuso sexual de niños y porque las personas interesadas en ver esas clases de materiales muchas veces no limitan su interés a fotos y fantasías, sino que por el contrario están practicando la pedofilia o aspiran a hacerlo en la vida real.

En la escena....

Experiencias de la Vida Real

Del detective Glen Klinkhart,
Unidad de Crímenes por ordenador del Departamento de Policía de Anchorage

No hace mucho tiempo, un amigo mío del FBI me llamó con un pedido. Me dijo que había recibido una transcripción de una sesión de Chat por relevos (IRC) y que quería hablarme de ello. Durante la correspondencia de dicha sesión, uno de los participantes había escrito un plan detallado sobre la preparación del secuestro de un niño pequeño en un centro comercial. El Chat indicaba que el centro comercial podría estar en algún lugar de nuestra ciudad. El agente del FBI me preguntó si estaría interesado en leer los registros de la sesión de Chat y darle mi opinión sobre la situación.

Cuando el agente llegó, miré la transcripción y quedé horrorizado con lo que leí. La sesión mostraba lo que parecían ser dos personas chateando en línea. Una, llamada “PITH”, aparentemente le envió al FBI los registros de la sesión de Chat y la otra era el sospechoso, conocido solo como “Kimmo”. Pith grabó el fichero con los registros de la sesión y entonces contactó a la policía e informó sobre el incidente. La sesión de Chat era una visión espeluznante y aterradora de un demente.

Las ocho páginas del Chat brindaban detalles extremadamente gráficos y sexualmente explícitos que incluían las formas bien específicas en las que el sospechoso dijo que disfrutaría “raptando” y “torturando” a su víctima. Durante el resto del Chat, el sospechoso, Kimmo, dio detalles sobre el centro comercial en cuestión que había escogido y la ubicación general de su cabina, al norte de la ciudad. Kimmo fue muy específico acerca de los actos sexuales que iba a perpetrar en contra de su víctima. Parecía que Kimmo había estado pensando y fantaseando con ese ataque desde hacía algún tiempo.

El FBI y nuestro departamento comenzaron inmediatamente a trabajar en el caso. En un momento, teníamos a 14 agentes y detectives policiales trabajando en la misma

investigación. Continuamos rastreando la ubicación de nuestro sospechoso entrando encubierto en salas de chateo de Internet buscando a Kimmo, rastreando su dirección IP y utilizando herramientas tales como órdenes de registro y comparecencia para obtener un rastro de información que nos condujera hacia nuestro sospechoso.

El rastro nos condujo a un padre divorciado que vivía en las afueras de la ciudad. Los agentes comenzaron a vigilarlo a él y a su casa. Otros verificaron su historial y aprendieron más sobre su modo de operar. Parecía que no tenía historial delictivo, sin embargo, era un experto en utilizar computadoras. Él también ajustó muchos de los detalles comunicados a Pith durante la alarmante sesión de Chat.

Obtuvimos órdenes de registro para la casa del sospechoso y nos preparamos para registrar su oficina también. En una mañana clara y fría, registramos la oficina y la casa de nuestro sospechoso. Otro grupo de oficiales intentó interrogar al sospechoso.

Al encararnos, el sospechoso actuó como si no supiera de que estábamos hablando. Negó tener conocimiento alguno sobre la sesión de Chat entre Pith y Kimmo. Al presentarle evidencia irrefutable, incluyendo un rastro electrónico que nos condujo directamente hacia la computadora de su casa, admitió finalmente que era Kimmo. Dijo que participaba en la sala de Chat porque en ese entonces estaba gravemente intoxicado. Le dijo a los investigadores que nunca había dañado a un niño y que nunca heriría a nadie.

Sus sistemas computarizados de la casa y el trabajo contaron otra historia. En la computadora de su casa y en varios medios computarizados encontramos cientos de imágenes de pornografía infantil, incluyendo imágenes de niños amarrados y violados. Kimmo desarrolló además una afición por coleccionar cientos de dibujos representando niños con sus cuerpos cortados, mutilados y expuestos de una manera perturbadora y sangrienta.

El sospechoso fue arrestado. Fue declarado culpable de posesión y distribución de pornografía infantil. Actualmente se encuentra cumpliendo en una prisión federal.

¿El sospechoso sólo estaba borracho cuando chateaba con Pith? ¿Realmente "nunca dañaría a un niño", tal como nos dijo? ¿Habría raptado algún niño de algún centro comercial y lo habría llevado a su cabaña para violarlo y torturarlo? Nunca lo sabremos con exactitud. Sí sé que al menos en los próximos años, este hombre no podrá cumplir sus planes, gracias al arduo trabajo del FBI, la oficina del Fiscal de los Estados Unidos y nuestro equipo de dedicados investigadores.

Categorías de Crímenes Cibernéticos No Violentos

La mayoría de los crímenes cibernéticos son delitos no violentos debido al hecho de que una característica definitoria del mundo en línea es la capacidad de interactuar sin que exista un contacto físico. El anonimato percibido y la "irrealidad" de experiencias virtuales son los elementos que hacen al ciberespacio un "lugar" tan atractivo para cometer crímenes.

Los crímenes cibernéticos no violentos se pueden dividir a su vez en varias subcategorías:

- Traspaso cibernético
- Robo cibernético
- Fraude cibernético
- Crímenes cibernéticos destructivos
- Otros crímenes cibernéticos

Un número de más actos criminales específicos tienen cabida en cada una de estas categorías.

Traspaso cibernético

En los delitos de *traspaso cibernético*, el criminal accede sin autorización a recursos de una computadora o red, pero no hace mal uso o daña los datos allí. Un ejemplo común lo constituye el hacker adolescente que violenta redes sólo “porque él (o ella) puede” – para afinar sus habilidades de hacker, para probarse ante sus coetáneos o porque es un reto personal.

Los traspasadores cibernéticos disfrutan el “fisgoneo”, leer Sus correos y documentos personales, ver qué programas tiene en Su sistema, qué sitios ha visitado, etc., pero no hacen nada con la información que encuentran. No obstante, el traspaso cibernético es un crimen en la mayoría de las jurisdicciones, generalmente conocido como “acceso no autorizado”, “violación de la seguridad de la red” o algo similar.

Los profesionales del mundo policial necesitan conocer bien las leyes en sus jurisdicciones y evitar desechar de forma automática una queja de intrusión en la red sencillamente porque la víctima no puede mostrar pérdidas o daños. Los administradores de redes necesitan conocer bien este crimen, porque en virtud de las regulaciones penales, una compañía puede procesar a intrusos sencillamente por acceder a la red o a sus computadoras sin autorización. Al respecto, podría ser más fácil construir un caso penal que una demanda civil, pues en muchas ocasiones la segunda requiere pruebas de los daños a fin de compensarlos.

Robo Cibernético

Existen muchos tipos diferentes de *robo cibernético* o modos de usar una computadora o red con el fin de robar información, dinero u otros objetos de valor. Debido a que el dinero es un motivador casi universal y a que la capacidad de robar a distancia reduce el riesgo del ladrón de ser detectado o capturado, el robo es uno de los crímenes cibernéticos más populares.

Los delitos de robo cibernético incluyen:

- *Desfalco*: se trata de malversar dinero o propiedades que le han sido confiados por otra persona para Su propio uso (por ejemplo, un empleado que usa su acceso legítimo al sistema computarizado de nóminas de la compañía para cambiar los datos de modo que reciba un dinero extra o que transfiera los fondos de las cuentas bancarias de la compañía a su propia cuenta personal)
- *Apropiación ilícita*: difiere del desfalco en que al criminal nunca le fueron confiados los objetos de valor, sin embargo, accede desde afuera de la organización y transfiere fondos, modifica documentos titulándose propiedades que nunca ha poseído o algo por el estilo
- *Espionaje industrial/empresarial*: en el que personas de dentro o fuera de la compañía usan la red para robar secretos comerciales (tales como la receta de un refresco de la competencia), datos financieros, listas confidenciales de clientes, estrategias de marketing u otra información que pueda utilizarse para sabotear el negocio u obtener una ventaja competitiva
- *Plagio*: es el robo de un documento original perteneciente a otra persona con el objetivo de hacerlo pasar como propio
- *Piratería*: es la copia no autorizada de softwares, música, películas, obras de arte, libros, etc. con derechos reservados, causándole pérdidas de ingresos al dueño legítimo de los derechos reservados
- *Robo de identidad*: se utiliza la Internet para obtener información personal de la víctima, tal como los números de seguridad social y licencia de conducción con el fin de asumir la identidad de esa persona para cometer actos delictivos u obtener dinero o propiedades o usar tarjetas de crédito o cuentas bancarias pertenecientes a la víctima
- *Envenenamiento del caché de DNS*: una forma de interceptación no autorizada en la que el intruso manipula el contenido del caché DNS de una computadora para redireccionar transmisiones de redes hacia sus propios servidores

En la escena....

Experiencias de la Vida Real

Comunicado de prensa, Departamento de Justicia de los Estados Unidos

Agentes federales arrestaron a un hombre de Jacksonville, Florida, en marzo de 2002 por robo de identidad en relación con el robo de los registros personales de 60,000 empleados de la base de datos computarizada de la Prudential Insurance Company. El hombre era un antiguo empleado de la Prudential, especialista en tecnologías de la información, y pretendía vender la información de la base de datos a través e Internet con el propósito de obtener tarjetas de crédito fraudulentas empleando las identidades robadas.

Los administradores de redes deben estar conscientes de que en muchos casos, la intrusión en la red es mucho más que un simple fastidio. El robo cibernético le cuesta a las compañías millones de dólares cada año. Los oficiales de la policía necesitan comprender que el robo no siempre involucra necesariamente dinero, también se pueden robar datos de una compañía y en la mayoría de las jurisdicciones existen leyes (incluyendo, en algunos

casos, leyes federales) que se pueden usar para procesar a aquellos que “sólo” roban información.

El robo cibernético está estrechamente relacionado con el fraude cibernético y, en algunos casos, ambos coinciden. Esta coincidencia se hace aparente cuando Usted encuentra casos de fraude cibernético que involucran apropiación indebida de dinero u otra propiedad.

Fraude Cibernético

Generalmente, el *fraude cibernético* se trata de la promoción de artículos falsos con el fin de obtener algo de valor o utilidades. Aunque se puede decir que es una forma de robo, el fraude difiere del robo en que, en muchos casos, la víctima le entrega consciente y *voluntariamente* el dinero o la propiedad al criminal – pero no lo hubiese hecho si el criminal no hubiese hecho una falsificación de algún tipo.

El fraude cibernético incluye los mismos tipos de estafas y esquemas que existían mucho antes de las computadoras y las redes. Por ejemplo, el estafador le manda un correo electrónico pidiéndole enviar dinero para ayudar a un pobre niño cuyos padres murieron en un accidente automovilístico, o le promete que si usted “invierte” una pequeña suma de dinero (que envía al estafador) y le envía el mismo mensaje a 10 amigos, Usted recibirá en el transcurso de 30 días miles de veces su “inversión”. Otros fraudes involucran la falsificación de credenciales para obtener negocios (y con frecuencia no brindan el servicio o el producto prometido). La Internet simplemente le facilita y agiliza las operaciones a estos estafadores y les da un mayor número de víctimas potenciales en quienes centrarse.

Los esquemas fraudulentos, con base en el ciberespacio o no, a menudo se aprovechan de la codicia de la víctima o de su buena voluntad. Los profesionales del orden creen que estos crímenes se pueden procesar en muchas ocasiones en virtud de leyes que no tienen nada que ver con el crimen por ordenador, tales como los estatutos generales sobre fraude del Código Penal o del Empresarial. El fraude normalmente va dirigido a individuos, pero los administradores de redes deben estar claros de que los estafadores algunas veces también centran su atención en compañías, enviando sus mensajes de caridad o sus esquemas de “vuélvete rico rápido” a personas del centro de trabajo donde pueden encontrar una gran audiencia. Tales “spam” deben reportarse al departamento informático de la compañía donde se seguirán los pasos para reportar el abuso a las autoridades y/o bloquear los correos provenientes de la dirección del estafador si el problema persiste.

En la escena...

Experiencias de la Vida Real

Comunicado de prensa, Departamento de Justicia de los Estados Unidos
Abogada de los Estados Unidos Emily M. Sweeney

Un hombre de Miami, Florida, fue acusado en septiembre de 2001 de estafar a postores a través del sitio de subasta en línea eBay al anunciar raras tarjetas de baseball y basketball, reunir los pagos de los postores y no enviar los productos. Fue acusado en virtud del

Artículo 18 del Código de los Estados Unidos, declarado culpable y sentenciado a 5 meses en prisión seguidos de 5 meses de confinamiento domiciliario (con monitoreo electrónico).

El fraude cibernético puede tomar otras formas. Cualquier modificación de los datos de la red para obtener un beneficio puede constituir un fraude (aunque algunos estados tienen crímenes por ordenador más específicos que aplican). Por ejemplo, un estudiante que entra a una red computarizada de un sistema escolar para cambiar las notas o una persona que accede a una base de datos de la policía para borrar el registro de su arresto o las multas por exceso de velocidad está cometiendo una forma de fraude.

Crímenes Cibernéticos Destructivos

Los *crímenes cibernéticos destructivos* incluyen a aquellos en los que se afectan los servicios de la red o se dañan o destruyen datos, más que robarlos o mal utilizarlos. Estos delitos incluyen:

- Entrar a una red y borrar datos o ficheros de programas
- Entrar a un servidor Web y “destrozar” páginas Web
- Introducir virus, gusanos y otros códigos maliciosos en una red o computadora
- Planear un ataque DoS que apague el servidor e impida a los usuarios legítimos acceder a los recursos de la red

Cada uno de ellos priva, de alguna forma, a los dueños y usuarios autorizados de los datos y/o redes del uso de los mismos.

El *vandalismo cibernético* puede ser un acto aleatorio hecho “sólo por diversión” por hackers aburridos con una veta maliciosa, o podría ser una forma de sabotaje electrónico para obtener ganancias (borrando todos los ficheros de la competencia en el negocio, por ejemplo). En algunos casos, el vandalismo cibernético se podría llevar a cabo con el fin de hacer una declaración personal o política (como en los *graffitis cibernéticos*).

CNN.com reportó el 8 de enero de 2002 que el número de los sitios Web “pintorreteados” aumentó en más de cinco veces entre el 2000 y el 2001. Inmediatamente después del aterrizaje forzoso en China de un avión espía de los Estados Unidos en el 2001, se reportaron numerosos incidentes de hackers chinos y americanos pintorreteándose mutuamente sus sitios Web en lo que se denominó “una guerra cibernética”.

El incremento del vandalismo cibernético subraya la necesidad no sólo de montar sistemas generales de detección de intrusos (IDSs), sino también de asegurar que se solucionen estas conocidas vulnerabilidades en los servidores Web, estando al tanto de los últimos tipos de ataques y aplicando fielmente las actualizaciones y “soluciones” que venden los comercializadores para remendar tales lagunas en la seguridad. Los profesionales de la informática necesitan estar conscientes de que las aplicaciones y los sistemas operativos viejos no fueron diseñados teniendo en mente una alta seguridad, sencillamente porque cuando salieron al mercado, el riesgo no era tan alto ni se comprendía tan bien la importancia de la misma. Por otra parte, los nuevos sistemas operativos y las nuevas aplicaciones podrían tener vulnerabilidades de seguridad que no se hayan descubierto

todavía. La mayoría de los vendedores de softwares son rápidos para solucionar los problemas de seguridad una vez que se conocen, pero esto generalmente no sucede hasta un hacker descubre y explota el problema.

Los oficiales de la policía, en muchos casos, necesitan leyes que afronten específicamente la intrusión en las redes a fin de procesar a los que cometen vandalismo cibernético, porque podría resultar difícil hacer que estas actividades encajen en los elementos de las leyes existentes con relación al vandalismo.

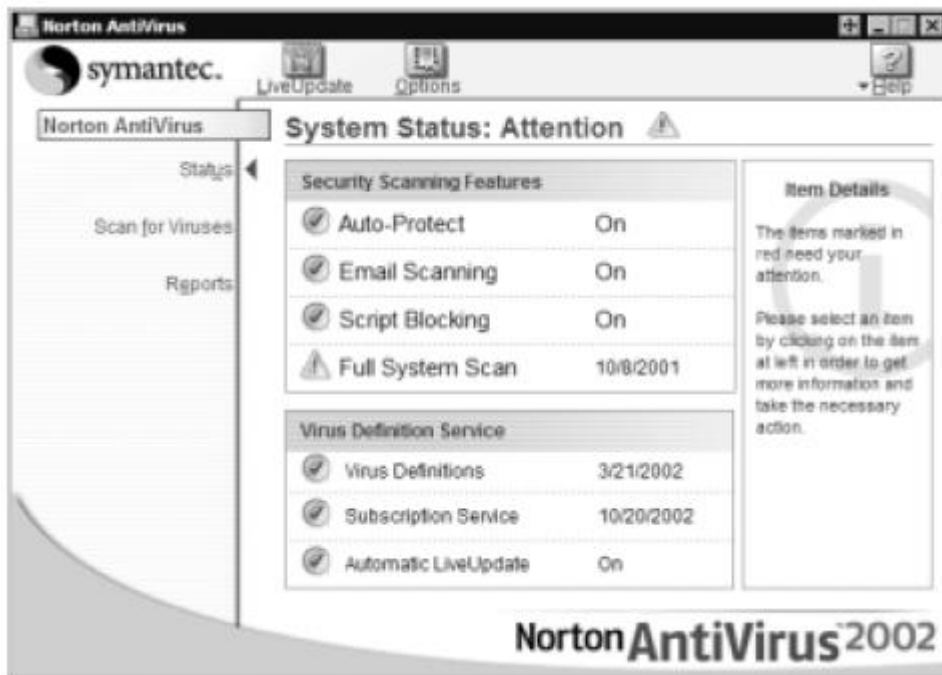
Los virus y otros códigos maliciosos representan un enorme problema para todas las computadoras conectadas a Internet. Existe alguna confusión, incluso en el mundo de la tecnología, acerca de la terminología usada para describir los códigos maliciosos. Un *virus* de computadora es un programa que causa un resultado no deseado – y muchas veces destructivo – cuando se ejecuta. Un *gusano* es un virus que se reproduce solo. Un *troyano* (o *caballo troyano*) es un programa aparentemente inofensivo o legítimo en cuyo interior se esconden códigos maliciosos; es una forma de introducir un virus o un gusano en la red o en la computadora.

Los códigos maliciosos representan daños a sistemas computarizados valorados en millones de dólares, y los escritores de virus son muy activos, creando constantemente nuevos virus y gusanos y modificando los viejos de modo que no sean detectados por los programas antivirus (AV). El advenimiento de modernos programas de mensajería electrónica que soportan mensajería y anexos HTML ha facilitado más que nunca la diseminación de los virus. Ya no es necesario entrar a una red para introducir códigos maliciosos – ahora Usted puede simplemente enviarle un correo a un usuario técnicamente ingenuo y estos se esparcirán rápidamente a través de la red de área local y más allá.

Los programas antivirus tales como el comercializado por SYMANTEC (Norton Antivirus, mostrado en la figura 1.3) y el McAfee constituyen una parte esencial de cualquier plan de seguridad de la red. Sin importar cuál paquete antivirus se utilice, es esencial que se actualicen frecuentemente sus *ficheros de definición de virus* usados para identificar y colocarle bandera roja a los conocidos códigos maliciosos.

Analizaremos los virus, gusanos y Troyanos más detalladamente en el Capítulo 6 “Comprendiendo las Intrusiones y los Ataques a las Redes”.

Figura 1.3 Un buen paquete de programas antivirus, actualizado frecuentemente, constituye una primera línea de defensa esencial.



Estadísticas Cibernéticas....

El Costo de los Códigos Maliciosos

Computer Economics, una organización de investigación californiana que asesora en relación con los negocios en el campo de la tecnología, publicó un reporte en el que estimaba que los virus y otros códigos maliciosos causaron en todo el mundo pérdidas superiores a los 13 billones de dólares estadounidenses en el 2001. Los críticos dudan de la fidelidad de la cifra y cualquier estimado será sólo eso, un estimado basado únicamente en los casos reportados y en la valoración de las pérdidas hecha por las compañías. Pero no existe duda de que los ataques de virus pueden costar más del valor de los datos perdidos. Se deben considerar además la pérdida de productividad durante el tiempo de inactividad resultante, los daños a la reputación de la compañía, la pérdida de negocios resultante y otros factores difíciles de medir. (Véase www.computereconomics.com/cei/press/pr92101.html para un análisis de las ramificaciones).

Otros Crímenes Cibernéticos No Violentos

Existen muchas más variedades de crímenes cibernéticos no violentos. Nuevamente, muchos de ellos sólo usan incidentalmente la Internet para cometer actos criminales que han existido siempre (incluyendo la profesión más antigua del mundo). Algunos ejemplos incluyen:

- Publicar/solicitar servicios de prostitución a través de Internet
- Juegos de azar por Internet

- Venta de drogas a través de Internet (ambas, drogas ilegales y drogas por prescripción)
- *Lavado de dinero electrónico*, o usar transferencias electrónicas de fondos para lavar ilegalmente el dinero obtenido
- *Contrabando cibernético*, o transferir a través de Internet productos ilegales tales como tecnologías de encriptación que están prohibidas en algunas jurisdicciones

La prostitución es ilegal en todos los estados de los Estados Unidos, excepto en Nevada y en muchas áreas rurales. Los estatutos en la mayoría de los estados están redactados de manera tal que solicitar servicios sexuales a través de Internet constituye un acto fuera de la ley. Además, de acuerdo con Mike Goodwin de la Electronic Frontier Foundation, en una entrevista titulada *La Prostitución e Internet* (publicada en www.bayswan.org/EFF.html), el uso del comercio interestatal para solicitar una “actividad ilegal” constituye un delito federal. El artículo 18 de 1952 del Código de los Estados Unidos define la “prostitución en violación de las leyes estatales” como una actividad ilegal.

Sin embargo, de acuerdo con la emisión del *E-Commerce Times* del 13 de marzo de 2001, las prostitutas de alta tecnología publican ampliamente sus servicios en Internet bajo el disfraz de “servicios de acompañante”. La prostitución en línea está, frecuentemente, muy asociada a los servicios de pornografía en línea, los cuales (a menos que hayan niños involucrados) están, por lo general, protegidos como libertad de expresión en los Estados Unidos en virtud de la Primera Enmienda a la Constitución.

Una cuestión legal interesante es esa de la “prostitución cibernética” que trata de intercambiar *sexo virtual* por dinero. Debido a que realmente no tiene lugar un contacto físico, estas actividades no son ilegales según los estatutos sobre prostitución de la mayoría de los estados. En 1996, el Congreso de los Estados Unidos aprobó la Ley de Decencia en las Comunicaciones, la cual prohibía las comunicaciones “indecentes” o “claramente ofensivas” en Internet. Entonces, en 1997, en el caso *Reno v. ACLU*, La Corte Suprema revocó la ley como inconstitucional (una violación de la Primera Enmienda en cuanto a la libertad de expresión). Es importante para los agentes del orden darse cuenta de que las leyes regentes del contenido y la conducta sexual en línea están en constante evolución. Esta es un área en la que es vital mantenerse actualizado porque lo que es legal hoy, podría resultar ilegal mañana y viceversa.

Los profesionales de las redes tienen que considerar otras cuestiones con respecto al contenido sexual. Incluso si no es un delito, poner o permitir material sexualmente ofensivo en la red de una compañía podría traer como resultado una demanda civil alegando acoso sexual. Los empleadores que crean un ambiente de “trabajo hostil” pueden ser demandados en virtud del Artículo VII de la Ley de Derechos Civiles de 1964.

Los juegos de azar en Internet han florecido con clientes en línea capaces de hacer apuestas en casinos virtuales usando tarjetas de crédito. En julio del año 2000, la Cámara de Representantes de los Estados Unidos sometió a votación y denegó una propuesta de Ley de Prohibición de Juegos de Azar por Internet. Sin embargo, el gobierno federal ha usado el Interstate Wireline Act (Artículo 18 del Código de los Estados Unidos 1084) para procesar operaciones de juegos de azar en línea. Esta ley prohíbe proponer o aceptar apuestas de los jugadores a través de líneas telefónicas o a través de otros “dispositivos

alámbricos” (los cuales incluyen las computadoras conectadas a Internet) a menos que un estado en particular lo autorice así. Como con muchos otros crímenes de Internet, la jurisdicción es un problema al procesar a los propietarios de juegos de azar por Internet.

Los juegos de azar por Internet es otra área en la cual las leyes pueden cambiar rápidamente y variar tremendamente de una jurisdicción a otra. En realidad, algunos estados se encargan personalmente de los juegos de azar en línea, ofreciendo ventas de lotería en Internet.

La venta de drogas por Internet representa otro gran negocio. Ambos, el tráfico ilegal de drogas y la venta de drogas por prescripción realizada por farmacias en línea han acrecentado los problemas. El impacto de Internet en el tráfico internacional de drogas ilegales tales como el opio ha sido estudiado por las Naciones Unidas y gobiernos individuales. En marzo del año 2000, las Naciones Unidas aprobaron una resolución con el objetivo de “impedir el uso de la World Wide Web para la proliferación del tráfico de drogas y el abuso” alentando a sus miembros a adoptar una serie de medidas para prevenir o reducir las ventas de drogas ilícitas a través de Internet.

Reseña de la Ley Cibernética...

Juegos de Azar en Línea y Fuera de Línea

En los Estados Unidos, los juegos de azar fuera de línea son legales en algunos estados y en otros no. Algunos países como Antigua y otros estados caribeños permiten y licencian las operaciones de juegos de azar a través de Internet. Algunos estados han promulgado estatutos prohibiendo los juegos de azar en Internet. En el 2000, Dakota del Sur aprobó una ley de este tipo, la Ley para Prohibir el Uso de la Internet para Ciertas Actividades de Juegos de Azar, la cual los convierte en una felonía en ese estado. (Sin embargo, la lotería estatal y los casinos licenciados en Dakota del Sur están exentos de ser procesados).

Las farmacias que operan a través de Internet vendiendo sustancias controladas podrían constituir un negocio legal y legítimo que funcione tanto como las farmacias tradicionales que venden por correo, si acataran las leyes estatales que las licencian y siguieran las prescripciones expedidas por los doctores de los pacientes. Otras farmacias en línea venden drogas por prescripción basándose meramente en un formulario completado por el “paciente” el que es supuestamente evaluado por un médico que nunca ha visto a ese “paciente” y sin requerir una verificación de identificación. Los mensajes SPAM bombardean los buzones de correos de los usuarios de la mensajería electrónica con anuncios no solicitados sobre drogas como la Viagra, píldoras dietéticas, Prozac, píldoras anticonceptivas y otros populares medicamentos por prescripción.

En los Estados Unidos, la Ley de Protección al Consumidor de Farmacias en Internet fue introducida por una Comisión de la Cámara pero no fue aprobada. Sin embargo, un número de leyes existentes son aplicables a la Internet. La Ley de Sustancias Controladas y la Ley de Cosméticos, Droga y Comida se pueden usar para procesar a los infractores en virtud de la ley federal, y cada estado tiene leyes en relación con las licencias de farmacias y los requerimientos para la prescripción y el despacho de drogas.

El Departamento de Justicia (DoJ), la Food and Drug Administration (FDA) y la Federal Trade Commission (FTC) tomaron medidas enérgicas contra las compañías que venden sustancias controladas a través de la Net sin prescripciones válidas. Además, los fiscales generales de varios estados demandaron a esta clase de farmacias para impedir que hagan negocios en esos estados. En marzo de 2001, las autoridades locales y federales cooperaron para cerrar una farmacia con sede en Oklahoma que, según se dice, vendía ilegalmente drogas por prescripción a través de la Net. Los oficiales de la policía deben familiarizarse con las muchas leyes estatales y federales que regulan las ventas de drogas por prescripción así como aquellas que tratan las ventas y posesión de drogas ilícitas.

El lavado de dinero electrónico involucra el uso de Internet para ocultar los orígenes del dinero obtenido por medios ilegales. El lavado de dinero es un crimen muy antiguo, pero el relativo anonimato de la Internet le ha facilitado a los criminales la conversión del “dinero sucio” en activos o inversiones aparentemente lícitos.

Nota

El origen del término *lavado de dinero* se dice data del hábito del famoso gángster de Chicago Al Capone de ocultar sus ganancias procedentes de los juegos ilegales en lavanderías operadas con monedas.

Las operaciones de juegos de azar en Internet analizadas anteriormente proporcionan un modo de lavar dinero: un criminal usa el efectivo obtenido ilegalmente en transacciones de juegos de azar. La banca en línea también le ofrece oportunidades a los criminales, quienes pueden abrir cuentas sin tener que darle la cara a los funcionarios del banco. El dinero se puede depositar en una cuenta bancaria secreta en el exterior o transferirse electrónicamente de un banco a otro ya que resulta muy difícil o imposible seguir sus rastros. Aunque los criminales aún enfrentan el reto de depositar inicialmente grandes sumas de efectivo en el sistema sin levantar sospechas, una vez que lo hacen, pueden mover estos fondos y manipularlos de una manera mucho más fácil y rápida con la comodidad de las actuales transferencias electrónicas.

El contrabando cibernético se refiere a los datos cuya posesión o transferencia es ilegal. Por ejemplo, en los Estados Unidos, las Regulaciones para el Tráfico Internacional de Armas (ITAR) prohíben la exportación de poderosos programas criptográficos e invocan prisión y/o multas de hasta 1 millón de dólares estadounidenses por enviar ese tipo de programa a alguien fuera de los Estados Unidos. En 1997, un Juez del Distrito de los Estados Unidos dictaminó que las regulaciones eran inconstitucionales y que violaban los derechos de libertad de expresión contenidos en la Primera Enmienda. En el 2000, la administración Clinton adoptó regulaciones nuevas y más flexibles para la exportación de programas de encriptación.

En virtud de la Ley de Propiedad Intelectual en el Milenio Digital (DMCA), constituye una ilegalidad poner a disposición del público softwares que burlen la protección de materiales con derechos de autor. Un criptógrafo ruso llamado Dmitri Sklyarov fue arrestado en Las Vegas en el 2001 por “traficar con” un programa que rompe los códigos de encriptación creados por Adobe para proteger sus productos eBook. Los cargos contra Sklyarov fueron

retirados a cambio de su consentimiento de testificar en contra de la compañía para la cual trabajaba, la cual fue acusada del mismo delito. Hasta el momento en que se escribió esto, el segundo caso aún estaba pendiente. Este, el primer caso delictivo invocado en esta sección de la DMCA, ha generado una gran controversia, sobre todo porque el software en cuestión es legal en virtud de las leyes de Rusia, país de Sklyarov. Existen muchos desacuerdos sobre las interpretaciones de varias secciones de la DMCA; un aspecto interesante es que la ley no parece prohibir la posesión (o incluso el uso) de softwares por los usuarios finales, sólo la “provisión” de dichos softwares a otros.

Reseña de la Ley Cibernética....

Convirtiendo Softwares en Ilegales

Un proyecto de ley introducido en el Senado de los Estados Unidos en el 2002 por el Senador Fritz Hollings prohibiría la creación, venta o distribución de softwares que no incluyeran estándares de seguridad aprobados por el gobierno. Los profesionales de la informática han especulado que en caso que se aprobara, la ley convertiría en ilegal a los sistemas operativos de plataforma abierta tales como Linux. En el actual ambiente nacional de consciencia sobre la importancia de la seguridad y con el interés internacional centrado en prevenir el terrorismo, podemos esperar ver más propuestas de leyes que conviertan en contrabando a determinados programas de software o incluso a los mismos datos.

En los Estados Unidos, la mayoría de los datos están actualmente protegidos por la Primera Enmienda, aunque existen excepciones obvias tales como la pornografía infantil (analizada anteriormente en este capítulo). El concepto de contrabando cibernético es relativamente nuevo y controversial. Los profesionales del orden siguen viendo este asunto a su manera, junto con legisladores que intentan equilibrar las libertades y los derechos de los usuarios de Internet con el deseo de proteger la sociedad de la información “nociva”.

Priorizando el Cumplimiento de la Ley en el Caso del Crimen Cibernético

Como el crimen cibernético prolifera, resultará obviamente imposible para las agencias policiales dedicarle el tiempo y el esfuerzo requeridos para investigar y procesar cada caso de actividad criminal relacionada con Internet. El establecimiento de categorías delictivas ayuda a las agencias a priorizar los deberes legales.

Los factores a considerar para decidir qué tipo de crimen cibernético va a tener la mayor prioridad para las autoridades incluyen:

- **Extensión del daño** Los crímenes cibernéticos que involucran violencia o violencia potencial contra personas (especialmente crímenes contra niños) son normalmente de alta prioridad; los crímenes de propiedad que tienen como resultado una gran pérdida monetaria, generalmente, tienen preferencia con respecto a aquellos en los que la pérdida es menor.
- **Frecuencia de los acontecimientos** A los crímenes cibernéticos que ocurren con más frecuencia, generalmente, se les dedica más esfuerzos coordinados que a aquellos que ocurren rara vez.

- **Disponibilidad de personal** Los crímenes cibernéticos que pueden ser investigados fácilmente por un detective podrían atraer más la atención de las agencias policiales sencillamente porque no hay suficientes recursos humanos para llevar a cabo investigaciones sofisticadas que requieran la presencia de muchos investigadores.
- **Entrenamiento del personal** Cuál crimen cibernético se investiga y cuál no depende a veces del entrenamiento que tengan los investigadores para manejarlo.
- **Jurisdicción** Las agencias, generalmente, prefieren concentrar sus recursos en los delitos que afectan a los ciudadanos locales. Aún si la agencia tiene jurisdicción legal, podría elegir no gastar recursos en crímenes cibernéticos que traspasen los límites jurisdiccionales.
- **Dificultad de la investigación** Muy relacionada a los dos factores anteriores, la dificultad de la investigación y la probabilidad de un resultado exitoso podría afectar la elección de cuál delito tiene la mayor prioridad.
- **Factores políticos** El clima político prevaleciente influye a menudo en las prioridades de las agencias. Si los políticos que dirigen la agencia tienen una preocupación especial sobre crímenes específicos, lo más probable es que estos tengan preferencia.

Al tratar con los oficiales de la policía en casos de crímenes cibernéticos, es importante que los profesionales de la informática comprendan cómo estos factores podrían influir en que un crimen cibernético sea investigado con más entusiasmo y procesado más enérgicamente que otros.

Combatiendo el Crimen Cibernético

Para combatir exitosamente el crimen cibernético, como sucede con cualquier otro tipo de crimen, primero tenemos que entenderlo. *Conoce a tus enemigos* es un buen consejo, sin tener en cuenta el tipo de guerra que planeamos librar. El primer paso al crear un plan para combatir el crimen cibernético es definirlo, de ambas formas: general y específicamente. Este capítulo le ha dado algunas definiciones que le servirán como punto de partida para identificar qué es un crimen cibernético y qué no lo es.

Otro elemento importante para determinar nuestra estrategia en contra del crimen cibernético es recopilar datos estadísticos de modo que podamos realizar un análisis para detectar patrones y tendencias. Sin estadísticas confiables, resulta difícil establecer políticas legales y de prevención efectivas.

Las estadísticas son las bases para el próximo paso: redactar leyes claras y que se puedan hacer cumplir cuando sea necesario enfrentar crímenes cibernéticos que no estén contemplados en las leyes existentes.

Finalmente, un esfuerzo efectivo de lucha contra el crimen tiene que educar a todos aquellos que lidian con el crimen cibernético o que son víctimas de él, a los de la comunidad del sistema penal, a los de la comunidad informática y a los de la comunidad en general.

Determinando Quién Combatirá el Crimen Cibernético

Por necesidad, la lucha contra el crimen cibernético debe involucrar a más partes, no sólo a la policía. Los legisladores deben hacer leyes apropiadas. La comunidad informática y la comunidad en general deben estar a la caza de señales de crimen cibernético y reportarlo a las autoridades, así como tomar medidas para evitar convertirse en víctimas de estos crímenes. La comunidad policial debe investigar, recopilar evidencias y construir casos que se puedan ganar en contra de los criminales cibernéticos. El jurado debe sopesar la evidencia y tomar determinaciones justas y razonables de culpabilidad o inocencia. El sistema correccional debe intentar rehabilitar a estos criminales que probablemente no cumplan con el estándar del “perfil criminal”.

Un gran problema al redactar, hacer cumplir, procesar e interpretar leyes sobre el crimen cibernético es la escasez de conocimientos técnicos por parte de las personas encargadas de estos deberes. Los legisladores, en la mayoría de los casos, no tienen un entendimiento real de las cuestiones técnicas y de qué es conveniente o no, o incluso posible, legislar. Los investigadores de la policía están adquiriendo cada vez más habilidades técnicas, pero en muchas jurisdicciones pequeñas, nadie en el departamento sabe cómo recuperar la evidencia digital clave.

El presupuesto podría no permitir traer asesores a los que hay que pagarles mucho dinero o, por ejemplo, enviar un disquete a algún servicio de recuperación de datos cuyos precios son muy altos (sin mencionar el hecho de que estas dos opciones pueden crear una cadena de asuntos de custodia que a la larga podría traer como resultado que los datos recuperados no sean admisibles como evidencia).

Los fiscales tienen la ventaja de poder traer a testigos expertos que expliquen las complejidades, pero también tienen que poseer un mínimo de conocimientos sobre las cuestiones técnicas involucradas para saber qué preguntar a esos testigos en el estrado. El jurado también tiene a menudo una gran responsabilidad sobre sí al evaluar los puntos esenciales de un caso de crimen cibernético. Si los miembros del jurado no tienen suficientes conocimientos técnicos para determinar por sí mismos si los elementos de un delito han sido probados, tienen que confiar en las opiniones contradictorias presentadas por los abogados y expertos sin comprender realmente la base de sus opiniones.

En la escena....

Experiencias de la Vida Real

Aquí tienen una ilustración de cómo casos de crímenes cibernéticos técnicamente complejos pueden representar un reto para los miembros del jurado, más que, por ejemplo, un caso de homicidio:

Para determinar si el acusado es culpable de homicidio, el jurado oirá testimonios tales como versiones de testigos oculares que vieron al acusado tomar un arma, apuntarle a la víctima y disparar, o testimonios de expertos forenses quienes declaran que las huellas dactilares del acusado estaban en el arma. La veracidad de las declaraciones de los testigos

podría estar en duda y el abogado defensor podría argumentar que el acusado manipuló el arma previamente, pero que no la usó para asesinar a la víctima, sin embargo las cuestiones básicas no son difíciles de comprender. Todos los del jurado saben lo que es un arma y está bien establecido que las huellas dactilares son únicas y que se pueden identificar positivamente como pertenecientes a una persona específica.

Por otra parte, en un caso que involucre el hackeo de una red de computadoras, los miembros del jurado podrían oír testimonios sobre puertos abiertos y explotaciones del TCP/IP y sobre cómo se puede usar la falsificación del IP para disfrazar el origen de una transmisión de red. Estos términos probablemente signifiquen poco para los miembros del jurado cuya única exposición a computadoras es en calidad de usuarios finales y los puntos más delicados de las comunicaciones de redes y de la seguridad no son temas que se puedan explicar fácilmente en el, por lo general, limitado período de tiempo disponible durante la declaración en el juicio. Si el jurado no comprende *cómo* ocurrió el delito, será difícil para ellos decidir si un acusado en particular lo cometió.

También los jueces tienen a menudo una falta de experiencia técnica que les dificulta hacer lo que hacen las cortes: interpretar las leyes. El hecho de que muchas leyes sobre crímenes por ordenador usen un lenguaje vago exacerba el problema.

La falta de conocimientos técnicos también entra en juego cuando los jueces dictan sentencia. En un intento por “hacer que el castigo esté acorde con el delito”, en muchas jurisdicciones los jueces ejercitan la creatividad al tratar con delitos relacionados con computadoras. En lugar de asignar las penas normalmente asociadas con conductas criminales, multas y/o encarcelamiento, los jueces están imponiendo sentencias tales como libertad condicional con “no uso de computadoras o redes” por un período específico de tiempo. En el mundo de hoy, donde las computadoras se están convirtiendo rápidamente en omnipresentes, una interpretación estricta de algunas sentencias le prohibiría a la persona el uso de la red telefónica y le haría prácticamente imposible el funcionar – y seguramente imposible para él o ella el obtener un empleo productivo.

Los oficiales de los correccionales no necesitan experiencia tecnológica para tratar con criminales cibernéticos presos, pero tienen ante sí el reto de una creciente población de prisioneros diferente a la típica clase baja de antaño, el delincuente mal educado que están acostumbrados a tratar. Los criminales de cuello blanco podrían correr especial peligro dentro de la población de una prisión general, pero el darle facilidades diferentes podría traer consigo quejas de políticos y entendidos de que están alojados en “clubes de campo” y que reciben tratamiento preferencial. Esta situación podría agravarse hasta el punto de surgir debates con acusaciones de discriminación racial ya que la mayoría de los criminales cibernéticos convictos son blancos, lo opuesto a la población de la prisión en general.

La respuesta a todos estos dilemas es la misma: programas de educación y consciencia. Estos programas deben estar dirigidos a todos los involucrados en la lucha contra el crimen cibernético, incluyendo:

- Legisladores y otros políticos
- Profesionales de la justicia penal

- Profesionales de la informática
- La comunidad en general y la comunidad del ciberespacio en particular

Educando a los que Luchan contra el Crimen Cibernético

Una estrategia efectiva para combatir el crimen cibernético requiere que eduquemos y entrenemos a todos los involucrados en prevenir, detectar, reportar o procesar el crimen cibernético. Incluso los criminales cibernéticos potenciales, con una educación correcta, podrían desviarse del comportamiento criminal.

Educando a los Legisladores y Profesionales de la Justicia Penal

Quienes redactan, hacen respetar y hacen cumplir la ley ya comprenden los elementos básicos de la legislación, investigación y del enjuiciamiento. Ellos necesitan capacitarse en los principios básicos de la tecnología de la información: cómo funcionan las computadoras, cómo funcionan las redes, qué se puede conseguir con la computación y qué no, y lo más importante, cómo se pueden cometer crímenes usando computadoras y redes.

Esta capacitación, para que resulte más provechosa, debe estar dirigida a la audiencia de la justicia penal en lugar de re-embalar el mismo material y enseñarlo de la misma manera que se emplea para capacitar a los profesionales de la informática. Aunque mucha de la información podría ser la misma, el objetivo y el alcance deben ser diferentes. Un investigador de crímenes cibernéticos no necesita conocer los detalles de cómo instalar y configurar un sistema operativo. Él o ella sí necesita conocer cómo un hacker puede aprovecharse de las configuraciones implícitas para obtener acceso no autorizado al sistema.

La capacitación necesaria para que los legisladores comprendan las leyes que proponen y llevan a votación es diferente a la capacitación que necesitan los detectives para descubrir evidencia digital. Los segundos deben recibir no sólo entrenamiento teórico, sino también entrenamiento práctico para trabajar con el descubrimiento, la recuperación, la codificación y decodificación de datos, y para leer e interpretar ficheros de auditoria y visores de sucesos. Los fiscales necesitan capacitación para comprender los significados de varios tipos de evidencia digital y la mejor forma de presentarlas en el juicio.

Las academias de policías deben incluir un bloque sobre la investigación de crímenes por ordenador en sus cursos básicos sobre investigación criminal. Las agencias deben, como norma, proveer a sus oficiales en servicio con una capacitación más avanzada en el tema del crimen por ordenador. Muchos buenos programas de capacitación sobre ciencia forense aplicada a la computación están disponibles, pero en muchas áreas estos tienden a ser seminarios muy caros, de corta duración, organizados por compañías del negocio para obtener ganancias, o programas regulares limitados a agencias de policías más grandes y más urbanas. Los matriculados tienden principalmente a ser detectives. Pocos estados tienen los currículos con la calidad requerida para la capacitación en el tema del crimen por ordenador en sus programas básicos de la academia o como una parte requerida de la educación para adultos de los oficiales.

En áreas rurales y jurisdicciones de pueblos pequeños, pocos, por no decir ningún oficial, tiene entrenamiento en la investigación de crímenes por ordenador, aunque esta situación está cambiando lentamente. Nuevamente, los oficiales que sí tienen el entrenamiento son por lo general detectives u oficiales de alto rango, sin embargo, el patrullero es, generalmente, es el primero en enfrentarse a la escena del crimen. Él o ella está en posición de reconocer y preservar (o, inconscientemente, destruir o permitir que se destruya) valiosa evidencia digital.

Sería ideal que todos los miembros del sistema de justicia penal recibieran algún entrenamiento básico en tecnología de redes y computadoras y en ciencias forenses. Sin embargo, esta es una meta irrealista a corto plazo. La mejor solución próxima es establecer y entrenar unidades o equipos para que se especialicen en crímenes relacionados con computadoras. Si cada cuerpo legislativo tuviera un comité de miembros adiestrados y concentrados en cuestiones tecnológicas, si cada departamento policial tuviera una unidad de investigación de crímenes por ordenador con un entrenamiento y una pericia especiales, y si cada oficina del Fiscal del Distrito tuviera uno o más fiscales que fueran especialistas en crímenes por ordenador, estaríamos muy cerca de construir un mecanismo efectivo y coordinado de lucha contra el crimen cibernético.

Por años, los cuerpos encargados de imponer el cumplimiento de la ley han quedado atrás en lo que se refiere a la adopción de tecnologías de computación en sus departamentos. Durante la última década, la comunidad policial ha comenzado a ponerse al día. Agencias federales como el FBI tienen excelentes potenciales en cuanto a la ciencia forense aplicada a la computación. Grandes organizaciones de policía tales como la Asociación Internacional de Jefes de Policía (IACP) y la Policía Internacional Futurista (PFI) han abrazado las cuestiones de la tecnología moderna y le dan a las agencias excelentes recursos. Los departamentos de policía metropolitanos y las agencias de policía estatales han reconocido la importancia de entender la computación y establecer unidades especiales y programas de capacitación para enfrentar las cuestiones del crimen por ordenador. Pero los cuerpos encargados de imponer el cumplimiento de la ley en los Estados Unidos y otros países tienen todavía un largo camino por delante para lograr que todas las agencias de la policía tengan las habilidades técnicas para comprender y combatir el crimen cibernético.

Esas agencias que todavía carecen de esa pericia pueden beneficiarse grandemente si trabajan en conjunto con otras agencias más sofisticadas desde el punto de vista técnico y se asocian con miembros de la comunidad informática seleccionados cuidadosamente para alcanzar el entrenamiento que necesitan y crear un plan de lucha contra el crimen cibernético para sus jurisdicciones. La Internet tiene alcance en las más remotas áreas del país y del mundo. El crimen cibernético no puede quedarse como una cuestión de los cuerpos encargados de imponer el cumplimiento de la ley en las grandes ciudades; los criminales del ciberespacio y sus víctimas pueden encontrarse en cualquier jurisdicción.

Educando a los Profesionales de la Informática

Los profesionales de la informática ya saben lo que es la seguridad informática y cómo se puede violar. La comunidad informática necesita ser educada en otras áreas:

- **Consciencia del delito electrónico** La comprensión de qué es y no es ilegal, la diferencia entre la ley civil y la penal, la penalidad y cuestiones legales.
- **Cómo se hacen las leyes** Esta área trata sobre cómo los profesionales de la informática se pueden involucrar a nivel legislativo testificando ante comisiones, compartiendo su pericia y dándole a conocer sus opiniones a miembros de los cuerpos gubernamentales.
- **Cómo se investigan los crímenes** Esta área trata sobre cómo los profesionales de la informática se pueden involucrar a nivel investigativo ayudando a la policía, en calidad de víctimas y partes interesadas y como asesores de las agencias encargadas de imponer el orden.
- **Cómo se procesan los crímenes** Esta área trata sobre cómo los profesionales de la informática se pueden involucrar a nivel de juicio como testigos expertos.
- **La teoría básica y el propósito detrás de la ley y el sistema de justicia penales** Esta área trata sobre cómo los profesionales de la informática deben respaldar las leyes en contra del crimen por ordenador.

Quizás el tema más controversial gira en torno a la actitud de muchos profesionales de la informática para con los policías y los cuerpos encargados de imponer la ley. Aunque no sucede así en todo el mundo, es común encontrar en algunas partes de la comunidad informática una antipatía hacia las figuras del gobierno y las autoridades.

Indudablemente existen varias razones para esta actitud. Las habilidades en el campo de la tecnología son altamente valoradas, así que los hackers expertos cosechan una cierta suma de admiradores, incluso entre muchos informáticos de compañías. La industria de la informática es joven, comparada con otras profesiones, y en gran medida, no ha estado regulada. Los profesionales de la informática le temen a la ineficiencia y a mayores dificultades que la sobre-regulación les impondría mientras realizan su trabajo, tal y como han visto sucederle a otras profesiones. Muchas personas del sector tecnológico no están familiarizados con los procedimientos legales, y la desconfianza hacia lo desconocido es una reacción común en los humanos. Finalmente, muchos de este sector creen en el eslogan de los hackers: “la información quiere ser libre” y no están de acuerdo con al menos algunas de las leyes sobre el crimen cibernético (particularmente aquellas que restringen las tecnologías de encriptación y convierten las violaciones de los derechos de reproducción de softwares, música o películas en delitos criminales).

Por todas estas razones y a fin de comprometer de forma activa al mundo informático en la lucha contra el crimen cibernético, afrontamos el reto de educar a los informáticos en que las leyes contra el crimen cibernético realmente funcionan en su beneficio. No seremos capaces de hacerlo a menos que le demos a estos profesionales que las leyes en sí son justas, que se hacen cumplir con justicia y que, efectivamente, se pueden hacer cumplir. Los administradores de redes y otros profesionales de la informática son generalmente personas ocupadas. Aún cuando creyeran que los criminales del ciberespacio deben ser

ajusticiados, no perderían el tiempo en reportar sospechas de violaciones de la seguridad o en trabajar con los policías en investigaciones si no confían en la competencia o integridad del sistema de justicia penal.

Una forma en que los informáticos pueden familiarizarse más y sentirse más cómodos con el proceso legal es exponiéndolos más a este. El personal de los cuerpos encargados de imponer la ley deberían solicitar activamente su ayuda e involucrarlos tanto como sea posible en la lucha contra el crimen cibernético, dándole una participación especial en el resultado.

Educando y Comprometiendo a la Comunidad

Finalmente, debemos educar a la comunidad en general, especialmente al subconjunto conformado por los usuarios finales de sistemas de redes y computadoras. Estas son las personas que, a menudo, son las víctimas directas del crimen cibernético y todos ellos, en última instancia, son víctimas indirectas en términos de costos extra que pagan cuando las compañías que patrocinan se convierten en víctimas de estos delitos y por los dólares extra en contribuciones que gastan cada año en respuesta a los crímenes relacionados con computadoras.

Iniciativas como la creación de grupos de vigilancia en el vecindario y otros programas similares le han dado a los ciudadanos un modo de convertirse en pro-activos en relación con la prevención del crimen en sus localidades físicas. Se pueden desarrollar programas educativos para enseñarles a los ciudadanos de la comunidad virtual cómo protegerse en línea por sí solos. Estos programas enseñarían a los usuarios de las redes sobre tipos comunes de crímenes cibernéticos, cómo reconocer cuando están en peligro de convertirse en víctimas de ellos y qué hacer en caso de que encuentren a un criminal cibernético. En algunas áreas tales como el fraude y la estafa en línea, este tipo de educación por sí sola reduciría grandemente el éxito de los estafadores. Organizaciones tales como los Ángeles del Ciberespacio (www.cyberangels.com) han sido creadas con este propósito.

Los encargados de hacer cumplir las leyes y los profesionales de la informática necesitan trabajar más de cerca con la comunidad (incluyendo negociantes, padres, estudiantes, profesores, bibliotecarios y otros) para formar un equipo de lucha contra el crimen cibernético que tenga las habilidades, los medios y la autoridad necesarios para reducir substancialmente los casos de crímenes en Internet.

Tornándose Creativos en la Lucha contra el Crimen Cibernético

La lucha contra el crimen cibernético tendrá posibilidades de éxito si la abordamos desde muchos ángulos diferentes. El proceso legal es sólo un modo de combatir el crimen. Los mejores métodos son los pro-activos y no los reactivos, o sea, es mejor prevenir el crimen antes de que suceda. Si eso no resulta, esta sección analiza algunas formas creativas en las que los negociantes e individuos pueden protegerse por sí mismos de algunas de las consecuencias de ser víctimas si ocurre un crimen cibernético.

Luchadores contra el Crimen...

Organizaciones de Lucha contra el Crimen Cibernético

La Alianza Nacional de Seguridad Cibernética es un esfuerzo conjunto entre la industria y el gobierno para promover la consciencia de seguridad en el ciberespacio mediante asistencia educacional y consciencia pública. Hay más información disponible en www.staysafeonline.info.

El Centro Nacional de Protección de Infraestructura (NIPC) se creó en 1998 y se encuentra ubicado en las oficinas centrales del FBI en Washington, D.C. Combina representantes de los gobiernos federal, estatal y local, el sector militar y el privado para proteger las infraestructuras críticas de la nación, incluyendo la Internet. Hay más información disponible en www.nipc.gov.

La Asociación Internacional de Especialistas en Sistemas de computación de Información (IACIS) es una organización internacional compuesta por voluntarios de las agencias encargadas de hacer cumplir la ley en la localidad, el estado y el país. La IACIS ofrece cursos de capacitación y educación en el campo de la ciencia forense aplicada a la computación. Hay más información disponible en <http://cops.org>.

Usando la Presión de Coetáneos para Combatir el Crimen Cibernético

Un modo de reducir la incidencia de crímenes en Internet es incitando a los grupos a aplicar la presión de coetáneos entre sus miembros. Si los criminales del ciberespacio se sienten avergonzados en vez de admirados, será un poco menos probable que asuman una conducta criminal. Este método es especialmente efectivo cuando se trata de jóvenes. Muchos hackers adolescentes entran en redes para impresionar a sus amigos. Si se le enseñara antes un código de ética de computación a los jóvenes con orientaciones tecnológicas, enfatizando en el respeto hacia la propiedad de otros y en que el territorio en el mundo virtual es tan importante como lo es en el mundo físico, quizás los hackers ya no serían admirados por la mayoría de los estudiantes honestos como no lo son los “chicos malos” que roban autos o entran a robar en casas.

Ciertamente se ha demostrado que la presión entre coetáneos y los cambios en las actitudes de los miembros de estos grupos pueden influenciar el comportamiento. En un alto grado, el creciente estigma social asociado al acto de fumar ha estado vinculado con una declinación en el porcentaje de fumadores en los Estados Unidos.

Por supuesto, algunas personas cometerán delitos sin tener en cuenta la presión de sus coetáneos, pero esta presión es una invaluable herramienta contra muchos de esos criminales cibernéticos que, fuera de ese entorno, son miembros íntegros de la comunidad y cuyo comportamiento criminal en línea refleja erróneamente la creencia de que “todos lo hacen”.

En la escena....

Experiencias de la Vida Real

Jorge González, el dueño de un portal de archivos compartidos en Internet, Zeropaid.com, aplicó un método innovador para combatir el intercambio de pornografía infantil a través de su sitio. Puso un número de ficheros fantasmas en el sitio que utiliza el popular programa de compartimiento de ficheros Gnutella. Estos ficheros fantasmas son identificados como imágenes porno infantiles, aunque no lo son. Cuando los usuarios tratan de acceder a estos ficheros, estos están “mutilados”. La dirección IP del usuario (que se puede utilizar para rastrear su identidad) se almacena y se coloca en el “Mural de la Vergüenza” del sitio. (El sitio del Mural de la Vergüenza fue creado realmente por un usuario de Gnutella quien se identificó a sí mismo como Lexx Nexus). Esta táctica es similar a las tácticas de algunos periódicos que publican el nombre de personas arrestadas por crímenes como conducir ebrio o prostitución. La premisa es que el temor a la publicidad disuade a algunas personas de cometer esos crímenes.

Usando la Tecnología para Combatir el Crimen Cibernético

En el espíritu de “pagar con la misma moneda”, una de nuestras mejores armas contra los crímenes tecnológicos es – lo adivinó – la tecnología. La industria de la seguridad de computadoras y redes trabaja fuertemente desarrollando hardware y softwares para ayudar a prevenir y detectar intrusiones en la red. Los comercializadores de sistemas operativos están incluyendo cada vez más características de seguridad incorporadas a sus sistemas operativos. En enero de 2002, Bill Gates anunció que, en lo sucesivo, la seguridad sería la máxima prioridad al desarrollar productos Microsoft y que los equipos de desarrollo de sus productos estaban provistos de una capacitación amplia en el tema de la seguridad.

Los productos de seguridad de los intermediarios, desde equipos de autenticación biométrica hasta softwares de muro de fuego, están disponibles en abundancia para evitar que los criminales cibernéticos invadan su red o sistema. Los paquetes de monitoreo y auditoria le permiten a los informáticos reunir información detallada para ayudar a detectar actividades sospechosas. Muchos de estos paquetes incluyen características de notificación que pueden alertar a los administradores de redes inmediatamente que la violación ocurra.

Los productos de recuperación de datos ayudan al personal de la investigación a obtener evidencia a pesar de los esfuerzos de los criminales por destruirla, y la policía puede – con una orden de registro – entrar a los sistemas protegidos de los criminales empleando las mismas herramientas que utilizan los hackers para entrar ilegalmente a los sistemas.

Analizaremos todas estas tecnologías y más en el Capítulo 7 “Comprendiendo la Prevención del Crimen Cibernético”, Capítulo 8 “Implementando la Seguridad del Sistema”, Capítulo 9 “Implementando Técnicas de Detección del Crimen Cibernético” y Capítulo 10 “Recopilando y Preservando la Evidencia Digital”.

Encontrando Nuevas Formas de Protección contra el Crimen Cibernético

No es posible prevenir todos los crímenes cibernéticos o evitar siempre convertirse en una víctima de estos crímenes. Sin embargo, las organizaciones y los individuos pueden dar

pasos de avance para minimizar el impacto que tendrá el crimen cibernético sobre ellos o sus organizaciones.

Por ejemplo, *The Austin Business Journal* reportó en la edición publicada el 28 de abril de 2000 que las compañías están sacando pólizas de seguro para cubrir los daños relacionados con crímenes cibernéticos. Como el problema del crimen cibernético va en aumento, es inevitable que las víctimas potenciales se aparezcan con nuevas formas de protegerse de sufrir pérdidas financieras.

Resumen

El crimen cibernético ya es un gran problema en todo el mundo – y está creciendo rápidamente. Los investigadores están luchando por ponerse al nivel, los legisladores están aceptando nuevas leyes para afrontar esta nueva manera de cometer crímenes, y las agencias de policías están formando unidades especiales encargadas de los crímenes por ordenador y están presionando a sus oficiales para que adquieran cada vez más habilidades técnicas.

Sin embargo, el problema del crimen cibernético es demasiado grande y está demasiado generalizado como para dejar que los políticos y la policía lo resuelvan. Los primeros, a menudo, no tienen la pericia técnica para aceptar leyes efectivas y los segundos adolecen de suficiente capacitación, personal y tiempo – sin mencionar la abrumadora cuestión de la jurisdicción – para enfrentarse a cualquiera de los atroces crímenes en Internet.

El crimen cibernético, como el crimen en general, es un problema social y legal. Para combatirlo exitosamente, tenemos que comprometer a las personas de la comunidad informática (muchos de ellos quizás estén renuentes a participar) y a aquellos de la población en general que se afectan, directa o indirectamente, con la actividad criminal que ha encontrado un refugio agradable en el mundo virtual.

Podemos utilizar un número de tácticas y técnicas, incluyendo el sistema legal, la presión entre coetáneos, y las tecnologías existentes y emergentes para prevenir el crimen cibernético. Si no resulta, podemos desarrollar respuestas formales e informales que detectarán el crimen cibernético de forma más inmediata, minimizando el daño hecho y dándonos más información acerca del incidente, incrementando las posibilidades de identificar y procesar exitosamente al criminal cibernético.

Todos estamos juntos en el mismo bote. El único modo de detener el crimen cibernético es trabajando en conjunto y compartiendo nuestros conocimientos y nuestra pericia en las diferentes áreas para conformar un equipo de lucha contra el crimen cibernético clase A.

Preguntas Realizadas con Frecuencia

Las siguientes preguntas realizadas con frecuencia, respondidas por los autores de este libro, están diseñadas para medir su comprensión de los conceptos presentados en este capítulo y para ayudarle con la implementación de estos conceptos en la vida real. Para

hacer que el autor conteste a sus preguntas, visite www.syngress.com/solutions y haga clic en el formulario “**Pregúntale al autor**”.

P: ¿La comunidad de investigadores se opone al uso de la encriptación?

R: La mayoría de los profesionales de este sector que se especializan en crímenes cibernéticos no se oponen al uso de la encriptación para comunicaciones legales. El Departamento de Justicia plantea su posición oficial en el sitio Web www.cybercrime.gov: “No nos oponemos al uso de la encriptación – todo lo contrario, pues una buena encriptación puede constituir una herramienta extraordinaria para prevenir el crimen. Creemos que el uso de una buena encriptación resulta fundamental para el desarrollo de la “Infraestructura Global de la Información” o la IGI. Estamos de acuerdo con que las comunicaciones y los datos deben ser protegidos – en tránsito y en almacenamiento – si la IGI es para ser usada en comunicaciones personales, transacciones financieras, atención médica, el desarrollo de una propiedad intelectual y otras aplicaciones. El uso generalizado de una encriptación irrecuperable por criminales, sin embargo, representa un riesgo serio para la seguridad pública.”

P: ¿La piratería de softwares es realmente un gran problema?

R: De acuerdo con algunos estimados, el carterista promedio obtiene sólo \$20 o \$30usd por cartera robada y el ladrón a mano armada (atracaador) \$50usd o menos. Por el contrario, los programas de software pirateados cuestan a menudo desde varios cientos hasta varios miles de dólares. Por consiguiente, desde el punto de vista económico, un acto de piratería de softwares es varias veces más “serio” que ser víctima de un ladronzuelo o un atracaador.

P: ¿Entonces por qué muchas personas sienten que la piratería de softwares no es un crimen serio?

R: Existen varias razones. La piratería de softwares no tiene el impacto emocional, cara a cara que tienen el robo de carteras y los atracos. El software es “intangible”, está conformado por bits y bytes de datos electrónicos, a diferencia de una pieza de propiedad física. La piratería de softwares no es un “robo” en el significado tradicional de la palabra, porque es tomado mediante copias, no privando al dueño de su uso. Muchas personas sienten que los términos de licencia de los comerciantes de softwares son injustos y es por eso que la piratería es de algún modo una represalia justificada. También existe un criterio general de que, como la copia de softwares está tan generalizada y parece no hacer daño alguno, no es un “crimen real” (similar al modo de pensar acerca del exceso de velocidad de muchas personas que nunca pensaron llevarse la luz roja).

P: ¿Con todos los productos de seguridad para redes y computadoras que existen actualmente en el mercado, por qué los sistemas no están completamente asegurados?

R: A pesar de todos los productos excelentes que encontramos disponibles en el mercado, la única computadora completamente segura es la que está apagada. En los entrenamientos con armas de fuego de los cuerpos encargados de imponer el cumplimiento de la ley, los oficiales aprenden sobre las “fundas de seguridad” que están diseñadas para evitar que el

criminal tome el arma del oficial y la use contra él o ella. La primera cosa que aprende un oficial que prueba una funda de seguridad es que es más complicada de usar que una tradicional, no asegurada y que el oficial debe practicar diligentemente o no será capaz de desenfundar su arma cuando sea necesario. La verdad es que la única funda totalmente segura es aquella en la que el arma está permanentemente pegada, por lo tanto no es accesible para el tipo malo, pero tampoco es accesible para el oficial. La seguridad de la red y las computadoras incluye este mismo acto de balance entre seguridad y accesibilidad, y los dos factores están siempre encontrados. Mientras más seguros estén sus sistemas, menos accesibles serán y viceversa. Debido a que el verdadero propósito de una red de computadoras es la accesibilidad, ninguna red será jamás 100% segura.

Referencias

- Reportes estadísticos del *Internet Fraud Complaint Center, IFCC* (Centro de Quejas de Fraudes Electrónicos)
www1.ifccfbi.gov/index.asp
- Computer Security Institute 2001 (Instituto para la Seguridad Electrónica) *Crimen por Ordenador y Sondeo de Seguridad*
www.gocsi.com/prelea/000321.html
- Estadísticas Básicas de Reportes de Crímenes de Cybersnicth
www.cybersnicth.net/csinfo/csdatabase.asp
- Consultora Meridien Research
www.meridien-research.com
- National Cybercrime Training Partnership, NCTP (Asociación Nacional de Entrenamiento contra el Crimen Cibernético)
www.nctp.org
- International Association of Chiefs of Police, IACP (Asociación Internacional de Jefes de Policía)
Conferencia de capacitación para el manejo de la información por parte de los cuerpos encargados de hacer cumplir la ley
www.iacptechnology.org/2002LEIM.htm
- Consejo de la Convención Europea sobre el Tratado del Crimen Cibernético
<http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185>
- Décimo Congreso de Naciones Unidas sobre la Prevención del Crimen y el Tratamiento a los Infractores, Viena, Abril del año 2000
www.uncjin.org/Documents/congr10/4r3e.pdf
- Código Penal de Texas, Capítulo 33, Crímenes por ordenador
www.capitol.state.tx.us/statutes/pe/pe003300.html#pe001.33.01

- Código Penal de California, Sección 502, Crímenes por Ordenador
<http://caselaw.lp.findlaw.com/cacodes/pen/484-502.9.html>
- *Terrorismo Cibernético: realidad o fantasía*, Mark M. Pollitt, Laboratorio del FBI
www.cs.georgetown.edu/~denning/infosec/pollitt.html
- Centro Nacional para Víctimas del Acecho Cibernético
www.ncvc.org/special/cyber_stk.htm
- Regulación de la Pornografía Infantil en Internet, página informativa
www.cyber-rights.org/reports/child.htm
- CNN.com, 8 de enero de 2002: Reporte: *El Vandalismo Cibernético aumentó en el 2001*
www.cnn.com/2002/TECH/internet/01/08/cybervandal.jump.idg/?related
- E-Commerce Times, 13 de Marzo de 2001: *Economía Nueva, La Profesión más Antigua*
www.ecommercetimes.com/perl/story/8121.html
- *Comprendiendo la Ley sobre los Juegos de Azar en Internet*, I. Nelson Rose, Profesor de Leyes
www.gamblingandthelaw.com/internet_gambling.html
- *Regulación de Farmacias en línea*, Amy Cassner-Sems
www.gase.com/cyberlaw/toppage1.htm
- Temas actuales de EduCause: Ley de Derechos de Reproducción del Milenio Digital
www.educause.edu/issues.dmca.html

Repasando la Historia del Crimen Cibernético

Tópicos que investigaremos en este capítulo:

- Explorando la criminalidad en los tiempos de las computadoras como estaciones de trabajo individuales
- Comprendiendo a los primeros phreakers, hackers y crackers
- Cómo los servicios en línea facilitaron el crimen cibernético
- Introduciendo la ARPANet: El oeste salvaje de la interconexión
- Observando el incremento de los crímenes a partir de la comercialización de la Internet
- Actualizando la historia del crimen cibernético

- ✓ Resumen
- ✓ Preguntas Realizadas con Frecuencia
- ✓ Referencias

Introducción

¿Cuántos años tiene el fenómeno del crimen cibernético? Es seguro decir que tan pronto se construyeron las primeras redes de computadoras, algunas personas ya buscaban modos de explotarlas para sus propios propósitos ilegales. La idea del robo es tan antigua como el concepto de la propiedad privada y un elemento de casi todas las sociedades está dedicado a tomar tanto como sea posible de lo que no es suyo – utilizando cualquier medio a su alcance.

Apenas fue ampliamente admitido que las computadoras almacenan algo de valor (información), los criminales vieron una oportunidad. Pero como mismo resulta difícil llegar a la víctima de un asalto que se mantiene encerrada todos los días en su propia casa, los datos en sistemas cerrados de estaciones de trabajo han sido difíciles de robar. Sin embargo, cuando esos datos comenzaron a moverse de una computadora a otra a través de redes, al igual que la víctima del robo que viaja de un lugar a otro, estos datos se volvieron más vulnerables. Las redes ofrecen otra ventaja: un punto de entrada. Aún si la información valiosa nunca fue enviada a través del cable, las idas y venidas de otros bits de datos abrieron un camino para que los intrusos entraran en la computadora, como un ladrón que se aprovecha de que la persona que vive con la víctima deje la puerta abierta al salir.

Sin embargo, el crimen cibernético no surgió como un auténtico problema de la noche a la mañana. En los primeros tiempos de la computación y la interconexión, el criminal promedio no poseía la pericia técnica o los conocimientos de hardware necesarios para aprovechar la oportunidad digital del día. Las computadoras eran monstruosidades de unidades centrales que costaban millones de dólares y solo existían pocas. Un aspirante a criminal cibernético difícilmente podía salir y comprar (o robar) una computadora, y aún si lo hacía, es improbable que supiera qué hacer con ella. No existían aplicaciones “cómodas para el usuario”; trabajar con los sistemas de entonces requería de la habilidad de “hablar” el *idioma de la máquina* – o sea, comunicarse en los 0 y 1 del cálculo binario que entendían las computadoras.

El problema del crimen cibernético emergió y creció cuando la computación se tornó más fácil y menos costosa. Hoy día casi todos los que viven en países industrializados tienen acceso a la tecnología de la computación; los niños aprenden a usar la PC en la escuela elemental y las personas que no pueden darse el lujo de tener una computadora propia, pueden usar de forma gratuita las PC de bibliotecas públicas o recintos universitarios, o pueden rentar tiempo de máquina en centros de negocios o Cyber-café. Las aplicaciones son de “señalar y hacer clic” o incluso se pueden activar mediante el uso de la voz. Ya no es necesario tener un título en Ciencias de la Computación para llevar a cabo tareas que otrora fueron complejas como enviar un correo electrónico o descargar ficheros de otra máquina a través de Internet. Algunos de los criminales cibernéticos de hoy son programadores talentosos (la elite de los hackers), pero la mayoría no lo son. Las habilidades técnicas avanzadas le facilitan a los criminales cibernéticos “hacer sus cosas” y cubrir sus trazas, pero estas habilidades no son de ninguna manera un requerimiento para el trabajo.

En este capítulo le echaremos una mirada a estas cuestiones:

- Los retos del crimen por ordenador en los días de las computadoras individuales (estaciones de trabajo)
- Cómo operaban los primeros criminales conectados a redes
- Cómo los miembros de la ARPANet (predecesora de la Internet) incrementaron las oportunidades para la actividad criminal
- Cómo el crecimiento fenomenal de la Internet comercial condujo a un aumento igualmente fenomenal del crimen cibernético
- Cómo el advenimiento de los servicios en línea fáciles de usar como CompuServe y America Online (AOL) facilitaron aún más la criminalidad en línea
- Dónde nos encontramos hoy y cómo las “últimas y mejores” tecnologías han creado nuevas vulnerabilidades en la seguridad

Primeramente volvamos a los años 1940, cuando el Doctor J. Presper Eckert y el Doctor John W. Mauchly inventaron una de las primeras computadoras digitales, el Integrador Numérico Electrónico y Computadora (ENIAC).

Explorando la Criminalidad en los Días de las Computadoras Individuales (estaciones de trabajo)

La ENIAC era una monstruosidad que necesitaba más de 1500pies cuadrados de espacio en piso, más que muchas de las “casas de principiantes” en la actualidad. Esta máquina gigantesca utilizaba más de 17,000 tubos de vacío y podía hacer alrededor de 1000 cálculos por segundo, comparado con los millones de cálculos por segundo alcanzados por las PC modernas, compactas y económicas.

La ENIAC fue un tremendo logro, pero los buenos doctores involucrados en esta creación no se durmieron en los laureles. En 1949 introdujeron la Computadora Binaria Automática (BINAC) que almacenaba datos en una cinta magnética. Poco tiempo después, inventaron la Computadora Automática Universal (UNIVAC), la primera computadora comercializada bajo un subsidio del gobierno de los Estados Unidos.

Cuando la primera UNIVAC fue entregada a la Oficina de Censos de los Estados Unidos en 1951, tenía el tamaño de la habitación y costaba 1 millón de dólares. El fabricante construyó eventualmente 46 UNIVAC para usuarios del gobierno y negociantes. Esta utilizaba cinta magnética que era más rápida que el sistema de fichas perforadas de la IBM que era su competidor directo.

Nota

Las primeras máquinas de tabulación por fichas perforadas fueron inventadas a finales del 1800 por un ingeniero nombrado Herman Hollerith. Al igual que la UNIVAC, la tecnología de fichas perforadas fue originalmente desarrollada para que la Oficina de Censos de los Estados Unidos la utilizara para clasificar y analizar sus datos. La Compañía de Máquinas Tabuladoras de Hollerith, fundada en 1896, fue adquirida por la IBM en 1924.

Estas primeras computadoras tenían algunas ventajas inherentes con respecto a la seguridad: eran inmensas y costosas, eran estaciones de trabajo y la mayoría del mundo no sabía realmente qué era una computadora y mucho menos cómo usarla.

Compartiendo Más que Tiempo

No tardarían mucho los científicos en enamorarse de las computadoras. El Procesador de Datos Programados (PD-1), desarrollado y comercializado por la Digital Equipment Corporation (DEC) en los años 1960, fue la primera computadora utilizada para compartir el tiempo comercial (o sea, los propietarios de las computadoras rentaban tiempo de máquina a otros negocios, escuelas, laboratorios y a programadores que no podían darse el lujo de comprar sus propias computadoras).

Debido a que numerosas personas y negocios usaban la misma computadora, los datos y programas almacenados en ella eran vulnerables. Por consiguiente, se abrieron las primeras puertas para el hackeo – y a pesar de los esfuerzos de los administradores de sistemas, comerciantes de productos para la seguridad y cuerpos encargados de hacer cumplir la ley, esas puertas no se han vuelto a cerrar desde entonces.

La Evolución de una Palabra

En los años 1960, el término *hacker* se usaba para referirse a alguien que se consideraba un “programador real”, quien dominaba los sistemas computarizados de aquellos días y era capaz de manipular programas para que hicieran más de lo que originalmente estaba concebido que hicieran.

A finales de los 60 y principios de los 70, el hackeo se asoció con el movimiento radical clandestino (“yippie”) y tomó un sabor contrario a lo establecido. Las agencias encargadas de hacer cumplir el orden comenzaron a arrestar a los *phreakers* por manipular los sistemas telefónicos, como analizaremos más detalladamente en la siguiente sección. En los años 80, el FBI hizo algunos de los primeros arrestos de alto perfil de hackers de computadoras (incluyendo el de Kevin Mitnick que se convirtió en algo así como “un mártir para la causa” dentro de la comunidad de los hackers). Películas como *WarGames (Juegos de Guerra)* de John Badham en los 80 y *Hackers* de Iain Softlwy en los 90 introdujeron en la corriente dominante el concepto del hacker como una figura brillante y de cierta forma romántica que violaba la ley (pero generalmente con nobles propósitos).

Nota

El primer grupo de hackers se formó, como es lógico, en el Instituto de Tecnología de Massachussets (MIT) en 1961, poco después que el MIT recibiera su primera PDP-1. El grupo llamado The Tech Model Railroad Club, estaba compuesto por miembros quienes programaban por el simple gusto de hacerlo – la esencia del hackeo en su sentido original.

Comprendiendo a los Primeros Phreakers, Hackers y Crackers

El hackeo en el sentido moderno de la palabra – cuando se aplica a alguien que entra sin autorización a los sistemas, generalmente desde un puesto remoto – no hubiese podido llegar a lo que es sin la red. Sin embargo, no podemos olvidar que las redes existieron mucho antes de que existieran las computadoras. Desde los años 40, cuando se crearon las primeras computadoras reales, la inmensa red telefónica global de nuestros días, cuya construcción comenzó a finales de los años 1800, ha estado creciendo a un ritmo constante por un período ya de 60 años.

Los primeros hackers electrónicos entraron al sistema telefónico para efectuar llamadas de larga distancia sin tener que pagarlas. Estos hackers de la red telefónica se conocieron como *phreakers*. Otro término que se originó durante los primeros años de la comunicación electrónica es *cracker*, empleado para describir a alguien que “fuerza” la seguridad de un sistema. Este término ahora se refiere a menudo a alguien que se especializa en descifrar contraseñas.

Hackeando la Red Telefónica de Ma Bell

Un estudiante del MIT nombrado Stewart Nelson, quien descubrió cómo usar la computadora del instituto para generar los tonos de acceso al servicio de larga distancia de la compañía de teléfonos, fue uno de los primeros llamados phreakers, de acuerdo con el artículo *Historia de los Hackers - Phreakers* en la sección Seguridad en las Redes/Internet del sitio Web About.com.

Algunos phreakers especialmente talentosos eran capaces de reproducir esos tonos simplemente silbando, pero la mayoría de los phreakers usaban un aparato llamado *blue box* (la caja azul), que era un generador de tonos para reproducir la frecuencia de 2600Hz. Los sistemas telefónicos actuales no usan el tono 2600 para el acceso de larga distancia, pero todavía existe un contingente activo de phreakers que se aprovechan de las complejidades de los sistemas modernos para encontrar nuevas formas de explotar la tecnología del sistema telefónico en su beneficio.

Phreakers Famosos

John Draper, veterano de la Fuerza Aérea de los Estados Unidos y técnico en ingeniería de la National Semiconductor, alias Capitán Crunch. Generalmente se le otorga el crédito de diseñar la caja azul original después de descubrir que el silbato que venía en las cajas de cereales del Capitán Crunch podía producir la señal de 2600Hz que concedía el acceso al servicio de larga distancia de AT&T. Draper fue arrestado y guardó prisión en una cárcel de mínima seguridad por causa de esta infracción. De acuerdo con la leyenda, dio seminarios mientras estuvo prisionero, enseñando a otros presos cómo hackear el sistema telefónico. Luego fue arrestado nuevamente en Nueva York.

Steve Jobs y Steve Wozniak, quienes fundaron luego la Apple Computer, aparecen reportados por varias fuentes (incluyendo al propio Wozniak que trabajó para Draper antes de conocer a Jobs) por haber hecho y vendido cajas azules a principios de los años 70.

Nota

La revista *2600 Magazine* y su sitio Web, fuentes populares para el hacker clandestino, recibieron sus nombres por la frecuencia de hackeo de la red telefónica de 2600Hz.

Hackeando la Red Telefónica en el otro Lado del Atlántico

El sistema telefónico británico tiene sus propios phreakers que datan de la época en que fue descubierta y explotada la “herramienta A” del hackeo para liberar las llamadas de larga distancia. Más tarde, los phreakers británicos construyeron “cajas beeper” que tenían el mismo propósito de las cajas azules en los Estados Unidos, pero que usaban diferentes juegos de frecuencias.

Una Caja para Cada Esquema de Color

Además de la caja azul original, los phreakers construyeron un número de otros equipos para burlar el sistema telefónico. La *caja roja* reproduce los tonos producidos cuando se depositan las monedas en un teléfono público, y una *caja negra* permite hacer llamadas exentas de pago desde el teléfono al cual está conectada.

No todos los hackeos de la red telefónica fueron hechos con el propósito de burlar el pago de las llamadas de larga distancia. La manipulación del sistema telefónico también era popular entre personas involucradas en otras actividades criminales para cubrir sus rastros al efectuar negocios ilegales a través del teléfono. La *caja de queso* fue concebida para conectar dos líneas a un teléfono de modo que le permitiera a los corredores de apuestas o negociantes de drogas recibir llamadas de otro lugar remoto y salir a través de la caja de queso para ocultar el número donde realmente estaban ubicados.

Del Phreaker al Hacker

Una gran cantidad de información acerca de los phreakers se encuentra disponible en la Web, incluyendo instrucciones detalladas para los phreakers “novatos”. La “actitud” de los phreakers (desprecio hacia las grandes corporaciones como la compañía de teléfonos y la creencia en el “derecho” de aquellos que son lo suficientemente inteligentes para estafar a estas corporaciones) formó la base de la subcultura posterior de los hackers. Muchos de los primeros hackers de computadoras comenzaron sus carreras criminales como phreakers de teléfonos.

Viviendo en la LAN: Los Primeros Hackers de Redes de Computadoras

En los años 70 salió al mercado la primera computadora personal asequible, la Altair 8800. La máquina se vendió por piezas que el comprador tenía que armar y una vez armada no hacía mucho porque el propietario también tenía que escribir sus propios programas para ella. No obstante, la Altair dio luz al hackeo como lo conocemos hoy. Este equipo hizo posible que los individuos tuvieran sus propias computadoras y aprendieran a programar.

Le siguieron otras computadoras de relativo bajo costo: la Commodore 64 fue un “juguete” popular que introdujo a muchos jóvenes, la mayoría adolescentes, en el disfrute de programar y más tarde, en el hackeo con todas las de la ley. La TRS-80 de la firma Radio Shack (conocida afectuosamente como la Trash 80, *basura 80*) y la PC original de la IBM trajeron consigo una computación más poderosa para las personas que estaban ansiosas por encontrar nuevas formas de explotar las capacidades del sistema. Pero fue la red de computadoras la que realmente le abrió las puertas a todos los hackers que sucedieron.

Las primeras “redes” de computadoras no estaban realmente conformadas por computadoras conectadas en red. Más bien consistían en una computadora – una unidad central - y muchas terminales que, conectadas a la unidad central, ejecutaban programas en ella y accedían a sus ficheros. Aunque esas terminales estaban conectadas en red en un sentido de la palabra, eran terminales “tontas” que no poseían poder de procesamiento por ellas mismas. Esta unidad central de compartimiento de tiempo conectaba a múltiples usuarios y les permitía compartir ficheros e impresoras. También le permitió a los primeros hackers acceder a los ficheros de otros usuarios de la unidad central.

Las desventajas de este tipo de red incluían el alto costo de la computadora y el único punto de fallas que esta representaba. Si el sistema se iba abajo, nadie en la red podía trabajar, pues las terminales que operaban eran tontas. *Mini-computadoras* (como la DEC PDP, VAX y la IBM AS/400) se crearon como alternativas más compactas y de un costo más bajo para la unidad central con todas las de la ley, pero estas máquinas todavía se basaban en terminales tontas y funcionaban esencialmente de la misma manera que las anteriores. Finalmente, la búsqueda de una forma mejor condujo a la creación de computadoras más pequeñas y menos costosas (entonces llamadas *microcomputadoras* y posteriormente denominadas *computadoras personales o PC*) que se podían colocar sobre el escritorio. Con cada trabajador teniendo una computadora con todas las de la ley en su escritorio, existía mucha más tolerancia a las fallas que con la unidad central; si una computadora se venía abajo, todos los demás podían seguir trabajando en sus computadoras.

Sin embargo, los trabajadores extrañaban algunas de las ventajas del entorno de unidad central, como la capacidad de compartir fácilmente ficheros con otros. La “Sneakernet” (red a zapato) – copiar ficheros en un disquete y transportarlo físicamente hacia otra computadora – era el mecanismo de trabajo, pero ese sistema no funcionaba muy bien cuando los usuarios que querían compartir ficheros estaban en diferentes partes del edificio o los ficheros eran demasiado grandes para que cupieran en un disquete. La solución era conectar la computadora de mesa (estación de trabajo) a una red, brindando los beneficios de compartimiento de recursos del sistema de unidad central y la tolerancia a fallas de las

computadoras descentralizadas. Las PC conectadas en redes nos dan, de muchas maneras, lo mejor de ambos mundos. También le dan a los hackers que se encuentran entre nosotros una vía de acceder a nuestra información, queramos compartirla o no.

En los años 70, investigadores del Centro de Investigaciones Xero's Palo Alto Research Center (PARC), crearon la Ethernet, la cual todavía conforma la base de la mayoría de las redes de área local (LANs) de la actualidad. DEC, Intel y Xerox se unieron en 1979 para crear los estándares de la Ethernet (originalmente llamada DIX por el nombre de las compañías) para facilitarle a los comerciantes la creación de productos compatibles. En 1983, El Instituto de Ingenieros Electrónicos y Electrotécnicos (IEEE) dio a conocer las especificaciones 802.3 basadas en cable coaxial grueso y nombradas 10Base5. La Ethernet le dio a las compañías una vía de conectar sus computadoras fácilmente y de forma relativamente económica, especialmente después de que el IEEE creara y estandarizara una segunda versión basada en cable coaxial fino (10Base2) en 1985. Las PC interconectadas comenzaron a emerger en los años 80 como una alternativa popular al uso de la unidad central (o, en algunos casos, además de ella).

Cómo los Sistemas de Boletines Electrónicos Fomentaron el Comportamiento Criminal

Además de interconectar las PC a un mismo servidor de archivos para crear una LAN, las PC se podían usar para conectarse entre sí desde lugares remotos utilizando un módem y una línea telefónica. Esto condujo al advenimiento del *sistema de boletines electrónicos (BBS)*, un sistema computarizado equipado con uno o más módems de modo que los usuarios pudieran marcar y descargar ficheros de él o enviar mensajes a una “junta” para llevar a cabo discusiones virtuales públicas.

Ward Christensen y Randy Suess crearon el software para el Sistema de Boletines Electrónicos Computarizados (CBBS) en los años 70 en Chicago. Lo describieron en un artículo publicado en la Revista *Byte Magazine* en 1978. El sistema fue un tremendo éxito y los BBS brotaron por todo el país.

Los primeros hackers y phreakers se aferraron a la idea del BBS como una vía de comunicarse entre ellos e intercambiar sus trucos y técnicas. La mayoría de las juntas incluían ambos servicios: el forum público y el servicio de mensajería electrónica entre los miembros del BBS. Aunque muchos BBS eran “sitios” legales donde los aficionados a la computación podían obtener y compartir el software que escribieron personalmente o analizar cuestiones actuales, el BBS tenía un atractivo natural para el elemento criminal. Los BBS generaron el primer método a gran escala de distribución de *warez* (jerga de los hackers para el software pirateado), con frecuencia juegos de computadora. Otros BBS se especializaron en compartir fotos pornográficas y/o cuentos.

Los primeros BBS eran lentos (los módems de 2400 baudios eran los mejores de la línea en aquel entonces) y costosos, a menos que tuviera suerte de vivir en la misma localidad de su

cohorte o que fuera un phreaker que no pagara las llamadas de larga distancia. A menudo resultaba difícil conectarse, porque la mayoría de los BBS se operaban desde la casa de alguien con un presupuesto limitado, de modo que el operador de sistemas promedio o sysop (la persona que ejecuta el BBS), no tenía un gran número de módems y líneas telefónicas. Mientras algunos sysop ejecutaban estos sistemas por diversión, muchos (especialmente aquellos que se dedicaban a la pornografía) le imponían a los miembros un impuesto mensual o anual por conectarse.

Algunos BBS todavía operan en la actualidad, pero la popularidad de esos forum comenzó a decaer en los años 1990, cuando el acceso a Internet se tornó comercialmente asequible y la naturaleza gráfica de la WWW hizo que los sistemas BBS, con sus dibujos ASCII, parecieran totalmente anticuados.

Cómo los Servicios en Línea Facilitaron el Crimen Cibernético

En los primeros días de la Internet comercial, conectarse no era necesariamente una proposición fácil. A diferencia de los sistemas operativos de hoy, los sistemas operativos en uso (mayormente Windows 3.x) no venían con la pila del Protocolo de Control de Transmisión/ Protocolo Internet (TCP/IP) incluida; tampoco incluían el software requerido para conectarse por marcación a Internet y usar sus aplicaciones (Winsock). El software correcto tenía que ser descargado, los complejos ficheros de configuración de textos debían ser editados y requería de una cierta cantidad de conocimientos técnicos (sin mencionar la paciencia) para complementarlo todo y conectarse exitosamente a Internet. Además, los usuarios tenían que hacerlo a través de los primeros proveedores de servicios de Internet Comercial (ISP), los cuales eran, a menudo, empresas nuevas en el sector creadas por un par de abelarditos con un presupuesto restringido, trabajando desde su apartamento. Estos empresarios generalmente no daban CD de instalación fácil para que los usuarios hicieran la configuración por sí mismos como la mayoría de los ISP hacen en la actualidad.

Sin embargo, existía un modo más fácil de conectarse: el servicio en línea. Compañías como CompuServe, Prodigy y AOL ofrecían acceso a sus “comunidades” de redes. Una vez que entraran al servicio, los usuarios podían descargar programas, enviar mensajes a los boletines electrónicos, encontrar información sobre una amplia variedad de tópicos y perder sorprendentes cantidades de tiempo en salas de chateo o sostener conversaciones privadas a través de la mensajería instantánea.

El mayor atractivo de estos servicios era lo fácil de usar. Ellos daban un disco que generalmente instalaba el programa apropiado automáticamente y configuraba la computadora de los usuarios, de modo que ellos no tenían que tener conocimientos del tema para conectarse. En los primeros tiempos, los servicios eran terriblemente costosos por los estándares modernos. En los años 80, costaba \$25usd *la hora* de conexión a CompuServe. Los precios disminuyeron a \$3usd la hora a principios de los 90, y, finalmente, los servicios pasaron a planes de uso ilimitado que costaban menos de 20usd al mes.

Los servicios en línea *no* eran, en los primeros tiempos, ISP. Más bien eran redes privadas de área amplia (WAN) en las cuales los miembros interactuaban entre sí, pero no con el “mundo exterior” de la Internet – eran similares a los BBS en esteroides. Luego los servicios proporcionaron puertas de enlace de correo electrónico, de modo que sus miembros podían intercambiar mensajes electrónicos con otros fuera de la red privada. Además añadieron el acceso a la WWW. Hoy día, la mayoría de los servicios en línea son también ISP. Aunque los proveedores regulares de servicio de Internet incrementaron dramáticamente la facilidad del uso de sus programas, muchos “principiantes en la Net” siguen creyendo que los servicios en línea son más fáciles de usar. Esta facilidad atrae a los criminales (junto con los usuarios oficiales) que no son particularmente muy competentes desde el punto de vista técnico.

Otro beneficio de los servicios en línea que atrae criminales es el anonimato que estos ofrecen. Generalmente, si usted abre una cuenta con un ISP regular, se le asigna un nombre de cuenta de usuario y una dirección de correo electrónico basada en el nombre. Es posible lograr que el proveedor cambie el nombre de su cuenta, pero esto representa muchas complicaciones y no se puede hacer con demasiada frecuencia. Los servicios como AOL permiten a los usuarios crear “nombres en pantalla” secundarios que pueden cambiar cada vez que lo deseen, facilitándole al criminal cambiar de identidades y cubrir sus huellas.

Introduciendo la ARPANet: el Oeste Salvaje de la Interconexión

Al principio (o lo que fue el principio de la vasta Internet global de nuestros días) existió la ARPANet. La ARPANet, finalmente, engendró a la Internet.

Estadísticas cibernéticas....

La Popularidad de los Servicios Online

De acuerdo con el sitio Web de la compañía AOL, en el año 2002, AOL tenía un estimado de 34 millones de miembros. Ahora la AOL es propietaria también de su antiguo competidor, CompuServe, que cuenta con aproximadamente 3 millones de miembros. Prodigy Communications, que fue el primer servicio en línea orientado al consumidor (fundado en 1984, un año antes que el servicio AOL), estima que su membresía es de 3.6 millones. El servicio en línea de Microsoft's Microsoft Network (MSN) tiene casi 9 millones de usuarios.

El Sputnik Inspira a la ARPA

En el año 1957, nadie podía haber previsto el sistema de comunicaciones que hoy conecta a amigos, familiares, socios de negocios y desconocidos en todo el mundo. En ese año, el presidente Dwight Eisenhower autorizó la creación de una Agencia de Proyectos de Investigación Avanzada para la Defensa (ARPA) en respuesta al lanzamiento del primer satélite artificial en órbita con la Tierra, Sputnik, por parte de la Unión Soviética.

El primer proyecto de la ARPA fue crear por sí misma un satélite para los Estados Unidos. No fue hasta años después que la agencia comenzó a trabajar con tecnologías de

computación e interconexión. En los años 60, como la guerra fría con la Unión Soviética continuaba, el gobierno consideró la posibilidad de una guerra nuclear y cómo mantener las comunicaciones si ocurría lo impensable. Así fue como comenzó la relación de la ARPA con la computación.

La ARPA Dirige sus Talentos hacia la Computación

El Dr. J.C.R. Licklider fue designado para llevar a cabo el proyecto de computación de ARPA en 1962. Él fue el responsable en gran parte de construir los comienzos de una red de área amplia conectada con sitios gubernamentales/militares y universitarios, usando vínculos redundantes, de modo que si quitaban un nodo, los mensajes podían seguir pasando al tomar otro camino. Esta red, basada en la tecnología de intercambio de paquetes, se creó en los años 60 y fue denominada ARPANet.

El primer nodo de la red fue instalado en la Universidad de California en Los Angeles (UCLA) en 1969. Otros nodos fueron instalados en la Universidad de Stanford, la Universidad de California en Santa Bárbara (UCSB) y en la Universidad de Utah en la Ciudad de Salt Lake City.

Las Aplicaciones de Redes Alcanzaron su Potencial

A principio de los años 70 , el correo electrónico – que sigue siendo hoy la “aplicación asesina” de Internet en términos de popularidad – fue inventado. Se crearon las puertas de enlace para conectar redes usando diferentes arquitecturas y se crearon especificaciones para lo que sería el Protocolo de Transferencia de Archivos (FTP).

A finales de los 70, se establecieron los grupos de noticias Usenet y aparecieron los primeros sitios interactivos multiusuarios, denominados *calabozos Multiusuarios* o MUDS. En ese entonces, la ARPANet ya existía y operaba desde hacía 10 años, aunque todavía estaba limitada mayormente a sitios gubernamentales y universitarios.

El Trabajo en Internet Continua Expandiéndose

En los primeros años 80, la suite TCP/IP fue definida como el estándar para las comunicaciones en la ARPANet. Poco tiempo después, se crearon los servidores de nombres encargados de la traducción de los nombres “amistosos” de computadoras y se utilizaron los caminos hacia las computadoras de las direcciones IP para enrutar mensajes de una computadora a otra.

La novela de ciencia ficción de William Gibson, *Neuromancer*, publicada en 1984, acuñó el término *ciberespacio* como una descripción del mundo en línea. En ese entonces, nadie tenía una idea de cuán poblado se tornaría pronto el ciberespacio.

La ARPANet de los Años 80

La red global continuaba creciendo, pero en 1986 solamente existían cerca de 500 anfitrionas (computadoras) en la Net. Por ese entonces, la Fundación Nacional para la Ciencia (NSF), que mantenía el backbone de Internet, estableció 5 centros de supercomputadoras, lo que trajo consigo un incremento dramático de las conexiones disponibles. Al siguiente año, en 1987, el número de anfitrionas había aumentado a 10,000 o 28,000 (en dependencia de la fuente que Usted consulte), y otro año más tarde, el backbone de la NSFNet alcanzaba los 1.544Mbps (una línea T-1). En 1989, todas las fuentes concuerdan con que existían más de 100,000 anfitrionas en la red.

La Internet de los 90

En 1990, la ARPANet dejó de existir y nació la Internet. En realidad, ARPA ya se había dividido en dos partes en los años 80: Milnet (para uso militar que se integró a la Red de Datos de la Defensa) y la NSFNet, que se ocupaba de las comunicaciones civiles. La NSF elevó nuevamente la velocidad del backbone a una T-3 (44.736Mbps). La NSFNet creció hasta lo que es hoy día la Internet comercial y en 1992 existían más de 1 millón de anfitrionas en Internet. En 1995, la NSFNet le entregó los servicios de backbone a proveedores de acceso a redes comerciales interconectadas (NAP) y se convirtió nuevamente en una red de investigaciones, estableciendo el Servicio de Backbone de Red de muy alta velocidad (vBNS) que conectaba a los cinco centros de supercomputadoras. La comercialización de Internet había comenzado.

El Gusano Merodea – y la Seguridad se Convierte en una Preocupación

Durante los primeros tiempos de la ARPANet, la seguridad era una preocupación importante para el contingente militar y al mismo tiempo, un asunto casi sin importancia para los científicos investigadores, quienes estaban más interesados en lo que la tecnología podía hacer que en asegurarla – de ahí la división de la red. El escaso número de nodos en la red limitaba el alcance de la amenaza impuesta por las rupturas de la seguridad. Sin embargo, en 1988, un *gusano* (un programa de auto-duplicación) apareció en Internet y atacó computadoras que tenían instalado el sistema operativo Berkeley UNIX, esparciéndose por todos los Estados Unidos, infectando a miles de computadoras y paralizando una gran porción de la Internet. Esta fue la llamada de alerta: de pronto los usuarios de Internet se percataron de que algo entre ellos albergaba malas intenciones. Habrían de seguir muchos más ataques de virus y hackeos.

Observando el Aumento de los Crímenes con la Comercialización de Internet

Por el año 1991, los usuarios de la mensajería electrónica habían comenzado a considerar la posibilidad de que sus comunicaciones a través de Internet fueran interceptadas. Philip Zimmermann sacó un programa de encriptación denominado *Pretty Good Privacy, PGP*, (*Bastante Buena Privacidad*), que podía emplearse para proteger mensajes sensibles. El

PGP también fue utilizado por criminales para ocultar la evidencia de sus crímenes a la policía.

El primer banco electrónico, denominado Primer Virtual, apareció en línea en 1994, creando una gran cantidad de nuevas oportunidades para los hackers. También en ese año, los investigadores comenzaron a trabajar en la “próxima generación” del Protocolo de Internet, llamado IPv6. El propósito primario de esta nueva versión era solucionar la escasez anterior de direcciones IP usando el espacio de direcciones de 32 bit del Protocolo de Internet vigente, IPv4, pero esta nueva versión tendría que afrontar otra preocupación: la seguridad del Protocolo de Internet.

En 1995, el Servicio Secreto de los Estados Unidos y la División Antidrogas (DEA) consiguieron intervenir la Internet para ayudar a construir un caso contra sospechosos acusados de producir y vender equipos ilegales de clonación de teléfonos celulares.

En 1996, el Congreso se tornó preocupado por la cantidad de pornografía intercambiada a través de Internet y aprobó la Ley de Decencia en las Comunicaciones (CDA), que más tarde se declaró inconstitucional. Mientras tanto, un cracker podía paralizar la Compañía de Redes de Acceso Público en Nueva York utilizando un ataque de hakeo que fue descrito en la revista *2600 Magazine*. Un “cancelbot” lanzado en la Usenet destruyó más de 25,000 mensajes de grupos de noticias, y en el mismo año, las computadoras del Departamento de Justicia de los Estados Unidos, la Agencia Central de Inteligencia y la Fuerza Aérea fueron hackeadas.

En los tres años siguientes, muchas más agencias gubernamentales y compañías prominentes tenían hackeados sus sistemas, incluyendo el Departamento de Comercio de los Estados Unidos, la UNICEF y el *New York Times*. Los sitios Web de eBay, Microsoft y del Senado de los Estados Unidos también fueron víctimas de los hackers. El virus Melissa causó que los servidores de mensajería electrónica de las compañías se paralizaran. Una página Web fraudulenta diseñada para aparentar ser la historia de una noticia financiera de la Bloomberg trajo como resultado el incremento del 31% de las acciones de una pequeña compañía tecnológica en respuesta a la falsa “noticia”.

Al arribar al año 2000, un enorme ataque DoS distribuido paralizó sitios Web bien importantes como Yahoo y Amazon. Apache, RSA Security y la Western Union fueron hackeadas, el gusano Código Rojo atacó a miles de servidores Web y el virus Sircam golpeó cuentas de correo electrónico en todo el mundo.

Sin embargo, los códigos maliciosos y los ataques de hackeo representan sólo una pequeña porción de toda la actividad criminal que de alguna forma usaba o dependía de la Internet. Desde el chanchullo sobre la infame “Carta de Nigeria” hasta el uso de la Net para preparar los ataques terroristas del 11 de septiembre de 2001, el crimen ha proliferado en la red – y lo continua haciendo.

Actualizando la Historia del Crimen Cibernético

El nuevo milenio trajo consigo la creciente popularidad de nuevas y excitantes tecnologías, tales como la interconexión inalámbrica y las opciones de conectividad de bajo costo, alta velocidad y “siempre en línea” mediante la *Digital Subscriber Line*, xDSL, (Línea de Suscripción Digital) y el módem de cable. Esas tecnologías se pueden conseguir en cada vez más lugares. Desafortunadamente, ellas también ofrecen nuevas oportunidades para los criminales cibernéticos por varias razones que exploraremos aquí.

Comprendiendo Cómo las Nuevas Tecnologías Crean Nuevas Vulnerabilidades

La mayoría de nosotros hoy estamos más conscientes de la importancia de la seguridad que hace una década atrás, seguridad con respecto a nuestras computadoras y también a nuestra vida en general. Ciertamente hoy existen más productos de seguridad en el mercado de los que existían hace unos años atrás. Los legisladores de todo el mundo han “tomado medidas enérgicas” contra actitudes tales como el acceso no autorizado, actitudes que en el pasado no estaban contempladas en las leyes penales.

Al parecer tenemos todos los elementos más importantes para reducir la incidencia del crimen cibernético: tenemos las leyes (“con dientes”), tenemos las herramientas, incluso tenemos la consciencia generalizada que a veces es el componente más difícil de un esfuerzo por prevenir el delito. ¿Entonces, por qué el crimen cibernético no sólo *no* ha desaparecido, sino que continua incrementándose?

Una razón importante para el incremento del crimen cibernético es el ritmo arrollador al que se están desarrollando nuevas tecnologías, que hacen nuestra experiencia en la computación más provechosa, más fácil, más rápida y más entretenida. Sin embargo, la comodidad y el rendimiento a menudo tienen un precio y ese precio es la seguridad.

Los criminales cibernéticos aman las nuevas tecnologías, incluyendo:

- Banda ancha
- Equipos inalámbricos
- Computación móvil y acceso remoto
- Tecnologías Web sofisticadas como Java, ActiveX, etc.
- Programas de mensajería electrónica de buena calidad que soportan HTML y scripting
- Comercio electrónico y banca en línea
- Mensajería instantánea
- Nuevos sistemas operativos

Los criminales cibernéticos también aman la estandarización. Si todos usan el mismo sistema operativo, el mismo visualizador Web, el mismo cliente de correo electrónico, o si todos los comerciantes se apegan a las mismas especificaciones, el atacante potencial tiene mucho menos que aprender y un mayor campo de juego.

Discutamos por qué estas nuevas tecnologías y la estandarización de las tecnologías de computación e interconexión son tan amadas por los criminales cibernéticos.

¿Por qué los Criminales Cibernéticos Aman la Banda Ancha?

Las tecnologías de banda ancha como xDSL, el módem de cable y los servicios de Internet por satélite le facilitaron la vida a los usuarios de Internet, pero también le facilitaron a los hackers la invasión a las computadoras y redes de esos usuarios. Debido a que las computadoras personales conectadas a redes de banda ancha como módem de cable o DSL se comportan más como computadoras conectadas a una red que como computadoras individuales que usan líneas telefónicas para conectarse a Internet, resulta más fácil explotar la tecnología para obtener el acceso no autorizado. Como consecuencia, los usuarios de banda ancha necesitan tener una mayor consciencia en cuanto a la seguridad que los usuarios que tienen acceso a Internet por marcación.

Estadísticas cibernéticas...

Uso de la Internet de Banda Ancha

De acuerdo a la *Cable Datacom News* de marzo de 2002, el número de suscriptores del servicio de banda ancha (módem de cable, DSL, satélite e inalámbrico fijo) en los Estados Unidos alcanzó la cifra de más de 6.4 millones en el año 2001. Esta cifra representa sólo el 10% de la penetración en el mercado de los Estados Unidos y el 22% en Canadá, pero los ingresos totales sobrepasan los 4.5 billones de dólares estadounidenses, y la mayoría de los expertos esperan que este mercado siga creciendo más cada año en el futuro inmediato.

El problema con la Conectividad 24/7

Una red es vulnerable a un ataque del exterior sólo cuando está conectada a una red exterior. Cuando la mayoría de los usuarios y compañías se conectaban a Internet con módems análogos o mediante conexiones por marcación ISDN, su vulnerabilidad al ataque era limitada, porque el sistema estaba disponible para los de afuera sólo durante una sesión. Cuando Usted terminaba de hacer lo que quería hacer en la Net, se desconectaba y su sistema “desaparecía” de Internet.

Además, la mayoría de los proveedores de servicios de Internet Comercial, ISP, usan un Protocolo Dinámico de Configuración de Máquinas (DHCP) para asignar direcciones IP a los usuarios que se conectan por marcación. Esto significa que su computadora conectada a Internet recibe una nueva dirección IP cada vez que se desconecta y se reconecta.

La DSL y el cable son referidas como tecnologías de “siempre en línea”. Usted no tiene que marcar cada vez que quiera entrar en Internet, sino que está conectado las 24 horas del día, los siete días de la semana. Esto hace que Usted pueda acceder a los recursos de Internet más rápida y fácilmente. También le facilita correr un servidor permitiéndole a otros usuarios autorizados a acceder desde una estación remota a los ficheros compartidos en su sistema. Debido a que su dirección IP generalmente es la misma mientras no se desconecta, estos clientes autorizados pueden encontrar su servidor más fácilmente de una

sesión de comunicación a la próxima. Por supuesto, si apaga las computadoras, se pierde la conexión (y se “cierra la puerta” a los hackers potenciales). Sin embargo, las computadoras actuales están concebidas para trabajar continuamente (y excepto por algunos periféricos tales como los monitores, generalmente trabajan mejor y duran más tiempo si lo hacen), así que muchos usuarios con habilidades técnicas nunca apagan sus sistemas.

El problema con las tecnologías 24/7 es que estas también facilitan el acceso a su sistema a gente no autorizada. Su exposición es mucho mayor porque Usted está “siempre abierto a los negocios”, dándole al hacker más tiempo de organizar un ataque de fuerza bruta para adivinar su contraseña o averiguar qué puertos TCP/UDP podrían estar abiertos y vulnerables. Además, como su dirección IP sigue siendo la misma, resulta más fácil para estos hackers regresar a su sistema la próxima vez que deseen hacer un poco de allanamiento virtual.

El Problema con la Conectividad a Alta Velocidad

Otra ventaja de la banda ancha es el incremento de la velocidad de conectividad. A diferencia de un módem análogo que está limitado a 56Kpbs (y prácticamente hablando, menos que eso debido a regulaciones federales y consideraciones sobre la línea), las compañías que brindan servicios de banda ancha y cable ofrecen descargas a alta velocidad, así como velocidades de carga a menudo más altas. Esto significa un mejor rendimiento para Usted – pero si su servicio ofrece una alta velocidad de carga, también significa que un intruso podrá arrebatarle sus ficheros con mayor rapidez.

Por suerte, en términos de seguridad por no decir en términos de posibilidades de uso, la mayoría de los servicios de banda ancha son asimétricos. Esto significa que las velocidades de carga y descarga no están creadas equitativamente. Como es típico en el caso de las cuentas de los consumidores, el índice de transferencia de carga está limitado a 128Kbps por las compañías de cables y de 128Kbps a 764Kbps por los proveedores de servicios de banda ancha.

Nota

La mayoría de los proveedores de servicios de Internet comercial limitan (o estrangulan) las velocidades de carga con el fin de desalentar a los usuarios de casa para que no usen servidores (lo que constituye una violación de muchos términos contractuales de servicio de DSL y cable).

Sin embargo, aún con estas limitaciones, generalmente la velocidad de carga es por lo menos dos veces mayor que la de un módem análogo – una ayuda para los hackers que descargan datos de Su computadora hacia la de ellos.

El problema con la Conectividad a Alta Velocidad y de Bajo Costo 24/7

Los problemas relacionados con la conectividad a alta velocidad 24/7 y los índices de datos transferidos a alta velocidad asociados con las tecnologías de banda ancha para consumidores también existen con las soluciones tradicionales a alta velocidad 24/7 para

empresas, tales como la T-1. Sin embargo, debido a que la mayoría de las líneas T-1 están conectadas a compañías que emplean profesionales de la informática, es más probable que las medidas de seguridad sean capaces de disminuir el riesgo en cuanto a seguridad.

El problema con el cable y la banda ancha es que esas tecnologías han llevado el acceso a alta velocidad y siempre en línea a usuarios de casa y pequeñas oficinas que no pueden darse el lujo de costearse una T-1. Estos usuarios menos sofisticados serán también menos propensos a estar conscientes del riesgo en cuanto a seguridad o a tener la pericia técnica o el presupuesto para implementar el nivel de seguridad apropiado.

La mayoría de las oficinas pequeñas y un creciente número de usuarios de casa corren el software *Network Address Translation*, NAT, que es un tipo de programa para compartir el acceso a Internet con varias PC en una LAN pequeña. Esto proporciona una pequeña medida de seguridad para los sistemas de la red local, porque el NAT le asigna direcciones IP privadas a las computadoras de sus clientes. Estas direcciones no son visibles en Internet. Sin embargo, la computadora anfitriona del NAT que está conectada directamente a Internet sí está expuesta.

Cómo proteger su Conexión de Banda Ancha

Si Usted tiene una computadora que utiliza una conexión a Internet de banda ancha y la computadora *no* está conectada a una LAN y no está funcionando como un servidor de Internet, un paso que puede dar es asegurarse de que la opción de compartir ficheros e impresoras no esté habilitada en esa computadora.

Otra laguna de seguridad común en los sistemas de Windows se denomina *vulnerabilidad IRDP*. Es causada por el ICMP Router Discovery Protocol (IRDP), habilitado por defecto en máquinas de Windows que están configuradas como clientes DHCP. El IRDP no es necesario cuando el servidor DHCP especifica la información del enrutador, pero los hackers lo pueden usar para añadir entradas de rutas implícitas que invalidarán la ruta implícita que da el servidor DHCP. Usted puede deshabilitar el IRDP editando el Registro de Windows.

Algunos usuarios de cable han encontrado que cuando la NIC utilizada para conectarse al módem de cable era instalada por la compañía que brinda este servicio (o por el usuario), Windows automáticamente vincula la tarjeta al TCP/IP y al servicio de Interconexión de Microsoft. Tener vinculada esta interfaz a la Interconexión de Microsoft abre sus sistemas a otros en el segmento de cable.

Nota

El Capítulo 8 “Implementando la Seguridad del Sistema” proporciona detalles sobre cómo deshabilitar la opción de compartir ficheros e impresoras en computadoras de Windows, UNIX/Linux y Macintosh, cómo editar el Registro para protegerse de la vulnerabilidad IRPD y cómo chequear y cambiar los vínculos de la NIC.

¿Cuál es más seguro: el DSL o el cable? El cable es una conexión compartida (o sea, todos en su barrio son parte del mismo segmento de red). En esencia, esto crea una red de área local, lo que significa que sus vecinos tienen acceso a Su sistema, tanto como las computadoras vecinas de cualquier LAN tienen acceso entre ellas.

Al igual que en una LAN regular, existen formas de protegerse de sus vecinos de red. El estándar DOCSIS (Especificación de Interfase de Datos Sobre Servicio de Cable) para módems de cable proporciona alguna medida de seguridad porque los módems que cumplen con esta especificación soportan encriptación de datos entre el concentrador del proveedor y la computadora del usuario. Los datos *no* se codifican entre el proveedor y el destino final (o sea, al navegar en Internet), pero este estándar sí ayuda a solucionar el problema del “compartimiento del segmento en el vecindario), pues otros en su segmento de cable no podrán leer sus datos si los interceptan. Las redes de cable que usan los estándares DOCSIS también evitan que su computadora anuncie sus recursos compartidos a la red usando protocolos NetBIOS (los que ocasionan que otras computadoras en la red aparezcan en la ventana de Entorno de Red o Sitios de Red en computadoras que estén corriendo Windows). Pero esté consciente de que un hacker podría aún conectarse a su computadora si él o ella conociera el nombre de su computadora y la dirección IP.

Los usuarios de DSL están conectados directamente a través de sus líneas telefónicas a la oficina central de la Compañía Telefónica (CO). Por lo tanto, el DSL proporciona muchas menos vulnerabilidades a los hackers, pero esto no significa que una conexión por DSL sea segura.

Nadie debe usar una conexión a Internet de banda ancha sin utilizar además un muro de fuego para protegerse de los intrusos externos. Los muros de fuego pueden filtrar los datos entrantes y los salientes y bloquear los puertos abiertos para impedirle a los hackers su entrada por los puntos usuales. Un muro de fuego puede ser un dispositivo de hardware o un programa de software que corra en la computadora conectada a Internet. El más reciente sistema operativo de escritorio, Windows XP, incluye, incluso, un software de muro de fuego.

Analizaremos cómo funcionan los muros de fuego y los varios tipos que existen en el Capítulo 7 “Comprendiendo la Prevención del Crimen Cibernético”.

¿Por qué los Criminales del Ciberespacio Aman los Inalámbricos?

Las tecnologías inalámbricas están emergiendo como la Próxima Gran Cosa en la interconexión de computadoras para el siglo XXI. Las especificaciones 802.11b del IEEE proporcionan estándares para la interconexión inalámbrica a 11Mbps utilizando transmisión de radio de amplio espectro. Una especificación más reciente, la 802.11g, permite duplicar la velocidad de las comunicaciones inalámbricas a 22Mbps. Esta especificación le da a las computadoras móviles la capacidad de llegar adonde ningún cable de Ethernet ha llegado antes – y seguir estando conectadas a la red local y/o a Internet.

El último sistema operativo de Microsoft, Windows XP, incluye soporte para la interconexión inalámbrica 802.11b. El montaje de una red inalámbrica es sencillo usando la interfase XP, como se muestra en la figura 2.1.

Figura 2.1 Usted puede montar una red inalámbrica rápida y fácilmente con Windows XP.



Bluetooth (diente azul) es una tecnología inalámbrica diseñada para habilitar una amplia variedad de dispositivos portátiles, tales como asistentes digitales personales (PDA) y teléfonos móviles, así como las más tradicionales computadoras laptop y de tipo cuaderno para conectarse a Internet.

Desafortunadamente, la posibilidad de acceder a una red sin una conexión física le facilita mucho más a los hackers el hacer lo mismo, porque no tienen que preocuparse por “conectarse” al cable. Si una red incluye un punto de acceso inalámbrico, es vulnerable a los intrusos externos, aún si no existe un servidor de acceso remoto o una conexión a Internet en la red.

El Problema con las Tecnologías Inalámbricas

¿Cuán seguras son hoy las tecnologías inalámbricas? Es importante comprender que la mayoría están basadas en transmisiones de radio que salen a través de las ondas de aire. Por ejemplo, los dispositivos Bluetooth transmiten en el espectro de 2.4GHz. Este es un rango no licenciado, así que cualquiera puede transmitir y recibir en él.

Las transmisiones a través de las ondas de aire pueden ser interceptadas y las antenas de 2.4GHz, los amplificadores y los transmisor-receptores se encuentran fácilmente en el mercado. Las señales se pueden captar a cientos de pies del punto de acceso. Las antenas

de alto alcance incrementan esta distancia. Todo esto es comida para el criminal cibernético.

Pero no es tan malo como suena. La especificación 802.11 del IEEE soporta dos tipos de transmisión de radio de amplio espectro:

- Frecuencia de Salto de Amplio Espectro (FHSS)
- Secuencia Directa de Amplio Espectro (DSSS)

El primer tipo, la FHSS, utiliza *frecuencia de salto*, que significa que la señal “salta” o cambia de una frecuencia a otra. (Para la Bluetooth, los saltos abarcan 79 frecuencias a intervalos de 1MHz y pueden llegar a hacer hasta 1600 saltos por segundo). Esto significa que un hacker no puede sintonizar una frecuencia y escuchar, tal y como Usted puede hacer con emisiones de radio de banda corta que usan una frecuencia fija. Sin embargo, esta provisión da solo una pequeña medida de seguridad.

La DSSS utiliza un patrón redundante de bit para cada bit de datos transmitidos (denominado código chipping). El objetivo es hacer a la señal más resistente a las interferencias y proporcionarle alguna tolerancia a las fallas. Si alguno de los bits se dañan durante la transmisión, la redundancia permite recuperar los datos originales.

Estadísticas cibernéticas...

¿Un Mundo sin Cables?

Las proyecciones del Banco de América anticipan que existirán 400 millones de usuarios inalámbricos en el 2003, de acuerdo con el escrito de Eric W. Pfeiffer en Forbes.com. La Corporación Internacional de Datos (IDC) reporta que más de 15 millones de suscriptores ya tienen acceso inalámbrico a Internet mediante PDA y teléfonos inteligentes.

Los estándares inalámbricos 802.11 sí proporcionan medidas de seguridad, tales como la autenticación y la encriptación. Desafortunadamente, la encriptación usada por estas tecnologías es débil y se puede violar de una manera relativamente fácil. Los pequeños dispositivos de mano como los teléfonos móviles tienen memoria y poder de procesamiento limitados. Esto significa que no se pueden emplear largos algoritmos de encriptación que requieren procesamientos densos.

Un programa denominado AirSnort, que corre en Linux, explota las debilidades de la encriptación inalámbrica para descubrir la clave de la encriptación WEP sencillamente con un monitoreo pasivo de la red inalámbrica. El hecho de que la WEP use claves estáticas (en lugar de claves dinámicas más seguras que cambien a intervalos regulares) convierte a esta tecnología en especialmente peligrosa.

Nota

Los estándares 802.11b del IEEE que regulan la tecnología inalámbrica definen el término WEP como Privacidad Inalámbrica Equivalente. Este protocolo también es referido como el Protocolo de Encriptación WEP (con las mismas siglas) o en literaturas más técnicas, sencillamente, como el Protocolo de Encriptación Inalámbrica (Usted lo adivinó – WEP).

En la escena...

Experiencias de la Vida Real

En el año 2001, la red de Sun Microsystem fue hackeada por dos intrusos quienes se encontraban en el estacionamiento de la compañía usando tarjetas de interconexión inalámbrica estándares.

En el 2002, una firma de seguridad llamada i-sec demostró cómo los hackers podían usar una papa frita Pringles para hacer una antena direccional capaz de localizar redes inalámbricas en el distrito financiero de Londres. También se pueden usar tazas de café o contenedores de metal similares. Estas antenas hechas en casa pueden incrementar la señal hasta 15 decibeles.

Aparte de la debilidad de los algoritmos de encriptación, la encriptación inalámbrica cubre sólo la transmisión entre la computadora de un usuario y la puerta de enlace inalámbrica que conecta la red inalámbrica a Internet. Cuando los datos alcanzan la puerta de enlace del Protocolo de Aplicación Inalámbrica (WAP), deben ser transferidos de la red inalámbrica a la red alamburada. Para hacer esto, la comunicación inalámbrica, la cual es en forma de WML (lenguaje de aumento o ganancia (**markup**) de texto basado en el lenguaje de aumento extensible), debe ser decodificada y re-codificada para ser transmitida en la red alamburada. Los datos son vulnerables durante esta “brecha de encriptación”.

Otro problema es que aunque los datos son codificados, la información sobre la dirección fuente y de destino no es codificada. Finalmente, la encriptación no está necesariamente habilitada por defecto cuando los componentes de interconexión inalámbrica están instalados. De acuerdo con la emisión de BBC News del 8 de marzo de 2002, un sondeo informal realizado por i-sec descubrió que el 67% de las redes en el sondeo tenían deshabilitada la encriptación.

De acuerdo con un artículo, *Explotando y Protegiendo las Redes Inalámbricas 802.11b*, publicado en el sitio Web de ExtremeTech en abril del año 2002, fueron realizadas pruebas de seguridad usando una antena Yagi sobre el techo del edificio de oficinas de Ziff Davis en Manhattan. Los que realizaron las pruebas pudieron encontrar más de 60 puntos de acceso inalámbricos y el 79% de ellos, asombrosamente, no tenía habilitada la encriptación. Vulnerabilidades similares fueron encontradas en la ciudad de Jersey y en Silicon Valley (Valle del Silicio).

La práctica de conducir de un lado a otro con una computadora portátil equipada con una NIC inalámbrica buscando señales de redes inalámbricas se denomina *guerra móvil* (un término acuñado por el experto en seguridad Meter Shipley) o *hackeo al paso*.

Cómo proteger su Conexión Inalámbrica

Organizaciones e individuos que utilizan tecnologías inalámbricas no quieren perder la comodidad, pero están reconociendo que resulta necesario tomar precauciones extras. Un

modo de hacer más seguras las redes inalámbricas es el uso de dispositivos de seguridad basados en hardware como las tarjetas inteligentes. Los usuarios no pueden acceder a los recursos sin pasar la tarjeta en cuestión por un lector de tarjetas.

Nota

Analizaremos más detalladamente la autenticación mediante la tarjeta inteligente y el control de acceso en el Capítulo 7 “Comprendiendo la Prevención del Crimen Cibernético”.

Otras medidas de seguridad inalámbricas que pueden implementar los fabricantes de dispositivos inalámbricos o los administradores de LAN inalámbricas (WLAN) incluyen:

- Alejar los concentradores inalámbricos de las ventanas y moverlos hacia el centro de los edificios
- Asegurarse de que la encriptación inalámbrica esté habilitada
- Deshabilitar los broadcasts en los concentradores de la red
- Cambiar las configuraciones implícitas como el Identificador de Servicio (SSID) y la contraseña implícita en el punto de acceso inalámbrico o enrutador
- Limitar el número de puntos de acceso inalámbrico también puede hacer que la WLAN sea menos vulnerable a accesos no autorizados
- Asignar direcciones IP estáticas a las NIC inalámbricas y deshabilitar el DHCP en el enrutador inalámbrico
- Auditorias de seguridad, en forma de un sistema de rastreo de direcciones MAC (control de acceso a los medios) que se puede usar para rastrear los dispositivos que acceden a la red inalámbrica
- Instalar un muro de fuego entre la WLAN y la LAN alambrada
- Poner los puntos de acceso inalámbrico en la zona conocida como *zona desmilitarizada (DMZ)*; también es referida como *red de perímetro* o *subnet oculta*, y configurar a los usuarios inalámbricos para que utilicen una red virtual privada (VPN) creando así un túnel seguro en la red
- Tratar a la red inalámbrica como si fuese una red pública y no enviar datos sensibles a través de ella sin tomar precauciones (como emplear otro método de encriptación además del WEP).

¿Por qué los Criminales Cibernéticos Aman la Computación Móvil?

En la década pasada, el alto precio de las computadoras portátiles – laptop, tipo cuaderno y de mano – fue disminuyendo mientras que el poder de procesamiento se fue igualando al de las máquinas de mesa. Esta tendencia ha sido buena para los empresarios que viajan, pues ahora pueden continuar trabajando mientras están en la carretera con poca pérdida en la productividad.

A menudo terminar el trabajo requiere de un acceso a la red corporativa y, por lo tanto, la mayoría de las laptop actuales traen incluidos módems y puertos Ethernet. Los viajeros pueden discar directamente al servidor de acceso remoto de la LAN de la compañía o llamar a un ISP local y hacer un túnel hasta la red de la compañía a través de Internet. Un

mayor número de hoteles está brindando ahora servicios de conexión a Internet a alta velocidad, a la que Usted puede conectarse mediante el puerto Ethernet de su computadora portátil o mediante la NIC PCMCIA (tarjeta de la PC).

Una vez que esté conectado a la LAN de la compañía mediante uno de estos métodos de acceso remoto, su computadora se convierte en otro nodo (temporal) en esa red local, y la tecnología de acceso remoto le permite realizar cualquier tarea que podía hacer desde una estación de trabajo alámbrica in situ. Esto es muy bueno para los empleados que tienen que estar lejos de la oficina, pero también es bueno para los hackers que buscan entrar sin ser invitados.

El Problema de la Computación Móvil

Recuerde que cada punto de acceso en la red crea otra vulnerabilidad más. Un servidor de acceso remoto proporciona un punto de acceso como lo hace un servidor VPN.

Por supuesto, la computación móvil también proporciona una consideración adicional con respecto a la seguridad: la posibilidad de que se roben la computadora entera. Usted podría pensar que este no es un problema de seguridad si no almacena información sensible en el disco duro de la computadora portátil, pero, ¿qué me dice de la configuración del software de acceso remoto o de la VPN que le permitiría a cualquiera en posesión de la computadora conectarse a la red de la compañía? Aunque para conectarse a la red se requiere una contraseña, muchos usuarios configuran sus sistemas para que “recuerden” sus contraseñas, de modo que no tengan que perder tiempo tecleándola cada vez que se conectan; por consiguiente, yendo en contra del propósito de seguridad de la contraseña en caso de que otra persona tome posesión de la computadora.

Estadísticas cibernéticas...

El Número de Trabajadores a Distancia Continúa Aumentando

De acuerdo con ebizChronicle.com, en el 2001 el número de empleados a distancia – que trabajan lejos de su oficina y se conectan a la red de la compañía a través de acceso remoto – creció a 32 millones sólo en los Estados Unidos. Las proyecciones estiman que para el 2004, casi 40 millones de trabajadores laborarán a distancia.

La computación móvil presenta algunas preocupaciones especiales en torno a la seguridad. La autenticación del usuario es una de las mayores. A diferencia del entorno corporativo, donde existen guardias de seguridad, cámaras de vigilancia y empleados listos que reconocen la presencia física de extraños sospechosos alrededor de los sistemas de computación, un usuario que se conecta a la red desde una estación remota no ofrece ninguna certeza de que él o ella sea la persona cuyas credenciales están siendo usadas.

Ah, y existe una razón más por la que los criminales cibernéticos aman las actuales computadoras móviles, potentes y de bajo costo: Ahora *pueden llevarlas* con ellos. Las computadoras compactas y ligeras son más fáciles de transportar hacia un lugar “seguro” como, por ejemplo, una cabina telefónica, desde donde el hacker puede iniciar una sesión

en línea difícil de rastrear o de llevar en una expedición de “hackeo al paso” para encontrar LAN inalámbricas a las cuales puedan conectarse a escondidas.

Cómo Proteger sus Computadoras Móviles y sus Conexiones de Acceso Remoto

La primera línea de defensa en la seguridad móvil es la seguridad física de la computadora portátil. Existen en el mercado muchos dispositivos de bloqueo para laptop. Los usuarios móviles deben ser instruidos para vigilar bien de cerca sus computadoras, especialmente en aeropuertos y otros lugares de mucho acceso público. Usted puede comprar dispositivos de hardware que emiten una señal de “localización” y programas de software que se pueden configurar para discar automáticamente o contactar el “lugar de residencia” a través de Internet la primera vez que la computadora entre en línea después de que alguien utilice una contraseña incorrecta.

Existen varios medios de solucionar el problema de la autenticación del usuario móvil. Por ejemplo, los servidores de acceso remoto basados en Windows ofrecen la posibilidad de configurar las cuentas de usuarios de modo que se requiera la *seguridad de regreso de llamada*. Esto significa que un número telefónico específico está asociado con esa cuenta de usuario. Cuando el usuario llama a la red e introduce su nombre de usuario y contraseña, el servidor no le da acceso inmediato. En su lugar, se desconecta y llama de regreso al usuario al número telefónico especificado y sólo entonces autoriza el acceso a los recursos de la red.

Esto significa que alguien que haya robado la laptop de un usuario con contraseñas “memorizadas” (o quien de alguna forma haya descubierto la contraseña del usuario y esté discando desde otro número) no podrá acceder a la red a menos que el hacker esté llamando desde la casa del usuario o de otro número previamente especificado. Este sistema funciona bien para los trabajadores a distancia quienes, generalmente, llaman a la red desde sus casas. Resulta menos útil para los empleados que viajan, los cuales podrían llamar de un hotel diferente cada día. Existen sistemas similares que, en vez de colgar y llamar de regreso al usuario, identifican el número a través del identificador de llamadas y lo verifican contra una lista de números de usuarios remotos aprobados. Si el número está en la lista, el usuario puede acceder a la red. Esto funcionaría mejor que la llamada de regreso en el caso de los usuarios que llaman desde diferentes lugares fijos.

Los servidores de acceso remoto de Windows le permiten establecer políticas de acceso remoto que controlen si los intentos de conexión remota están autorizados. Otro método de autenticación de los usuarios remotos es el servidor RADIUS (Servicio de Llamadas Para Usuarios con Acceso Remoto). RADIUS es un protocolo de seguridad que soporta múltiples métodos de autenticación y permite transmisiones encriptadas entre el cliente y el servidor. RADIUS le permite a los administradores establecer limitaciones y restricciones en las tareas que un usuario remoto puede realizar una vez que se haya conectado a la red, basado en las configuraciones para esa cuenta de usuario. RADIUS se puede usar para administrar de forma centralizada múltiples servidores de acceso remoto o servidores VPN usando las mismas políticas.

Nota

Las compañías también deberían haber establecido políticas que especifiquen las normas que regulan el acceso remoto a la red. Estas normas se le deben distribuir a todos los empleados cuyas cuentas autorizan conexión remota. Existe una simple política de acceso por marcación en el sitio Web del Instituto SANS:

www.sans.org/newlook/resources/policies/Dial-in_Accesss_Policy.pdf. El documento está en formato PDF, usted necesitará Adobe Acrobat o Acrobat Reader para abrirlo (el segundo se puede descargar gratuitamente del sitio Web www.adobe.com).

Otras medidas que pueden mejorar la seguridad de las conexiones por acceso remoto incluyen:

- El uso del acceso a una aplicación dedicada de modo que el usuario remoto se conecte a una aplicación específica en el servidor de la red usando protocolos de propietario. Esto significa que el usuario conectado no tendrá acceso a otros recursos de la red. Este sistema funciona bien en casos en los que los usuarios remotos necesitan realizar sólo una tarea específica como, por ejemplo, chequear el correo electrónico.
- El uso de la autenticación de dos factores. En este sistema, se requieren dos componentes separados para acceder satisfactoriamente a la red: el primero es *algo que Usted conoce* y el segundo es *algo que Usted tiene o algo que Usted es*. Además de proporcionar una contraseña (algo que Usted conoce), también tendrá que proporcionar un detalle de hardware, tarjeta inteligente o un identificador biométrico como una huella digital (algo que Usted tiene).
- Utilización de la seguridad de regreso de llamada para trabajadores a distancia y otros usuarios de acceso remoto que se conectan siempre desde el mismo número.
- El uso de la encriptación para comunicaciones sensibles a través de las líneas telefónicas públicas o Internet.
- El uso de políticas de acceso remoto para restringir lo que pueden hacer en la red los usuarios por marcación así como el día y la hora en que ellos pueden conectarse y otros parámetros.

El acceso remoto abre las redes corporativas a empleados, socios y clientes – y a intrusos no deseados. Es importante tomar precauciones de seguridad extras en cada punto al que puedan acceder desde afuera.

¿Por qué los Criminales Cibernéticos Aman las Tecnologías Sofisticadas de Mensajería Electrónica e Internet?

La WWW global actual es un “sitio” diferente al de hace 10 años atrás. A principio de los años 90, la mayoría de las páginas Web consistían en texto plano y gráficos. Las limitaciones de HTML y la lenta amplitud de banda de la mayoría de las conexiones a Internet obligaron a los diseñadores Web a seguir la advertencia de “déjala simple, estúpido”.

Hoy día ha cambiado totalmente el panorama. Los sitios Web destellan y danzan. Presentaciones y una interacción cada vez más sofisticadas son posibles gracias a tecnologías como Java y Visual Basic scripting y controles ActiveX. Nuevos lenguajes de aumento o ganancia (**markup**) como el HTML Dinámico (DHTML) y el XML brindan oportunidades a los diseñadores de sitios Web para traspasar los límites. El predominio de conexiones de alta velocidad hacen factibles las aplicaciones Web de amplio ancho de banda.

Pero una vez más, el realce de las características de un hombre o una mujer es una laguna de seguridad de otro. Los *Scripts* (guiones) son programas que corren cuando Usted accede a sitios Web en los que ellos están incrustados. Lo que haga el programa depende del programador. La mayoría de los guiones Web persiguen un propósito útil e inofensivo; por ejemplo, un guión Java puede producir efectos visuales como nieve cayendo o un texto animado. Las applets y los guiones pueden crear también herramientas calculadoras, interfaces de chateo, juegos o relojes.

Sin embargo, programadores maliciosos pueden usar estas tecnologías para sus propios propósitos nefastos. Aunque existen muchos tipos de anexos, componentes de página Web y otros aspectos de las tecnologías Web y de mensajería electrónica que pueden presentar riesgos de seguridad, los más preocupantes son aquellos que realmente pueden correr códigos y hacer cosas en Su o (a) Su computadora. En la mayoría de los casos, este tipo de material – a veces conocido como *contenido activo* porque puede correr por sí mismo en Su máquina, es benigno y está diseñado con el fin de realizar tareas específicas para administrar o actualizar una página en pantalla, correr una animación, realizar un cálculo, etc. Pero el contenido activo también puede incluir códigos maliciosos que pueden hacerle a su PC todo tipo de cosas malas si lo autoriza a correr sin verificarlo previamente. Es por eso que la mayoría de los expertos en seguridad recomiendan que los usuarios (y administradores de redes) examinen el contenido activo. Hasta ahora, la política de seguridad más segura es negarse a aceptar el contenido activo. Sin embargo, esta alternativa también podría impedirle la utilización de características que Usted necesite que dependan del contenido activo. Otras estrategias incluyen el requerirle al contenido activo mostrar credenciales válidas antes de ser autorizado a correr o aceptar el contenido activo sólo de sitios de Internet o direcciones especificadas (que se sabe son seguras). Si fue escrito por un programador malicioso, el contenido activo puede introducir virus, gusanos, puertas traseras y toda clase de otros códigos cuestionables y puntos de acceso a sus sistemas y redes.

Este mismo problema (además de otros) que aplica a los visualizadores Web, también aplica a los actuales programas sofisticados de clientes de mensajería electrónica que permiten mostrar en pantalla los correos HTML, correr los guiones incrustados en los mensajes de correo y enviar anexos. Aquí nuevamente, el contenido activo –que hace presentaciones sofisticadas y trabajo de interacción – abre las puertas a potenciales violaciones de la seguridad.

El Problema con los Guiones Web y los Controles

Los guiones y controles se pueden usar para realizar tareas en su computadora sin su conocimiento – incluyendo el monitoreo de sus comunicaciones con otros o la cancelación de ficheros claves en su disco duro. Java y Active X le dan a los programadores una forma de correr el programa que gusten en su computadora. El código malicioso puede simular una solicitud de registro de entrada y enviarle al hacker las credenciales de la contraseña que Usted introdujo, todo sin su conocimiento.

Existen muchas formas en las que su visualizador Web puede exponerse a códigos maliciosos. Seguir vínculos de otros sitios Web o hacer clic sobre vínculos en mensajes de correo electrónico o correos de grupos de noticias pueden conducirlo hacia una página que corra un guión malicioso.

Cómo proteger su Visualizador Web de Códigos Maliciosos

Por estas mismas preocupaciones en cuanto a la seguridad, se ha creado un número de mecanismos para proteger a los usuarios desprevenidos de la Web de contenidos potencialmente peligrosos. Los códigos se pueden firmar digitalmente para verificar que procedan de un vendedor legítimo y por lo tanto sea seguro descargarlos. La mayoría de los visualizadores Web modernos le permiten seleccionar el nivel de seguridad deseado. Usted puede deshabilitar Java y/o ActiveX o puede configurar el visualizador para que le avise cuando encuentre un guión de modo que Usted pueda decidir si lo corre basándose en su confianza en el sitio (o en la carencia de ella).

Por ejemplo, el visualizador Web Internet Explorer de Microsoft le permite seleccionar un nivel de seguridad predefinido (Bajo, Medio Bajo, Medio o Alto), como se muestra en la figura 2.2. El nivel seleccionado determina si los controles ActiveX no firmados serán descargados y si Usted será notificado antes de descargar cualquier contenido que se considere potencialmente inseguro.

Si ninguno de los niveles de seguridad preestablecidos funcionan para Usted, también puede crear sus propias configuraciones de seguridad personalizadas, como se muestra en la figura 2.3.

Figura 2.2 Los visualizadores modernos le permiten establecer los niveles de seguridad.

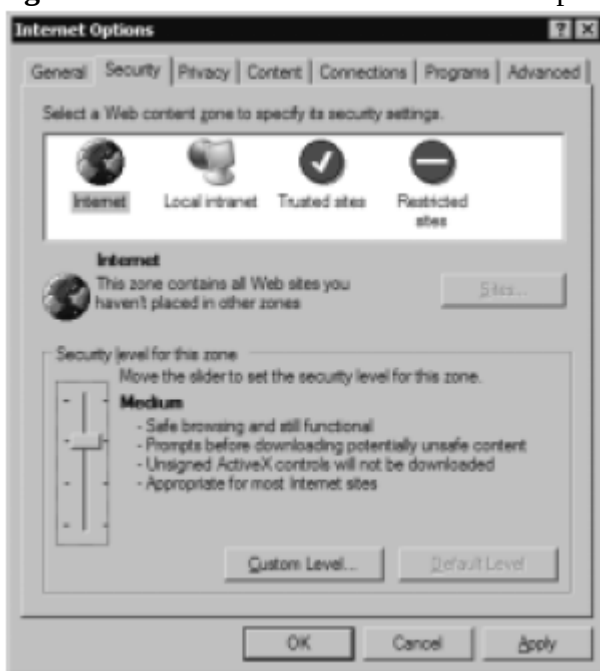


Figura 2.3 Usted puede crear configuraciones de seguridad personalizadas en lugar de usar niveles predefinidos.



Debido a que la Web es una de las aplicaciones de Internet más utilizadas, es importante asegurarse de que no esté exponiendo su sistema y su red a ataques de hackeo a través del código que corre su visualizador.

El problema con los Queridos Clientes de la Mensajería Electrónica

Los mismos riesgos inherentes a los visualizadores Web que corren guiones y controles afloran nuevamente cuando Usted usa un cliente de mensajería electrónica que le permite recibir mensajes con formato HTML, los cuales pueden tener las mismas clases de códigos maliciosos incrustados.

En los primeros días de la mensajería electrónica, los programas eran simples y los mensajes eran básicamente de sólo texto. Este sistema ofrecía muchas menos oportunidades para las violaciones de seguridad, pero también limitaba la eficacia de las comunicaciones por correo electrónico. Cuando se hizo posible enviar ficheros como anexos a los mensajes, las puertas se abrieron a un nuevo riesgo. Inicialmente, los anexos eran por lo general fotos (.jpg, .gif, etc) o ficheros de texto que eran demasiado grandes para ser incluidos en el propio mensaje. El problema se agrava cuando un anexo es o contiene un programa ejecutable. Ficheros con extensiones .exe, .com o .bat son ejemplos obvios, pero existen muchos otros ficheros que pueden correr códigos, infectar su sistema con virus o hacerle mucho daño. Estos incluyen ficheros salva-pantalla (.scr) y ficheros de enlace (.lnk). Los ficheros del Registro (.reg) pueden editar el Registro de Windows y los ficheros .url pueden abrir páginas Web que corren códigos maliciosos. Ficheros de documento (como los ficheros .doc de Word) pueden incluir macros que son, sencillamente, programas pequeños. Los escritores de virus le han sacado provecho al potente soporte de Visual Basic para Aplicaciones (VBA) en aplicaciones Office de Microsoft para crear virus macros que pueden infectar sus sistema si Usted abre el documento que contiene el macro.

En la escena...

Experiencias de la Vida Real

En 1999, un virus macro de Word denominado Melissa comenzó a propagarse a través de la Internet y causó problemas de rendimiento y denegación de servicio debido a una sobrecarga en servidores de correo de todo el mundo. De acuerdo con el Centro de Coordinación del CERT (Equipo de Respuesta a Emergencias de Computación) de la Universidad de Carnegie-Mellon, Melissa afectó al menos 100,000 computadoras en la primera semana tras su aparición.

El Melissa original era relativamente benigno (apagaba servidores debido a la sobrecarga, pero no dañaba nada en las computadoras de los usuarios). Poco tiempo después de que los principales fabricantes de virus (como Symantec y McAfee) actualizaran sus ficheros de definición para proteger a los usuarios de sus productos del virus Melissa, los escritores de virus comenzaron a hacerle modificaciones al código original. Algunas de estas modificaciones eran más destructivas llevando cargas explosivas que destruían ficheros o enviaban de vuelta al escritor del virus informaciones personales.

Un programador de Nueva Jersey nombrado David Smith fue arrestado por fiscales federales y declarado culpable por haber creado el virus. Los estimados del daño causado por Melissa sólo en América del Norte oscilan entre los 80 millones y los 385 millones de dólares. Mucha de la evidencia que vincula a Smith con Melissa fue recopilada por

ICSA.net, que dirige a un equipo de expertos en seguridad encubiertos denominado IS Recon. Este grupo recopila información acerca de los hackers clandestinos y las amenazas potenciales a la seguridad de computadoras y redes.

Cómo Proteger su Correo Electrónico

Para evitar los problemas asociados con los modernos programas de mensajería electrónica, Usted debería configurar su cliente de correo electrónico para que no haga una “vista previa” (la que visualiza mensajes, incluyendo mensajes HTML sin que haga clic sobre ellos para abrirlos); también debería instalar un paquete antivirus que verifique la presencia de virus en los correos entrantes y salientes y tener cuidado de no abrir anexos a correos electrónicos con extensiones sospechosas a menos que esté absolutamente seguro de su origen.

En el caso de la mayoría de los virus distribuidos en correos electrónicos, una vez que un virus ha infectado una máquina, se enviará automáticamente a todos los miembros de la libreta de direcciones de la víctima, aparentando ser un mensaje procedente de la víctima. Esto significa que Usted no puede asumir que un anexo es seguro sólo porque reconozca el nombre en la casilla “De” del mensaje.

Debido a estos problemas, los programas de correo electrónico están diseñados con más seguridad – a veces tanta que la funcionalidad del cliente se ve severamente limitada. Por ejemplo, Microsoft Outlook 2002, por defecto, no le permitirá abrir anexos con ficheros ejecutables, aún si está absolutamente seguro de la validez y seguridad del fichero. Esta restricción podría ser buena para el usuario “promedio”, pero no para personas como creadores de softwares que necesitan enviar programas de aquí para allá regularmente. Afortunadamente, Usted puede obtener un software complementario que le permitirá cambiar este comportamiento sobre-protector si constituye un problema para Usted.

En muchos casos, la configuración correcta de la aplicación puede librarlo de muchos problemas. Por ejemplo, Microsoft Word ahora le permite configurar la seguridad de modo que el sistema le avisa antes de correr ningún macro. Si Usted abre un documento que no debería tener macros y aparece en pantalla el mensaje preguntándole si deshabilita los macros, seleccione hacerlo y puede leer el mismo documento sin correr los códigos potencialmente peligrosos.

¿Por qué los Criminales Cibernéticos Aman el Comercio Electrónico y la Banca en Línea?

La mayoría de nosotros hemos oído la cita erróneamente atribuida al famoso ladrón de bancos Willie Sutton en contestación a la pregunta: “¿Por qué Usted roba bancos?”. La respuesta: “Porque allí es donde está el dinero”. Sin tener en cuenta quien la dijo realmente, tiene sentido.

También tiene sentido que aparezca un número cada vez mayor de criminales en línea, porque cada vez hay más dinero en ella. El comercio electrónico, la banca en línea y

tecnologías afines han traído como resultado que transacciones financieras de millones de dólares tengan lugar a través de las conexiones de redes.

Estadísticas Cibernéticas....

Predicciones del Comercio Electrónico

Forrester Research (www.forrester.com) predice que en el 2004, la suma total de transacciones de comercio electrónico alcanzará los 3.5 *trillones* de dólares sólo en los Estados Unidos, con otro 1.6 trillones de dólares en Asia y 1.5 trillones de dólares en Europa Occidental.

Quizás la creciente popularidad de las compras, la banca, el almacenamiento y otras actividades financieras en línea, se resume mejor en el título de un artículo publicado por Nua acerca de un estudio en el estado de Penn sobre las actividades en Internet: *Sexo afuera, Comercio Electrónico adentro*. El estudio indicaba que los usuarios de Internet están invirtiendo de manera global proporcionalmente menos tiempo cada año (basado en los datos del período 1997-2001) en buscar en línea materiales sobre sexo y más tiempo en negocios y transacciones financieras.

El Problema con el Comercio Electrónico y la Banca en Línea

La naturaleza abierta y el amplio alcance de la Internet la convierte en un forum perfecto para realizar negocios. Se pueden llevar a cabo transacciones entre una empresa y un cliente de la calle de enfrente o de cualquier parte del mundo. Esos ciberespacios amplios y abiertos también exponen a ambos: al comprador y al vendedor, a riesgos que no están presentes o, al menos no en la misma extensión, en las transacciones cara a cara.

Estadísticas cibernéticas....

Transacciones Fraudulentas en Línea

De acuerdo con el sitio Web informativo de Nua sobre tendencias y estadísticas (www.nua.com), el fraude en línea alcanzó los 700 millones de dólares en el 2001.

Epaynews.com reportó que Meridien Research estimó que el costo del fraude en Internet alcanzaría entre los 5 y los 15 billones de dólares en el 2005. La cifra más baja está basada en compañías que invierten en softwares antifraudes; la más alta predice qué sucederá sin tal inversión. (Véase www.epaynews.com/statistics/fraud.html#1).

Cuando los compradores tienen que introducir la información de su tarjeta de crédito para efectuar una compra, se preocupan con toda razón de que la información pueda caer en manos equivocadas. Algunos dirían que el proporcionarle esta información a un vendedor con base en la Web no es diferente a darla a través del teléfono, pero esta filosofía no toma en cuenta la diferencia entre una conexión telefónica y una transacción en Internet.

Una llamada telefónica establece un circuito temporalmente privado dedicado directamente entre el que llama y el que recibe. Aunque es posible interceptar una línea telefónica, es

relativamente difícil y costoso. La información enviada por correo electrónico o por un formulario de la Web viaja por la muy pública Internet y pasa por un número de nodos (servidores y enrutadores) durante su trayecto. Es vulnerable a ser interceptada y, a menos que la información esté encriptada, podría ser usada para efectuar compras no autorizadas.

En la escena....

Experiencias de la Vida Real

Como resultado de que un mayor número de compañías estén vendiendo en línea, han ocurrido en muchas ocasiones violaciones de la seguridad que exponen la información de las tarjetas de crédito de los clientes. BiblioFind.com, un vendedor de libros, reveló en marzo del año 2001 que sus servidores, que almacenan los datos de las tarjetas de crédito de sus clientes, han estado sujetos a una ruptura de la seguridad que tomó cuatro meses. En diciembre del mismo año, CreditCards.com, una firma procesadora de tarjetas de crédito, tuvo más de 50,000 números de tarjetas de crédito robados de su sitio Web.

Charles Schwab Corporation y la compañía corredora en línea E*TRADE descubrieron lagunas de seguridad en sus redes que expusieron las cuentas de operaciones bursátiles de los clientes.

Internet también le facilita a los criminales intercambiar esta información obtenida ilegalmente. Listados de números de tarjetas de crédito robados aparecen en grupos de noticias que son visitados por individuos con mentalidad criminal.

De hecho, la incidencia de fraude con tarjetas de crédito en transacciones en línea es significativamente mayor que aquella con métodos de compra más tradicionales. De acuerdo con un documento sobre el fraude con tarjetas de crédito publicado por la Sección de Investigaciones del Centro Nacional contra Crímenes de Cuello Blanco (NW3C), los estimados calculan que el porcentaje total del fraude con tarjetas de crédito es aproximadamente del 0.80% de todas las transacciones con tarjetas de crédito, pero la misma fuente estima que entre el 3 y el 5% de todas esas transacciones llevadas a cabo en línea son con cuentas fraudulentas.

Las compras con tarjetas de crédito no son las únicas transacciones financieras en línea que exponen a los consumidores al riesgo. Un creciente número de profesionales ocupados están recurriendo a la comodidad de la banca en línea para depositar, transferir dinero y pagar cuentas. Aunque uno podría asumir que los bancos, de todos los negocios, seguramente han de tener implementadas adecuadas medidas de seguridad, se ha descubierto un número de brechas serias en la seguridad de algunos sistemas bancarios en línea.

En el 2000, una falla en el software empleado por un banco en línea con base en Palo Alto, California, le permitía a cualquiera abrir una cuenta y usarla para transferir fondos de las cuentas de otros clientes sin su permiso usando los números de cuenta y de enrutamiento para la cuenta de la víctima. (Esos números están impresos en los talonarios de cheques, así que lo único que necesitaría el ladrón es mirar un cheque de la víctima). El Barclays Bank en el Reino Unido ha reportado violaciones de la seguridad en sus servicios en línea

que permitían mostrar a otros la información de las cuentas de los clientes. Problemas similares han rondado a otros bancos en línea de todo el mundo.

Hoy parece que casi todas las transacciones financieras –desde comprar galletas Girl Scout hasta financiar un préstamo para una casa- se pueden realizar en línea. Cada vez que Usted envía información sensible a través de la NET, tiene que estar consciente de los riesgos. El pasado noviembre, una empresa de seguridad electrónica descubrió una falla de seguridad en el software que muchos asesores hipotecarios usan para procesar solicitudes de préstamos. La falla trajo como consecuencia la visualización en Internet de solicitudes completadas por cientos de clientes, exponiendo informaciones como los números de Seguridad Social que podrían usarse para robar sus identidades.

En la escena...

Experiencias de la Vida Real

En mayo de 2001, los investigadores del FBI presentaron cargos por fraude con tarjetas de crédito, fraude bancario y otros fraudes en línea arribando a un estimado total de 117 millones de dólares contra casi 100 individuos y empresas como parte de la *Operation Cyberloss*.

Cómo proteger su Comercio Electrónico y sus Transacciones Bancarias en Línea

Proteger el comercio electrónico y las transacciones bancarias en línea debe ser un esfuerzo mancomunado de todos los que participan. El “trío de protección” incluye a:

- Los profesionales de la informática que corren los servidores de bancos o de comercio electrónico
- El consumidor que disfruta de los servicios de comercio electrónico y banca en línea
- La comunidad de la ley y el orden

El papel de los profesionales de la informática es asegurar los servidores que se usan para efectuar transacciones financieras, utilizando tecnologías como los muros de fuego con el fin de evitar que los de fuera los penetren y roben información confidencial, y encriptaciones potentes en aras de proteger los datos cuando viajan desde los consumidores hasta el servidor a través de los ISP. Los Capítulos 7 y 8 analizan la seguridad del servidor Web y protocolos como Secure Sockets Layer (SSL), Transport Layer Security (TLS) y Secure http (S-http) que se pueden usar para transmitir datos de forma segura a través de los visualizadores Web.

Los consumidores también tienen que estar conscientes de los peligros de las transacciones en línea de modo que puedan tomar precauciones como no dar nunca los números de sus tarjetas de crédito e información similar a menos que el sitio Web o el formulario sean seguros. Los consumidores necesitan comprender cómo asegurar las computadoras de sus casas u oficinas que usan para realizar transacciones en línea, porque sus contraseñas y otras informaciones personales se pueden almacenar en sus propios discos duros locales, y cómo configurar apropiadamente las opciones de seguridad en sus visualizadores Web.

En la escena...

Experiencias de la Vida Real

Un popular banco en línea llamado Egg, con sede en el Reino Unido, detectó intentos de abrir cuentas bancarias fraudulentas en línea en el año 2000 y contactó al Nacional Crime Squad (Equipo Nacional contra el Crimen), que pudo rastrear y arrestar a los aspirantes a pillos.

Los agentes del orden deben comprender el alcance y la naturaleza del problema del fraude en línea y deben ser instruidos sobre cuál información obtener, cómo rastrear y preservar la evidencia y sobre los recursos privados y federales que pueden proporcionarle guía e información al tratar con estos tipos de casos.

La jurisdicción, como de costumbre, es un tema. El gobierno de los Estados Unidos creó, en mayo de 2000, el Centro de Quejas de Fraudes Electrónicos (IFCC) para proporcionarle una vía a las víctimas del crimen en línea de presentar quejas e informaciones a una fuente centralizada en lugar de tener que descubrir qué agencia de la ley y el orden tiene jurisdicción en su situación en particular. El IFCC es dirigido por el FBI en sociedad con el NW3C.

¿Por qué los Criminales Cibernéticos Aman la Mensajería Instantánea?

La mensajería instantánea (IM) le da a los usuarios de Internet la posibilidad de comunicarse en tiempo real próximo con otros en cualquier parte del mundo. Es una aplicación que inspira mucha pasión: Usted lo mismo la ama que la odia. Algunas personas consideran la “IM’ing” una pérdida de tiempo y una intrusión, pero otras pasan felizmente horas en casa y en el trabajo comunicándose por esta vía. Sí tiene ventajas incluso en el entorno empresarial, Usted puede tener respuestas inmediatas a sus preguntas sin tener que esperar a que un correo electrónico pase o tener que pagar por llamadas de larga distancia.

Tan cómoda como podría ser, el software de mensajería instantánea (AIM de AOL e ICQ, el MSN Messenger de Microsoft, el Yahoo Instant Messenger y otros) representa serios riesgos de seguridad, además de proporcionarles a los criminales una vía fácil de comunicarse con otros para planear o discutir sus crímenes.

Estadísticas cibernéticas...

La Popularidad de la Mensajería Instantánea

De acuerdo con un artículo de Reuters publicado en *USA Today* en enero del año 2002, en ese entonces, aproximadamente 100 millones de usuarios se habían registrado en el servicio AIM de AOL.

El Problema con la Mensajería Instantánea

Por defecto, la mayoría de los productos de mensajería instantánea están configurados para mantenerse activos todo el tiempo, corriendo en el fondo, y transmitir que el usuario está en

línea aún cuando la interfase del programa está cerrada. Esto no sería tan malo excepto porque el software de mensajería instantánea también permite el envío de ficheros entre usuarios, lo que significa que no resulta tan difícil para un hacker entendido usar este canal abierto para transferir virus ocultos en Troyanos u otros “regalos” no deseados.

También se pueden explotar otras fallas de programación de la IM para ejecutar códigos maliciosos. Por ejemplo, algunas versiones de los programas AIM e ICQ de AOL estaban sujetas a un error de “desbordamiento del búfer” si a la aplicación se le enviaban más códigos de los que podía manejar. Este error le permitió a los hackers descargar códigos maliciosos hacia la computadora objetivo. Aunque este problema particular fue solucionado en las venideras versiones del software, resulta imposible saber cuántas personas continuaron usando inconscientemente la versión con fallas del software tras revelarse el problema.

En febrero de 2002, se reportaron dos bugs (errores de programación) en el software del MSN Messenger de Microsoft: uno que expone nombres y direcciones de correo electrónico en la lista de contactos de la víctima y otro potencialmente más peligroso que le puede permitir a un hacker tomar control del programa y realizar tareas en la computadora del usuario aprovechándose de una laguna de seguridad en el Explorador de Internet conocida como *Document.Open()* bug.

Aunque los comercializadores de los productos de IM son bastante buenos sacando al mercado soluciones para estas fallas de seguridad una vez que se conocen, se continúan encontrando nuevas explotaciones y muchos usuarios no actualizan sus softwares muy a menudo. Ellos podrían ignorar el problema hasta que se convierten en víctimas de él. Los administradores de redes y otros profesionales de la informática deben mantenerse actualizados en estos temas suscribiéndose a revistas informativas sobre seguridad y visitando regularmente los sitios Web de boletines informativos sobre dicho tema. Entonces deben trabajar para educar a los usuarios en sus organizaciones sobre las vulnerabilidades de la seguridad y velar por que estén instaladas las actualizaciones y soluciones una vez que salgan al mercado.

Otro posible problema de seguridad es el registro de la IM que guarda el contenido de las discusiones en línea. Un hacker podría acceder a él y exponer conversaciones privadas.

De hecho, los comercializadores de productos de IM generalmente admiten que sus productos no son seguros y en sus acuerdos con el usuario final, recomiendan que no los usen para comunicaciones sensibles. No obstante, muchos usuarios empresarios discuten asuntos personales, financieros y decisiones sobre presupuestos, estrategias de mercado y otras informaciones confidenciales a través de los mensajes instantáneos.

Otro problema con el software de IM es que no existe un mecanismo confiable de autenticación para verificar que la persona que le está enviando un mensaje a través de Internet es realmente la que dice ser. Cualquiera puede crear una cuenta de IM utilizando un nombre y una información falsos. Por esta razón, los mensajes instantáneos son también una vía popular para los pedófilos, estafadores y otros criminales de entrar en contacto con sus víctimas y conocer a aquellos que escogieron para sus crímenes.

Cómo Proteger su Sistema de las Fallas de Seguridad de la Mensajería Instantánea

La mejor forma de evitar los problemas de seguridad inherentes a la mensajería instantánea es no usar los programas o usarlos sólo cuando sea necesario y nunca para comunicaciones sensibles o asuntos de extrema importancia. Muchas empresas bloquean los puertos utilizados por el software de IM en sus muros de fuego para evitar que los empleados usen los programas.

Si Usted tiene que usar la IM, aquí tiene algunas cosas que puede hacer para reducir el riesgo:

- Bloquear la opción de transferencia de ficheros y juegos en el muro de fuego.
- Si los usuarios sólo necesitan comunicarse con otros dentro de la compañía, los administradores pueden instalar programas de IM que corran en la Intranet, reduciendo la exposición a la Internet.
- Los usuarios deben cerrar completamente el programa cuando no lo estén usando (si sólo cierran la interfaz puede provocar que el programa siga corriendo en el fondo – verifique la bandeja del sistema o la lista de procesos en uso para asegurarse).
- Los usuarios no deben aceptar mensajes de personas desconocidas.
- Algunos programas de IM le permiten bloquear la visualización de su dirección IP para los destinatarios. Si usted no confía completamente en la persona con la que está conversando, será mejor que habilite esta opción.
- Salga y desconéctese de su cuenta o, si necesita conservar los registros, mueva los ficheros para otro lugar que no sea el implícito e encriptelos.

Al igual que las otras tecnologías que hemos analizado, el software de IM puede ser usado para bien o mal. Debido a que los programas fueron originalmente diseñados para el chateo recreativo, la seguridad no ha sido una prioridad alta, pero si Usted utiliza la mensajería instantánea en un entorno empresarial o en una máquina de la casa que tiene almacenados datos sensibles, es importante tener en cuenta las ramificaciones de seguridad.

¿Por qué los Criminales Cibernéticos Aman los Nuevos Sistemas Operativos y las Nuevas Aplicaciones?

Las demandas del usuario y las capacidades de hardware que se incrementan rápidamente traen como resultado que cada pocos años salgan al mercado nuevos sistemas operativos (o al menos nuevas versiones). Cada nueva encarnación incluye nuevas e ingeniosas características y, en muchos casos, las versiones nuevas son más estables y tienen mejor rendimiento que sus predecesoras. Parece que los usuarios apenas tienen tiempo de aprender un sistema operativo antes de que sea hora de mejorarlo. Lo mismo es válido para las aplicaciones de productividad; una vez que Usted eleva el nivel de prestaciones del sistema operativo, a menudo necesita una nueva versión de su procesador de texto o softwares gráficos compatibles con éste.

Este sistema es genial para las compañías de softwares, las que logran una gran cantidad de nuevas ventas – pero también es genial para los hackers por un par de razones:

- Softwares nuevos, especialmente sistemas operativos que incluyen cambios dramáticos como Windows 2000 de Microsoft o Mac OS X de Apple, que nunca salen perfectos de la caja en relación con la incontable cantidad de horas de comprobación beta que requieren. La versión 1.0 (y a veces algunas otras versiones sucesoras) es casi siempre al menos un tanto imperfecta y los hackers, a menudo, pueden explotar esas imperfecciones.
- Aún si el software es perfecto, los usuarios no están bien familiarizados con él todavía y pudieran desconfigurarlo de modo que se creen vulnerabilidades en la seguridad.

Es por eso que los criminales cibernéticos se alegran cuando Usted actualiza la máquina con el mejor y más reciente software. Eso le abre a ellos una ventana de oportunidades antes de que se reporten las imperfecciones y salgan al mercado los parches de seguridad – y antes de que los usuarios aprendan a configurar los nuevos sistemas para alcanzar la máxima seguridad.

No hay mucho que Usted pueda hacer al respecto, excepto quizás dejar pasar la tentación de ser uno de los “primeros adoptadores” de cada uno de los softwares que aparecen. Incluso si Usted espera por la versión 2.0 o por una posterior, tendrá que lidiar con la curva de aprendizaje de los usuarios. Los administradores de redes deben ser especialmente cautelosos y monitorear de cerca las violaciones de seguridad durante el período inmediato posterior a actualizaciones importantes o a la introducción de un software completamente nuevo.

¿Por qué los Criminales Cibernéticos Aman la Estandarización?

Quizás suene como una contradicción decir que los criminales cibernéticos aman lo nuevo y lo diferente y después voltear y decir que ellos aman la estandarización, pero realmente no lo es. Lo que entendemos por estandarización es que todos (o una gran mayoría) usen los mismos sistemas operativos, las aplicaciones, los protocolos y el hardware.

La estandarización le facilita las cosas a los hackers porque no tienen que aprender a manipular docenas de diferentes tipos de sistemas. Cuando un producto se convierte en estándar, también se convierte en un blanco favorito de los hackers, crackers y escritores de virus. Los usuarios de los sistemas operativos de Windows son más vulnerables al ataque que los usuarios de otros sistemas, en gran parte, porque la gran mayoría de las computadoras de los usuarios corren Windows. Es una cuestión de sentido común: Si Usted quiere hacer la mayor cantidad de daño con un virus, escribe uno dirigido al sistema operativo más popular.

Usted no ve muchos hackers allá afuera tratando de crackear el OS/2Warp (sistema operativo para los clientes de la IBM que tiene un muy pequeño porcentaje del mercado de las computadoras de mesa). Podría no ser una coincidencia que muchos de los clientes existentes del OS/2 estén desplegados en la industria bancaria, un negocio que requiere de toda la seguridad que pueda alcanzar.

La estandarización posibilita la interconexión y las comunicaciones entre computadoras en una gran escala, pero también les posibilita a los hackers hacer sus daños en una gran escala. Los estándares son buenos toda vez que hacen que el hardware y el software de una computadora funcionen sin problemas, pero si su negocio maneja informaciones sensibles, una forma de hacer a sus sistemas menos vulnerables es utilizar una solución de marca registrada en lugar de una solución industrial estándar.

Haciendo Planes para el Futuro: Cómo Frustrar al Criminal Cibernético del Mañana

¿Qué significa toda esta información si hacemos planes para un futuro en el que todos posiblemente seamos víctimas del crimen cibernético? ¿Tendremos que renunciar a nuestras conexiones rápidas y siempre en línea y retornar a los módems por marcación? ¿Tendremos que renunciar a las comodidades de la computación inalámbrica y móvil y retornar a los visualizadores Web basados en textos Lynx y al programa de correo electrónico PINE? ¿Tendremos que dejar de chatear en línea y hacer cola nuevamente en las ventanillas de los servi-autos de los bancos? ¿Tendremos que aferrarnos a nuestro antiguo software una vez que hemos aprendido a usarlo o tendremos que cambiar para algún software exótico de marca registrada del que nadie más ha oído jamás?

Por supuesto que no haremos nada de eso, probablemente no podamos hacer nada de eso. Lo que *podemos* hacer es estar conscientes de los peligros que representa cada uno de los grandes milagros tecnológicos y tomar medidas que nos protejan de la explotación criminal de esas tecnologías mientras nos seguimos permitiendo el disfrute de sus beneficios. Los Capítulos del 4 al 8 de este libro proporcionan detalles bien específicos sobre cómo alcanzar este objetivo.

Resumen

Aquellos que no pueden recordar el pasado están condenados a repetirlo. –George Santayana

Las computadoras y la interconexión existen solamente desde hace pocas décadas. Por lo tanto, el crimen cibernético tiene una historia breve pero colorida. ¿Qué podemos aprender de esa historia que nos ayude a construir un futuro en línea más seguro?

Como hemos leído a través de algunos de los acontecimientos que nos trajeron hasta donde estamos hoy, podemos observar que el ciberespacio continua pareciéndose mucho al Oeste Americano de los años 1800: caótico e inestable, una nueva frontera del oeste que aún no ha sido dominada. La ARPA tiene su propia agenda, las universidades de investigación involucradas en los comienzos de la Net tienen sus grandes sueños, las compañías que aparecieron en línea en los 90 tienen sus planes de marketing, los individuos que “viven en línea” tienen sus razones y los criminales que se aprovechan de la tecnología tienen sus motivos. Sin embargo, no hubo un gran plan maestro por el que la Internet evolucionara hasta ser la parte integral de nuestras vidas que hoy ocupa. Más bien “creció de esa forma”

y el resultado fue una mezcla de sistemas y tecnologías que funcionan sorprendentemente bien a pesar de su naturaleza al azar.

Con el advenimiento del siglo veinte, la Internet entra en una nueva fase de su existencia. La ley y el orden están llegando a la nueva frontera del oeste, convirtiéndola en un “sitio” más seguro – y quizás menos creativo y divertido – donde trabajar y jugar. Aquellos que extrañan los “buenos tiempos de antes” cuando la Net era competencia de sólo unos pocos selectos y el crimen en línea no era – o no parecía ser- un problema, no están entendiendo: El genio no regresará a la botella.

Los especialistas que hacen cumplir la ley saben que los métodos policiales que funcionan en las áreas rurales no son necesariamente los apropiados para las zonas densamente pobladas y más pobres de la ciudad y viceversa. La Internet de hoy no es el pequeño pueblo virtual que solía ser, ahora es un animado entorno urbano internacional. Y si somos nosotros los responsables de convertirla en un entorno seguro para nosotros y nuestros hijos, nuestras tácticas de combate contra el crimen cibernético tendrán que reflejar eso- lo mucho que deseamos que no sea así.

Preguntas Realizadas con Frecuencia

Las siguientes preguntas realizadas con frecuencia, respondidas por los autores de este libro, están diseñadas para medir su comprensión de los conceptos presentados en este capítulo y para ayudarlo con la implementación de estos conceptos en la vida real. Para hacer que el autor conteste a sus preguntas, visite www.syngress.com/solutions y haga clic en el formulario “**Pregúntale al autor**”.

P: ¿Y qué hay con el Servicio de Internet por satélite? ¿Tiene las mismas vulnerabilidades de seguridad que el DSL y el cable?

R: Los servicios de Internet por Satélite como DirecPC y Starband utilizan una antena parabólica para transmitir señales desde y hacia un satélite geoestacionario (de posición fija) que se encuentra a 22,300 millas por encima de la tierra. Las ondas de radio (que viajan a la velocidad de la luz o aproximadamente a 186,000 millas por segundo) tienen que hacer el viaje doble cuando Usted manda una comunicación vía satélite hacia una computadora en cualquier lugar del mundo. Durante este viaje, las ondas de radio son vulnerables a interceptaciones, exactamente como sucede con otras tecnologías inalámbricas. A diferencia de una transmisión inalámbrica con base en la tierra, la transmisión por satélite le permite al atacante escuchar desde cualquier lugar en un área inmensa (el rango de recepción del satélite). Los sistemas satelitales usan frecuencias de salto y tecnologías de múltiple acceso que dividen la señal, haciéndola, de algún modo, más difícil de ser interceptada. Además, algunos sistemas como DirecPC usan una VPN para la conexión, lo que le impide a los usuarios montar sus propias VPN para solucionar las preocupaciones en cuanto a la seguridad. Por otra parte, debido a que el satélite ofrece una mejor amplitud de banda que la mayoría de las tecnologías inalámbricas, resulta más fácil utilizar métodos de autenticación y de codificación potente.

P: ¿Es importante si tengo una dirección IP estática o una dinámica?

R: Sí. Aunque existen ventajas al tener una dirección IP estática (como la posibilidad de correr un servidor Web, sitios FTP o una VPN), la seguridad no es una de ellas. Muchos proveedores de banda ancha dan una dirección IP estática, pero otros usan tecnologías que cambian regular y automáticamente su dirección IP (todos los días o incluso cada una hora) y algunos dan varias direcciones IP de modo que Usted mismo pueda cambiarla manualmente cuando lo desee. Esto le dificulta al hacker el seguir atacando su sitio una vez que lo haya encontrado.

P: ¿Es importante qué protocolos de autenticación para acceso remoto se usen? ¿Existen algunos más seguros que otros?

R: La respuesta es otro rotundo “sí”. Los dos protocolos de autenticación más comunes usados para conexiones por marcación PPP (Protocolo de Punto por Punto) son el PAP (Protocolo de Autenticación de Claves) y el CHAP (Protocolo de Autenticación llamado Challenge Handshake). El PAP solamente envía el nombre y la contraseña del usuario a través de la red hacia el servidor en forma de texto plano. Si los paquetes son interceptados por el camino, la contraseña puede ser leída y robada. El CHAP utiliza la encriptación simétrica para proteger las contraseñas enviadas a través de la red. Sin embargo, el modo en que el CHAP funciona crea un nuevo problema. El servidor genera una clave aleatoria denominada *challenge* y la envía al cliente, el cliente usa la clave para encriptar la contraseña y envía de regreso la contraseña encriptada hacia el servidor. El servidor busca la contraseña del usuario en su base de datos, usa la misma clave para encriptarla y compara el resultado con la contraseña encriptada enviada por el cliente. Aunque la contraseña de texto plano no pasa jamás a través de la red con este método, el servidor tiene que almacenar una versión de texto plano de la contraseña del usuario en su base de datos con el fin de hacer la encriptación para comparar. Si un intruso accede a la base de datos del servidor, este tendrá las contraseñas para todos los usuarios. RADIUS es una alternativa más segura.

Referencias

- John Draper: *Viva como un Hacker*
www.rit.edu/~gpm8967/imm/Draper/index.html
- Internet Timeline v5.6 de Hobbes
www.zakon.org/robert/internet/timeline
- El Gusano de Internet de 1988
<http://world.std.com/~frnl/worm.html#p3>
- Centro de Quejas de Fraudes Electrónicos
www1.ifccfbi.gov/index.asp

- ComputerUser.com: *Seria Ruptura de Seguridad en la Banca en Línea*
www.computeruser.com/newstoday/00/01/31/news4.html
- Cable Datacom News, Cable Modem Info Center
www.cabledatacomnews.com/cmhc
- Seguridad DSL/Cable: Vínculo con Guide Picks
<http://compnetworking.about.com/cs/dslcablesecurity>
- *Seguridad del Acceso Remoto a la Red*
<http://home.indy.net/~sabronet/secure/remote.html>
- ExtremeTech: *Explotando y Protegiendo las Redes Inalámbricas 802.11b*
www.extremetech.com
- Instituto SANS: *Seguridad en el Satélite de Internet*
<http://rr.sans.org/wireless/satellite.php>

Comprendiendo a las Personas en la Escena

Tópicos que investigaremos en este capítulo:

- **Comprendiendo a los Criminales del Ciberespacio**
- **Comprendiendo a las Víctimas del Ciberespacio**
- **Comprendiendo a los Investigadores del Ciberespacio**

- ✓ **Resumen**
- ✓ **Preguntas Realizadas con Frecuencia**
- ✓ **Recursos**

Introducción

El crimen cibernético, por definición, involucra a computadoras y redes. Sin embargo, con lo sofisticada que se ha tornado la tecnología y lo fascinante que podría ser la ciencia de la inteligencia artificial (AI), no hemos arribado todavía al punto en que las computadoras pueden – por sí mismas – realizar una actividad criminal. Las máquinas son extremadamente dóciles (a veces resulta difícil creer que las estamos forzando para que trabajen) y totalmente amorales. Ellas hacen lo que se les dice que hagan, sin protestas, lamentos o motivos ulteriores. Un crimen cibernético involucra siempre al menos a un ser humano quien origina, planea, prepara e inicia el acto criminal.

Pero, por lo general, el criminal cibernético no es la única persona en la escena del crimen cibernético. Algunos crímenes cibernéticos aparentan no tener víctimas, como es el caso de una intrusión a una red que ocurre sin que nadie sepa sobre ello, en la que no se daña ningún fichero y no se “roba” o malversa ninguna información. En la mayoría de los casos, sin embargo, alguna o algunas personas terminan dañadas a la larga por causa de los actos de los criminales cibernéticos. Estas víctimas podrían ser trabajadores que pierden tiempo productivo debido a un ataque DoS o que tienen que rehacer su trabajo por causa del vandalismo cibernético. Podrían ser accionistas de la compañía que pierden dinero debido a los recargos por el ancho de banda que un hacker utiliza. Podrían ser gerentes que pierden “puntos” con sus jefes por motivo del impacto en sus presupuestos. Podrían ser administradores informáticos que pierden sus empleos por “permitir” que suceda el ataque. En la mayoría de los casos de crímenes cibernéticos, si busca bien, encontrará una víctima.

Cuando se reportan estos crímenes a la policía o a otras agencias del orden, se involucra a más personas. Los investigadores que recopilan pistas para descubrir la identidad del criminal cibernético y reunir la evidencia pueden pasar días, semanas o meses en un solo caso. Las aptitudes, el conocimiento, la perseverancia y la determinación de un investigador podrían tener un profundo impacto en el éxito del caso.

Cuando el crimen cibernético ocurre en el entorno empresarial, el personal directivo también se ve inevitablemente envuelto. Como mencionamos en los capítulos precedentes, el personal de las agencias del orden y los profesionales de la informática que necesitan cooperar en el proceso investigativo, a menudo, se enfrentan. Los gerentes que saben que el crimen cibernético está dañando lo esencial de la compañía y que tienen un interés personal en minimizar el daño y ver a los criminales cibernéticos responder ante la justicia, asumen con frecuencia una posición única de facilitar la cooperación entre los otros jugadores.

En este capítulo, le echaremos un vistazo – muy de cerca – a todas esas personas en la escena del crimen cibernético. Examinaremos los papeles de ambos: los criminales cibernéticos y las víctimas, y cómo interactúan –a veces de modo que reflejan la relación del “mundo real” criminal-víctima y a veces de modo bastante diferente.

Trataremos de entrar en las cabezas de los criminales cibernéticos y comprender qué los motiva. Mostraremos cómo los criminales cibernéticos se pueden dividir en una serie de

categorías diferentes y cómo determinar la categoría a la que pertenece un pillo cibernético puede protegerlo a Usted de sus acciones. También buscaremos patrones que nos ayuden a predecir quién será la víctima del crimen cibernético y analizaremos formas de hacer menos vulnerables a víctimas potenciales.

Entonces regresaremos a los profesionales en la escena: los oficiales de la policía e investigadores privados o corporativos y los profesionales de la informática empleados por las compañías afectadas o que han sido traídos en calidad de asesores. Discutiremos las características de un buen investigador de crímenes cibernéticos y el tipo de currículum y preparación que pueden darle al aspirante a detective cibernético una ventaja para el empleo. Además nos concentraremos en los problemas específicos de los profesionales de la informática y de la policía cuando intentan colaborar y cómo ellos pueden superar estos problemas.

Finalmente le echaremos una mirada especial al papel que juega el oficial ejecutivo jefe (CEO) o director en crímenes cibernéticos relacionados con empresas. Examinaremos qué necesitan el equipo de informáticos y la policía – y qué no – de la directiva superior y cómo los directores pueden facilitar el proceso investigativo a veces colmado de confrontaciones.

A este punto, Usted podrá estarse preguntando por qué este libro parece alejarse de repente de los tópicos técnicos de la computación y de las leyes para hurgar en una “ciencia suave” como la psicología. ¿Por qué Usted – un profesional de la informática o un oficial del orden – necesita “comprender” al criminal cibernético? ¿Por qué debería importarle qué motiva a una persona así a infringir la ley? ¿Qué diferencia hay para Usted si algunos tipos de personalidad (y recuerde que las compañías también tienen “personalidades”) son más propensos que otros a ser víctimas de crímenes cibernéticos? ¿Un investigador no sigue siéndolo a pesar del tipo de crimen que se haya cometido? ¿Por qué son necesarias aptitudes especiales o características personales para un investigador de crímenes cibernéticos? Las respuestas a estas preguntas se las daremos a medida en que avance en este capítulo. Específicamente:

- Le mostraremos como un entendimiento de los principios básicos de la *psicología criminal* puede colocarlo a Usted a un paso adelante del criminal cibernético. Usted verá como conocer qué motiva a un criminal puede ayudarlo a capturarlo – o incluso a tomar medidas para prevenir que ocurra el próximo crimen.
- Aprenderá sobre *perfiles criminales*, un tema analizado con frecuencia y con frecuencia mal representado en los medios de comunicación populares.
- Hablaremos sobre la ciencia de la *victimología* – el estudio de las características de la víctima del crimen con el objetivo de determinar por qué los criminales escogen a ciertas personas como sus víctimas.
- Discutiremos las *aptitudes para la carrera* con respecto al investigador criminal. Descubrirá por qué algunas personas están mejor preparadas para este papel que otras. Aprenderá por qué, en muchos casos, la investigación tiene tanto de arte como de ciencia.

El elemento humano no es sólo un componente importante de cada caso criminal, incluyendo a los crímenes cibernéticos – a menudo es el más fascinante. Iremos al grano de los detalles técnicos (y habrán muchísimos) en los capítulos posteriores. Pero, primero,

vamos a ahondar en las cuestiones complejas y con frecuencia confusas que rodean a las personas que cometen, son víctimas o dedican sus días de trabajo a prevenir, solucionar y enjuiciar el crimen cibernético.

Comprendiendo a los Criminales Cibernéticos

Una serie de disciplinas científicas están dedicadas a comprender mejor a los criminales y el comportamiento criminal. La *psicología criminal* es el estudio de la mente criminal y de lo que lleva a una persona a adoptar un comportamiento ilegal o socialmente desviado. Usted puede concebir la psicología criminal como una subcategoría de la *psicología forense* que se ocupa de los asuntos emocionales y conductuales pertenecientes a los sistemas legislativos y legales e incluye a los psicólogos de la policía (quienes tratan las cuestiones emocionales y conductuales con los oficiales de la policía), a los psicólogos sociales (quienes estudian el comportamiento de grupo y las implicaciones sociales más extensas de las cuestiones psicológicas) y otros. El trabajo de un psicólogo criminal puede también coincidir con el del *criminólogo*, quien estudia a los criminales, el crimen, el efecto del sistema de justicia penal, los factores sociales en la conducta criminal y los índices de crímenes.

Nota

La *psicología forense* es una disciplina diferente de la *psiquiatría forense*, definida por la American Academy of Psychiatry and the Law (AAPL) como “una sub-especialidad médica que incluye la investigación y la práctica clínica en las muchas áreas en las que se aplica la psiquiatría a las cuestiones legales”. (Véase <http://flash.lakeheadu.ca/~pals/forensics/forensic.htm>). Los psiquiatras forenses son doctores en medicina que pueden tratar a pacientes, prescribir drogas controladas y practicar la medicina. Los psicólogos forenses pueden trabajar también directamente con pacientes, pero los psicólogos criminales generalmente se concentran en el estudio de los casos de criminales para detectar patrones, analizar conductas y hacer predicciones y perfiles basados en sus análisis.

En la escena...

En el FBI

La *Ciencia Conductual* es un término amplio que se refiere al uso de métodos científicos para estudiar la conducta de criaturas vivas (incluyendo a los humanos). Las *ciencias conductuales* se usan a menudo como un término colectivo que se refiere a la psicología, sociología, antropología y otras ciencias que estudian la conducta de personas o animales. El FBI emplea el término de una manera mucho más específica como en el nombre de su Unidad de Ciencia Conductual (BSU, Behavioral Science Unit) de su academia de entrenamiento en Quantico, Virginia.

Dicha unidad se concentra en el estudio de la conducta humana relacionada con los criminales y el crimen. El personal del FBI que labora en la BSU está entrenado como agentes especiales que además tienen títulos avanzados en psicología, sociología, criminología, etc. La BSU es famosa por sus éxitos en crear perfiles criminales de asesinos

en serie y otros criminales violentos. Ésta utiliza una serie de metodologías tales como el análisis computarizado del crimen, la psicología clínica forense y la psicología criminal aplicada para ayudar a otras agencias del orden a resolver crímenes y capturar a los criminales.

Muchos de los especialistas en ciencia conductual del FBI son personas de renombre fuera de la agencia. Robert Ressler, John E. Douglas, James T. Reese y Roy Hazelwood son todos famosos por su trabajo como parte de la BSU en varios casos de alto perfil.

En las últimas décadas ha evolucionado una nueva especialidad psicológica: la *psicología investigativa*. La psicología investigativa es la aplicación del conocimiento de principios psicológicos al trabajo policial y a la investigación criminal.

A pesar del interés del FBI y de muchas agencias policiales grandes de aplicar métodos científicos como la psicología criminal a las investigaciones policiales, muchos oficiales de la policía a nivel local aún están escépticos. ¿Por qué debería importarme el *entender* a los criminales?, se preguntan. “Todo lo que quiero es capturarlos y ponerlos tras las rejas”.

Esta actitud se debe generalmente a un malentendido del significado de la palabra *entendimiento*. Uno de sus significados, en efecto, es “simpatía, empatía o tolerancia”. La policía (como es lógico) no ve razón alguna para mostrar esta clase de sentimiento hacia los que infringen la ley, especialmente hacia personas que causan daños a otros al hacerlo. No les estamos pidiendo mostrar este significado de la palabra *entendimiento*.

El otro significado de la palabra es “percibir y explicar el significado o la naturaleza de alguien o algo”. Ese es el tipo de entendimiento que Usted necesita como un oficial de la policía o un profesional de la informática envuelto en la investigación de crímenes cibernéticos, pues él lo relaciona con la forma de pensar y las motivaciones del criminal cibernético. Usted necesita esa clase de entendimiento, porque lo ayudará a capturar al criminal y ponerlo tras las rejas.

Creando Perfiles de los Criminales Cibernéticos

La creación de perfiles criminales es el arte y la ciencia de describir las características de un criminal (físicas, intelectuales y emocionales) basándose en la información recopilada en la o las escenas del crimen. Un *perfil criminal* es una valoración psicológica realizada antes del hecho – o sea, sin conocer la identidad del criminal. El perfil consiste en un conjunto de características definidas que es probable sean compartidas por los criminales que cometen un tipo particular de crimen. El perfil se puede usar para limitar el campo de sospechosos o evaluar la probabilidad de que un sospechoso en particular haya cometido el crimen.

La creación de perfiles por parte de la policía se ha enfrentado a una serie de connotaciones desafortunadas debido a la concentración de los medios de comunicación en el término al describir las prácticas discriminatorias de la policía. En la mente de algunos miembros del público, todos los perfiles creados por la policía están asociados con perfiles *raciales*, lo

que a su vez ha venido a significar tratar a las personas como sospechosos criminales basándose meramente en su origen étnico o la apariencia de un origen étnico.

Por otra parte, en algunos círculos la efectividad percibida de la creación de perfiles ha alcanzado proporciones casi místicas. Películas como *El Silencio de los Corderos* de Jonathan Demme y *Cazador de Hombres* de Michael Mann han glorificado y exaltado el papel del creador de perfiles criminales, haciendo parecer que la creación de perfiles es algo casi cercano a lo mágico. Los creadores de perfiles en las películas son capaces de echarle una mirada a la escena del crimen y describir infaliblemente las características físicas del criminal y sus antecedentes.

No resulta tan fácil ni es tan así en la vida real, pero la creación de perfiles es una valiosa herramienta que le puede dar a los investigadores muchas pistas acerca de la persona que comete un crimen específico o series de crímenes. Sin embargo, es importante comprender que un perfil – aún uno construido por los mejores creadores de perfiles en el campo – sólo proporcionará una idea del *tipo* general de persona que cometió el crimen; un perfil *no* apuntará a una persona específica como sospechosa. Aunque buenos perfiles pueden aproximarse increíblemente a la ocupación del infractor, a los antecedentes educacionales, a las experiencias en su niñez, al estado civil, e incluso a su apariencia física general, siempre existirán muchos individuos que encajen en un perfil dado.

La creación de perfiles es sólo una herramienta entre muchas para conducir una investigación y construir un caso criminal. Un perfil *no* es evidencia, sino un punto de partida que puede ayudar a los investigadores a concentrarse en el o los sospechosos correctos y comenzar a obtener evidencia.

Nota

La creación de perfiles ha sido usada por la policía desde hace ya algún tiempo. Aunque a menudo se le acredita su “invención” al FBI, una forma menos sofisticada de crear perfiles y de reconstruir el crimen fue utilizada en el caso de Jack, el Destripador, en Londres en los años 1880. Para efectuar un estudio histórico de la creación de perfiles, véase el artículo: *Creación de perfiles criminales: Cómo comenzó y cómo lo usa Wayne Petherick*, localizado en el sitio Web de la Biblioteca del Crimen www.crimelibrary.com/criminology/criminalprofiling2.

Comprendiendo Cómo Funciona la Creación de Perfiles

La creación de perfiles es considerada por algunas personas – incluyendo aún a algunos oficiales de la policía – una exótica táctica investigativa de “último recurso”. Esos escépticos identifican el trabajo del creador de perfiles con el de los “parasicólogos forenses” que ofrecen sus poderes clarividentes para ayudar a solucionar crímenes. La creación de perfiles, sin embargo, es un proceso basado en la recopilación de información y en el análisis de la misma con la aplicación de la lógica.

Los creadores de perfiles infieren la personalidad del criminal y otras características basándose en los siguientes indicadores:

- Sus observaciones del crimen y de la escena del crimen
- El testimonio de testigos y víctimas
- Su conocimiento de psicología humana y psicología criminal
- La existencia de patrones y correlaciones entre los diferentes crímenes

John E. Douglas, ex creador de perfiles del FBI, dice en su libro *Cazador de Mentas*, “La conducta refleja la personalidad”. Los creadores de perfiles examinan la conducta del criminal y hacen una descripción de su personalidad.

A menudo, una parte importante del trabajo del creador de perfiles la constituye el comparar los hechos y las impresiones de un grupo de crímenes y determinar si es probable que los crímenes hayan sido cometidos por la misma persona. Los criminales repetidos son, para sorpresa de nadie, criaturas de hábitos, excepto por el hecho de que continúan cometiendo crímenes. Ellos tienden a hacer las cosas de la misma forma cada vez, lo que se conoce en el argot popular como el *modus operandi* del criminal (método de operación o MO). Las conductas que un criminal repite en cada escena del crimen, especialmente si la conducta parece satisfacer una necesidad psicológica (lo opuesto a ser una cuestión de sentido práctico) son también conocidas como la *firma* del criminal. Los criminales cibernéticos, al igual que otros criminales, a veces se regalan por sus modus operandis o firmas.

Existen dos métodos básicos de crear perfiles: el inducido y el deductivo. Cada uno está basado en un método particular de razonamiento o de lógica. Generalmente, el *razonamiento inducido* funciona de lo específico a lo general, mientras que el *razonamiento deductivo* funciona de lo más general a lo más específico.

Con el razonamiento inducido, Usted comienza con observaciones o información, después propone una teoría que aplica a nuevas circunstancias. Con el razonamiento deductivo, usted comienza con una premisa y después propone conclusiones específicas basadas en la premisa. Para comprenderlo mejor, véase los ejercicios de razonamiento inducido y deductivo de la Universidad del estado de San José en www.sjsu.edu/depts/itl/graphics/induc/ind-ded.html.

Creando perfiles con el Razonamiento Inductivo

El método de *creación de perfiles con el razonamiento inductivo* se basa en estadísticas y en un análisis comparativo para crear un perfil. Se recopila información acerca de los criminales que han cometido un tipo específico de crimen. La información puede tomar la forma de estudios formales de criminales convictos, de observación informal de criminales conocidos, entrevistas clínicas u otras a criminales que se conoce han cometido ciertos crímenes y de datos ya disponibles en bases de datos.

Al analizar los datos y establecer correlaciones, el creador de perfiles infiere que las características comunes a un número estadísticamente significativo de infractores que cometen un tipo particular de crimen son aplicables a otros criminales que cometen el mismo tipo de crimen. El modelo de creación de perfiles con el razonamiento inductivo tiende a producir resultados no específicos y generalizados.

Creando perfiles con el Razonamiento Deductivo

Una deducción es un argumento en el cual, ciertas cosas han sido establecidas, otras diferentes vienen necesariamente a través de estas. – Aristóteles

El método de *creación de perfiles con el razonamiento deductivo* se basa en la aplicación del razonamiento deductivo a la evidencia observable. Los investigadores recopilan información general sobre el crimen y los creadores de perfiles arriban a conclusiones específicas sobre las características del criminal, basándose en la experiencia, el conocimiento y el pensamiento crítico de los creadores de perfiles. La victimología, la escena del crimen, la evidencia forense y el análisis conductual son todos componentes del proceso deductivo.

El método deductivo cuenta con varios pasos bien diferenciados:

1. *Se plantea un problema.*
2. *Se recopila información.*
3. *Se formula una hipótesis de trabajo.*
4. *Se comprueba la hipótesis.*
5. *Se evalúan los resultados de la comprobación.*
6. *Se llega a una o más conclusiones.*

Las hipótesis se pueden comprobar utilizando el *pensamiento de si/entonces*. Podríamos comenzar con una hipótesis como “Los hackers son mayormente inofensivos.” Si nuestra hipótesis es correcta, los datos deberían mostrar que la gran mayoría de los incidentes de hackeo no causan pérdidas monetarias u otros daños a las compañías o a los individuos cuyos sistemas son hackeados. Encontrar uno o dos incidentes de pérdidas o daños no desaprobaría la hipótesis – pero si encontramos una gran cantidad de casos que son inconsistentes con nuestra hipótesis, podemos considerarla no válida. Nuestra conclusión, entonces, podría ser la opuesta a la hipótesis con la que comenzamos: los hackers *no* son “mayormente inofensivos”.

Los creadores de perfiles que emplean el método deductivo, a menudo, mencionan que el éxito depende de la capacidad de “entrar en la mente” del criminal, de pensar como piensa el criminal para entender sus motivos y predecir sus futuras acciones. Los mejores creadores de perfiles deductivos podrían afirmar que ellos se guían por la intuición o que usan el sentido común para crear los perfiles. Sin embargo, un estudio profundo generalmente revela que el “sentido común” al que ellos se refieren es un proceso de pensamiento lógico aplicado a la evidencia contundente que han obtenido y observado. Este proceso de pensamiento puede tener lugar de manera subconsciente, conduciéndolos a

los “sentimientos intuitivos” que no salen realmente de la nada y que son, por el contrario, el resultado de largas horas o días de procesamiento subconsciente de información.

A diferencia del proceso inductivo, que se basa en datos estadísticos (y que puede ser procesado por una computadora al igual o mejor que por un ser humano), el razonamiento deductivo requiere una inteligencia que las máquinas todavía no poseen. El pensamiento deductivo no es sólo una aptitud, es un talento con el que algunas personas parecen haber nacido y que otras nunca logran aprender. Los detectives más talentosos tienden a ser maestros de razonamiento deductivo. Más adelante en este capítulo, en la sección “Comprendiendo a los investigadores cibernéticos” analizaremos los requisitos y las características de un buen investigador.

Nota

Quizás uno de los más famosos defensores del razonamiento deductivo fue Sir Arthur Conan Doyle, el escritor y físico escocés que creó al personaje de Sherlock Holmes en los años 1880. Doyle resumió el método deductivo de forma bastante sucinta: “Es una antigua máxima que tengo que cuando Usted ha excluido lo imposible, lo que queda, aunque improbable, tiene que ser la verdad.”

Usos del Perfil Criminal

Un perfil no puede, por sí solo, resolver un caso criminal. Sin embargo, el perfil se puede usar para varios propósitos:

- Para limitar el espectro de sospechosos
- Para vincular crímenes afines
- Para darle a los investigadores pistas valiosas a seguir

Aunque el perfil no constituye por sí mismo evidencia de la culpabilidad de un sospechoso en particular, puede ser usado en la corte conjuntamente con el testimonio de los testigos expertos. Los *testigos expertos*, a diferencia de otros testigos en un caso penal, están autorizados a dar opiniones. Un testigo experto puede hacer referencia a un perfil criminal como la base de una opinión de que existe una alta probabilidad de un vínculo entre un sospechoso en particular y una escena del crimen en particular. Analizaremos más detalladamente a los testigos expertos y sus testimonios en el Capítulo 11, “Construyendo el Caso de Crimen Cibernético”.

La creación de perfiles basada en la recopilación de una gran cantidad de datos sobre el crimen cibernético y sobre aquellos que lo cometen puede servir para otro propósito. Cuando la imagen de un criminal cibernético típico comienza a entrar en el enfoque, podríamos vernos forzados a reexaminar nuestras propias concepciones erróneas sobre los criminales cibernéticos basadas en mitos de los medios de comunicación y unos cuantos casos anecdóticos.

Reexaminando los Mitos y las Concepciones Erróneas sobre los Criminales Cibernéticos

Películas como *Juegos de Guerra* y *Hackers* nos dieron la imagen hollywoodense del criminal cibernético, una que tiende a ser simplificada y romantizada. En aquellas películas, los hackers eran todos genios incomprendidos con corazones de oro que sólo están tratando de salvar al mundo, a pesar de la interferencia del gran gobierno malo. Las noticias, por otra parte, a menudo exageran en la dirección opuesta. Ellos pintan a cualquiera que crea en la distribución de softwares de fuente abierta como un pirata peligroso determinado a socavar los cimientos de nuestra sociedad capitalista. La verdad, como es usual, se encuentra en algún lugar entre estos dos extremos.

Ahora que el acceso a Internet es una actividad básica, la mayoría de los miembros del público general ha escuchado sobre el crimen cibernético y muchos sostienen opiniones en los extremos del espectro. Algunas de las concepciones erróneas más comunes en relación con los criminales cibernéticos incluyen:

- Todos los criminales cibernéticos son “abelarditos” – brillantes, pero socialmente ineptos.
- Todos los criminales cibernéticos tienen un muy alto coeficiente de inteligencia y un gran conocimiento técnico.
- Todos los criminales cibernéticos son del sexo masculino, generalmente adolescentes.
- Todos los jóvenes adolescentes con computadoras son peligrosos criminales cibernéticos.
- Los criminales cibernéticos no son “verdaderos” criminales porque no operan en el “mundo real”.
- Los criminales cibernéticos nunca son violentos.
- Todos los criminales cibernéticos encajan perfectamente en un perfil.

La mayoría de estas concepciones erróneas están basadas en estereotipos. ¿Podríamos decir que de eso se trata la creación de perfiles, de estereotipar? Qué es un estereotipo, en resumidas cuentas? El diccionario define el término como “una imagen o idea estandarizada y excesivamente simplificada que tiene una persona o un grupo de personas. La clave aquí (y la diferencia entre un estereotipo y un perfil) es *la simplificación excesiva*. Un perfil criminal es complejo y se basa en datos contundentes. Un estereotipo es un recurso que le permite a Usted evitar la recopilación de datos contundentes y aplicar un hecho “conocido” (o una declaración ampliamente aceptada como tal) a situaciones individuales.

¿Están siempre errados los estereotipos? Por supuesto que no. Si no hubiese algo de verdad en una creencia, al menos algunas veces, nunca se convertiría en un estereotipo. El peligro de confiarse en estereotipos –especialmente en el contexto de la investigación de crímenes y la aplicación de las leyes – es que dejan ciego al investigador y cierran su mente ante todas las posibilidades. Los criminales habilidosos pueden sacar ventaja de esos estereotipos y literalmente “huir con el asesinato” (y crímenes menores) sencillamente por no encajar en el conocido estereotipo.

En la escena...

¿Cómo y Por Qué Estereotipamos?

La palabra *estereotipo* se deriva del proceso de crear platos gravados en metal para impresión. Una vez creado el plato, se “pone” la imagen y no puede ser fácilmente cambiada. Por consiguiente, la palabra se convirtió en una descripción de la “imagen puesta” o una opinión que las personas aplican a toda una categoría de personas.

A menudo los estereotipos contienen una pizca de verdad; las mujeres sí tienden a ser más emocionales que los hombres; los asiáticos sí practican más las artes marciales que los occidentales; los ricos son diferentes a Usted, a mí y a Ernest Hemingway (ellos tienen más dinero). El peligro de los estereotipos es que estos proporcionan una manera “rápida y sucia” – y a menudo engañosa e imprecisa – de juzgar a las personas que no conocemos.

Estereotipar es un “atajo” que tenemos a mano y el cerebro humano se siente atraído por él. Todos nosotros basamos algunas de nuestras creencias en estereotipos; cuando simplemente no tenemos suficiente información para formarnos una opinión, tendemos a dar por sentado lo que hemos escuchado de otros, leído en libros o visto en la televisión. Los medios de comunicación son uno de los más grandes perpetuadores de los estereotipos. Muchas comedias se basan en estereotipos comunes. Esto no persigue necesariamente una intención malvada. Cuando Usted tiene que contar una historia en el espacio de una situación cómica de media hora o en una película de dos horas, los atajos se convierten en una necesidad. Sin embargo, mientras más se repite un estereotipo en particular, hay más probabilidades de que creamos en él.

En el sitio www.psc-cfp.gc.ca/publications/monogra/mono3_e.htm se encuentra disponible una excelente y detallada discusión sobre los estereotipos y cómo estos se utilizan en la interacción social.

Observemos de cerca cada una de las concepciones erróneas de nuestra lista y analicemos cómo surge cada una y por qué son generalmente suposiciones imprecisas.

Todos los Criminales Cibernéticos son “Abelarditos” – Brillantes, pero Socialmente Ineptos.

Como sucede con muchas concepciones erróneas, esta surgió de un pasado en el que era más cierta de lo que es hoy día. Retomando el análisis histórico del Capítulo 2 sobre los primeros tiempos de las computadoras y la interconexión, pocas personas comunes tenían acceso a los gigantescos sistemas de unidad central que además eran costosos y nada cómodos para los usuarios y que se definieron con la palabra *computadora*.

¿Quiénes sí tenían acceso? Los “tipos científicos” en lugares como el MIT. Estos eran los hombres con el corte de los pinchos y reglas de cálculo en sus bolsillos. El trabajo con las primeras computadoras requería grandes aptitudes matemáticas. Entonces no existían “usuarios” de computadoras. Si Usted quería interactuar con la máquina, necesitaba ser un programador. La programación era un proceso meticuloso que requería paciencia y la

voluntad de dedicar enormes cantidades de su tiempo a codificar. No propiciaba el cultivar oportunidades para aparecer en las páginas de sociedad de los periódicos. Cuando salía al mundo por la noche (*si salía*), ¿qué tenía para hablar después de pasar sus días encerrado con un grupo de tubos al vacío, estudiando minuciosamente listados de 1 y 0? No mucho que otros pudieran entender o interesarle.

La palabra *abelardito* tiene un par de significados diferentes y aún más connotaciones. El *Diccionario Encarta del 2001* de la Microsoft lo define como “un entusiasta decidido cuyo interés se considera demasiado técnico o científico y quien parece enfrascarse obsesivamente en él”. Esta es una acertada descripción de una gran proporción de los aficionados a las computadoras de los años 50, 60 y 70. Hoy día, sin embargo, las computadoras son casi omnipresentes. Las aptitudes requeridas para usar la Net para propósitos maliciosos son mucho menos complejas de lo que solían ser. Todavía algunas personas encajan en el estereotipo del “abelardito”, pero muchos de los criminales cibernéticos actuales – especialmente los estafadores y los criminales sexualmente motivados que utilizan Internet para encontrar víctimas – son amables y encantadores y tienen aptitudes sociales altamente desarrolladas.

En la escena....

Asesino Cibernético en Serie

En el año 2000, un ciudadano de Kansas nombrado John Robinson fue arrestado por asalto sexual y se convirtió en un sospechoso de los asesinatos de varias mujeres en un período de 15 años. Lo que hizo a este caso único fue el método de conseguir a las víctimas: a través de salas de chateo en Internet, la mayoría de ellas dedicadas al sadomasoquismo. Aunque él tenía un expediente criminal (había sido previamente arrestado por robo y fraude) se presentaba a sus víctimas como un hombre de negocios profesional y rico. El juicio de Robinson por tres de sus asesinatos, el cual fue pospuesto en varias ocasiones, estaba programado para Septiembre del 2002. Para más información, véase www.mayhem.net/Crime/robinson.html.

Todos los Criminales Cibernéticos Tienen un Muy Alto Coeficiente de Inteligencia y un Gran Conocimiento Técnico

Nuevamente este es un estereotipo basado en hechos anticuados. Aquellos primeros expertos en matemáticas del MIT tendían a encajar en él, pero este tiene poca relevancia para el criminal cibernético actual. Entrar en línea ahora es tan fácil como apuntar con el ratón y hacer click. Aunque algunos crímenes cibernéticos – tales como escribir y distribuir nuevos virus o preparar ataques de intrusión contra redes altamente protegidas – requieren pericia técnica, muchos otros crímenes cibernéticos pueden ser (y son) cometidos por personas con un índice de inteligencia promedio o por debajo del promedio, con poco o ningún entrenamiento y aptitudes técnicas.

Las estafas cibernéticas pueden ser llevadas a cabo por cualquier persona capaz de enviar correos electrónicos o utilizar programas de chateo en Internet. El robo de datos es, a menudo, un simple asunto de arrastrar y soltar. Incluso los crímenes que dependen de

complejas explotaciones técnicas pueden ser realizados por hackers ineptos llamados *script kiddies*, que sólo usan el código escrito por otros para hacer daño. Cientos de sitios Web y grupos de noticias les proporcionan a los aspirantes a hackers, que no tienen ni idea desde el punto de vista tecnológico, esas herramientas pre-configuradas o automatizadas que se pueden emplear para crackear sistemas.

Para más información, véase el artículo *No Tema a la Segadora, Témale a los Script Kiddies* ubicado en el sitio Web About.com en <http://netsecurity.about.com/library/weekly/aa111600a.htm>.

Todos los Criminales Cibernéticos Son del Sexo Masculino, Generalmente Adolescentes

Este es un estereotipo doble. Presupone dos grupos: el de los criminales cibernéticos y el de las mujeres. La ciencia y la matemática en general y la computación en particular han sido tradicionalmente del dominio predominante del género masculino. Además, las estadísticas policiales muestran que hay más probabilidades de que los hombres cometan crímenes de cualquier tipo que las mujeres.

En la escena...

De los Script Kiddies a los Click Kiddies

Los script kiddies, quienes usan guiones escritos por otros para entrar a redes, crackear contraseñas, causar estragos o daños, tienen que tener, al menos, la suficiente habilidad técnica para introducir los comandos apropiados y ejecutar el guión. El fenómeno más reciente en la “involución del hackeo”, de acuerdo con el experto en seguridad David Rhoades, es el *click kiddie*, quien hackea sencillamente apuntando con el ratón y haciendo click, cortando y pegando. Esto se hizo posible gracias a sitios Web que hacen todo el trabajo por ellos. La excelente presentación de Rhoades sobre este tema, denominada *Hackeando para las Masas*, está disponible en línea en www.clickkiddie.net.

Sin embargo, las estadísticas también muestran que la brecha entre los géneros está disminuyendo. Alrededor de los finales de los años 90, los arrestos de mujeres constituían aproximadamente el 22% de todos los arrestos (con mujeres representando aproximadamente el 14% de los delincuentes violentos y alrededor del 29% de los delincuentes que cometían crímenes de propiedad), de acuerdo con el Buró de Estadísticas de Justicia del Departamento de Justicia de los Estados Unidos (www.ojp.usdoj.gov/bjs/crimoff.htm#women). La misma fuente indica que durante los años 90, el número de acusadas femeninas convictas por delitos graves en las cortes estatales se incrementó en más del doble comparado con la tasa de las condenas a hombres.

Los criminales de cuello blanco han sido tradicionalmente hombres – pero algunos expertos sostienen la teoría de que esto sucedió porque, hasta hace pocos años, las posiciones corporativas de alto nivel (que representan mejores oportunidades y tentaciones) eran ocupadas casi exclusivamente por hombres. Ahora que las mujeres están entrando en el mundo ejecutivo, están siendo arrestadas cada vez más delincuentes femeninas por

malversación, fraude y otros cargos por crímenes de cuello blanco. Para obtener información teórica y estadística, véase el artículo *Integridad en la Suite Corporativa: Previsores de Fraudes de Fémimas* por Collins, Muchinsky, Mundfrom y Collins en www.cj.msu.edu/~faculty/collinsintegrity.html.

La computación ya no es una profesión de sólo hombres. Las estadísticas del Departamento de Comercio de los Estados Unidos muestran que el 28.5% de los programadores ahora son mujeres. Aunque sólo un pequeño porcentaje de programadores (de cualquiera de los géneros) usa sus aptitudes para propósitos ilegales, las mujeres están adquiriendo definitivamente los medios para cometer crímenes por ordenador en mayor cuantía que antes.

Randy Nichols, presidente de la Comsec Security y profesor de Criptografía y Seguridad en la Universidad George Washington en Washington D.C. fue citado en el *Irish Times* en enero del año 2000: “A nivel mundial ni una sola mujer ha sido acusada de una felonía cometida con una computadora.” Sin embargo, han existido unas cuantas hackers femeninas renombradas. Para leer un artículo que contiene entrevistas con hackers femeninas discutiendo sobre el machismo en la comunidad de los hackers, véase el sitio Web de noticias ABC: <http://abcnews.go.com/sections/tech/dailynews/hackerwomen000602.html>.

En la escena....

La Profesión más Antigua del Mundo y la Primera Mujer Hacker Famosa

Una mujer que usaba el pseudónimo de Susan Thunder provino de un grupo de estrellas de rock y se convirtió en una phreaker de teléfonos y una hacker de computadoras. Se especializó en entrar a computadoras militares y eventualmente se asoció con los hackers de triste fama Ron y Kevin Mitnick. De hecho, a ella se le garantizó la inmunidad de no ser procesada por testificar en contra de ellos cuando fueron arrestados por sus propias actividades de hackeo.

Dado su historial, sólo era lógico que Susan se convertiría en una experta de lo que se conoce en el mundo del hackeo como *ingeniería social* – o sea, persuadir a usuarios autorizados para que revelen sus contraseñas. Dicen que a menudo lograba este objetivo manteniendo relaciones sexuales con el personal militar que tenía la información que ella buscaba.

El “típico perfil de criminal cibernético” ofrecido por Nichols – hombre, blanco, entre 19 y 30 años de edad – aún es válido para referirnos a la generalidad, pero cada año lo va siendo menos. Cada vez en mayor número, aquellos que cometen crímenes cibernéticos provienen de ambos géneros, de todas las razas y todos los grupos de edades.

Todos los Muchachos Adolescentes con Computadoras Son Criminales Cibernéticos Peligrosos

Una vez más, los medios de comunicación son los mayores responsables de este estereotipo. Es una creencia común en algunos lugares que todos los muchachos

adolescentes con una computadora pasan sus noches entrando a las computadoras del Departamento de Defensa en busca de códigos para disparar misiles nucleares. Esta imagen es reforzada por historias como la del reportaje en el verano del 2001 sobre una “sociedad secreta de anarquistas cibernéticos adolescentes” que derribó el sitio Web corporativo de Steve Gibson, un bien conocido experto en seguridad. Incluso el FBI no pudo ayudar a Gibson a encontrar a los hackers. (Para ver la historia íntegra vaya a <http://grc.com/dos/grcdos.htm>). Las redes televisivas ruedan documentales como el episodio *20/20 Monday* que caracterizaba a una “banda” en línea de hackers adolescentes llamada Infierno Global. Libros como *Los diarios del Hacker: Confesiones de Hackers Adolescentes* publicados por McGraw-Hill/Osborne Media perpetúan aún más el temor de muchas personas y la desconfianza hacia los adolescentes con computadoras.

Nadie puede discutir que los adolescentes que disfrutan cometiendo vandalismo contra sitios Web corporativos o tratando de penetrar sistemas computarizados del gobierno sean criminales, y tal conducta constituye un problema. Tampoco nadie puede discutir que los adolescentes llenos de rabia que abren fuego sobre sus compañeros de clase y profesores sean criminales peligrosos. Sin embargo, la mayoría de nosotros se da cuenta de que la mayor parte de los adolescentes – incluso los huraños, molestos y rebeldes – jamás adoptaría tal conducta extrema.

Lo mismo es válido para la gran mayoría de chicos adolescentes que tienen aptitudes para la computación. Lo más lejos que llegan usando sus computadoras para actividades ilegales es a descargar música o softwares para su propio uso personal mediante servicios como Napster o grupos de noticias “warez”. Aunque esta actividad podría resultar “peligrosa” para los balances finales de las compañías disqueras o de los vendedores de softwares, es un crimen del mismo nivel del de copiar canciones de un CD hacia una cinta para compartirla con un amigo. No está en la misma categoría de derribar los sistemas que ejecuta Wall Street o infiltrarse en las computadoras de los sistemas bancarios internacionales.

Los Criminales Cibernéticos No Son “Verdaderos” Criminales Porque No Operan en el “Mundo Real”

Muchos criminales cibernéticos creen en ese mito – o al menos lo utilizan para justificar y racionalizar su conducta. Incluso personas que detienen la actividad ilegal, a menudo, se comportan en línea de una manera en la que no hubieran pensado comportarse en sus “vidas reales” – mintiendo, engañando a sus esposas con relaciones “virtuales” o, simplemente, actuando de forma brusca y detestable.

Este fenómeno es tan corriente que toda una especialidad, la *ciber-psicología*, nació alrededor de este. Publicaciones como *Ciberpsicología & Comportamiento* (www.liebertpub.com/CPB/default1.asp), listas de correos profesionales y sitios Web como los del Centro de Estudios Computer-Mediated Communication (CMC) (www.december.com/cmc/study/center.html) han examinado la doble ilusión de irrealdad y anonimato que conduce a las personas a comportarse de forma diferente (y a veces mal) en el ciberespacio.

La tecnología como la del chateo en línea, las celdas para múltiples usuarios (MUDs) y los programas de realidad virtual han distorsionado la capacidad de algunos usuarios de distinguir entre qué es real y qué no lo es. Muchos usuarios de Internet, especialmente aquellos que son nuevos para el mundo en línea, parecen ver a las personas que están del otro lado de su línea de módem similares a personajes en un programa interactivo y ven las interacciones y relaciones que establecen con esas personas como un juego no más.

Como estas personas no están siendo “ellos mismos” en las interacciones en línea, quizás crean que nadie más lo es. De ahí que en sus mentes encuentren correcto inventar historias elaboradas y engaños que podrían cruzar la línea hasta llegar al fraude ilegal. Además, como pueden firmar utilizando pseudónimos (servicios en línea como AOL le permiten crear de manera fácil y rápida nuevos nombres de usuarios, haciéndolo incluso más tentador), ellos piensan que nadie sabe quiénes son o qué hacen en línea. Para esas personas que no tienen un control interno real en cuanto a valores éticos y morales de la persona y que se comportan “adecuadamente” sólo por temor a las consecuencias externas (desaprobación social o cárcel), este forum les proporciona una excusa para deshacerse de todas las inhibiciones. Si le adicionamos a esta evidencia anecdótica que muchos de los que frecuentan las salas de chateo disminuyen aún más sus inhibiciones ingiriendo alcohol mientras navegan por la Net, Usted tendrá la receta para el comportamiento antisocial.

Por supuesto, esta idea de que nada en línea es real y por lo tanto nada de lo que Usted haga allí “cuenta”, es una falacia. Pero es un viejo truco de los criminales despersonalizar a sus víctimas; verlas como algo menos que seres humanos reales les facilita el hacerles daño. Este auto-engaño se hace mucho más fácil en el ciberespacio, pues ellos nunca tienen que ver los rostros u oír las voces de sus víctimas; las personas con las que el criminal lidia pueden quedar convenientemente como sólo palabras en una pantalla de computadora.

Los Criminales Cibernéticos Nunca son Violentos

Como la Internet es un medio más virtual que físico, parece lógico asumir que aún siendo el crimen cibernético un crimen real, no es un crimen *violento*. Después de todo es la posibilidad de cometer sus crímenes desde lejos lo que atrae en primera instancia a muchos criminales a la Net

Es cierto que un gran porcentaje de los crímenes cibernéticos reportados son fraudes, robos y casos de acceso no autorizado. Sin embargo, es interesante destacar que el crimen cibernético reportado con mayor frecuencia en la base de datos Cybersnitch (www.cybersnitch.net) es la pornografía infantil, la que generalmente se clasifica como un crimen violento o potencialmente violento por dos razones: el daño hecho a los niños que son usados para tomar las fotografías y el potencial del material para incitar a los pedófilos a realizar sus fantasías con niños reales. Las intrusiones de hackers son el segundo tipo de crimen reportado con más frecuencia; el tercero es el acecho electrónico que también puede ser considerado un crimen violento, porque aterroriza a la víctima, y los acechadores cibernéticos son conocidos a menudo por continuar acechando a sus víctimas en la vida real.

Algunas personas podrían argüir que la pornografía infantil y el acecho cibernético no son en sí mismos crímenes físicamente violentos, pero resultaría difícil hacer tal afirmación de los depredadores que utilizan la Internet para encontrar gente vulnerable a las que puedan atraer hacia una reunión para violarlos, asaltarlos o matarlos. Además de estos delincuentes violentos que generalmente actúan solos, los terroristas que usan la Internet para recaudar dinero, planear sus actividades, reclutar nuevos miembros y comunicarse con los otros son criminales violentos de la especie más peligrosa.

Los criminales cibernéticos, como los criminales en general, comprenden una línea continua que va desde el niño cuya curiosidad le provoca tratar de hackear la red de alguien sólo para ver si se puede hacer, sin intención de hacer daño, hasta el hombre que llevó a cabo el ataque al World Trade Center en la ciudad de Nueva York. Esta consideración nos lleva a nuestra última concepción errónea.

Todos los Criminales Cibernéticos Encajan Perfectamente en un Perfil

Podríamos construir un perfil del tipo de persona que comete un crimen cibernético en particular, pero es imposible crear un perfil donde encajen todos los criminales cibernéticos, así como es imposible hacer un perfil exacto de todos los violadores de las leyes del tránsito. El que excede los límites de velocidad de forma casual es probable que tenga una personalidad diferente y diferentes motivaciones a la del conductor ebrio habitual o a la del motorista indignado que usa su vehículo como un arma para tumbar a los transeúntes. Así mismo, el estafador cibernético es una criatura completamente diferente al acechador cibernético quien, por su parte, no se parece al típico hacker.

Incluso dentro de una categoría particular de crimen cibernético, la fisiología, la psicología y las motivaciones de cada criminal son diferentes. Sin embargo, algunas similitudes nos permiten pintar un cuadro bien amplio del criminal cibernético “típico”. Debemos recordar, sin embargo, que para que un perfil sea útil en nuestras investigaciones, debe estar basado en los hechos de un caso individual.

Construyendo un Perfil del Típico Criminal Cibernético

Como un primer paso en la construcción de un perfil (y recuerden que este es *sólo* el primer paso) podemos observar algunas generalidades que la mayoría de las veces aplican a los criminales cibernéticos en todas las categorías. Es importante ver estas características como *probabilidades*, no como reglas absolutas. Existen excepciones para cada caso. Dicho esto, la mayoría de los criminales cibernéticos presentan al menos algunas de estas características:

- **Al menos un mínimo de habilidades técnicas** Esta suposición se basa en el sentido común. Aunque, como mencionamos anteriormente, resulta más fácil que nunca conectarse a Internet sin ser un as en computación, la mayoría de las personas que usan Internet para propósitos ilegales son capaces de encontrar el camino en el ciberespacio sin mucha ayuda. Las personas generalmente utilizan las herramientas con las que se sienten cómodos,

especialmente al realizar actividades de alto riesgo como cometer un crimen. Para usar la Internet con el fin de llevar a cabo un acto planeado como lo es un crimen, Usted debe ser capaz de realizar tareas básicas como enviar un e-mail, navegar por la Web o registrarse en una línea de chateo. Algunos crímenes requieren de mucha más pericia. El criminal cibernético típico no es una persona que sienta fobia por las computadoras o que se valide en la Net por primera vez.

▪ **Indiferencia ante la ley o un sentimiento de estar por encima o más allá de la ley** Pocas personas, incluyendo a los criminales, piensan de sí mismos que son “malos”. La mayoría de los infractores de las leyes, aunque no todos, justifican sus acciones viendo a las leyes (al menos las que infringen) como malas. Los criminales cibernéticos, como otros criminales habituales, a menudo, expresan indiferencia o desdén por las leyes. Ellos no son del tipo de personas que creen que Usted debe cumplir con la ley sólo *porque* es la ley. En vez de ello, tienden a creer que es justo infringir las leyes que ellos consideran irracionales. En algunos casos, ellos sienten que ellos, por sus aptitudes especiales, inteligencia, posiciones o circunstancias están por encima de las leyes. Por ejemplo, un empleado que se refiere al ladrón común como un pillo podría creer que malversar dinero de su empleador es correcto, porque la compañía paga muy poco y sobrecarga con trabajo a sus empleados. Otros criminales cibernéticos creen que las leyes sencillamente no aplican en el ciberespacio, retornando al aspecto de “irrealidad” que mencionamos anteriormente.

▪ **Una vida activa de fantasías** Muchos criminales cibernéticos utilizan la Internet como un canalizador de sus fantasías. A menudo, ellos construyen nuevos personajes que usan en línea – con ambos objetivos: ocultar sus verdaderas identidades y evitar ser detectados, y porque disfrutan “representar el papel” de alguien diferente a ellos mismos. Los estafadores pueden inventar esquemas elaborados basados en sus fantasías. Los acechadores erigen fantasías alrededor de sus víctimas. Los pornógrafos infantiles lidian con fantasías sexuales. Los hackers sueñan con “hackear el mundo”, tomando el control sobre otras personas al controlar sus sistemas computarizados. Esta se relaciona con la siguiente característica común de los criminales cibernéticos.

▪ **Un “fanático del control” y/o la naturaleza de asumir riesgos** Los criminales, a veces, consumen más energías para una retribución, desde el punto de vista práctico, menor, en cometer crímenes de la que consumirían si dirigieran sus esfuerzos a realizar un trabajo socialmente más aceptable. ¿Por qué entonces adoptan un comportamiento de tan alto riesgo? Para algunos es el riesgo de ser atrapado lo emocionante de hacer algo prohibido, lo que hace atractiva la vida del crimen. Para otros, es el sentido de control que perciben al manipular o burlar a otros. Aunque estas dos características parecen entrar en conflicto, pueden existir simultáneamente en la misma persona. El elemento de asumir riesgos proporciona la “prisa”, mientras que escapar una vez más de la detección hace que el criminal cibernético se sienta seguro y controlado.

▪ **Motivaciones fuertes – pero las motivaciones podrían ser totalmente diferentes** Como hemos visto, toma tiempo y energía cometer la mayoría de los crímenes. La comisión de crímenes cibernéticos exige de un esfuerzo extra y de un cierto número de habilidades. La mayoría de los criminales cibernéticos están fuertemente motivados, pero las motivaciones van desde el simple deseo de divertirse hasta la necesidad o el deseo de

obtener dinero, impulsos emocionales o sexuales, motivos políticos o compulsiones oscuras causadas por enfermedades mentales o condiciones psiquiátricas. El discernir la motivación para un crimen en particular es un aspecto importante en la construcción de un perfil útil sobre el criminal que lo cometió.

Reconociendo las Motivaciones del Criminal

Estas son las palabras de un instructor de academia de policías al preguntársele, ¿“Por qué los criminales cometen crímenes? Porque son criminales”. Ojala fuese tan simple. Las personas violan las leyes por muchas razones diferentes. Algunas de esas razones podrían incluso parecer razonables como las de la madre que fue despedida del trabajo y que no tiene dinero y roba comida de bebé para alimentar a su niño. Por otra parte, muchas personas en situaciones desesperadas encuentran soluciones a sus problemas que no interfieren con el cumplimiento de la ley. Algunos criminales cibernéticos – por ejemplo, el leal empleado de mucho tiempo que de repente malversa fondos de las compañía para pagar cuentas médicas inesperadas o salir relativamente de problemas – podría hacerlo también por causa de la desesperación. Sin embargo, la mayoría de ellos son impulsados por motivos muchísimo menos nobles: la codicia, el enojo, la lujuria o sencillamente el aburrimiento.

¿Por qué importan los motivos? En muchas jurisdicciones, un elemento importante para probar la culpabilidad es demostrar que el acusado posee todos los componentes del así llamado *triángulo del crimen*: los medios (el modo de cometer el crimen), el motivo (una razón para hacerlo) y la oportunidad (estar en el lugar correcto en el momento correcto para cometer el crimen). Por lo tanto, comprender el motivo del criminal resulta útil en dos puntos de la investigación: cuando estamos creando un perfil para ayudarnos a identificar al sospechoso correcto y después, cuando presentamos el caso en contra de nuestro sospechoso.

Los motivos comunes para cometer crímenes cibernéticos incluyen:

- Sólo por diversión
- Ganancia monetaria
- Enojo, venganza y otras necesidades emocionales
- Motivos políticos
- Impulsos sexuales
- Padecimientos psiquiátricos serios

Vamos a examinar cada uno de estos motivos de forma individual y vean cómo cada uno de ellos puede aplicar al criminal cibernético.

Sólo por Diversión

Los hackers jóvenes son los criminales cibernéticos con más probabilidades de caer en esta categoría. De acuerdo con J. Maxwell en el boletín informativo *Auditoría del Procesamiento de Datos Electrónicos, Control y Seguridad* (citado en

<http://faculty.ncwc.edu/toconnor/315/315lec12.htm>), los hackers que lo hacen por diversión pueden dividirse en varias categorías:

- *Los Pioneros*, que están fascinados por la tecnología. Ellos disfrutan aprender cómo los sistemas funcionan a través de un proceso de prueba y error y hackean como una experiencia de aprendizaje.
- *“Los Pícaros”*, hackers traviesos que no tienen intención de hacer ningún daño. Este es el tipo que podría hackear un sitio Web y dejar un mensaje inocuo como “J.B. estuvo aquí”.
- *Los Exploradores*, que se deleitan “yendo a donde ningún hacker ha ido antes” – o, al menos, adonde ellos mismos no han estado nunca. Su curiosidad los lleva a entrar en redes sólo para ver qué hay.
- *Los jugadores de juegos* que ven el hackeo de sistemas como un juego, enfrentándose a las medidas de seguridad de la red y motivados por el deseo de “ganar” al entrar en ellas.

Otro de los tipos de personalidad de hackers mencionado por Maxwell es *el adicto*, que podría comenzar como cualquiera de esos tipos de carácter, pero que se vuelve psicológicamente dependiente de la actividad. A ese punto, el pionero, el pícaro, el explorador o el jugador ya no estaría hackeando realmente sólo por diversión, sino porque él o ella *necesita* hackear para sentirse bien o normal.

La característica distintiva del hacker “por diversión” es el disfrute. A diferencia de otros criminales cibernéticos que utilizan la computadora e Internet como el medio para un objetivo, para estos hackers, hackear es el objetivo en sí mismo. Ellos podrían ver la computadora como un juguete y toda la Internet como su campo de juego.

Estos hackers “por diversión” no obtienen ningún beneficio práctico o financiero de su hackeo; de hecho, este pudiera ser un hobby costoso para aquellos que actualizan continuamente sus propios sistemas de computadora con el objetivo de hacer que la experiencia de hackear sea más rápida y más satisfactoria.

Ganancia Monetaria

Si el amor al dinero es la raíz de todo mal, no es una sorpresa que muchos crímenes cibernéticos – como muchos crímenes fuera de línea – estén motivados por el deseo de obtener beneficios financieros. “Hackear por dólares” puede cubrir muchos delitos diferentes, incluyendo la malversación, el espionaje corporativo y la venta de los servicios de hackeo de uno a otros que tienen motivos monetarios o no monetarios (el “hacker por contrato”).

La mayoría de los estafadores cibernéticos lo hacen por dinero. Su motivo podría ser obtener dinero en sus propias manos o propiedades o servicios sin tener que pagar.

Los criminales cibernéticos motivados por dinero vienen en todos los “sabores” – masculinos, femeninos, jóvenes, viejos, adinerados, pobres o de clase media. Algunos nunca pasaron el preuniversitario, otros tienen títulos avanzados. Los *criminales de cuello blanco* (malversadores, ladrones de secretos comerciales, etc.) tienden a ser profesionales

educados, a menudo en el medio de un estancamiento de sus carreras o de un estado de agotamiento. *Los estafadores* son en general sociables y encantadores, capaces de persuadir a otros para que hagan lo que ellos quieren. *Los hackers por contrato* son, generalmente, técnicos de alto nivel quienes, a su entender, sólo “están haciendo un trabajo”.

Enojo, Venganza y Otras Necesidades Emocionales

El dinero no es el único motivo o, incluso, el más fuerte para cometer crímenes. Muchos delitos criminales, especialmente aquellos que involucran violencia (y amenaza de violencia) o destrucción de propiedad, son cometidos por motivaciones emocionales: enojo, furia o venganza por agravios reales o imaginados.

El enojo puede conducir a las personas a hacer cosas que de otra forma no harían. Los psicólogos afirman que tratar con una persona que esté muy molesta, herida o emocionalmente angustiada es como lidiar con alguien que está mentalmente disturbado o bajo la influencia de alcohol o drogas. En realidad, las emociones fuertes causan un desprendimiento de adrenalina que sí actúa sobre el cuerpo y el cerebro como una droga, trayendo como resultado cambios fisiológicos y psicológicos (fuerza física desmedida, una mayor actitud alerta, una “visión de túnel”, o una obsesión inmediata con el problema). Una persona muy molesta es – temporalmente, al menos- una persona emocionalmente disturbada.

Los criminales cibernéticos que actúan por enojo podrían ser amantes o esposos rechazados, empleados despedidos, socios de negocios que sienten que han sido engañados o estafados, u otros que creen que les han hecho algo muy malo a ellos o a alguien por quien se preocupan. Sus crímenes van desde amenazas terroristas (por ejemplo, correos electrónicos amenazando con asaltar o matar a alguien) hasta ultrajar un sitio Web de una compañía con profanidades o desmantelar la red de una organización con ataques DoS o virus electrónicos.

La venganza difiere del enojo en que, generalmente, es mejor planeada y no es una respuesta inmediata. Esto lo hace un acto menos emocional y, por consiguiente, pudiera ser más peligroso, porque el criminal cibernético motivado por la venganza tiene más tiempo de pensar en el plan, cubrir sus huellas y reducir la probabilidad de ser capturado.

Casi todo el mundo, bajo una presión lo suficientemente fuerte, es capaz de arremeter contra alguien cuando está furioso. Por lo tanto, el criminal cibernético motivado por el enojo puede ser alguien que normalmente no comete actividades criminales. El crimen podría parecer no tener carácter alguno. Tal como cuando un investigador pregunta en el caso de un crimen motivado por dinero: ¿“Quién podía beneficiarse desde el punto de vista financiero?”, el investigador debería enfocar un crimen que aparenta estar motivado por enojo con la pregunta: ¿“Quién ha sido lastimado o es cercano a alguien que ha sido lastimado?”

El enojo y la venganza no son los únicos motivos que involucran emociones. Los criminales cibernéticos cometen crímenes por satisfacer otras necesidades emocionales y psicológicas. Por ejemplo, los hackers podrían entrar en sistemas protegidos para probarse a sí mismos ante sus amigos, para obtener un sentido de pertenencia al grupo. De hecho, los hackers a veces cometen actos en grupos que no cometerían si estuvieran solos. La “mentalidad de grupo” (o de *pandilla* en casos extremos) es un fenómeno con el que los psicólogos están familiarizados y del que está consciente la mayoría de los oficiales del orden. Grandes grupos pueden asumir personalidades de sus propios miembros y convertirse en la suma de sus partes. Los hackers podrían incitarse unos a otros, animándose entre ellos a ir más lejos sin que nadie quiera ser el primero en decir “no” y perder su estatus ante los ojos de sus coetáneos.

Los hackers también cometen crímenes para atraer la atención. Esto es especialmente real en los hackers adolescentes que quieren avergonzar a sus familias o simplemente hacer que los miembros de la familia o las figuras con autoridad los noten.

Otra motivación emocional para el hackeo es la lealtad a un amigo o el deseo de “ayudar” a alguien – por ejemplo, el hacker del preuniversitario que no quiere que su novia suspenda Cálculo y tenga que ir a una escuela de verano, de modo que entra al sistema computarizado de la escuela y cambia su nota colocando una C en lugar de una F.

Motivos políticos

Los criminales cibernéticos motivados por la política incluyen a miembros de grupos extremistas y radicales de ambos lados del espectro político que utilizan la Internet para divulgar propagandas, atacar sitios Web y redes de sus enemigos políticos, robar dinero para financiar sus actividades combativas o planear y coordinar sus crímenes en el “mundo real”.

Estos son algunos ejemplos:

- El caso de 1996 en que los “hacktivistas” se infiltraron en el Departamento de Justicia de los Estados Unidos a través de su sitio Web, borrando los ficheros Web del mismo y reemplazándolos por sus propias páginas de protesta contra la recientemente aprobada Ley de Decencia en las Comunicaciones.
- La cantidad de ultrajes a sitios Web que incluían el mensaje “Kevin libre” (en referencia a Kevin Mitnick, quien fuera arrestado por crímenes por ordenador) en 1998.
- Las “guerras cibernéticas” entre los hackers de Estados Unidos y China en el verano del año 2000, seguidas de disputas internacionales por el aterrizaje de un avión espía norteamericano en China.

Los criminales cibernéticos con motivaciones políticas van desde hackers relativamente benignos que sólo quieren hacer una declaración política hasta grupos terroristas organizados como Hezbollah, Hamas y al Qa’ida. *El terrorismo cibernético* se trata de usar la Internet y las habilidades de computación para afectar o derrumbar la infraestructura crítica y los servicios gubernamentales de un país. Aunque hasta el momento en que se está escribiendo este libro no se han implementado ataques de gran escala, los expertos en

seguridad advierten que algunas organizaciones terroristas están o estarán en condiciones de llevar a cabo tales ataques y podrían representar una enorme amenaza para el gobierno y las operaciones comerciales.

El criminal motivado por la política generalmente le dedica una gran parte del tiempo a su causa y a menudo (lo que no quiere decir que siempre) tiene un expediente criminal previo por delitos como traspaso criminal, disturbios y actividades similares. Los verdaderos terroristas son especialmente peligrosos porque están dispuestos a morir por su causa. A menudo también cuentan con amplias redes de personas con ideas afines a las que pueden llamar para que los ayuden en sus misiones y a ocultarlos de la policía.

Impulsos sexuales

El sexo es uno de los instintos más fuertes en todos los animales, incluyendo a los humanos. Los psicólogos y psiquiatras discuten sobre qué hace que los sentimientos sexuales normales se conviertan en pervertidos, pero no existe duda de que la desviación sexual (definida como el comportamiento sexual que está fuera de la norma o que rompe con las reglas de la sociedad) es común entre ciertos tipos de criminales.

No todos los comportamientos sexualmente desviados son ilegales o considerados dañinos. Sin embargo, cuando la excitación sexual viene asociada con violencia o con objetos de deseo inapropiados como los niños, puede resultar en una actividad criminal seriamente lastimosa.

Los criminales cibernéticos motivados por el sexo incluyen estos tipos:

- *Pedófilos pasivos*, quienes usan la Internet para acceder y descargar pornografía infantil y utilizan fotos e historias de niños teniendo sexo (generalmente con adultos) para alimentar sus propias fantasías. Aún si nunca realizan esas fantasías en la vida real, en los Estados Unidos y muchos otros países, resulta ilegal incluso poseer pornografía infantil en forma fotográfica. Esta ley se basa en la asunción de que los niños son dañados en la toma de las fotografías. Las leyes sobre pornografía generalmente aplican sólo a la representación visual; la palabra escrita (historias sobre sexo infantil) está protegida por La Primera Enmienda. La cuestión de la “pornografía infantil visual”, que utiliza imágenes de alta calidad generadas en computadoras en lugar de fotografías reales, es un tema de intenso debate. En abril de 2002, la Corte Suprema revocó las leyes federales convirtiendo en ilegal esta forma de pornografía infantil. En el momento en que fue escrito este libro, el Departamento de Justicia y los miembros del Congreso intentaban reescribir esas leyes de forma más específica, de modo que prohibieran la pornografía infantil virtual, que es indistinguible de la real, mientras aprueban la ley para que se convierta en un modelo Constitucional.

- *Pedófilos activos*, quienes usan la Internet para encontrar a sus víctimas. Estos criminales generalmente coleccionan también pornografía infantil, pero no se limitan a sus fantasías. A menudo entran a salas de chateo que son frecuentadas por niños y entablan con ellos conversaciones virtuales, tratando de ganarse su confianza y atraerlos a una reunión en persona. Entonces podrían violar a los niños o simplemente cortejarlos, prefiriendo seducirlos gradualmente hasta conducirlos hacia las relaciones sexuales. Como los niños de una cierta edad (la cual varía de un estado a otro) no son considerados capaces de consentir en tener sexo, la conducta sexual con un menor es todavía un crimen, incluso si el niño está de acuerdo. Generalmente el delito se define como *relaciones sexuales con un menor* o alguna categoría de *asalto sexual*.

- *Fanáticos del sadomasoquismo* o sexo sadomasoquista, quienes se excitan infligiendo dolor a otros (sádicos) o por que les inflijan dolor a ellos (masoquistas). Aunque el comportamiento sadomasoquista entre adultos que realizan este acto por su propia y libre voluntad no es considerado, por lo general, un crimen, algunos individuos sádicos buscan socios en la Internet y entonces llevan las actividades más allá del nivel con el que el socio contaba o con el que estuvo de acuerdo, hiriendo seriamente o, a veces, incluso, matando a sus víctimas.

- *Violadores en serie* que comienzan relaciones (heterosexuales u homosexuales) en línea y después invitan a sus víctimas a encontrarse en la vida real, sólo para violarlas. Los violadores en serie, a menudo, tienen problemas al tener sexo en una situación amorosa normal. Sólo logran excitarse cuando el sexo es violento y forzado. Los psicólogos consideran la violación como un crimen motivado por el enojo o por el poder más que un crimen motivado por el sexo, pero este es ciertamente un elemento importante sólo en calidad de “herramienta del crimen”.

- *Asesinos sexuales en serie*, quienes – al igual que los violadores en serie – navegan por salas de chateo y foros en Internet en busca de víctimas. La literatura psiquiátrica reconoce dos tipos de asesinos en serie: organizados y desorganizados. El *asesino organizado*, por lo general, tiene un alto coeficiente de inteligencia, es sociable y encantador y casi siempre casado o vive con una pareja. Los *asesinos desorganizados* son casi exactamente lo opuesto, su coeficiente de inteligencia es generalmente bajo y son solitarios socialmente inadecuados y están ansiosos durante la comisión del crimen. Los asesinos organizados tienden a ser muy controlados y nada emocionales y a menudo se diagnostican como antisociales (como era Ted Bundy, uno de los más famosos asesinos sexuales en serie del país). De hecho, los asesinos sexuales en serie, a pesar de la motivación sexual para sus crímenes, pertenecen a la próxima categoría de motivación: padecimiento psiquiátrico serio.

Padecimiento Psiquiátrico Serio

El comportamiento criminal no es, por sí mismo, un indicativo de padecimiento mental. Si lo fuese, quizás se pudiera tratar clínicamente. Sin embargo, algunos criminales son motivados a comportarse de modo ilegal y antisocial por padecer de condiciones

psiquiátricas, especialmente aquellas que se manifiestan con síntomas tales como la falta de control del impulso y la falta de inhibición, alucinaciones y delirios, paranoia, hiperactividad e incapacidad de concentrarse o posesión de problemas para comunicarse.

Personas que sufren de trastornos de la personalidad, esquizofrenia, trastorno afectivo bipolar, agresión, depresión, problemas de adaptación y trastornos sexuales tales como la parafilia son más propensos a tener un comportamiento criminal, de acuerdo con *Padecimientos Psiquiátricos Asociados con la Criminalidad*, de William H. Wilson, Dr. y Kathleen A. Trott, Dra. (www.emedicine.com/med/topic3485.htm). La conducta ilegal también puede ser producto de una psicosis inducida por el consumo de alcohol o drogas o de condiciones causadas por daños traumáticos al cerebro.

Podría resultar más fácil para tales personas ocultar su padecimiento mental en la comunidad en línea, donde no tienen que entrar en contacto físico con otros, que en el mundo real. El crimen cibernético motivado por padecimientos psiquiátricos puede resultar difícil de investigar y resolver, precisamente porque las motivaciones del criminal no parecen lógicas o racionales. Podemos comprender por qué un delincuente motivado por el dinero comete crímenes, aún cuando no aprobamos ese comportamiento. Sin embargo, podríamos no ser capaces de comprender con facilidad las acciones de una persona mentalmente enferma.

Reconociendo las Limitaciones del Análisis Estadístico

De acuerdo con el autor Samuel Clemens que escribió bajo el famoso pseudónimo de Mark Twain, “Existen tres tipos de mentiras: las mentiras, las malditas mentiras y las estadísticas”. Muchos miembros del público desconfían del análisis estadístico y de los argumentos basados en estadísticas y esto es correcto. Todo el que ha trabajado con datos estadísticos o ha seguido a los contendientes de una campaña política sabe que, durante la presentación, se pueden manipular los mismos hechos para apoyar conclusiones divergentes.

Los perfiles criminales se basan en las probabilidades. Las probabilidades se basan en patrones estadísticos que han sido discernidos durante el estudio de casos similares del pasado. Como hemos visto, la creación de perfiles puede ser una herramienta útil y los investigadores de crímenes cibernéticos – quienes enfrentan desafíos especiales debido a la complejidad y la naturaleza global de la Internet – necesitan todas las herramientas que puedan conseguir. Sin embargo, es importante recordar que un perfil cuidadosamente construido puede estar completamente errado. La investigación debe darle forma al perfil, el perfil nunca deberá darle forma a la investigación.

Clasificando por Categorías a los Criminales Cibernéticos

En el Capítulo 1, analizamos la importancia de clasificar por categorías a los crímenes cibernéticos. En la sección anterior, vimos una forma en que estos pudieran ser clasificados, basados en sus motivaciones para cometer crímenes. Existe otra forma de

clasificar a los infractores que usan la Internet: por el papel que juega la Internet en su actividad criminal. Este papel generalmente se divide en dos amplias categorías:

- Criminales que usan la Net como una herramienta del crimen
- Criminales que usan la Net incidentalmente al crimen

En las secciones siguientes, examinaremos las diferencias entre estas dos categorías. También observaremos una categoría especial del criminal cibernético: el que nunca ha realizado una actividad criminal en la “vida real”, pero que se convierte en criminal a través de una persona en línea.

Criminales que Usan la Net como una Herramienta del Crimen

Muchos tipos de crímenes cibernéticos dependen del uso de una red de computadoras para llevar a cabo el acto criminal. Esto no significa que este mismo delito no se pueda cometer sin computadoras y redes; significa que en este caso la red fue usada directamente para cometer el crimen.

Aquí tienen una analogía para facilitar la comprensión de este concepto: un asesinato se puede cometer utilizando varios métodos –una pistola, un cuchillo, un veneno, incluso un vehículo motor. Aunque el resultado final (la muerte de la víctima) es el mismo en todos los casos, el asesinato no se puede hacer de la misma manera si la herramienta es diferente. Asimismo, un malversador pudiera robar dinero de una compañía sin utilizar una red, pero lo haría de una forma diferente. Si el malversador sí usa una red para desviar fondos, la red es una herramienta de ese crimen.

Una red puede ser empleada como una herramienta del crimen por diferentes tipos de criminales cibernéticos. Una red es usada con más frecuencia como una herramienta por:

- Criminales de cuello blanco
- Estafadores cibernéticos
- Hackers, crackers y atacantes de redes

Criminales de Cuello Blanco

El término *criminal de cuello blanco* se deriva, por supuesto, de la imagen del oficinista o profesional que tradicionalmente viste atuendos de negocio (camisa blanca y corbata) para trabajar. Los crímenes de cuello blanco pueden incluir muchos delitos diferentes, tales como:

- Cambio de los registros en las computadoras de la compañía para darle al criminal un aumento de sueldo no autorizado o para eliminar o cambiar evaluaciones negativas del empleado o rellenar cuentas de gastos.
- Acceso y uso de información interna para adquirir acciones o garantías, lo que constituye una violación a lo establecido por la SEC (Comisión de Valores de los Estados Unidos).

- Venta de información de la compañía a extraños, uso de información interna para obtener sobornos de los clientes, socios del negocio o competidores, o uso de información confidencial para propósitos de chantaje.
- Manipulación de cuentas electrónicas para apropiarse del dinero de los clientes o de la compañía o de propiedades para sí mismo.
- Falsificar los libros de la compañía o los estados financieros para darle información falsa a los acreedores, inversionistas, Impuestos Internos, auditores internos, etc. – a menudo para cubrir otros crímenes.

Estudios de crímenes de cuello blanco han mostrado que estos infractores pueden dividirse en varias subcategorías, basándose en sus motivaciones subyacentes:

- El criminal de cuello blanco *resentido* que engaña a la compañía porque se siente engañado *por* la compañía. Normalmente se trata de un empleado de mucho tiempo que ha esperado mucho por un aumento o una promoción o que ha recibido una evaluación de empleado negativa, lo que, a su forma de ver, es inmerecido. Esos criminales cibernéticos adoptan algo de la mentalidad de Robin Hood, convencidos de que sólo están tomando de la compañía rica – que puede afrontar la pérdida e incluso se la merece – y dándoselo al pobre (generalmente ellos mismos).
- El criminal de cuello blanco *deliberado* no tiene una ética personal que le prohíba robar. A diferencia del infractor descrito previamente, no existe un período de formación de enojo o resentimiento. Este tipo comienza la actividad criminal tan pronto como surge la oportunidad. Estos criminales cibernéticos pueden ser bien brillantes y planear meticulosamente sus crímenes. Generalmente tienen en mente un objetivo monetario. El plan maestro es poner el dinero robado en un lugar seguro (como por ejemplo en una cuenta de banco en el exterior). Tras una cierta cantidad de años o al llegar a una suma específica de dinero, planean retirarse y vivir en algún sitio lujoso más allá de la jurisdicción de la ley. Por lo general ellos son muy disciplinados y cuidadosos, extrayendo sólo pequeñas sumas de dinero a la vez de modo que no se note.
- El criminal de cuello blanco *desesperado* que roba en respuesta a problemas financieros personales serios. Estos problemas pueden ser impredecibles, como por ejemplo, una crisis médica o legal en la familia. Más a menudo, sin embargo, ellos son el resultado del mal juicio: juegos prohibidos, alcohol o problemas de drogas, perdiendo dinero en malas inversiones o viviendo por encima de sus posibilidades para impresionar a otros. Estos criminales cibernéticos son, a menudo, descuidados, volviéndose más desfachatados a medida que sus situaciones empeoran. Por consiguiente, ellos son el tipo de criminal de cuello blanco con más probabilidades de ser capturado.

Los criminales de cuello blanco, a veces, se entregan ellos mismos dejando pistas que despiertan las sospechas del investigador, tales como:

- Ingresos inexplicables, propiedades o un estilo de vida mucho más alto del que el que el trabajo de la persona le puede proporcionar
- Transacciones de mucho dinero en efectivo
- Múltiples cuentas bancarias en diferentes bancos, especialmente en bancos de diferentes ciudades o países
- Múltiples negocios con la misma dirección

- Corporaciones en “papeles” que no tienen asentamientos físicos y no parecen realizar ningún producto o brindar algún servicio

En el sitio Web del Centro Nacional de Fraudes de Cheques: www.ckfraud.org/whitecollar.html, se encuentra disponible una lista detallada de los tipos de crímenes de cuello blanco y estafas. Algunos de los crímenes descritos en esta lista pertenecen más apropiadamente a nuestra próxima sección acerca de los estafadores cibernéticos.

Luchadores contra el crimen....

El Luchador Contra el Crimen de Cuello Blanco

La revista del *Luchador contra el Crimen de Cuello Blanco* es una buena fuente de información acerca del crimen de cuello blanco con consejos y trucos sobre cómo evitar ser víctima de él e información para los oficiales de la policía y fiscales sobre cómo lidiar con los delitos de cuello blanco. En el sitio Web de la revista: www.wccfighter.com, están disponibles un ejemplar e información de suscripción.

Estafadores Cibernéticos

Los estafadores utilizan la Internet como una herramienta para alcanzar “marcas” (su terminología para víctimas) que de otra forma no hubieran podido alcanzar. El correo electrónico, los sitios Web y las salas de chateo pueden convertirse en herramientas de los estafadores para propagar sus esquemas fraudulentos.

De acuerdo con la Guía del Comprador en línea (en www.netaction.org/shoppers/fraud.html), la Comisión de Comercio Federal relaciona los timos más frecuentemente reportados como los siguientes:

- **Subastas por Internet:** Los interesados envían su dinero, pero no reciben el producto prometido, o reciben una propiedad que no es la que debería ser.
- **Estafadores de servicios por Internet:** Los clientes prepagan los servicios de acceso y entonces las compañías quiebran y desaparecen, o los clientes son engatusados para pagar por servicios que no quieren (por ejemplo, mediante avisos de búsqueda oficial que implican que Usted perderá su registro de nombre de dominio si no le envía dinero al estafador). En otra variación, un Proveedor de Servicios de Internet envía cheques a las personas de una lista de correos por un valor de \$3.50; a menos que los receptores lean la impresión fina, no se dan cuenta que al cobrar ese cheque, están aceptando la compra de servicios por Internet que serán cobrados mediante sus compañías telefónicas.
- **Fraude de tarjetas de crédito:** Este tipo de fraude involucra a individuos y compañías turbias que pretenden (o realmente lo hacen) vender un servicio o un producto vía tarjeta de crédito con el objetivo de recopilar información de la tarjeta de crédito de la víctima y utilizarla para hacer compras fraudulentas. Transferir la información de una tarjeta a otra falsificada es una práctica denominada *skimming* (desnatando).
- **Discado de módem internacional:** Los usuarios de Internet son persuadidos para descargar un marcador gratis o un programa visualizador (generalmente con el objetivo de

descargar pornografía “gratis”) que desconecta sus módems y marca un número de larga distancia internacional o un número 900 de pago por minuto trayendo como resultado que la factura de teléfono del usuario venga con una deuda enorme e inesperada.

- **“Embutir” la Web:** Este crimen involucra ofertas de servicios gratuitos como el de anfitrión Web por un período de prueba sin obligaciones, después del cual los usuarios tienen que pagar por el mismo en sus cuentas telefónicas o con sus tarjetas de crédito, aún cuando nunca estuvieron de acuerdo con continuar con el servicio transcurrido el período de prueba. (Véase www.ftc.gov/bcp/online/pubs/alerts/webalrt.htm para más información).

- **Marketing a varios niveles (MLM) y esquemas piramidales:** Los estafadores juegan con la codicia de los usuarios y el deseo de hacerse ricos rápidamente si se reclutan – por un precio bien alto – y les prometen enormes ganancias si reclutan a otros. La *carta en cadena* es una variación del esquema piramidal como lo es el *esquema Ponzi* (denominado así porque Charles Ponzi estafó exitosamente a cientos de personas utilizando este método en los años 1920). Todos esas estafas ya existían mucho antes de la Internet, pero la capacidad actual de comunicarse rápida y fácilmente con un inmenso número de personas en todo el mundo les ha proporcionado una nueva vida. (Véase <http://skepdic.com/pyramid.html> para obtener explicaciones detalladas sobre cómo funcionan el esquema piramidal, el de carta en cadena, el Ponzi y otros esquemas MLM – y por qué *no* funcionan para los reclutas ingenuos que son sus víctimas).

- **Fraudes relacionados con viajes y vacaciones:** Esta es la variante de la era de la Internet del tele marketing fraudulento tradicional. Las “ofertas” de viajes y las vacaciones gratuitas fraudulentas (que incluyen toda clase de costos ocultos) abundan. Estas incluyen la venta de millas de pasajeros frecuentes que están al borde de expirar, vouchers junto a esquemas piramidales, ofertas de bait and switch (es una táctica de venta en la que el cliente es atraído por la oferta de un producto barato y lo convencen para que compre otro de un precio superior) y otras ofertas de viajes demasiado buenas para ser reales.

- **“Oportunidades” de negocios e inversiones:** Estas van desde los fraudes de trabajo en casa que requieren que Usted compre un costoso set de principiante y no le dan trabajos reales hasta programas de compra-venta y solicitudes de inversiones en bienes raíces sin valor. De acuerdo con el Buró de Mejores Negocios (www.bbb.org/library/faithscams.asp), la cantidad de estafadores en el campo de las inversiones que intentan aprovecharse de las creencias religiosas de sus víctimas ha crecido dramáticamente. La SEC mantiene un sitio Web sobre cómo evitar estas estafas: www.sec.gov/investor/pubs/cyberfraud.htm.

- **Fraudes relacionados con productos para el cuidado de la salud y servicios:** Estos incluyen productos para reducir peso, productos antienviejecimiento y otros alternativos para el cuidado de la salud que se comercializan bajo derechos falsos y no probados; venta en línea de drogas por prescripción que no requiere que el paciente sea examinado por un médico; marketing a varios niveles de productos para la salud; y otras estafas que buscan aprovecharse de personas que están enfermas o temerosas por su salud. Existen varias organizaciones y agencias que combaten este tipo de fraude, como, por ejemplo, el Consejo Nacional contra el Fraude en la esfera de la salud (www.ncah.org).

Luchadores contra el crimen...

La Línea de la Comisión Comercial Federal para los Casos de Fraude

La Comisión Comercial Federal brinda información al cliente, toma quejas y mantiene una base de datos de compañías reportadas por participar en el fraude en línea. Los consumidores que han sido víctimas de fraude o de prácticas comerciales engañosas o injustas (en línea o no) pueden contactar a la agencia a través de su línea telefónica de ayuda gratuita 1-877-FTC-HELP o pueden completar el formulario de quejas en línea en [http://rn.ftc.gov/dod/wsolcq\\$.startup?Z_ORG_CODE=PU01](http://rn.ftc.gov/dod/wsolcq$.startup?Z_ORG_CODE=PU01). Los casos de fraude en Internet, los de tele marketing y los casos de robo de identidad se introducen en una base de datos segura denominada El Centinela del Consumidor (www.consumer.gov/sentinel). Esta base de datos fue puesta a disposición de las agencias de policías de todo el mundo. La oficina del Fiscal General del Estado en la mayoría de los estados también maneja estos tipos de casos de fraudes.

Una buena fuente de noticias, información y vínculos relacionados con todos los tipos de estafas y casos de fraudes (incluyendo una sección de Alerta de Fraude) es el sitio Fraudes y Estafas: www.swindles.com. Este sitio se actualiza diariamente. Scamwatch, parte de InterGOV Internacional (www.scamwatch.com) es otra buena fuente para reportar fraudes y otros crímenes. En la base de datos de la InterGOV aparece un enorme número de fraudes, así como los tipos reportados con más frecuencia en la FTC, incluyendo fraudes en los juegos de azar, en la reparación de créditos, en los grados universitarios, en las ofertas de premios y muchos más.

Hackers, Crackers y Atacantes de Redes

La red es una importante herramienta que le facilita el “trabajo” a los criminales de cuello blanco y a los estafadores, pero es una herramienta absolutamente esencial para los hackers. Resultaría imposible para los hackers cometer sus crímenes sin la Net.

En el Capítulo 1 analizamos los tipos de crímenes que cometen los hackers: acceso no autorizado, robo de datos o servicios, y crímenes cibernéticos destructivos tales como el estropeo de sitios Web, el lanzamiento de virus, ataques DoS y otros ataques que echan abajo un servidor o una red. En el Capítulo 6, Usted conocerá los detalles técnicos sobre el funcionamiento de la mayoría de estos ataques.

Los hackers aprenden su “oficio” de diferentes formas: equivocándose, estudiando sistemas operativos de redes y protocolos para aprender sus vulnerabilidades y, quizás la más significativa, de otros hackers. Existe una enorme red clandestina (en el sentido tradicional de la palabra, no en el técnico) donde los nuevos en este mundo del hackeo pueden obtener información y aprender de otros hackers más experimentados.

Sitios Web como www.2600.com (originalmente una revista de phreakers telefónicos), www.hackers.com (que se anuncia como “para todos, desde el hacker hasta la ama de casa, desde el estudiante hasta el científico”), y www.atomicvoid.net (una fuente de herramientas de hackeo/ataque) brindan oportunidades para conocer en línea a otros hackers. Así hacen

grupos de noticias como alt.hackers y alt.2600.hackerz y listas de correos como la FreeBSD Hackers Digest en FreeBSD.org. Artículos en línea tales como *Cómo Convertirse en un Hacker* (www.tuxedo.org/~esr/faqs/hacker-howto.html) proporcionan una guía para las personas que se sienten atraídas por el estilo de vida de los hackers. Conferencias de hackers como la DEF CON y The Black Hat Briefings brindan oportunidades del mundo real para que los hackers se encuentren. Un dato interesante es que las organizaciones que patrocinan estos encuentros, durante los últimos años se han convertido en una corriente cada vez más dominante, atrayendo ahora, además de a los hackers, a profesionales de la seguridad y oficiales del gobierno.

Existe una jerarquía definida en la comunidad de los hackers. Los hackers “reales” – programadores expertos y genios en el trabajo con redes que escriben el código y descubren las explotaciones – sienten desdén por los script kiddies, quienes solo utilizan softwares escritos por otros para entrar en sistemas o lanzar ataques sin entender realmente cómo funciona. La cultura del hacker también se divide en dos grupos:

- **Los sombreros negros:** entran a los sistemas de forma ilegal para obtener ganancias personales, notoriedad o con otros propósitos nada legítimos.
- **Los sombreros blancos:** escriben y prueban softwares de fuente abierta, trabajan para corporaciones con el fin de ayudarlas a reforzar su seguridad, trabajan para el gobierno ayudando a capturar y enjuiciar a los hackers de sombrero negro o emplean sus habilidades con propósitos nobles y legales.

También hay hackers que se refieren a ellos mismos como *sombreros grises*, quienes operan en algún sitio intermedio entre los dos grupos primarios. Los hackers de sombreros grises podrían violar la ley, pero ellos consideran que tienen un propósito noble para hacerlo. Por ejemplo, podrían crackear sistemas sin autorización y después notificar a los dueños del sistema sobre la falibilidad del mismo como un “servicio público” o encontrar lagunas de seguridad en los softwares y entonces publicarlas en aras de forzar a los comercializadores a crear parches o soluciones para el problema.

Nota

La distinción de sombrero blanco o negro se ha vuelto más confusa, pues los ex hackers criminales dan conferencias o han conseguido trabajo en corporaciones como expertos en seguridad y, porque organizaciones como Black Hat, Inc. han añadido una “pista de sombrero blanco” a sus programas de capacitación por conferencias. Sólo en las antiguas películas del oeste Usted puede guiarse por el color del sombrero de una persona como indicación palpable de su carácter. En el mundo cibernético de hoy, la mayoría de las personas – incluidos los hackers – no son ni malos ni buenos. Un hacker que se identifica como un hacker de sombrero blanco podría sucumbir ante la tentación de cometer un acto ilegal y los que se auto-declaran sombrero negro pueden reformarse y convertirse en unos de los “buenos”.

El así llamado “hacking ético” puede ser un negocio lucrativo si un hacker cuenta con las habilidades requeridas, incluyendo las aptitudes sociales necesarias para funcionar en el mundo corporativo. Los asesores les cobran a las compañías \$10,000 o más para probar su

seguridad intentando hackear sus sistemas y dándole reportes y recomendaciones para rellenar las lagunas de seguridad que ellos encuentran. (Véase www.research.ibm.com/journal/sj/403/palmer.html para tener más información sobre el hackeo ético).

Criminales que Usan la Net Incidentalmente al Crimen

Algunos criminales usan la red en relación con sus crímenes, pero la Net no es una herramienta real de los crímenes. O sea, la red no se usa para cometer la *actividad criminal*, aunque se puede usar para prepararse para ella o para guardar las incidencias de esa actividad criminal. Ejemplos de este tipo de criminalidad incluyen:

- Criminales que usan la Net para encontrar víctimas
- Criminales que usan computadoras o redes para guardar incidencias
- Criminales que usan el correo electrónico o el servicio de chateo para comunicarse con los cómplices

Aún en casos donde la red no es una herramienta del crimen, ésta puede proporcionar evidencia del intento criminal y pistas que ayuden a los investigadores a rastrear a los criminales. Analizaremos cada una de estas situaciones en las secciones siguientes.

Criminales que Usan la Net para Encontrar Víctimas

Podría parecer que el uso de la Net para encontrar víctimas la convertiría en una herramienta del crimen. En algunos casos, el criminal procede a usar la Internet para realmente cometer el crimen – por ejemplo, enviando cartas electrónicas en cadena, mandando a través del correo electrónico avisos ficticios pretendiendo ser del proveedor de servicios de Internet de la víctima que solicitan la información de la tarjeta de crédito o conduciendo a las víctimas hacia un sitio Web que trata de venderles productos bajo falsas pretensiones). En esos casos, la Internet es una herramienta del crimen, pero el acto inicial de buscar víctimas potenciales no es en sí un acto criminal. Por lo tanto, un pedófilo o un violador u otro criminal que usa la Net para encontrar víctimas, pero después comete la actividad criminal en el mundo real, está usando la Internet incidentalmente al crimen. Sin embargo, la Internet se puede usar para montar una operación encubierta que virará la tortilla y llevará al criminal a revelar su identidad a la policía.

Criminales que Utilizan Computadoras o Redes para Guardar Incidencias

Las personas que realizan una actividad criminal no relacionada con computadoras como el tráfico de drogas, el juego ilegal u otros “negocios” ilícitos pueden usar las computadoras para guardar los registros financieros, las listas de clientes y otra información relacionada con la actividad criminal y usar la Internet para transferir estos ficheros a un lugar fuera de obra donde estará segura de no ser encontrada por la policía.

Transferir registros comerciales a la computadora de un amigo o a un servicio de almacenamiento de datos en Internet no va contra la ley, de modo que el uso de la Net es incidental a esta actividad criminal, aún cuando esos ficheros podrían constituir una importante evidencia del crimen real.

Criminales que Usan el Correo Electrónico o el Servicio de Chateo para Comunicarse con los Cómplices

Los criminales que trabajan en grupos – grupos terroristas, redes de robos, hackers de sombrero negro – a menudo usan el correo electrónico y el chateo de la misma forma en que los usuarios legítimos lo hacen: para comunicarse con personas con las que trabajan. La correspondencia en sí no constituye un crimen, es la actividad ilegal que está siendo planeada o discutida la que es criminal. Sin embargo, la correspondencia se puede utilizar no sólo para demostrar las intenciones del criminal y ayudar a rastrearlo, sino también, en algunos casos, para probar la existencia de una conspiración criminal. Esto es importante, porque si existen los elementos de una conspiración, se pueden presentar cargos contra todos los miembros de la misma, no sólo contra la o las personas que cometieron físicamente el crimen.

Reseña de la Ley Cibernética...

Conspiración Criminal

Los términos de los estatutos sobre conspiración varían en diferentes jurisdicciones, pero la mayoría de los estados consideran la conspiración un delito preparatorio o a medias. El cargo de conspiración es un delito aislado, pero debe ser presentado conjuntamente a otro delito criminal. Generalmente, una conspiración criminal existe cuando dos o más personas acuerdan que uno o más de ellos cometerá un delito de felonía y uno o más de los conspiradores llevará a cabo algún acto manifiesto en correspondencia con el acuerdo. En otras palabras, si en la corte el fiscal puede demostrar (por ejemplo, recopilado vía correo electrónico de conformidad con una orden de registro o interceptado legalmente por orden judicial) que tal acuerdo fue hecho y además puede probar que al menos una de las partes dio algunos pasos hacia la comisión del crimen, *todas* las partes pueden ser acusadas de conspiración criminal, se haya o no completado exitosamente el crimen.

No Criminales en la Vida Real que Cometan Crímenes en Línea

En algunas situaciones, personas que no son criminales en la vida real, asumen una conducta criminal en línea. Estas incluyen a criminales cibernéticos accidentales y criminales cibernéticos situacionales. *Los criminales cibernéticos accidentales* no tienen intenciones criminales. Cometan actos ilegales en línea porque ignoran la ley o no están familiarizados con la tecnología. Un ejemplo lo constituye alguien que tenga una conexión por módem de cable o que esté usando el acceso a Internet de banda ancha disponible en algunos hoteles y abra la carpeta de Entorno de Redes en su computadora (el listado de visualización de la red) y vea otras computadoras allí. Por curiosidad, haga clic a uno de los íconos sólo para ver qué sucede. Si se encuentra con una computadora en la red con un sistema operativo de baja seguridad o que no requiere de un nombre de usuario y

contraseña para registrarse y que tenga activada la opción de compartir ficheros en la red, podrá acceder a los ficheros compartidos en esa computadora.

Si nuestro usuario hipotético no es muy experto en cuestiones técnicas o legales, podría incluso no percatarse de que esos ficheros están en la computadora privada de otra persona (o al menos eso pensaba el dueño). O podría pensar que como son accesibles, es legal verlos. Sin embargo, en dependencia de que cómo sean los estatutos del estado en relación con el acceso no autorizado, podría ser un crimen acceder sin permiso a cualquier otra computadora a través de una red, aún si el usuario de esa computadora, quizás inconscientemente, se lo facilitó desde el punto de vista tecnológico.

El comportamiento de los *criminales cibernéticos situacionales* refleja un fenómeno interesante que analizamos anteriormente – la disociación psicológica experimentada por algunas personas cuando se conectan. Esta disociación puede causar que algunas personas que, en la vida real, se consideran ciudadanos íntegros y respetuosos de la ley que nunca cometerían deliberadamente un crimen realicen una actividad ilegal cuando asumen su “otra personalidad” mientras están conectados.

Estas personas podrían tener deseos reprimidos por satisfacer en una conducta ilícita que ellos controlan mediante auto-disciplina, pero que se sienten libres de desatar cuando se conectan a Internet, porque allí ellos pueden ser (en sus propias mentes) “otra persona”. Literalmente, ellos llevan una doble vida como un día moderno de drjekyllandmrhyde@aol.com.

Comprendiendo a las Víctimas del Ciberespacio

El término *víctima* se deriva de la palabra en latín *victima*, que significa “un animal ofrecido en sacrificio”. Hoy día la palabra se usa para referirse a alguien o a algo dañado por algún acto o circunstancia. La víctima del crimen es la persona *a la que* le sucede el crimen, la persona dañada por el acto ilegal de un criminal.

El campo de la *victimología* trata de recopilar datos y en efecto crear perfiles sobre las víctimas del crimen. Esta información resulta útil por varias razones:

- Le permite a los oficiales del orden predecir qué tipos de persona o personalidad son más propensos a convertirse en víctimas de ciertos crímenes y prevenirlos. Esto, por su parte, le da a las víctimas potenciales la oportunidad de tomar medidas para protegerse.
- Le permite a los oficiales del orden crear mejor el perfil del criminal, porque los patrones en la elección de la víctima son una parte importante del perfil criminal.
- Le permite a los oficiales del orden utilizar el perfil de la víctima como cebo para los criminales, para hacer que salgan del anonimato.

La víctima de un crimen es, en muchas ocasiones, el testigo clave contra el infractor. Utilizando las técnicas de la victimología, incluso una víctima difunta puede proporcionar pistas importantes para los investigadores. De acuerdo con Amy Goldman, autor de *La importancia de la victimología en la creación del perfil criminal*: “Cada pregunta

respondida con respecto a la víctima es en realidad una ventana a la psiquis del infractor y, además, responde preguntas sobre el infractor”.

En la escena....

Utilizando la Victimología para Encubrirse

Los oficiales han estado investigando a un pedófilo en línea que era sospechoso de atraer a niños a encuentros personales y violarlos. Un oficial encubierto creó un personaje en línea – el de una niña de 12 años – basándose en las características de las víctimas escogidas anteriormente por el pedófilo. Entonces el oficial frecuentó las salas de chateo que se sabía que el pedófilo frecuentaba, con la esperanza de que este tratara de acordar un encuentro en la vida real con el oficial disfrazado de niña. De esta forma, la policía podría monitorear el lugar del encuentro e identificar positivamente al criminal.

Es muy importante, en cualquier operación encubierta, evitar cometer incitaciones que causarían que la evidencia contra el infractor fuese rechazada por la corte. Generalmente, las cortes han sostenido que los oficiales pueden “dar una simple oportunidad “ para que alguien cometa un crimen – como hizo el oficial de nuestro ejemplo pretendiendo ser una niña que encajara en el perfil de las víctimas del pedófilo y esperando a que este iniciara el contacto y la asediara. La incitación ocurre cuando los oficiales van más allá de dar la oportunidad, intentando abiertamente de inducir, atraer o persuadir al sospechoso para que cometa el acto criminal. Por ejemplo, si nuestro oficial (haciendo el papel de la niña) contactara con el pedófilo, se “acercara” a él y le pidiera encontrarla para tener sexo, eso podría considerarse una incitación.

Clasificando por Categorías a las Víctimas del Crimen Cibernético

Podemos crear categorías de víctimas del crimen cibernético, de la misma forma en que hicimos con los criminales cibernéticos. Nuevamente, es importante destacar que no todas las víctimas encajan bien en estas categorías y algunas de las categorías coinciden algunas veces. Algunas características comunes de las víctimas incluyen:

- Personas que son nuevos en la Net
- Personas que son ingenuos por naturaleza
- Personas discapacitadas o poco aventajadas
- “Desesperados” que están ávidos, solos o que tienen otras necesidades emocionales
- Pseudos-víctimas que reportan haber sido victimizadas, pero que realmente no lo fueron
- Personas que son sencillamente lo suficientemente desafortunadas como para estar en el lugar equivocado (el virtual) en el momento equivocado

Tomemos un momento para revisar cada una de estas características y comprender porqué las personas en estos grupos son especialmente vulnerables al crimen cibernético.

Nuevos en la Net

“El nuevo” en Internet podría no estar familiarizado aún con los fraudes comunes que causarían que un veterano en la Net suspirara y dijera: “Oh, uhm, esa historia de nuevo, no”. Además, los nuevos, a menudo, no son conscientes de las prácticas de seguridad comunes y de las conocidas lagunas de seguridad en los softwares. Ellos podrían no percatarse de que sus sistemas pueden ser infectados con virus, simplemente, por abrir un anexo a un correo o visitar el sitio Web equivocado. Quizás tampoco conocen que los virus se pueden enviar desde sus propias máquinas sin su conocimiento.

Los usuarios de computadoras que no tienen mucha experiencia interactuando en línea pudieran confiarse más de los que “conocen” a través del chateo. Pudieran creer que porque *ellos* son honestos en sus comunicaciones en línea, los demás también lo son.

Con la enorme cantidad de personas que se conecta a Internet por primera vez cada año, los criminales cibernéticos tienen siempre un cultivo fresco de recién llegados de quienes alimentarse. En sus esfuerzos por educar al público sobre el crimen cibernético, los profesionales de la informática y los policías deberían prestar especial atención a los nuevos usuarios de Internet, hacerles saber que pueden ser blancos de estafadores y otros infractores y proporcionarles información sobre cómo reconocer y evitar esquemas cuestionables.

Ingenuos por Naturaleza

Algunos grupos son más ingenuos por naturaleza que otros – aunque los miembros individuales de estos grupos podrían no ser ingenuos en lo absoluto. El muy joven y el anciano han sido, durante mucho tiempo, los favoritos de los estafadores y esa preferencia se transfiere al mundo en línea.

Los más jóvenes tienen a menudo una perspectiva distorsionada del mundo, especialmente si han tenido una vida con mucha protección. Ellos podrían no haber interiorizado todavía la idea – incluso si se lo han dicho – de que existen personas malas que quieren dañar a otras. Podrían pensar que si son buenos con otros, todas serán amables con ellos. Además, los niños son curiosos por naturaleza y están ansiosos por complacer, lo que puede ser una combinación peligrosa de cualidades cuando entran en contacto con un criminal cibernético. Los niños son, por supuesto, el blanco de algunos de lo peor de lo peor de Internet: los pedófilos.

Muchos ancianos se sienten incómodos con las nuevas tecnologías, porque no crecieron con ellas. Ellos podrían disfrutar ayudando a la gente, un rasgo que los estafadores pueden explotar. Cuando los ancianos son víctimas de un comportamiento criminal, podrían vacilar para reportarlo – incluso si han sido estafados con miles de dólares – porque sienten que, de alguna forma, ellos también son culpables por ser “estúpidos”. Los esquemas tradicionales de fraude por correo que tenían como blanco a los ancianos han reencarnado: el fraude por correo electrónico.

Las agencias establecedoras del orden están reconociendo el creciente problema enfrentado por víctimas jóvenes y viejas y están desarrollando programas diseñados para ayudar a esos “conductores del estudiante” y a la gente que ha disminuido un poco la velocidad en la supercarretera de la información sin llegar a cansarse. Los profesionales de la informática y los agentes del orden pueden colaborar con las escuelas y los centros de ancianos para incrementar la consciencia y educar a estos grupos vulnerables.

Discapacitados y Poco Aventajados

El discapacitado mental y físico y el poco aventajado también pueden ser blancos de criminales particularmente reprensibles que – con el objetivo de identificar a las víctimas potenciales – buscan bases de datos en línea y frecuentan listas de correos diseñadas como grupos de apoyo para personas con discapacidades.

Los foros en línea pueden ser especialmente importantes como un medio de interacción social y una fuente de amistad para personas con ciertas discapacidades que limitan su movilidad, como la paraplejía, o que hagan que sea poco aconsejable que se acerquen a grupos de personas como desórdenes del sistema inmunológico o que tengan alterada su apariencia como daños traumáticos. Las agencias del orden pueden asociarse a firmas informáticas para brindarle un valioso servicio ayudando a estas personas a crear una mayor consciencia del crimen cibernético mientras las ayudan a aprender a aprovechar las posibilidades de la computación con el fin de mejorar sus vidas.

Desesperados

Las personas desesperadas son blancos excelentes para los criminales cibernéticos. Ellos podrían estar buscando amor en todos los sitios equivocados del ciberespacio, estar buscando desesperadamente salvación a través de grupos religiosos en Internet, tener una necesidad extrema de dinero o tener alguna otra necesidad emocional o física. De cualquier forma, su desesperación los hace vulnerables – a los estafadores estilo Lotario quienes entablan relaciones románticas con la intención de estafar a la pareja, o a los evangelistas sin ética a quienes quieren hacer dinero a costa de las añoranzas espirituales de otros, a los creadores de esquemas de hacerse rico en poco tiempo, a los prestamistas de Internet o a los agentes empleadores fraudulentos.

Dado que la desesperación es generalmente una condición temporal o intermitente y dado que, parafraseando a Henry David Thoreau, aquellos que la sufren, por lo general llevan una vida de desesperación *silenciosa*, podría resultar más difícil identificar y advertir a esas víctimas potenciales sobre su vulnerabilidad. Los investigadores que detectan este patrón de victimización para un criminal cibernético en particular pueden, sin embargo, usar la información para efectuar una acción encubierta colocando como “carnada” a aquel que encaje en el perfil de la víctima.

Seudo-víctimas

Sigmund Freud podría haber estado en lo cierto cuando dijo que a veces un tabaco es sólo un tabaco, pero a veces una víctima *no* es sólo una víctima. Existen personas que, por varias razones, reportan crímenes que nunca ocurrieron o actúan como víctimas cuando no lo son (y pudieran, de hecho, ser los verdaderos perpetradores).

Las motivaciones de estas *seudo-víctimas* cubren todo el espectro de:

- Personas que toman represalias o expresan su enojo hacia otra persona acusándola falsamente de un crimen.
- Personas que quieren atención; pretender ser la víctima de un crimen las hace sentir “especiales”.
- Personas que dicen ser víctimas de un crimen para cubrir el hecho de que ellos mismos lo cometieron.
- Personas que pretenden ser víctimas a fin de reclamar dinero de los fondos de ayuda a las víctimas, organizaciones caritativas o compañías de seguros.
- Personas que honestamente creen que se ha cometido un crimen en contra de ellos cuando han sido las víctimas de un comportamiento no ético o inmoral – pero no ilegal.

Aunque la vasta mayoría de los reportes de víctimas son genuinos, cuando los investigadores interrogan a las víctimas de un crimen, deben estar siempre conscientes de la posibilidad de que se trate de una *seudo-víctima*. En la mayoría de los estados, los estatutos consideran un delito criminal el archivar un reporte de crimen falso. Tales cargos podrían ser apropiados en todos los ejemplos, excepto en el último.

En el Lugar Equivocado (el Virtual) en el Momento Equivocado

Es cierto que los depredadores humanos, como sus semejantes en el reino animal, a menudo buscan como presa a los miembros más débiles de la manada, o a aquellos que ellos consideran los más débiles. Sin embargo, no todas las víctimas de un crimen son elegidas porque demuestren alguna vulnerabilidad. Algunos criminales son indiscriminados y eligen sus víctimas al azar – el primero en llegar. A veces acabar como víctima de un crimen cibernético es sólo una cuestión de estar en el lugar equivocado (el virtual) en el momento equivocado.

Al crear perfiles, ya sea de los criminales o de las víctimas, así como los especialistas deben buscar patrones, también tienen que cuidarse de no imaginar patrones que no existen. El hecho de que las víctimas de un criminal *no* encajen en un perfil también puede ser una información valiosa para el investigador.

Hacer que la Víctima sea Parte del Equipo de Lucha contra el Crimen

Cuando apareció por primera vez la especialidad de la victimología en los años 1940, aquellos que estudiaban la victimización tendían a ver a las víctimas como objetos dignos de lástima, personas débiles que eran vistas, a menudo, como contribuidores de su propia

mala suerte. Más tarde, esto se conoció como la mentalidad de “culpar a la víctima” y le cedió el terreno a la actitud más prevaleciente de hoy – a las víctimas se les debe dar más facultades a través de la educación y el acceso a recursos. En gran medida, el cambio fue en respuesta a las feministas que protestaban contra el tratamiento denigrante y humillante que sufrían a veces las víctimas femeninas de un crimen – especialmente las víctimas de violaciones o abusos sexuales – de manos de los policías y las cortes.

Muchas víctimas hoy prefieren no definirse a sí mismas como víctimas debido a la imagen de debilidad e impotencia que implica este calificativo. De acuerdo con la *Teoría de la Victimología*, de T.O. Connor (<http://faculty.ncwc.edu/toconnor/300/300lect01.htm>), el término preferido ahora es *sobreviviente*, una palabra que implica fortaleza.

Muchos estados han promulgado un proyecto de ley sobre los Derechos de las Víctimas de un Crimen y otras legislaciones que imponen requerimientos a las agencias establecedoras del orden de seguir ciertas pautas al tratar con las víctimas de un crimen. Muchas agencias ahora fijan citas para las víctimas de un crimen con profesionales entrenados para ofrecer asesoría y guía a las víctimas y en algunos casos para “proteger” a las víctimas del personal policial hostil o demasiado mayor.

Los derechos de las víctimas garantizados por estas leyes incluyen, por lo general:

- El derecho a ser notificado cuando el infractor irá a juicio
- El derecho a estar presente en el juicio, ya sea personalmente o representado por un abogado
- El derecho a ser informado sobre la disposición del caso
- Si el sospechoso es condenado, el derecho a ser informado y a reclamar si el sospechoso queda en libertad condicional
- El derecho a ser informado de si el sospechoso va a quedar en libertad y de la fecha en que esto ocurriría
- El derecho a ser tratado con dignidad por el sistema de justicia penal
- El derecho a ser informado de los servicios sociales y de la ayuda financiera para víctimas que están disponibles
- El derecho a ser compensados por sus pérdidas en la medida de lo posible

Los programas de compensación a las víctimas son generalmente programas fundados por el estado, diseñados para ayudar a pagar gastos médicos y otros asociados al hecho de haber sido víctima de un crimen. En algunos casos, las cortes les exigen a los infractores la restitución directa a las víctimas o a las fondos de compensación. Estos programas generalmente son administrados por la oficina del Fiscal General del Estado.

Reseña de la Ley Cibernética...

Programas de Servicios para Víctimas

El Departamento de Justicia de los Estados Unidos dirige la Oficina para Víctimas de Crímenes (OVC), la cual organiza actividades para la Semana Nacional por los Derechos de las Víctimas de Crímenes en Abril y brinda noticias, investigaciones, estadísticas y otros

recursos en www.ojp.usdoj.gov/ovc. Usted puede encontrar ejemplos de programas de servicios para víctimas de crímenes en estos sitios:

www.oag.state.tx.us/victims/victims.htm (Texas)

<http://legal.firn.edu/victims> (Florida)

www.scattorneygeneral.org/public/victimassist.html (Carolina del Sur)

www.ago.state.nm.us/Advocate/victim_services_advocate.html (Nuevo México)

www.ag.state.il.us/crimevictims/crime.htm (Illinois)

www.ago.state.ma.us/videfault.asp (Massachusetts)

www.doj.state.wi.us/cvs (Wisconsin)

www.caag.state.ca.us/cvpc/fa_victims_services.html (California)

www.oag.state.ny.us/crime/crime.html (Nueva York)

Otros estados tienen programas similares.

Comprendiendo a los Investigadores Cibernéticos

¿Son las investigaciones de crímenes cibernéticos sólo “lo mismo de antes” para los detectives de la policía? ¿Se requieren las mismas características de la personalidad, habilidades y conocimientos para las investigaciones cibernéticas que para las investigaciones criminales en general? ¿Necesitan los investigadores de crímenes cibernéticos un entrenamiento especial? En las siguientes secciones trataremos estas interrogantes y construiremos un perfil de un investigador cibernético efectivo.

Nota

Generalmente no existe un calificador oficial o una posición llamada *investigador cibernético*, aunque las agencias locales tienen la libertad, por lo general, de crear sus propios calificadores, de modo que no podemos decir con certeza que ese calificador no existe. Utilizamos el término aquí para referirnos a las personas cuyos deberes investigativos incluyen los crímenes cibernéticos. En la mayoría de las agencias no se reportan ni se investigan suficientes delitos relacionados con computadoras como para justificar la desviación de personal hacia la investigación exclusiva de estos tipos de crímenes. Incluso en agencias mayores como el Departamento de Policía de los Ángeles (LAPD), sólo un número reducido de los 900 empleados son parte de la unidad de crímenes por ordenador del departamento.

Reconociendo las Características de un Buen Investigador Cibernético

Un buen investigador cibernético debe poseer las cualidades necesarias de cualquier buen investigador criminal, incluyendo:

- **Excelente poder de observación:** Un investigador debe notar cosas, incluyendo las “pequeñas cosas”.

- **Buena memoria:** En aras de juntar las muchas pistas que aparecen en el transcurso de una investigación, un detective debe ser capaz de recordar hechos, nombres, lugares y fechas o podría obviar una conexión vital.
- **Poder de organización:** Un buen investigador no sólo recuerda información sino que es capaz de organizarla de forma lógica de modo que los patrones y las correlaciones se tornen aparentes.
- **Poder de documentación:** Un buen investigador no conserva toda esa información en su cabeza, es capaz y está dispuesto a escribirla meticulosamente de modo que se pueda compartir con otros y se use como base para construir el caso.
- **Objetividad:** El investigador no debe permitirse prejuicios personales, relaciones o sentimientos que afecten su capacidad de evaluar objetivamente la evidencia.
- **Conocimientos:** Un investigador efectivo conoce las leyes criminales, las reglas de la evidencia, la teoría de la victimología, la psicología criminal, los conceptos y procedimientos investigativos y sabe sobre el apoyo científico, los servicios de los laboratorios y los recursos de dentro y fuera de la agencia.
- **Capacidad de pensar como un criminal:** Los mejores investigadores tienen una consciencia “innata” de los procesos mentales de los criminales y pueden ponerse en el lugar de un infractor y predecir sus actos.
- **Imaginación constructiva controlada intelectualmente:** El investigador debe ser lo suficientemente creativo como para considerar todas las posibilidades, examinar hechos y después extrapolar conclusiones.
- **Curiosidad:** Los mejores investigadores son curiosos innatos. No se satisfacen sólo con aclarar el caso. No es suficiente para ellos determinar que el sospechoso cometió el crimen; ellos quieren saber por qué y cómo fue cometido exactamente.
- **Resistencia:** La investigación es un trabajo duro que, por lo general, exige largas horas. Un buen investigador debe estar físicamente preparado para este reto.
- **Paciencia:** La investigación resulta, muchas veces, un proceso interminable. Con frecuencia los progresos se hacen pasito a pasito. A menudo las pistas no conducen a ningún lugar, resulta que los sospechosos principales tienen coartadas y el investigador tiene que comenzar todo desde cero.
- **Amor por aprender:** De aprender es de lo que realmente se trata la investigación – aprender sobre los hechos de un caso, aprender sobre las personas involucradas, a veces, incluso, convertirse en un “experto instantáneo” en otro campo, como el de las redes de computadoras a fin de comprender los aspectos técnicos del crimen.

Además de estas cualidades genéricas, un investigador especializado en crímenes cibernéticos necesita algunas características adicionales:

- **Un entendimiento básico sobre computación:** Mientras más sepa el investigador sobre cómo funcionan las computadoras (incluyendo ambos, hardware y software), mejor.
- **Un entendimiento sobre los protocolos de redes:** El crimen cibernético, por definición, involucra a una red. Aún si el investigador tiene un buen dominio de la tecnología de la computación en un contexto de estación de trabajo, eso no significa que comprenderá cómo funcionan las intrusiones y los ataques a las redes, qué le sucede al correo electrónico cuando abandona el sistema del remitente o cómo un visualizador Web solicita y descarga páginas, gráficos o guiones.

- **Conocimiento de la jerga tecnológica:** Todas las vocaciones y la mayoría de los hobbies tienen una *jerga* única, una terminología que significa muy poco fuera de ese campo y que los miembros utilizan como “abreviatura” para comunicarse entre ellos. Un buen investigador tiene que ser capaz de “hablar el idioma”.
- **Un entendimiento sobre la cultura de los hackers:** Se dice que se necesita a un hacker para atrapar a otro (generalmente hackers reformados que venden sus servicios como expertos en seguridad). Hay un grano de verdad en este axioma. Resulta mucho más fácil rastrear a los hackers si Usted comprende su mentalidad y los protocolos (esta vez en el sentido no técnico) de interacción en la comunidad de los hackers. Al igual que los oficiales de narcóticos necesitan estar íntimamente familiarizado con la forma en que los traficantes de drogas interactúan entre sí, los investigadores de crímenes cibernéticos deben especializarse igualmente en la cultura de los hackers.
- **Conocimiento sobre temas de seguridad de redes y computadoras:** Para investigar crímenes de hackeo y de ataques o intrusiones a redes, el investigador debe estar familiarizado con los “huecos” de seguridad más comunes, los productos de seguridad (como los muros de fuego) y las prácticas y pólizas de seguridad.

Debe quedar claro de la lista anterior que los investigadores de crímenes cibernéticos generalmente necesitan un entrenamiento extensivo a fin de operar efectivamente en esta área tan especial. En las grandes agencias policiales generalmente se reconoce esta necesidad; en ellas los profesionales de la informática y los graduados en Computación podrían ser reclutados para llevar las investigaciones de crímenes cibernéticos o podrían llamar a asesores externos para asistir a los detectives en estas investigaciones. Sin embargo, en las pequeñas agencias, demasiado a menudo, se le asigna el caso de crimen cibernético al oficial de turno, sepa este o no algo sobre computadoras. Casi tan malo como esto es la situación común en la que al oficial del departamento que es considerado el as en computación (lo que puede significar que es desde un “experto programador” hasta “el único en el departamento que sabe cómo formatear un disquete”) se le asignan todos los casos de crímenes cibernéticos. Como este oficial es visto por los administradores de la agencia como un experto en computadoras – aún si está muy lejos de serlo – se espera que el recién designado investigador de crímenes cibernéticos atienda asuntos que están muy por encima de sus capacidades.

Clasificando por Categorías a los Investigadores Cibernéticos de acuerdo con sus Aptitudes

Debido a que el *nivel* de aptitudes de aquellos que realizan investigaciones de crímenes cibernéticos varía tremendamente, podemos clasificar por categorías a la mayoría de los investigadores cibernéticos de acuerdo con sus aptitudes:

- **Investigadores que se especializan en crímenes relacionados con computadoras/redes:** Primero son investigadores con un interés secundario en la tecnología. Generalmente son oficiales de la policía o personal de seguridad de corporaciones.

- **Especialistas en Computación que conducen investigaciones:** Primero son profesionales de la informática con un interés secundario en la investigación/el trabajo policial. A menudo trabajan como asesores en agencias policiales.
- **Aquellos con las mismas aptitudes que están entrenados o interesados en la investigación y la informática:** Estos están involucrados en el crimen cibernético/por ordenador desde los comienzos de sus carreras. Podrían tener un entrenamiento paralelo en ambos campos, como un especialista doble en justicia criminal e Ingeniería de redes o programación. Podrían trabajar para agencias policiales o como asesores independientes y generalmente son muy demandados y perciben altos salarios.
- **Aquellos que no tienen aptitudes reales o interés en la investigación ni en la informática:** Estos podrían ser oficiales de la policía que fueron “ascendidos para quitarlos del medio” a la división de detectives y consiguieron un caso de crimen cibernético por casualidad. Ellos no están realmente interesados en el trabajo investigativo y preferirían estar patrullando. No están entrenados ni aman el trabajo con las computadoras y redes. Afortunadamente, no hay muchos investigadores cibernéticos que encajen en esta categoría.

Reclutando y Entrenando a los Investigadores Cibernéticos

La interrogante se ha hecho antes: ¿Es la investigación una habilidad o un talento? Usted podría preguntarse cuál es la diferencia y qué importancia puede tener la respuesta a esta pregunta.

Una *habilidad* se puede aprender; un *talento* es innato. La mayoría de las actividades creativas involucran a ambos. Casi todo el mundo puede tomar clases de piano, aprender a leer música y tocar canciones simples. Esta es una habilidad que se puede desarrollar mediante la práctica. Sin embargo, algunas personas nacen con la habilidad de “tocar a oído”, de sentarse a un piano e interpretar una canción que nunca antes han oído sin ver una partitura o de componer piezas originales. Eso es talento y el mejor maestro no puede enseñárselo si Usted no lo tiene.

La investigación es, como hemos mencionado, un proceso creativo. Requiere de ciertas habilidades que pueden ser aprendidas y desarrolladas, pero los mejores investigadores también son talentosos; se puede decir que tienen “olfato para ello” o pensar que poseen algún sentido de intuición casi mágico. También hay personas que parecen tener un ángel natural para las computadoras. El individuo raro que sea talentoso en ambas áreas debería ser reclutado de inmediato por las agencias de policía.

Pero el talento en crudo no es suficiente para convertirse en un maestro en la esfera de la investigación cibernética, como no lo es para convertirse en un maestro del piano. Se requiere de entrenamiento para desarrollar y perfeccionar las habilidades de modo que estas vayan de la mano con el talento.

Las comisiones estatales para la supervisión del entrenamiento de la policía (a veces denominadas POST, por *Peace Officers Standards and Training* (Entrenamiento y Superación Estándar de los Oficiales de Paz), aunque en Texas está la Comisión de Texas para la Educación y la Superación Estándar de los Oficiales del Orden o TCLEOSE, Texas

Commission on Law Enforcement Officer Standards and Education) deberían incorporar en sus programas académicos un entrenamiento básico sobre el crimen cibernético. Casi todos los oficiales que trabajan en el mundo actual se encuentran eventualmente con crímenes cibernéticos. Como los primeros en responder, los oficiales de las patrullas necesitan conocer cómo manejar la evidencia electrónica, aún si no están llevando a cabo la investigación.

Debería existir un entrenamiento avanzado sobre crímenes cibernéticos – y debería ser obligatorio – para aquellos que realmente llevan la investigación. Las nuevas tecnologías (y las nuevas formas de usarlas para cometer crímenes) están emergiendo constantemente, así que los investigadores de crímenes cibernéticos tienen que estar actualizados con las últimas informaciones.

Organizaciones como la Asociación Internacional de Jefes de Policía (www.theiacp.org), la Asociación de Investigadores de Crímenes de Alta Tecnología (www.htcia.org) y la Asociación Internacional de Especialistas de la Investigación Electrónica (www.iacis.com) pueden proporcionar pautas y recursos para el entrenamiento.

Facilitando la Cooperación: los CEOs en la Escena

Hay otra persona importante involucrada en los crímenes cibernéticos que victimizan a negocios y grandes organizaciones: el oficial ejecutivo jefe de la compañía (CEO) o gerente. Los ejecutivos de las empresas están viendo a sus organizaciones cada vez más expuestas a la amenaza de la actividad criminal – y, en algunos casos, a la responsabilidad criminal – de personas de fuera y de adentro de la organización que utilizan las computadoras y redes para cometer actos ilegales.

La primera medida que los ejecutivos de las empresas deben tomar al descubrir la actividad criminal es reportarla a la policía. La decisión de reportar el crimen no siempre es tan simple como suena. Si cada violación de la ley fuese reportada, investigada y enjuiciada, nuestro sistema de justicia penal se hubiera venido abajo por la sobrecarga. Por ejemplo, en muchos estados constituye un delito criminal llamar a alguien por un nombre profano en un lugar público. Sin embargo, si eso le sucediera a Usted, a menos que la situación empeorara, probablemente Usted no llamaría a la policía. ¿Por qué? Porque consciente o subconscientemente Usted hace un análisis de beneficios/costos y determina que el tiempo y el esfuerzo que tiene que emplear para hacer una declaración jurada oficial y quizás retornar para testificar en la corte, además del riesgo de enfurecer *realmente* al infractor, no valen la pena los beneficios de presentar cargos.

Del mismo modo, si los oficiales de las compañías descubrieran que un hacker ha penetrado su red, pero los daños o pérdidas han sido mínimos o nulos, podrían decidir no reportarlo ya que el tiempo de inactividad del personal clave, el riesgo de la mala publicidad para la compañía si otros se enteran de que esta fue hackeada, conjuntamente con otros factores, hacen que el costo de hacer el reporte sea mayor que los beneficios.

Otra razón por la que las compañías víctimas de un crimen cibernético dudan en reportarlo es la cuestión de su propia responsabilidad. Aunque el crimen fue cometido en su contra,

cabe la posibilidad de que sus clientes puedan demandarlos por negligencia por permitir que esto sucediera (como algunas de las víctimas de los ataques terroristas al World Trade Center de la ciudad de Nueva York demandaron a las líneas aéreas que también fueron víctimas de ellos). La percepción hoy día es que una compañía es legalmente responsable de prepararse para cualquier posible contingencia a fin de protegerse a sí misma y a sus clientes. Esta visión ha sido sostenida por jurados quienes les han dado grandes sumas de dinero a los demandantes en muchos casos de negligencia. Aún cuando los clientes no demandan, los accionistas podrían enojarse y los inversionistas podrían retener la entrega de fondos si la red de la compañía parece no ser segura.

Los gerentes también podrían estar renuentes a mostrarle la información almacenada en su red a los investigadores gubernamentales. Esto es especialmente cierto si se estuviera llevando a cabo alguna actividad no tan legal – por ejemplo, estrategias “creativas” para el pago de los impuestos. Resulta mucho más fácil asumir los costos causados por el crimen, si existen algunos, y emplear el tiempo y el dinero para asegurar la red en lugar de reclamar justicia contra aquellos que la perpetraron. De hecho, en algunos casos, el descubrimiento del acceso no autorizado no hará que te promuevan a gerente; el administrador de la red o el especialista en seguridad cuyo trabajo es prevenir tales incidentes no estará muy ansioso por decirle a los jefes que los hackers encontraron un modo de violar sus medidas de seguridad.

Es importante para los gerentes percatarse de que ellos tienen un interés personal en trabajar con la policía para rastrear y presentar cargos contra los criminales cibernéticos que le cuestan tiempo y dinero a la compañía y, en algunos casos, causan daños irreparables a la reputación del negocio. Hay más probabilidad de que los gerentes cooperen con la policía si el proceso investigativo no está envuelto en un velo de misterio. La educación, como siempre, es la clave.

Resulta esencial que los gerentes, así como sus equipos de informáticos, entiendan cómo funciona una investigación criminal, su propio rol dentro de la misma y cuestiones especiales que forman parte de la recopilación, preservación y presentación de la evidencia digital. Anteriormente mencionamos que los profesionales de la informática y los oficiales del orden a veces entran en contradicción en sus esfuerzos por alcanzar un objetivo común: traer al criminal cibernético ante la justicia. Los gerentes, quienes ven dañados sus balances finales, pueden estar en una posición única de facilitar la cooperación entre ambos si han sido desde el principio una parte del equipo de lucha contra el crimen cibernético.

Resumen

Cuando hablamos de crimen cibernético no sólo hablamos de computadoras. También hablamos de personas. Comprender el crimen cibernético es el primer paso para combatirlo. Comprender a las personas en la escena del crimen cibernético – aquellos que lo cometen, las víctimas del mismo y aquellos que trabajan para detenerlo – es el primer paso hacia la comprensión del crimen cibernético.

Los criminales cibernéticos no pueden ser fácilmente comprendidos como un grupo porque realizan una gran variedad de actividades criminales muy diferentes por razones muy diferentes. Sin embargo, los podemos comprender mejor si los dividimos en categorías y analizamos cada grupo por separado. Comprender los motivos, las características y los comportamientos típicos de los criminales en cada grupo, conjuntamente con el análisis de la evidencia en cada caso en particular puede ayudarnos a crear un perfil criminal que contribuirá a identificar y capturar a los infractores.

Parte del perfil criminal incluye el estudio del tipo de persona que los criminales eligen como víctimas. La victimología también sirve a otros propósitos, nos permite predecir dónde va a dar el próximo golpe el criminal cibernético y prevenir a las futuras víctimas potenciales. Los perfiles de las víctimas también se pueden usar en operaciones encubiertas que atraen al criminal cibernético fuera del mundo virtual y hacia el mundo real.

Los investigadores del crimen cibernético necesitan tener todas las características requeridas para cualquier investigador criminal, más algunas otras extras. Los detectives del ciberespacio no sólo tienen que ser inteligentes, lógicos, objetivos, pacientes, curiosos, estar en forma físicamente, sino que además deben tener algún conocimiento y entendimiento sobre computadoras, redes, jerga técnica, el trasfondo del hacker y temas de seguridad informática. Es por eso que los investigadores de crímenes cibernéticos bien entrenados, habilidosos y talentosos son tan demandados. Las agencias de policía tendrían que pagar supersalarios para tenerlos – especialmente considerando la discrepancia entre la compensación en el sector público y el mundo corporativo para los profesionales de la informática. Sin embargo, un investigador cibernético profesional puede ser invaluable para las agencias de policía, las que pueden esperar ver que la incidencia del crimen cibernético continúe incrementándose en una cifra exponencial para el futuro inmediato.

Comprender la tecnología del crimen cibernético es fácil comparado con comprender a las personas que llevan a cabo los crímenes. El factor humano es a veces el componente más inexplicable en una investigación.

Preguntas Realizadas con Frecuencia

Las siguientes preguntas realizadas con frecuencia, respondidas por los autores de este libro, están diseñadas para medir su comprensión de los conceptos presentados en este capítulo y para ayudarle con la implementación de estos conceptos en la vida real. Para hacer que el autor conteste a sus preguntas, visite www.syngress.com/solutions y haga clic en el formulario **“Pregúntale al autor”**.

P: Las subastas en Internet se mencionan como uno de los crímenes en línea reportados con mayor frecuencia. ¿Esto significa que todas las subastas en línea son estafas?

R: No. La mayoría de las subastas en línea son legítimas. Sitios de subastas reconocidos como eBay intentan dar protecciones publicando opiniones de sus vendedores proporcionadas por personas que han hecho negocios con ellos. Los sitios de subastas generalmente colocan recomendaciones de seguridad y pautas que ayudarán a los usuarios a protegerse contra el fraude. Sin embargo, las subastas sí le ofrecen una oportunidad a

negociantes inescrupulosos de engañar a sus clientes. Es importante ser muy cuidadosos al comprar mercancías a través de un sitio de subastas.

P: ¿Por qué los estafadores continúan timando aún cuando pueden hacer más dinero realizando un trabajo legítimo o incluso cuando la estafa no los beneficia desde el punto de vista financiero – o los beneficia muy poco?

R: De acuerdo con el estudio *Impostores y Engañados: Observaciones sobre los Hombres de Confianza y sus Víctimas, Informantes y su Presa, Espías Políticos e Industriales y Ciudadanos Ordinarios*, por Richard Blum (véase www.fraudaid.com/Why-Con-artists-Scam.htm), el estafador típico es impulsivo y compulsivo y adicto a las estafas que hace porque le dan la “altura” de haber podido engañar a alguien. Blum concluye que la mayoría de los estafadores muestran los síntomas de trastorno de personalidad antisocial. De acuerdo con el *Diagnóstico y Manual Estadístico de Desórdenes Mentales*, cuarta edición (DSM-IV), que es la referencia primaria sobre diagnóstico usada por los profesionales de la salud de los Estados Unidos, las características de personas con trastornos de personalidad antisocial incluyen:

1. Problemas para cumplir con normas sociales con respeto hacia comportamientos legales como indican actos llevados a cabo repetidamente que constituyen motivos de arresto.
2. Engaños como indican las mentiras repetidas, el uso de alias o la estafa a otros para obtener ganancias personales o placer.
3. Impulsividad o problemas para continuar planeando.
4. Irritabilidad y agresividad como indican los enfrentamientos físicos o asaltos repetidos.
5. Imprudencia al no tomar en cuenta la seguridad propia o de otros.
6. Irresponsabilidad consistente como indican los problemas repetidos para mantener una actitud consistente en el trabajo u obligaciones financieras honrosas.
7. Carencia de remordimientos como indica el comportamiento de ser indiferente o de racionalizar el haber herido, maltratado o robado a otro.

P: Qué factores debería considerar una compañía antes de reclutar a hackers para trabajar como especialistas en seguridad de una compañía o especialistas en crímenes por ordenador para agencias de la policía?

R: Esta es una tendencia basada en la noción de que “se necesita un hacker para atrapar a otro” (o para proteger una red de otro hacker). Ciertamente es real que aquellos que han cometido crímenes están íntimamente familiarizados con la forma en que estos se cometen y pueden ser frustrados. La policía ha utilizado tradicionalmente la pericia de criminales, usando estudios hechos por personas condenados por crímenes. Sin embargo, las agencias de policías no considerarían contratar a antiguos ladrones como detectives de crímenes de propiedad o a asesinos condenados como investigadores de homicidios. Contratar a hackers que han infringido la ley en el pasado representa un número de problemas que ambos sectores, el privado y el público, deberían tener en mente.

Por lo pronto, muchos tipos de hackers son filosóficamente opuestos a grandes negocios. Aunque pudieran ser persuadidos de trabajar para una compañía si lograran tentarlos con enormes salarios a hacer lo que normalmente hacen – jugar con computadoras – no

encajarían de todos modos en el entorno estructurado de una compañía. Los hackers son por lo general solitarios que no siguen el modelo corporativo, lo que enfatiza el trabajo de equipo. Quizás más importante, un hacker que ha sido culpable de una actividad criminal en el pasado puede exponer a su compañía a correr riesgos sustanciales si él o ella no se ha reformado realmente. La red de su organización podría ser usada para lanzar ataques de hackeo cuando su “hacker profesional” se aburra de los deberes asignados. Esto podría dejar abierta la compañía a cuestiones de responsabilidad serias. Su hacker también podría crear “puertas traseras” en su sistema, de modo que si Usted lo despide o él se cansa de jugar el juego corporativo y se marcha, pueda regresar y tener acceso pleno a su red.

Existen especialistas en seguridad informática que son tan habilidosos como los hackers, pero que nunca eligieron utilizar sus habilidades para infringir la ley. Los oficiales de compañías deberían pensar detenidamente y considerar todas las ventajas y desventajas antes de contratar a un hacker sólo porque “es lo que se hace” actualmente. Las agencias de policía, en la mayoría de los casos, están obligadas por sus propias políticas y las reglas de su comisión estatal a no contratar personas que hayan sido condenadas por delitos criminales serios. Muchos hackers criminales, sin embargo, nunca han sido arrestados o condenados. Las agencias se están percatando finalmente de que es interés suyo contratar a personas con habilidades en computación. La mayoría de ellas realizan rigurosas investigaciones del pasado de las personas a contratar que revelan cómo ellos adquirieron sus habilidades y cómo las usaron en el pasado.

Referencias

- *Psicología Forense y Psiquiatría Forense: Una Panorámica*
<http://flash.lakeheadu.ca/~pals/forensics/forensic.htm>
- *Perfil Criminal: Cómo Comienza y Cómo se Usa*
www.crimelibrary.com/criminology/criminalprofiling2
- Base de conocimientos de los métodos de investigación de la Universidad de Cornell:
Pensamiento Deductivo e Inductivo
<http://trochim.human.cornell.edu/kb/dedind.htm>
- Monografía de la Comisión de Servicio Público de Canadá: *Estereotipando*
www.psc-cfp.gc.ca/publications/monogra/mono3_e.htm
- About.com: *No le Temas a la Muerte, Témele al Script Kiddie*
<http://netsecurity.about.com/library/weekly/aa111600a.htm>
- Buró de Estadísticas de Justicia del Departamento de Justicia de los Estados Unidos:
Infractoras
www.ojp.usdoj.gov/bjs/crimoff.htm#women
- *Integridad a la Suite Corporativa: Previsores de Fraudes Femeninos*
www.cj.msu.edu/~faculty/collinsintegrity.html

- *The Irish Times: Expertos en Seguridad ante los retos del WAP*
www.ireland.com/newspaper/finance/2000/0121/fin41.htm
- *Guía para Compradores en Línea Netaction*
www.netaction.org/shoppers/fraud.html
- *Comisión Federal de Comercio*
www.ftc.gov
- *Centro Nacional de Chequeo de Fraudes: Tipos de Crímenes de Cuello Blanco*
www.ckfraud.org/whitecollar.html
- *Enfermedades Psiquiátricas Asociadas con la Criminalidad*
www.emedicine.com/med/topic3485.htm
- *Diario de los Sistemas IBM: Hackeo Ético*, por C. C. Palmer
www.research.ibm.com/journal/sj/403/palmer.html
- *La Importancia de la Victimología en la Creación de Perfiles Criminales*, por Amy Goldman
<http://isuisse.ifrance.com/emmaf/base/impvic.html>
- *Teoría de la Victimología*, por T. O. Connor
<http://faculty.ncwc.edu/toconnor/300/300lect01.htm>

Comprendiendo los Principios Básicos de la Computación

Tópicos que investigaremos en este capítulo:

- **Comprendiendo el Hardware de la Computadora**
- **Comprendiendo el Lenguaje de la Máquina**
- **Comprendiendo los Sistemas Operativos de la Computadora**

- ✓ **Resumen**
- ✓ **Preguntas realizadas con frecuencia**
- ✓ **Recursos**

Introducción

En el Capítulo 3 mencionamos que, además de las habilidades investigativas tradicionales, un buen investigador de crímenes cibernéticos necesita un entendimiento profundo de la tecnología que se usa para cometer estos crímenes. Al igual que un investigador de homicidios debe conocer algo sobre patología humana básica para comprender el significado de la evidencia provista por los cadáveres – rigidez cadavérica, lividez, patrones de las salpicaduras de sangre, etc. – un investigador de crímenes cibernéticos necesita conocer cómo operan las computadoras como para reconocer y preservar la evidencia que ellas ofrecen.

Un principio básico de la investigación criminal es que no existe el “crimen perfecto”. No importa cuán cuidadoso sea un criminal, siempre deja algo suyo en la escena del crimen o toma algo de ella. Estas pistas pueden ser obvias o pueden estar bien ocultas o ser muy sutiles. Aunque un criminal cibernético, generalmente, nunca visita el lugar donde ocurre el crimen (la computadora o la red de destino), la misma regla de error de los crímenes tradicionales es válida: todo el que accede a una red, a un sistema o a un fichero deja una huella detrás. Criminales muy sofisticados desde el punto de vista técnico pueden ser capaces de cubrir esas huellas, al igual que los criminales cuidadosos y sofisticados son capaces de hacerlo en el mundo físico – pero, en muchos casos, ellos no destruyen completamente la evidencia, solo dificultan el encontrarla.

Por ejemplo, un ladrón podría tener el cuidado de limpiar todas las huellas digitales de todo lo que tocó durante su estancia en la residencia, borrando la evidencia más obvia y a veces la más útil que prueba que él estuvo allí. Pero si al hacerlo, pedacitos de tela del paño que usa se adhieren a alguna de las superficies y él se lleva el paño y más tarde es encontrado en posesión suya, la policía podría tener una forma de vincularlo con la escena del crimen. Asimismo, el criminal cibernético podría tener el cuidado de borrar los ficheros comprometedores de su disco duro e, incluso, ir más lejos y formatearlo. Para aquellos que no son muy habilidosos desde el punto de vista técnico parecerá que los datos desaparecieron, pero un investigador que comprenda cómo se almacena la información en el disco se dará cuenta de que la evidencia podría estar todavía en el disco, aún si no es inmediatamente visible (tanto como las huellas digitales latentes) y tomará las medidas apropiadas para recuperar y preservar esa evidencia.

Los profesionales de la informática que están leyendo este libro y que ya tienen un buen entendimiento sobre tecnología se podrían preguntar si pueden saltarse este capítulo. Nosotros les recomendamos que lo lean. Podría ser útil para aquellos que tengan previsto trabajar con oficiales de la policía y técnicos de la escena del crimen para ver la computación desde una nueva perspectiva: cómo puede servir de evidencia y cuáles detalles tecnológicos son los más importantes de comprender desde el punto de vista *investigativo*. La mayoría de los profesionales de la informática están acostumbrados a ver una computadora, el hardware de redes, los softwares y los protocolos en términos de *hacer que las cosas funcionen*. Los investigadores ven estos artículos en términos de lo que pueden revelar que sea competente, relevante y material para el caso. Un administrador de redes familiarizado con el sistema operativo de Windows, por ejemplo, sabe que es posible

mostrar en pantalla las fechas de modificación de ficheros, pero él o ella podría no haber considerado cuán crucial podría ser esta información en una investigación. Similarmente, un investigador de la policía que no es experto en tecnología podría percatarse de la importancia de la información, pero no darse cuenta de que tal información está disponible, porque no es obvia cuando el sistema operativo está utilizando la configuración por defecto. Una vez más, cada parte tiene la mitad de las piezas para el rompecabezas. Si las dos partes trabajaran en conjunto, el rompecabezas se armara mucho más rápidamente.

En este Capítulo brindamos una panorámica de cómo las computadoras procesan y almacenan la información. Primeramente analizaremos el hardware, después el software (particularmente el sistema operativo) sobre el cual las computadoras personales trabajan. Al final de cada sección, resumimos cómo la información en esa sección puede ser útil para los investigadores de crímenes cibernéticos.

Comprendiendo el Hardware de la Computadora

Hoy día, la mayoría de las personas que operan en el mundo de los negocios o como personal administrativo en el sector público se exponen a las computadoras. Sin embargo, el hecho de que ellos usen las computadoras todos los días no significa que las entiendan. Esto tiene sentido. La mayoría de nosotros conducimos autos todos los días sin que necesariamente sepamos sobre mecánica. Incluso personas con suficientes aptitudes para la mecánica como para cambiar el aceite y las bujías de su propio auto podrían no comprender realmente cómo funciona un motor de combustión interna. Similarmente, podemos encender nuestros televisores y cambiar los canales (algunos de nosotros podemos incluso programar los relojes en nuestros videos) sin saber realmente cómo se transmiten los programas vía satélite o por cable.

La mayoría de los usuarios casuales toman por sentado que si le echan gasolina al auto, este los lleva adonde quieran ir y si pagan la cuenta del servicio de cable, el show continuará. Aunque no entendamos estas tecnologías, ellas han existido el tiempo suficiente como para que nos sintamos cómodos con ellas. Para los usuarios de la “primera generación”, sin embargo, el antiguo modelo T Ford les debe haber parecido una máquina misteriosa y escalofriante e imágenes que de alguna forma volaban invisibles por el aire y aterrizaban en una pequeña caja en las salas de las personas parecían una auténtica magia para los primeros propietarios de televisores.

Debemos recordar que muchas de las personas que usan computadoras hoy día son miembros de la “primera generación” de usuarios de computadoras – personas que no crecieron con computadoras en todas las oficinas, mucho menos en casi todas las casas. Para ellos, las computadoras todavía tienen el sabor de algo mágico, algo inexplicable. Algunos investigadores criminales habilidosos entran dentro de esta categoría. Al igual que la lucha efectiva contra el crimen cibernético requiere que pongamos al tanto del proceso legal a los profesionales de la informática, también requiere que informemos del procesamiento electrónico al personal del orden – de cómo las máquinas funcionan “bajo la cubierta”.

El primer paso es abrir el chasis y observar dentro todas las partes y piezas de una computadora y lo que estas hacen, de modo que podamos comprender el papel que cada una de ellas juega en crear y retener la evidencia electrónica.

Mirando Dentro de la Máquina

Las máquinas nos han estado facilitando la vida desde hace muchos siglos. Los científicos están de acuerdo con que una de las características que distinguen al hombre de la mayoría de las otras especies es la capacidad de hacer y utilizar herramientas. De muchas maneras, las eras históricas están definidas por sus herramientas. La era agraria, cuando la mayoría de los humanos eran agricultores, le cedió el paso a la era industrial del siglo XIX, cuando las compañías productoras reinaban y la máquina de vapor y el ferrocarril proporcionaron una vía de comercializar los productos manufacturados. A principios del siglo XX, las estaciones comerciales generadoras de electricidad se esparcieron, lo que nos condujo a la era electrónica, dándole a nuestras máquinas el “poder del rayo”. Al arribar al siglo XX, nos encontramos justo a mediados de la era digital, o sea, la era de la información, en la que nos hemos convertido en dependientes de las computadoras para conducir nuestras infraestructuras nacionales (muchos sienten que nos hemos convertido en demasiado dependientes de ellas).

A pesar de lo que Usted sienta con respecto a esas máquinas, parece que estas llegaron para quedarse – por lo menos, a menos y hasta que alguna catástrofe global como un pulso electromagnético mundial de inmensas proporciones generado por el sol las deje a todas inutilizables y nos sumerja a nosotros nuevamente en el caos. Como se han vuelto más poderosas, las computadoras son capaces de realizar tareas más complejas y realizarlas a una velocidad cada vez mayor.

Sin embargo, en su nivel más básico, todo lo que una computadora hace es calcular números. Como se explicará más adelante en este capítulo, todos los datos – texto, imágenes, sonidos, programas – deben ser reducidos a números para que la computadora los “entienda”. De acuerdo con el *Diccionario de Inglés Mundial Encarta 2001* de Microsoft, la definición de una computadora es un dispositivo electrónico que acepta, procesa, almacena e imprime datos a altas velocidades de acuerdo con instrucciones preprogramadas.

Componentes de una Computadora Digital

Sin importar si es un pequeño modelo de mano o un sistema de ordenador central grande, una computadora digital está formada por los mismos componentes básicos:

- Una unidad de control
- Una unidad de procesamiento
- Una unidad de memoria
- Unidades de entrada y salida

Por supuesto, debe haber una forma para que todos estos componentes se comuniquen entre sí. La arquitectura de una PC es estándar, lo que facilita intercambiar partes entre diferentes computadoras. La base del sistema es una placa base, cariñosamente llamada *motherboard* (placa madre).

En la escena...

Computadoras Digitales vs. Computadoras Analógicas

Las máquinas en las que pensamos hoy día cuando oímos la palabra *computadora* son *computadoras digitales*. Existe otro tipo de computadora, la *computadora analógica*. Ambos tipos de máquinas realizan cálculos matemáticos, pero las computadoras analógicas representan números usando voltajes. La diferencia más importante entre las computadoras digitales y las analógicas es que los sistemas analógicos operan sobre variables continuas en lugar de añadir y sustraer dígitos. Las computadoras analógicas son consideradas obsoletas por muchos en la actualidad, pero de hecho todavía hay computadoras analógicas en uso. Algunos teóricos de la computación creen que las computadoras analógicas son realmente más poderosas que las digitales. Para una descripción de las computadoras analógicas, visite www.science.uva.nl/faculteit/museum/AnalogComputers.html. (Recursos adicionales sobre este tópico aparecen en la sección “Referencias” al final de este Capítulo).

El Papel de la Motherboard (Placa Madre)

La mayoría de los otros componentes se conectan a la placa principal y todos ellos se comunican a través de los senderos electrónicos (circuitos) que están impresos en la placa. A través de las *ranuras de expansión* se pueden añadir placas base adicionales. La interfaz electrónica entre la placa madre y estas placas adicionales, tarjetas y conectores se denomina *bus*. El bus es el camino en la placa madre que conecta a los componentes y les permite interactuar con el procesador.

La placa madre es la unidad de control de la computadora. Esta está conformada realmente por muchos componentes:

- La placa base impresa misma (PCB) que está compuesta por varias capas finas o una sola superficie bidimensional sobre la que está fijo el sistema de circuitos.
- Reguladores de voltaje que reducen la señal de 5V del suministrador de energía al voltaje requerido por el procesador (por lo general 3.3V o menos).
- Capacitores que filtran las señales.
- El chipset integrado que controla la interfaz entre el procesador y todos los otros componentes.
- Controladores para el teclado y los dispositivos de entrada y salida (SCSI integrada, sonido y videos incorporados, etc.)
- Un chip de memoria de sólo lectura programable y que puede ser borrado (EPROM) que contiene el software núcleo que hace funcionar directamente el hardware del sistema.
- Un chip CMOS operado por baterías que contiene las configuraciones del BIOS y el reloj de tiempo real que mantiene la hora y la fecha.

- Enchufes y ranuras para anexar otros componentes (procesador, memoria principal, memoria caché, tarjetas de expansión, suministrador de energía).
- Puerto y/o pines (headers) para conectar cables y dispositivos (en serie, paralelos, USB, IDE, SCSI, IR, IEEE 1394/FireWire) y conectores de pata para el conmutador, los indicadores LED, bocinas y ventilador del procesador.

La distribución y organización de los componentes en la placa madre se denomina su *factor forma*. El factor forma determina el tamaño y la forma de la placa y dónde se localizan sus puertos integrados, así como el tipo de suministrador de energía que está diseñado para usar. El tipo de chasis de la computadora debe estar acorde con el factor forma de la placa madre o las aperturas en la parte trasera del chasis no corresponderán correctamente con las ranuras y los puertos en la placa madre. Los factores forma típicos de la placa madre incluyen:

- **ATX/ mini ATX**, actualmente el factor forma más popular. Todas las placas madres Intel actuales son ATX. Los conectores de puertos y los conectores de ratón PS/2 están incorporados. El acceso a los componentes resulta por lo general más fácil y el suministrador de energía ATX proporciona una mejor ventilación para reducir los problemas de sobrecalentamiento.
- **AT/ Baby AT**, el más común de los factores forma de la placa madre de una PC anterior a 1997, todavía ampliamente utilizado. El suministrador de energía se conecta a la placa con dos conectores etiquetados P8 y P9; al revertirlos se puede destruir la placa madre.
- **LPX/Mini LPX**, generalmente usada por grandes fabricantes de computadoras de marca para ahorrar espacio en chasis pequeños. Utiliza una “placa hija” o una tarjeta aumentadora que se conecta a la placa madre. Entonces se le conectan tarjetas de expansión a la placa aumentadora.
- **NLX**, una versión modernizada y mejorada de la LPX. Este factor forma también es utilizado por vendedores de computadoras de marca.

Nota

Para un análisis más detallado sobre los componentes de la placa madre y los factores forma, véase www.pcguide.com/ref/mbsys/index.htm.

El papel del Procesador y la Memoria

Dos de los componentes más importantes en una computadora son el procesador y la memoria. Repasemos brevemente lo que hacen estos componentes.

El Procesador

El *procesador* (abreviatura de *microprocesador*) es un circuito integrado en un solo chip que realiza los cálculos básicos en una computadora. A veces el procesador es denominado CPU (*unidad central de procesamiento*), aunque muchos usuarios de computadoras usan ese término para referirse a la “caja” de la PC – el chasis y su contenido – sin monitor, teclado y otros periféricos externos.

El procesador es la parte de la computadora que hace todo el trabajo de procesamiento de datos. Los procesadores reciben entrada en forma de cadenas de unos y ceros (denominada *comunicación binaria* que analizaremos más adelante en este capítulo) y usan circuitos lógicos o fórmulas para crear la salida (también en forma de unos y ceros). Este sistema se implementa a través de conmutadores digitales. En las primeras computadoras, los tubos de vacío eran usados como conmutadores. Más tarde fueron reemplazados por los *transistores*, que eran mucho más pequeños y rápidos y no tenían partes movibles (convirtiéndolos en conmutadores de *estado sólido*). Entonces los transistores se agruparon para formar chips de *circuitos integrados*, hechos de materiales (particularmente de silicona) que conducen la electricidad sólo en condiciones específicas (en otras palabras, un *semiconductor*). A medida en que un solo chip se fueron incluyendo más y más transistores, los chips se fueron tornando cada vez más pequeños y menos costosos de hacer. En 1971, Intel fue la primera en usar esta tecnología para incorporar algunos componentes lógicos separados en un chip y llamarlo *microprocesador*.

Los procesadores son capaces de realizar diferentes tareas usando instrucciones programadas. Los sistemas operativos modernos permiten aplicaciones múltiples para compartir el procesador usando un método conocido como *time-slicing* o *división del tiempo en slots*, en el cual el procesador trabaja sobre datos de una aplicación, después conmuta para la próxima (y la próxima y la próxima) tan rápidamente que al usuario le parece que todas las aplicaciones están siendo procesadas simultáneamente. Este método se denominado *función multitareas* y existen un par de formas en que estas pueden ser acometidas. Algunas computadoras tienen más de un procesador. Con el fin de aprovechar los procesadores múltiples, la computadora debe correr un sistema operativo que soporte el multiprocesamiento. Analizaremos la función multitarea y el multiprocesamiento con más profundidad en la sección “Comprendiendo los Sistemas Operativos de las Computadoras” más adelante en este capítulo.

El procesador en sí es una pieza ultra-fina de cristal de silicona, de menos de 1 milímetro de grosor que tiene millones de conmutadores electrónicos diminutos (transistores) incrustados en ella. Esta incrustación se hace mediante una *fotolitografía*, donde se trata de fotografiar el patrón del circuito y grabarlo químicamente sobre el fondo. El chip es una parte de un *wafer* que es una pieza redonda de sustrato de silicio sobre la cual están grabados de 16 a 256 chips individuales (en dependencia del tamaño del *wafer*). Entonces los chips se *encapsulan*, que es el proceso de cotejar los diminutos puntos de conexión en el chip con los pines que conectarán el procesador al enchufe de la placa madre y revestir el chip frágil con una cubierta externa.

Nota

El embalaje del procesador determina el tipo de ranura o enchufe que le acoplará. Los estilos de embalajes incluyen el DIP (Dual Inline Package), el PGA (Pin Grid Array) y sus variaciones (un embalaje cuadrado plano que se conecta a un enchufe en la placa madre con una serie de pines como en la Intel 80286 hasta la 80486 y en las primeras Pentium) y el SEC (Single Edge Contact) que monta el chip sobre una pequeña placa base (a veces llamada *tarjeta hija*), cuyo borde se conecta a una ranura en la placa madre. Las computadoras portátiles a veces tienen el chip del

procesador soldado directamente a la placa madre para ahorrar espacio o usan un módulo móvil especial que incluye el procesador, el caché secundario y el chipset.

Antes de ser encapsulados, los chips son probados para asegurarse de que realicen sus tareas apropiadamente y para determinar su velocidad. La velocidad del procesador depende de la calidad de la producción, del diseño del procesador, de la tecnología del proceso, del tamaño del circuito y del troquelado. Los chips más pequeños generalmente pueden correr más rápido, porque generan menos calor y utilizan menos energía. A medida que los chips han disminuido en tamaño, se han tornado más rápidos. El tamaño del circuito del chip del procesador original 8088 era de 3 micrones; los chips de las Pentium modernas son de 0.25 micrones o menos. El sobrecalentamiento disminuye el rendimiento y mientras más energía se usa, más se calienta el chip. Por esta razón, los nuevos procesadores trabajan a voltajes más bajos que los antiguos. También están diseñados como chips de doble voltaje, en el cual el *voltaje principal* (el interno) es menor que el *voltaje de entrada/salida* (el externo). La misma placa madre puede soportar procesadores que usen voltajes diferentes, porque tienen reguladores de voltaje que convierten el voltaje de la fuente de energía en el voltaje requerido por el procesador que está instalado.

Aún trabajando a voltajes más bajos, los procesadores modernos de alta velocidad se calientan mucho. Los disipadores de calor y los ventiladores del procesador ayudan a conservar baja la temperatura. Una práctica popular con hackers y aficionados al hardware denominada *overclocking* (configurar el procesador para que trabaje más rápido de lo normal) causa que los procesadores se sobrecalienten fácilmente. Para enfrentar este problema existen elaborados y costosos sistemas de enfriamiento por agua y refrigeradores Peltier que funcionan como minúsculos aires acondicionados de estado sólido.

Nota

Para más información acerca de cómo funciona el llamado *overclocking* de procesadores, véase www.hiphardware.com/editorials/overclocking/index.shtml. Numerosos sitios Web como www.overclockers.com y www.overclockershideout.com proporcionan consejos sobre esta práctica y venden productos de enfriamiento y otros accesorios afines.

Memoria del Sistema

El término *memoria* se refiere a un chip donde se almacenan los datos. Algunos usuarios de computadoras novatos podrían confundir los términos *espacio en disco* y *memoria*. Es por eso que Usted escucha la pregunta, “¿Cuánto me queda de memoria en mi disco duro?” En un sentido, el disco realmente sí “recuerda” datos. Sin embargo, el término *memoria* es más apropiado usarlo para describir un chip que almacena datos de forma temporal y es más comúnmente usado para referirse a la *memoria del sistema* o a la *memoria de acceso aleatorio (RAM)* que almacena las instrucciones con las cuales el procesador está trabajando actualmente y los datos que están siendo procesados actualmente. En otras partes de la computadora se usan chips de memoria de varios tipos: existen memorias caché, memoria de video, etc. La RAM es llamada memoria *de acceso aleatorio* porque los datos se pueden leer desde cualquier lugar de la memoria en cualquier orden.

La cantidad de RAM instalada en su computadora influye en la cantidad de programas que se pueden abrir simultáneamente y en el rendimiento de la computadora. La memoria es un sistema común de *embotellamiento* (o sea, es el componente más lento en el sistema que ocasiona que otros componentes trabajen a una velocidad menor a la de su rendimiento potencial). Los datos que se almacenan en la RAM, a diferencia de los datos almacenados en discos o en algunos otros tipos de memorias, son volátiles. Esto significa que los datos se pierden cuando está apagado el sistema o cuando no hay energía.

Cada chip de RAM tiene un gran número de *direcciones* de memoria o *celdas*, organizadas en filas y columnas. Un solo chip puede tener millones de celdas. Cada dirección guarda un número específico de bits de datos. En un *módulo de memoria* se combinan múltiples chips, el cual es una pequeña placa base que Usted inserta en una ranura de memoria en la placa madre de la computadora. Estos módulos se denominan SIMMs (*módulos de memoria simple en línea*) o DIMMs (*módulos de memoria dual en línea*). El controlador de memoria, que es parte del chipset de la placa madre, es el “policía de tránsito” que controla qué chip de memoria va a ser escrito o leído en un momento dado. ¿Cómo van los datos de la memoria al procesador? Toma un bus – el bus de memoria (o bus de datos), eso es. Como mencionamos anteriormente, un *bus* es un canal que lleva las señales electrónicas que representan a los datos de un componente a otro dentro de la PC.

La RAM puede ser leída y escrita. Las computadoras usan otro tipo de memoria, la ROM (*memoria de sólo lectura*) para almacenar programas importantes que necesitan estar disponibles permanentemente. Un tipo especial de ROM, mencionado anteriormente, la EPROM (una ROM programable que se puede borrar) se usa en situaciones en las que Usted podría necesitar cambiar, ocasionalmente, pero no a menudo, los datos. Una función común de la EPROM (o EEPROM que es una PROM que se puede borrar eléctricamente) es almacenar programas BIOS “actualizables”, los cuales, por lo general, permanecen igual, pero podrían necesitar ser actualizados ocasionalmente. Técnicamente, la EPROM no es de sólo lectura el 100% del tiempo, pues puede ser borrada y re-escrita, pero la mayoría de las veces sólo es leída, no escrita. Los datos almacenados en la ROM (incluyendo la EPROM) *no* se pierden cuando se apaga el sistema.

Otro tipo de memoria usado en las PC es la *memoria caché*. La memoria caché es mucho más rápida que la RAM, pero también mucho más costosa, así que existen menos de estas. La memoria caché almacena los datos a los que se ha accedido recientemente. Está organizada en capas entre la RAM y el procesador. La primaria o de nivel 1 (L1) es la más rápida; cuando el procesador necesita una parte específica de datos, el controlador de la caché la busca primeramente en la caché L1. Si no está ahí, el controlador va hacia la secundaria o la caché L2. Si el controlador aún no encuentra los datos, entonces busca en la RAM. Cuando fue escrito este libro, la memoria caché L1 costaba aproximadamente 100 veces lo que costaba una RAM normal o una SDRAM, mientras que la caché L2 costaba de 4 a 8 veces el precio de la RAM más costosa en el mercado. La caché acelera considerablemente el procesamiento, porque, estadísticamente, es probable que los datos usados más recientemente se vuelvan a necesitar. Tomándolos de la memoria caché más rápida en lugar de de la memoria RAM más lenta se incrementa el rendimiento general.

Nota

Existen otros tipos de caché además de la memoria caché del procesador. Por ejemplo, los visualizadores Web crean una caché en el disco duro donde almacenan las páginas Web a las que accedieron recientemente, de modo que si se requieren nuevamente estas mismas páginas, el visualizador puede acceder a ellas desde el disco duro local. Este sistema es más rápido que navegar en Internet para descargar nuevamente las mismas páginas. La palabra *caché* (pronunciada “cash”) significaba originalmente “un lugar secreto donde se almacenan cosas” y de manera apropiada, la caché de la Web puede ser una valiosa fuente de información que podría ser de utilidad a los investigadores, como analizaremos en el Capítulo 10 “Recopilando y Preservando la Evidencia Digital”.

La memoria caché usa una RAM estática (SRAM) en lugar de una RAM dinámica (DRAM) que se utiliza para la memoria del sistema. La diferencia es que la SRAM no requiere de un refrescamiento periódico para conservar los datos que están almacenados allí, como es el caso de la DRAM. Esto hace que la SRAM sea más rápida. Sin embargo, la SRAM, al igual que la DRAM, pierde sus datos cuando la computadora se apaga.

El Papel de los Medios de Almacenamiento

El término *medios de almacenamiento* se emplea, generalmente, para referirse a los medios de almacenar datos permanentemente (o sea, almacenamiento no volátil que retiene los datos sin energía eléctrica). Los datos se pueden almacenar más o menos permanentemente en diferentes tipos de medios, incluyendo:

- Discos duros
- Discos flexibles
- Discos compactos (CD) y discos versátiles digitales/ de video (DVD)
- Cintas
- Memoria Flash (CompactFlash, SmartMedia, Memory Stick)
- Otros medios desmontables (discos Zip y Jaz, microdrives, magneto-ópticos)

Echémosle una mirada breve a cómo funcionan estos medios.

Discos Duros

Hoy día, el disco duro es generalmente el medio primario de almacenamiento permanente en una computadora. Sin embargo, las primeras PC no tenían discos duros. De hecho, las primeras computadoras (antes de la PC) no tenían ningún tipo de medio de almacenamiento de datos. Usted tenía que teclear en cada programa que quisiera abrir, cada vez que lo abriera. Más tarde, se utilizaron las fichas perforadas o cintas para almacenar programas y datos. El próximo avance tecnológico nos trajo el almacenamiento en cintas magnéticas. Las grandes unidades centrales utilizaban grandes rollos de cinta, mientras que las primeras microcomputadoras usaban cintas de audio casetes para almacenar programas y datos. Cuando la computadora IBM y sus clones aparecieron, las computadoras estaban utilizando

discos flexibles (del tipo de 5.25 pulgadas que realmente eran flexibles). Modelos más costosos tenían dos torres de disco flexible, una para descargar programas y una segunda para salvar datos – pero todavía no tenían disco duro.

Estadísticas Cibernéticas

Tamaños de los Discos Duros

La IBM introdujo su primer disco duro en 1956, pero el verdadero “abuelo” de los actuales discos duros fue la torre Winchester, que no fue introducida hasta los años 70. El tamaño físico estándar de los discos en aquel tiempo era de 14 pulgadas (el tamaño de los platos que están amontonados para conformar el disco). En 1979, la IBM hizo un disco de 8 pulgadas y Seagate le siguió los pasos en 1980 con el primer disco duro de 5.25 pulgadas que fue usado en las primeras PC. Tres años más tarde, los discos se hicieron aún más pequeños; se introdujo el disco de 3.5 pulgadas. Este se convirtió en un estándar para las PC. Discos mucho más pequeños (menos de 2 pulgadas) fueron creados más tarde para su uso en laptop y computadoras portátiles. La “microtorre” de la IBM redujo el diámetro del plato a 1 pulgada.

El tamaño de los platos de un disco duro se denomina su *factor de forma*. Las dimensiones pequeñas de platos hacen más que ahorrar espacio dentro de la computadora; también mejoran el rendimiento del disco (ahorran tiempo), porque los cabezales no tienen que moverse tanto.

Los primeros discos duros que venían con las PC proporcionaban un espacio de almacenamiento de 5MB – una gran cantidad comparada con la de los discos flexibles. La PC XT de la IBM vino con un disco duro gigantesco de 10MB. Los discos duros actuales están alcanzando capacidades de 200GB a precios mucho menores que los de aquellos discos que, en comparación, eran diminutos. A pesar del hecho de que son mucho más grandes, más rápidos, menos frágiles y más confiables, los discos duros de hoy día están diseñados básicamente de la misma forma que aquellos de años atrás.

Los discos duros están compuestos por uno o varios *platos* (discos redondos y planos). Los platos están apilados uno sobre otro sobre un eje que rueda a través de un orificio en el medio de cada plato, como los LP en los tocadiscos antiguos. Hay un motor anexo al eje que hace rotar los platos, el cual está hecho de algún material rígido (generalmente aleación de aluminio o un cristal compuesto) y están cubiertos de una sustancia magnética. Los *cabezales* electromagnéticos escriben información en los discos en forma de impulsos magnéticos y leen de ellos la información grabada.

Los datos pueden escribirse en ambas caras de cada plato. La información se graba en *pistas*, que son círculos concéntricos en los que se escriben los datos. Las pistas se dividen en *sectores* (unidades más pequeñas). Por ende, un bit particular de datos reside en un sector específico de una pista específica en un plato específico. Más adelante en este capítulo, cuando analicemos los sistemas operativos de las computadoras y los sistemas de ficheros, Usted verá cómo se organizan los datos de modo que los usuarios puedan localizarlos en el disco.

Los discos duros generalmente se conectan a la placa madre de la computadora a través de una de las siguientes interfaces:

- Sistema Electrónico Integrado/Mejorado (IDE/EIDE), denominado así porque el controlador del disco está dentro o integrado a la placa lógica del disco. También se refieren a él como ATA (Anexo de Tecnología Avanzada), un estándar del Instituto Nacional Americano de Estándares (ANSI). Casi todas las placas madres de las PC modernas incluyen dos conectores EIDE. A cada conector se pueden conectar hasta 2 dispositivos ATA (discos duros o torres de CD-ROM) en una *configuración Terminal maestro/esclavo*. Uno realiza las funciones de “maestro”, el cual responde primero a pruebas o señales en el *interrupción* (una señal de un dispositivo o programa para el sistema operativo que ocasiona que este se detenga brevemente para determinar qué tarea debe hacer a continuación) que es compartida con el otro, la torre “esclava” que comparte el mismo cable. Las configuraciones programables por el usuario en las torres determinan cuál actuará como maestro, esclavo o controlado por cable. Si este último es seleccionado por ambas torres, la primera torre de la cadena será la Terminal maestro.
- Interfaz pequeña del Sistema Computarizado (SCSI, que se pronuncia “scuzzy”), otro estándar ANSI que proporciona una transferencia de datos más rápida que el IDE/EIDE. Algunas placas madres tienen conectores y controladores SCSI dentro de su estructura. Para aquellas que no los tienen, Usted puede adicionar discos SCSI instalando una tarjeta controladora SCSI en una de las ranuras de expansión. Existen varias versiones diferentes de SCSI. Formas posteriores proporcionan tasas de transferencia más rápidas y otras mejoras. Los dispositivos se pueden “encadenar” en un bus SCSI, cada uno con un número de identificación diferente. En dependencia de la versión del SCSI, los SCSI con ID 8 o 16 pueden anexarse a un controlador (con el controlador usando un identificador, por ende permitiendo que el SCSI 7 o 15 sea periférico).

Nota

Para mayor información acerca de la SCSI, incluyendo comparaciones entre la SCSI y otras interfaces de disco, véase los artículos que aparecen en www.scsi-planet.com/vs.

Aunque la mayoría de los discos duros usan la interfaz IDE/EIDE o la SCSI, existen otras maneras de conectar discos a Su computadora. La micro-torre, mencionada anteriormente, se conecta a través de una tarjeta PC (también llamada PCMCIA por la Asociación Internacional de Tarjetas de Memoria para Computadoras Personales que creó el estándar). También se encuentran disponibles las unidades de disco FireWire (IEEE 1394) y USB.

Los datos escritos en un disco duro generalmente permanecen allí a menos o hasta que son sobrescritos por más datos o borrados físicamente por un magneto. Con la cancelación simple de los datos empleando las utilidades de administración de ficheros del sistema operativo el usuario *no* se deshace de ellos. Sólo elimina el puntero usado por el sistema de ficheros para localizarlos físicamente en el disco. Los datos en sí (en forma de cambios físicos realizados a la superficie magnética del disco) continúan todavía allí y se pueden recuperar utilizando un programa especial de recuperación.

Muchos usuarios piensan que al formatear un disco duro borran todos sus datos, pero esto no ocurre necesariamente así. El formateo define la estructura del disco. El *formateo de bajo nivel* (LLF), que define físicamente en qué parte del disco se encuentran las pistas y los sectores, sí borra los datos. Sin embargo, los discos modernos son formateados a bajo nivel en la fábrica. Los usuarios no realizan formateos de bajo nivel en los discos IDE y SCSI actuales. Entonces, cuando analizamos el formateo, generalmente estamos hablando del *formateo a alto nivel* (HLF). Este término se refiere al proceso de definición de la estructura del sistema de ficheros. Por lo tanto, decimos que un disco ha sido formateado en FAT o NTFS (sistemas de ficheros que analizaremos posteriormente en este capítulo).

Antes de que podamos formatear un disco duro, tenemos que fragmentarlo. Esto significa dividir el disco en *volúmenes*, los que generalmente aparecen para el sistema operativo como *unidades lógicas*, identificadas por diferentes letras. El disco está dividido en unidades lógicas para conseguir un mejor rendimiento y una mejor organización de los datos. Cada unidad lógica puede formatearse por separado. Por supuesto, Usted puede fragmentar el disco como una partición simple. Los esquemas y las herramientas de fragmentación varían en dependencia del sistema operativo y del sistema de ficheros. Opuesto a la creencia popular, el FDISK y otras utilidades de fragmentación no borran los datos en un disco, ellos sólo borran y manipulan las tablas de partición. Aunque herramientas como Partition Magic previenen de que su uso borrrá los datos en un disco, esto no es cierto. La advertencia está concebida para el usuario promedio que no será capaz de recuperar los datos después de haber usado dicha utilidad. Sin embargo, las técnicas profesionales de recuperación de datos aún *pueden* recuperar los datos (aunque los datos podrían estar *fragmentados* – o sea, el contenido de un fichero podría estar esparcido por diferentes áreas del disco y podría recuperarse en bits y pedazos).

En la escena...

Dejando Limpio un Disco Duro

Existen formas de borrar completamente los datos en un disco, pero el usuario promedio (y el criminal cibernético promedio) no tomará, por lo general, estas medidas. Los softwares que dejan el disco en “cero” lo hacen sobrescribiendo todos los unos y los ceros que conforman los datos en el disco y reemplazándolos con ceros. Estos programas son denominados a menudo programas de “limpieza”. Algunos de estos programas hacen varios pases, sobrescribiendo lo que ya fue sobrescrito recientemente para una mayor seguridad. Sin embargo, en algunos casos, las pistas de datos en el disco son más amplias que la corriente de datos que se escribió sobre ellas. Esto significa que algunos de los datos originales aún podrían estar visibles y ser recuperables con técnicas sofisticadas.

Un potente magneto también puede borrar o mezclar los datos en un medio magnético. Este proceso se denomina *desmagnetización*. Generalmente torna inutilizable el disco sin restaurar las pistas de sincronización instaladas en la fábrica. Habría que desmantelar los platos para borrar completamente todos los datos en cada uno de ellos, pero existe un equipo en el mercado que desmagnetizará todos los platos dejándolos intactos.

En entornos de muy alta seguridad como operaciones sensibles del gobierno, los discos que contienen información clasificada, por lo general, se destruyen físicamente (se pulverizan, incineran o se exponen a un abrasivo o ácido) para evitar la recuperación de los datos.

Unidad de Almacenamiento Desmontable

Existen varios tipos populares de *medios desmontables*, denominados así porque el disco en sí está separado de la *unidad*, el dispositivo que lee y escribe en él. Por supuesto, algunos discos duros se pueden separar de la computadora. Los racks and bays del disco desmontable le permite a Usted introducir o sacar fácilmente una unidad de disco duro IDE o SCSI de la docking bay que permanece conectada a la ATA de la computadora o a la interfaz SCSI. Las unidades de disco duro también se pueden insertar en bays externos que se pueden conectar o desconectar fácilmente del puerto USB de la computadora. La distinción es que en esos casos Usted está extrayendo la *unidad entera*, no solamente el disco, mientras que con el verdadero medio de almacenamiento desmontable, la unidad permanece conectada a la computadora y sólo el medio – disco, cinta o tarjeta – es extraído. Los medios desmontables incluyen los siguientes:

- **Discos flexibles o disquetes** En los primeros tiempos de las computadoras personales los discos flexibles eran grandes (primero de 8 pulgadas, más tarde de 5.25 pulgadas de diámetro), finos y flexibles. Los “floppies” actuales, por lo general y con más precisión llamados *disquetes*, son más pequeños (3.5 pulgadas), rígidos y menos frágiles. El disco que se encuentra dentro de la cubierta del disquete es plástico, cubierto de un material magnético. La unidad en la que Usted inserta el disquete contiene un motor para hacer girar el disquete de modo que los *cabezales* de la unidad, hecho de diminutos electro-magnetos, puedan leer y escribir en diferentes lugares del disquete. Los disquetes estándares soportan hoy 1.44MB de datos. La tecnología SuperDisk (creada por Imation Corporation) brinda una capacidad de almacenamiento de 120MB o 240MB en disquetes del mismo tamaño.

- **CD y DVD** Los CD y DVD son discos rígidos que miden un poco menos de 5 pulgadas de diámetro, hechos de un plástico duro con una fina capa de revestimiento. Los CD y los DVD se denominan *medios ópticos* porque las unidades de CD y DVD usan un rayo láser junto con un sensor opto-electrónico para escribir y leer los datos que están “quemados” en el material de revestimiento (un compuesto que cambia de reflectante a no reflectante cuando el láser lo calienta). Los datos están codificados en forma de huecos o baches increíblemente minúsculos en la superficie del disco. Los CD y DVD funcionan de forma similar, pero los últimos pueden almacenar más datos porque los huecos y las pistas son más pequeños, ya que los DVD usan un método más eficiente de corrección de errores (que usa menos espacio) y porque los DVD pueden tener dos capas de almacenamiento en cada lado en lugar de una sola.

- **Cinta** La cinta magnética es una forma relativamente barata de unidad de almacenamiento desmontable, especialmente para hacer copias de seguridad de datos. Es menos útil para datos a los que uno necesita tener acceso frecuente porque es un medio de *acceso secuencial*. Usted tiene que correr la cinta hacia delante o hacia atrás para localizar los datos que desea. En otras palabras, para ir del fichero 1 al 20, Usted tiene que recorrer

todos los ficheros del 2 al 19, por el contrario de los medios de *acceso directo* como los discos, en los que los cabezales se pueden mover directamente al sitio donde se encuentran los datos a los que Usted desea acceder sin tener que ir de uno en uno por todos los otros ficheros.

▪ **Memoria Flash** Las tarjetas de memoria flash y los sticks son populares por almacenar y transferir pequeñas cantidades de datos (por lo general de 8MB a 512MB). Por ejemplo, se usan comúnmente para almacenar fotos en cámaras digitales (y transferirlas después a la computadora) y para almacenar y transferir programas y datos entre computadoras de mano (PC de bolsillo y dispositivos Palm OS). Aunque llamada “memoria”, a diferencia de la RAM, el medio flash es de almacenamiento no volátil. Eso significa que los datos son retenidos hasta que son deliberadamente borrados o sobrescritos. Las tarjetas flash y los sticks incluyen Compact Flash, tarjetas SmartMedia y stick de memoria de la Sony. Las tarjetas de memoria flash PCMCIA también están disponibles en el mercado. Los lectores/escribtores de memoria flash vienen en muchas computadoras de mano y en algunas laptop o computadoras cuaderno y los lectores externos se pueden conectar a la PC a través del puerto USB o el puerto serie.

▪ **Otros medios desmontables** Existen otros tipos de medios desmontables tales como los venerables discos Zip y Jaz hechos por Iomega que contienen uno o más platos de disco duro en una cartuchera desmontable que se inserta en una unidad (que contiene el motor y los cabezales). Iomega introdujo recientemente cartucheras Peerless de gran capacidad y unidades para hacerle copias de seguridad a discos duros grandes (de hasta 20GB). La tecnología magneto-óptica (MO) utiliza una combinación de las tecnologías magnética y óptica por láser.

Siguen apareciendo nuevas opciones de unidades de almacenamiento desmontables. Estas son muy cómodas en un mundo en el que la computación se va tornando cada vez más móvil. Tecnologías como el almacenamiento holográfico están en desarrollo y se espera que haya un gran crecimiento de las capacidades de almacenamiento de datos en el futuro.

Nota

Para mayor información acerca de las posibilidades teóricas de las técnicas de almacenamiento holográficas, véase el artículo del *Scientific American* “En el horizonte: Almacenamiento Holográfico” en el sitio Web de la revista: www.sciam.com/2000/0500issue/0500toigbox5.html

¿Por qué Esto le Conciérne al Investigador?

¿Por qué el investigador de un crimen cibernético necesita saber la diferencia entre la RAM y el espacio en disco, qué hace un microprocesador o la función de la memoria caché? Comprender qué hace cada parte de la computadora garantiza que Usted también comprenda en qué lugar de la máquina podría estar la evidencia (datos) que necesita – y donde *no* perder su tiempo buscándola.

Por ejemplo, si Usted sabe que la información en la RAM se pierde cuando se apaga el equipo, Usted tendrá más cuidado de no apagar inmediatamente una computadora que va a ser confiscada por orden judicial. Usted querrá evaluar la situación: ¿Fue capturado el

sospechoso mientras trabajaba en la computadora? La información en la que estaba trabajando el sospechoso *no* se salvará necesariamente si Usted apaga el sistema. El contenido de las sesiones de chateo abiertas, por ejemplo, podría perderse para siempre si no se guarda automáticamente. Usted querrá considerar el mejor modo de preservar estos datos volátiles sin comprometer la integridad de la evidencia. Usted podría salvar los datos actuales, imprimir lo que aparece en pantalla o incluso hacer que su fotógrafo de la escena del crimen tome fotos de la pantalla para evitar que se pierda la información en la RAM.

Comprender cómo se almacenan los datos y cómo se accede a ellos desde el disco duro y los medios desmontables le ayudará a reconocer por qué a menudo se pueden recuperar los datos aún cuando el criminal cibernético piensa que los “borró”, eliminando simplemente los ficheros o formateando el disco.

Los investigadores también deberían estar conscientes de las muchas opciones que existen de medios desmontables que le permiten a los criminales cibernéticos almacenar datos, que son evidencia, en un lugar aparte de la computadora, transferir fácilmente los datos a otra computadora o hacer copias de los datos que se pueden usar en caso de que los originales en el disco duro de la computadora sean destruidos. La presencia de cualquier unidad de medios desmontables (disquete, CD-R, cinta, etc.) significa que definitivamente existe una posibilidad de que los hayan salvado y se los hayan llevado. Desafortunadamente, la ausencia de tales unidades no niega la posibilidad, porque muchos medios desmontables son externos y portátiles, pueden ser trasladados fácil y rápidamente de una computadora a otra conectándolos a la máquina a través de un puerto serial, paralelo, USB u otro.

El Lenguaje de la Máquina

El hardware de la computadora y los accesorios como discos duros y medios desmontables podrían proporcionar la evidencia física de un crimen cibernético. Sin embargo, en la mayoría de los casos el hardware en sí no es realmente la evidencia; este sólo *contiene* la evidencia. De modo similar, una carta escrita por un criminal pudiera considerarse evidencia, pero la página física y la tinta no son las que demuestran la culpabilidad, sino las palabras escritas en la página que indican el estado mental culpable del criminal o que dan una confesión escrita de los actos del criminal. Si esas palabras están en un idioma que la policía, los fiscales y el jurado pueden entender, usarlas como evidencia resulta fácil. Por otra parte, si las palabras están escritas en un idioma extranjero, usarlas como evidencia podría resultar más difícil, porque tendrían que ser traducidas por una persona que comprenda ambos idiomas.

En un sentido, la mayoría de los datos de la computadora están escritos en un idioma extranjero. Los datos almacenados en computadoras están escritos en el “lenguaje” de unos y ceros o *lenguaje binario* (también llamado *lenguaje de máquina* o *código de máquina*). Aunque relativamente pocos humanos pueden programar en puro lenguaje de máquina y pocos investigadores de crímenes cibernéticos aprender a traducir la codificación magnética que representa los unos y ceros en un disco a datos “reales” (comprensibles), resulta útil para los investigadores comprender cómo funciona el lenguaje binario en aras de

anticiparse a preguntas que pudieran surgir por parte de la defensa en un caso donde se presentan datos electrónicos como evidencia.

En la escena...

Llegando al Nivel más Bajo

El lenguaje de máquina es el nivel más bajo del lenguaje de programación. El próximo escalón hacia arriba es el *lenguaje ensamblador*, que le permite a los programadores utilizar nombres (o *nemotécnicos*) representados por caracteres ASCII en lugar de sólo números. El código escrito en lenguaje nemotécnico es traducido al lenguaje de máquina por un programa llamado *ensamblador*.

Sin embargo, la mayoría de los programadores escriben sus códigos en *lenguajes de alto nivel* (por ejemplo, BASIC, COBOL, FORTRAN, o C++). Los lenguajes de alto nivel son más “amistosos” que otros lenguajes en cuanto se asimilan más a los lenguajes que los humanos leen y escriben para comunicarse mutuamente y menos al lenguaje de máquina que las computadoras “comprenden”. Aunque para las personas resulta más fácil trabajar con ellos, los lenguajes de alto nivel se deben convertir en lenguaje de máquina para que la computadora use el programa. Esto lo hace un programa denominado *compilador*, que reorganiza las instrucciones en el código fuente, o un *intérprete*, que inmediatamente ejecuta el código fuente. Debido a que muchas plataformas electrónicas diferentes emplean diferentes lenguajes de máquina, existen diferentes compiladores para un solo lenguaje de alto nivel que hace que el código corra en diferentes plataformas.

Paseando por un Mundo de Números

Trabajar con números, más allá del método primitivo de representar simplemente cada artículo contado como uno (por ejemplo, tallar una muesca en el escritorio de madera del investigador por cada caso resuelto), requiere que usemos un *sistema base* para agrupar artículos de modo ordenado, de manera que nos sea más fácil seguir la cuenta.

¿Quién está en cuál base?

La mayoría de nosotros está bien familiarizado con el sistema numérico de base 10, también denominado *sistema numérico decimal*. Muchas fuentes le otorgan el crédito a las primeras culturas Indias de haber creado este sistema numérico hace aproximadamente 5000 años; más tarde fue refinado en el mundo árabe. Este sistema usa 10 dígitos (del 0 al 9) para representar todos los números posibles. El valor de cada dígito depende de su *lugar*. Mientras Usted se mueve a la izquierda al leer el número, cada lugar representa 10 veces el valor de su derecha. O sea, que el dígito 1 puede representar 1, 10, 100, 1000, etc. en dependencia de su lugar como lo define el número de dígitos hacia su derecha. Un *punto decimal* se usa para permitir que números menores que 1 se representen.

Nosotros usamos la base 10 todo el tiempo, es nuestro sistema numérico día a día. Cuando vemos un número decimal como el 168, entendemos que el 1 representa un *cien*, el 6

representa seis *diez* y el 8 representa ocho *unos*, basados en el lugar ocupado por cada dígito en relación con los otros.

La base 10 funciona bien para el conteo humano porque tenemos 10 dedos (también llamados *dígitos*) que podemos usar para contar. Los historiadores creen que esto explica el desarrollo y la popularidad del sistema numérico decimal. Los pueblos primitivos consideraban que era fácil contar hasta 10 con sus dedos y después hacer una marca en la arena o en la piedra para representar cada grupo de 10.

Sin embargo, las computadoras funcionan con impulsos eléctricos que tienen dos estados discretos. Usted puede visualizar este sistema al pensar en un interruptor estándar de luz. El bombillo puede estar en uno de los dos estados posibles en un momento dado: encendido o apagado. Esto es una señal *digital*. Nosotros no tenemos 10 estados diferentes para representar los 10 dígitos del sistema decimal a la computadora, pero sí podemos representar todos los números posibles usando el sistema numérico de base 2, también llamado *sistema numérico binario*.

Comprendiendo el Sistema Numérico Binario

El sistema numérico binario usa sólo dos dígitos, 0 y 1. Cada dígito binario (0 o 1) se denomina *bit*. En la numeración binaria, como en la decimal, el valor de un dígito está determinado por su lugar. Sin embargo, en el binario, cada lugar representa dos veces el valor del lugar hacia su derecha (en lugar de 10 veces como en el de base 10).

Nota

Un *byte* generalmente equivale a 8 bits. Los bytes son las unidades que las computadoras usan por lo general para representar un carácter (una letra del alfabeto, un número o un símbolo). Ocho bits también se denominan un *octeto*, especialmente en el contexto de las direcciones IP.

Esto significa que el número binario *1000* no representa un mil, sino que representa ocho (su equivalente decimal) porque ese es el valor del cuarto lugar a la izquierda. Un cero es un ocupante que indica que ese lugar no tiene valor y un uno indica que un lugar tiene el valor asignado a él. Por lo tanto, *1111* representa 15 en decimal, porque cada lugar (empezando desde la derecha) tiene un valor de 1, 2, 4 y 8. Al sumar estos valores resulta 15.

Convirtiendo de Binario a Decimal

Aunque los procesadores de las computadoras deben trabajar con numeración binaria, los humanos preferimos trabajar con sistemas numéricos que utilizan más dígitos, porque resulta menos confuso para nosotros lidiar con un número que luce como el 139 que con su equivalente binario: 10001011.

La tabla 4.1 muestra los valores de los primeros 12 lugares de un número binario, comenzando desde la derecha. Si el dígito binario es un 1, el valor mostrado se le asigna a este; si es un 0, no se le asigna valor alguno. La segunda línea de la tabla muestra los dígitos de un típico número binario.

Tabla 4.1 Valores por lugar de los dígitos binarios

Valor	2048	1024	512	256	128	64	32	16	8	4	2	1
Dígito	1	1	0	1	0	0	0	1	1	0	0	1
Binario												

Al observar este número binario, 110100011001, vemos que los bits que están “encendidos” (representados por los 1) tienen valores de 1, 8, 16, 256, 1024 y 2048. Si sumamos todos estos valores, obtenemos 3353. Este es el equivalente decimal del número binario.

Convirtiendo de Binario a Hexadecimal

Otro sistema numérico que se emplea a veces para hacerle a los humanos más agradable el sistema binario es el *hexadecimal*, o sistema *hex*, o base 16. ¿Por qué no usar solamente nuestro familiar sistema decimal y convertirlo a binario en lugar de aprender otro sistema numérico? El hex es útil porque resulta más fácil convertir del hex a binario. Como el hex usa 16 dígitos, cada byte (8 dígitos binarios) puede ser representado por 2 dígitos hex. El hex también produce números más cortos que el decimal para trabajar.

El hex necesita 6 símbolos más que el decimal para representar todos sus dígitos, de modo que usa los dígitos decimales estándares del 0 al 9 para representar los primeros 10 dígitos y entonces usa las primeras seis letras del alfabeto, de la A a la F, para representar los 6 dígitos remanentes. La tabla 4.2 muestra los dígitos hexadecimales y sus equivalentes decimales.

Tabla 4.2 Dígitos hexadecimales y sus equivalentes decimales

Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Utilizando este sistema, por ejemplo, el número decimal 11,085 es equivalente al número hex 2B4D y el número decimal 1409 es equivalente al número hex 581. En el primer caso, es obvio que estamos tratando con un número hexadecimal, pero si vemos el número 581, ¿cómo sabemos si es un número decimal o un hexadecimal? Para solucionar este problema, los números hex están indicados por un prefijo 0x o un sufijo H. Por lo tanto, nuestro equivalente hex de 1409 se escribiría 0x581 o 581H.

En el mundo de la computación, Usted encontrará que algunos números (como direcciones IP) son tradicionalmente representados por sus equivalentes decimales, mientras que otros

(direcciones de memoria y direcciones MAC) son tradicionalmente representados por sus equivalentes hexadecimales.

Convirtiendo de Texto a Binario

Las computadoras “piensan” en binario, pero las personas (con excepción de los raros genios matemáticos) no. Nosotros tendemos a trabajar con palabras y muchos de los datos que introducimos en nuestras computadoras son en forma de texto. ¿Cómo la computadora procesa estos datos? A la larga deben convertirse en “lenguaje” binario que es el que la computadora comprende.

Los ficheros de texto están codificados comúnmente en ASCII (en UNIX y sistemas operativos basados en MS-DOS) o en Unicode (en Windows NT/2000). ASCII son las siglas de *American Standard Code for Information Interchange* (Código Estándar Americano para el Intercambio de Información), el cual representa los números binarios como texto. El lenguaje ensamblador usa caracteres ASCII para la programación. Cada carácter del alfabeto, dígito numérico o símbolo está representado por una cadena específica de dígitos binarios de 1 byte. (En un fichero binario, no hay correlación de uno a uno entre los caracteres y los bytes).

Los caracteres ASCII son usados por sistemas operativos basados en textos y programas como versiones MS-DOS y WordPerfect anteriores a la 5.0. Por el contrario, los programas gráficos usan imágenes bitmap o figuras geométricas en lugar de caracteres para crear objetos visualizados.

Nota

El conjunto ampliado de caracteres ASCII incluye caracteres adicionales como formas para dibujar imágenes, de modo que los objetos gráficos pueden ser simulados. MS-DOS utiliza el ASCII ampliado para visualizar menús, cartas de bares y otras formas que son basadas en líneas rectas

Codificando Ficheros que No son de Textos

El esquema original de codificación ASCII empleaba caracteres de 7 bits y está diseñado para tratar con texto plano solamente. Entonces surgió Internet y las personas querían enviarse mutuamente ficheros a través del correo electrónico. El software del servidor de correos fue diseñado para tratar con el conjunto de caracteres ASCII y otro esquema de codificación de 7 bits, el EBCDIC, Código Ampliado de Intercambio Decimal Codificado en Binario que fue creado por la compañía IBM para sus mini-computadoras y unidades centrales. Esto funcionaba bien mientras todos enviaban ficheros de texto plano. Sin embargo, había un problema si Usted quería enviar imágenes, audio, programas o ficheros creados en aplicaciones que no producían texto plano, porque la mayoría de los ficheros que no son de texto usan caracteres de 8 bits. Incluso los documentos creados por procesadores de texto no son salvados generalmente como ficheros ASCII sino como ficheros binarios (en aras de preservar la información al formatear).

La respuesta a este problema fue emplear un esquema de codificación que pudiera representar ficheros que no eran de texto como texto. Los programadores vinieron con soluciones como Extensiones Decodificadas y Multipropósito de Correo por Internet (MIME) para convertir ficheros que no eran de texto en texto ASCII. Así se podría enviar sin problemas a través de Internet una foto u otro fichero de no texto. Un fichero codificado luce al ojo humano como una masa de caracteres ASCII sin significado, pero cuando es decodificado por el software del receptor, vuelve a su forma original. Las MIME ofrecen una serie de ventajas con la decodificación en cuanto soporta el envío de anexos múltiples y contenido multimedia interactivo. Quizás lo más importante, soporta idiomas como el Japonés, Chino y Hebreo que no utilizan el alfabeto romano.

Otro esquema de codificación, denominado BinHex, es usado a menudo por los softwares de Apple Macintosh. Los ficheros de Macintosh difieren de los creados por Windows y algunos otros sistemas operativos en que los primeros constan de dos partes, llamadas *forks* – una que contiene los datos actuales y otra que contiene información atributo y valores paramétricos. Existen en el mercado programas que convierten a los ficheros en un solo torrente de byte para enviarlos a través de la red. Los ficheros Macintosh se pueden enviar a través de las MIME, usando sus especificaciones de encapsulación esbozadas en el RFC1740.

Los visualizadores Web también soportan las MIME, de modo que pueden visualizar ficheros que no tienen formato HTML. También existe una versión de las MIME llamada S/MIME que soporta la codificación de mensajes.

¿Por qué Esto le Conciernen al Investigador?

Los investigadores podrían no ser capaces de interpretar el lenguaje de la máquina, pero deberían comprender qué es lo que ven. Los unos y los ceros de la computación, los números hexadecimales que lucen raros empleados en algunos tipos de direccionamientos y las indescifrables “sandeces” de los ficheros codificados con MIME podrían parecer no tener significado, pero al traducirlos apropiadamente pueden contener evidencia valiosa.

Al igual que un investigador no debería botar una carta encontrada en la escena del crimen sólo porque da la casualidad que fue escrita en Chino, tampoco debería desechar datos electrónicos como inútiles sólo porque los investigadores no los entienden. Puros datos binarios o datos que han sido codificados para enviar a través de una red podrían ser menos cómodos para trabajarlos que textos o imágenes decodificadas, pero por lo general se pueden convertir a una forma legible con el software apropiado.

También es importante para los investigadores comprender la diferencia entre el tipo de codificación que estamos analizando aquí, que está hecha para hacer que los datos sean reconocidos y puedan ser utilizados por una computadora y la *encriptación*, cuyo propósito es hacer que humanos no autorizados para ello reconozcan y usen los datos. Los datos codificados están concebidos para que puedan decodificarse fácilmente y el software para

hacerlo está ampliamente difundido en el mercado. Los datos encriptados están concebidos para que resulte difícil o imposible descifrarlos sin la clave apropiada.

Sólo el hecho de que un fichero haya sido encriptado puede ser, en algunos casos, una bandera roja que despierte sospecha o una pieza para encontrar la causa probable que se necesita para obtener una orden o efectuar un arresto. Por lo tanto, conocer la diferencia entre un fichero codificado y uno encriptado le ahorrará tiempo a los investigadores y aumentará su credibilidad ante un juez.

En la escena...

¿Crea La Encriptación una Causa Probable?

Los investigadores saben que la causa probable generalmente no se basa en un hecho o pedazo de evidencia sino que más bien comprende varias piezas, que al juntarlas, llevaría a una persona prudente y razonable a creer que el crimen fue cometido por el sospechoso. Los profesionales de la ley a veces se refieren a estas piezas de forma colectiva como *la totalidad de las circunstancias*. La Cuarta Enmienda de la Constitución de los Estados Unidos exige que la causa probable, basada en la totalidad de las circunstancias, sea mostrada antes de que se expida una orden de registro.

¿La existencia de un fichero encriptado (o ficheros encriptados) en una computadora establece una causa probable para registrar esa computadora y examinar los ficheros, partiendo de la teoría de que “sólo los culpables tienen algo que ocultar”? En otras palabras, si la novia de un sospechoso de pornografía infantil le dice a Usted que existen ficheros encriptados en la computadora de la familia que ella no puede abrir, ¿es esta una razón suficiente para una orden de registro? Dada la naturaleza de la causa probable, la respuesta es no – por lo menos, no por sí sola. Por lo general, la encriptación por sí sola no sería suficiente para satisfacer la definición de causa probable. El uso de esta no es ilegal en los Estados Unidos (en algunos países sí lo es) y muchas personas interesadas en la privacidad usan la encriptación para proteger datos que no tienen nada que ver con la actividad criminal.

Sin embargo, el hecho de que los datos estén encriptados puede usarse como una de las piezas para llegar a la causa probable. Si Usted tiene otras evidencias que indiquen, por ejemplo, que un sospechoso descarga regularmente fotos pornográficas de niños (como el testimonio de un conocido pornógrafo infantil de que el sospechoso le pedía fotos de este tipo, interceptaba mensajes, etc.), la existencia de ficheros encriptados en el disco duro del sospechoso pudiera ampliar la sospecha de que allí se almacenaron fotos ilícitas.

Otras consideraciones incluyen si todos los ficheros en un disco están encriptados o sólo algunos selectos. La primera situación es más indicativa de alguien que sólo se interesa generalmente por la privacidad, mientras que la segunda sirve como bandera roja de que esos ficheros en particular podrían contener algo de interés para los agentes de la ley. Analizares más detalladamente la encriptación en el Capítulo 7 “Comprendiendo la Prevención del Crimen” en la sección sobre criptografía.

Comprendiendo los Sistemas Operativos de las Computadoras

Cuando una computadora inicia, el sistema operativo se carga hacia su memoria y proporciona las bases o *plataforma* sobre la que corren los programas de aplicación. Aunque la gran mayoría de las computadoras personales de hoy día corren alguna versión de uno de los tres sistemas operativos más populares (Windows, UNIX/Linux o Macintosh OS), existen miles de sistemas operativos diferentes. Algunos de ellos son sistemas operativos de redes como NetWare que corren en servidores, pero no funcionan como sistemas operativos escritorio/cliente. Algunos corren en computadoras centrales grandes o pequeñas como las z/OS y la OS/400 de la IBM, y algunos están diseñados para estaciones de trabajo de calidad superior, tales como la Solaris de Sun y la AIX de la IBM (ambas basadas en UNIX). Otros son sistemas operativos propietarios empleados para dispositivos específicos tales como el Sistema Operativo de Interconexión de Cisco (IOS) que corre en enrutadores Cisco o SCOUT, los cuales ejecutan aplicaciones de redes. Algunos se usan como sistemas operativos incrustados en una variedad de dispositivos, tales como Windows CE, QNX y Symbian. Algunos son sistemas operativos experimentales tales como GNU HURD y SkyOS.

Nota

Para una lista de los muchos sistemas operativos que se están desarrollando, véase la página de Proyectos Actuales de Sistemas Operativos www.cs.arizona.edu/people/bridges.oses.html.

Comprendiendo el Papel del Software del Sistema Operativo

El sistema operativo actúa como una suerte de enlace entre el hardware de la computadora y los programas de aplicación que se usan para realizar tareas específicas (como procesar textos o descargar y enviar correos electrónicos). Este también proporciona la posibilidad de administrar ficheros, brinda seguridad y coordinación entre programas de aplicación y programas utilitarios que están corriendo simultáneamente. Los sistemas operativos se pueden clasificar de diferentes formas:

- *Sistemas operativos basados en texto (o basados en caracteres)* tales como MD-DOS y UNIX/Linux realizan las tareas más rápidamente porque no cumplen con los parámetros requeridos para visualizar gráficos complejos, pero muchas personas los encuentran menos manejables que los sistemas operativos GUI, porque Usted tiene que aprender y teclear comandos para realizar tareas. La mayoría de los sistemas operativos basados en texto pueden correr simuladores de programas para darles una interfaz gráfica. Los ejemplos incluyen a Windows 3.x para MS-DOS y KDE para Linux.
- *Sistemas operativos multiusuarios:* generalmente corren en sistemas de computadoras centrales y permiten que más de un usuario se valide a través de terminales, y corren programas simultáneamente. El término también se refiere, a veces, a sistemas operativos (como Windows NT/2000/XP) que permiten que sólo un usuario se valide a la vez, pero identifica a diferentes usuarios por una cuenta de usuario a la que se le asigna un *perfil de usuario* que define la configuración, las preferencias y los documentos que son específicos para este usuario. Los sistemas operativos de servidores (tales como Windows

NT/2000/.NET Server, Novell NetWare y UNIX) les permiten a múltiples usuarios validarse en el servidor dentro de la red y acceder a sus recursos, aunque sólo un usuario está validado de forma interactiva (en la máquina local).

- *Sistemas operativos multitareas*: son aquellos que le permiten a Usted correr más de un programa a la vez. MS-DOS es un sistema operativo que puede efectuar sólo una tarea a la vez; en otras palabras, Usted tiene que cerrar una aplicación antes de que pueda comenzar otra. El esqueleto de Windows, corriendo sobre DOS, le permite efectuar multitareas. UNIX, OS/2 de la IBM, Windows 9x/ME y NT/2000 y los posteriores son todos verdaderos sistemas operativos multitareas.

- *Sistemas operativos de procesamiento múltiple*: son capaces de usar las posibilidades de más de un microprocesador instalados en el sistema, asignándole diferentes programas para correr en diferentes procesadores o permitiéndole que diferentes partes de un solo programa corran en diferentes procesadores. Por ejemplo, los sistemas operativos Windows 9x/ME no reconocen o usan múltiples procesadores, pero Windows NT/2000/XP/.NET sí. (El número de procesadores depende de la versión del sistema operativo). UNIX y Macintosh también soportan múltiples procesadores.

Diferenciando los Tipos de Sistemas Operativos Multitareas y de Procesamiento Múltiple

Diferentes sistemas operativos soportan tales características como la de multitareas y procesamiento múltiple de diferentes formas. El tipo de multitareas o de procesamiento múltiple que use un sistema operativo en particular depende de su *arquitectura* – o sea, su diseño y estructura.

Multitareas

Este sistema operativo de multitareas funciona por *división del tiempo en slots* – o sea, permitiendo que múltiples programas usen pequeñas partes del tiempo del procesador, uno detrás del otro. Los sistemas operativos de las computadoras personales utilizan dos tipos básicos de multitareas: el cooperativo y el preventivo. El *cooperativo* fue usado por Windows 3.x y también anteriormente, corriendo sobre MS-DOS, así como por los sistemas operativos Macintosh anteriores al OS X. En este tipo de entorno multitareas, cada programa debe ser escrito de modo que *sus procesos* (tareas o programas ejecutables) usen el procesador por un corto período de tiempo y después le cedan el control del procesador a otros procesos. Mientras los programas sean escritos para cooperar, este sistema funciona. Sin embargo, programas mal escritos pueden asumir el control del procesador y negarse a cederlo. Cuando esto sucede, el sistema puede congelarse o colapsar.

El sistema de multitareas preventivo es más eficiente. Este método pone al mismo sistema operativo a cargo del procesador. De esta forma, un programa mal escrito no puede acaparar el control del procesador. Si trata de hacerlo, el sistema operativo se apodera de su uso del procesador y se lo da a otro proceso. Un componente en el meollo del sistema operativo denominado *programador* es responsable de asignarle el uso del procesador a cada programa en turno. Algunos sistemas operativos le permiten a Usted asignar

prioridades a determinados procesos de modo que ellos aparezcan primero cuando necesiten usar el procesador. El procesamiento preventivo es usado por Windows 9x y versiones posteriores, UNIX, OS/2 y Macintosh OS X.

Procesamiento múltiple

Aún si una computadora tiene más de un procesador físicamente instalado, podría no poder realizar procesamiento múltiple. Para ello, el sistema operativo tiene que ser capaz de reconocer la presencia de múltiples procesadores y usarlos. Algunos sistemas operativos como Windows 9x, no soportan el procesamiento múltiple. Incluso entre aquellos que sí lo hacen, no todos los sistemas operativos de procesamiento múltiple están creados igualmente.

Existen tres métodos para soportar procesamiento múltiple:

- Procesamiento múltiple asimétrico (AMP o ASMP)
- Procesamiento múltiple simétrico (SMP)
- Procesamiento múltiple totalmente paralelo (MPP)

Con el *procesamiento múltiple asimétrico*, a cada procesador se le asignan tareas específicas. Un procesador primario actúa como el “Terminal maestro” y controla las acciones de los otros, los procesadores secundarios.

El *procesamiento múltiple simétrico* hace que todos los procesadores estén disponibles para todos los procesos individuales. Los procesadores comparten el volumen de trabajo, distribuido más o menos equitativamente, lo que incrementa el rendimiento. El procesamiento múltiple simétrico también es denominado *procesamiento múltiple bien acoplado*, porque los procesadores múltiples continúan usando sólo un fragmento del sistema operativo y comparten la memoria de la computadora y los recursos de entrada y salida.

El *procesamiento múltiple totalmente paralelo* es un medio de triturar grandes cantidades de datos, distribuyendo el procesamiento entre cientos o miles de procesadores que podrían estar corriendo en el mismo chasis o por separado, en computadoras que se encuentran distanciadas. Cada procesador en un sistema MPP tiene su propia memoria, sus propios discos, aplicaciones y fragmentos del sistema operativo. El problema radica en que los datos se dividen en muchos pedazos que son procesados simultáneamente por los múltiples sistemas.

Nota

El MMP se usa generalmente en entornos gubernamentales, académicos e investigativos que corren grandes y complejos sistemas computarizados. En raros casos se usa en máquinas de mesa o típicos servidores comerciales, aunque existe un tipo de procesamiento paralelo denominado *computación distribuida* que usa grandes cantidades de computadoras personales ordinarias dentro de una red para resolver un problema, dividiendo la tarea entre múltiples máquinas. Uno de los

ejemplos mejor conocidos de este tipo de procesamiento se realizó en el proyecto de Búsqueda de Inteligencia Extraterrestre (SETI). SETI@Home recluta voluntarios en Internet que instalen en sus computadoras de la casa el software que le permite a sus sistemas, durante el tiempo de inactividad, procesar una porción de la cantidad total de datos recopilados por radio-telescopios y analizarla en busca de señales que podrían haber sido originadas por seres inteligentes en el espacio.

Un documento que señala las ventajas del modelo de procesamiento paralelo de la computación distribuida usado en el SETI y otros proyectos se encuentra disponible en <http://roland.grc.nasa.gov/~mallman/papers/prime-delay.pdf> (formato PDF).

El procesamiento múltiple simétrico es el tipo de procesamiento múltiple soportado por los principales sistemas operativos, incluyendo Windows NT/2000/XP/.NET, Linux, BSD y otras versiones de UNIX, BeOS y OS/2 Warp. Para sacarle provecho a las posibilidades del procesamiento múltiple, los programas que corren en máquinas con múltiples procesadores y sistemas operativos tienen que estar *multithreaded* - o sea, deben estar escritos de forma que les permita ejecutar tareas en pequeñas partes ejecutables denominadas *threads*. Windows 2000, XP y .NET también soportan una característica denominada *afinidad del procesador* que proporciona una funcionalidad similar a la del AMP.

Diferenciando entre los Sistemas Operativos Propietarios y los de Fuente Abierta

La mayoría de los sistemas operativos comerciales son *propietarios* – o sea, los vendedores mantienen en secreto el código fuente (las instrucciones de programación) y los acuerdos de licencia prohíben la “ingeniería reversible” (o sea, dismantelar los componentes del software y replicarlos). Los vendedores no dependen sólo del acuerdo de licencia para evitar que Usted lleve a cabo una ingeniería reversible. Cuando Usted compra el software, este ha sido *compilado*; en otras palabras, un programa compilador ha traducido el código fuente (escrito en un lenguaje de un nivel más alto comprensible para el programador) al lenguaje de la máquina comprensible para ella. Este proceso de compilación le dificulta o imposibilita a los programadores replicar el código fuente original, que es necesario para hacerle cambios al software.

Sin embargo, algunos sistemas operativos se distribuyen como *productos de fuente abierta*, significando que el código fuente está disponible para el público y los creadores sin costo alguno. Cualquiera es libre de modificar el código para mejorarlo. La única “trampa” es que la licencia, aunque libre, generalmente obliga a los programadores a revelar sus mejoras o incluso a ponerlas a disposición del público sin costo alguno.

El sistema operativo de fuente abierta más notable (aunque no el único) es Linux, que está basado en el sistema operativo UNIX. (Algunas versiones de UNIX, como FreeBSD, son de fuente abierta; otras como AIX, HP-UX y Solaris no lo son). Para confundir más las cosas, aunque el código fuente de Linux es gratis, vendedores como Red Hat, Caldera y

Corel comercializan sus propias “distros” (término de Linux para *distribuciones*). El término *fuelle abierta* no significa necesariamente que la versión compilada sea gratis – sólo lo es el código fuente.

Linux fue creado en virtud de la Licencia Pública General GNU (GPL), por Linus Torvalds y a él le debe su nombre. El acuerdo de licencia deja claro que los creadores que modifiquen o distribuyan el software pueden cobrar por el servicio si así lo desean, lo que no *pueden* hacer es mantener en secreto el código fuente o patentar los productos (a menos que la patente tenga licencia para que todos lo usen gratuitamente).

Nota

Usted puede leer todos los términos de la GPL GNU en el sitio de la GNU: www.gnu.org/licenses/gpl.html#SEC1. Para más información acerca de la Iniciativa de Fuente Abierta (OSI), visite www.opensource.org.

Si el software de fuente abierta es gratis – o, al menos lo es el código fuente- ¿por qué no todos lo usan en lugar del software comercial propietario que cuesta muchísimo? Existen varias razones:

- Existen decenas de versiones diferentes o “distros” de cada sistema operativo o aplicación de fuente abierta. Esto puede resultar confuso para los usuarios que no saben cuál seleccionar.
- Porque todos pueden hacer modificaciones al sistema operativo, Usted no tiene la estandarización que tiene con el software propietario. En otras palabras, una versión de Linux podría funcionar bien con la configuración de su hardware, pero quizás otra distro no.
- A menudo, los drivers del dispositivo no se encuentran fácilmente para sistemas operativos de fuente abierta, así que los tiene que escribir Usted mismo. Esto va más allá de las capacidades de muchos consumidores y usuarios comerciales (en otras palabras, que no son “genios de la computación”).
- Generalmente no está incluida la garantía en los softwares de fuente abierta y no existe soporte técnico (aunque algunas compañías como Red Hat embalan sus distros de Linux y en esencia venden la garantía y los servicios de soporte técnico acompañados por el software “gratis”). Esto resulta especialmente importante para los usuarios comerciales, que generalmente no usan un software que no incluya soporte técnico por parte del vendedor.

La comunidad de fuente abierta ha criticado a los vendedores de softwares propietarios como Microsoft y Apple por mantener en secreto su códigos fuente. Como resultado, Apple Computer, ha abierto por primera vez su código fuente para Darwin, el corazón del Mac OS X, que está basado en UNIX. Para más información acerca del proyecto OpenDarwin, véase el sitio Web de Apple para creadores: <http://developer.apple.com/darwin/projects>.

Una Panorámica de los Sistemas Operativos Comúnmente Usados

Los sistemas operativos más usados comúnmente por las microcomputadoras hoy día son aquellos hechos por la Microsoft, los sistemas operativos Macintosh de la Apple y las varias distros de Linux y otros sistemas operativos basados en UNIX. En esta sección, veremos brevemente los siguientes sistemas operativos:

- DOS
- Windows 3.x
- Windows 9.x (95, 95b, 95c, 98, 98SE, ME)
- Windows NT 3.51 y 4.0 (versiones Workstation y Server)
- Windows 2000 (versiones Professional y Server)
- Windows XP (versiones Home y Professional)
- Linux/UNIX
- OS/2 y BeOS
- Macintosh

En el momento en que fue escrito este libro, el sistema operativo .NET Server de la Microsoft aún estaba siendo probado en beta, pero se puede esperar que se despliegue ampliamente dentro del entorno corporativo cuando salga al mercado. La figura 4.1 muestra el “árbol genealógico” de la Microsoft, representando la evolución cronológica de los actuales sistemas operativos de Windows.

Comprendiendo el DOS

DOS es el primer sistema operativo de disco utilizado en las PC originales de la IBM. Hoy día, muchas computadoras aún corren algunas formas del DOS. La más popular es la versión de Microsoft, MS-DOS. La IBM obtuvo la licencia del DOS de la Microsoft y comercializó una versión denominada PC-DOS que venía incluida en sus primeras PC. Digital Research vendió una versión denominada DR-DOS que fue comercializada posteriormente por Caldera como DR-OpenDOS. Existe una versión de fuente abierta del DOS llamada FreeDOS. Para más información sobre este producto, véase el sitio Web de la FreeDOS: www.freedos.org.

Las primeras versiones del DOS usaban un sistema de ficheros denominado FAT12 (analizaremos más detalladamente los sistemas de ficheros en la próxima sección). Las versiones MS-DOS de la 3.x a la 6.x soportaban el FAT 16 junto con el FAT 12 y ambos se usaban como sistemas operativos para estaciones de trabajo y como el sistema operativo sobre el que se montaba Windows (mediante la versión 3.11), porque las primeras versiones de Windows no eran verdaderos sistemas operativos, sólo esqueletos gráficos que requerían tener el DOS de fondo. La versión MS-DOS 7.0 que también soportaba el FAT 12 y el FAT 16 era parte del sistema operativo Windows 95. En ese punto de la evolución de los sistemas operativos de Microsoft, el esqueleto se integró con el sistema operativo y los usuarios no instalaron más MS-DOS y Windows como dos productos separados. Windows 95b (también llamado OEM Service Release 2 o OSR 2) se integró con una nueva versión de MS-DOS, la versión 7.1, que soportaba el sistema de ficheros FAT32.

Figure 4.1 The Microsoft family tree

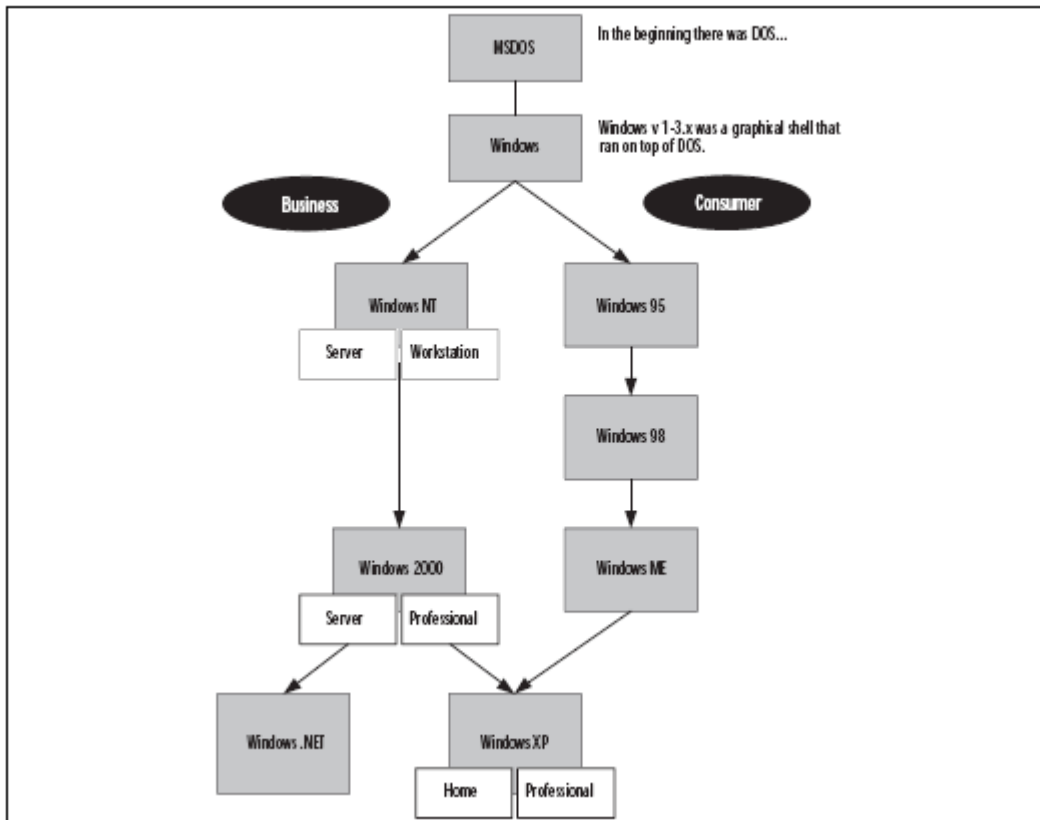


Figura 4.1 Árbol genealógico de Microsoft

MSDOS Al comienzo existía el DOS...

Windows Windows 1.3x era un esqueleto gráfico que corría sobre DOS

Comercio

Consumidor

Windows NT
Servidor/Estación de trabajo

Windows 95

Windows 98

Windows 2000
Servidor/Profesional

Windows ME

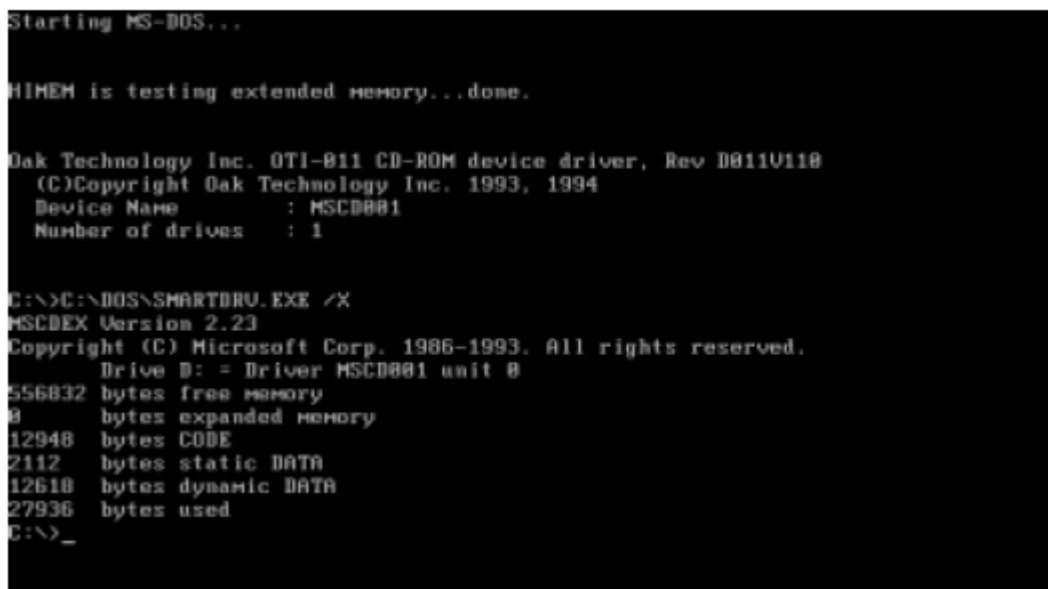
Windows.NET

Windows XP
Casa/Profesional

El MS-DOS como sistema operativo para estaciones de trabajo está basado en texto y no es capaz de realizar tareas múltiples. Tiene varias limitaciones, tales como la incapacidad de trabajar con particiones de disco superiores a 2GB o memorias mayores a 1MB (a menos que Usted use el software de Esquema de Memoria Expandida o EMS). Windows 3.x usa el EMS para poder realizar tareas múltiples. El DOS fue creado sobre el lenguaje de programación BASIC y la mayoría de las versiones incluyen una versión de BASIC. La interfaz MS-DOS se muestra en la figura 4.2.

Figura 4.2 MS-DOS tiene una interfaz basada en texto.

Figure 4.2 MS-DOS has a text-based interface.



```
Starting MS-DOS...

HIHEM is testing extended memory...done.

Oak Technology Inc. OTI-011 CD-ROM device driver, Rev D011U110
(C)Copyright Oak Technology Inc. 1993, 1994
Device Name      : MSCD001
Number of drives  : 1

C:\>C:\DOS\SMARTDRV.EXE /X
MSCDEX Version 2.23
Copyright (C) Microsoft Corp. 1986-1993. All rights reserved.
Drive D: = Driver MSCD001 unit 0
556832 bytes free memory
0 bytes expanded memory
12948 bytes CODE
2112 bytes static DATA
12618 bytes dynamic DATA
27936 bytes used
C:\>_
```

Las ventajas del MS-DOS incluyen el tamaño (la versión 6.22 cabe en tres disquetes), su relativa simplicidad, el bajo costo, y el hecho de que correrá sobre un hardware más antiguo y menos potente que no tiene suficiente memoria ni espacio en disco para soportar sistemas operativos más modernos.

Desde Windows 1.x hasta 3.x

En sí no son verdaderos sistemas operativos, sino más bien complementos del MS-DOS. Las versiones de Windows de la 1.x a la 3.x fueron diseñadas para llevar una interfaz gráfica al entorno computarizado de Microsoft. Las versiones 1 y 2 no fueron muy populares, pero como dice el dicho, a la tercera va la vencida, Windows 3.0, sacado al mercado en 1990, fue el inicio de la dominación de Microsoft sobre el mercado de los sistemas operativos.

En la escena...

¿Quién Le “Robó” Qué a Quién?

Resulta un cliché popular dentro de la comunidad de las computadoras personales que Microsoft le “robó” (o al menos obtuvo) la idea de una interfaz gráfica para Windows de su principal competidor en aquel entonces, Apple. Como la mayoría de los clichés, es real sólo en parte. Es cierto que Apple sí creó un sistema operativo gráfico para su computadora con Arquitectura de Software Local Integrado (LISA), que fue oficialmente sacado al mercado en 1983, justamente antes de que Microsoft anunciara Windows y casi dos años antes de que Windows 1.0 realmente se pusiera a disposición del público. Sin embargo, Apple no “inventó” la idea de la unidad de interfaz gráfica manejada por Mouse, como muchas personas creen. La Xerox Alto (nombrada así por el Centro de Investigaciones de Palo Alto, donde fue creada) y las computadoras Star fueron realmente las primeras computadoras personales en usar estas características, tiempo atrás en los años 70. Steve Jobs (de Apple) y Bill Gates (de Microsoft) visitaron Palo Alto y “tomaron prestadas” las ideas de Xerox, que más tarde aparecieron en la Lisa (y más tarde en la Macintosh) y en Windows.

Para más información sobre la Alto, véase www.fortunecity.com/marina/reach/435. Para ver la interfaz de la Lisa, visite <http://members.fortunecity.com/pcmuseum/lisadsk.htm>. Para observar la interfaz de Windows 1.0 y las siguientes versiones de Windows (hasta la XP), visite www.infosatellite.com/news/2001/10/a251001windowshistory-screenshots.html#win101.

Windows 3.x aún se usa en muchas computadoras en el mundo hoy día. Al igual que el MS-DOS, corre sobre hardwares más antiguos y para él se hicieron muchas aplicaciones. Windows 3.x sobre MS-DOS es conocido como un *sistema operativo de 16 bits*, lo que significa que puede procesar 2 bytes (lo que equivale a 16 bits) a la vez. Una de sus limitaciones es la incapacidad de manejar nombres de ficheros de más de 8 caracteres (con una extensión de tres caracteres).

Nota

Los primeros sistemas operativos de microcomputadoras usados por la Commodore PET, Tandy TRS-80, Texas Instruments TI/99 y la Apple II fueron sistemas operativos de 8 bits.

Windows 3.11 adicionó el acceso a ficheros de 32 bits (una nueva forma de acceder al disco), actualizó los drivers del dispositivo y el reparador de problemas. Otra versión popular de Windows 3.1 y 3.11 se denominó Windows for Workgroups, que incluía por primera vez componentes integrados de redes. Incluía soporte para Microsoft Mail y servicios de acceso remoto y demandaba un rendimiento de entrada/salida del disco mayor en el 50 – 150 por ciento. Windows for Workgroups facilitaba el trabajo de redes máquina a máquina y lo tornaba más cómodo que los primeros sistemas operativos de Microsoft. Esta se hizo muy popular en pequeños entornos comerciales. La interfaz de Windows 3.11 se muestra en la figura 4.3.

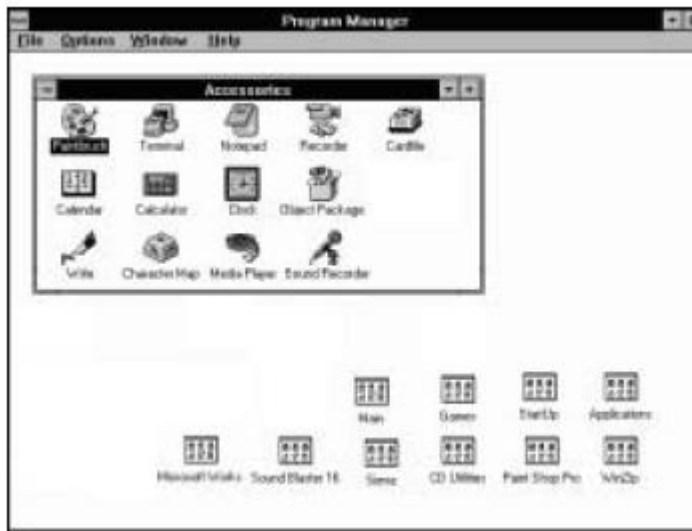


Figura 4.3 Windows 3.x corría sobre MS-DOS, proporcionando una interfaz gráfica.

Windows 9x (95, 95b, 95c, 98, 98SE y ME)

Windows 95 fue un nuevo sistema operativo muy importante cuya salida al mercado estuvo acompañada de una gran fanfarria por parte de Microsoft y la comunidad de la computación. Sacado al mercado en Agosto de 1995, Windows 95 fue el primer sistema operativo consumidor de 32 bits de Microsoft; sin embargo, es un sistema operativo *híbrido* en lugar de un verdadero OS de 32 bits. Para una compatibilidad con programas más antiguos escritos para Windows 3.x, aún existe una buena cantidad de códigos de 16 bits en Windows 95.

Windows 95 fue diseñado para proporcionarles a los usuarios una interfaz completamente nueva (apartando el viejo Manipulador de Programas e incorporando el ahora familiar botón de inicio y la barra de tareas) y muchas características mejoradas, tales como:

- Multitareas preventiva (sólo para programas de 32 bits)
- Soporte para nombres de ficheros largos (hasta 256 caracteres) mediante el sistema de ficheros VFAT
- Plug and Play (lo que facilita la instalación del hardware)
- Administración de programas (una gran ayuda para los usuarios de laptop)
- La papelerera de reciclaje (la que facilita la recuperación de ficheros borrados)
- Soporte para acceso telefónico de redes incluido en el sistema operativo

Windows 95 se tornó tremendamente popular y fue el comienzo del árbol genealógico de Windows 9x, que incluye a Windows 98 y ME. La interfaz de Windows 95 aparece en la figura 4.4.

Figure 4.4 Windows 95 provided a whole new look and many new features.



Figura 4.4 Windows 95 brinda una imagen completamente nueva y muchas características nuevas.

La segunda salida al mercado de Windows 95, popularmente llamada 95b y oficialmente denominada OSR 2, no estuvo a disposición de los consumidores en los estantes. Estuvo concebida para que los fabricantes de equipos originales (OMS o vendedores de hardware de PC) lo instalaran en las máquinas que vendían. La versión 95b adicionó el soporte para el sistema de ficheros FAT32. Una variante del 95b, llamada OSR2.1, adicionó un soporte USB rudimentario. Otra variante, la OSR2.5, a menudo llamada Windows 95c, adicionó el visualizador Web Internet Explorer 4.0 como un componente integrado.

El siguiente escalón en la línea 9x de sistemas operativos de Microsoft para consumidores fue Windows 98, sacado al mercado apropiadamente en Junio de 1998. Esta fue la primera versión disponible para consumidores como un paquete de softwares que soportaba FAT32 (además de los “antiguos” sistemas de ficheros FAT12 y FAT16). Windows 98 también adicionó mejoras de mercado e interconexión, mejor soporte de hardware, soporte infrarrojo (IrDA), y una Interfaz de Energía y Configuración Avanzada (ACPI). También incluía el Escritorio Activo (que podría adicionarse a Windows 95 instalando el visualizador Internet Explorer 4.0) y soportaba monitores múltiples. Windows 98 reemplazaba los antiguos ficheros de Ayuda por un sistema HTML indexado y fácil de encontrar que era mucho más funcional y adicionaba una serie de soluciones automáticas a los problemas conjuntamente a la actualización en línea de componentes/drivers, Windows Update. Windows 98SE (segunda edición) adicionó unas cuantas características nuevas como el Compartimiento de Conexión a Internet (ICS) y el soporte para DVD-ROM.

El próximo (y presumiblemente el último) en la línea de Windows 9x es Windows ME, abreviatura de Edición Milenio, sacado al mercado en Septiembre de 2000. El ME adicionaba varias características de multimedia como programas de edición de videos e

incluía un mejor soporte para la interconexión en casa, pero no constituyó una mejora significativa. El ME es presumiblemente el último en la línea de 9x, porque la línea 9x de sistemas operativos de Windows, orientada hacia los usuarios de casa y la línea de Windows NT/2000, orientada hacia el mundo del comercio, se fundieron en una con el surgimiento de Windows XP.

Windows NT

Microsoft diseñó Windows NT para el escritorio corporativo y el mercado de los servidores. NT viene en dos versiones: Workstation para los escritorios y Server para los servidores. NT fue sacado al mercado en 1993 y se basó en parte del trabajo realizado conjuntamente por Microsoft e IBM antes de sus diferencias por el OS/2. Por lo tanto, muchas de las características de NT, tales como su código puro de 32 bits, su alto rendimiento y el seguro sistema de ficheros son similares a las características del OS/2. NT es el primer sistema operativo de Microsoft que *no* se basa en MS-DOS. Sin embargo, puede correr programas MS-DOS creando una máquina virtual que simula el entorno DOS sobre el cual pueden correr las aplicaciones DOS.

Nota

¿Qué significan las iniciales NT? En sus primeros tiempos, Microsoft decía que las iniciales significan *Nueva Tecnología*. Posteriormente (cuando no se le pudo seguir llamando “nueva” a la tecnología), Microsoft cambió su historia y dijo que no significaban nada. David Curtler fue la fuerza impulsora en la creación de Windows NT.

Las diferencias primarias entre Windows 9x y Windows NT son la estabilidad y la seguridad. El entorno comercial requiere de un sistema operativo que no colapse con frecuencia, uno que sea lo suficientemente seguro como para proteger los datos sensibles almacenados en las computadoras de las compañías. La arquitectura de Windows NT incorpora una capa de abstracción del hardware (cariñosamente denominada HAL) que evita que las aplicaciones de los softwares hagan llamadas directas al hardware. Esto convierte a NT en un sistema más estable y menos propenso a colapsos, pero también significa que algunas aplicaciones escritas para Windows 9x no correrán en Windows NT.

NT 3.1 fue sacado al mercado en 1993, un año antes que Windows 95. La interfaz se asemejaba a Windows 3.x, pero el núcleo era completamente diferente. Un factor significativo era el modo en que NT manejaba la memoria. A diferencia de Windows 3.x, cada programa corría en su propia dirección de memoria. Esto significaba que si un programa colapsaba, no se llevaría con él el resto de los programas que estaban corriendo. Las características de seguridad incluían una validación obligatoria (el usuario debía tener un nombre de usuario y una contraseña para entrar en la computadora). NT también introdujo soporte para un nuevo sistema de ficheros. El Sistema de Ficheros NT (NTFS) ofrece un mejor rendimiento, así como la posibilidad de establecer permisos (denominados *permisos NTFS* o *permisos a nivel de fichero*) en ficheros y carpetas individuales. NT 3.51 y las versiones anteriores también incluían soporte para el sistema de ficheros del OS/2 originario de la IBM, Sistema de Ficheros de Alto Rendimiento (HPFS).

NT 4.0 fue una actualización significativa que salió al mercado en 1996. La interfaz se asemejaba a la de Windows 95 e incluía herramientas de administración para usuarios avanzados, soluciones automáticas, un monitor de red (un analizador de protocolo incluido o un software “rastreador”), un administrador de tareas (una herramienta que brinda información sobre las aplicaciones y los procesos que están en ejecución) y soporte para políticas del sistema y perfiles de usuario que le permiten a los administradores un control más fácil del entorno de escritorio del usuario. Servicios de acceso remoto y soporte incluido para redes privadas virtuales (VPN) a través del Protocolo para Túneles Punto a Punto (PPTP) fueron otras mejoras. NT 4.0 no incluía soporte para HPFS. En la figura 4.5 se muestra la interfaz de Windows NT 4.0.

Aunque Windows NT Workstation tiene muchas ventajas sobre los sistemas operativos 9x, nunca se hizo popular para los usuarios de casa por varias razones:

- NT no soporta Plug and Play, de modo que la instalación del hardware es más difícil y NT es más “quisquilloso” con respecto al hardware que soporta.
- NT no es óptimo para jugar. Muchos juegos populares de Windows 9x y DOS no correrán en NT, porque el software de juego necesita acceso directo al hardware, lo que NT no permite.
- NT Workstation cuesta cerca del doble de lo que cuesta Windows 9x.
- NT es más complejo y menos “manejable para el usuario” y sus medidas de seguridad extras son consideradas innecesarias e inconvenientes por muchos usuarios de casa.

Figure 4.5 Windows NT 4.0 provided an interface similar to that of Windows 95.



Figura 4.5 Windows NT 4.0 ofrecía una interfaz similar a la de Windows 95.

A pesar de su poca popularidad en el mercado del consumidor, Windows NT – ambas versiones: Workstation y Server, se hizo inmensamente popular en el entorno comercial con el producto para servidores de Microsoft, superando y sobrepasando al NetWare de

Novell como un servidor de autenticación de redes. Windows NT hizo enormes avances dentro de los mercados de la mensajería por Internet y el servidor Web, los que fueron anteriormente dominados por UNIX.

Windows 2000

Aunque Windows NT proporcionó mucha más estabilidad y seguridad que los sistemas operativos 9x, a fin de continuar creciendo dentro del mercado compartido entre los comerciantes y los consumidores, especialmente al competir con UNIX, Microsoft necesitaba algo mejor. Windows 2000 salió al mercado en Febrero de 2000, representando al menos la misma cantidad de cambios que representaron las actualizaciones desde Windows 3.x hasta el 95. Al igual que NT, Windows 2000 es realmente una familia de productos: Professional (el sistema operativo escritorio/cliente que reemplaza a NT Workstation) y tres versiones del software para servidores (Server, Advanced Server y Datacenter Server). La página de inicio de Windows 2000 Pro se muestra en la Figura 4.6.

Los sistemas operativos de Windows 2000 están contruidos sobre el núcleo de NT, pero con la interfaz de Windows 98 y literalmente cientos de mejoras. Muchas características que faltaban en NT (aunque algunas de ellas podrían adicionarse con un software complementario de intermediarios) tales como la encriptación de ficheros, cuotas de disco y finalmente!- Plug and Play estaban incluidas en Windows 2000. Nuevas características de seguridad incluyen soporte para el protocolo de autenticación estándar de Internet Kerberos, Seguridad IP (IPSec) para encriptar datos que viajan a través de la red, Política de Grupo (un reemplazo mucho más robusto y poderoso para las políticas de sistema), y el Protocolo para Túneles (L2TP) para redes privadas virtuales más seguras. La mayor diferencia entre la interconexión con NT y Windows 2000 es la adición del Directorio Activo, un servicio de directorio similar en cierta forma al NDS de Novell que proporciona una base de datos centralizada para administrar la seguridad, los datos del usuario y los recursos distribuidos.

Para más información sobre Windows 2000 y el Directorio Activo, un buen punto de partida es el sitio Web de Windows 2000 de Microsoft: www.microsoft.com/windows2000.

Figure 4.6 Windows 2000 is built on NT technology.



Figura 4.6 Windows 2000 está construido sobre la tecnología NT.

Windows XP

En Octubre de 2001, Microsoft sacó al mercado otra actualización de escritorio no tan significativa, esta vez llamada Windows XP. Una cosa que hace especial a XP es el hecho de que es una actualización de ambas líneas de sistemas operativos de escritorio, la de Windows 9x y Windows NT, que se fusionaron nuevamente en una sola línea de producto – una especie de ella. Aunque ambas están basadas en el núcleo de NT que es el más estable, XP viene en dos versiones diferentes: XP Home Edition para consumidores y XP Professional para los usuarios del mundo del comercio.

La Home Edition de XP se centra en el entretenimiento (fotografía digital, música y video), juegos y otras actividades orientadas al consumidor, junto a características que facilitan más que nunca la conexión a Internet y la conectividad en casa. La Professional Edition incluye todas las características de XP Home más otras adicionales que están orientadas hacia el usuario corporativo, tales como el Escritorio Remoto (una aplicación “light” para servidores terminales que le permite a Usted acceder a su escritorio XP desde cualquier lugar a través de la red), encriptación de ficheros, soporte para sistemas de procesadores múltiples y características de conectividad avanzadas. La interfaz de Windows XP Professional se muestra en la figura 4.7. Note que no es el escritorio XP implícito, ha sido totalmente personalizado para mostrar la gran flexibilidad que brinda el sistema operativo que le permite a los usuarios “tenerlo a su estilo”.

Figure 4.7 Windows XP combines the best of the 9x and NT/2000 worlds.

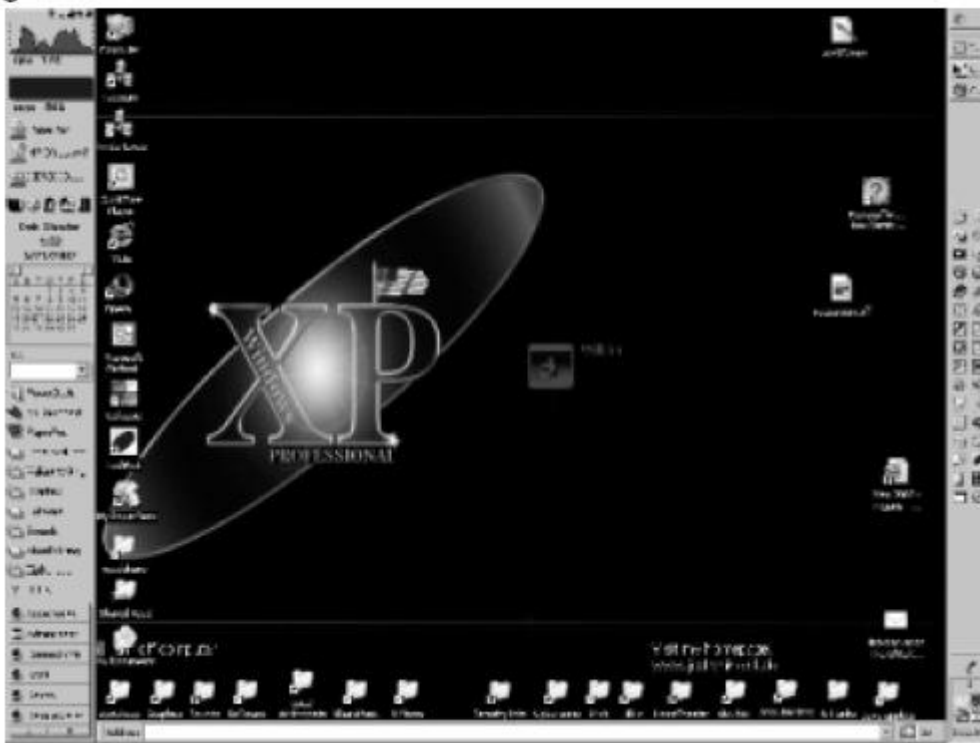


Figura 4.7 Windows XP combina lo mejor de los mundos de 9x y NT/2000.

Una computadora con Windows XP Pro, al igual que con NT Workstation y Windows 2000 Pro, puede ser un miembro de un dominio de Windows (una red basada en un servidor), mientras que las computadoras con XP Home, al igual que con los sistemas Windows 9x, pueden usarse para acceder a recursos del dominio, pero no pueden formar parte de este. Las características útiles incluidas en ambas versiones de XP son:

- Muro de fuego incluido en Internet para una mayor seguridad
- Protección de ficheros de Windows que evita que se cambien accidentalmente los principales ficheros del sistema operativo
- Conmutación rápida de usuario que le permite a los usuarios cambiar la cuenta de usuario en la que estaban validados sin cerrar las aplicaciones (en computadoras que no son parte del dominio)
- Una serie de nuevos magos que lo guían a Usted a través de tareas realizadas comúnmente como transferir ficheros y configuraciones de una computadora a otra, configurar una red, publicar en la Web, etc.

Windows XP es un sistema operativo de escritorio/cliente solamente. Aunque no había salido al mercado en el momento en que fue escrito este libro, su sistema operativo correspondiente para servidores es Windows .NET Server (actualmente probándose en beta). Para más información sobre Windows XP, un buen punto de partida es la página de inicio de XP de Microsoft, www.microsoft.com/windowsxp/home/default.asp. Usted puede encontrar más información acerca de .NET Server en www.microsoft.com/windows.netserver.

Linux/UNIX

UNIX existe desde los años 60 aproximadamente, cuando fue creado en los laboratorios Bell conjuntamente con científicos del MIT y, por ende, ocupa un lugar cimero en la mayoría de las competencias dentro del mercado de los sistemas operativos para PC. Generalmente usado para servidores, más que para máquinas de mesa, UNIX es un sistema operativo con base de texto muy poderoso y complejo (y de alguna forma hostil para los usuarios) que corren muchos de los servidores de correo, servidores Web y otros en Internet.

UNIX se formó fuera del sistema de unidad central Multics (Servicio de Computación e Información Multiplexado) creado en el MIT, pero era un sistema operativo completamente nuevo diseñado para crear un entorno computarizado multiusuario que soportaría una gran cantidad de usuarios. Originalmente corría en las enormes máquinas de tiempo compartido PDP que se usaban en universidades y centros gubernamentales en los años 60 y 70. La primeras versiones de UNIX fueron escritas en lenguaje ensamblador, pero las posteriores fueron escritas en el lenguaje de programación de alto nivel C. A finales de los 70, la popularidad de UNIX comenzó a expandirse más allá del mundo académico, y en los primeros tiempos de la Internet corría en la mayoría de las computadoras VAX que se

conectaron a Internet. En los años 80, se desarrollaron más versiones de UNIX y su uso se expandió al mundo de los negocios.

Todavía hoy existe un gran número de versiones diferentes de UNIX, incluyendo la AIX de la IBM, Solaris de Sun Microsystems, HP-UX de Hewlett-Packard, BSD de Berkeley, SCO UNIX de Santa Cruz Operations (que esa compañía le compró a Novell en 1995), y otras. El sistema X Window fue creado para adicionar un esqueleto gráfico a UNIX y hacerlo más manejable para los usuarios. Realmente no es una GUI, sino un protocolo que se puede usar para formar una GUI, como el Entorno de Escritorio Común (CDE). Sin embargo, las interfaces gráficas de UNIX tienden a ser, en cierto modo, toscas y feas comparadas con las interfaces de Windows y los puristas de UNIX rechazan la GUI, prefiriendo el entorno de línea de comando de mayor rendimiento.

En 1991, el estudiante finlandés Linus Torvals escribió un sistema operativo basado en UNIX que denominó Linux (mencionado brevemente con anterioridad en este capítulo) y lo distribuyó de forma gratuita a través de los grupos de noticias de Internet. Linux se impuso dentro de los programadores y después entre los usuarios, quienes estaban buscando una alternativa para Microsoft Windows. Aunque Linux se usa a menudo para correr servidores (especialmente servidores Web que corren el software de fuente abierta para servidores Apache Web) es más apropiado para el escritorio que UNIX. Linux es un sistema operativo basado en texto como UNIX, pero cuando se hizo popular como un sistema operativo de escritorio, los creadores desarrollaron rápidamente una variedad de esqueletos gráficos que corrían sobre él, tanto como Windows 3.x corría sobre MS-DOS. Estos esqueletos incluían el Kool Desktop Enviroment (KDE) y GNOME que es parte del proyecto GNU y se puede descargar gratuitamente del sitio Web de GNOME, www.gnome.org. Usted puede ver la interfaz KDE en la figura 4.8.

El sistema operativo 2 (OS/2) comenzó como un esfuerzo conjunto entre la IBM y Microsoft en los años 80 para reemplazar al DOS. El OS/2 original (versión 1) estaba basado en texto, pero era un sistema operativo de 16 bits, a diferencia de la versión del DOS de aquel entonces (versión 3.0) que era de 8 bits. La versión 2.0 incluía una interfaz gráfica y era un verdadero sistema operativo de 32 bits. El OS/2 fue diseñado para ofrecer la estabilidad y la posibilidad de realizar tareas múltiples que el DOS no tenía. El escritorio del OS/2 se muestra en la figura 4.9.

Después de que Windows 3.0 de Microsoft comenzó a hacerse popular, Microsoft retiró su apoyo para el OS/2, aunque basó el corazón de Windows NT en el corazón del OS/2. La IBM era en realidad una compañía de hardware, no una de software, de modo que cuando Microsoft abandonó el proyecto, la IBM firmó un contrato con la Commodore y tomó prestado de la Amiga la GUI orientada al objeto para el OS/2. La versión 2.11 adicionó soporte para el procesamiento múltiple simétrico y pudo correr programas de Windows 3.x, así como aplicaciones escritas para el OS/2. En 1994, la IBM sacó al mercado el OS/2 Warp 3.0. Este incluía soporte para Internet (el primer OS para consumidores en hacerlo) y su sucesor, OS/2 Warp Connect, soportaba todos los protocolos de redes importantes: TCP/IP, IPX y NetBIOS.

En 1996, “Merlín” (OS/2 4.0) salió al mercado con una interfaz más atractiva y soporte para OpenGL y la máquina virtual de Java. Desafortunadamente para la IBM, en aquel entonces, Windows había alcanzado un gran empuje y la mayoría de las aplicaciones fueron escritas para él. El OS/2 era incapaz de correr aplicaciones de Windows de 32 bits, una limitación que afectaba seriamente su popularidad. La IBM detuvo el desarrollo del OS/2 y aún estaba atascada en la versión 4 en el momento en que fue escrito este libro, aunque ha continuado siendo popular en determinadas industrias como la bancaria, y la IBM continua dándole su apoyo mientras también comercializa el OS/2 Warp Server para el comercio electrónico.

Figure 4.9 OS/2 featured the Workplace Shell interface.



Figura 4.9 OS/2 ofrecía la interfaz gráfica para el puesto de trabajo.

El BeOS es un sistema operativo monousuario que tiene algunas similitudes con UNIX, pero no es un clon de UNIX (UNIX es un sistema operativo multiusuario). BeOS fue diseñado con un propósito específico: servir de plataforma para aplicaciones de audio, video y otras “cercanas al tiempo real”. El BeOS soporta el multiprocesamiento y el procesamiento por hebras. Fue creado por dos ex-empleados de la Apple y la primera versión pública fue sacada al mercado en 1995 para la PowerPC; más tarde en 1998 fue traducida a la plataforma de Intel x86. La versión actual soporta la conectividad TCP/IP y las conexiones por marcado PPP. El OS también ha sido usado en equipos para Internet (máquinas dedicadas de correo electrónico/Web que no tienen la funcionalidad de las buenas computadoras) y video caseteras digitales.

Las computadoras de Apple Macintosh difieren de las PC compatibles con Intel en muchas cosas, una de las cuales es el hecho de que son propietarias; Apple hace ambas cosas: el hardware y el software para el sistema operativo. Los sistemas operativos Mac no corren en las PC y los sistemas operativos de las PC no corren en las Mac (aunque es posible usar un software especial de *máquina virtual* que le permite a Usted correr un sistema operativo de PC en una ventana sobre el sistema operativo Mac).

La última versión del sistema operativo Mac, denominada OS X, es un gran cambio con respecto a las versiones anteriores, porque está basada en una versión de UNIX llamada Darwin. El OS X de Macintosh combina el poder subyacente del código UNIX con una GUI bonita y manejable para el usuario llamada Aqua. Mac ha sido siempre popular en instituciones educativas y entre diseñadores gráficos, pero el OS X está ganando

popularidad entre ambos: los usuarios tradicionales de UNIX y los fanáticos de Windows. En la Figura 4.10 se muestra la interfaz del Mac OS X.

El OS X ofrece soporte incluido para escribir CD y DVD y es fácil de conectar a una red de área local y/o Internet. El soporte está incluido para acceder a ficheros en las PC de Windows a través de la red y existen softwares como SAMBA que le permiten a Usted compartir sus ficheros Mac con máquinas de Windows conectadas a la red. Con el OS X, Mac finalmente sumó características tan avanzadas como la multitarea preventiva y la memoria protegida e incluyó soporte para el multiprocesamiento simétrico, USB y FireWire (IEEE 1394). Apple está también comercializando una versión para servidores, OS X Server, que soporta clientes corriendo Mac, Windows, UNIX y Linux. Para mayor información sobre el OS X, véase el sitio Web de Apple, www.apple.com/macosex.

Figure 4.10 Macintosh OS X features an attractive, usable interface on a UNIX OS.



Figura 4.10 Macintosh OS X brinda una interfaz atractiva y utilizable en un UNIX OS.

Comprendiendo los Sistemas de Ficheros

Un factor importante relacionado con el sistema operativo usado por la computadora es el *sistema de ficheros*, que define la estructura para organizar y localizar los datos en el disco. Los datos se almacenan en *clusters*, que son unidades que miden un tamaño específico en bytes. Un fichero se puede almacenar a través de muchos clusters, pero datos de diferentes ficheros no están almacenados en el mismo cluster. Eso significa que si, por ejemplo, un cluster mide 12KB y un fichero sólo 2KB, habrán 10KB de espacio desperdiciado en ese

cluster. El manejo y el tamaño de los clusters resulta muy diferente entre los diversos sistemas de ficheros. Otras diferencias incluyen el tamaño máximo de partición soportada, la fiabilidad y la seguridad.

La mayoría de los sistemas de ficheros almacenan datos en una estructura jerárquica de árbol. Los contenedores llamados *directorios* o *carpetas* guardan ficheros (y también pueden guardar subdirectorios o subcarpetas), organizados por grupos para una mejor administración. El máximo nivel jerárquico se denomina *raíz* o *directorio raíz*. El sistema de ficheros es la estructura completa del directorio que consiste en el directorio raíz y todos los subdirectorios y ficheros por debajo en la jerarquía.

Los diferentes sistemas operativos usan diferentes sistemas de ficheros y algunos sistemas operativos soportan más de un sistema de ficheros. Los más familiares son aquellos usados por los sistemas operativos de Microsoft:

- FAT12
- FAT16
- VFAT
- FAT32
- NTFS

En las siguientes secciones, veremos algunas de las características de cada sistema de ficheros, conjuntamente con sistemas de ficheros menos comunes de encontrar utilizados por sistemas operativos que no son de Microsoft.

FAT12

FAT es la abreviatura de *tabla de distribución de ficheros*. El sistema de ficheros FAT fue creado para ser usado por los sistemas operativos DOS. La primera versión de FAT se denominó FAT12, porque sus tablas de distribución empleaban un número binario de 12 dígitos (12 bits) para la información del cluster. El FAT12 fue útil para los muy pequeños discos duros que venían con la IBM PC original (menores a 16MB). También se usa para formatear disquetes flexibles.

FAT16

El FAT16 fue creado para discos mayores de 16MB y por un largo período de tiempo fue el sistema de ficheros estándar para formatear discos duros. Como probablemente Usted puede suponer, este usa entradas de tablas de distribución de 16 bits. El FAT16 (a menudo referido como solo FAT) es soportado por todos los sistemas operativos de Microsoft, desde el MS-DOS hasta Windows XP. También es soportado por algunos sistemas operativos que no son de Microsoft, incluyendo el OS/2 y Linux. Este soporte lo convierte en el sistema de ficheros más compatible a nivel universal. Sin embargo, tiene muchos inconvenientes, incluyendo:

- El FAT16 no se ajusta bien a discos grandes. Debido a que el tamaño del cluster se incrementa en la medida en que el tamaño de partición del disco se incrementa, un disco grande (de más de 2GB aprox.) formateado con FAT16 tendrá una gran cantidad de espacio desperdiciado.
- El FAT16 no soporta compresión a nivel de fichero. El esquema de compresión usado con FAT16, como, por ejemplo, el implementado por DriveSpace, requiere que toda la unidad lógica sea comprimida.
- El FAT16 no soporta seguridad a nivel de fichero (asignación de permisos a ficheros individuales y carpetas).

Nota

Es posible que Usted lea en algunas fuentes que el FAT16 está limitado a 2GB, pero en realidad este no es el caso (aunque sí se torna ineficiente en discos más grandes). MS-DOS no le permitirá a Usted crear una partición FAT16 mayor de 2GB, pero Usted *puede* crear particiones FAT16 (hasta los 4GB) en Windows NT/2000. Estas particiones FAT16 más grandes no son soportadas ni reconocidas por MS-DOS o Windows 9x.

VFAT

FAT Virtual o *VFAT* es un driver del sistema de ficheros que fue introducido en Windows for Workgroups 3.11 y soportado por Windows 95. Sus ventajas son que opera en modo protegido y proporciona la posibilidad de usar nombres de ficheros largos con FAT16. VFAT no es un sistema de ficheros, sino una extensión de programa que maneja nombres de ficheros por encima de la limitación 8.3 impuesta por el FAT16 original.

FAT32

El FAT32 usa una tabla de distribución de 32 bits. Fue soportado primeramente por la versión OSR2 de Windows 95 (95b) y diseñado para mejorar la funcionalidad del FAT16 adicionando características como:

- Más eficiente uso del espacio con discos duros grandes al usar clusters más pequeños.
- Soporte para particiones mayores, hasta 2 terabytes, en teoría (Windows soporta particiones FAT32 de hasta 32GB).
- Mayor confiabilidad, debido a la inclusión de una copia de seguridad de la información estructural de los datos importantes en el sector de arranque.

El FAT32 también tiene desventajas, incluyendo el hecho de que es incompatible con MS-DOS, Windows 3.x, Windows 95a, Windows NT y algunos sistemas operativos que no son de Microsoft (aunque los drivers del FAT32 los comercializan los intermediarios que venden Windows 95, NT e incluso sistemas operativos que no son de Microsoft como

Linux). Adicionalmente, la overhead usada por el FAT32 puede disminuir considerablemente el rendimiento.

NTFS

NTFS, el sistema de ficheros original de Windows NT, fue diseñado para ser más robusto y seguro que otros sistemas de ficheros de Microsoft. Soporta particiones muy grandes (hasta 16 exabytes, en teoría) y le permite a Usted crear volúmenes que abarcan dos o más particiones. Usted puede establecer permisos de acceso a nivel de fichero para controlar quién puede leer, cambiar o acceder al fichero. Esto aplica a los usuarios que acceden al fichero tanto desde la máquina local como a través de la red y es un complemento de los permisos de compartimiento en la red que están establecidos a nivel de carpeta/directorio. El NTFS es más confiable, porque soporta una característica llamada *hot fixing*, un proceso en el que el sistema operativo detecta un sector dañado en el disco y reubica automáticamente los datos almacenados en ese sector en un sector en buenas condiciones, después marca el sector dañado de modo que no sea usado por el sistema. Este proceso se hace muy rápidamente, sin la consciencia o intervención del usuario o aplicaciones.

El esquema de compresión usado por el NTFS le permite a Usted comprimir datos sobre una base de fichero a fichero para ahorrar espacio en disco y archivar ficheros viejos. Esto es mucho más seguro que la compresión a nivel de unidad usada por Windows 9x, en la cual la pérdida de un solo fichero compactado con todo el contenido de la unidad significaba que se perdieran todos los datos de la misma.

La versión del NTFS incluida en Windows 2000 y la anterior (NTFS 5.0) soporta la encriptación de ficheros. Esta característica se denomina Sistema de Encriptación de Ficheros (EFS) y se basa en la criptografía clave pública y certificados digitales. Para más información acerca del EFS, véase la Windows & .NET Magazine en www.winntmag.com/Articles/Index.cfm?ArticleID=5387&Key=Internals. Note que NTFS 5.0 también soporta *cuotas de disco*, lo que involucra la capacidad del administrador de establecer límites en cuanto al espacio de disco que puede ser usado por usuario y por disco.

Nota

Service Packs 4 y el posterior para Windows NT 4.0 adicionan soporte para NTFS 5.0, de modo que NT puede acceder a unidades locales formateadas en NTFS 5.0. Sin embargo, NT no es capaz de usar toda la funcionalidad de NTFS 5.0 (por ejemplo, la encriptación EFS no es soportada en NT).

Otros Sistemas de Ficheros

Usted podrá encontrar otros sistemas de ficheros como:

- CDFS, el sistema de ficheros usado para escribir datos en CDs
- HPFS, el sistema de ficheros original del OS/2 de alto rendimiento

- Ext2fs, VFS y los sistemas de ficheros Journaling usados por Linux
- Sistema Jerárquico de Ficheros Macintosh (HFS)
- Sistemas de ficheros de redes

Debido a que el sistema de ficheros determina cómo se almacenan los datos en un disco, es importante estar familiarizado con el sistema de ficheros cuando Usted está llevando a cabo la recuperación de datos. La tabla 4.3 muestra cuáles sistemas de ficheros son soportados por varios sistemas operativos de Microsoft (sin añadir drivers de intermediarios).

Tabla 4.3 El sistema operativo de Microsoft y su correspondiente sistema de ficheros

Sistema Operativo	FAT12	FAT16	FAT32	NTFS
MS-DOS	x	x		
Windows 3.x	x	x		
Windows 95a	x	x		
Windows 95b	x	x	x	
Windows 98	x	x	x	
Windows ME	x	x	x	
Windows NT	x	x		x
Windows 2000	x	x	x	x
Windows XP/.NET	x	x	x	x

Resumen

Los investigadores de crímenes cibernéticos necesitan estar íntimamente familiarizados con el modo interno de trabajar de las computadoras y el software que corre en ellas, al igual que los investigadores de homicidios deben estarlo con la patología humana básica. Eso incluye comprender la función de todos los componentes del hardware que se unen para conformar una computadora y cómo esos componentes interactúan entre ellos.

Resultaría difícil para un investigador llevar adelante una investigación apropiada en un país extranjero donde él o ella no domine el idioma local, pues muchas pistas podrían pasar desapercibidas si el investigador no puede entender la información recopilada. Así mismo, un investigador de crímenes cibernéticos debe tener un conocimiento básico del “lenguaje” empleado por las máquinas para procesar datos y comunicarse con otra. Aunque un investigador de este campo no podría hablar todos los idiomas humanos, resulta útil ser capaz, al menos, de reconocer en qué idioma está escrita la evidencia, pues esa evidencia podría ser significativa y seguramente ayudará al investigador a encontrar a alguien que la pueda traducir. Similarmente, aunque se supone que un investigador de crímenes cibernéticos no pueda programar en binario, ayuda el reconocer el significado de los datos que están en formato binario o hexadecimal y si pueden o no ser valorados como evidencia.

Las computadoras hoy día corren una variedad de sistemas operativos y sistemas de ficheros y el trabajo del investigador de localizar evidencia se hará de modo diferente en dependencia del sistema que se utilice. Un buen investigador de crímenes cibernéticos está

familiarizado con los sistemas operativos más comunes y con el modo en que sus sistemas de ficheros organizan los datos en el disco.

Aunque toda esta información podría parecer demasiado técnica para el policía “no-genio” – y quizás podría parecer demasiado obvia para el profesional de la informática- es importante que los investigadores que aspiran a especializarse en crímenes por ordenador y crímenes cibernéticos tengan un buen conocimiento de que una comprensión técnica puede conducir a comprender el crimen cibernético y a los criminales. Ahora que Usted comprende cómo funcionan las computadoras, en el próximo capítulo ahondaremos en cómo se comunican dentro de una red.

Preguntas Realizadas con Frecuencia

Las siguientes preguntas realizadas con frecuencia, respondidas por los autores de este libro, están diseñadas para medir su comprensión de los conceptos presentados en este capítulo y para ayudarle con la implementación de estos conceptos en la vida real. Para hacer que el autor conteste a sus preguntas, visite www.syngress.com/solutions y haga clic en el formulario “**Pregúntale al autor**”.

P: ¿Qué quieren decir los términos *velocidad de transferencia de datos* y *tiempo de búsqueda* en relación con discos duros?

R: Esas son formas de medir el rendimiento de un disco duro. La *velocidad de transferencia de datos* se refiere a la cantidad de bytes por segundo (bps) que la unidad de disco es capaz de transferir al procesador. Generalmente esto se mide, en el caso de los discos actuales, en megabytes por segundo, y las velocidades entre 5 y 40 son comunes. Mientras mayor sea este número, mejor será el rendimiento del disco. El *tiempo de búsqueda* se refiere al tiempo de intervalo que transcurre desde que el procesador le pide un fichero al disco hasta que este recibe el primer byte de ese fichero. Este tiempo se mide en milisegundos (entre 7 y 20 es lo típico) y mientras menor sea este número, mayor será el rendimiento.

P: ¿Cómo una torre de CD-R escribe datos en un CD?

R: Los CD-Recordable o CD-R o discos, a diferencia de los CD regulares de sólo lectura, tienen una capa de color (generalmente verdoso) sobre el disco, que está cubierta por una capa de oro reflectante. Ambas capas minúsculas descansan sobre una pieza rígida de plástico llamada *substrato*. La unidad de CD-R tiene un *láser de escritura* que es más poderoso que el láser de lectura en una unidad regular de CD-ROM. Este láser más poderoso calienta la capa de color desde arriba y llega al substrato. El proceso de calentamiento cambia la transparencia del color en ese lugar, creando un “bache” que no es reflectante. Este bache forma una marca legible que es leída como dato por la unidad de CD. El mismo esquema de codificación es usado por los CD regulares. Es por eso que una unidad regular de CD-ROM puede leer discos CD-R.

P: ¿Cómo funciona la memoria virtual?

R: Cuando un sistema operativo soporta el uso de la memoria virtual, este crea un fichero en el disco duro (llamado *fichero de intercambio* o *fichero página*) en el cual puede “intercambiar” datos entre la RAM y el disco. El sistema detecta cuáles áreas de la memoria física (RAM) no han sido usadas recientemente. Entonces copia los datos de ese lugar en memoria en el fichero en el disco duro. Esto significa que habrá más espacio en la RAM, lo que le permite a Usted correr aplicaciones adicionales o aumentar el rendimiento de las aplicaciones que se están ejecutando en ese momento. Cuando el procesador necesita los datos almacenados en el fichero de intercambio/fichero página, se puede transportar del disco duro de vuelta hacia la RAM. Los datos se almacenan en unidades llamadas *páginas*. El uso de la memoria virtual puede disminuir el rendimiento si el sistema tiene que introducir y extraer frecuentemente los datos de la RAM. Ese intercambio frecuente trae como resultado el *estropeamiento del disco*, lo que generalmente es una señal que Usted necesita para aumentarle la memoria física a la computadora.

Referencias

- Computadoras análogas
www.science.uva.nl/faculteit/museum/AnalogComputers.html
- Museo de Computadoras Análogas
<http://dcoward.best.vwh.net/analog/analog1.htm>
- EETimes: *Modelo de Computadora Análoga de Trumps Turing*
www.eetimes.com/story/OEG19981103S0017
- Información sobre el Overclocking
www.overclockers.com y www.overclockershideout.com
- Guía PC: *Unidades de Disco Duro*
www.pcguide.com/ref/hdd/index.htm
- *Cómo funcionan los Discos Duros*
www.howstuffworks.com/hard-disk.htm
- *Cómo funcionan las Unidades de Discos Flexibles*
<http://howstuffworks.lycoszone.com/floppy-disk-drive.htm>
- *Cómo funcionan las Memorias Flash*
<http://howstuffworks.lycoszone.com/flsh-memory.htm>
- *Cómo funcionan las Unidades de Almacenamiento Desmontables*
<http://howstuffworks.lycoszone.com/removable-storage.htm>

- *Cómo funcionan los Sistemas Operativos*
<http://howstuffworks.lycoszone.com/operating-system.htm>
- GNU Licencia Pública General
www.gnu.org/licenses/gpl.html#SEC1
- Iniciativa de Fuente Abierta
www.opensource.org
- Proyectos de Fuente Abierta de la Apple
<http://developer.apple.com/darwin/projects>
- El proyecto FreeDOS
www.freedos.org
- Windows 2000
www.microsoft.com/windows2000
- Windows XP
www.microsoft.com/windowsxp/home/default.asp
- Windows .NET Server
www.microsoft.com/windows.netserver
- Linux DistroWatch
www.distrowatch.com

Comprendiendo los Principios Básicos de la Interconexión

Tópicos que investigaremos en este capítulo:

- **Comprendiendo Cómo las Computadoras se Comunican en una Red**
- **Comprendiendo los Protocolos TCP/IP Utilizados en Internet**

- ✓ **Resumen**
- ✓ **Preguntas Realizadas con Frecuencia**
- ✓ **Referencias**

Introducción

En el Capítulo 4 analizamos cómo las computadoras – ambos elementos: hardware y software – aceptan, procesan y almacenan datos. Una década atrás, eso habría sido todo lo que necesitaríamos para continuar con nuestro análisis. Muchas PC, especialmente computadoras caseras, funcionaban como sistemas individuales. Hoy día, sin embargo, la máquina local es sólo el punto de partida para los investigadores de crímenes por ordenador. Ahora la mayoría de las computadoras – y por la naturaleza del crimen cibernético, todas las computadoras involucradas en este tipo especial de delito – están conectadas a una red. Esa red podría ser una de área local, la Internet global, o ambas.

La conectividad de redes crea nuevas oportunidades tanto para los criminales como para los usuarios de computadoras legítimos. Comprender los crímenes cibernéticos más orientados hacia la tecnología, como el acceso no autorizado a través de la red (hacking) – y de hecho, incluso determinar si ha ocurrido o no un crimen – puede depender de la comprensión sobre cómo las computadoras interconectadas se comunican entre sí.

Muchos ataques de hacking, diseñados para echar abajo una computadora o red o congestionar el sistema de modo que los usuarios legítimos no puedan entrar, se basan en la explotación de las características de los protocolos de red, generalmente de la suite de Protocolos TCP/IP (Protocolo de Control de la Transmisión/Protocolo de Internet). Para lanzar esos ataques, un criminal debe comprender cómo funciona el TCP/IP. Así mismo, para que un investigador documente cómo se hizo el ataque y determine de dónde pudo haber sido lanzado, el investigador debe entender el funcionamiento de los protocolos TCP/IP.

Un investigador de robos con fuerza que no comprenda cómo funcionan los cierres de las puertas (los mecánicos y electrónicos) y cómo se pueden forzar, podría obviar pistas y pasar por alto las formas en que un intruso del mundo real pudo haber entrado a una residencia o a un negocio. Conocer este tipo de información podría ayudar a sacar en claro la identidad del ladrón. Constituye una parte importante para probar el caso, porque si Usted puede demostrar que el criminal usó habilidades especiales o herramientas para entrar (lo opuesto a encontrar la puerta abierta y entrar), generalmente Usted crea un caso más sólido en las mentes de los miembros del jurado. La entrada forzada indica premeditación en lugar de un delito “del momento”. Similarmente, un investigador de crímenes cibernéticos que no comprenda el proceso de lograr entrar a una computadora interconectada es probable que pase mucho trabajo para interpretar pistas digitales, rastrear al criminal y construir el caso.

Incluso para crímenes de naturaleza menos técnica, la red le da a los criminales un número infinito de locaciones adicionales para almacenar ficheros que ofrecen evidencias de un crimen. Los investigadores deben estar conscientes de este hecho o podrían pasar por alto fragmentos cruciales de evidencia. Por ejemplo, un pornógrafo infantil podría ser cuidadoso al transferir todos sus ficheros gráficos ilegales hacia una locación geográficamente lejana de su computadora de la casa, borrando los originales del disco duro. La revisión de la computadora del sospechoso podría no revelar nada incriminatorio.

Sin embargo, los registros de la red podrían demostrar cuándo y hacia dónde se hicieron las transmisiones y el software rastreador puede capturar los paquetes reales durante la transmisión. Los registros de clientes FTP u otros programas usados para transferir los datos podrían revelar el sitio hacia donde se realizaron las transferencias. Un investigador que no comprenda cómo se envían los datos a través de las redes o que no esté consciente de la existencia de ficheros de registro o de la importancia de las configuraciones de programas no sabría siquiera cómo comenzar a buscar evidencia.

En este capítulo, retomaremos el hilo del Capítulo 4, analizando cómo funcionan las computadoras, pero enfocándonos ahora en cómo ellas trabajan en la red: enviando y recibiendo datos (a nivel físico), implementando modelos de interconexión estándar y usando protocolos industriales estándares. Nuevamente, cada sección se resume con una explicación de por qué la información le interesa a los investigadores de crímenes cibernéticos y cómo se puede emplear en la detección y el enjuiciamiento de los delitos penales.

Comprendiendo Cómo las Computadoras se Comunican en una Red

El propósito de una red es permitir el compartimiento entre computadoras. Eso significa compartir datos, programas de aplicación, periféricos de hardware como las impresoras e incluso un mecanismo común de autenticación de modo que el compartimiento de los otros elementos ocurra más fácil y transparentemente para el usuario.

La primera forma de “interconexión” (cuando la mayoría de las computadoras eran simples estaciones de trabajo) se denominó *sneakernet* (red a zapato), porque involucraba la transportación física de los datos, softwares o hardware a compartir con la computadora remota. En otras palabras, si Usted quería compartir un fichero de datos o un programa de software con otra persona que usaba una máquina diferente, Usted lo copiaba para un disco flexible y caminaba a través de la habitación o del edificio (o, en algunos casos, usaba el servicio postal o el mensajero privado para entregarlo en el pueblo o en el país). Compartir una impresora podía resultar aún más incómodo; Usted copiaba para un disco flexible el fichero que quería imprimir y se lo llevaba al usuario dichoso (o no dichoso) que tenía una impresora conectada a su computadora. Ese usuario tenía que parar lo que él o ella estaba haciendo e insertar el disco flexible, abrir el documento y mandarlo a imprimir por Usted. De modo alternativo, Usted podía transportar la impresora de una computadora hacia otra. Las impresoras a menudo descansaban sobre carritos con ruedas para poder transportarlas. Sin importar cómo Usted lo hiciera, compartir impresoras resultaba incómodo y consumía tiempo antes de la llegada de las redes de área local. La alternativa- darle una impresora a cada usuario – a menudo resultaba demasiado costosa para ser factible.

Pronto se hizo obvio que existía una manera mejor: conectar las computadoras a través de cables de modo que los datos (incluyendo los documentos a imprimir) se pudieran enviar de una computadora a otra sin que alguien tuviese que hacer el viaje físico. De hecho, esta fue una de las razones más populares para que las compañías implementaran las redes locales en los primeros tiempos de la interconexión. El hardware y el software de la interconexión se han hecho más sofisticados con los años y ahora podemos hacer más que enviar ficheros.

Las aplicaciones de redes nos permiten comunicarnos rápida y fácilmente mediante el correo electrónico, el chateo o la mensajería instantánea, poner a disposición de otros usuarios de redes informaciones en sitios Web, correr aplicaciones en servidores remotos desde nuestro propio escritorio a través de servicios Terminal y mucho más.

Enviando Bits y Bytes a Través de una Red

Debido a que todos los datos procesados por computadoras son, a la larga, reducidos a cadenas de 0 y 1, toda la comunicación de la red involucra la transmisión y recepción de estos datos binarios (bits y bytes). Esta información binaria se puede enviar a través de cables de cobre en forma de impulsos eléctricos; a través de cables ópticos en forma de pulsos de luz o a través del aire en forma de señales de radio o microondas, pulsos láser o infrarrojos. Sin tener en cuenta el medio, las señales representan los 0 y 1 que conforman todos los datos electrónicos. El proceso de convertirlos en estos pulsos de energía se denomina *codificación de señales o modulación de señales*.

Existen varios métodos de codificación que especifican exactamente cómo los 0 y 1 binarios deben ser representados eléctricamente. Por ejemplo, el esquema de codificación Manchester establece que un 1 binario se representa con bajo voltaje para la primera mitad del bit y con alto voltaje para la segunda. Un 0 se representa con la señal opuesta: la primera mitad con alto voltaje y la segunda con bajo. Este sistema aparece representado gráficamente en la Figura 5.1.

Como Usted puede ver, cada bit consiste en un cambio de voltaje, lo mismo de bajo a alto (representando un 1) como de alto a bajo (representando un 0). La transición, denominada *transición de reloj* es usada por el adaptador de la red que recibe la señal para determinar el inicio y final de cada bit. Este método de codificación se usa para redes Ethernet 10BaseT – redes que envían señales a través de cables (UTP) no revestidos y torcidos a 10Mbps. Los esquemas de codificación empleados para otras arquitecturas de redes (como Fast Ethernet, también llamada 100BaseX) son diferentes. Esto se debe a que la codificación Manchester incrementa la frecuencia a la que la señal se transmite y resulta difícil o imposible de implementar a la velocidad de transmisión de 100Mbps de la Fast Ethernet.

Figure 5.1 The Manchester encoding scheme is one method of representing binary data electrically.

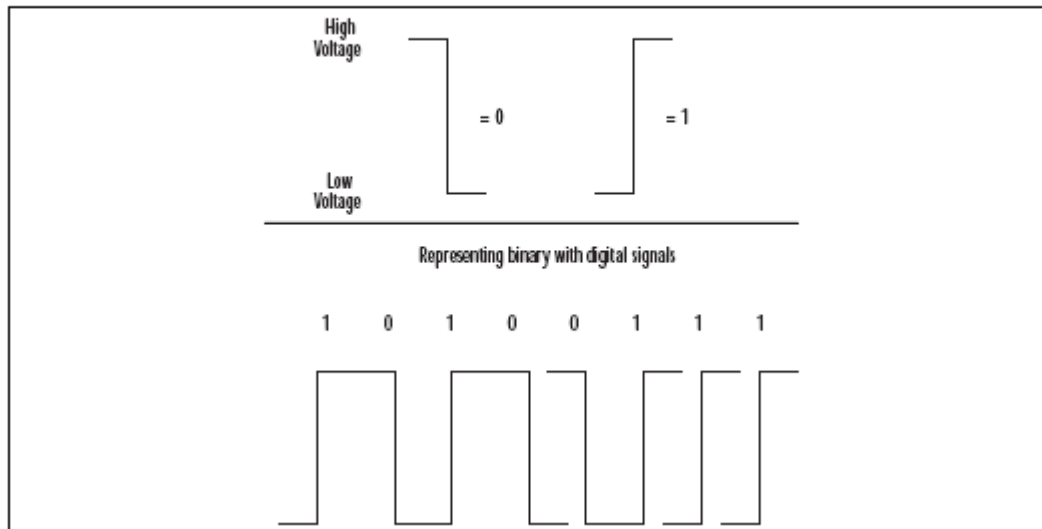


Figura 5.1 El esquema de codificación Manchester es un método de representar eléctricamente los datos binarios.

Nota

Si existe una interferencia procedente de una fuente externa (un motor, una transmisión de radio u otra fuente que cree un campo electromagnético fuerte), la señal se puede interrumpir. Esto podría destruir algunos de los bits, trayendo como resultado una pérdida de datos.

Métodos de Señalización Digital y Análoga

El tipo de señalización que mejor representa la información binaria, en la que hay dos posibles estados (apagado o encendido), que representan dos valores específicos (0 o 1), se denomina *señalización de estado discreto*. Las *señales digitales* son estados discretos, mientras que las *señales análogas* no lo son. Las señales análogas cambian de estado gradualmente, de una forma continua, en lugar de pasar directa e instantáneamente de un estado discreto a otro. Las señales análogas se pueden trazar en forma de ondas, como muestra la Figura 5.2.

Si un interruptor de luz ordinario que tiene dos posiciones – encendido y apagado – representa la señalización digital, entonces un interruptor “dimmer”, que le permite usar un botón o un control para moverse a través de niveles de “encendido” antes de llegar a “apagado” representa como funcionan las señales análogas. Cientos de dispositivos de nuestro mundo actual ilustran la diferencia entre las señales digitales y análogas – por ejemplo:

Figure 5.2 Analog signals are continually changing waves of energy.

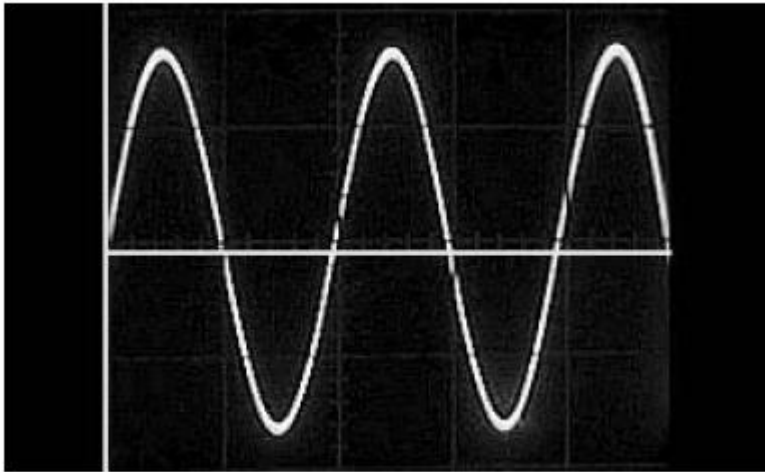


Figura 5.2 Las señales análogas están cambiando continuamente ondas de energía.

- Relojes análogos con una manecilla que se mueve continuamente alrededor de los números que indican la hora y los relojes digitales que cambian al instante de un minuto al próximo.
- Sintonizadores de radio análogos con un dial que le permite sintonizar gradualmente a través de las frecuencias y los sintonizadores digitales que le permiten marcar la frecuencia exacta que desea.
- Termómetros análogos en los que el mercurio se eleva gradualmente y los termómetros digitales que visualizan una temperatura específica.

Las señales análogas, obviamente, son más complejas que las digitales. Medir las señales análogas involucra la medición de las tres características siguientes: amplitud, frecuencia y fase. La *amplitud* es la intensidad de la señal. En la ilustración, la altura de la onda representa su amplitud. La *frecuencia* se refiere al tiempo que le toma a una onda completar el ciclo. La frecuencia se denota por el número de ciclos por segundo, denominado *hercio*. La *fase* mide el estado de una onda con relación a otra; esto se mide en *grados*.

Vivimos en un mundo análogo por naturaleza. Aunque el tiempo, las frecuencias de radio y la temperatura se pueden representar digitalmente, sabemos que en realidad existen estados “intermedios” que no son representados por dispositivos digitales. Sin embargo, para la mayoría de los propósitos, la representación digital es suficiente o incluso preferible. Es más simple que la análoga y generalmente menos vulnerable a interferencias. Una onda continua puede interrumpirse por pequeñas distorsiones que no afectarán el estado discreto de las señales digitales.

Nota

Aunque las señales digitales son menos vulnerables a interferencias que las análogas, lo opuesto es real cuando se llega a la *atenuación*, que es la pérdida de intensidad de la señal a través de la distancia. Las señales análogas son

generalmente capaces de ir más lejos que las digitales sin debilitarse de forma que la transmisión resulte inestable.

Otras ventajas de las transmisiones digitales sobre las análogas incluyen:

- **Rendimiento** Las conexiones digitales generalmente son más rápidas.
- **Efectividad en el costo** Generalmente resulta menos costoso manufacturar dispositivos digitales que análogos.
- **Confiabilidad** Debido a su simpleza, las señales digitales son generalmente más confiables.
- **Seguridad** Generalmente resulta más fácil asegurar transmisiones digitales

Por otra parte, las señales análogas generalmente son más fáciles de multiplexar. Esto se refiere a usar un solo vínculo para enviar múltiples torrentes o *canales* de información. Así es como funciona la TV por cable, transmitiendo docenas o incluso cientos de canales diferentes de programación a través de un cable.

¿Cómo funciona la Multiplexación?

Las señales se pueden multiplexar de diferentes formas. Por ejemplo, diferentes torrentes de información se pueden enviar en frecuencias separadas. Esto se denomina *multiplexación por división de frecuencia* (FDM) y es el método típico para multiplexar señales análogas. Cada canal se transmite en una frecuencia diferente, pero en la misma línea. Se requiere de un equipo especial llamado *multiplexor/demultiplexor* en ambos extremos de la transmisión, en el de enviar y en el de recibir, de modo tal que los canales de frecuencia se puedan separar para ser usados cuando lleguen a su destino.

Otro método de multiplexación se denomina *multiplexación por división de tiempo* o TDM. Este método se puede usar para multiplexar señales digitales. En lugar de usar frecuencias diferentes, la TDM rompe cada una de las señales en pequeños pedazos llamados *segmentos*, y estos se transmiten a través del vínculo uno detrás del otro. En el otro extremo, los segmentos que conforman cada señal individual se unen nuevamente. Este sistema es similar en cierta forma al de *intervalos de tiempo* usado por los procesadores de las computadoras para aparentar estar trabajando simultáneamente en múltiples tareas.

Si el medio de transmisión es cable óptico se puede usar otro método de multiplexación denominado *multiplexación por división en longitud de onda de alta intensidad* (DWDM). Como la luz se puede separar en diferentes longitudes de onda, las señales por separadas se pueden transmitir usando longitudes de onda separadas.

Nota

Este análisis sobre la multiplexación es una panorámica muy simplificada de un tema complejo. Si Usted está interesado en conocer más detalles técnicos, diríjase a las siguientes fuentes:

- Bell Labs: *¿Qué importancia tiene la Multiplexación para las Comunicaciones?*
www.bell-labs.com/technology/multiplex
- Explicación sobre la FDM:
www.cs.williams.edu/~cs105/f01/text/ch3/DigitalTrans_13.html
- Explicación sobre la TDM:
www.cs.williams.edu/~cs105/f01/text/ch3/DigitalTrans_9.html
- Clase individual sobre la DWDM por el Consorcio Internacional de Ingeniería
www.iec.org/online/tutorials/dwdm

Factores Direccionales

En dependencia del método de señalización, las señales pueden viajar en una sola dirección (unidireccional) o en ambas direcciones (bidireccional). Las señales bidireccionales pueden viajar en ambas direcciones consecutiva o simultáneamente. Estos tres métodos diferentes de viaje de la señal se identifican como sigue:

- **Transmisiones simplex** Estas son transmisiones unidireccionales que funcionan como una calle de un solo sentido. El viaje está permitido en una sola dirección. Los primeros sistemas de TV por cable usaban este tipo de transmisión porque la información (programas de TV) era entregada al consumidor; no había necesidad de que el consumidor enviara transmisiones de retorno. La mayoría de las compañías de servicios por cable han mejorado su infraestructura para soportar señalizaciones de dos vías que son necesarias para los servicios de Internet por cable y para servicios de entretenimiento que requieren que el consumidor se comunique con la compañía (como Pay-Per-View). Otras compañías han mantenido sus esquemas de señalización en un solo sentido y utilizan las líneas telefónicas para las transmisiones en dirección contraria de los consumidores. Otro ejemplo de transmisión en un solo sentido es un sistema de dirección público. Se transmiten mensajes de voz amplificada, pero no existe un mecanismo para recibir mensajes de retorno.

- **Transmisiones medio – duplex** En estas transmisiones, la transmisión de señales es bidireccional, pero la señal puede viajar en un solo sentido a la vez. Esto es similar a una carretera de dos vías sobre un puente que es tan estrecha que sólo un vehículo puede pasar por ella a la vez. Un carro que venga en la dirección opuesta debe esperar para entrar al puente hasta que el vehículo que venga en dirección contraria haya salido de ella. Las señales medio duplex se usan a menudo para las comunicaciones de radio de dos vías; los oficiales del orden están familiarizados con este tipo de transmisión, porque esta es la forma en que opera la mayoría de los radios de la policía. Usted puede hablar cuando oprime el botón de Transmitir, pero no puede escuchar nada de lo que están diciendo del otro lado de la transmisión. La otra persona debe esperar hasta que Usted haya terminado de transmitir para que él o ella pueda responder. Si ambos tratan de transmitir a la vez, pisarán la señal del otro y ninguna de las transmisiones pasará.

- **Transmisiones totalmente duplex** Las señales se transmiten en ambas direcciones y pueden viajar simultáneamente a través del aire o del cable. Esto es similar a una carretera de dos carriles y dos sentidos sobre un puente, donde los vehículos pueden pasar a la vez yendo en sentidos opuestos. Las líneas regulares de teléfono funcionan de esta forma;

cuando Usted tiene una conversación telefónica con otra persona, ambas pueden hablar a la misma vez y mientras Usted habla puede oír (aunque posiblemente no comprenda) lo que la otra persona está diciendo.

Si aplicamos estos métodos de transmisión a la interconexión de computadoras, debe ser obvio que las transmisiones totalmente duplex brindan mejor rendimiento que los otros métodos. Se puede enviar y recibir datos simultáneamente. Las tarjetas de redes y los módems son capaces de transmitir en modo medio duplex y en totalmente duplex. La línea debe soportar también la transmisión totalmente duplex. Las conexiones digitales requieren de dos pares de cables por separado: uno para enviar y otro para recibir. Las transmisiones análogas pueden dividir las señales de envío y recepción en dos frecuencias individuales.

Factores de Tiempo

Cuando un adaptador de la red u otro dispositivo de red recibe una señal, este necesita *información de tiempo* para interpretar correctamente las señales. A esto le denominan *sincronizar los bits*. Existen dos formas básicas de cumplir este objetivo y el método de transmisión puede ser *sincrónico* o *asincrónico*, en dependencia de cuál método se utilice. La diferencia es la siguiente:

- **Asincrónico** En el inicio de cada mensaje está incluido un *bit de inicio*; este bit se usa como una señal para que el dispositivo receptor sincronice su reloj con el del dispositivo remitente.
- **Sincrónico** Un mecanismo de sincronización incluido en la transmisión sincroniza los relojes de los dispositivos receptor y remitente.

Interferencia de Señal

Las señales de la red pueden ser interrumpidas por una interferencia externa que puede causar pérdida o distorsión de los datos. Anteriormente mencionamos que las señales digitales son menos vulnerables a interferencias. El tipo de medio usado para transmitir las señales (cable de cobre, cable óptico u ondas aéreas) también afecta la vulnerabilidad a interferencias. Dos tipos comunes de interferencia de los que oír hablar son:

- **Interferencia electromagnética (EMI)** La energía electromagnética (EM) está conformada por ondas alternas de campos eléctricos y magnéticos. El espectro electromagnético abarca desde rayos X y rayos gamma en el extremo más cercano, ondas de luz cerca del medio y ondas de radio en el extremo más lejano. La Marina de Estados Unidos utiliza señales de grandes longitudes de onda, denominadas *frecuencia extra larga (ELF)*, para comunicarse con los submarinos. Las microondas tienen pequeñas longitudes de onda de aproximadamente un milímetro. Todos los equipos electrónicos pueden generar EMI o señales electromagnéticas no deseadas. Cuando la EMI interfiere transmisiones de radio (tales como conversaciones telefónicas), a menudo se le llama *ruido*. Si interfiere transmisiones de datos, puede causar pérdida o cambios de los datos.
- **Interferencia de frecuencia de radio (RFI)** Las frecuencias de radio son las longitudes de onda entre cerca de 10kHz y 100GHz. La RFI se refiere a la recepción de señales de

radio no deseadas y realmente es un subconjunto de la EMI. Las redes inalámbricas utilizan frecuencias de radio para enviar y recibir señales de la red. Si transmisores de radio cercanos usan la misma frecuencia (o una aproximada) para transmitir, esto puede interferir las transmisiones de datos de la red. Los monitores de computadoras, procesadores y otros dispositivos también generan señales o frecuencias de radio y pueden ser fuentes de interferencia. La RFI puede originarse de muchas fuentes.

La energía electromagnética es capaz de causar diferentes efectos, en dependencia de la frecuencia. La EM en el extremo más bajo (rayos X) puede ionizar átomos porque sus longitudes de onda son muy pequeñas. Las microondas, un poco más arriba en el espectro, son capaces de hacer vibrar a las moléculas de agua, lo que las calienta (así es como funciona un horno microondas). Objetos de metal (por ejemplo, antenas) generan corriente cuando chocan con la EM. Esta señal se puede pasar entonces a circuitos que son capaces de decodificar la señal como son los receptores de radio o televisión. Las ondas EM se generan constantemente, de modo que la EMI puede ser una fuente importante de interrupción de la transmisión.

En la escena...

Preparándose para el EMP

Un súbito arranque inmenso de EM se denomina un *pulso electromagnético* o EMP. Un EMP puede ser producido por una explosión nuclear; se producen rayos gamma que interactúan con las moléculas de aire para producir un campo electromagnético muy fuerte seguido de una corriente de conducción que fluye en dirección opuesta. Un EMP puede destruir o dañar equipos electrónicos, generadores de energía, tuberías de metal y cableados y todo lo que sea vulnerable a una subida de voltaje eléctrico. Chips semiconductores – incrustados en todo, desde elevadores hasta aviones y que controlan muchas de las máquinas de las que depende nuestra sociedad moderna, incluyendo nuestro sistema militar – son especialmente susceptibles al EMP. La energía EM calienta el chip y lo puede derretir completamente.

El revestimiento metálico se puede usar para “endurecer” dispositivos vulnerables y protegerlos de la posibilidad de EMP. Sin embargo, el proceso es muy costoso y en algunos casos disminuye la funcionalidad del equipo. La mayoría de los análisis sobre detonación nuclear se han centrado en el efecto radioactivo sobre la vida orgánica, pero los efectos de un EMP acompañante sobre los dispositivos electrónicos podrían crear un tipo diferente de devastación para la que podríamos no estar preparados.

Para más información sobre la amenaza de un EMP, véase la transcripción del testimonio ante el Comité sobre Seguridad Nacional de la Cámara de Representantes en 1997, *La Amenaza que Representa un Pulso Electromagnético para los Sistemas Militares Estadounidenses y la Infraestructura Civil*, en el sitio Web http://commdocs.house.gov/committees/security/has197010.000/has197010_1.HTM.

Paquetes, Segmentos, Datagramas y Tramas

Las señales representan bits individuales y esos bits a menudo se agrupan en bytes para más comodidad, pero las computadoras envían datos a través de la red en unidades más grandes: paquetes, segmentos, datagramas o tramas. Un *paquete* es un término genérico, generalmente definido como un “trozo” de datos de un tamaño conveniente para ser transmitido. En lugar de enviar un fichero grande entero como una cadena larga de bits, el fichero se divide en bloques y cada uno de estos bloques se transmite individualmente. Este sistema permite comunicaciones más eficientes en la red porque una computadora no “acapara” el ancho de banda de la red al enviar una gran cantidad de datos. En Internet existen múltiples rutas de un remitente en particular a un destino específico. Este sistema también permite que los bloques individuales de datos tomen rutas diferentes.

La mayoría de las redes, incluyendo la Internet, corren en protocolos TCP/IP. A nivel de transporte, una unidad de datos se denomina *segmento* cuando el TCP es el protocolo capa de transporte. Para tornar más confuso un tema ya confuso, se le denomina un *datagrama de usuario* cuando se usa el Protocolo de Datagrama de Usuario (UDP). Un paso más abajo, a nivel de red (IP), los trozos de datos que se enrutan a través de la red se denominan *datagramas*. Si nos movemos hacia abajo al nivel de enlace de datos (en el que operan Ethernet y otros protocolos capa de enlace), la unidad de datos con la que trabajamos se denomina *trama*.

La Internet usa *tecnología de intercambio de paquetes* para mover más efectivamente grandes cantidades de datos transmitidos por múltiples computadoras a través de los mejores senderos hacia sus destinos. Cada paquete viaja independientemente. Cuando todos los paquetes que conforman una comunicación arriban a la computadora destino, se reorganizan apropiadamente utilizando la información contenida en sus *encabezados*. Un paquete se puede concebir como un sobre electrónico que contiene los datos, así como las direcciones y otras informaciones relevantes (como por ejemplo las secuencias y la información del checksum).

Métodos de Control de Acceso

Cuando se transmiten señales en una red, debe existir algún mecanismo para “dirigir el tráfico” – o sea, una forma de asegurar que cuando múltiples computadoras estén enviando señales, todos los paquetes de datos lleguen a salvo a sus destinos. Esto se denomina el *método de control de acceso*.

Los populares métodos de control de acceso se agrupan en tres categorías: métodos de contención, método de paso de señales y método de sondeo. Echémosle una mirada breve a cada uno de ellos:

- **Métodos de contención** Estos incluyen el CSMA/CD (Portador con acceso múltiple y detección de colisión), utilizado en redes Ethernet, y el CSMA/CA (Acceso múltiple por detección de portadora con evitación de colisión), usado en redes Appletalk. En ambos casos, las computadoras que quieren transmitir datos en la red deben competir o *contender*

para usar el cable u otro medio. Si dos estaciones intentan enviar al mismo tiempo, ocurre una colisión. CSMA/CD y CSMA/CA difieren en el modo de enfrentar el problema de la colisión. En el caso del primero, se detectan las colisiones de datos y se envían nuevamente los datos tras una cantidad aleatoria de tiempo. En el caso del segundo, se coloca un mensaje de “intento de transmitir” como un “tanteo” antes de que la computadora transmita los datos reales.

- **Métodos de paso de señales** Estos eliminan la posibilidad de una colisión al utilizar una señal circulante denominada *ticket* para determinar qué computadora puede transmitir. Una computadora en una red de paso de señales es más “cortés”, pues en lugar de comenzar su transmisión cada vez que tenga algo que decir, espera pacientemente a que llegue su turno (cuando el *ticket* llega a ella) y envía datos sólo cuando “tiene la palabra”.

- **Métodos de sondeo** Estos son similares en alguna medida a los de paso de señales, excepto que en lugar del grupo de computadoras que organizan el tráfico circulando un *ticket*, una unidad central actúa como un “presidente” preguntándole a los miembros del “comité” en forma sucesiva si tienen algo que decir. Como las computadoras siguen estas “reglas de procedimiento parlamentario”, la transmisión de datos tiene lugar de una forma ordenada, y nuevamente, no existe peligro de colisión de datos.

Tipos de Redes y Topologías

Las redes se pueden clasificar de muchas formas. Por ejemplo, de acuerdo con su *alcance* físico (la dimensión del área que una red abarca geográficamente) como sigue:

- **Red de área local (LAN)** Confinada a un área geográfica, como por ejemplo, un solo edificio o varios edificios que se encuentren muy próximos.
- **Red de área amplia (WAN)** Conecta locaciones en áreas ampliamente dispersas, usando la tecnología como por ejemplo, líneas telefónicas regulares, líneas arrendadas o satélite.
- **Red de área metropolitana (MAN)** Cubre un área de aproximadamente la dimensión de una ciudad típica.

En estas redes se emplean diferentes medios, protocolos y tecnologías, en dependencia de en cuál de estas tres categorías se encuentre la red.

Otro asunto importante es el diseño o la topología de la red. El término *topología* se refiere a si los cables están dispuestos en una línea que va directamente de computadora a computadora (un bus), en un círculo que va de computadora a computadora con la última conectada a la primera (un anillo) o en forma de rayos en la que cada una va conectada a un concentrador central (una estrella). Una cuarta topología, la *malla*, se crea cuando se conectan todas las computadoras entre sí, creando senderos de datos redundantes y una alta tolerancia a fallos a costa de incrementar la complejidad a medida en que la red crece.

Las comunicaciones inalámbricas pueden utilizar una *topología celular* como la que se emplea ampliamente en las redes de teléfonos inalámbricos. En este caso, un área se divide en celdas ligeramente traslapadas, representando puntos de conexión.

El diseño físico de una red influye sobre otros factores, como por ejemplo, el método de acceso a los medios (y por ende el tipo de cable) que se utilice. Todos los factores físicos (tipo de cable, método de acceso, topología, etc.), considerados en conjunto, definen la *arquitectura* de la red. Las arquitecturas de redes más conocidas incluyen la Ethernet, ARCnet, Token Ring y AppleTalk.

Usted puede clasificar redes basándose en su arquitectura o en los estándares y las especificaciones para tipo de medios, topología física y lógica, método de acceso, limitaciones de distancia, dimensiones de los paquetes, encabezados y otros criterios. Las arquitecturas más populares son:

- **Ethernet** Creada en los años 1960 y basada en el método de acceso CSMA/CD, con especificaciones creadas por Digital, Intel y Xerox (regulada por los estándares IEEE 802.3).
- **Token Ring** Creada por la IBM y basada en el método de paso de señales (regulada por los estándares IEEE 802.5)

Las redes Ethernet se pueden dividir en subcategorías, dependiendo del tipo de cableado que se use, la topología y la velocidad de transferencia soportada, como sigue:

- **Ethernet 10Base5** Utiliza cable coaxial grueso, una topología de bus y transfiere datos a 10Mbps. A veces denominada Ethernet “estándar”, aunque hoy día es menos común que otros tipos.
- **Ethernet 10Base2** Utiliza cable coaxial fino, una topología de bus y transfiere datos a 10Mbps.
- **Ethernet 10Base-T** Utiliza cable UTP, una topología de estrella y transfiere datos a 10Mbps.
- **100Base-T** Similar a la 10Base-T, transfiere datos a 100Mbps. A veces denominada *Fast Ethernet* (Ethernet rápida).
- **1000Base-T** Similar a la 10Base-T, pero transfiere datos a 1000Mbps (1 Gbps). A veces denominada *Ethernet Gigabit*.

Nota

Existen otras subarquitecturas de Ethernet que utilizan diferentes medios o tienen especificaciones ligeramente diferentes. Por ejemplo, la 100Base-FL utiliza cableado de fibra óptica.

¿Por qué le concierne esto al investigador?

Comprender cómo los datos binarios se traducen en señales eléctricas u ópticas ayuda a los investigadores a comprender cómo esas señales pueden ser capturadas a través del cable o de las ondas del aire y, en algunos casos, traducidas nuevamente a su forma de datos. Esta es la forma más insidiosa de “allanar” la red, porque no deja la misma cantidad o el mismo tipo de pistas que podrían estar presentes cuando un criminal emplea métodos de un nivel más alto para robar datos. Ser capaz de identificar el tipo de red con la que está trabajando,

le da a Usted un punto de partida para comprender cómo se embalan y se transmiten los datos y qué vulnerabilidades en particular se encuentran en el nivel físico.

En las próximas secciones, Usted conocerá tipos específicos de medios y cómo algunos son más susceptibles que otros a una intercepción no autorizada. Conjuguar esta información con conocimientos sobre la teoría de la señalización le ayudará a reconocer qué pueden y qué no pueden lograr criminales cibernéticos con pericia técnica cuando están determinados a entrar a una red.

Comprendiendo los Modelos y Estándares de la Interconexión

Un *protocolo de red* es un conjunto de reglas que las computadoras utilizan para comunicarse. Hubo que crear los protocolos para que dos computadoras que intentan transferir datos entre sí fueran capaces de “comprenderse”.

Los primeros protocolos de redes fueron *propietarios* – o sea, cada vendedor de productos de redes creaba su propio conjunto de reglas. Las computadoras que usaban un producto específico se comunicarían entre sí, pero no podían comunicarse con computadoras que usaran un producto de red de otro vendedor. Esta situación tenía el efecto de limitar un negocio a un tipo específico de equipamiento de un vendedor en particular – en otras palabras, una compañía estaba limitada a comprar los productos de un vendedor específico si sus sistemas tenían que comunicarse entre sí.

La solución a este problema fue la creación de protocolos basados en *estándares abiertos*. El Departamento de Defensa de los Estados Unidos (DoD) creó el modelo original de interconexión en el que se basa el TCP/IP. Más tarde, la Organización Internacional de Estandarización (ISO) lo perfeccionó y se basó en él, creando el *modelo de Interconexión de Sistemas Abiertos* o *OSI*. Estos estándares fueron publicados de modo que estuvieran disponibles para aquellos vendedores que quisieran crear productos que se adhirieran a ellos. Como resultado, los consumidores ya no están forzados a comprar todos los productos de un mismo vendedor y la ventaja para el vendedor es que sus productos son mucho más compatibles y, por ende, se pueden usar en redes que utilicen también productos de otro vendedor.

Un modelo brinda una descripción fácil de entender de una arquitectura de red y sirve de base para estándares. Si vemos los modelos de redes más populares, observaremos que todos usan capas para representar áreas de funcionalidad. En el caso del OSI, cada especificación en capas utiliza los servicios de la capa de abajo para enriquecer el servicio. La división en capas proporciona una división lógica de responsabilidad, donde cada capa cumple funciones prescritas.

El Modelo de Interconexión OSI

Aunque el modelo DoD se creó primero, comenzamos observando el modelo OSI, porque se ha convertido en el punto de referencia común para el análisis de los protocolos de redes y los dispositivos de conexión. El modelo OSI se usa como una pauta abarcadora para

describir el proceso de comunicación de redes. No todas las implementaciones de protocolos concuerdan con el modelo OSI, pero este sirve como un buen punto de partida para comprender cómo los datos se transfieren a través de la red.

Las Siete Capas de OSI

El modelo OSI consta de siete capas. El número 7 tiene muchas connotaciones históricas. Algunos piensan que significa balance perfecto o incluso divinidad. Por sí o por no, este fue un factor cuando los diseñadores del modelo OSI decidieron cómo desglosar las capas funcionales. Es seguro decir que dentro de la comunidad técnica, las siete capas del modelo OSI son, por lo menos, tan legendarias como los Siete Pecados Capitales y las Siete Maravillas del Mundo.

Los datos pasan de una capa a la otra de abajo en la computadora remitente hasta que la capa física finalmente pone los datos en el cable de red. En la máquina receptora, los datos viajan de regreso hasta la pila en orden opuesto. Aunque los datos viajan por las capas hacia abajo en una parte de la transmisión y hacia arriba en la otra, el enlace de comunicación lógico es entre cada capa y la homóloga correspondiente, como se muestra en la Figura 5.3.

Así es como funciona el sistema: cuando los datos van hacia abajo a través de las capas, se *encapsulan*, o se encierran en una unidad mayor, mientras que cada capa adiciona su propia información de cabecera. Cuando los datos encapsulados llegan a la computadora receptora, el proceso ocurre al revés; la información pasa hacia arriba a través de cada capa y mientras viaja, la información encapsulada sale, una capa a la vez. La información adicionada por la capa de red, por ejemplo, es leída y procesada por la capa de red en la parte receptora. Tras procesar, cada capa elimina la información cabecera adicionada por su homóloga en la parte remitente.

Cuando la capa de aplicación finalmente le presenta los datos recibidos a la aplicación de usuario en la computadora receptora, los datos tienen de nuevo aproximadamente la misma forma que tenían cuando fueron enviados por la aplicación de usuario en la máquina que los originó. (La forma es idéntica sólo si las computadoras, los sistemas operativos, las aplicaciones y las configuraciones usados por el remitente y el receptor son idénticas). La Figura 5.4 ilustra cómo se adiciona la información de cabecera a los datos mientras avanzan hacia abajo a través de las capas.

Figure 5.3 The OSI networking model uses seven layers to represent the communication process.

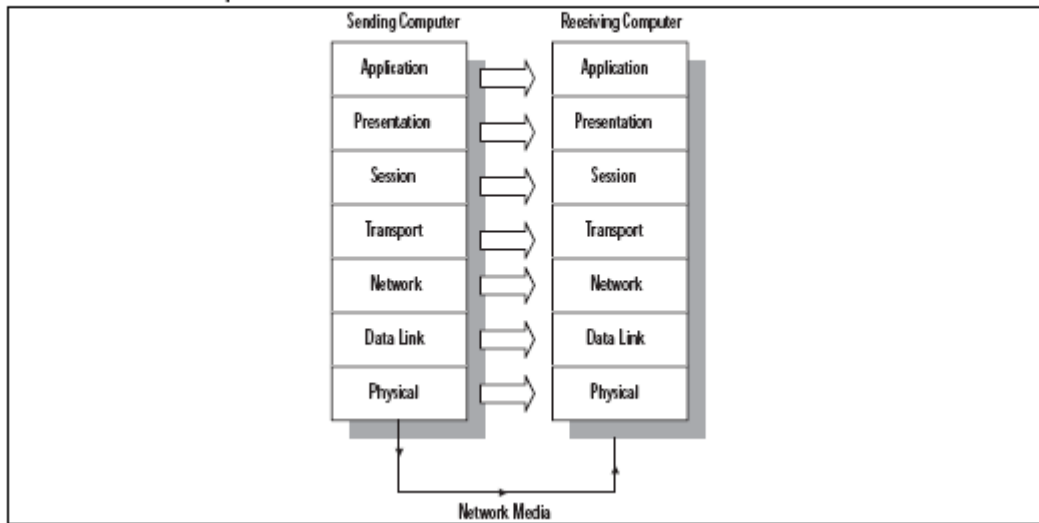


Figura 5.3 El modelo de interconexión OSI utiliza siete capas para representar el proceso de comunicación.

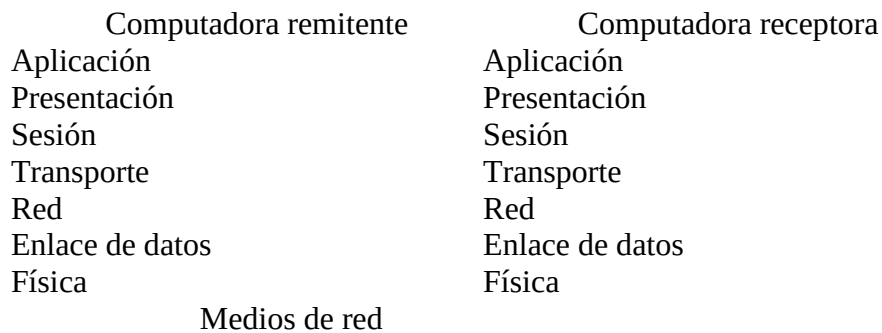


Figure 5.4 Protocols at each layer (except the physical layer) add header information to the data.

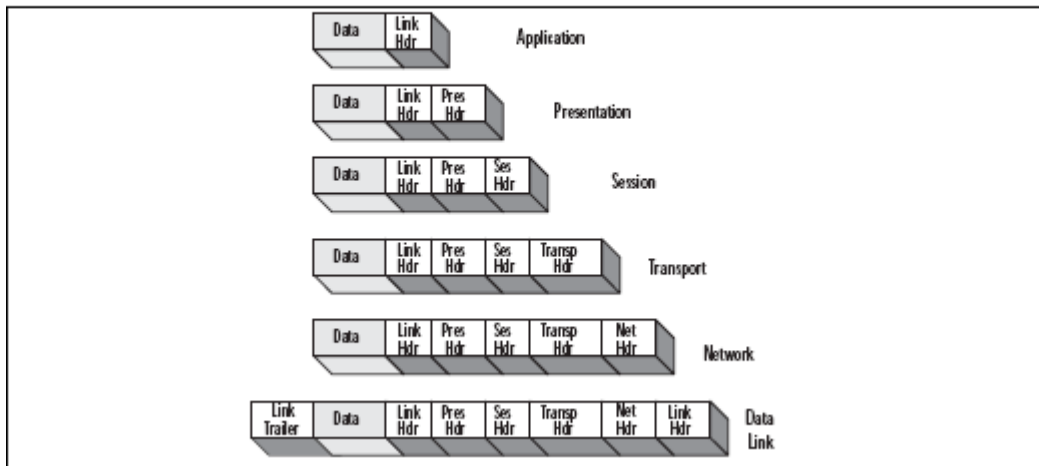
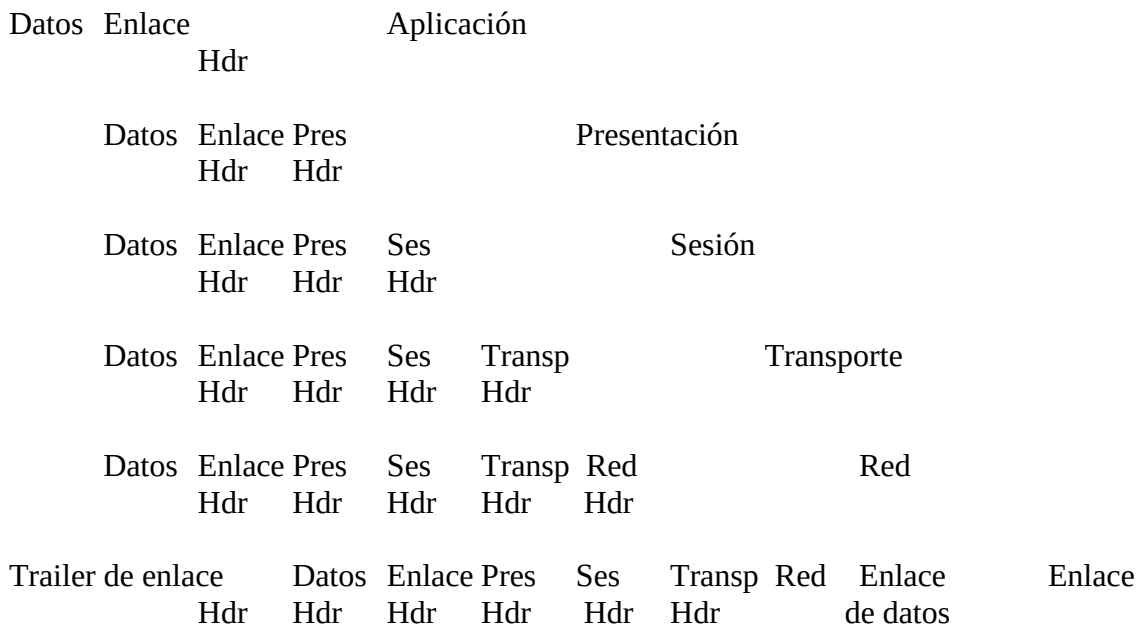


Figura 5.4 Los protocolos en cada capa (excepto la capa física) adicionan información de cabecera a los datos.



Muchos libros enseñan las capas del OSI “al revés” – o sea, comenzando con la capa de abajo. De hecho, a menudo, se refieren a la capa física como la Capa 1, la capa de enlace de datos como la Capa 2, etc. Otras descripciones comienzan (aparentemente de modo más

lógico) con la capa superior. La forma de verlo depende no del hemisferio en que Usted viva, sino de si está afrontando el proceso de comunicación desde el punto de vista de la computadora remitente o de la computadora receptora.

La Tabla 5.1 muestra la función de cada una de las siete capas, de “arriba hacia abajo”, pero conservando el esquema numérico tradicional.

Tabla 5.1 Cada capa del modelo OSI prescribe un conjunto específico de funciones.

Número de la capa/ Nombre de la capa	Función
7 Aplicación	Soporta los procesos de aplicación y de usuario final; brinda servicios de transferencia de ficheros, correos electrónicos y otros servicios de softwares de redes
6 Presentación	Lidia con las diferentes formas en que se representan los datos (compresión, encriptación), traduciendo del formato de aplicación al formato de red o viceversa.
5 Sesión	Establece, controla y pone fin a las conexiones entre aplicaciones en cada extremo.
4 Transporte	Transfiere los datos entre las máquinas, se ocupa del reconocimiento, chequeo de errores, recuperación y control del flujo.
3 Red	Se encarga del enrutamiento e intercambio utilizando direcciones lógicas (direcciones IP) al crear circuitos virtuales. Responsable del control de la congestión y la secuencia de paquetes.
2 Enlace de datos	Dividida en dos subcapas: control de acceso a los medios (MAC), que se ocupa de cómo las computadoras acceden a los datos y los transmiten en la red; y control de enlace lógico (LLC), que se ocupa de la sincronización de las tramas, del control del flujo y del chequeo de errores en el nivel de enlace.
1 Física	Interactúa con el hardware para dar la cadena real de bits como señales en los niveles eléctrico y mecánico.

El Modelo de Interconexión DoD

Cuando el DoD creó la pila de protocolos TCP/IP para la ARPAnet, el modelo OSI no había sido creado aún, de modo que el modelo usado era ligeramente diferente, de cierta forma más simple. A veces se le denomina modelo TCP/IP, pero casi siempre se le dice modelo DOD. Consiste en sólo cuatro capas, comparado con las siete capas del modelo OSI. Las capas del modelo DoD se corresponden aproximadamente con las del modelo OSI, como se muestra en la Figura 5.5.

Los varios protocolos en la suite TCP/IP encajan perfectamente en las capas del modelo DOD. Recuerden que el modelo DOD fue diseñado en los años 1970. El modelo OSI apareció una década más tarde con el objetivo de definir más específicamente las capas de funcionalidad para los componentes de redes.

Figure 5.5 The four layers of the DoD model map roughly to the seven OSI layers.

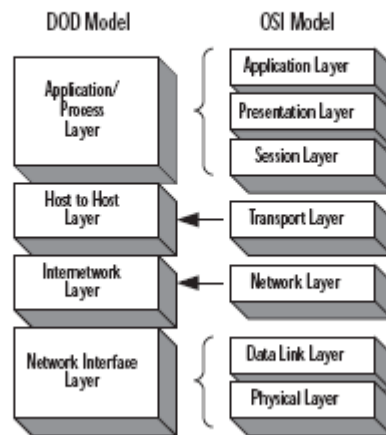


Figura 5.5 Las cuatro capas del modelo DoD se corresponden aproximadamente con las siete del modelo OSI.

Modelo DOD	Modelo OSI
Capa de aplicación/proceso	Capa de aplicación
	Capa de presentación
	Capa de sesión
Capa máquina a máquina	Capa de transporte
Capa Internet	Capa de red
Capa de interfaz de red	Capa de enlace de datos
	Capa física

La Capa de Aplicación / Proceso

La capa superior del modelo DOD abarca las tres capas superiores del OSI: aplicación, presentación y sesión. Por ende, cuando un artículo o libro se refiere al TCP/IP, Usted podría leer que la encriptación de datos, el chequeo de errores y el control de diálogo tiene lugar en la capa de aplicación. Recuerde que esto *no* significa la capa de aplicación del OSI y evitará confusiones.

La capa de (Transporte) Máquina a Máquina

La capa de máquina a máquina es denominada a veces capa de transporte, incluso en los diagramas de cuatro capas del DoD, y se puede representar como la capa de transporte del modelo OSI. Los protocolos TCP, UDP y DNS operan aquí.

La Capa Internet

La capa Internet se corresponde mucho con la capa de red del OSI. Los protocolos IP, ICMP (Protocolo de Control de Mensajes de Internet) y ARP (Protocolo de Resolución de Direcciones) funcionan en esta capa. Como analizamos anteriormente, el ARP traduce direcciones lógicas a direcciones MAC. Esta traducción es necesaria porque las capas más bajas pueden procesar solo las direcciones MAC.

La Capa de Interfaz de Red

La capa de interfaz de red se corresponde con las capas física y de enlace de datos del OSI. La suite TCP/IP en sí no tiene protocolos que operen en estas capas más bajas, pero usa los protocolos de la capa física y de la de enlace de datos de la Token Ring y de la Ethernet estándar.

Los Estándares de la Capa Física / de Enlace de Datos

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), al igual que la ISO, crea estándares. El Proyecto 802 fue nombrado así por el año y el mes en que se reunió el comité original, Febrero de 1980. Las especificaciones 802 del IEEE abordan varios aspectos de la capa física y de la de enlace de datos. Las más pertinentes para el administrador de red promedio son:

- **802.2** Establece estándares para la implementación de la subcapa LLC de la capa de enlace de datos.
- **802.3** Establece especificaciones para una red Ethernet usando CSMA/CD, una topología lineal o de bus estrella y transmisión de banda base.
- **802.5** Esta especificación establece estándares para una red de paso de señales, como por ejemplo, la Token Ring, usando una topología de estrella física /anillo lógico.
- **802.7** Establece criterios para redes usando transmisión de banda ancha.
- **802.8** Establece especificaciones para el uso de fibra óptica como un medio de la red.
- **802.11** Establece estándares para la interconexión inalámbrica.

¿Por qué esto le concierne al investigador?

Los modelos OSI y DoD conforman la base para comprender cómo las comunicaciones de redes están preparadas para la transmisión y cómo las señales que pasan a través de los medios son procesadas cuando llegan a su destino.

Los profesionales de la interconexión están preparados para solucionar problemas de comunicación “de abajo hacia arriba”, comenzando con la capa física y ascendiendo a través de los modelos. Los investigadores también son una especie de solucionadores de problemas y los mismos métodos de solucionarlos son apropiados al investigar crímenes cibernéticos que se basan en la implementación técnica, como por ejemplo, un acceso no autorizado o ataques a redes. Comprender la información de cabecera puede ser crucial

para rastrear la fuente del ataque, y el primer paso para comprenderla es saber cómo, cuándo y dónde esa información es adicionada al paquete de datos.

Comprendiendo el Hardware de la Red

De la misma forma que Usted necesita conocer el hardware que conforma una PC para comprender cómo funciona una computadora, necesita estar familiarizado con el hardware que posibilita la comunicación de la red a fin de comprender cómo funciona ese proceso de comunicación. Las redes pueden ser desde muy pequeñas (dos computadoras enlazadas directamente) hasta muy grandes (amplias áreas de Internet que se basan en dispositivos de hardware complejos para enlazar redes locales enteras en locaciones distantes). Sin embargo, toda interconexión de computadoras comienza con una *interfaz* conectando cada computadora a la red.

El Papel de la NIC

La *tarjeta de interfaz de red (NIC)* es el dispositivo de hardware más esencial para establecer la comunicación entre computadoras. Aunque existen formas de conectar computadoras sin una NIC (mediante módem a través de líneas telefónicas o a través de un cable serial “cero módem”, por ejemplo), en la mayoría de los casos, donde existe una red, hay una NIC (o, para ser más precisos, al menos una NIC por cada computadora participante).

La NIC es responsable de preparar los datos para que sean enviados a través de los medios de la red. El modo exacto de preparación depende del medio que se use. Una NIC de una Token Ring es diferente a la de una Ethernet, por ejemplo. Por lógica tiene que serlo, pues utilizan métodos de acceso diferentes. Y aún cuando las redes Ethernet 10Base2, 10Base5 y 10Base-T utilizan el CSMA/CD como su método de acceso, emplean diferentes tipos de cable y de conector, aunque es posible conseguir una tarjeta “combo” que tiene conectores para las tres.

La NIC se debe corresponder con el tipo de bus para el que Usted tiene una ranura abierta en la computadora. Debe ser del tipo correcto de acceso a los medios, debe tener el conector correcto para el cable que use su red y debe estar en condiciones de transferir datos a la velocidad apropiada. (Ethernet normalmente transmite a 10Mbps o 100Mbps, y la Token Ring corre a 4Mbps o 16Mbps).

El Papel de los Medios de Red

Los *medios de red* son las tecnologías inalámbricas o por cable con las que se envía la señal. Los tipos de cable incluyen el coaxial grueso y fino (similares al de los medios de TV por cable, pero no el mismo), cable par trenzado (como el que se usa para las líneas telefónicas modernas, existen de dos tipos: blindado y sin blindar, o cable de fibra óptica que envía pulsos de luz a través de finos filamentos de cristal o plástico para una comunicación más rápida y estable, pero es costoso y difícil de trabajar con ellos. Los medios inalámbricos incluyen ondas de radio, láser, infrarrojo y microondas.

Los datos pueden ser capturados directamente de los medios por personas no autorizadas, “interceptando” el cable y utilizando un analizador de protocolos para abrir paquetes y visualizar los datos de adentro. Los cables de cobre son especialmente fáciles de comprometer de este modo, pero los datos también pueden ser interceptados en el cableado de fibra óptica utilizando un dispositivo llamado *splitter óptico*. Las transmisiones inalámbricas también son fáciles de interceptar. La práctica de la “guerra móvil” es popular entre los hackers que configuran sistemas laptop con tarjetas de redes inalámbricas y después merodean en busca de redes inalámbricas abiertas para conectarse a ellas. Como muchos negocios dejan la configuración implícita en sus puntos de acceso inalámbricos y no eligen usar protocolos de encriptación inalámbricos, sus redes están ampliamente abiertas para cualquiera con una computadora portátil, una NIC inalámbrica y una pequeña cantidad de conocimientos técnicos. En el Capítulo 8, “Implementando la Seguridad del Sistema” se aborda en detalles el tema de la seguridad inalámbrica).

En la escena...

Cuando el Medio es la Línea Telefónica

La interconexión con acceso remoto utiliza las líneas telefónicas como el medio de la red y un *módem* (un dispositivo que modula y desmodula señales para convertirlas del formato digital de la computadora al formato análogo del sistema telefónico público y viceversa) en lugar de una NIC. Para establecer una conexión de marcado con una computadora remota, se utilizan los *protocolos de enlace* como por ejemplo, el PPP (Protocolo de Punto a Punto) y el SLIP (Protocolo de Internet de Línea Serial). Entonces se usa una pila regular de protocolos de red/transporte como el TCP/IP para comunicarse con la computadora remota y otras computadoras en su red local. Esta es la forma en que Usted se conecta a su servidor remoto del ISP, y, a través de él, a la conexión del ISP con Internet. Una vez conectado a la red remota, Usted puede validarse empleando la misma cuenta de usuario y contraseña que utiliza al registrarse en el sitio, y puede hacer todo (si tiene los permisos de acceso apropiados) lo que podría hacer desde una máquina físicamente conectada por cables a la red remota. La única diferencia es la velocidad; las líneas telefónicas son mucho más lentas que las conexiones LAN más lentas.

Otro tipo de acceso remoto involucra la creación de una *red privada virtual (VPN)* que le permite “abrir un túnel” a través de Internet usando protocolos especiales de túneles, como por ejemplo:

- Protocolo de Túnel Punto a Punto (PPTP)
- El Protocolo de Túnel Capa 2 (L2TP)
- Capa 2 Transportadora (L2F)
- Protocolo de Seguridad IP (IPSec)

Estos protocolos permiten una conexión privada (encriptada) con una computadora remota cuando ambas están conectadas a Internet, permitiendo comunicaciones privadas a través de una infraestructura pública (y ahorrando el costo de larga distancia si el servidor remoto se encuentra geográficamente distante). Para más información acerca de la VPN, véase la

clase en www.wkmn.com/newsite/vpn.html o la panorámica sobre la VPN en www.intranetjournal.com/foundation/vpn-1.shtml.

Los Roles de los Dispositivos de Conectividad de Redes

Los dispositivos de conectividad de redes hacen exactamente lo que su nombre implica: conectan dos o más segmentos de cable. Los dispositivos de conectividad complejos pueden servir a dos propósitos aparentemente opuestos: se usan para dividir grandes redes en pequeñas partes (llamadas *subredes* o *segmentos*, en dependencia del tipo de dispositivo) y se usan para fusionar redes pequeñas con una red mayor denominada *internetwork* o *Internet*. Los dispositivos de conectividad menos complejos no hacen ninguna de las dos funciones; se emplean meramente como puntos de conexión para las computadoras en una red (o segmento de red) o para amplificar las señales de las computadoras interconectadas, lo que aumenta la distancia a la que las transmisiones pueden ser enviadas. Ellos pueden también:

- Conectar segmentos de redes que usen diferentes tipos de medio (por ejemplo, cable coaxial fino y UTP)
- Segmentar la red para reducir el tráfico sin dividir la red en subredes IP individuales.

Analizaremos brevemente algunos de estos dispositivos en las siguientes subsecciones.

Repetidores y Concentradores

Los *concentradores* y los *repetidores* son dispositivos de conexión. Los analizamos juntos porque, en muchos casos, son lo mismo. De hecho, Usted oirá referirse a los concentradores como *repetidores multipuerto*. Los repetidores conectan dos segmentos de red (generalmente cable coaxial fino o grueso) y potencian la señal de modo que la distancia del cableado se puede extender más allá de los límites en los que la atenuación o debilitación interfiere con la transmisión estable de los datos.

Un repetidor se usa para extender la longitud utilizable de un tipo de cable dado. Por ejemplo, una red Ethernet 10Base5, usando cable coaxial grueso, tiene un máximo de longitud de segmento de cable de 500 metros o 1640 pies. A esa distancia comienza a tener lugar la *atenuación* (pérdida de la señal debido a la distancia). Pero cuando Usted coloca un repetidor al final del cable y anexa otra longitud al segundo puerto del repetidor, la señal se potencia y los datos pueden seguir viajando sin daño o pérdida, como se muestra en la Figura 5.6.

Figure 5.6 Repeaters address the problem of attenuation (signal loss due to distance).

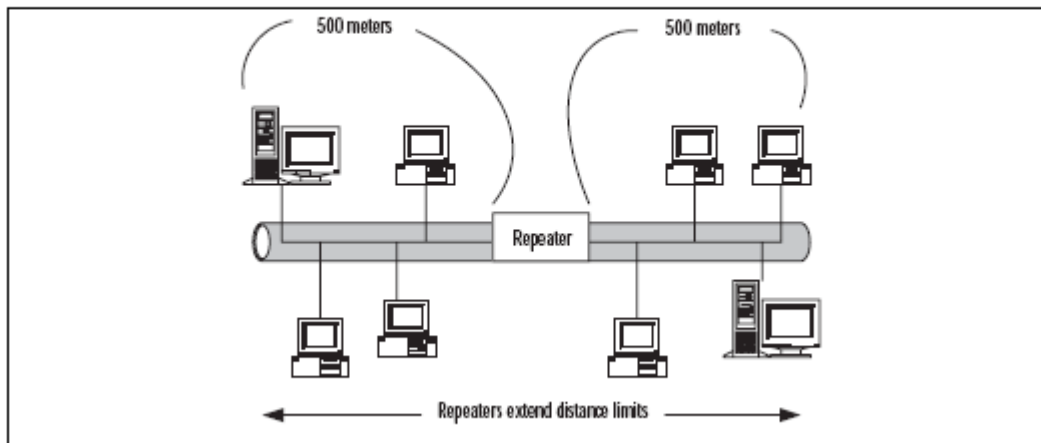


Figura 5.6 Los repetidores solucionan el problema de la atenuación (pérdida de la señal debido a la distancia).

500 metros

500 metros

Repetidor

Los repetidores extienden los límites de distancia.

Nota

Los repetidores no son dispositivos muy “inteligentes”. Ellos simplemente potencian cualquier señal que reciban, sin distinguir entre datos y ruido, y pasan la señal. Tampoco son muy “cortes”. No siguen el proceso usual del CSMA/CD, que usan las NIC de prestar atención al tráfico antes de transmitir. Un repetidor potencia y transmite, incluso si el otro nodo está a mitad de una transmisión. Esta situación, por supuesto, trae como resultado una colisión de datos, lo que significa que los datos tienen que ser reenviados y el rendimiento de la red resulta negativamente impactado. También tenga en cuenta que los repetidores no segmentan o dividen la red de forma lógica, y no filtran el tráfico. Usted no puede reducir la carga de tráfico o incrementar el ancho de banda disponible de la red usando repetidores; Usted sólo puede amplificar la señal y extender la longitud máxima del cable.

En la escena

La Diferencia entre los Repetidores y los Amplificadores

Un repetidor potencia la señal que viaja a través del cable de una Ethernet casi de la misma forma en que un amplificador potencia la entrada de señal de un viejo transmisor de radio. La diferencia entre un repetidor y un amplificador no radica en lo qué hacen, sino en el tipo de señales a las que se lo hacen.

Los amplificadores potencian señales análogas (como aquellas usadas en la red telefónica pública o en antiguos sistemas estéreos caseros); los repetidores potencian las señales digitales empleadas en la mayoría de las comunicaciones de computadoras.

Los concentradores son diferentes a los repetidores básicos, toda vez que el repetidor generalmente tiene sólo dos puertos, mientras que el concentrador puede tener muchos más (por lo general de 5 a 64 o más). Los concentradores se pueden conectar también a otro concentrador, proporcionando aún más puertos. Los concentradores se usan generalmente con el cable par trenzado de la Ethernet, y la mayoría de los concentradores modernos son repetidores con múltiples puertos. Ellos también fortalecen la señal antes de pasarla de regreso a las computadoras conectadas a ellos. Los concentradores se pueden clasificar de esta forma:

- **Concentradores pasivos** Estos concentradores sirven sólo como puntos de conexión; ellos no potencian la señal. Los concentradores pasivos no requieren de electricidad y por lo tanto, no usan un cable de energía como los concentradores activos.
- **Concentradores activos** Estos concentradores sirven como punto de conexión y amplificador de señal. Los datos que entran, pasan de retorno a todos los puertos. Los concentradores activos requieren de energía eléctrica.
- **Concentradores inteligentes o “listos”** Estos son concentradores activos que incluyen un chip microprocesador con capacidades de diagnóstico, de modo que Usted puede monitorear la transmisión en puertos individuales.

Otro tipo de concentrador, llamado *concentrador de intercambio*, opera en la capa de enlace de datos en lugar de en la física y es más comúnmente llamado *switch*.

Nota

Los concentradores presentan un riesgo de seguridad porque todos los mensajes que van hacia todas las computadoras pasan por todos los puertos. Esto le facilita a una persona no autorizada, que puede acceder a los salones u oficinas de los servidores donde radican los concentradores, conectar sencillamente una laptop e interceptar datos.

Puentes

Los *puentes* operan en la capa de enlace del modelo OSI. Los puentes pueden separar una red en segmentos, pero no pueden *dividirla en subredes* como lo hacen los enrutadores. En otras palabras, si Usted usa un puente para separar físicamente dos áreas de la red, aún así parece ser una red completa para los protocolos de niveles más altos.

Un puente monitorea las tramas de datos que recibe para construir una tabla de direcciones MAC, empleando las direcciones fuente en las tramas. Esta es una tabla simple que le dice al puente en qué lado radica una dirección en particular. Entonces el puente puede estudiar la dirección de destino en una trama y, si está en la tabla, determinar si la deja cruzar el puente (si la dirección está en el otro lado) o no (si la dirección está en el lado de donde se recibió).

De esta forma, se genera menos cantidad de tráfico innecesario, porque cuando una computadora en el lado A envía un mensaje a otra computadora que también está en el lado A, la señal va sólo a aquellas computadoras del lado A. Las computadoras en el lado B, en el otro lado del puente, continúan alegremente con sus tareas y no tienen que lidiar jamás con el mensaje.

Los puentes pueden disminuir la congestión de la red porque pueden hacer algunos filtros básicos de datos basados en la dirección MAC de la computadora destino. Cuando la transmisión llega al puente, este no la dejará pasar al otro lado de la red si la dirección MAC de la computadora destino se sabe que está en el mismo lado de la red que la computadora remitente, como se muestra en la Figura 5.7.

Figure 5.7 Bridges segment networks to reduce traffic.

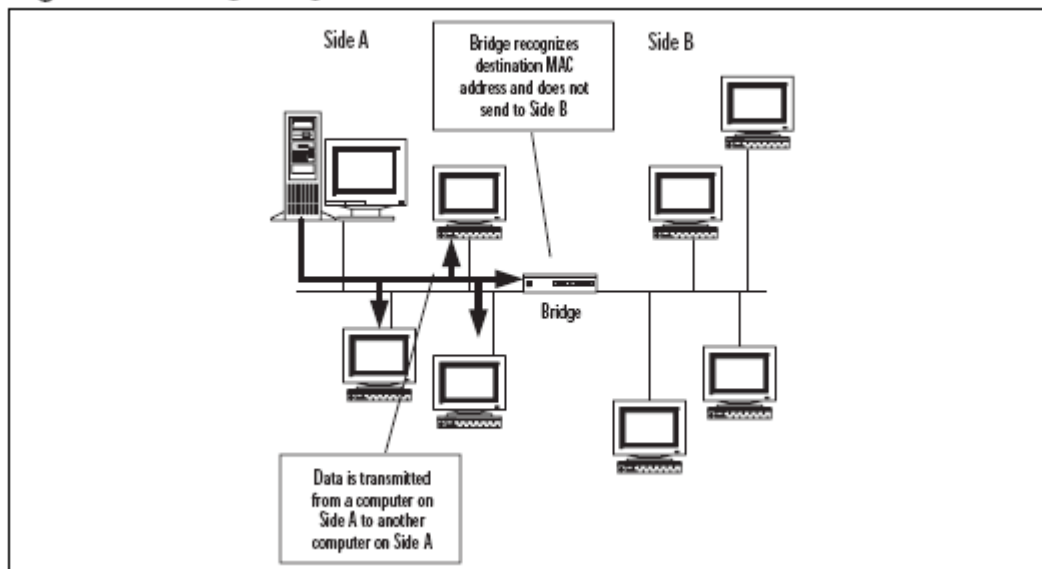


Figura 5.7 Los puentes segmentan redes para reducir tráfico.

Lado A	El puente reconoce la dirección MAC de destino y no envía al Lado B	Lado B

Puente

Los datos se transmiten de una computadora en el Lado A hacia otra computadora en el Lado A.

En la escena....

Tipos de Puentes

Existen diferentes tipos de puentes. Aunque todos los tipos trabajan en la capa de enlace de datos, algunos operan en la subcapa inferior MAC y otros en la subcapa superior LLC. Existen algunas diferencias importantes entre los tipos de puentes. Una pregunta práctica es si Usted puede utilizar un puente para conectar segmentos de red que empleen métodos de acceso a los medios diferentes (por ejemplo, un segmento Ethernet y uno Token Ring). La respuesta es sí – o no, en dependencia del tipo de puente al que se haga referencia.

Un puente que opera en la subcapa LLC, a veces denominado *puente de traducción*, puede conectar segmentos usando diferentes métodos de acceso. Sin embargo, un puente de nivel más bajo (uno que opere en la subcapa MAC) no puede hacerlo. Sin embargo, cualquier tipo puede conectar segmentos empleando medios físicos diferentes – o sea, un segmento cableado con coaxial fino y un segmento corriendo sobre cable UTP.

Los puentes de traducción *no* traducen entre protocolos. Los puentes ignoran los protocolos de red/transporte empleados para la comunicación y no dependen de ellos. Los puentes pueden usar solamente las direcciones MAC. Como los puentes no analizan los protocolos de capas superiores como el IP, no pueden tomar decisiones sobre dónde enviar las tramas de datos basados en la dirección IP.

Switches

Los switches de la capa 2, o concentradores de intercambio, trabajan en la capa de enlace de datos y están instalados en lugar de los concentradores activos que han sido usados más frecuentemente para conectar computadoras en una red con cable UTP. Reemplazar concentradores por switches cuesta un poco más que emplear sólo concentradores, pero ofrece ventajas importantes.

Un switch combina las características de los concentradores y los puentes. Al igual que un puente, un switch construye una tabla de direcciones MAC. El switch sabe qué interfaz de red de computadoras (identificada por su dirección física) está conectada a cuál de sus puertos. Entonces puede determinar la dirección de destino para un paquete en particular y lo enruta solamente hacia el puerto al que la NIC está conectada. Obviamente, este sistema reduce una buena cantidad del uso innecesario del ancho de banda, pues el paquete no se envía al resto de los puertos donde será ignorado cuando esas computadoras determinen que no estaba destinado a ellos. En la Figura 5.8 se ilustra este proceso.

Figure 5.8 Switches reduce traffic by sending data only out the port with which the destination MAC address is associated.

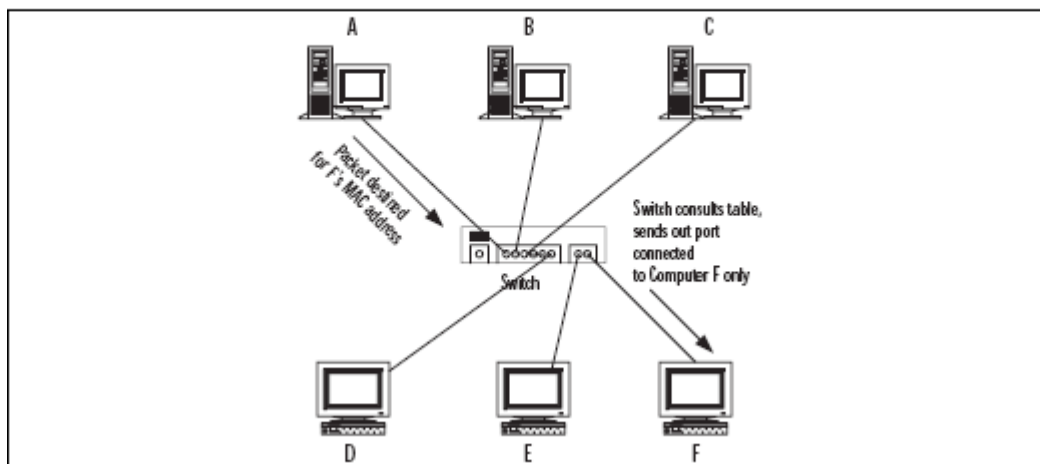
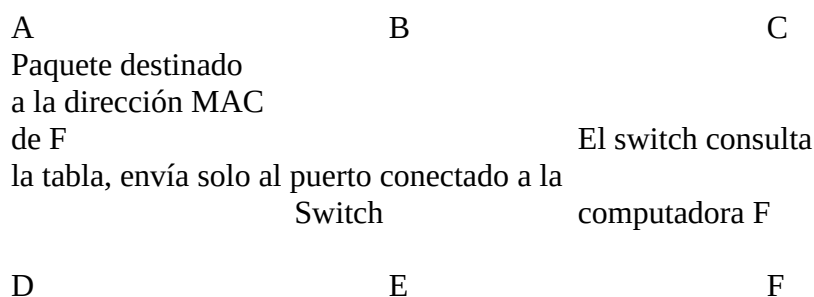


Figura 5.8 Los switches reducen tráfico al enviar datos sólo al puerto al que está asociada la dirección MAC de destino.



El uso de switches en lugar de concentradores crea “dominios de colisión” individuales para cada segmento (la longitud del cable entre el switch y cada nodo). Esto significa que una computadora en particular recibe sólo los paquetes direccionados a ella, a una dirección multicast a la que ella pertenezca o a la dirección broadcast. Usted incrementa el ancho de banda potencial de esta manera por el número de dispositivos conectados al switch, porque cada computadora puede enviar y recibir al mismo tiempo que uno o más nodos lo hacen.

Los switches pueden reenviar tramas de datos más rápidamente que los puentes porque en lugar de leer toda la trama Ethernet entrante antes de reenviarla al segmento de destino, el switch generalmente lee la dirección de destino en la trama y entonces la retransmite al segmento correcto. Es por eso que los switches pueden ofrecer menos retrasos y retrasos de menos duración en toda la red, trayendo como resultado un mejor rendimiento.

Recientemente un tipo de switch que opera en la capa de red o Capa 3 del modelo OSI, se convirtió en una popular opción de conectividad. Un switch de Capa 3, a veces referido como *switch enrutador*, es de hecho un tipo de enrutador. Aunque un switch de Capa 2 (concentrador de intercambio) es incapaz de distinguir protocolos, un switch de Capa 3 realmente realiza las funciones de un enrutador. Un switch de Capa 3 puede filtrar los

paquetes de un protocolo específico para permitirle a Usted continuar reduciendo el tráfico de la red.

Los switches de Capa 3 realizan las mismas tareas que los enrutadores y se pueden utilizar en las mismas locaciones en las que tradicionalmente se emplea un enrutador. Sin embargo, el switch de Capa 3 supera la desventaja de rendimiento de los enrutadores, por lo que el enrutamiento es una de las prioridades de la tecnología de los switch. Los switches de Capa 3, manufacturados por compañías como Cisco (uno de los más conocidos fabricantes de los enrutadores tradicionales) se han convertido rápidamente en la solución de excelencia para la conectividad de redes empresariales.

Enrutadores

Al igual que los concentradores y los switches, los enrutadores son dispositivos de conectividad multipuerto. A diferencia de los concentradores y los switches de Capa 2, los enrutadores son apropiados para usar en redes grandes y complejas porque son capaces de utilizar la dirección IP lógica para determinar hacia donde necesitan ir los paquetes.

¿Cómo el uso de la dirección IP ayuda a simplificar el proceso de enrutamiento? Recuerde que una dirección IP se divide en dos partes: el ID de la red y el ID de la máquina. El ID de la red es la clave aquí porque “restringe” la locación de una computadora destino en particular actuando casi de la misma forma en que lo hace el código ZIP para la oficina de correos.

Los enrutadores se emplean para manejar tareas de enrutamiento complejas. También reducen la congestión de la red al confinar mensajes broadcast a una sola subred. Un enrutador puede ser un dispositivo dedicado (como aquellos hechos por Cisco) o una computadora corriendo un sistema operativo que es capaz de actuar como enrutador. Windows 2000, al igual que Windows NT, puede funcionar como un enrutador cuando dos tarjetas de redes están instaladas y el reenvío IP está habilitado.

Los enrutadores son capaces de filtrar, de modo que Usted puede, por ejemplo, bloquear el tráfico entrante. Esta capacidad le permite al enrutador actuar como un *muro de fuego*, creando una barrera que evita que paquetes indeseables entren o salgan de un área designada de la red. Sin embargo, en general, si se configura un enrutador para que filtre mucho, su rendimiento será menor. Más adelante, en este capítulo, analizaremos en detalles cómo funciona el enrutamiento IP, en la sección sobre direccionamiento IP.

En la escena...

El matrimonio entre el puente y el enrutador

Aunque su nombre podría sonar como el resultado increíble de algún experimento de ADN recombinante, el *brouter* es un dispositivo que intenta combinar las características de los puentes y los enrutadores en una solución con lo “mejor de ambos mundos”. Esto puede resultar de utilidad cuando algunos nodos en la red están corriendo protocolos no routables (trazables), como el NetBEUI, mientras otros usan protocolos que se benefician con el

enrutamiento. Un brouter funciona como un enrutador, empleando direcciones IP para tomar decisiones de enrutamiento cuando los paquetes son enviados empleando un protocolo routable (trazable) como el TCP/IP, pero si se utiliza uno no routable (trazable), el brouter emplea la dirección MAC para funcionar como un puente. Como realiza las funciones de enrutador y puente, los brouters operan en ambas capas del modelo OSI: la de enlace de datos y la de red. Los brouters no se ven muy a menudo en las redes actuales.

En la escena...

Utilizando el ID de Red para “Limitar la Búsqueda”.

En un pueblo pequeño, todas las calles podrían compartir el mismo código ZIP, de modo que una carta dirigida a 100 Hall Street, Alguna Ciudad, Texas, no necesita realmente un código ZIP. Llegará a su destino, porque sólo existe una oficina de correos en esa ciudad y puede ubicar fácilmente todas las calles del pueblo. Sin embargo, en una ciudad grande con varios códigos ZIP, una carta dirigida a 100 Hall Street, Gran Ciudad, Texas, presentará mayores dificultades para llegar a su destino. Esto sucede porque existen varias oficinas de correos en la Gran Ciudad, cada una diseñada para servir a sólo una parte designada de la ciudad. Es el código ZIP el que identifica cuál de esas estaciones de oficina de correos se encargará de la entrega de la carta, así como el ID de red identifica en cuál subred o parte de la red se encuentra la computadora destino.

Pero la oficina de correos debe “estar al tanto del código ZIP” a fin de utilizar esa información. O sea, los empleados que clasifican el correo en la oficina de correos deben entender lo que significan los códigos ZIP. Si los empleados que realizan esta tarea proceden de una época anterior al surgimiento de los códigos ZIP, verán una serie de números al final de la dirección, y sin entender su significado, los ignorarán. Al igual que esos empleados postales de un tiempo atrás, los puentes y otros dispositivos de capas inferiores no reconocen las direcciones IP ni las utilizan al tomar decisiones sobre adónde enviar los datos.

Sin embargo, los enrutadores que trabajan en la capa de red donde opera el IP, pueden comprender y emplear las direcciones IP. Un enrutador también mantiene una tabla, pero, a diferencia de un puente o un switch, que sólo lidia con direcciones MAC, la tabla de enrutamiento le dice al enrutador cómo llegar a otras redes conocidas (o subredes), basándose en el ID de la red. Entonces, cuando un paquete llega a la red apropiada, se utiliza el ID de la máquina para llegar a la computadora específica a la que estaba destinado.

Puertas de enlace

Las puertas de enlace no se implementan generalmente como “dispositivos” (aunque pueden serlo). En vez de ello, se implementan como programas de software corriendo en

servidores. Sin embargo, como también se emplean para conectar redes distintas, abordaremos brevemente qué son y por qué se implementan en muchas redes.

Las puertas de enlace operan normalmente en los niveles superiores del modelo OSI – por lo general en la capa de aplicación – y se pueden usar para conectar dos redes que empleen protocolos completamente diferentes. Por ejemplo, una puerta de enlace SNA (la más reciente versión de Microsoft se denomina Host Integration Server) le permite a las computadoras personales que corren sistemas operativos Windows comunicarse con una computadora central de la IBM, aún cuando los dos sistemas ven al otro como “alienígena”. Otro tipo de puerta de enlace se emplea para permitir que las máquinas Windows, que utilizan el protocolo de compartimiento de ficheros SMB, le “hablen” a un servidor de ficheros que corre NetWare NOS y emplea el protocolo NCP (NetWare Core Protocol). Existen otros tipos diferentes de puertas de enlace, como las puertas de enlace de correo electrónico, que traducen entre protocolos de correo electrónico.

¿Por qué le concierne esto al investigador?

El hardware de la red controla la manipulación de los datos una vez que estos abandonan la computadora y comienzan su viaje a través de la red. Comprender cómo trabajan los dispositivos de red ayuda a los investigadores a comprender cómo se pueden capturar las señales mientras transitan por la red y cómo una persona no autorizada que es capaz de acceder a los lugares puede conectar una laptop a un concentrador y capturar el tráfico de datos o interceptar un cable empleando un splitter e interceptar los datos que fluyen a través de él.

Comprendiendo el software de la red

Los sistemas operativos modernos tienen implícitas capacidades de interconexión. Los primeros sistemas operativos de PC como el DOS (y el esqueleto de Windows que corría en ellos) no las tenían. No fue hasta la versión 3.11, con Windows for Workgroups, que Microsoft incluyó componentes de redes. Como su nombre implica, la versión de Windows fue diseñada para funcionar en una pequeña red local de máquina a máquina. Windows NT adicionó la funcionalidad de servidor de autenticación (Microsoft llamó al servidor de autenticación *controlador de dominio*), pero con las primeras versiones de NT, la atención estaba centrada en la LAN, no en la WAN. En aquel tiempo, los sistemas operativos de Microsoft no se consideraban lo suficientemente escalables para redes empresariales, y la mayoría de los servidores de Internet eran máquinas UNIX. Con Windows 95 se hizo más fácil para los usuarios conectarse a Internet y NT 4.0 soportaba servicios Web (Internet Information Server) que facilitaron el hospedaje de sitios Web en Internet o en las redes internas. Windows 2000 contribuyó de forma significativa a la conectividad de Internet y adicionó características a los productos de servidores que lo tornaron más apropiado para el trabajo con computadoras a nivel empresarial, incluyendo un robusto servicio de directorio (Directorio Activo), protocolos de seguridad estándares para la industria como Kerberos e IPSec, y soporte de agrupamiento y balance de carga. La próxima generación de servidores Windows, .NET, continúa esta tendencia y abraza la idea de que “la red es la computadora” en mayor medida que nunca.

El término *sistema operativo de red (NOS)* se utiliza de tres formas diferentes:

- A veces se emplea para referirse a cualquier sistema operativo de computadora que tenga incluido componentes de redes como es el caso de todos los sistemas operativos de las populares PC actuales. Por lo tanto, Windows 9x, NT, 2000, XP y .NET (junto con la mayoría de las versiones de Linux, UNIX, Macintosh y OS/2 Warp) se consideran NOS, no así MS-DOS, Windows 3.1 y anteriores.
- A veces se emplea para referirse a los componentes del sistema operativo que posibilita la interconexión. Por ejemplo, los actuales sistemas operativos de Windows incluyen servicios de compartimiento de ficheros e impresión (conocidos como el servicio de Servidor en NT), que le permiten a la computadora actuar como un servidor y compartir sus recursos con otros sistemas, y el Cliente para Redes Microsoft (conocido como el servicio de Estación de Trabajo en NT), que le permite a la computadora conectarse y acceder a los recursos compartidos de otros sistemas. Estos componentes, conjuntamente con las pilas de protocolos sobre los cuales opera la red, son referidos, a veces, como el NOS.
- A veces se emplea para referirse al software del sistema operativo del servidor – como Windows NT Server, Windows 2000 Server o NetWare – especialmente cuando funciona como un servidor de autenticación que mantiene una base de datos de seguridad que contiene todas las cuentas de la red.

En las siguientes secciones veremos cómo funciona la computación cliente/servidor y analizaremos el software del servidor y el del cliente que funcionan de conjunto para habilitar las comunicaciones dentro de la red. También estudiaremos los sistemas de ficheros de la red y cómo ellos difieren de los sistemas de ficheros locales, así como los protocolos que gobiernan el proceso de comunicación de la red.

Comprendiendo la Computación Cliente/Servidor

El término computación cliente/servidor tiene diferentes significados, en dependencia del contexto en que se emplee. Alguna documentación utiliza el término limitadamente, para referirse a aplicaciones en las cuales la mayor parte del procesamiento se realiza en un servidor. Por ejemplo, SQL Server es una aplicación de base de datos que utiliza la energía del servidor para clasificar los datos en respuesta a una pregunta y después retorna sólo los resultados al cliente. Este sistema contrasta con Access de Microsoft, en el que los ficheros de base de datos están almacenados en un servidor, pero una pregunta del cliente resulta en la transferencia de todo el fichero hacia la máquina cliente, donde tiene lugar la clasificación.

Utilizando este significado del término, *thin client computing* es la forma primordial de la computación cliente/servidor. Con el software de thin client como los servicios terminales de Microsoft, el sistema operativo corre en el servidor, y todas las aplicaciones corren allí, sólo la representación gráfica de la pantalla de escritorio corre en la máquina cliente. Esto significa que las máquinas clientes pueden ser sistemas de baja energía con procesadores modestos y pequeñas cantidades de RAM – máquinas que no son capaces de correr por sí mismas el sistema operativo. Por ende, un usuario puede trabajar en Windows 2000

utilizando un sistema antiguo 80486 que sólo tiene 16MB de RAM, porque el sistema operativo no está corriendo realmente en ese sistema antiguo – sólo se está usando como un Terminal para acceder al OS en el servidor.

Redes basadas en servidores de autenticación

Un segundo y más amplio significado del término *computación cliente/servidor* se refiere a una red basada en un servidor de autenticación. Este es un servidor que controla el acceso a la red, almacenando una base de datos de seguridad que sostiene la información de las cuentas de los usuarios de toda la red. Cuando un usuario quiere validarse en la red, la computadora cliente contacta a su servidor de autenticación. El servidor chequea su base de datos para asegurarse de que el usuario está autorizado y para determinar el nivel de acceso permitido para ese usuario (generalmente basado en grupos de seguridad a los que pertenece el usuario). El servidor de autenticación es un punto de seguridad centralizado y un punto de administración de los recursos de la red y debe correr softwares de servidores especiales (y generalmente costosos). En redes Microsoft, este tipo de red se denomina *dominio* y el servidor de autenticación se demoniza *controlador de dominio*. Los servidores UNIX y Netware también brindan servicios de autenticación en redes.

Nota

En el Capítulo 7, cuando analicemos los conceptos de seguridad, analizaremos mucho más detalladamente *la autenticación*, que se refiere a la verificación de la identidad de un usuario o una computadora.

Los sistemas operativos de servidores de autenticación como el NT Server usan una base de datos plana que contiene la información de las cuentas, pero la tendencia es hacia el empleo de bases de datos jerárquicas denominadas *servicios de directorio*, como el NDS de Novell y el Directorio Activo de Microsoft. El nuevo Macintosh OS X Server utiliza un servicio de directorio un poco menos robusto llamado NetInfo. Todos estos servicios tienen algo en común: son compatibles con los estándares del LDAP (Protocolo de Acceso al Directorio Ligerito). Este es un estándar industrial basado en las especificaciones de la ISO X.500, y la adherencia a los estándares le permite a los servicios de directorio de diferentes vendedores operar entre sí dentro de una red.

Estas redes cliente/servidor (o basadas en servidores) ofrecen muchas ventajas, especialmente para redes grandes. Debido a que la seguridad y la administración son centralizadas, este tipo de red puede asegurarse y administrarse mejor que el modelo de red alternativo.

Redes máquina a máquina

Las redes sin un servidor de autenticación se denominan *redes máquina a máquina* o de *grupos de trabajo*. Este modelo es apropiado para redes pequeñas con sólo pocas computadoras, en ambientes donde no se requiere de una alta seguridad. En un grupo de trabajo, todas las computadoras pueden ofrecer servicios de cliente y de servidor.

Nota

En este contexto, el término *servicios de servidor* significa solamente que las computadoras hacen que sus recursos sean accesibles a otras computadoras en la red (los comparten con ellas). Las computadoras en un grupo de trabajo no tienen que correr softwares de servidores costosos, aunque un grupo de trabajo puede tener máquinas corriendo softwares tales como Windows 2000 Server, operando como *servidores miembro* en lugar de controladores de dominio. El factor clave que las diferencia es que en un grupo de trabajo no existe un servidor de autenticación, aunque pueden existir otros tipos de servidores (servidores de ficheros e impresoras, de acceso remoto, de fax, etc.).

Los grupos de trabajo son menos costosos para implementar redes basadas en servidores, por varias razones:

- Se debe comprar un software para el sistema operativo del servidor, que cuesta desde varios cientos hasta varios miles de dólares, para implementar una red basada en servidor.
- El software del servidor requiere generalmente de un hardware más poderoso que los sistemas operativos de escritorio, de modo que necesitaría comprar una maquinaria más costosa para correrlo.
- Las redes basadas en servidores requieren generalmente de un administrador de red dedicado para realizar las muchas tareas que implica la administración y el mantenimiento de una red, lo que conllevaría a la necesidad de contratar personal adicional o de trabajo extra por parte de un empleado ya existente.

A pesar de la ventaja del costo de los grupos de trabajo, estos son menos seguros, porque el usuario de cada computadora puede administrar sus recursos. En aras de acceder a recursos de cualquier otra computadora en el grupo de trabajo, un usuario debe tener una cuenta local creada en esa máquina, o alternatively, cada recurso compartido puede protegerse con una contraseña. Cualquiera de estos métodos se torna muy engorroso cuando hay más de un puñado de usuarios y/o más de unos pocos recursos compartidos.

Con el primer método, un usuario podría necesitar cuentas en una docena de computadoras o más. Con el segundo, el usuario tendría que recordar docenas o incluso cientos de contraseñas diferentes a fin de acceder a diferentes carpetas o impresoras compartidas. Este escenario contrasta con la red basada en un servidor de autenticación, donde cada usuario tiene un solo nombre de usuario y una sola contraseña para validarse ante toda la red. El usuario puede entonces acceder a cualquier recurso de cualquier máquina en la red para el que se le han asignado los permisos apropiados. Aunque los administradores sí tienen que asignar permisos para cada recurso compartido, desde el punto de vista del usuario, este es un sistema mucho más simple. Cuando los grupos de trabajo crecen a más de 20 o 25 computadoras, generalmente resulta ventajoso convertirlos en un modelo centralizado basado en un servidor.

Software de servidor

Recuerde que todos los sistemas operativos modernos, incluso las ediciones para consumidores de casa, tienen un *componente de servidor* (como el compartimiento de ficheros e impresoras para redes Microsoft) que les permiten compartir sus recursos. Cuando nos referimos aquí al software de servidor, estamos hablando de sistemas operativos capaces de ofrecer servicios de autenticación de red (así como otros servicios como DNS, servicios Web o servicios de acceso remoto). Existen también muchas *aplicaciones* de servidores (como el servidor de base de datos SQL, el servidor muro de fuego/Proxy ISA, el servidor de mensajería Exchange, etc.) que se pueden instalar solamente en un sistema que corra un sistema operativo de servidor.

Los principales sistemas operativos de servidores en uso hoy día incluyen:

- **Microsoft Windows NT y 2000 Server** Existen varias versiones de ellos. La familia de NT 4.0 incluye el Standard Server (Servidor Estándar), la Enterprise Edition (Edición Empresarial) y la Terminal Server Edition (Edición de Servidor Terminal). La familia de Windows 2000 incluye el Standard Server (Servidor Estándar), el Advanced Server (Servidor Avanzado) y el Datacenter Server (Servidor de Centro de Datos). Los productos de más alto nivel incluyen características adicionales y/o soportan más memoria y un mayor número de procesadores. Al escribir este libro, la próxima generación del producto de Microsoft para servidores, .NET Server, no había salido al mercado.
- **Novell NetWare** Solamente una década atrás, NetWare tenía la mayoría de la base instalada para softwares de servidores de autenticación de redes en los Estados Unidos. Este perdió terreno con la introducción, por parte de Microsoft, de Windows NT 4.0 y después Windows 2000 (que incluían un servicio de directorio similar al NDS de NetWare). Anteriormente al NetWare 5, se requería la pila de protocolos IPX/SPX para conectarse a servidores NetWare. Ahora NetWare puede correr sobre el IP puramente. Al escribir este libro, la versión actual de NetWare era la versión 6.
- **UNIX/Linux en muchos, muchos “sabores” diferentes** UNIX ha existido desde el comienzo de la interconexión y de Internet. Linux es un sistema operativo basado en UNIX que también se puede correr en el escritorio. UNIX es un muy poderoso sistema operativo para servidor, pero se considera que su aprendizaje resulta muy complicado. Es un sistema operativo basado en caracteres, pero sus interfaces gráficas están disponibles. Existen docenas de diferentes distribuciones populares, comerciales y gratuitas, de UNIX y Linux.

Apple hizo su OS X en una versión para servidores, la cual soporta clientes Macintosh, Windows, UNIX y Linux e incluye servidor Web Apache, mensajería POP e IMAP y servicios DNS y DHCP. OS X Server corre solamente en sistemas Macintosh (G3, G4 e iMac). Aunque no está ampliamente implementada en este momento, la versión para servidores OS X es menos costosa que los productos de Microsoft y Novell y mucho más interactiva que otras versiones de UNIX. Para más información sobre OS X Server, véase la sección de Preguntas Realizadas con Mayor Frecuencia FAQ en www.apple.com/macosx/server/faq/index.html.

Software de cliente

La mayoría de los sistemas operativos modernos también pueden funcionar como clientes de redes. Esto incluye a los sistemas operativos analizados anteriormente, con la posible excepción de NetWare. Sin embargo, resultaría ineficiente y costoso correr NT Server o Windows 2000 Server, por ejemplo, como un cliente de escritorio – solamente el sistema operativo cuesta 10 veces más que los sistemas operativos de Windows diseñados para el escritorio (9x/ME, NT Workstation, 2000/XP Professional, etc.). UNIX se emplea mayormente como un servidor, pero Linux está creciendo en popularidad como un sistema operativo de escritorio/cliente. Mac OS X viene en forma de cliente y de servidor. Novell no hace un sistema operativo de cliente del suyo propio; los clientes NetWare corren generalmente en sistemas operativos de Windows o UNIX con software de cliente NetWare instalado (y los protocolos IPX/SPX, si es necesario).

Esto saca a relucir un punto importante: Las máquinas clientes no tienen que correr necesariamente un sistema operativo hecho por el vendedor del software para servidores de redes. Con el apropiado software de aditamento instalado, los clientes basados en Macintosh y UNIX pueden acceder a los servidores Windows y los clientes de Windows y Macintosh pueden acceder a servidores UNIX, etc.

Los sistemas operativos clientes más populares son:

- **NT Workstation y 2000/XP Professional** Los clientes basados en Windows son, hasta ahora, los sistemas operativos clientes más populares, sin tener en cuenta el tipo de servidor que esté corriendo en la red. Novell hace softwares clientes para todas las versiones de Windows, y Microsoft también incluye su propio software cliente NetWare con sistemas operativos de Windows. SAMBA es un software que corre en una máquina UNIX y le permite a las computadoras de Windows acceder a sus recursos. (Los clientes MS-DOS y Windows 3.x continúan en uso en algunos negocios, y Windows 9x/ME o XP Home Edition se pueden utilizar para acceder a un dominio de Windows, aunque esas computadoras no pueden realmente unirse al dominio. Esto significa que un usuario con una cuenta de dominio válida puede validarse desde el sistema, pero la computadora no tiene cuenta de computadora y por ende, es menos segura y no puede ser administrada como una máquina con NT/2000 o XP Professional).

- **Linux** Novell, Microsoft y Apple brindan softwares clientes de aditamento para permitir que máquinas UNIX y Linux accedan a algunos o a todos sus recursos. Por ejemplo, los Servicios de Microsoft para UNIX se adicionan a un servidor NT o Windows 2000 para permitir la autenticación de clientes Linux y UNIX. (Note que no se soportan todas las distribuciones). El proyecto SAMBA también ha creado un programa denominado Winbind para permitir que las estaciones de trabajo basadas en UNIX en redes con múltiples sistemas operativos (a veces llamadas *redes híbridas o heterogéneas*) se validen en dominios de Windows con plena funcionalidad. NetWare v6 le permite a los clientes Linux acceder a recursos sin instalar el software cliente NetWare, empleando un visualizador Web o a través de la opción nativa de acceso a ficheros para clientes Linux usando el NFS (Sistema de Ficheros de Redes).

▪ **Macintosh OS 8/9 y OS X** Los servicios de Microsoft para Macintosh le permiten a los clientes Mac acceder a los servidores Windows. El Módulo de Autenticación de Usuario Microsoft (UAM) brinda un mecanismo de encriptación de contraseñas utilizado por usuarios Mac para validarse ante los servicios de Protocolo de Ficheros Apple (AFP). Novell proporciona el Cliente NetWare para el sistema operativo Mac, que puede instalarse en máquinas Macintosh para acceder a servidores NetWare 5 o, alternativamente, se pueden instalar Servicios de NetWare para AppleShare en el servidor NetWare (en cuyo caso no se requiere de un software cliente). Netware 6 permite el acceso a través del visualizador o del compartimiento nativo de ficheros sin instalar el software cliente. El último sistema operativo Mac, el OS X, está basado en UNIX y se conecta fácilmente a servidores UNIX. Las versiones más antiguas pueden emplear softwares de emulación Terminal para conectarse a servidores UNIX.

Sistemas de Ficheros de Redes y Protocolos de Compartimiento de Ficheros

Los *sistemas de ficheros de redes* y los *protocolos de compartimiento de ficheros* le permiten a los usuarios acceder y actualizar ficheros de computadoras remotas como si estuvieran en la computadora local. Ellos pueden hacer irrelevantes diferentes sistemas de ficheros de la máquina remota al acceder a los recursos de esa máquina a través de la red. Esta es la razón por la cual una computadora con Windows 9x, que no soporta NTFS y no puede acceder localmente a ficheros NTFS, es capaz de leer y escribir en ficheros NTFS que están guardados en una computadora remota con Windows NT/2000. Los mecanismos populares para el compartimiento de ficheros a través de una red incluyen:

- **Protocolo SMB (Bloque de Mensajes de Servidor)** Microsoft utiliza este protocolo para permitirle a las aplicaciones clientes acceder y escribir en ficheros remotos y solicitar servicios de aplicaciones del servidor en sistemas remotos. SMB está incluido en los sistemas operativos de Windows. SAMBA es una implementación del SMB y el Sistema Común de Ficheros de Internet (CIFS), que se puede instalar en computadoras UNIX para permitirle a los clientes de Windows acceder a sus ficheros como si fueran servidores SMB.
- **Sistema Común de Ficheros de Internet (CIFS)** CIFS es un protocolo propuesto como un estándar de Internet para permitir el acceso a ficheros remotos a través de Internet. El CIFS se considera una versión abierta (no propietaria) del SMB. Ambos, SMB y CIFS, corren sobre la pila de protocolos TCP/IP.
- **Protocolo central de NetWare (NCP)** NCP es realmente un conjunto de protocolos que brinda acceso a ficheros e impresoras, entre otros servicios, entre los clientes y los servidores remotos en redes NetWare. NCP corre sobre IPX o IP.
- **Sistema de Ficheros de Red (NFS)** NFS es una aplicación cliente/servidor creada por Sun Microsystems que corre sobre TCP/IP para permitir el acceso a ficheros remotos. NFS usa el método de comunicación de Llamada de Procedimiento Remoto (RPC). NFS es usado por máquinas UNIX/Linux para el acceso a ficheros remotos y se puede instalar en computadoras de Windows y Macintosh.

Un Asunto de Protocolo de Red

A fin de que cualquier comunicación de red tenga lugar entre computadoras, las computadoras deben correr un *protocolo de red* común. Los protocolos son sencillamente conjuntos de reglas que definen el proceso de comunicación. Algunos textos comparan los protocolos con las lenguas, pero una mejor comparación es con la gramática y la sintaxis de una lengua – las reglas que determinan el uso de la lengua. Piénselo de esta forma: Incluso si Usted aprende todas las palabras o el vocabulario de una lengua extranjera, no podrá comunicarse correctamente con un hablante de la lengua si Usted no comprende las reglas para ordenar esas palabras en oraciones.

Los protocolos de redes trabajan generalmente de conjunto en pilas o suites de protocolos. Una *pila* es dos o más protocolos trabajando en diferentes capas del modelo OSI o del DoD. Por ejemplo, el TCP y el IP forman una pila de protocolos, con el TCP trabajando en la capa de transporte y el IP en la capa de red. El intercambio Secuenciado de Paquetes (SPX) y el IPX trabajan de conjunto, con el SPX realizando los deberes de la capa de transporte y el IPX llevando a cabo las tareas de la capa de red. Una suite incluye protocolos adicionales como los protocolos de la capa de aplicación FTP y Telnet, incluidos en la suite TCP/IP.

En los primeros días de las redes Microsoft, la mayoría de las redes eran pequeñas LAN, de modo que simples protocolos eran suficientes para establecer la comunicación. La Interfaz Extendida de Usuario NetBIOS (NetBEUI), un producto del protocolo NetBIOS (Sistema de Entrada/Salida Básico de la Red) creado por IBM, fue usada para las comunicaciones en la red. NetBIOS y NetBEUI se basan en nombres asignados a computadoras, denominados *nombres NetBIOS*, para identificar las computadoras en una red. No existe un mecanismo para que la red se identifique a sí misma, lo que significa que las transmisiones que utilizan este protocolo no pueden viajar entre dos redes diferentes.

En la escena...

Cómo Funcionan los Protocolos

Los protocolos de redes establecen reglas para cosas como el modo en que las computadoras se identifican y se localizan en una red. Por ejemplo, el Protocolo de Internet (IP) y el de Intercambio de Paquetes de Internet (IPX) manejan el direccionamiento y el enrutamiento de paquetes en la capa de red del modelo OSI. Sin embargo, ellos usan esquemas de direccionamiento completamente diferentes. Es como la diferencia entre el servicio postal, que utiliza Su número de calle y nombre para ubicar la casa, y un sistema satelital que emplea las coordenadas geográficas para encontrar la misma estructura. Las coordenadas geográficas podrían ser de poca ayuda para un trabajador postal a la hora de entregar una carta y la dirección de Su casa no significaría nada para el sistema satelital.

En la medida en que las redes crecieron y se interconectaron, se hicieron necesarios protocolos más complejos, de modo que los mensajes pudieran ser *enrutados* entre diferentes redes. Las redes NetWare dependían, hasta hace poco, de los protocolos IPX/SPX. IPX/SPX es una pila de protocolos routables (trazables) que usa un sistema de direcciones de redes y direcciones de redes internas para identificar a la red y a la computadora.

La pila de protocolos más popular hoy día es TCP/IP. Primeramente, porque es el protocolo de Internet y cualquier computadora que se conecte a Internet debe tener instalado el TCP/IP. Este utiliza un esquema de direccionamiento que lo hace extremadamente routable (trazable), de modo que es apropiado para las redes más grandes. También se puede correr en las redes más pequeñas, aunque su poco rendimiento y la complejidad de administración podrían hacerlo menos adecuado que el NetBEUI para redes pequeñas, no enrutadas. Sin embargo, TCP/IP es la pila de protocolos de redes de excelencia para la mayoría de las redes actuales. En la siguiente sección, analizaremos detalladamente la suite de protocolos TCP/IP.

Nota

IPX/SPX también se pueden usar en redes que no tengan servidores NetWare. Algunas redes Microsoft corren IPX/SPX – o su versión de Microsoft, llamada NWLink – para brindar una mayor seguridad cuando la red local está conectada a Internet. Debido a que la mayoría de las computadoras en Internet no tienen instalado el IPX/SPX, no pueden acceder a máquinas que corran solamente esa pila de protocolos.

Comprendiendo los protocolos TCP/IP utilizados en Internet

El Protocolo de Control de Transmisión/Protocolo de Internet (también referido como la *pila de protocolos TCP/IP* o solamente *TCP/IP*) es un componente de la red, familiar, aunque poco comprendido, para la mayoría de los administradores de redes modernas y profesionales de la tecnología de la información.

Si Usted trabaja en cualquiera de los entornos de redes que no sean muy pequeños, existen posibilidades de que se haya tropezado con el TCP/IP. Sin embargo, solamente unos pocos años atrás, el TCP/IP era visto como un protocolo algo lento, difícil de configurar, usado principalmente por redes universitarias o gubernamentales que participaban en un exótico proyecto de redes de área amplia llamado ARPANet. El TCP/IP era considerado demasiado lento y complejo para ser una opción apropiada para la mayoría de las LAN de organizaciones privadas.

Los grupos de trabajo de Microsoft e IBM corrían bien sobre el NetBEUI, un protocolo de transporte rápido y simple que podía ser configurado fácil y rápidamente por cualquiera que no tuviera grandes conocimientos. Las LAN NetWare de Novell usaban la pila IPX/SPX, que era routable (trazable) y por eso, se podía utilizar en redes más grandes basadas en servidores. Pocas redes comerciales tenían necesidad de un conjunto de protocolos poderoso, pero costoso, como el TCP/IP. Entonces algo sucedió: la Internet.

La Necesidad de Protocolos Estandarizados

El alcance de la ARPANet se expandió y creció hasta formarse la Internet comercial que conocemos hoy día. Aunque cambiada en muchas formas con respecto a sus primeros tiempos, la red global aún corre sobre la suite de protocolos TCP/IP creado para la

ARPANet. En aras de que las computadoras de todo el mundo se comuniquen entre sí, debe existir un conjunto de protocolos común, estandarizado – y el TCP/IP cumple ese cometido.

Aunque TCP/IP es una pila de protocolos “universal” que permite la comunicación entre máquinas que corren sistemas operativos diferentes o incluso que corren sobre diferentes plataformas, las diferentes implementaciones de los vendedores de protocolos podrían diferir ligeramente. Usted lo verá en los diferentes comandos utilizados para realizar las mismas tareas utilitarias. Por ejemplo, en redes Microsoft, el comando **ipconfig** se emplea para visualizar la información de configuración del TCP/IP. En redes basadas en UNIX, la misma tarea se realiza utilizando el comando **ifconfig**. Así mismo, el **tracert** de Microsoft es el **traceroute** de UNIX, etc.

En la escena...

El Esfuerzo por Destronar al TCP/IP del Puesto de Rey de la Internet

Han habido intentos ocasionales de usurpar la posición del TCP/IP como el protocolo de excelencia para Internet. La suite del protocolo de Interconexión de Sistemas Abiertos, basada en el famoso (o infame) modelo de interconexión de siete capas OSI, fue concebida con la idea de derrocar al titular y reemplazar al TCP/IP como un estándar universal para las comunicaciones en Internet. De hecho, a finales de 1980, el gobierno de los Estados Unidos, que jugó una parte importante en la creación y el desarrollo del TCP/IP, hizo planes para retirarlo paulatinamente en favor de la suite OSI. No resultó muy bien de esta manera. El TCP/IP resultó ser la pila de protocolos que se negó a retirarse tranquilamente.

Fue como si alguien hubiera anunciado que ellos descubrieron un reemplazo para la suciedad y sugiriera que desenterráramos todos los árboles y plantas y después las “reinstaláramos” en la sustancia nueva y superior. Reestructurar la enorme y cada vez mayor Internet global para “plantarla” en un entorno de protocolo diferente – sin tener en cuenta cualquier ventaja que el nuevo entorno podría ofrecer – es tan sólo una tarea demasiado abrumadora.

Una Breve Historia sobre el TCP/IP

Como dijera el filósofo alemán Friedrich Schlegel: “El objetivo de la historia es la realización gradual de todo lo que es prácticamente necesario”.

La necesidad práctica es la fuerza impulsora que está detrás de las invenciones y creaciones más importantes, y la necesidad de un conjunto confiable de protocolos de comunicación apropiado para conectar grandes redes conllevó a la creación de la pila TCP/IP.

En los años 1960, la interconexión de computadoras se encontraba en su infancia. Los muchos beneficios de conectar computadoras de modo que pudieran compartir recursos estaban sólo comenzando a hacerse aparentes. El equipamiento era costoso y los productos

de diferentes fabricantes eran sumamente incompatibles. Pocas entidades comerciales tenían el dinero o la inclinación de molestarse en crear redes locales, mucho menos la intención de hacer que sus computadoras “hablaran” con sistemas distantes.

El Departamento de Defensa de los Estados Unidos reconoció el valor de establecer enlaces de comunicación electrónica entre las instalaciones militares principales. (Penoso como podría parecer, una motivación primaria fue el deseo de mantener posibilidades de comunicación en el caso de la destrucción masiva que vendría con la guerra nuclear). Las principales universidades también se involucraron en proyectos de redes. El DoD fundó sitios de investigación en todos los Estados Unidos, y en 1968, la Agencia de Proyectos de Investigaciones Avanzadas (ARPA) firmó contrato con una compañía llamada Bolt, Beranek y Newman (más tarde llamada sencillamente BBN) para construir una red basada en tecnología de intercambio de paquetes.

Al siguiente año nació la ARPANet cuando su primer *nodo*, o punto de conexión, fue instalado en la Universidad de California en Los Ángeles. En el período de tres años, la red se había expandido por todos los Estados Unidos y dos años después, al continente europeo.

Era importante que los protocolos de redes, el conjunto de reglas que gobierna el proceso de comunicación, fueran confiables y escalables para acomodar múltiples sitios redundantes y que anticiparan el crecimiento (aunque nadie en ese entonces esperaba la tasa de crecimiento que estaba por venir). Quizás siguiendo el trillado consejo de “si quieres algo bien hecho, hazlo tú mismo”, los creadores de la ARPANet diseñaron un nuevo grupo de protocolos que cumplieran con esos requisitos. Su primer intento fue el Protocolo de Control de Red (NCP), pero demostró ser inapropiado a medida que el tráfico se incrementaba. A mediados de los años 70, la necesidad fue nuevamente la madre de la invención y se implementó la suite de protocolos TCP/IP.

El Protocolo de Internet y el Direccionamiento IP

Una de las mayores virtudes del TCP/IP – y una razón primaria que lo ha convertido en el estándar para redes grandes, incluyendo la Internet – es su esquema de direccionamiento escalable, que puede acomodar redes de todas las dimensiones. En aras de comunicarse a través de una red utilizando los protocolos TCP/IP, una computadora debe tener una dirección IP única en esa red. La dirección IP puede ser asignada manualmente por un administrador de la red o puede ser asignada automáticamente por un servicio de direccionamiento automático (ver la siguiente sección sobre direccionamiento automático). De cualquier forma, no habrá comunicación IP sin una dirección.

Bajo el actual sistema de direccionamiento IP, IPv4, “solamente” existen un poco más de 4 billones de direcciones IP posibles (4,294,967,296, o 2^{32} , para aquellos que gustan de ser precisos). Al comienzo, (a principios de los 80), esto parecía ser más que suficiente para el futuro inmediato. En aquel entonces, cuando las especificaciones IP se estandarizaron, se impuso una estructura de direccionamiento jerárquica de dos niveles que consistía en el ID de la red (a veces llamado el *prefijo de la red*) y el ID de la máquina anfitriona. Las redes

se dividían en “clases”: A, B y C (así como D y E, pero estas últimas dos no estaban asignadas a redes, sino que se reservaban para fines especiales). Esto es a lo que se le denomina *direccionamiento de clases*. Un método más reciente de identificar redes a través de un “prefijo IP” se denomina *enrutamiento interdominio sin clases (CIDR)*, que analizamos brevemente en el Capítulo 4. En lugar de designar redes como Clase A, B o C, una red es referida como una /16, una /24, etc., en dependencia del número de bits utilizado para la porción ID de la dirección de la red.

Direcciones IP Lógicas vs. Direcciones MAC Físicas

La dirección IP es una dirección “lógica” asignada por el administrador de la red. No guarda relación directa con la dirección “física” de la tarjeta de interfaz de la red (a menudo referida como la *dirección MAC*, porque se emplea en la subcapa de control de acceso a los medios de la capa de enlace de datos del OSI).

Cambiar una dirección IP de una computadora (o para ser más precisos, de una NIC individual) es una función de software. Si Usted tiene privilegios administrativos, resulta tan simple como hacer clic con el ratón unas pocas veces para abrir el mensaje apropiado en pantalla y teclear un nuevo número. (La parte más difícil es saber qué número teclear).

Por otra parte, la dirección MAC está codificada en el chip de la tarjeta de red en la Ethernet típica. Algunas tarjetas de redes dan la posibilidad de cambiar la dirección MAC a través de configuraciones de saltos o “flasheando” el chip con un software especial, pero esto no es usual. En la mayoría de los casos, la dirección MAC sigue siendo la misma.

Nota

Usted podría imaginarse la dirección IP de forma análoga a Su dirección, con dos partes representando la calle donde Usted vive y la casa específica en esa calle (como las dos partes de una dirección IP que representan la red en donde “vive” la computadora y la máquina anfitriona específica en esa red). La dirección de la calle es una dirección “lógica”, toda vez que fue asignada (probablemente por la ciudad). Un voto del gobierno municipal puede cambiar el nombre de la calle o incluso el esquema numérico, del mismo modo en que el administrador de la red puede cambiar fácilmente la dirección IP de una computadora. La dirección MAC es más similar a las coordenadas geográficas (latitud y longitud) que identifican la ubicación de Su casa. Estas son permanentes y no pueden ser cambiadas por antojo del gobierno de la ciudad.

La dirección MAC de una Ethernet es un número de 48 bit representado en hexadecimal, de modo que luce más o menos así: 00-80-C8-6A-FA-00. Si Usted está utilizando una máquina de Windows, podrá encontrar la dirección física de su tarjeta Ethernet tecleando **ipconfig/all** en la línea de comandos, lo que le dará la información mostrada en la Figura 5.9.

Figure 5.9 You can find out a computer's IP address using the `ipconfig` command in Windows.

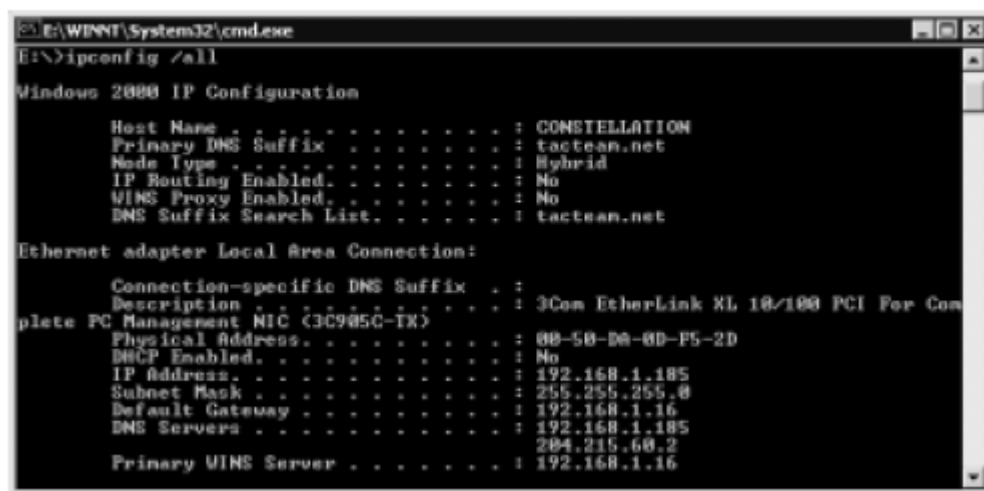


Figura 5.9 Usted puede averiguar la dirección IP de una computadora de Windows usando el comando **ipconfig**.

Figure 5.10 You can use the GUI to find out your Ethernet address with an OS X system.



Figura 5.10 Usted puede utilizar la interfaz gráfica para averiguar su dirección Ethernet con un sistema OS X.

En sistemas Linux, el comando para averiguar su dirección MAC es **ifconfig -a**. El método difiere según los diferentes “sabores” de UNIX. Por ejemplo, en HP-UX, Usted usa el comando **lanscan**. Con Macintosh OS X, Usted selecciona, del menú de **Apple, Preferencias del Sistema**, entonces selecciona **Red**, elige su adaptador Ethernet del menú desplegable en la casilla **Mostrar** y la dirección de hardware se visualizará (además de la información de la configuración del TCP/IP) como se muestra en la Figura 5.10.

Como puede ver en estos pantallazos, las direcciones IP y MAC están en dos formatos muy diferentes y no tienen relación lógica entre sí. El Protocolo de Resolución de Direcciones (ARP) es responsable de “llevar la cuenta” de cuáles direcciones IP se corresponden con cuáles direcciones físicas y de transmitir esa información de modo que las computadoras puedan comunicarse en el nivel físico (interfaz de la red).

Direccionamiento estático

Los administradores pueden asignar manualmente direcciones IP a cada computadora en una red, usando las utilidades de configuración del TCP/IP (que varían en dependencia del sistema operativo). Esto funciona bien cuando la red es pequeña y es necesario cuando Usted tiene computadoras (generalmente servidores) que necesitan tener siempre la misma dirección IP. La Figura 5.11 muestra la hoja de propiedades del TCP/IP que se emplea para asignar una dirección IP estática a una computadora con Windows 2000.

Figure 5.11 Network administrators can manually assign IP addresses (called “static addresses”) to computers.



Figura 5.11 Los administradores de redes pueden asignarle manualmente a las computadoras direcciones IP (llamadas “direcciones estáticas”).

Cuando Usted asigna manualmente una dirección, también debe introducir la máscara de la subred correcta y, si la red está enrutada, la dirección IP de la puerta de enlace implícita (el enrutador o la computadora que realiza las funciones de enrutamiento). Aunque el direccionamiento manual consume más tiempo si tiene muchas computadoras y resulta fácil cometer errores al introducir los datos, lo que podría traer como consecuencia la pérdida de la conectividad o un comportamiento extraño de la red, a veces existen buenas razones para asignar direcciones manualmente. Si no existe un mecanismo para el direccionamiento automático en la red, obviamente las direcciones necesitan ser asignadas manualmente.

También hay ciertos sistemas como los controladores de dominio y los servidores DNS y WINS que necesitan tener direcciones estáticas.

Direccionamiento automático

En el caso de redes muy grandes, el direccionamiento manual consume mucho tiempo y es propenso a errores (duplicación de direcciones). La asignación automática de direcciones puede ser hecha por un servidor que corra el servicio DHCP (Protocolo Dinámico de Configuración de la Máquina Anfitriona). El DHCP puede ser el mejor amigo del administrador de la red – a menos que el administrador no lo configure apropiadamente, en cuyo caso puede ser una fuente de pesadillas. El fin del DHCP es asignar dinámicamente direcciones IP en la medida en que las computadoras entren a la red. La computadora sólo tiene que estar configurada en las propiedades del TCP/IP para obtener una dirección IP (y otra información de configuración del TCP/IP) de un servidor DHCP y el servicio hace el resto. Este sistema tiene varias ventajas:

- **Ahorro de tiempo** Los administradores de redes no tienen que introducir tediosamente una y otra vez, para cada máquina de la red, la dirección IP, la máscara de la subred, las direcciones de los servidores DNS y WINS y otras informaciones. Así mismo, si la dirección IP para el servidor DNS de la red cambia, no tiene porqué hacerse el cambio en todas las máquinas; se hace en la configuración del servidor DHCP y la nueva dirección se disemina automáticamente hacia las computadoras clientes cuando estas obtienen una dirección.
- **Más exactitud** La posibilidad de teclear mal una dirección en una de las máquinas se elimina. El alcance de las direcciones se define sólo una vez, en el servidor DHCP, y la direcciones son administradas por el servidor. No existe la posibilidad de que el servidor “olvide” que una dirección específica ya le fue asignada a otra máquina y duplique la dirección.
- **Uso más eficiente de las direcciones** Si el número de direcciones disponibles es limitado, el DHCP optimiza su uso, pues sólo “arrienda” las direcciones a computadoras por un período de tiempo predeterminado en lugar de asignarlas permanentemente, como ocurre con la asignación manual. Cuando una computadora se desconecta de Internet, su dirección puede ser cedida de modo que se le pueda asignar a un sistema diferente.

Usted debe configurar las computadoras clientes para que le pidan una dirección al servidor DHCP. En Windows, configurar una computadora para obtener una dirección de un servidor DHCP es simple. En el menú de propiedades del TCP/IP, simplemente revise la opción **Obtener automáticamente una dirección IP**.

Nota

El DHCP funciona con la mayoría de los sistemas operativos. Nació del BootP, el protocolo de arranque-asignación que fue originalmente diseñado para permitirle a las estaciones de trabajo sin discos iniciar un sistema operativo desde la red. El DHCP adiciona más funcionalidad, permitiéndole a los administradores configurar muchas opciones diferentes. El servidor DHCP puede asignar otras informaciones

del TCP/IP, como la puerta de enlace implícita y las direcciones de los servidores DNS y WINS, así como asignar una dirección IP.

Otros servicios pueden asignar direcciones IP bajo ciertas circunstancias. Por ejemplo, en Windows 98/2000 y posteriores, el servicio APIPA (Direccionamiento IP Privado Automático) y el Compartimiento de Conexión a Internet (ICS) pueden asignar direcciones IP. El APIPA fue incluido en Windows 2000 para facilitar la configuración del TCP/IP y ayudar a asegurar que una computadora pudiera comunicarse en una red TCP/IP pequeña que no tuviera un servidor DHCP. En versiones pasadas de los sistemas operativos de Microsoft, antes de la salida de Windows 98 y de Windows 2000 más tarde, si una computadora no tenía una dirección introducida manualmente y no era capaz de contactar un servidor DHCP cuando entraba en línea, no podía pertenecer a una red TCP/IP. Con APIPA, la computadora primeramente intenta alcanzar un servidor DHCP y negociar la renta de una dirección IP. Sin embargo, si esto falla, entonces la computadora toma la iniciativa y se asigna a sí misma una dirección del rango APIPA reservado de 169.254.0.1 hasta 169.254.255.254 con una máscara de subred de 255.255.0.0. Esto le permite a la computadora comunicarse en la red, usando temporalmente la dirección APIPA hasta que pueda alcanzar un servidor DHCP.

El ICS es otra característica nueva introducida en Windows 98/2000. Se emplea para permitir que múltiples computadoras accedan a la conexión a Internet o a otra conexión externa a través de una sola dirección IP pública. El ICS es una parte de Windows 2000 Network y Conexión por marcación y se puede habilitar en una computadora con Windows 2000 Professional o Windows 2000 Server que tenga una conexión a Internet por marcado, permitiéndole así a otras computadoras en la LAN compartir esa conexión utilizando la NAT (Traducción de Dirección de la Red).

Cuando Usted habilita el ICS, la máquina anfitriona que está compartiendo su conexión se configurará con una dirección IP de 192.168.0.1 con una máscara de subnet de 255.255.255.0. La computadora ICS también se convierte en un *adjudicador DHCP*. Este rol difiere del de un servidor DHCP en que la computadora no tiene que estar corriendo un sistema operativo de servidor. El adjudicador DHCP tiene un alcance predefinido de direcciones IP que le puede dar a las computadoras clientes que están compartiendo su conexión a Internet. Esas direcciones entran dentro de un rango privado de direcciones Clase C, la red 192.168.0.0.

El Futuro del IP

La versión actual del IP (IPv4) utiliza direcciones de 32 bit. Esta da un total de aproximadamente 4 billones de direcciones individuales únicas, en teoría. Desafortunadamente, en la práctica, existen muchas menos direcciones utilizables. Esta situación es desafortunada, porque todas las computadoras que se conectan a Internet – con la excepción de aquellas que se conectan a través de proxies y NAT – deben tener una dirección única. La popularidad de Internet ha excedido los sueños más descabellados de aquellos que crearon el Protocolo de Internet. Además, las asignaciones de direcciones en los primeros tiempos no fueron hechas con la eficiencia en mente. Muchas direcciones

fueron “desperdiciadas” – por ejemplo, todo el rango de direcciones 127.x.y.z no se usa, porque está asignado como una dirección “loopback” para probar la pila de protocolos TCP/IP local, desperdiciando más de 16 millones de direcciones. En los primeros días de la Internet, los bloques de direcciones Clase A y B, con aproximadamente 16 millones y 65,000 direcciones anfitrionas fueron asignados, respectivamente, a organizaciones que no necesitaban esa cantidad de direcciones.

Nota

En 1991, existía un poco más de 1 millón de máquinas anfitrionas en la Internet global. En 1997, existían más de 16 millones. En el 2000, de acuerdo con la Sociedad de Internet, había un estimado de 50 millones. Si continúa creciendo a ese ritmo, la perspectiva de utilizar todas las direcciones disponibles se hará real.

Como una consecuencia, el mundo se está quedando sin direcciones IP disponibles. A medida que el número de dispositivos de Internet aumenta, con PDA, teléfonos celulares y aplicaciones domésticas que se espera se conecten a la Red en el futuro, la necesidad de más direcciones se hará imperiosa. Se necesita una nueva versión del IP – una que proporcione un mayor número de direcciones. Ahí es donde entra a relucir el IPv6.

El IPv6 o IPng (ng es la abreviatura de *próxima generación*) es la nueva versión del IP. Fue diseñada por la IETF (Grupo de Trabajo en Ingeniería de Internet) como el paso superior del IPv4. Se basa en el IPv4 y es una progresión natural. El IPv6 utiliza direcciones de 128 bit. Proporciona un total de direcciones IP, que representado exponencialmente, es de 2^{128} . El número real tomaría una línea completa de espacio en este párrafo; es seguro decir que definitivamente son “muchos”. Usted lo puede instalar como una implementación de software y es compatible con el IPv4 que actualmente se usa en Internet y en otras redes TCP/IP. La intención específica del IPv6 fue que trabajara eficientemente tanto en redes de alto rendimiento como son las de modo de transferencia asincrónica (ATM) como en redes de poco ancho de banda (las que incluyen a las de tecnologías inalámbricas).

No es probable que Usted despierte un día y vea de repente un anuncio que diga que en una fecha específica, a una hora específica, la Internet va a cambiar para el IPv6. La nueva versión se espera reemplace gradualmente al IPv4, y las dos coexistirán por varios años mientras ocurra la transición. Como el IPv6 proporciona tantas posibles direcciones, todo el espacio de direcciones original del IPv4 se mantendrá intacto para asegurar la mayor compatibilidad con las direcciones del IPv6, haciendo que la transición sea más fácil de implementar.

Cómo Funciona el Enrutamiento

Las computadoras en Internet se envían paquetes entre sí de una o dos formas:

- Directamente (si las computadoras fuente y de destino están en la misma subred)
- Indirectamente (si las computadoras fuente y de destino están en subredes diferentes) reenviando los paquetes hacia un enrutador

El enrutamiento IP se trata de descubrir un camino desde la computadora remitente (o el enrutador que reenvía) hasta la computadora de destino, cuya dirección está indicada en el encabezado IP. En concepto, este proceso no es diferente a lo que Usted hace cuando planifica un viaje desde su casa a un lugar distante. Para recorrer un trayecto, Usted se sienta con un mapa y traza la mejor ruta basándose en varios factores. Distancia, simplicidad, y congestión podrían ser algunas cosas a considerar al decidir qué caminos tomar.

El *enrutamiento IP* se refiere al reenvío de paquetes desde una computadora fuente hacia una computadora de destino pasando por los enrutadores que soportan el enrutamiento IP. Cada computadora tiene una tabla de números de red, conocida como *tabla de enrutamiento*. Para cada número de red aparece una dirección de puerta de enlace, la cual se utiliza para llegar a esa red. La puerta de enlace no se tiene que conectar directamente a la red de destino; este es sólo el punto de partida. Cada puerta de enlace, o enrutador, por donde el mensaje debe pasar se le denomina *salto*. En cada enrutador, la dirección IP de destino en el paquete se compara con la tabla de enrutamiento y se utiliza la mejor ruta para decidir el punto final del próximo salto. Usted podría decir que un viaje de 1000 saltos comienza con un solo paso: la dirección de puerta de enlace incluida en la tabla de enrutamiento para un número de red específico.

Generalmente un enrutador se conecta a dos o más redes o subredes. El enrutador, un dispositivo dedicado o una computadora que actúa como enrutador, se dice tiene una *interfaz* para cada red a la que se conecta.

La interfaz del enrutador se puede conectar a una LAN o a una WAN. La interfaz de red de área extensa puede ser un módem, un adaptador de Terminal ISDN u otro dispositivo de conexión a los medios de la WAN. La interfaz de la LAN es una tarjeta adaptadora de red.

Cada interfaz debe tener una dirección IP con un ID de red apropiado para la red a la cual está conectada. El enrutador funciona en la capa de Internet del modelo de interconexión DoD (la capa de red del modelo OSI).

Enrutamiento estático

El enrutamiento viene en dos “sabores” básicos: estático y dinámico. Con el enrutamiento IP estático, la tabla de enrutamiento se debe construir manualmente; un administrador debe introducir, una a una, las direcciones IP que definen las rutas hacia las redes remotas. El enrutamiento estático no sólo requiere que Usted configure minuciosamente la tabla de enrutamiento; también debe introducir manualmente todos los cambios, adiciones y cancelaciones que ocurran. Esta reprogramación de los enrutadores cada vez que se haga un cambio puede resultar tediosa y consumir mucho tiempo. ¿Por qué nadie usaría el enrutamiento estático? Realmente, la mayoría de las redes hoy día no lo hacen, pero el enrutamiento estático sí tiene algunas ventajas:

- El enrutamiento estático se puede implementar con un mínimo de equipamiento. No es necesario un dispositivo de enrutamiento dedicado; Usted puede configurar una computadora multihomed con Windows NT o Windows 2000 para que sea un enrutador estático. Una computadora multihomed es una que tiene dos o más interfaces de red.
- El costo inicial de implementar el enrutamiento estático es menor que el del enrutamiento dinámico debido al costo de los dispositivos de enrutamiento. Sin embargo, estos ahorros iniciales se pueden compensar con la simplificación de la administración y la reducción de personal-horas necesarios para mantener los enrutadores dinámicos.
- Usted tiene un control más específico sobre los enrutadores empleados en una situación de enrutamiento estático, ya que introduce manualmente las rutas en la tabla. Usted puede borrar o cambiar rutas y asegurarse de que los paquetes utilicen la ruta deseada.

Sin embargo, estos beneficios no son generalmente suficientes para hacer del enrutamiento estático una solución atractiva para los administradores de redes debido a las muchas desventajas del método:

- No existe una tolerancia real a fallas en un entorno de enrutamiento estático. Si uno de los enrutadores deja de estar disponible, los otros no pueden detectar su ausencia. Como la red enrutada de forma estática es generalmente un entorno de un solo camino (sólo un camino disponible entre dos extremos), esto puede traer como resultado alguna incapacidad de la máquina anfitriona para comunicarse con otras en la red.
- Se requiere de un buen mantenimiento administrativo para mantener actualizadas las tablas de enrutamiento en una red estática si resulta necesario añadir o eliminar nuevas rutas.
- El enrutamiento estático es apropiado sólo para pequeños grupos de redes interconectadas (aquellos que tienen de dos a 10 redes). Con más de esa cantidad, la administración se hace imposible.

Utilizando un protocolo de enrutamiento dinámico, la tabla se configura y actualiza automáticamente, porque el enrutador dinámico se puede comunicar con otros enrutadores en la red y “aprender” de ellos. Este sistema le ahorra al administrador una gran cantidad de tiempo.

Protocolos de Enrutamiento Dinámico

Los enrutadores que corren protocolos de enrutamiento dinámico pueden conformar automáticamente sus propias tablas de enrutamiento y hacer modificaciones cuando cambie la red. Estos cambios se propagan por toda la red al comunicarse entre sí los enrutadores dinámicos. Dos conocidos protocolos de enrutamiento dinámico son el RIP (Protocolo de Información de Enrutamiento) y el OSPF (Abrir Primero el Camino más Corto).

El RIP se ha utilizado por muchos años y funciona bien con redes pequeñas y medianas, aunque no escala bien para grupos grandes de redes interconectadas. El RIP es un protocolo de vector a distancia (para más información, véase el recuadro En la Escena), con un conteo máximo de 15 saltos. Para fines prácticos, esto significa que si toma más de 15 saltos para llegar a la otra red (subred), el RIP no funcionará.

El RIP para el IP funciona enviando, en intervalos regulares, un anuncio que contiene la información de su tabla de enrutamiento. Otros enrutadores RIP reciben este mensaje y añaden la información a sus propias tablas. De esta forma, la información de rutas se esparce a través de toda la red. La versión 1 del RIP envía sus anuncios a través de paquetes broadcast. La versión 2 también puede enviar anuncios a través de paquetes broadcast, pero puede utilizar también paquetes multicast. Los enrutadores RIP también usan *actualizaciones inmediatas* para esparcir su información. La actualización ocurre por un cambio en la red, como por ejemplo, un fallo en la puerta de enlace. Cuando un enrutador detecta la falla, este actualiza su propia tabla y luego envía inmediatamente la nueva información en lugar de esperar el próximo período de actualización programado.

El OSPF supera algunas de las limitaciones impuestas por el RIP. El OSPF fue diseñado para manejar los tipos de redes que el RIP no maneja bien: redes interconectadas grandes y complejas. El OSPF es eficiente; no requiere de mucho overhead. Esto es especialmente importante en entornos de grandes redes interconectadas para los cuales está diseñado. Además, el SPF, algoritmo del OSPF (Abrir Primero la Trayectoria más Corta), no es vulnerable a bucles de enrutamiento que pueden plagar las rutas del RIP. El SPF calcula la trayectoria más corta entre el enrutador y las redes remotas creando y manteniendo un mapa de las redes interconectadas. El mapa se denomina *base de datos de estado de enlace* y el OSPF es referido como el *protocolo de estado de enlace*.

En la escena...

Protocolo de Vector a Distancia vs. Protocolo de Enrutamiento de Estado de Enlace

Una de las formas más significativas en que difieren el RIP y el OSPF es en los algoritmos empleados para calcular las decisiones de enrutamiento. El RIP es lo que se denomina un *protocolo de vector a distancia*; el OSPF es referido como un *protocolo de estado de enlace*.

Algoritmos de Vector a Distancia

Los algoritmos de vector a distancia se denominan también algoritmos Bellman-Ford o Ford-Fulkerson. Los últimos autores fueron los primeros en documentar la clase de algoritmo de vector a distancia, que se basa en la ecuación de Bellman, que conforma la base de la programación dinámica.

Los algoritmos de vector a distancia son un estándar antiguo que se utilizó para los cálculos de enrutamiento de redes en la infancia de la conectividad global en los años 1960, en la ARPANet que fue la predecesora de la Internet actual.

Los algoritmos de vector a distancia permiten puertas de enlace (enrutadores) para compartir e intercambiar la información de la tabla de enrutamiento. Esto ofrece un gran beneficio sobre los protocolos de enrutamiento estático, los cuales requieren que las tablas se construyan y mantengan manualmente. El RIP descendió de los protocolos de interconexión Xerox y el nombre de *Protocolo de Información de Enrutamiento* fue utilizado primero en conjunción con XNS. Otra variación se denomina Berkeley's Routed.

Los algoritmos de vector a distancia, a pesar de sus grandes ventajas sobre el enrutamiento estático, sufren de varias limitaciones. La máxima longitud de trayectoria es de 15 saltos y estos son vulnerables a los bucles de enrutamiento, causados por un comportamiento denominado *conteo hasta el infinito*. El RIP y los otros protocolos de vector a distancia fueron diseñados para usar en redes de tamaño moderado, no para redes interconectadas tan vastas como la Internet. Es por ello que estos se implementan como IGP (Protocolos de Pasarela Internos).

Esto nos lleva a la necesidad de otro tipo de protocolo de enrutamiento que pueda manejar mejor el enrutamiento sobre redes enormes y distintas. Ahí es donde entran a relucir los algoritmos de estado de enlace.

Algoritmos de Estado de Enlace

El protocolo de estado de enlace utilizado por el OSPF mapea la red y actualiza la base de datos (denominada *base de datos de estado de enlace*) cada vez que se le hagan cambios a la red. Los protocolos de estado de enlace son referidos también como *SPF (Primero la Trayectoria más Corta)* o *protocolos de base de datos distribuida*. El primer protocolo de estado de enlace fue diseñado para usar en la ARPANet. Más tarde se le hicieron modificaciones para reducir el exceso de tráfico y adicionar tolerancia a fallas.

Un protocolo de enrutamiento de estado de enlace construye una vista consistente de una red al mapear la topología de la misma. Cada enrutador broadcast (o multicast) los datos sobre la longitud (en cost) de la trayectoria hasta cada uno de sus enrutadores vecinos. Esa información se disemina hacia todos los nodos en la red. Los protocolos de estado de enlace son más eficientes, pero más complejos que los protocolos de vector a distancia.

A medida que la base de datos de estado de enlace crece, los requerimientos de memoria y procesador y el tiempo necesario para calcular las rutas se incrementan. En aras de solucionar este problema con los protocolos de estado de enlace, el OSPF divide las redes interconectadas en áreas (grupos de redes contiguas) que se conectan entre sí a través de un área backbone o área cero. Cada enrutador conserva una base de datos de estado de enlace sólo para aquellas áreas que están conectadas al enrutador. Los protocolos de estado de enlace utilizan paquetes dirigidos al TCP para comunicarse con otros enrutadores directamente en un área, reduciendo el tráfico broadcast en la red.

Con los protocolos de estado de enlace la convergencia ocurre tan pronto como se actualizan las bases de datos, evitando los problemas de convergencia lenta de los algoritmos de vector a distancia. Los protocolos de enrutamiento de estado de enlace permiten también la seguridad de los mensajes de actualización registrados. Los paquetes de descripción de la base de datos se transmiten de una manera segura y están protegidos por un *checksum*. Los registros de estado de enlace también están protegidos por temporizadores que los eliminan de la base de datos si un paquete nuevo no llega dentro del plazo especificado. Para más seguridad, los mensajes se pueden autenticar a través de una contraseña.

En una red OSPF, la base de datos está sincronizada entre los enrutadores OSPF, los cuales la usan para calcular rutas en la tabla de enrutamiento. El OSPF emplea el algoritmo Dijkstra, que proviene de la esfera de las matemáticas denominada *teoría gráfica*, para calcular la trayectoria más corta hasta un destino desde una fuente dada. El OSPF soporta el balance de carga y el enrutamiento multitrayectorias y se puede usar con ambas redes: redes broadcast (tales como Ethernet) o redes no broadcast (como ATM o X.25). El OSPF tiene diferentes protocolos para los tipos de redes broadcast y multicast.

Las tablas de enrutamiento utilizadas por un protocolo de vector a distancia como el RIP tienen una estructura plana; todos los enrutadores RIP en el conjunto de redes interconectadas deben contener una entrada para cada red. Las redes no están divididas en áreas o grupos; todas son vistas como entidades individuales – por eso la descripción de “plana”. Los protocolos de estado de enlace como el OSPF crean una estructura jerárquica al dividir el conjunto de redes interconectadas en áreas. Cada enrutador OSPF pertenece a un área, identificada por un número de 32 bit denominado *número de área*. Esta área reduce considerablemente el tamaño de la tabla de enrutamiento para cada enrutador, ya que tiene que conservar entradas solo para su área.

Los Protocolos de la Capa de Transporte

Los protocolos TCP/IP que operan en la capa de transporte del modelo OSI (la capa máquina a máquina del modelo DoD) son el TCP (Protocolo de Control de Transmisión) y el UDP (Protocolo de Datagrama de Usuario). Estos dos protocolos ofrecen dos tipos diferentes de servicios de conexión:

- TCP es un protocolo orientado a la conexión.
- UDP es un protocolo *no orientado a la conexión*.

El protocolo más apropiado para enviar un mensaje dado depende de cuál sea la prioridad mayor: la confiabilidad o la velocidad. Un protocolo orientado a la conexión como el TCP ofrece mejor control de errores, pero su mayor overhead implica una pérdida de rendimiento. Un protocolo no orientado a la conexión como el UDP, por otra parte, sufre en el terreno de la confiabilidad, pero sin los deberes de chequear errores, es más rápido. He aquí más información sobre los dos tipos de servicios:

- **Servicios orientados a la conexión** Como proveedor de servicios orientados a la conexión, el TCP primero establece una conexión virtual entre las computadoras remitente y receptora. Esto se hace mediante el uso de mensajes de reconocimiento y respuesta.
- **Servicios no orientados a la conexión** Un protocolo de transporte no orientado a la conexión como el UDP no brinda el servicio de dividir un mensaje en paquetes (también llamado *datagramas*) y reagruparlo en el otro extremo, como lo hace el TCP orientado a la conexión. Como el UDP no secuencia los paquetes a los que los datos arriban, un programa de aplicación que utilice el UDP tiene que ser capaz de asegurar que arribe todo el mensaje y que se encuentre en el orden correcto. Para ahorrar tiempo de procesamiento, las aplicaciones de redes que tienen que intercambiar unidades de datos muy pequeñas y

por ende, hacer muy pequeñas reagrupaciones de mensajes, podrían emplear el UDP en lugar del TCP.

En la escena...

La Diferencia entre los Servicios Orientados a la conexión y los Servicios no Orientados a la Conexión

La analogía más común para diferenciar las comunicaciones orientadas a la conexión y las no orientadas a la conexión compara los diferentes servicios disponibles en una oficina de correos. Si Usted se encuentra en Boston y necesita enviar un reporte importante al director de la sucursal de su compañía en El Paso, podría ponerlo en un sobre, pegarle la cantidad de sellos requerida y echarlo en el buzón de la esquina. Este sería el modo más fácil y rápido de ocuparse de la tarea, pero no tendría idea de cuándo o si el reporte llegó a su destino.

Por otra parte, Usted podría ir a la oficina de correos y llenar una tarjeta para enviar el reporte mediante el servicio de correo registrado y certificado con un recibo de retorno solicitado. Costaría más y tomaría más tiempo y esfuerzo de su parte, pero sería una forma de comunicación más confiable. Recibiría una notificación cuando el paquete haya sido entregado, demostrando que fue recibido realmente por la persona a la que estaba destinado.

Los servicios orientados a la conexión se asemejan al segundo ejemplo, aunque ellos realmente van un paso más allá: ellos establecen la conexión antes de enviar los datos. Esto sería como si antes de enviar su correo certificado, Usted hablara por teléfono con el director de la sucursal en El Paso y le dijera que va a enviar el correo, de modo que él esté a la espera de su llegada. Si Usted es una persona que piensa en los detalles (o un paranoico), podría incluso pedirle que lo llame cuando lo reciba y le diga que todas las páginas están allí en secuencia y que el reporte no se dañó por el camino. Eso es, en esencia, lo que hace un servicio orientado a la conexión. Usted se tomó molestias para asegurar que su comunicación fuera lo más confiable posible, pero a costa del tiempo (y los cargos por la llamada telefónica de larga distancia) para ambos: Usted y el receptor.

¿Cuál Puerto en una Tormenta (Broadcast)?

Gracias a la capacidad de realizar multitareas de Windows 2000 y de otros sistemas operativos modernos, Usted puede utilizar simultáneamente más de una aplicación de red. Por ejemplo, puede utilizar su visualizador Web para acceder a la página de inicio de su compañía al mismo tiempo que su software de mensajería electrónica está descargando sus correos. Usted sabe que el TCP/IP usa una dirección IP para identificar su computadora en la red y llevar los mensajes al sistema correcto, pero ¿cómo esta separa la respuesta a Su solicitud del visualizador de los correos entrantes si ambos arriban a la misma dirección IP?

Ahí es donde entran a relucir los puertos. Si las dos partes de una dirección IP, que representan la identificación de la red y la identificación de la máquina anfitriona

(computadora individual), son similares al nombre de una calle y al número individual de la calle, Usted podría pensar en el número de puerto como un identificador del apartamento o suite en específico dentro del edificio.

TCP y UDP, los protocolos de la capa de transporte, asignan números de puerto a cada aplicación, de modo que los datos dirigidos al visualizador Web en el Apartamento A no se envían al programa de mensajería electrónica en el Apartamento B.

La tabla 5.2 muestra algunos de los puertos comúnmente usados (los puertos designados utilizan ciertos servicios o ciertas aplicaciones por defecto).

Tabla 5.2 Puertos específicos están designados para el uso de ciertos servicios o ciertas aplicaciones.

Número de Puerto	Servicio/Aplicación
7	Eco
20,21	Protocolo de Transferencia de Ficheros (FTP)
23	Telnet
25	Protocolo Simple de Transferencia de Correo (SMTP)
53	Sistema de Nombre de Dominio (DNS)
68	Protocolo de Configuración Dinámica de Servidores (DHCP)
69	Protocolo de Transferencia de Archivos Trivial (TFTP)
80	Protocolo de Transferencia de Hipertexto (HTTP)
88	Kerberos
110	Protocolo de Oficina de Correo, versión 3 (POP3)
119	Protocolo de Transferencia de Noticias
143	Protocolo de Acceso a Mensajes electrónicos almacenados en un servidor de Internet (IMAP)
161	Protocolo Simple de Gestión de Redes (SNMP)
220	IMAP 3

La Dirección MAC

Cuando analizamos la “dirección” de una computadora, en el contexto del TCP/IP, generalmente nos estamos refiriendo a su dirección IP. La dirección IP es una dirección *lógica*; puede ser asignada por el administrador (o por un servidor DHCP) y puede cambiarse fácilmente. Sin embargo, cada tarjeta o interfaz de red también tiene una dirección *física*, denominada *dirección de Control de Acceso a los Medios (MAC)*. Esta dirección, por lo general, es quemada permanentemente en un chip de la NIC y no se puede cambiar tan fácilmente (aunque algunos fabricantes de NIC le permiten cambiar la dirección MAC “flasheando” la tarjeta con un software especial).

¿Cómo se correlaciona la dirección MAC con la dirección IP? Véalo de esta manera: Una ciudad o un condado puede asignarle un nombre de calle y un número de casa a una

estructura física, pero esta es realmente sólo una dirección “lógica”. Esta dirección se puede cambiar; a veces un grupo del vecindario pide que una calle sea renombrada o el ayuntamiento de la ciudad cambia el esquema numérico para facilitar una respuesta de emergencia o para acomodar una construcción nueva. Pero el lugar donde se encuentra el edificio también tiene una dirección “física” – sus coordenadas geográficas. Cuando se mide la tierra, el lugar se identifica con grados de longitud y altitud y esos puntos permanecerán constantes a pesar de los cambios de nombre y número de calle. Esa dirección física es como la dirección MAC de la NIC; (casi siempre) será la misma.

Las direcciones MAC en tarjetas Ethernet son generalmente números hexadecimales de 12 dígitos, con una parte de la dirección identificando al vendedor de la NIC. El IEEE le asigna esta parte al vendedor. Dos NIC no deben tener la misma dirección MAC (aunque esto realmente no se convierte en un problema a menos que las dos direcciones idénticas estén en la misma red). El ARP mapea direcciones IP para direcciones MAC.

Resolución de Nombres

¿Qué hay en un nombre? Cuando se trata de interconexión de computadoras, la respuesta es: mucho. En redes basadas en el TCP/IP, los puntos finales de la comunicación son las direcciones IP de las máquinas anfitrionas y las computadoras de destino. Pero las direcciones IP son difíciles de recordar para los humanos. Solo imagine un mundo en que las personas se identificaran únicamente con números – ¿cuán más difícil resultaría mantener claras esas identificaciones si tuviera que recordar que el colega que acaba de conocer se llama 1000101000110111 en lugar de Bob? La mayoría de los programas de software tampoco están escritos para estar “conscientes” de las direcciones IP. El acceso a la red estaría lleno de errores si todos tuvieran que recordar la dirección IP de cada máquina anfitriona con la que ellos quisieran comunicarse.

Debe existir un mecanismo entonces que le permita a los usuarios y programas acceder a los recursos de la red mediante el nombre de una computadora o máquina anfitriona, en lugar de solo direcciones IP. Ese es el papel del *servicio de resolución de nombres*. Los servicios de resolución de nombres en uso en las redes actuales se dividen en dos extensas categorías:

- Resolución de nombres NetBIOS
- Resolución de nombre de máquina anfitriona

En las siguientes secciones, veremos el “cómo y el porqué” de la resolución de nombres NetBIOS, definiremos y analizaremos los métodos principales de resolver nombres NetBIOS, incluyendo el Servicio de Nombres de Internet de Windows. Luego abordaremos la resolución de nombres de máquinas anfitrionas y examinaremos cómo los nombres jerárquicos empleados en la Internet (como www.shinder.net) son resueltos en direcciones IP, centrándonos en el Sistema de Nombre de Dominio y su más reciente encarnación, el DNS Dinámico.

Resolución de nombres NetBIOS

Una compañía llamada Sytek, Inc. creó el NetBIOS en 1983 para la IBM. El protocolo de transporte NetBIOS fue diseñado para acomodar pequeñas LAN localizadas en un solo segmento, y el protocolo de transporte NetBEUI es un producto del protocolo de transporte NetBIOS. NetBEUI utiliza el conjunto de instrucciones provisto con el estándar NetBIOS y lo ha “extendido” – de ahí el nombre Interfaz Extendida de Usuario NetBIOS (NetBEUI).

Los programas escritos para la interfaz NetBIOS usan los nombres NetBIOS como los “puntos finales” de las comunicaciones. Cada computadora en una red NetBIOS debe tener un nombre NetBIOS, que consiste en 16 bytes. Sólo los primeros 15 bytes del nombre NetBIOS son configurables por el usuario. El byte 16 es usado por el sistema operativo para denotar la disponibilidad de los servicios de la red. Los programas NetBIOS *deben* conocer el nombre de la computadora de destino a fin de establecer una sesión.

En aras de acceder a la computadora de destino se utiliza un broadcast. Los mensajes broadcast son enviados a todas las computadoras en un segmento de la red, en lugar de a un destino específico. Esto significa que todas las computadoras deben estar en la misma subred física, pues normalmente los mensajes broadcast no cruzan los enrutadores. En instalaciones de redes mayores (más de aproximadamente 40 o 50 computadoras), el volumen de tráfico broadcast se tornaría tan “fuerte” por la congestión en la red que ninguna información útil podría pasar.

De modo que el NetBIOS se basa en el broadcast, está limitado a un solo segmento y utiliza nombres NetBIOS como puntos finales de las comunicaciones. Esto representa un reto significativo para los programas NetBIOS que necesitan funcionar en una red basada en el TCP/IP. La pila de protocolos TCP/IP fue diseñada para trabajar en grandes conjuntos de redes interconectadas, con los segmentos separados por enrutadores. Los enrutadores no reenvían broadcasts por defecto. Por lo tanto, las aplicaciones NetBIOS no podrán acceder a los recursos de las computadoras localizadas en otro segmento. Incluso si abrimos los puertos NetBIOS en los enrutadores, aún tendremos el problema de las aplicaciones NetBIOS que utilizan sólo nombres NetBIOS. Antes de que la solicitud puede pasar a la pila de protocolos TCP/IP, el nombre NetBIOS debe ser convertido o *resuelto* en una dirección IP.

Todo el proceso de enlazar un nombre NetBIOS con una dirección IP se denomina *resolución de nombres NetBIOS*. En aras de lograr que el TCP/IP “se preocupe” por los nombres NetBIOS y lidie con ellos en un modo ordenado, necesitamos adicionarle algo a la pila de protocolos TCP/IP. Este “aditamento” se denomina *NetBIOS sobre TCP/IP*, abreviado como NETBT o NBT. La NetBT se implementa en la interfaz de la capa de sesión NetBIOS.

Cuando una solicitud de servicios de la red pasa de la aplicación de usuario a la capa de aplicación de la pila TCP/IP, la NetBT intercepta la solicitud y el nombre NetBIOS es resuelto en una dirección IP. Tras ser descubierta la dirección IP, la solicitud pasa, ahora incluyendo la dirección IP de la computadora de destino. Esta se mueve en dirección vertical hacia la pila de la capa de transporte, luego a la capa de red y a través de la capa de enlace de datos y la capa física hasta el cable (o a los medios inalámbricos).

En la escena...

Comprendiendo la Necesidad de la Resolución de Nombres NetBIOS

He aquí una analogía para ayudarle a comprender la necesidad de la resolución de nombres NetBIOS. Un niño pequeño le escribe una carta a su madre y se la dirige a “Mamá”, el *nombre cariñoso* con el que él la identifica. Si el niño fuese a dejar esta carta sobre la mesa de la cocina, no habría problemas para que esta llegue a la computadora de destino (Mamá). Esto es porque la mesa de la cocina está en el segmento local (la cocina de la casa de Mamá). Pero, si el niño echara la carta en un buzón, la oficina de correos se vería ante un gran reto al tratar de hacer que la carta llegue al destino correcto. “Mamá” es como un nombre NetBIOS en el que no hay una dirección routable (trazable). Sin embargo, si el padre del niño toma esa carta y la pone en otra sobre que tiene en el frente ambas cosas: Mamá y la dirección de la casa, la oficina de correos podría entregar el mensaje. La dirección de la casa es una dirección routable (trazable), de modo que la carta ahora encontrará su camino hacia la mamá correcta. Lo que hizo papá es similar a lo que el NetBT hace por los nombres NetBIOS. Esta convierte las solicitudes de nombres NetBIOS en solicitudes de direcciones IP, de forma tal que el mensaje o la comunicación llegue a la máquina deseada.

NetBIOS y NetBEUI, que utilizan un espacio de nombre plano para la identificación de computadoras y no incluyen ningún método de identificación de la red en la que reside una computadora, son, consecuentemente, protocolos *no routables (trazables)*. Pero cuando el nombre NetBIOS se convierte en una dirección IP, que sí identifica la red, nuestro mensaje se torna en una solicitud routable.

Los sistemas operativos de Microsoft emplean varias formas diferentes de resolver nombres NetBIOS en direcciones IP. Es por ello que resulta de vital importancia para las aplicaciones NetBIOS poder acceder a la dirección IP de una máquina de destino en una red basada en TCP/IP. Si el nombre NetBIOS no puede ser resuelto, la aplicación NetBIOS no podrá establecer una sesión con la máquina de destino. Los nombres NetBIOS se pueden resolver con los siguientes mecanismos:

- Caché de nombres NetBIOS
- Servidores de nombres NetBIOS
- Broadcasts
- Fichero LMHOSTS

El caché remoto de nombres NetBIOS contiene los mapeos de nombres y direcciones IP de las máquinas accedidas recientemente. Este caché es examinado antes de que cualquier otro método de resolución de nombres NetBIOS tenga lugar.

Un servidor de nombres NetBIOS conserva las trazas de los nombres NetBIOS y sus direcciones IP asociadas. En el mundo real, el NetBIOS se emplea de forma generalizada sólo en redes Microsoft y casi todos los servidores de nombres NetBIOS corren WINS de Microsoft. Es improbable que Usted se encuentre con alguna otra implementación de servidores de nombres NetBIOS, así que desde este momento en adelante nos referiremos a

los servidores de nombres NetBIOS como servidores WINS. Los servidores WINS tienen dos funciones básicas. La primera es el registro de los nombres NetBIOS, donde el servidor WINS registra los nombres NetBIOS y las direcciones IP de las computadoras. Un servidor WINS actualiza dinámicamente y automáticamente los nombres NetBIOS de los clientes cuando los clientes de WINS comienzan. La segunda función importante de un servidor WINS es resolver las preguntas sobre nombres NetBIOS cuando los clientes NetBIOS le preguntan al servidor WINS por la dirección IP de una máquina NetBIOS de destino.

Incluso en redes basadas en TCP/IP, los clientes NetBIOS también pueden preguntar (broadcast) por la dirección IP de una máquina de destino. La efectividad del método broadcast es limitada, porque, por defecto, los enrutadores no pasan tráfico por los puertos UDP 137 y 138 (el servicio de nombres NetBIOS y los servicios de datagramas NetBIOS, respectivamente). Por ende, la resolución de nombres NetBIOS a través del método broadcast funciona sólo cuando los clientes de destino se encuentran en el mismo segmento.

El fichero LMHOSTS es un fichero de texto estático, actualizado manualmente que contiene los mapeos de nombres NetBIOS y direcciones IP para las máquinas NetBIOS. El fichero LMHOSTS resuelve nombres NetBIOS leyendo el fichero de arriba hacia abajo. Esto significa que las computadoras accedidas con mayor frecuencia deben tener sus nombres colocados en la parte superior, mientras que los ficheros accedidos con menor frecuencia deben tener sus nombres colocados hacia la parte inferior. Debido a su naturaleza estática, el fichero LMHOSTS no funciona bien en redes que utilicen direcciones IP asignadas dinámicamente o en grandes redes empresariales.

Los nombres NetBIOS también pueden ser resueltos por métodos de resolución de nombres de máquinas como el fichero HOSTS o el servidor DNS (que analizaremos en la próxima sección) si otros métodos de resolución de nombres NetBIOS han fallado.

Resolución de Nombres de Máquinas

Los nombres de máquinas se utilizan para identificar computadoras en Internet. Recuerde que cualquier tipo de nombre, ya sea un nombre NetBIOS plano o un nombre de máquina jerárquico, es sólo una comodidad para los seres humanos. Las computadoras trabajan sólo con números, de modo que para ser utilizables, los nombres de máquinas, al igual que los nombres NetBIOS, a la larga tienen que ser resueltos en direcciones IP.

Cuando la Internet se encontraba en su infancia, los nombres de máquinas se resolvían en direcciones IP a través de un fichero de texto plano llamado hosts.txt. Este fichero se encontraba en el Centro de Información de Redes del Instituto de Investigaciones Stanford (SRI-NIC). Cada vez que una máquina se añadía a la red o la dirección IP de una máquina existente se cambiaba, el fichero hosts.txt debía ser editado. Entonces había que descargar este fichero hosts.txt del SRI-NIC de modo que todas las máquinas de la red tuvieran una lista precisa de los nombres de las máquinas y las direcciones IP para la resolución de nombres de máquinas.

Existieron varios problemas con el uso del fichero hosts.txt. Primeramente, este utilizaba un espacio de nombre plano como aquel visto en el NetBIOS. El espacio de nombre plano requería que cada computadora tuviera un nombre diferente. En segundo lugar, mientras más máquinas se unían a la red, el tráfico en SRI-NIC se convertía en un cuello de botella significativo para las comunicaciones de la red. En tercer lugar, el tamaño del fichero hosts.txt se incrementaba, lo que traía como consecuencia largos tiempos de descarga y un rendimiento reducido para las búsquedas.

Nota

Los sistemas operativos Microsoft aún utilizan un fichero Hosts para la resolución de nombres de dominio completamente calificados; sin embargo, este fichero Hosts no usa la extensión .txt (ni ninguna). Un error común en crear un fichero Hosts en Notepad u otros editores de texto es que la aplicación lo salva con la extensión .txt y así no funcionará.

Para solucionar estos problemas, en 1987 Paul Mockapetris creó y propuso el Sistema de Nombre de Dominio (DNS). El DNS fue diseñado para ser un sistema de nombre jerárquico, con responsabilidad sobre la base de datos DNS distribuida en vez de centralizada. Por esa razón, los nombres de máquinas actuales son *jerárquicos*. Estos tienen múltiples partes, tantas como tiene el nombre de una persona en la cultura estadounidense moderna. Su apellido identifica a la familia a la cual pertenece, y su primer y segundo nombres identifican a un individuo dentro de esa familia. Los nombres de máquinas funcionan de la misma manera, excepto que la “familia” es un dominio y pueden existir subdominios dentro de un dominio. Es por ello que dos computadoras pueden tener el mismo nombre de computadora, siempre y cuando estén en dominios diferentes (al igual que no hay problema al diferenciar entre dos personas llamadas Bob cuando una se llama Bob Smith y el otro Bob Jones). Hay miles de máquinas en Internet llamadas www., aunque este es generalmente un nombre asignado a una máquina virtual – la función de servidor Web corriendo en una computadora que podría tener un nombre completamente diferente. Sin embargo, sus “nombres completos” son únicos. No hay problema para diferenciar entre www.shinder.net y www.tacteam.net porque sus nombres de dominio son diferentes.

En la cima de la jerarquía del DNS está el *dominio raíz*. El dominio raíz, a veces, aparece representado como un período rodeado de marcas de cotación (“.”) o como un espacio rodeado por marcas de cotación. Justo debajo del dominio raíz están los *dominios de nivel superior*. Los dominios de nivel superior consisten en una designación de dos o tres letras, como, por ejemplo, .com, .net, .org (llamados *dominios genéricos*) o .au, .us, .de (llamados *códigos de países*). Los *dominios de segundo nivel* se encuentran debajo de los dominios de nivel superior. Estos dominios de segundo nivel se nombran según las organizaciones que poseen los nombres de dominio – por ejemplo, “BrandXDrugs.com”. Un nombre de dominio de segundo nivel se puede obtener de una secretaría de dominios, como Network Solutions, Inc (NSI). El dominio raíz, los dominios de nivel superior y los dominios de segundo nivel son los únicos aspectos centralizados del DNS. Luego que una compañía o un individuo registra un nombre de dominio de segundo nivel con un funcionario de la

secretaría de dominios, ellos son libres de crear tantos *subdominios* como deseen – esos subdominios se ubican dentro del dominio de segundo nivel, como en “sedatives.BrandXDrugs.”

Nota

Se continúan aprobando nuevos registradores de nombres de dominio. Para un listado actualizado de registradores autorizados, véase el sitio Web de ICANN: www.icann.org/registrars/accredited-list.html.

La combinación de un nombre de máquina y su nombre de dominio es referida como un *nombre de dominio completamente calificado (FQDN)*. Todas las máquinas participantes en el DNS son identificables por sus FQDN. Los servidores que mantienen una base de datos mapeando los nombres de máquina y dominio en direcciones IP se denominan *servidores DNS*.

Las computadoras en redes TCP/IP están configuradas con la dirección IP de un servidor DNS como parte del establecimiento de las propiedades TCP/IP. Cuando un nombre de máquina necesita ser resuelto, la computadora (llamada *cliente DNS*) envía una solicitud al servidor DNS. El servidor DNS busca en su base de datos y responde con la dirección IP asociada al nombre de máquina o, si el nombre no se encuentra en su base de datos, el servidor le puede preguntar a otros servidores DNS para encontrar la dirección.

Debido a que el DNS debe trabajar para resolver nombres a través de Internet, una serie de estándares gobiernan su implementación. Por ejemplo, los nombres de máquinas deben seguir convenciones específicas sobre nombres. Estas se explican detalladamente en los artículos 952 y 1123 del RFC. De acuerdo con estos estándares, los nombres están limitados a letras mayúsculas y minúsculas (A-Z y a-z), a los números 0-9 y al guión (-).

El DNS también es empleado por el Directorio Activo de Microsoft (Windows 2000 y controladores de dominio posteriores) para la resolución de nombres. Los servidores DNS de Microsoft permiten el uso de otros caracteres como el guión inferior (_) en los nombres de máquinas porque ellos soportan UTF-8, un súper conjunto del conjunto de caracteres ASCII que le permite utilizar alfabetos de otros idiomas. Sin embargo, estos nombres no serán reconocidos por muchos de los servidores DNS basados en UNIX en Internet.

Utilidades del TCP/IP

Una serie de herramientas de software asociadas con los protocolos TCP/IP pueden ser utilizadas por los investigadores. Las pilas TCP/IP de vendedores diferentes no son idénticas, como tampoco lo son las utilidades de diagnóstico y de obtención de información que están incluidas. En esta sección, nos concentraremos en las utilidades que vienen con la suite TCP/IP de Windows. También mencionamos sus equivalentes (si son aplicables) en implementaciones de UNIX/Linux.

Nota

Las herramientas TCP/IP que analizamos aquí son las utilidades de línea de comandos que están incluidas en las pilas TCP/IP de varios sistemas operativos. Las utilidades de terceros están disponibles (muchas de ellas gratuitas) que ofrecen interfaces gráficas para realizar las mismas funciones.

Utilidades de Verificación de Conexión, Identificación y Rastreo

Varias utilidades de línea de comandos se pueden usar para comprobar la conectividad TCP/IP, obtener información sobre la configuración TCP/IP, configurar propiedades y rastrear la ruta que toma un paquete en la red. Esas herramientas incluyen las siguientes:

- PING
- NSLOOKUP
- IPCONFIG/IFCONFIG
- ROUTE
- TRACERT/TRACEROUTE
- ARP

PING, abreviatura de *Rastreador de Paquetes de Internet*, se usa para determinar si una conexión TCP/IP se puede establecer con una dirección en particular. Usted puede PING una computadora o un enrutador en la red local o en una red remota, o Usted puede comprobar la configuración de la pila TCP/IP realizando PING a la dirección de bucle 127.0.0.1. El PING funciona enviando mensajes de solicitud eco ICMP a la computadora de destino, luego retorna un mensaje de respuesta eco. La respuesta le muestra el número de paquetes enviados y recibidos (junto con el porcentaje de paquetes perdidos, si hubo alguno) y el tiempo en milisegundos que toma para que un paquete haga todo el recorrido. Como se muestra en la Figura 5.12, usted puede PING una computadora por la dirección IP o por el nombre. Si Usted hace PING por el nombre, la respuesta le da la dirección IP de la computadora.

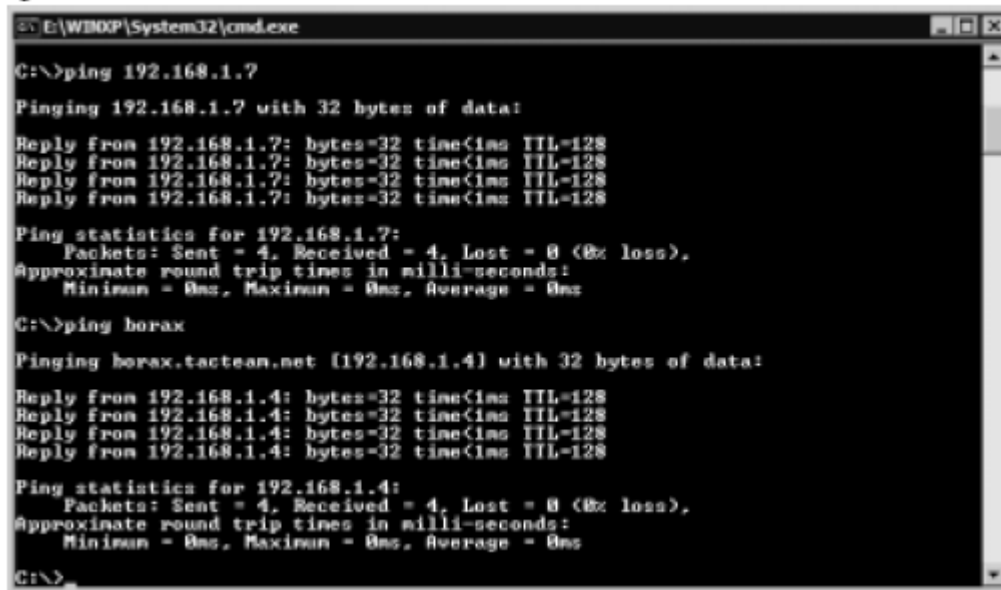
PING incluye una docena de parámetros que se pueden emplear para controlar aún más el comportamiento de la función PING. En la Tabla 5.3 se muestran parámetros disponibles.

Tabla 5.3 Parámetros PING

Parámetro	Función
-t	Hace PING a la máquina específica hasta que lo detengan (PING continuo) presionando ctrl.-C.
-a	Resuelve direcciones en nombres de máquinas.
-n count	Especifica el número de solicitudes eco a enviar.
-l size	Especifica el tamaño del búfer de envío.
-f	Pone la bandera de No Fragmentar en el paquete.
-i TTL	Hora de vivir.
-v TOS	Tipo de servicio.
-r count	Registra la ruta para el conteo de saltos.
-s count	Representación de fecha para contar saltos.
-j host-list	Ruta de fuente flexible en la lista de máquinas.

- k host list Ruta de fuente estricta en la lista de máquinas.
- w timeout Tiempo muerto en milisegundos a esperar por cada respuesta.

Figure 5.12 The PING command provides TCP/IP connectivity information.



```
E:\WINDOWS\System32\cmd.exe
C:\>ping 192.168.1.7

Pinging 192.168.1.7 with 32 bytes of data:
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping borax

Pinging borax.tactean.net [192.168.1.4] with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figura 5.12 El comando PING brinda información sobre la conectividad TCP/IP.

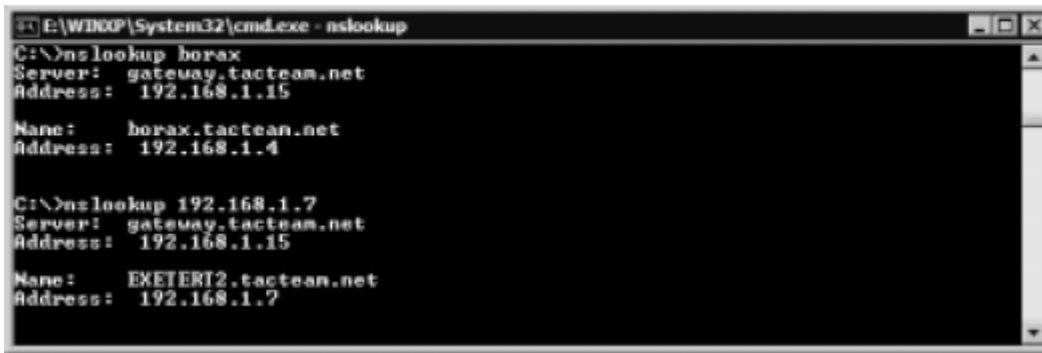
Para más información acerca del empleo del PING y sobre cómo funciona la utilidad PING, véase www.cisco.com/warp/public/63/ping_traceroute.html#ping.

NSLOOKUP se emplea para encontrar el nombre de máquina asociado con una dirección IP (o viceversa), como se muestra en la figura 5.13. NSLOOKUP le pide a los servidores DNS información acerca de las máquinas y los dominios. NSLOOKUP puede ser un punto de inicio para rastrear criminales cibernéticos que utilizan sus direcciones IP.

Para más información sobre el uso del NSLOOKUP, véase la página del manual de Sistemas para UNIX: www.stopspam.org/usernet/mmf/man/nslookup.html.

El comando **ipconfig** (en máquinas Windows) brinda la información básica sobre la configuración TCP/IP. La figura 5.14 muestra los resultados de **ipconfig** (corre con el parámetro **/all**).

Figure 5.13 The NSLOOKUP utility can be used to discover the hostname associated with an IP address.



```
E:\WDROP\System32\cmd.exe - nslookup
C:\>nslookup borax
Server: gateway.tactean.net
Address: 192.168.1.15

Name: borax.tactean.net
Address: 192.168.1.4

C:\>nslookup 192.168.1.7
Server: gateway.tactean.net
Address: 192.168.1.15

Name: EXETERI2.tactean.net
Address: 192.168.1.7
```

Figura 5.13 La utilidad NSLOOKUP se puede utilizar para descubrir el nombre de la máquina asociado a una dirección IP.

Figure 5.14 The ipconfig /all command in Windows provides configuration information.



```
E:\WDROP\System32\cmd.exe
C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : xpedition
    Primary Dns Suffix . . . . . : tactean.net
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : tactean.net

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : tactean.net
    Description . . . . . : 3Com 3C920 Integrated Fast Ethernet
    Controller (3C985C-IX Compatible)
    Physical Address. . . . . : 88-B8-D8-15-EF-92
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 192.168.1.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.7
    DNS Servers . . . . . : 192.168.1.15
                           192.168.1.185
    Primary WINS Server . . . . . : 192.168.1.185
    Secondary WINS Server . . . . . : 192.168.1.15

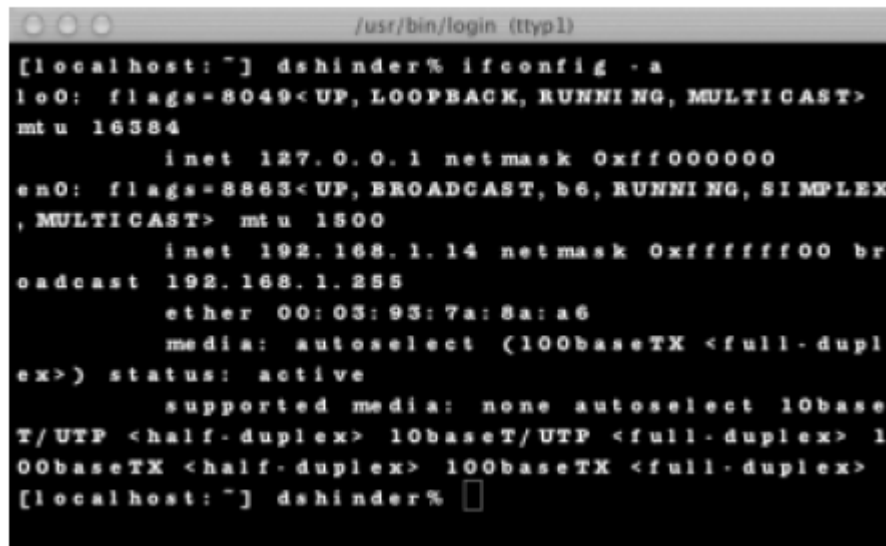
C:\>
```

Figura 5.14 El comando ipconfig /all en Windows ofrece información sobre la configuración.

Como puede ver, esta utilidad le da a Usted una gran cantidad de información acerca de la configuración de la máquina, incluyendo el nombre de la misma y el sufijo DNS asignado a ella, el adaptador Ethernet instalado (y su dirección física o MAC), la dirección IP, la máscara de la subred, la puerta de enlace implícita y los servidores DNS y WINS asignados. Vemos que esta información fue asignada manualmente por el administrador, porque el DHCP no está habilitado. También podemos observar que la máquina no está actuando como un enrutador IP o un proxy WINS.

En máquinas UNIX/Linux, podemos disponer de alguna información básica sobre la configuración utilizando el comando **ifconfig** con el parámetro **-a**. Esto se muestra en la Figura 5.15, empleando el sistema operativo Macintosh OS X.

Figure 5.15 The command used to display configuration information in UNIX is **IFCONFIG -a**.



```

/usr/bin/login (tty1)

[localhost:~] dshinder% ifconfig -a
lo0: flags=8049<UP, LOOPBACK, RUNNING, MULTICAST>
mtu 16384
    inet 127.0.0.1 netmask 0xffff0000
en0: flags=8863<UP, BROADCAST, b6, RUNNING, SIMPLEX, MULTICAST>
mtu 1500
    inet 192.168.1.14 netmask 0xfffff000 broadcast 192.168.1.255
    ether 00:03:93:7a:8a:a6
    media: autoselect (100baseTX <full-duplex>) status: active
    supported media: none autoselect 10baseT/UTP <half-duplex> 10baseT/UTP <full-duplex> 100baseTX <half-duplex> 100baseTX <full-duplex>
[localhost:~] dshinder% 
```

Figura 5.15 El comando utilizado para visualizar la información sobre la configuración en UNIX es **IFCONFIG-a**.

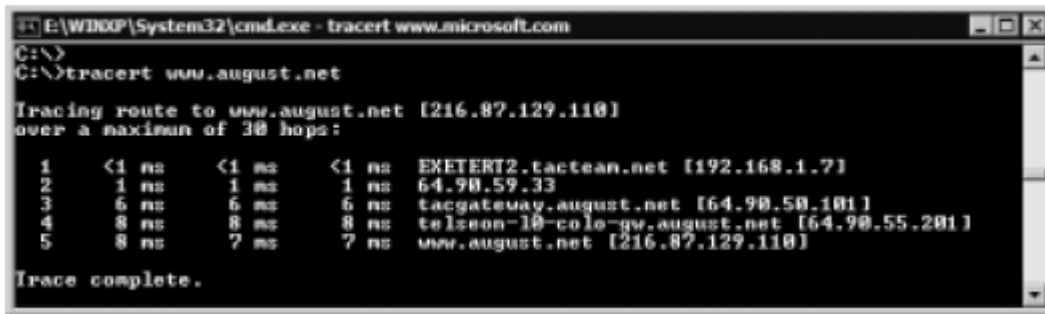
Como puede apreciar, la información aparece en formatos diferentes, pero aún así Usted puede determinar la dirección IP de la computadora, la máscara de la subred (en hexadecimal en lugar de en decimal), la dirección física Ethernet y otras informaciones básicas.

La utilidad **ROUTE** se utiliza en máquinas de Windows y en aquellas basadas en UNIX para visualizar y manipular manualmente las tablas de enrutamiento de la red. Usted puede añadir, borrar o modificar rutas con esta herramienta, aunque generalmente no es necesario, pues Windows puede construir automáticamente una tabla de enrutamiento utilizando el RIP o el OSPF. Además, en computadoras UNIX, los daemons de la tabla de enrutamiento del sistema como **routed(8)**, que utilizan el RIP y el Protocolo de Detección de Enrutadores de Internet (IRDP), se encargan de esa tarea. Para visualizar la información de la tabla de enrutamiento, use el comando **ROUTE PRINT**.

Los comandos **TRACERT** (en Windows) y **TRACEROUTE** (en UNIX) se emplean para rastrear la ruta tomada por un paquete para llegar a una máquina remota. Usted puede especificar una dirección IP o un nombre de máquina como la máquina de destino. Los resultados le mostrarán el número de “saltos” requeridos para llegar al destino, así como la cantidad de tiempo (en milisegundos) por cada salto. Usted puede ver los nombres de los enrutadores a través de los cuales pasa el paquete. También puede especificar un número

máximo de saltos a usar en la búsqueda de la computadora objetivo. La figura 5.16 ilustra el seguimiento de una ruta que fue completada en cinco saltos.

Figure 5.16 The TRACERT and TRACEROUTE commands allow you to view the route taken by a packet to a remote destination.



```
E:\WINDDP\System32\cmd.exe - tracert www.microsoft.com
C:\>
C:\>tracert www.microsoft.com

Tracing route to www.microsoft.com [216.87.129.110]
over a maximum of 30 hops:
  0  <1 ns    <1 ns    <1 ns    EXETER12.tactean.net [192.168.1.7]
  1  1 ns      1 ns      1 ns      64.90.59.33
  2  6 ns      6 ns      6 ns      tacgateway.august.net [64.90.50.101]
  3  8 ns      8 ns      8 ns      telson-10-colo-gw.august.net [64.90.55.201]
  4  8 ns      7 ns      7 ns      www.august.net [216.87.129.110]

Trace complete.
```

Figura 5.16 Los comandos TRACERT y TRACEROUTE le permiten visualizar la ruta tomada por un paquete hacia un destino remoto.

El comando **ARP** (Protocolo de Resolución de Direcciones) le permite visualizar y manipular las entradas en el caché ARP. El caché ARP es una lista de ambas direcciones: la IP y la física correspondiente (MAC) para computadoras que recientemente han tenido una conexión con una computadora en la que Usted está corriendo la utilidad ARP. Esa utilidad también le permite añadir y borrar entradas en el caché.

Utilidades de Estadística de la Red

Las utilidades de estadísticas pueden proporcionarle información acerca de las conexiones de la red. Estas incluyen:

- NETSTAT
- NBTSTAT

El comando **NETSTAT** se puede emplear en computadoras basadas en UNIX y en computadoras de Windows para obtener información sobre las conexiones actualmente activas que usan diferentes protocolos (TCP, UDP, RAW o socket UNIX). Con este comando se visualiza cada conexión en una línea separada, mostrando la dirección local (computadora y puerto) y la dirección remota (o “extranjera”), así como el estatus (estado) de la conexión. En la figura 5.17 se muestran los resultados del uso del comando **NETSTAT**.

También existen parámetros que se pueden utilizar con **NETSTAT** para brindar información diferente o adicional. Algunas de estas informaciones pueden ser útiles para los investigadores. Por ejemplo, saber que existen puertos abiertos y a la escucha en la máquina es un tema de seguridad importante cuando la computadora está conectada a Internet.

En la tabla 5.4 se muestran los parámetros **NETSTAT**.

Figure 5.17 The **NETSTAT** command can be used to display current active connections.

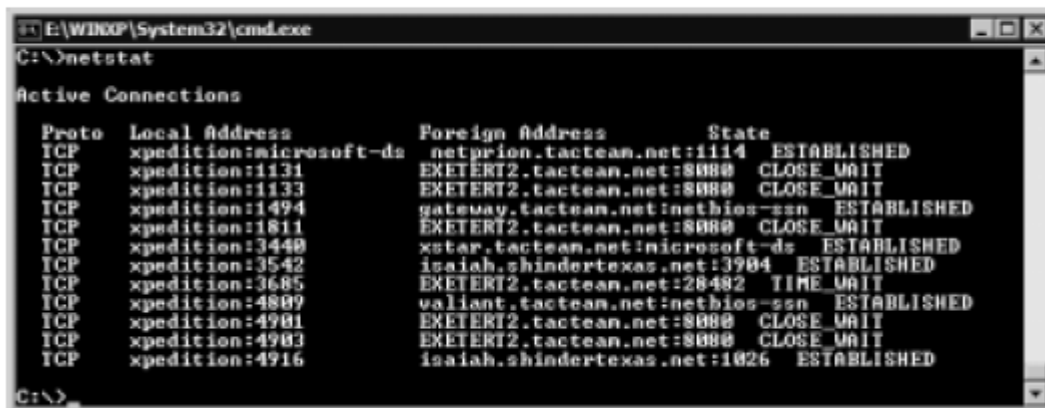


Figura 5.17 El comando **NETSTAT** se puede emplear para visualizar las conexiones actualmente activas.

Tabla 5.4 Parámetros **NETSTAT**

Parámetro	Función
-a	Muestra todas las conexiones, incluyendo los puertos a la escucha.
-e	Muestra las estadísticas Ethernet, como son el número de bytes de datos recibidos y enviados (puede ser combinado con la opción -s).
-n	Muestra las direcciones y los números de puerto en forma numérica.
-o	Muestra el proceso de reconocimiento del ID asociado con cada conexión.
-p proto	Muestra sólo las conexiones para el protocolo especificado por <i>proto</i> (por ejemplo, TCP).
-r	Muestra la tabla de enrutamiento (la misma información que Usted obtiene con el comando ROUTE PRINT EN Windows).
-s	Muestra las estadísticas por protocolo.

Herramientas de Monitoreo de la Red

Existen disponibles muchas herramientas para monitorear la actividad de la red e incluso capturar los paquetes transmitidos y hurgar dentro de ellos. Algunas de esas herramientas están incluidas en los sistemas operativos modernos, algunas son distribuidas gratuitamente en Internet como “artículos libres de costo” y otras se le deben comprar a vendedores intermediarios.

Protocolo Simple de Gestión de Redes

El Protocolo Simple de Gestión de Redes (SNMP) no es una utilidad en sí mismo, sino que es un protocolo utilizado para pasarle mensajes sobre el estatus de dispositivos distribuidos por la red a máquinas configuradas para recibir esos mensajes de estatus. Las máquinas que reportan su estatus corren el software *agente* SNMP y las máquinas que reciben los mensajes de estatus corren el software de *gestión* SNMP. Una forma de recordar cómo esto funciona es imaginarse el software agente como el “agente secreto” que obtiene información sobre un dispositivo de red y luego reporta la información a su “jefe” en la oficina central.

Aunque el nombre del protocolo le llevaría a creer que la función primaria es permitirle “gestionar” objetos en la red, la gestión en este contexto está más relacionada con el monitoreo y no con efectuarle realmente cambios a los dispositivos. El SNMP le permite auditar las actividades de servidores, estaciones de trabajo, enrutadores, puentes, concentradores inteligentes y cualquier dispositivo conectado a una red que soporte la instalación del software agente.

Para que el software agente recopile información referente a un servicio en particular, se debe crear una *Base de Información de Gestión (MIB)*. La MIB es una base de datos y una colección de instrucciones acerca de cómo y qué información se debe obtener del sistema. El agente es responsable de reportar la información obtenida por la MIB. Sin embargo, por lo general, los agentes no ofrecen la información espontáneamente, sino que un sistema de gestión SNMP debe preguntarle antes de que este diga lo que sabe. Existe una excepción para esta regla, llamada *mensaje trampa*. Un mensaje trampa es enviado espontáneamente por un agente a sistemas de gestión SNMP que han sido configurados para enviar.

Analizadores de Protocolo (“Rastreadores”)

Los analizadores de protocolo le permiten a los profesionales de las redes capturar y analizar el tráfico en la red. Estos pueden ser dispositivos de hardware o programas de software y, a menudo, son referidos como *rastreadores de paquetes*. Los sistemas operativos de Microsoft, NT, 2000 y .NET vienen con un analizador de protocolo incluido denominado *Monitor de Red (NetMon)*.

El Microsoft NetMon es un software analizador de protocolos que le permite a Usted capturar y analizar el tráfico en su red. Está incluido en los sistemas operativos para servidores Windows NT y Windows 2000. La versión de NetMon que viene con el sistema operativo tiene un alcance limitado; no le permite poner el adaptador de la red en “modo promiscuo”. Cuando un adaptador se encuentra en modo promiscuo, puede escuchar todo el tráfico en el segmento, incluso si ese tráfico no está destinado a la máquina que corre el software Monitor de Red. Una versión de NetMon más robusta está incluida en el Servidor de Gestión de Sistemas de Microsoft (SMS).

Aún con sus limitaciones, la versión “light” del Monitor de Red es una herramienta muy útil para evaluar la actividad en la red. Usted puede emplear la herramienta para recopilar

datos de la red y analizarlos en la marcha o para guardar las actividades registradas para otro momento. Esta le permite monitorear la actividad en la red y configurar disparadores (triggers) para cuando ciertos eventos o datos crucen el cable, lo que podría ser de utilidad si está buscando determinadas palabras claves en comunicaciones de correo electrónico que se mueven a través de la red.

Nota

Cualquier persona con privilegios administrativos puede instalar el Monitor de Red en una computadora de la familia de Windows Server y comenzar a “escuchar” la actividad en el cable. Esta es (entre muchas) una de las razones por las que se debe considerar cuidadosamente el número de personas dentro de una organización a las que se le asignen privilegios administrativos. El Monitor de Red también puede detectar cuando otra persona en el segmento está utilizando el Monitor de Red y darle su ubicación.

El programa Monitor de Red le permite capturar solamente aquellas tramas que le interesan, basándose en el protocolo, la fuente o la computadora de destino. Usted puede aplicarle a los datos que ya terminó de recopilar filtros aún más detallados y exactos, los que le permitirán ubicar con exactitud los elementos precisos que podría estar buscando dentro de los datos capturados. Para más información acerca del Monitor de Red de Microsoft, véase el artículo Q 148942 en el sitio Web de Microsoft.

En la escena...

Encontrando los Artículos Q

Usted puede encontrar una gran cantidad de información acerca de los productos Microsoft, incluyendo instrucciones de uso detalladas, en la Base de Datos Técnica de Microsoft (anteriormente denominada Base de Conocimientos), que puede buscar en <http://support.microsoft.com/default.aspx?In=EN-GB&pr=kbinfo&>.

Los analizadores de redes se pueden encontrar con muchos vendedores diferentes, incluyendo los siguientes:

- Sniffer Technologies, en sociedad con Network Associates, hace una serie de herramientas de análisis de redes, incluyendo versiones hechas específicamente para redes inalámbricas, redes a nivel corporativo y soluciones portátiles.
- Sniff-Tech comercializa un producto llamado ANASIL que incluye captura de protocolo y decodificación para protocolos usados en redes Microsoft, UNIX, NetWare y AppleTalk.
- Ethereal es un programa de análisis de protocolo para UNIX y Windows que se puede descargar gratuitamente de www.ethereal.com.

A menudo, los hackers utilizan softwares rastreadores para, encubiertamente, capturar paquetes y leer su contenido (que puede incluir las contraseñas de la red). Protegerse contra “ataques de rastreo” no autorizados requiere que los datos estén encriptados mientras viajan a través de la red (como lo hace el Protocolo de Seguridad IP, IPSec). Hay más

información disponible sobre los programas rastreadores para Windows y UNIX en www.packetattack.com/network_analysis_sniffers.html.

¿Por qué esto le concierne al investigador?

Una comprensión de la interconexión cliente/servidor y de lo que sucede a niveles superiores (más allá del físico) cuando las computadoras se comunican entre sí resulta vital para comprender las vulnerabilidades de seguridad que le permiten a los hackers acceder a las computadoras y redes sin autorización. Los protocolos TCP/IP son la base de la comunicación en Internet, y los criminales cibernéticos expertos están íntimamente familiarizados con su funcionamiento y saben cómo explotar sus características para obtener acceso o atacar y derrumbar servidores y redes.

La información de este capítulo conforma la base para comprender las descripciones más detalladas del Capítulo 6, “Comprendiendo las Intrusiones y los Ataques a las Redes” y también le ayudará a comprender las funciones de los mecanismos de seguridad descritos en el Capítulo 7, “Comprendiendo la Prevención del Crimen Cibernético” y en el Capítulo 8, “Implementando la Seguridad en el Sistema”.

Resumen

La interconexión de computadoras es un tema complejo, en parte debido a las siguientes razones:

- Existen muchas formas diferentes de enlazar computadoras a nivel físico utilizando diferentes tipos de medios y diferentes diseños o topologías.
- Existen muchos métodos diferentes de controlar el acceso a los medios y “dirigir el tráfico” a nivel de enlace.
- Existen muchas formas diferentes de manejar el direccionamiento y el enrutamiento de mensajes entre computadoras a nivel de red.
- Existen diferentes métodos de lidiar con la transferencia de datos a nivel de transporte.
- Existen una serie de protocolos y mecanismos de compartimiento de ficheros que se pueden utilizar para la comunicación de las computadoras a niveles superiores.

Una buena comprensión de la interconexión requiere de conocimientos sobre cómo los datos, convertidos en pulsos de luz o eléctricos, son enviados a través del cableado o las ondas de aire, así como sobre los procesos utilizados en los extremos de emisión y recepción con el fin de preparar esos datos para enviarlos y para traducir los datos recibidos nuevamente en una forma utilizable por las aplicaciones y, a la larga, por los usuarios de las computadoras.

Para una mayor eficiencia, los datos se dividen en trozos manejables llamados *paquetes*, y son estos paquetes los que se transmiten a través de una red. La estructura del paquete y el tamaño varían, en dependencia de los protocolos en uso. Los protocolos de redes son reglas que gobiernan los procedimientos exactos que siguen las computadoras al enviar y recibir datos. A fin de estandarizar estos procesos de modo que los sistemas que utilizan

diferentes plataformas de hardware y software de sistema operativo puedan comunicarse entre sí, se han creado modelos y especificaciones de interconexión, de forma tal que los vendedores puedan usarlos como pautas para asegurar la compatibilidad.

Los modelos OSI y DoD se han dividido en capas para definir las tareas específicas a realizar por los protocolos en los diferentes niveles o peldaños dentro del proceso de comunicación en la red. En el nivel físico, cada computadora que se comunicará en la red requiere de, al menos, una interfaz de red, generalmente en forma de tarjeta de interfaz de red o NIC. Las redes más simples requieren sólo de NIC y cableado para habilitar la comunicación. Para configuraciones de redes más complejas, una serie de dispositivos de hardware operan en diferentes capas para proporcionar una conectividad más eficiente. Estos dispositivos incluyen concentradores, conmutadores, puentes y enrutadores. Las puertas de enlace (generalmente implementadas como software) operan en los niveles más altos y se encargan de la traducción entre los diferentes protocolos.

Los sistemas operativos modernos vienen con capacidades de interconexión incluidas y los costosos sistemas operativos para servidores brindan muchos servicios de redes además del compartimiento de impresoras y ficheros, incluyendo autenticación, resolución de nombres, acceso remoto e incluso la capacidad de funcionar como un enrutador. Los servidores de autenticación brindan una seguridad de la red y una gestión de recursos centralizadas. Las diferentes plataformas de sistema operativo se basan en diferentes protocolos de compartimiento de ficheros y esquemas de autenticación, pero la mayoría de los vendedores de sistemas operativos ofrecen interoperabilidad con otros sistemas operativos, porque muchas de las redes actuales son heterogéneas.

Obviando el sistema operativo o la plataforma de red, la mayoría de las redes actuales corren sobre protocolos TCP/IP. El TCP/IP es la pila de protocolos más routable y, por tanto, la más apropiada para grandes redes enrutadas. Es indispensable para la conexión a Internet. Este capítulo brinda una panorámica básica sobre el hardware y el software de la interconexión y una explicación de alto nivel sobre cómo se llevan a cabo las comunicaciones TCP/IP. Usted puede consultar muchos libros y sitios Web excelentes para obtener más detalles acerca de cada uno de estos aspectos de la interconexión de computadoras. Algunas buenas referencias están relacionadas en la sección de Fuentes al final de este capítulo.

Preguntas Realizadas con Frecuencia

Las siguientes preguntas realizadas con frecuencia, respondidas por los autores de este libro, están diseñadas para medir su comprensión de los conceptos presentados en este capítulo y para ayudarle con la implementación de estos conceptos en la vida real. Para hacer que el autor conteste a sus preguntas, visite www.syngress.com/solutions y haga clic en el formulario **“Pregúntale al autor”**.

P: ¿Cuál es la diferencia entre direcciones IP públicas y privadas?

R: Las direcciones públicas son visibles para la Internet. Estas deben ser únicas a través de la Internet global. Generalmente son asignadas a los ISP por la IANA (Autoridad de Números Asignados de Internet) y luego asignadas a los clientes por sus ISP. Las direcciones públicas se denominan, a veces, *direcciones routables o trazables*, porque pueden ser encaminadas a través de la Internet. Las direcciones IP privadas no son routables en la Internet; son usadas en redes (internas) privadas y provienen de uno de los rangos de direcciones reservados para el direccionamiento privado. Cualquiera puede utilizar las direcciones privadas, y la dirección de cada computadora necesita ser única solamente dentro de la red privada. Los rangos de direcciones privadas son 10.xxx.xxx.xxx (con una máscara de subred de 255.0.0.0), 172.16.xxx.xxx (con una máscara de subred de 255.255.0.0) y 192.168.xxx.xxx (con una máscara de subred de 255.255.255.0).

Además, las direcciones IP en el rango 169.254.xxx.xxx están reservadas para el uso de servicios APIPA. Para más información, véase el RFC 1597 sobre el direccionamiento privado en www.pku.edu.cn/academic/research/computer-center/tc/html/RFC1597.html.

P: ¿Cómo pueden todas las computadoras de una red local acceder a Internet a través de una sola conexión a Internet?

R: Existen varias formas de que una LAN pueda compartir una conexión a Internet. Si el ISP asigna múltiples direcciones IP públicas, las computadoras pueden estar conectadas a un enrutador, con el enrutador conectándose a Internet a través de una línea de teléfono, cable DSL, ISDN o T-1. Si el ISP adjudica solamente una dirección pública para la conexión, las computadoras pueden estar conectadas a un dispositivo NAT (Traducción de Direcciones de Redes) – ya sea un dispositivo dedicado o una computadora corriendo NAT. Esta máquina NAT se conecta con Internet y las otras computadoras (los clientes NAT) pasan a través de ella para acceder a los recursos de Internet. A las computadoras clientes se les asignan direcciones IP privadas (manualmente, a través de un servidor DHCP en la red o a través del servicio de adjudicación de direcciones IP de NAT). La máquina NAT traduce las direcciones privadas en públicas y mantiene una tabla con la que conserva las trazas de qué solicitud de Internet vino de cuál computadora interna. Los servidores Microsoft incluyen un buen servicio NAT; las computadoras con Windows 98/ME, 2000 y XP Professional incluyen una versión “Light” de NAT llamada Compartimiento de Conexión a Internet (ICS). En el mundo de Linux/UNIX, la traducción de direcciones es referida a menudo como *enmascaramiento IP*. Productos NAT como Vicomsoft e IPNetRouter (de Sustainable Networks) están disponibles para sistemas Macintosh. Para más información sobre NAT, véase el RFC 2663 en www.ietf.org/rfc/rfc2663.txt?number=2663.

P: ¿Cuál es la diferencia entre los protocolos de enlace PPP y SLIP usados para la interconexión por marcación?

R: SLIP fue diseñado exclusivamente para el TCP/IP y no es apropiado si la LAN a la que Usted se está conectando usa una pila de protocolos de red/transporte diferente, como por ejemplo IPX/SPX. Además, SLIP no soporta DHCP, de modo que cuando Usted lo configura, debe introducir una dirección IP estática. Muchos ISP no asignan direcciones estáticas de clientes (a veces referidas como *direcciones “clavadas”*), sino que usan DHCP

para asignar una nueva dirección cada vez que disca. El PPP es un protocolo de enlace más moderno que soluciona estos problemas. Este soporta protocolos no TCP/IP como IPX/SPX y NetBEUI y permite el uso de múltiples protocolos. PPP soporta la negociación automática de direcciones IP, de modo que trabaja con servidores DHCP y también permite el uso de checksums para el chequeo de errores – algo que SLIP no hace. Básicamente, PPP fue diseñado para reemplazar a SLIP, pues es mucho más flexible. Ambos protocolos no son protocolos de interconexión en su totalidad; se usan solamente para establecer un enlace entre líneas telefónicas. Se requiere otro protocolo (como TCP/IP o IPX/SPX) para comunicarse con aplicaciones en la computadora o red remota.

P: ¿Cómo el TCP y el UDP utilizan puertos para distinguir entre múltiples aplicaciones empleando simultáneamente los protocolos?

R: Cada aplicación que utilice TCP o UDP se identifica a sí misma con un número de 16 bit llamado *número de puerto*. La información de encabezado del UDP y el TCP que se añade a los paquetes de datos en la capa de transporte de la computadora remitente (antes de que los paquetes bajen a la capa IP) contiene los números de puerto para ambas computadoras: la computadora fuente y la de destino. Por ende, aún si hay docenas de aplicaciones corriendo a la vez que usan el protocolo TCP o UDP, los paquetes correctos son entregados a cada aplicación basándose en el número de puerto de destino, y las respuestas regresan utilizando el número de puerto de la computadora fuente que aparece en el paquete recibido (que se convertirá en el número de puerto de destino en el mensaje de respuesta).

P: ¿Dónde puedo encontrar una lista completa de los famosos puertos TCP y UDP?

R: La IANA (Autoridad de Números Asignados de Internet) mantiene listas de todos los tipos de números utilizados en Internet, incluyendo la lista de números de puertos famosos. Para esta información, véase www.iana.org/assignments/port-numbers.

P: Si la versión actual del Protocolo de Internet es la 4, ¿por qué la “nueva generación” se denomina IPv6? ¿Por qué nos saltamos el IPv5?

R: Un protocolo stream experimental de tiempo real llamado *ST* o *Protocolo Stream de Internet* usaba la versión número 5 en el encabezado IP de sus paquetes. ST fue diseñado como un protocolo orientado a la conexión que opera en el nivel de red al igual que el IP no orientado a la conexión. El ST nunca fue concebido para reemplazar al IP, sino para operar en calidad de complemento como parte de la familia IP para la transmisión de audio, video, etc. usando tecnología streaming. Como la identificación v5 ya fue empleada, se le asignó a la nueva versión del IP la designación IPv6. (Para más información sobre el ST, véase el RFC 1819 en [ftp://ftp.isi.edu/in-notes/rfc1819.txt](http://ftp.isi.edu/in-notes/rfc1819.txt)).

P: ¿Cuáles son algunas de las herramientas de rastreo que se pueden usar para capturar y analizar paquetes en redes UNIX?

R: Algunas de las herramientas comunes de rastreo para UNIX incluyen Ethereal (que mencionamos anteriormente, en versiones para UNIX y Windows), tcdump (incluida en los

sistemas operativos BSD), ipgrab (disponible en <http://home.xnet.com/~catchmike/MSB/Software>), tcpflow (captura solamente, pero almacena datos en un formato conveniente para el análisis de protocolo; se encuentra disponible sin costo alguno en la Web en www.circlemud.org/~jelson/software/tcpflow). También existen programas rastreadores para versiones de UNIX específicas, como Snoop para Solaris, Etherfind para Sun Osm y nettle/ntfmt para HP-UX.

Referencias

- Bell Labs: *Ventajas de las Señales Digitales*
www.bell-labs.com/technology/digital/advantages.html
- *Fundamentos de las Telecomunicaciones: Transmisión Digital y Análoga*
www.privateline.com/manual/three.html
- Explicación sobre la multiplexación
<http://williams.comp.ncat.edu/Networks/multiplexing.htm>
- Explicación sobre la multiplexación por división de frecuencia
www.cs.williams.edu/~cs105/f01/text/ch3/DigitalTrans_13.html
- Explicación sobre la multiplexación por división de tiempo
www.cs.williams.edu/~105/f01/text/ch3/DigitalTrans_9.html
- Clase sobre DWDM del Consorcio Internacional de Ingenieros
www.iec.org/online/tutorials/dwdn
- Bell Labs: *¿Qué importancia tiene la multiplexación para las comunicaciones?*
www.bell-labs.com/technology/multiplex
- Sesión del Comité para la Seguridad Nacional sobre el EMP
http://commdocs.house.gov/committees/security/has197010.000/has197010_1.HTM
- Prensa Asociada: *Expertos nombran pulso electromagnético ataque terrorista*
www.globalsecurity.org/org/news/2001/011001-attack03.htm
- *El pulso electromagnético*
<http://home.swbell.net/kkmartin/emp.htm>
- *Clase sobre redes*
<http://punch.engr.wisc.edu/~orchard/net-tutorial>
- Mundo de la interconexión
www.helmig.com

- Manual de redes
www2.edc.org/cope/networkprimer
- Windows 2000 Server
www.microsoft.com/windows2000/server/default.asp
- Novell NetWare Server
www.novell.com
- Macintosh OS X Server
www.apple.com/macosx/server
- Sistemas operativos UNIX
www.cs.arizona.edu/people/bridges/os/unix.html
- Sistemas operativos Linux
www.linux.org
- Servicios de Windows para UNIX
www.ehsco.com/reading/20000807ncr1.html
- Sitio Web MacWindows para Soluciones de Integración Windows-Macintosh
www.macwindows.com
- *Introducción a los protocolos de Internet*
<http://oac3.hsc.uth.tmc.edu/staff/snewton/tcp-tutorial>
- *Clase sobre enrutamiento TCP/IP y IPX*
www.sangoma.com/fguide.htm
- *Lista de recursos del TCP/IP*
www.private.org.il/tcpip_rl.html

Comprendiendo las Intrusiones y los Ataques a Redes

Tópicos que investigaremos en este capítulo:

- Comprendiendo las intrusiones y los ataques a redes
- Reconociendo las actividades preataque
- Comprendiendo el crackeo de contraseñas
- Comprendiendo las explotaciones técnicas
- Atacando con troyanos, virus y gusanos
- Hackeando para no especialistas en tecnologías
- Desplegando un equipo de respuesta a incidentes

- ✓ Resumen
- ✓ Preguntas Realizadas con Frecuencia
- ✓ Referencias

Introducción

Como analizamos en capítulos anteriores, existen muchos tipos diferentes de crímenes cibernéticos, cometidos por todas las clases de criminales cibernéticos – algunos de ellos con muy pocos conocimientos técnicos o aptitudes. Sin embargo, gracias a los medios de difusión masiva y a algunos filmes populares, la mayoría de las personas asocia el término *crimen cibernético* con un tipo específico de delito: hackear un sistema o una red desde el exterior de una organización. Incluidos en esta poco amplia definición están los ataques maliciosos diseñados para colapsar computadoras y congestionar redes, aún cuando no tiene lugar una “entrada ilegal” real. De cualquier forma, se presume que el criminal tenga un elevado nivel de conocimientos sobre computadoras y redes.

A diferencia del estafador cibernético que necesita conocer sobre computadoras sólo lo suficiente para enviar correos electrónicos masivos, o del pornógrafo infantil cuyos conocimientos técnicos están limitados a cargar o descargar ficheros, el intruso o atacante de redes ha podido contar, tradicionalmente, con un número determinado de aptitudes. Evadir las medidas de seguridad y colarse por los huecos que los programadores dejan en aplicaciones y sistemas operativos con el fin de acceder al servidor de otra persona requiere de conocimientos (y a veces de talento). Es necesaria una vasta comprensión sobre cómo funcionan los protocolos de redes para explotar sus características y derrumbar sistemas o redes enteras. O al menos una vez fue así.

Los hackers dedicados invierten cientos o incluso miles de horas perfeccionando técnicas de intrusión y ataques. Hoy día, sin embargo, muchos hackers que entran o derrumban redes no son verdaderos hackers – al menos, en el sentido original de la palabra (la cual se refería a los “prodigios en computación”, cuyo dominio de la tecnología era la clave de su habilidad para penetrar y crackear sistemas). Eso es porque los “verdaderos” hackers, generosamente, han puesto a disposición de los demás los frutos de sus conocimientos y de su labor en forma de guiones y programas ejecutables que hacen todo el trabajo. Los “script kiddies” que los usan quizás sean tratados despectivamente como “aspirantes a hackers” por aquellos con conocimientos técnicos, pero las herramientas de hackeo continúan proliferando, compartiéndose libremente a través de los grupos de noticias “warez” y sitios Web, facilitando así las intrusiones y los ataques. Ya el que podría ser un intruso o atacante no tiene que aburrirse aprendiéndose los aspectos técnicos de las vulnerabilidades de Windows o de las fallas de seguridad del TCP/IP. Ahora cualquiera, sin entrenamiento alguno, consigue colarse en una red de la competencia o lanzar un ataque masivo de denegación de servicio contra una compañía cuyas políticas no le agradan.

Resulta importante para los investigadores de crímenes cibernéticos que llevan casos por acceso no autorizado o ruptura de la integridad de una red comprender los principios básicos del funcionamiento de las técnicas de intrusión y de los ataques a sistemas, aunque los intrusos y los atacantes no necesiten necesariamente comprender los aspectos técnicos de lo que están haciendo. Después de todo, el investigador podría ser requerido a testificar en la corte sobre un tema importante que debe ser establecido en cada caso penal: si existe la causa probable para efectuar el arresto. Podría resultar difícil convencer a un jurado de

que Usted tenía evidencia suficiente para creer que el acusado cometió un crimen si Usted no puede explicar con exactitud *cuál* es el crimen y *cómo* se cometió exactamente.

En este capítulo, ofrecemos panorámicas sobre los aspectos técnicos de varios tipos de intrusiones y ataques. Comenzamos con un análisis de las actividades preparatorias de un intruso que podrían preceder a un ataque:

- Escaneo de puertos abiertos en la red objetivo
- Ocultar la dirección IP del atacante y otra información identificativa
- Colocar programas de software o dispositivos de hardware (tales como programas troyanos o monitores por pulsación) para obtener datos preliminares que ayudarán al atacante a efectuar el ataque

Seguidamente le echaremos un vistazo a cómo los intrusos crackean contraseñas para obtener acceso a sistemas y redes. Aprenderá acerca de los ataques de crackeo mediante fuerza bruta, de cómo las contraseñas almacenadas en un sistema pueden ser descubiertas y explotadas y cómo los hackers utilizan la ingeniería social para engañar a los usuarios autorizados y hacer que revelen sus contraseñas.

Posteriormente analizaremos los muchos tipos de explotaciones técnicas que los hackers emplean para acceder o atacar computadoras interconectadas, incluyendo las explotaciones de aplicaciones, sistemas operativos y protocolos. También abordaremos los fenómenos “script kiddie” y “clic kiddie” y le mostraremos cómo personas con casi ninguna pericia técnica pueden usar herramientas fáciles de conseguir para iniciar con un salto sus carreras de hackers. Finalmente, analizaremos cómo las compañías crean equipos de respuesta a incidentes para lidiar con esas intrusiones y esos ataques cuando ocurren, y cómo el equipo de respuesta interna puede colaborar con la policía para aumentar la probabilidad de que el intruso o atacante sea rastreado y exitosamente procesado.

Nota

Algunos de los ataques y las explotaciones analizadas en este capítulo podrían ser consideradas “obsoletas” por algunos. Sin embargo, eso es real sólo si asumimos que todos los sistemas están corriendo las versiones más recientes de los softwares y que se han aplicado todos los parches de seguridad. Desafortunadamente, este no es el caso. En un mundo donde un número sustancial de computadoras gubernamentales y comerciales aún corren MS-DOS y Windows 3.x, sería ingenuo asumir que las vulnerabilidades de los sistemas operativos y las aplicaciones más antiguos ya no son relevantes.

Comprendiendo las Intrusiones y los Ataques a Redes

Las intrusiones y los ataques a redes vienen en muchas formas y de todas las direcciones. Aunque las amenazas externas (generalmente a través de Internet) atraen la mayor atención,

los ataques y las intrusiones pueden – y a menudo es así – provenir de empleados, contratistas y otros del lugar o de dentro de una red local. Recuerde que sólo porque alguien esté autorizado a acceder a una red no significa que él o ella tenga autorización para acceder a *todos* sus recursos.

No podemos continuar asumiendo que los atacantes son particularmente expertos en computadoras. En un tiempo, un atacante tenía que tener un nivel mínimo de aptitudes para lanzar un ataque, pero hoy día las herramientas que son muy fáciles de conseguir automatizan completamente el proceso de ataque. En realidad, un ataque puede provenir de casi cualquiera que tenga la motivación y el deseo de hacerlo.

Luchadores contra el crimen....

Considerando las Amenazas Internas

Todos los crímenes cibernéticos, en sus muchas definiciones, comprenden el uso de una red para acceder a sistemas. Sin embargo, cuando los investigadores se enfrentan al robo o la destrucción de datos o a ataques que colapsan servidores, no se debería descontar la posibilidad de un “trabajo interno”. No todos los ataques o entradas no autorizadas a sistemas provienen de Internet, también pueden provenir de cualquier lugar de la LAN o de un acceso físico a las máquinas afectadas.

Algunas intrusiones y algunos “ataques” pueden incluso no ser intencionales. Usuarios con sólo los conocimientos técnicos suficientes para ser peligrosos podrían experimentar y cambiar configuraciones y hacer colapsar el sistema o la red. Personas curiosas podrían tropezarse con recursos inseguros a los que no deberían tener acceso, y empleados, tratando de hacer las cosas más cómodas para ellos (por ejemplo, instalar puntos de acceso inalámbricos de modo que tengan conexión a la red cuando llevan sus Laptops hacia la sala de conferencias para reuniones), pueden abrir huecos de seguridad inconscientemente.

En las siguientes secciones examinaremos la diferencia entre una intrusión y un ataque; analizaremos varios tipos de ataques, incluyendo los accidentales y daremos algunas pautas para prevenir las rupturas intencionales de la seguridad interna.

Intrusiones vs. Ataques

Resulta importante para los investigadores comprender la diferencia entre una intrusión y un ataque porque de cualquier forma hubo una entrada no autorizada a la red o al sistema y esto puede constituir un factor importante al probar los elementos de un delito criminal. Se pueden cometer ataques sin entrar a la red o al sistema, como en el caso de los ataques DoS. Estos ataques sobrecargan los recursos de la red y provocan que esta no esté disponible para los usuarios legítimos, pero el atacante nunca accede a ninguna computadora dentro de ella.

Si los investigadores y jueces no comprenden esta diferencia (lo que sólo pueden lograr comprendiendo los aspectos técnicos del funcionamiento de los ataques), podrían presentar cargos que serían desestimados en la corte o cargos errados contra un criminal cibernético. Esto sería similar a una situación en la cual nadie del equipo de policías comprendiese la

diferencia entre los delitos de robo a mano armada y robo. El primero requiere que tenga lugar un asalto físico o una amenaza de perjuicio corporal serio durante la comisión o el intento de comisión de un robo. El segundo requiere que el delincuente entre ilegalmente al local de otra persona para cometer un robo. Si los oficiales de la policía arrestan a un sospechoso por entrar a una casa y robar un televisor mientras los residentes salieron y presentan cargos contra él por robo a mano armada (y si el fiscal lleva un caso como este a juicio), el sospechoso seguramente será encontrado inocente, porque el estado no tiene prueba de los elementos del delito de robo a mano armada. Esta situación nunca sucedería porque los oficiales de la policía están entrenados en las diferencias técnicas de ambos casos desde el tiempo en que iban a la academia de policías, y todos los fiscales son muy versados en estas diferencias. Sin embargo, es completamente posible imaginar que se presenten cargos errados en un caso de crimen por ordenador, sencillamente porque ninguno de los involucrados comprende los aspectos técnicos de estos tipos de crímenes.

Reseña sobre la Ley Cibernética....

Reseña sobre la Ley Cibernética: Analizando la Ley

Como un ejemplo de cuán importante resulta comprender los elementos del delito, que varían de acuerdo con los estatutos y las jurisdicciones, la sección 33.02 del Código Penal de Texas define la “Ruptura de la Seguridad de una Computadora” como lo siguiente:

Una persona comete un delito si la persona accede conscientemente a una computadora, red de computadoras o sistema computarizado sin el consentimiento efectivo del propietario.

A primera vista, parecería que este delito no aplica a ataques en los que no hay entrada a la red. El estatuto demanda el “acceso” como un elemento del delito, y una definición estándar de la palabra en el diccionario es “un medio de entrada”. Sin embargo, para comprender lo que pretendía la legislatura cuando aprobó este estatuto, regresemos a las definiciones *legales* que aplican a este capítulo del Código Penal en particular, contenidas en la sección 33.01. Allí, el término “acceso” se define como:

Acercarse, instruir, comunicarse con, almacenar datos en, recuperar o interceptar datos de, alterar datos o softwares en, o *hacer uso de cualquier recurso de una computadora, red de computadoras, programa o sistema computarizado.*

Como puede ver, esta definición es más abarcadora. La clave para presentar cargos contra un atacante DoS es la frase en *italica*. Debido a que el ancho de banda de una red es un recurso de una red de computadoras, y debido a que el atacante en realidad sí hace uso de ese recurso, este podría ser acusado en virtud de la sección 33.02.

Es muy importante para los oficiales del orden analizar cuidadosamente los estatutos en virtud de los cuales ellos intentan presentar cargos y, si tienen dudas, consultar al fiscal del distrito o al Ministro de Justicia para clarificar el lenguaje de los estatutos.

Por ende, resulta importante ser precisos cuando nos referimos a crímenes por ordenador específicos. Los atacantes DoS no deben ser referidos como *intrusos* cuando no ocurre ninguna intrusión. Asimismo, no todos los intrusos pueden clasificarse precisamente como *atacantes* – aunque aquellos que acceden y destruyen datos o plantan virus son apropiadamente llamados por ambos nombres.

Reconociendo los Ataques Directos de los Distribuidos

Existen dos maneras diferentes en las que los atacantes pueden lanzar sus ataques contra un sistema o una red. Un *ataque directo* es lanzado desde una computadora usada por el atacante (a menudo después de una intrusión previa; se emplean herramientas de ataque como escáners de puertos para encontrar víctimas potenciales).

Un *ataque distribuido* es más complejo. Los ataques distribuidos usan el o los sistemas de otra persona, no el del atacante, para realizar las tareas que directamente lanzan el ataque. En este tipo de ataque existen múltiples víctimas que incluyen no sólo al blanco del ataque sino a sistemas remotos intermediarios desde los cuales el ataque es lanzado y que son controlados por el atacante. Nos referimos a los intermediarios como *agentes o zombies*. Este tipo de ataque, por supuesto, torna más difícil el rastreo del perpetrador porque los paquetes de ataque que llegan a la víctima tienen múltiples direcciones fuente y ninguna de ellas es la dirección del causante del ataque. Los comandos del atacante para el intermediario, a menudo, están encriptados para dificultar aún más el rastreo. Las transmisiones encriptadas no pueden ser leídas por un rastreador de paquetes (un analizador de protocolo).

Un ataque distribuido funciona un poco como la broma práctica en la que el bromista llama a numerosas pizzerías simulando ser un cliente y pide que las pizzas sean entregadas en la dirección de otra persona. La víctima primaria es el residente de la dirección objetivo quien termina con una gran cantidad de pizzas no deseadas, pero los vendedores de pizzas también son víctimas, porque sus recursos son utilizados sin su previo conocimiento o consentimiento para llevar a cabo el ataque.

Nota

Para comprender mejor el concepto de DoS, los tecnicismos de los que hablaremos más adelante en este capítulo, llevemos el escenario de la broma de las pizzas descrito en esta sección un paso más allá. Si nuestro atacante está realmente determinado, podría llamar no sólo a vendedores de pizzas, sino también a todos los restaurantes chinos, floristas y otros negocios de “hacemos entregas” en el área, coordinando los pedidos de modo que todos los mensajeros converjan sobre la víctima al mismo tiempo. Si hay muchas furgonetas de entrega parqueadas en la misma calle de modo que los familiares de la víctima no pueden entrar, esto traería como resultado una *denegación de servicio* para los usuarios legítimos de la entrada.

Los atacantes que usan el método distribuido pueden lanzar sus ataques simultáneamente desde docenas, cientos o incluso miles de máquinas conectadas a Internet en todo el mundo. Esto significa que de esta forma se puede generar mucho más tráfico del que es posible generar con ataques estándar de una fuente. De acuerdo con el Taller sobre Herramientas de Intrusos en Sistemas Distribuidos, CERT, el atacante tiene un modelo típico de ataque distribuido usando computadoras UNIX, que controla varios sistemas llamados *masters*. Cada master controla un gran número de agentes corriendo *daemons* - el software que se usa para lanzar el ataque. Los daemons se instalan en las máquinas agentes explotando el sistema operativo o las vulnerabilidades de protocolo. Todo este proceso se puede automatizar de modo que se descubran y penetren agentes potenciales, se instale el daemon en todos ellos, y se tomen medidas para ocultar el hecho que ocurrió una intrusión, usando guiones por lotes. (Analizaremos más detalladamente la automatización del ataque en la próxima sección).

En la Tabla 6.1 se esboza el proceso de ataque distribuido (después de la instalación de los daemons).

Tabla 6.1 El proceso de ataque distribuido

Paso	Componente	Acción
1	Daemon (o agente)	Se anuncia a sí mismo ante los “masters” que han sido predefinidos
2	Master	Hace figurar al daemon como “listo y dispuesto” para ser usado para el ataque
3	Atacante	Da los comandos a los masters para lanzar el ataque
4	Master	Da los comandos a los daemons en los agentes para lanzar el ataque (con parámetros específicos como la identidad del objetivo y la duración del ataque)
5	Daemon	Lanza el ataque sobre la víctima especificada

Debido a que los componentes de este modelo están organizados en forma de pirámide, con un atacante controlando a varios masters que a su vez controlan a numerosos agentes/daemons, es más fácil inhabilitar el sistema de ataque más cerca del extremo superior, donde hay menor cantidad de sistemas con los que lidiar. Si los masters son inhabilitados, los agentes y su software daemon no podrán funcionar. Por supuesto, la técnica de inhabilitación más efectiva es encontrar al atacante, inhabilitando toda la secuencia del ataque.

Ataques Automatizados

Un *ataque automatizado* es uno realizado por un programa computarizado en lugar de que el atacante realice manualmente los pasos de la secuencia de ataque. Por algún tiempo, los

hackers han distribuido las herramientas de ataque que facilitan el lanzamiento de ataques a redes. Sin embargo, antes del 2000, la mayoría de estas herramientas iniciarían sólo una secuencia de ataque; el lanzamiento de las secuencias de ataque adicionales requerían de la intervención del atacante humano. Sin embargo, herramientas más recientes como Nimda y Code Red son capaces de iniciar continuamente, por sí mismas, nuevos ciclos de ataque. Este creciente nivel de automatización hace que estos ataques sean más peligrosos y más generalizados. De acuerdo con CERT, la creciente automatización y sofisticación de las herramientas de ataque es una de las tendencias más significativas dentro de la comunidad de hackers “Black Hat”.

Las actuales herramientas de ataque pueden realizar todo el proceso de ataque. En lugar de que el hacker tenga que realizar el escaneo de puertos con una herramienta para identificar los sistemas vulnerables, después usar una herramienta diferente para penetrar la red de la víctima y después otra herramienta para propagar el ataque, ahora una herramienta puede hacerlo todo. Esto acelera el proceso, así como se lo facilita a los hackers que carecen de conocimientos técnicos para montar un ataque exitoso. Algunas herramientas de ataque son ejecutadas en la línea de comandos, pero muchas de ellas tienen interfaces gráficas fáciles para el usuario, así como detallados ficheros de ayuda para instruir a los atacantes en su uso. Quizás también existan ficheros de configuración que le permitan a los usuarios personalizar el ataque.

En aras de evitar la detección por softwares IDS que se basan en el reconocimiento de patrones, las herramientas modernas pueden emplear diferentes técnicas – como la selección aleatoria – para interrumpir patrones que dispararían la detección por el IDS. Además, muchas de las herramientas usan protocolos comunes como HTTP e IRC (Internet Relay Chat) que disfrazan sus paquetes haciendo que luzcan como tráfico normal de Internet. Estas herramientas se encuentran ampliamente disponibles a través de sitios FTP anónimos y grupos de noticias de hackers en Internet. Los hackers también pueden modificar herramientas legítimas de análisis de redes si tienen el código fuente, convirtiéndolas en herramientas de ataque al adicionarles el código para explotar las vulnerabilidades que ellos encuentran.

Nota

Resulta irónico que los hackers pongan a disposición de otros sus herramientas de ataque en sitios FTP anónimos, pues los sitios FTP y TFTP anónimos son, a menudo, explotados por atacantes. Hackers con conocimientos pueden crear fácilmente herramientas y guiones que intenten una validación anónima; prueban varios comandos como **pwd**, **mkdir** y **rmdir** (para imprimir el directorio de trabajo, hacer un directorio y borrar un directorio en los sistemas UNIX/Linux, respectivamente) y plantan un troyano en el sitio FTP que luego le posibilite al hacker acceder al sistema desde un puesto remoto sin una contraseña.

“Ataques” Accidentales

Algunas intrusiones y algunos “ataques” podrían realmente no ser intencionales. Los colapsos de servidores o redes pueden ser causados por usuarios experimentando, visitando sitios Web que corren códigos maliciosos o descargando inconscientemente e introduciendo un virus en el sistema. De hecho, un gran número de ataques de virus son iniciados accidental o inconscientemente. El mismo usuario que parece haber enviado el virus a través del correo electrónico es, a menudo, una víctima del ataque, porque muchos virus y gusanos están escritos para propagarse accediendo a la libreta de direcciones de la víctima y enviando correos infectados a todas las direcciones allí encontradas.

Los ataques accidentales pueden ser tan destructivos como los deliberados y el personal de seguridad de la red tiene que estar igual de vigilante para protegerse de ellos. Sin embargo, desde la perspectiva de la policía, la *intención* del perpetrador importa mucho. La mayoría de los delitos criminales requieren que un acto sea cometido intencionalmente o al menos conscientemente, de modo que los elementos del delito podrían no estar presentes si un empleado causa una intrusión o un ataque sin intención – aún si sus actos fueron descuidados. Por otra parte, algunos actos aún se consideran criminales si está presente un estado menor de culpabilidad (imprudencia o negligencia). Es muy importante para los investigadores estar conscientes del estado mental culpable que se especifica como un elemento de cada delito para llevar a cabo una acusación. Si no se especifica el nivel de culpabilidad, el código penal generalmente define un nivel de culpabilidad “por defecto” que aplica.

Previendo las Rupturas Intencionales de la Seguridad Interna

Los usuarios, dentro de la red, están en la mejor posición para acceder a informaciones o sabotear la integridad de la red. De acuerdo con la mayoría de los estudios sobre seguridad informática, como se documenta en el RFC 2196, las pérdidas reales (en términos monetarios, de productividad, reputación y otros daños tangibles e intangibles) son mayores en el caso de las rupturas de seguridad internas que en aquellas que proceden del exterior. Los atacantes internos son más peligrosos por varias razones:

- Las personas, dentro de la red, generalmente conocen más sobre la compañía, la red, la distribución del o de los edificios, los procedimientos operativos normales y otras informaciones que les facilitan acceder a ella sin ser detectados.
- Los atacantes internos generalmente tienen, al menos, algún grado de acceso legítimo y les podría resultar fácil descubrir contraseñas y huecos en el sistema de seguridad que se está utilizando.
- Los hackers internos saben qué información está en la red y qué acciones causarían el daño mayor.

Prevenir tales problemas comienza con los mismos métodos empleados para prevenir compromisos de seguridad no intencionales, pero va un paso más allá. En gran parte, las

rupturas no intencionales se pueden prevenir mediante la educación. Obviamente, esto no tendrá el mismo efecto sobre usuarios de la red que intentan quebrar la seguridad. El mejor modo de prevenir tales rupturas depende, en parte, de las motivaciones del o los empleados en cuestión.

La implementación de auditorias ayuda a detectar rupturas internas de la seguridad al registrar eventos de seguridad específicos. Los administradores pueden, de esta forma, rastrear si hubo algún acceso a objetos como ficheros o carpetas, la cuenta de usuario usada para ello, si los usuarios ejercen los derechos de usuario y si entran o salen de la computadora o red. Los modernos sistemas operativos de redes incluyen la función de auditoria. En el Capítulo 8 “Implementando la Seguridad del Sistema” se analizan los métodos para auditar eventos de seguridad. La interpretación y el uso de ficheros de trazas de auditoria de seguridad se analizan en el Capítulo 9 “Implementando las Técnicas de Detección del Crimen Cibernético”.

Los muros de fuego son útiles para evitar que los empleados básicamente dóciles visiten accidentalmente (o conscientes de las consideraciones de seguridad) sitios Web peligrosos o envíen tipos específicos de paquetes fuera de la red local. Sin embargo, los muros de fuego tienen un uso más limitado en prevenir rupturas intencionales de la seguridad interna. Limitar sencillamente el acceso de los usuarios a la red externa no puede detener a los de adentro que están determinados a destruir, modificar o copiar datos. Como tienen acceso físico, pueden copiar datos en medios desmontables o en una computadora portátil (incluyendo máquinas de bolsillo minúsculas) o quizás incluso, imprimirlos en papel y borrarlos del lugar. Ellos pueden cambiar el formato de los datos para disfrazarlos o, más aún, pueden emplear la esteganografía para ocultarlos dentro de ficheros aparentemente inocentes y después cargar los ficheros en los servicios de almacenamiento de datos con base en la Web.

En un entorno de alta seguridad, se deben tomar medidas para evitar este tipo de robo. Por ejemplo:

- Instalar computadoras sin torres de discos flexibles – o incluso estaciones de trabajo sin ninguna unidad de disco.
- Aplicar un sistema o una política de grupo que le impida a los usuarios instalar softwares (como el requerido para que una computadora de mesa pueda comunicarse con una computadora de bolsillo o con un dispositivo Palm OS).
- Cerrar el chasis de la máquina y cubrir el acceso físico a los puertos series, puertos USB y otros puntos de conexión, de modo que no puedan conectar dispositivos desmontables.

La ruptura intencional de la seguridad interna constituye un problema serio y las políticas de la compañía deberían tratarlo como tal. Analizaremos este tópico con más profundidad en el Capítulo 7 “Comprendiendo la Prevención del Crimen Cibernético” en la sección sobre el diseño y la implementación de políticas de seguridad.

Previnando Intrusiones Externas No Autorizadas

Las intrusiones y los ataques externos son la preocupación más importante de muchas compañías cuando se trata de cuestiones de seguridad de redes. En una serie de casos de alto perfil en los años recientes, los servidores Web de organizaciones prominentes como Yahoo! y Microsoft han sido hackeadas. Intentos de penetrar redes gubernamentales sensibles, tales como los sistemas del Pentágono, ocurren regularmente. Los ataques distribuidos de denegación de servicio (DDoS) se roban las primeras páginas de los diarios cuando hacen colapsar a servidores e impiden que los usuarios de Internet accedan a sitios populares.

La buena noticia acerca de las intrusiones externas es que el o las áreas a controlar están más concentradas que en el caso de los ataques internos. Generalmente existe sólo un número limitado de puntos de entrada a la red desde el exterior. Ahí es donde un muro de fuego apropiadamente configurado puede resultar invaluable, permitiendo el tráfico autorizado a la red mientras deniega el no autorizado. Por otra parte, la popularidad de los muros de fuego asegura que los hackers dedicados saben cómo estos funcionan y dedican una gran cantidad de tiempo y esfuerzo a encontrar formas de vencerlos.

Nota

Los factores psicológicos influyen en las formas en las que las compañías manejan varios tipos de rupturas de seguridad. Generalmente, las rupturas internas son vistas por las compañías como problemas con el personal y son manejadas desde el punto de vista administrativo. Las externas quizás se parezcan más a violaciones y se procesan más frecuentemente como actos criminales. Debido a que el intruso externo puede provenir de cualquier lugar, en cualquier momento, el sentido de inseguridad y temor a lo desconocido puede ocasionar que las organizaciones reaccionen de un modo más fuerte ante este tipo de amenaza. Por ende, existe más probabilidad de que involucren a los oficiales de la policía cuando la ruptura es externa. Los oficiales podrían entonces concluir (erróneamente) que la proporción de rupturas externas con respecto a las internas es mayor de que lo es en realidad.

Planificándose para Fallos del Muro de Fuego

Las organizaciones no deberían depender nunca de un muro de fuego para proporcionar una protección del 100%, aún contra intrusos externos. Para ser efectivo, un plan de seguridad debe ser multifacético y multicapas. Aunque los administradores pueden esperar que un muro de fuego mantenga a los intrusos completamente alejados de la red, su plan debe tener en consideración la posibilidad de que el muro de fuego puede fallar, y deben abordar cuestiones como:

- Si los intrusos *logran* entrar, ¿cuál es el plan de contingencia?
- ¿Cómo pueden ellos reducir el monto del daño que pueden causar los atacantes?
- ¿Cómo se pueden proteger los datos más sensibles o valiosos?

Intrusos Externos con Acceso Interno

Un tipo especial de intruso externo es el de afuera que entra *físicamente* con Sus facilidades para acceder a Su red. Aunque no es un verdadero interno porque él o ella no está autorizado a estar allí y no tiene una cuenta válida en la red, este intruso disfruta muchas de las mismas ventajas del verdadero interno.

En la escena....

Planificación Táctica

Al tratar con intrusos en la red, los administradores de redes deberían practicar lo que los oficiales de la policía en sus entrenamientos de tácticas defensivas denominan *pensamiento de si/entonces*. Esta estrategia se trata de considerar todas las salidas posibles de una situación dada y entonces plantear la pregunta: “Si esto sucede, *entonces* ¿qué se podría hacer para protegernos de las consecuencias?”. Las respuestas a estas preguntas deberían conformar la base de la política de seguridad de la organización.

Esta táctica requiere que los administradores sean capaces de planear respuestas en detalles, lo que significa pensar de forma específica en lugar de general. La evaluación de la amenaza a la seguridad debe basarse, en parte, en la comprensión de las motivaciones de las personas que inician el ataque y en parte, en los aspectos técnicos del tipo de ataque que es iniciado. En un entorno de alta seguridad, estas tareas deberían ser responsabilidad de un *equipo de respuesta a incidentes*. Analizaremos más adelante en este capítulo la distribución de tales equipos.

Reconociendo el “Hecho del Ataque”

Si no funcionan las medidas preventivas (y es probable que a veces no lo hagan), el próximo paso para los administradores de redes es cambiar a modo reactivo y tratar de minimizar el daño. Antes de que puedan hacerlo, tienen que tener una forma de reconocer que está teniendo lugar un ataque.

Los sistemas de detección de intrusiones (IDS) utilizan dos métodos para identificar que está ocurriendo un ataque:

- **Reconocimiento de patrones** Analizando ficheros, el tráfico de la red, secuencias en RAM, u otros datos en busca de señales de ataque repetidas o reconocibles, tales como incrementos inexplicables del tamaño del fichero o cadenas particulares de caracteres.
- **Reconocimiento del efecto** Identificando los resultados de un ataque, tales como un colapso del sistema causado por una sobrecarga o un reinicio repentino sin razón.

Resulta fácil programar un IDS para reconocer patrones específicos, pero los atacantes pueden vencerlo haciéndoles pequeños cambios a los patrones o fragmentando los paquetes de ataque – o sea, dividiendo los mensajes de ataque o códigos en paquetes fragmentados. Un número de explotaciones TCP/IP usa paquetes fragmentados. Estas explotaciones se denominan *ataques frag*. El reconocimiento del efecto es más difícil porque los “efectos” a

menudo se asemejan al tráfico normal de la red o a problemas causados por fallas en el hardware o software.

El problema con los IDS – en realidad, con todos los softwares – es que hace exactamente sólo lo que se le diga que haga. Hasta ahora, la verdadera inteligencia artificial (programas que puedan “pensar”) no ha sido alcanzada. Los oficiales de la policía saben que el factor humano – la intuición y la habilidad de hacer deducciones lógicas – puede ser muy importante a la hora de detectar y solucionar crímenes. Desafortunadamente, ningún dispositivo o programa puede observar el comportamiento de los sistemas de computadoras y los componentes de las redes y reconocer intuitivamente que algo malo está sucediendo. Esto explica por qué los administradores humanos serán siempre un ingrediente importante al crear una postura de seguridad apropiada en cualquier organización y por qué la eterna vigilancia es más que sólo un lema para las personas con responsabilidades de seguridad.

Identificando y Clasificando los Tipos de Ataques

El *tipo de ataque* se refiere a *cómo* un intruso consigue entrar a Su computadora o red (si en verdad lo consigue) y *qué hace el atacante* una vez que él o ella consiguió entrar (o sin conseguir entrar). Algunos de los tipos de ataques más comunes incluyen los ataques de ingeniería social, los ataques DoS, el escaneo y el spoofing, los ataques “nucleares” y la diseminación de códigos maliciosos. Si Usted tiene un conocimiento básico de cómo funciona cada tipo de ataque, estará mejor armado para defenderse de ellos.

Nos resulta útil clasificar estas intrusiones y estos ataques diferentes en categorías como las siguientes:

- Actividades previas a la intrusión o al ataque
- Métodos de crackeo de contraseñas
- Explotaciones técnicas (tomando ventajas de las características de las aplicaciones, los sistemas operativos o protocolos)
- Ataques con códigos maliciosos (troyanos, virus, gusanos)

Las siguientes secciones analizan los tipos específicos de ataques que aplican en cada categoría.

Reconociendo las Actividades Previas a la Intrusión o al Ataque

Los documentos sobre cómo hackear a menudo dividen el proceso de hackear/atacar en pasos como sigue:

1. Preataque
2. Acceso inicial
3. Acceso completo al sistema
4. Plantar “puertas traseras” para futuros accesos
5. Cubrir trazas

La fase del preataque se centra en adquirir información. Los hackers experimentados le dicen a los novatos que aprendan de sus futuras víctimas tanto como puedan antes de iniciar un ataque. Esta información “de inteligencia” es de vital importancia para un hacker que tiene una meta concreta como, por ejemplo, el espionaje corporativo.

En la escena....

Planeando el Hackeo y Hackeando el Plan

Los hackers más exitosos planean sus estrategias de ataque casi tan minuciosamente como una unidad militar o un equipo de la policía SWAT planea un golpe o un asalto. Entonces llevan a cabo el hackeo de acuerdo exactamente con el plan. Estos son los verdaderos profesionales y son los más difíciles de aprehender y de quienes nos resulta más difícil defendernos. Los hackers a quienes capturan, por lo general, son descuidados, precipitados o inexpertos. Por el contrario, los hackers amateur “tocan de oído”, entrando en los sistemas y merodeando en busca de algo de interés. El término *amateur* se refiere a alguien que hace algo por entretenimiento, sólo por el gusto de hacerlo. Los hackers profesionales (hackers de alquiler) saben exactamente detrás de qué andan. Entran, lo cogen y salen rápidamente como un maestro del robo. La fase de planear puede durar mucho más que la ejecución real del hackeo. Cuando capturan a hackers profesionales, generalmente, es porque son muy egoístas y alardean de sus logros con las personas erradas.

Conseguir la información antes del ataque y planearlo comprende determinar la meta del hackeo, determinar el blanco del ataque (la red o el sistema que debe ser comprometido para alcanzar la meta) e identificar las debilidades del objetivo que pueden ser explotadas para llevar a cabo el hackeo. Planear el ataque también puede incluir tomar medidas para disfrazar la identidad del atacante o colocar programas preliminares o dispositivos para entrar al sistema llegada la hora de realizar el ataque. Algunas actividades específicas previas al ataque incluyen:

- Escaneo de puertos para identificar objetivos potenciales y sus debilidades
- IP spoofing para disfrazar la identidad del atacante
- Colocar troyanos en el sistema objetivo
- Colocar dispositivos de rastreo y softwares (como registradores de tecleos) en el sistema objetivo
- Colocar analizadores de protocolo (rastreadores) para capturar transmisiones hacia y desde el sistema objetivo

En las siguientes secciones analizaremos más detalladamente estas actividades.

Escaneo de Puertos

Un *puerto* es, en su significado más simple, un punto donde la información entra o sale de una computadora. Los protocolos TCP y UDP usan números de puerto para dar “subdirecciones” individuales con el fin de identificar a qué servicio o aplicación está destinada la información entrante o de dónde se origina la información saliente.

El término *escáner de puerto*, en el contexto de seguridad en la red, se refiere al software que usan los hackers para determinar, desde un puesto remoto, qué puertos TCP/UDP están abiertos en un sistema dado y por ende, son vulnerables para atacar. Los escáners también son empleados por los administradores para detectar vulnerabilidades en sus propios sistemas en aras de corregirlas antes de que un intruso las encuentre. Las herramientas de diagnóstico de redes como la famosa SATAN (Herramienta del Administrador de Seguridad para Analizar Redes), una utilidad de UNIX, incluye opciones sofisticadas de escaneo de puertos.

El escaneo se usa con varios propósitos antes de la penetración y/o el ataque:

- **Enumeración de objetivos** Localizando sistemas anfitriones que están abiertos para atacar
- **Identificación del objetivo** Identificando el sistema objetivo
- **Identificación del servicio** Identificando los servicios o puertos vulnerables en el sistema objetivo

Nota

Una expresión común entre los hackers es “Un buen escáner de puertos vale más que mil contraseñas”.

Un buen programa de escaneo puede localizar una computadora objetivo en Internet (una que sea vulnerable al ataque), determinar qué servicios TCP/IP están corriendo en la máquina y probar esos servicios en busca de vulnerabilidades de seguridad. El Nmap (www.insecure.org/nmap) es un popular escáner de puerto de fuente abierta que se encuentra gratuitamente en la Web. Muchos programas de escaneo se encuentran disponibles sin costo alguno en Internet. Para una buena fuente de información acerca del escaneo y algunas técnicas y softwares populares de escaneo, véase www.garykessler.net/library/is_tools_scan.html.

El *escaneo de puertos* se refiere a un medio de localizar puertos “de escucha” TCP o UDP en una computadora o en un enrutador y obtener la mayor cantidad de información posible acerca del dispositivo a través de los puertos de escucha. Los servicios y las aplicaciones TCP y UDP usan un número de *puertos bien conocidos* (véase “¿Quién está escuchando?”, en la sección En la Escena), que han sido ampliamente publicados. El hacker utiliza sus conocimientos sobre estos puertos comúnmente empleados para extrapolar información.

Por ejemplo, Telnet usa normalmente el puerto 23. Si el hacker encuentra ese puerto abierto y a la escucha, sabe que probablemente esté habilitado Telnet en esa máquina. Entonces puede tratar de infiltrar el sistema, por ejemplo, adivinando la contraseña apropiada en un ataque de fuerza bruta.

En la escena...

¿Quién está escuchando?

Las asignaciones oficiales de puertos bien conocidos están documentadas en el RFC 1700, disponible en la Web en www.freesoft.org/CIE/RFC/1700/index.htm. Estas asignaciones de puertos son hechas por la IANA (Autoridad Asignataria de Números en Internet). En general, un servicio utiliza el mismo número de puerto con UDP que con TCP, aunque existen algunas excepciones. Los puertos asignados fueron, originalmente, aquellos del 0 al 255, pero el número se expandió más tarde hasta el 1023.

Algunos de los puertos bien conocidos empleados más comúnmente incluyen:

- puerto TCP/UDP 20: FTP (datos)
- puerto TCP/UDP 21: FTP (control)
- puerto TCP/UDP 23: Telnet
- puerto TCP/UDP 25: SMTP
- puerto TCP/UDP 53: DNS
- puerto TCP/UDP 67: BOOTP Server
- puerto TCP/UDP 68: BOOTP cliente
- puerto TCP/UDP 69: TFTP
- puerto TCP/UDP 80: HTTP
- puerto TCP/UDP 88: Kerberos
- puerto TCP/UDP 110: POP3
- puerto TCP/UDP 119: NNTP
- puerto TCP/UDP 137: servicio de nombres NetBIOS
- puerto TCP/UDP 138: servicio de datagramas NetBIOS
- puerto TCP/UDP 139: servicio de sesión NetBIOS
- puerto TCP/UDP 194: IRC
- puerto TCP/UDP 220: IMAPv3
- puerto TCP/UDP 389: LDAP

Los puertos 1024-65, 535 se denominan *puertos registrados*. Esos números no están controlados por la IANA y pueden ser usados por procesos y aplicaciones de usuarios. Algunos de ellos son usados tradicionalmente por aplicaciones específicas (por ejemplo, SQL usa el puerto 1433) y podrían ser de interés para los hackers.

A disposición existe un total de 65,535 puertos TCP (y la misma cantidad de puertos UDP) para ser usados para varios servicios y aplicaciones. Si un puerto está abierto, responde cuando otra computadora intenta contactarlo a través de la red. Programas de escaneo de puertos como Nmap se emplean para determinar qué puertos están abiertos en una máquina en particular. El programa manda paquetes para una amplia variedad de protocolos y examinando qué mensajes reciben respuestas y cuáles no, crea un mapa de los puertos de escucha de la computadora.

El escaneo de puertos en sí no daña la red o el sistema, pero le proporciona a los hackers una información que pueden usar para penetrar la red. Debido a que las personas que

realizan escaneos de puertos, a menudo, no son muy buenas, estas con frecuencia falsifican la dirección IP fuente para ocultar su identidad.

El *escaneo a medias* (también llamado *escaneo abierto a medias* o *escaneo FIN*) intenta evitar la detección enviando sólo paquetes iniciales o finales en lugar de establecer una conexión. Un escaneo a medias comienza el proceso SYN/ACK con una computadora objetivo, pero no lo completa. (Véase la descripción de este proceso en la próxima sección sobre explotaciones TCP/IP). Los softwares que realizan escaneos a medias como el Jakal, se denominan *escáners furtivos*. Muchos detectores de escaneo de puertos son incapaces de detectar el escaneo a medias.

Reseña de la Ley Cibernética...

¿Debería Ser Ilegal el Escaneo?

Algunos en la industria de la Informática argumentan que el escaneo de puertos no debería ser ilegal, porque “no hace ningún daño”. Ellos dicen que el escaneo de puertos es similar a tocar el timbre de alguien para ver si hay alguien en casa – no en sí un crimen. Sin embargo, las leyes se promulgan no sólo para proteger a las personas del daño físico real, sino también para proteger su privacidad y sus intereses en su propia propiedad. Aquellos del otro lado de la discusión dicen que el escaneo de puertos realmente se asemeja más al equivalente virtual de alguien que va de puerta en puerta en un edificio de apartamentos probando cuál está cerrado y dónde se puede entrar con facilidad. Aunque esta práctica quizás no haga un daño real si el “escáner de puerta” sólo recopila información y no entra a los lugares, y aunque la persona quizás tenga el derecho de estar en el corredor público, en la mayoría de las jurisdicciones tal comportamiento causaría, como mínimo, incomodidad a los residentes de los apartamentos y atraería la atención de la policía.

En el año 2000, en *Moulton vs. VC3*, una Corte del Distrito de los Estados Unidos en Georgia reglamentó que el escaneo de puertos no daña una red y por ende no constituye un crimen o crea una causa de acción para un juicio civil. Aunque las leyes federales en relación con el fraude y el abuso por ordenador fueron cambiadas por el paso de la Ley de Patriotas de los Estados Unidos en el 2001, aún existe un requerimiento de que deben existir pérdidas o daño para demandar por violación. Para mayor información sobre los principios éticos y la legalidad del escaneo de puertos, véase el artículo en el sitio Web del Instituto SANS: <http://rr.sans.org/audit/ethics.php>. Para ver un documento de opiniones que sostiene que el escaneo no es legal a pesar de la resolución de Moulton, véase el artículo del *Journal of Technology Law and Policy* (*Periódico de la Ley y las Políticas Tecnológicas*) en <http://grove.ufl.edu/~techlaw/vol6/Preston.html>.

Nota

Una buena fuente sobre el escaneo de puertos para administradores de redes es www.doshelp.com/trojanports.htm, que detalla los puertos que deberían bloquearse para una mayor seguridad.

Spoofing de Direcciones

El diccionario define el término *spoof* como una broma de buen gusto, pero la definición del verbo indica una acción menos benigna: “engañar a alguien” (Diccionario *Encarta World Dictionary* de Microsoft del año 2001). Los hackers utilizan direcciones falsas para engañar a otras computadoras y hacerlas pensar que el mensaje se originó desde una máquina diferente. Aunque la falsificación o el spoofing del IP es probablemente el más popular, no es el único método de falsificación empleado por los hackers. Existen otros como el spoofing del ARP, el spoofing de la Web y el spoofing del DNS.

Spoofing o Falsificación del IP

Se trata de cambiar los encabezamientos del paquete de un mensaje para indicar que este procede de una dirección IP diferente a la de la verdadera fuente. En esencia, la computadora remitente se hace pasar por otra máquina, engañando al receptor para que acepte el mensaje. La dirección falsa es, normalmente, un puerto confiable que le permite al hacker recibir, a través de un muro de fuego o enrutador, un mensaje que, de otro modo, hubiese sido filtrado. De estar configurados correctamente, los muros de fuego modernos protegen del spoofing o falsificación del IP.

El spoofing se usa siempre que sea beneficioso para una máquina hacerse pasar por otra. A menudo se usa en combinación con uno de los otros tipos de ataques. Por ejemplo, una dirección falsa se utiliza para ocultar la verdadera dirección IP del atacante en el Ping de la Muerte, Teardrop y otros ataques. Los servicios RPC (Llamada de Procedimiento Remoto), el sistema X Window, los servicios *r* de UNIX (*rlogin*, *rsh*, etc.) y cualquier otro servicio que utilice autenticación de dirección IP son susceptibles al spoofing del IP.

Tras decidir cuál será la víctima, el próximo paso del spoofing es encontrar la dirección de una máquina confiable. Las comunicaciones legítimas entre la máquina confiable y la víctima pueden ser interceptadas y examinadas. A menudo, los hackers usan un ataque DoS contra la máquina confiable para evitar que se comunique en la red. Entonces se pueden modificar los encabezamientos del paquete para simular que los mensajes del atacante proceden de una máquina confiable y los paquetes son enviados a un servicio o puerto que use autenticación de direcciones. Uno de los aspectos más difíciles del spoofing del IP es la necesidad de adivinar correctamente los números de la secuencia de la máquina confiable. Este proceso se ha tornado más fácil para el atacante gracias a las numerosas herramientas de spoofing que están disponibles en la Web.

Spoofing o Falsificación del ARP

El Protocolo de Resolución de Direcciones (ARP) mantiene el *caché ARP*. Esta es una tabla que traza las direcciones IP con las direcciones MAC (físicas) de las computadoras en la red. Este caché es necesario porque la dirección MAC se usa a nivel físico para localizar la computadora destino a la cual debe ser entregado el mensaje. Si no hay entrada de caché para una dirección IP en particular, el ARP envía un mensaje a todas las computadoras en la subred, pidiendo que la máquina con la dirección IP en cuestión responda con su

dirección MAC. Cuando esta responde, es añadida al caché ARP. El *spoofing del ARP*, también denominado *envenenamiento del ARP*, es un método de enviar respuestas falsas que traen como resultado entradas incorrectas en el caché. Esto a su vez trae como consecuencia mensajes subsiguientes enviados a la máquina equivocada (la máquina cuya dirección MAC se enlazó incorrectamente con la dirección IP). Una vez más, este proceso ha sido automatizado por herramientas de hackers tales como ARPoison y Parasite.

Spoofing del DNS

Se refiere a dos métodos de causar que un servidor DNS dirija incorrectamente a los usuarios:

- “Envenenamiento” del caché DNS (similar al envenenamiento del ARP en el que se introduce información incorrecta en el caché) de servidores de resolución de nombres, trayendo como resultado que esos servidores dirijan a los usuarios hacia sitios Web equivocados o que se envíen correos electrónicos a servidores de mensajería equivocados.
- Usar el recurrente mecanismo del DNS para pronosticar el pedido que un servidor DNS le enviará y responder con información falsa. (Para mayor información sobre cómo funciona la recurrencia, véase el artículo *Panorámica del DNS con un Análisis sobre el Spoofing del DNS* en <http://rr.sans.org/DNS/DNS.php>).

En la escena....

¿Qué hace tan peligroso al Spoofing del DNS?

Debido a que el Sistema de Nombres de Dominio (DNS) es responsable de dirigir la resolución de nombres de dominio (tales como www.microsoft.com) en direcciones IP equivalentes (por ejemplo, 206.122.10.6), cualquier reemplazo exitoso de una dirección válida por una diferente provoca que las personas que están tratando de acceder al nombre de dominio visiten la dirección TCP/IP equivocada. Esto le da a los atacantes la posibilidad de crear su propio sitio Web que hacen pasar por un sitio legítimo, e intentar robar toda clase de información interponiéndose entre el usuario y el sitio real. De modo alternativo, los atacantes pueden asumir completamente el papel aparente del sitio real. Debido a que el DNS ayuda a mediar en el acceso a la Web, al FTP, a correos electrónicos y otros servicios, las oportunidades de causar daño inherentes al spoofing del DNS son serias y poderosas.

Cualquiera de estos métodos le permite al atacante interceptar el correo de la víctima o crear páginas Web falsas que le den a los usuarios una información errónea. Este método se puede usar, incluso, para hacer que la víctima proporcione su información personal a través de formularios en la Web. (Véase la sección sobre spoofing de la Web en el análisis acerca de las explotaciones del visualizador más adelante en este capítulo).

Colocación de Troyanos

Los Troyanos o *softwares de caballo troyano* son programas que aparentan ser legítimos o inocentes, pero que realmente hacen más que o en lugar de sus propósitos aparentes.

Analizaremos a los Troyanos de manera general más adelante en el capítulo, en la sección “Atacando con Troyanos, virus y gusanos”. Como parte de la fase de preataque, un hacker puede plantar en la computadora de la víctima un programa Troyano que instale programas de registro de tecleos para obtener información para el ataque principal o que cree los mecanismos a través de los cuales el atacante entrará más adelante al sistema. Un caso notorio del segundo ejemplo lo constituyó el Back Orifice Trojan, que pudo ser disfrazado como un componente de otro programa de software inocuo y, una vez instalado, creaba una “puerta trasera” en los sistemas de Windows 95/98 para que los atacantes tomaran el control de la computadora de la víctima. Para más información sobre el Back Orifice, véase www.nwinternet.com/~pchelp/bo/bobasics.htm.

Colocación de Softwares y Dispositivos de Trackeo

Si un atacante tiene acceso onsite al sistema de la víctima, un modo de recopilar contraseñas y otras informaciones previo al ataque es colocar un dispositivo físico de trackeo en el sistema (un registrador de tecleos). Este es un dispositivo muy pequeño, de aproximadamente 2 pulgadas de largo y media pulgada de diámetro que se puede instalar en menos de un minuto; Usted sencillamente desconecta el teclado de la computadora y lo conecta al rastreador, y entonces conecta el rastreador en el puerto del teclado de la computadora. Para la mayoría de los usuarios resulta imperceptible.

Dentro del rastreador hay un microchip y un chip de memoria no volátil (similar a la tarjeta CompactFlash o al stick de memoria). En dependencia de la cantidad de memoria en el dispositivo, este puede registrar, en cualquier lugar, desde unas pocas hasta docenas de páginas de tecleos, por ejemplo, 64KB de memoria serían cerca de 32 páginas. No hay necesidad de instalar ningún software en la computadora para que el rastreador funcione y es compatible con varios sistemas operativos. No requiere de baterías o alguna fuente de energía externa; el dispositivo extrae energía de la computadora. Una vez que los tecleos son capturados, el atacante quita el dispositivo y lo conecta a otra computadora. Los datos capturados se pueden proteger con contraseñas; una vez que se introduzca la contraseña correcta, se pueden leer en Notepad o en otro editor de texto. Después se pueden guardar los datos en un fichero y se puede borrar la memoria en el dispositivo. Un ejemplo de un dispositivo de registro de tecleos es el KeyGhost (véase www.keyghost.com).

Existen programas de software que también pueden realizar el registro de tecleos, pero el atacante necesita ser capaz de entrar al sistema para instalar el software. La ventaja del dispositivo físico es que puede capturar las contraseñas necesarias para validarse. Los softwares rastreadores capturan sólo los tecleos hechos después de que el sistema operativo inicia, mientras que el dispositivo de hardware puede capturar tecleos hechos antes de que el sistema operativo corra – por ejemplo, cambios hechos al sistema BIOS.

En la escena....

El Registro de Tecleos como una Herramienta Investigativa y de Monitoreo

Los registradores de tecleos y los programas de espionaje no son usados exclusivamente por criminales. Los investigadores policiales emplean dispositivos y softwares de registro

para obtener evidencias de delitos. A principios del 2000, Nicodemo S. Scarfo, Jr. fue acusado de juego ilegal, mafia y actividades de prestamista basados en la evidencia encontrada en un fichero de su computadora, que había sido encriptado con PGP. Los investigadores utilizaron un registrador de tecleos con el propósito de obtener la información necesaria para romper la encriptación. Los abogados de la defensa trataron de suprimir la evidencia, arguyendo que el uso de la herramienta era equivalente a un registro inconstitucional. Sin embargo, la corte se pronunció en contra de la petición de supresión y Scarfo fue encontrado eventualmente culpable.

Los vendedores de esos programas, a menudo, les venden sus productos a las agencias de policía y algunos, como Codex Data Systems han comenzado a ofrecer gratuitamente sus softwares a las agencias de policía, militares, y de la inteligencia, después de los ataques terroristas del 11 de Septiembre de 2001.

Los registradores de tecleos y los programas de espionaje tienen otros propósitos legítimos. Las compañías podrían usarlos para monitorear las computadoras de los empleados y las actividades en Internet (de acuerdo con la política de la compañía) y los padres pueden usarlos para supervisar lo que hacen sus hijos en la Net.

Cualquier tipo de registrador de tecleos guarda las pantallas que aparecen en la computadora que no son tecleadas por el usuario – estos no guardan, por ejemplo, sitios Web a los que accede el usuario, ficheros que abre el usuario o correos que lee. Otros programas de espionaje pueden hacer mucho más que sólo capturar los tecleos. Muchos de esos programas le permiten a la persona que instala y configura el software especificar criterios que dispararán la captura de pantallazos. Algunos de los programas pueden incluso renombrarse a sí mismos y cambiar su lugar en el disco para evitar la detección. Algunos ejemplos de programas de espionaje incluyen el WinWhatWhere Investigator (www.winwhatwhere.com), Spector Pro (www.spectorsoft.com) y Data Interception by Remote Transmisión o D.I.R.T. (www.codexdatasystems.com).

Colocación de Softwares Analizadores de Protocolo y de Captura de Paquetes

Los monitores de redes, también llamados *analizadores de protocolo*, le permiten a los administradores capturar y analizar el tráfico en sus redes con el propósito de solucionar los problemas o monitorear la actividad en la red. Los hackers pueden usar las mismas herramientas para capturar paquetes furtivamente y leer la información existente en ellos. Los analizadores que permiten colocar el adaptador de red en modo promiscuo son especialmente útiles para los hackers. En este modo, el adaptador puede capturar el tráfico enviado o recibido de cualquier computadora en el segmento de red. Algunos analizadores como el Monitor de Red incluido en Windows 2000 Server de Microsoft, limitan la captura a paquetes enviados hacia o procedentes de la máquina que está corriendo el software analizador. Sin embargo, una versión más poderosa de NetMon de Microsoft viene acompañando al producto SMS (Servidor de Gestión de Sistemas) y permite el uso del modo promiscuo.

Esos programas son *rastreadores* de redes. Cualquier persona con privilegios de Administración puede instalar el Monitor de Red en una computadora de la familia de Windows 2000 Server y comenzar a “escuchar” la actividad en la red. Los administradores – o hackers que han comprometido una cuenta administrativa – pueden usar la herramienta para recopilar datos de la red y analizarlos sobre la marcha, o pueden guardar las actividades registradas para revisarlas posteriormente. Es posible configurar disparadores para cuando ciertos eventos o datos crucen el cable, de modo que la herramienta puede usarse, por ejemplo, cuando ciertas palabras claves en las comunicaciones por correo electrónico se muevan a través de la red. El programa del Monitor de Red le permite a los usuarios capturar sólo esas tramas que les interesan, basados en el protocolo o en la computadora fuente o destino. Filtros aún más exactos y detallados se les puede aplicar a los datos recopilados, permitiéndole a la persona encargada del monitoreo ubicar los elementos precisos que está buscando dentro de los datos capturados.

La figura 6.1 muestra el contenido de un paquete capturado. Usted puede ver el mensaje de texto (“Windows 2000 es genial”) que fue enviado a través de la red.

Figure 6.1 Packet sniffers such as Network Monitor can reveal the contents of messages sent on the network.

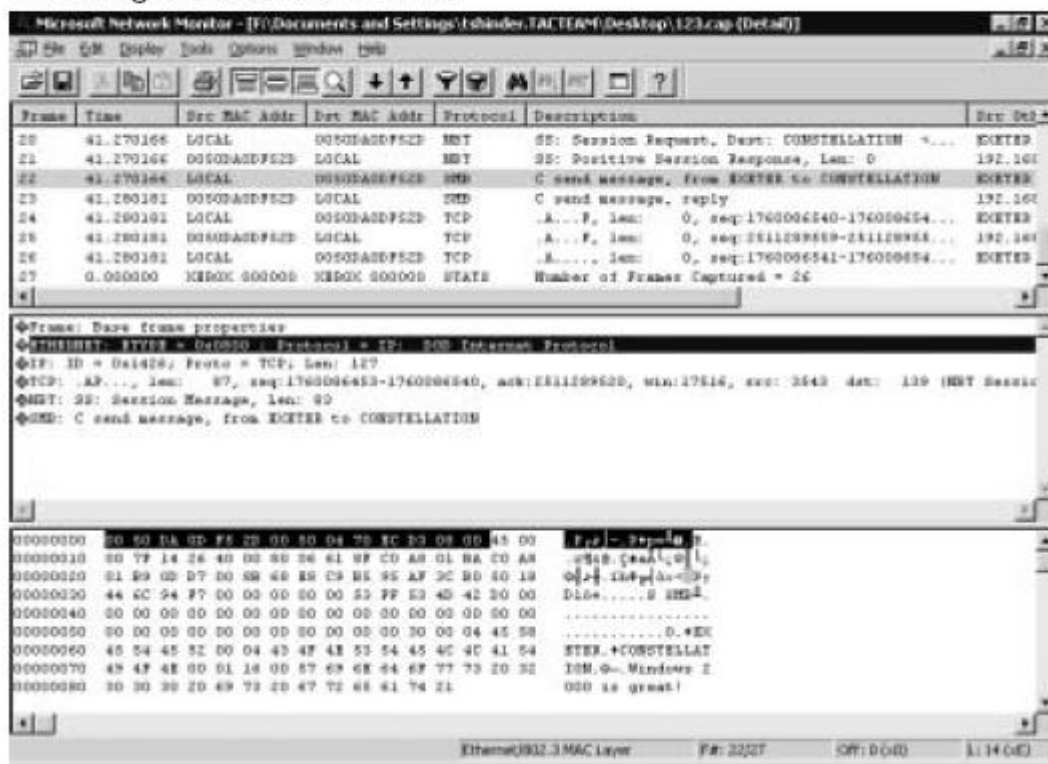


Figura 6.1 Los rastreadores de paquetes como el Monitor de Red pueden revelar el contenido de mensajes enviados en la red.

Existen disponibles docenas de programas comerciales de rastreo de paquetes. Sniffer Pro (www.sniffertechnologies.com) es probablemente el más popular. Existen otros como

LANsleuth de SSI (www.lansleuth.com) y Sniff'em (www.yasc.net/home2.html). Además existen disponibles muchos rastreadores gratuitos/pendientes de pago, tales como:

- PacketBoy (www.pro-soft.de/products/netboys/index.htm) que decodifica los protocolos TCP/IP, NetWare y Apple Talk
- Ethereal (www.ethereal.com), para Windows y UNIX
- Trace Wolf (www.simtel.net/pub/pd/16981.html) para Windows 9x/ME

El software de rastreo, generalmente, debe ser instalado en la misma red local de la computadora de la víctima; no funciona de modo remoto a través de Internet. Sin embargo, los hackers pueden explotar fallas como aquellas en el SNMP para tomar el control sobre concentradores, conmutadores y enrutadores o usar otras tácticas para tomar el control sobre una computadora en la LAN con el propósito de implementar el rastreo.

Nota

El sistema Carnivore del FBI, ahora renombrado DCS 1000, es una herramienta de monitoreo de red que funciona de modo similar a los softwares comerciales de rastreo. Se instala en locaciones ISP para llevar a cabo una vigilancia electrónica y capturar datos tales como comunicaciones por correo electrónico enviadas a o procedentes de personas sospechosas de terrorismo y otras actividades ilegales. Una característica del sistema DCS 1000 es la capacidad de filtrar transmisiones de acuerdo con el tipo de comunicación (e-mail, transacciones en la Web, etc.) de modo que sólo se interceptan mensajes de un tipo específico. Para obtener detalles sobre cómo funciona el sistema, véase www.howstuffworks.com/carnivore1.htm.

Prevención y Respuesta

No existe un modo de prevenir el escaneo de puertos – pero los profesionales de la informática pueden controlar que los escáners encuentren o no puertas abiertas a sus redes. Una medida de seguridad importante para los administradores es usar el software de escaneo de puertos para conocer las vulnerabilidades de su propia red y entonces cerrar los puertos abiertos de modo que otros no puedan usarlos para acceder. La mayoría de los muros de fuego registran los intentos de escaneo de puertos y se puede descargar, gratuitamente o pendiente de pago, por ejemplo, el Jammer, Lockdown2000 o Nukenabber e instalarlo para notificarle al administrador que se han escaneado puertos y proporcionarle la dirección IP de donde se originó el escaneo.

El spoofing del IP se puede evitar usando la verificación de la dirección fuente en el enrutador, en caso que este soporte esta función. Otras medidas que se pueden tomar para protegerse del spoofing incluyen:

- Usar autenticación encriptada.
- Configurar el enrutador para rechazar cualquier mensaje del exterior que parezca venir de una dirección (local) interna.

Los administradores pueden evitar el spoofing del ARP empleando tablas ARP estáticas. Una tabla estática es configurada manualmente por el administrador de modo que las respuestas broadcast no resulten en una actualización automática del caché. El problema de esta solución es que no funciona bien con redes muy grandes; la carga sobre el administrador para mantener al día las tablas sería insoportable. Otra solución es el *MAC binding*. Este método se habilita en los conmutadores de la red y permite la actualización automática, pero cuando una dirección IP en particular ha sido asociada con una dirección MAC, esa asociación no puede ser cambiada excepto por una acción administrativa. Además, algunas herramientas monitorean los cambios en el caché con una notificación automática para los administradores, de modo que ellos estarán alertas ante cualquier intento de usar el spoofing del ARP.

Los administradores pueden evitar el spoofing del DNS asegurando los servidores DNS en Internet y utilizando la versión más reciente del software DNS. Por ejemplo, vulnerabilidades anteriores se han solucionado en BIND, versiones 8 y 9, y las vulnerabilidades presentes en los servidores DNS con Windows NT han sido resueltas en la versión Windows 2000.

Los muros de fuego configurados apropiadamente pueden ayudar a mantener a los Troyanos fuera de la red y softwares como el Trojan Remover aseguran poder eliminar programas troyanos aún cuando el antivirus no pueda detectarlos. Las pautas habituales para la protección contra virus (no abrir anexos no solicitados, descargar ficheros sólo de sitios con reputación, aplicar diligentemente soluciones de seguridad) también pueden ayudar a protegernos de los Troyanos.

Los dispositivos de registro de tecleos son imposibles de detectar a través de un software. El examen físico del cable que conecta el teclado a la computadora revela la presencia de tales dispositivos. Los programas anti-registro de tecleos pueden escanear en busca de actividad de registro de tecleos y detectar registradores basados en software. Un ejemplo es el anti-registrador de tecleos que se puede descargar, pendiente de pago, del sitio www.webattack.com/get/antikey.shtml.

Las medidas de protección contra los rastreadores incluyen limitar el acceso físico a la red (porque el software rastreador debe instalarse en una computadora en la subred local), usar conmutadores en lugar de concentradores para evitar que todos los paquetes vayan a todos los sistemas en la red y usar encriptación. Esta última solución no evitará que los rastreadores capturen paquetes de la red, pero sí que el hacker pueda leer los datos que están dentro de ellos. El software “anti-rastreador” se puede usar para escanear la red en busca de rastreadores o computadoras cuyos adaptadores de la red estén corriendo en modo promiscuo. Existen en el mercado anti-rastreadores para UNIX y Windows. Para más información, véase www.securitysoftwaretech.com/antisniff/overview.html.

Comprendiendo el Crackeo de Contraseñas

El mejor modo de entrar en un sistema es “engañándolo” para que piense que Usted es un usuario autorizado. En muchos casos, Usted puede hacerlo sencillamente usando un

nombre y una contraseña de una cuenta válida. Este método se denomina *crackeo de contraseñas*. En esta sección, veremos las herramientas y los recursos que los hackers emplean para crackear contraseñas. Los investigadores necesitan estar al tanto de todas las técnicas y herramientas que se pueden usar para hacerse pasar por un usuario legítimo y cómo estas funcionan. Comprender cómo se logró un crackeo proporciona pistas valiosas sobre el nivel de conocimientos del cracker y sobre cuán determinado está él o ella a entrar en una red en particular, así como otras características que pueden ayudar a encontrar al culpable.

En cuanto a seguridad informática se refiere, existen tres modos básicos para validar la identidad del usuario: el método de “lo que Usted sabe” (con la contraseña siendo lo que usted sabe); el método de “lo que Usted tiene”, el cual requiere la posesión física de algún objeto como por ejemplo, una tarjeta inteligente, y el método de “qué es Usted”, el cual usa datos biométricos tales como una huella digital o de la retina o un escaneo del iris. Analizaremos más detalladamente estos métodos en el Capítulo 7 “Comprendiendo la Prevención del Crimen” en la sección sobre autenticación. Para los propósitos de este análisis, resulta importante conocer que la gran mayoría de las redes se basan sólo en el primer método, así que cualquiera que sepa o pueda deducir la contraseña correcta que va con un nombre de usuario válido puede entrar.

Nota

Las contraseñas se usan para muchos fines: para registrarse en una computadora local o en una red, para acceder a sitios Web o FTP protegidos con contraseñas, para acceder al correo electrónico, para abrir documentos protegidos con contraseñas, para regresar al escritorio después que el protector de pantalla se activó e, incluso, para entrar al programa de configuración del BIOS. Muchos usuarios, incapaces de recordar docenas de contraseñas diferentes, usan la misma para todo. Aunque esta estrategia simplifica la vida del usuario, también simplifica el trabajo del cracker. Una vez que él o ella tenga una contraseña, esta funciona como un “ábrete sésamo” para todo lo que el usuario tenga protegido con contraseña.

El crackeo de contraseñas se trata de adquirir contraseñas válidas. Esto se puede hacer de varias maneras, incluyendo:

- Fuerza bruta
- Recuperación y explotación de contraseñas almacenadas en el sistema
- Uso del software de decodificación de contraseñas
- Ingeniería social

En las siguientes secciones, analizaremos cada uno de estos métodos y las formas para protegerse de ellos.

Fuerza Bruta

La fuerza bruta quizás no es la solución más elegante para un hacker en busca de una contraseña, pero puede ser muy efectiva – especialmente si no se han impuesto políticas de contraseñas seguras. En su forma más simple, un atacante de fuerza bruta prueba posibles contraseñas hasta que encuentra la correcta. Aunque este proceso lo puede hacer manualmente alguien con mucho tiempo y paciencia, en la práctica generalmente se hace (de modo mucho más eficiente) usando un programa que corra a través de todas las palabras en un fichero de diccionario, que es, sencillamente, una larga lista de palabras (en lo que a veces se denomina *ataque de diccionario*) y otras posibles combinaciones de caracteres.

Algunos de esos programas de crackeo son muy sofisticados y le permiten al cracker implementar reglas o criterios. Por ejemplo, si el cracker es capaz de obtener alguna información sobre la contraseña – por ejemplo, el cracker sabe que esta consiste en cinco caracteres alfa y tres numéricos – él o ella puede crear una regla que limitará los intentos del programa a las contraseñas que cumplan con estos criterios (apple123, seven890, etc.). Esta estrategia reduce el número de contraseñas posibles y acelera el proceso de crackeo.

Los programas de crackeo de contraseñas tienen también un uso legítimo. Quizás un empleado abandona la compañía o muere repentinamente sin revelar las contraseñas que se usaban para proteger ficheros importantes, las cuales necesitan ahora otros empleados para acceder a ellos. Incluso si él estuviera presente, a veces los empleados olvidan sus contraseñas. Los programas comercializados para propósitos legítimos generalmente se denominan programas de *recuperación de contraseñas*, pero, por supuesto, el mismo software puede ser usado por los crackers para propósitos nada legítimos. Por ejemplo, el NTAccess de Softwares Sunbelt funciona creando un disco de arranque, después usa la herramienta para modificar el disco de arranque con el fin de recomponer la contraseña del administrador. Otro programa, el Locksmith de Winternals le permite a Usted recomponer la contraseña de cualquier cuenta de forma remota. Algunas compañías brindan el servicio de recuperación de contraseñas. Una de ellas es Password Crackers Inc. (www.pwcrack.com).

Nota

Algunos programas de recuperación se centran en contraseñas de sistemas operativos y otros en contraseñas de aplicaciones. El software Passware en www.lostpassword.com es un sistema modular que le permite a Usted seleccionar módulos de acuerdo con sus necesidades, recuperar contraseñas en Windows NT, 2000, XP, Excel, Access, Outlook, Word, WinZip, WordPerfect, Quickbooks, ACT y más. El Kit de Passware incluye todos los módulos y una versión demo se puede descargar gratuitamente del sitio.

Algunos de estos programas de crackeo no funcionarán en Windows 2000/XP cuando se use encriptación de ficheros (EFS) y los programas que hemos analizado recomponen contraseñas *locales* – aquellas almacenadas en una computadora específica – no

contraseñas de redes tales como aquellas almacenadas en el Directorio Activo de Windows 2000 y usadas para registrarse en el dominio.

Algunos esquemas de protección de contraseñas son más difíciles de crackear que otros. Las contraseñas en documentos creados con versiones más antiguas a Microsoft Office y los ficheros compactados son notoriamente fáciles de crackear con softwares fáciles de conseguir. Con cualquier esquema de contraseñas, mientras mejores sean las contraseñas (más largas y más complejas), más tiempo tomará crackearlas. Para difíciles trabajos de crackeo, algunas herramientas como LOphtCrack versiones 3 y posteriores (mostrada en la Figura 6.2) le permiten a Usted dividir la tarea en partes y usar múltiples máquinas simultáneamente para realizar el crackeo en un método denominado *crackeo distribuido*.

Figure 6.2 Widely available tools such as LOphtCrack use comparative analysis to crack passwords.



Figura 6.2 Herramientas fáciles de conseguir como LOphtCrack usan análisis comparativo para crackear contraseñas.

En la escena...

Crackeando 101 en la Web

En cientos de sitios Web, los crackers principiantes pueden obtener información sobre cómo vencer contraseñas y descargar herramientas como LOphtCrack, NTcrack, Cracker Jack y Dictionary Maker. Como todos los sitios de hackers, estos sitios vienen y van rápidamente y pasan de un dominio a otro para evitar el escrutinio. Si se realiza una búsqueda de *herramientas de crackeo de contraseñas* aparecen miles de resultados, pero probablemente Usted encontrará que muchos de ellos resultan en mensajes de “fichero no encontrado” cuando trata de acceder a ellos. Sin embargo, si Usted es persistente, no resulta difícil encontrar toda la información que necesita para comenzar a crackear. Existen ficheros de diccionarios en muchos idiomas. Un sitio popular para descargar diccionarios es <ftp://ftp.cerias.purdue.edu/pub.dict>.

Ninguna de estas herramientas es ilegal (aún), de modo que la policía no puede hacer mucho acerca de su fácil adquisición. Sin embargo, es bueno que los investigadores estén conscientes de dónde los criminales cibernéticos obtienen las herramientas que usan para cometer crímenes, así como también resulta útil saber cuáles puntos de venta en un área venden (legalmente) veneno, dinamita, armas u otros artículos que se pueden utilizar para propósitos ilegales.

Explotación de Contraseñas Almacenadas

Tratar de adivinar contraseñas, incluso con un software para acelerar el proceso, es un asunto tedioso. Resultaría mucho más fácil si un cracker encontrara un listado de contraseñas tirado por algún lugar. Bueno, en algunos casos, eso es exactamente lo que sucede – la lista está allí mismo para ser tomada en el disco duro de la computadora. Las contraseñas deben almacenarse en algún sitio; después de todo, ¿de qué otra forma sabría el sistema si un usuario ha introducido la contraseña correcta? Además, la mayoría de las personas tienen varias contraseñas diferentes además de sus contraseñas de validación. Estas se usan para acceder al correo electrónico, para entrar a sitios Web restringidos, etc. En lugar de memorizar todas esas contraseñas secundarias, muchos usuarios eligen que el sistema “recuerde” la contraseña por ellos. Como las computadoras tienen poca memoria (usted se recordará de que todos los datos en la RAM se pierden cuando la computadora se reinicia), esas contraseñas “recordadas” deben almacenarse en un fichero en algún lugar. Todo lo que el cracker tiene que hacer es poner sus pequeñas y ansiosas manos sobre ese fichero.

Gracias a Dios es un poco más complicado que eso. En la mayoría de los casos, las contraseñas no se almacenan en un fichero de texto plano que el cracker puede, sencillamente, abrir y leer, excepto en casos en que un usuario olvidadizo cree un fichero de esa clase que le recuerde diligentemente las contraseñas para varios servicios y aplicaciones. Generalmente, las contraseñas almacenadas son *encriptadas* o *codificadas*.

Por ejemplo, los sistemas UNIX almacenan contraseñas en el fichero `/etc/passwd`, conjuntamente con otras informaciones del usuario. Las contraseñas son encriptadas con una función de codificación. La computadora no compara la contraseña real que Usted teclea con una lista para determinar si lo valida; en su lugar, la contraseña que Usted introduce es codificada y el valor codificado resultante se compara con aquel de la contraseña (codificada) almacenada.

Este sistema suena al seguro, pero no es así. El software de crackeo sólo necesita ser un poquito más sofisticado. Si el cracker puede llegar al fichero de contraseñas, el programa usa cualquier función de codificación que use el sistema y encripta las posibles contraseñas (generándolas a través de los métodos de fuerza bruta y de diccionario), entonces compara los resultados con las contraseñas encriptadas en el fichero de contraseñas. Esta técnica se denomina *análisis comparativo*.

Nota

Los sistemas UNIX y Linux pueden usar *contraseñas fantasmas* para evitar las técnicas de análisis comparativo. Si están habilitadas las contraseñas fantasmas, la contraseña encriptada en el fichero `passwd` es reemplazada por una `x`. Las contraseñas reales se almacenan en otro fichero denominado `/etc/shadow`. ¿Cuál es la ventaja de almacenar la información en un fichero diferente, especialmente cuando todos los que están familiarizados con UNIX saben el nombre y la locación del fichero? El secreto es que al fichero `/etc/shadow` se puede acceder sólo desde la cuenta raíz. Aunque a las cuentas de grupos generalmente no se le asignan contraseñas, esto es posible. Las contraseñas de grupo pueden ser fantasmas al igual que las contraseñas de usuarios. En ese caso, las contraseñas encriptadas se almacenan en un fichero llamado `/etc/shadow`.

Los sistemas NetWare almacenan las contraseñas en los ficheros `bindery NETBAL.SYS` o `NETVAL.SYS` (en versiones más antiguas de NetWare) o en la base de datos NDS (en versiones 4.x y posteriores). La contraseña se almacena como un atributo de un objeto o una propiedad. El objeto podría ser una cuenta de usuario, una impresora o similar.

Las máquinas con Windows 9x almacenan las contraseñas en ficheros nombrados según la cuenta de usuario correspondiente con la extensión `.pwl`, en el directorio raíz del sistema (llamado Windows por defecto). Las contraseñas son encriptadas, pero se usa un débil algoritmo de encriptación, de modo que resulta fácil crackear esas contraseñas con softwares como Glide. Sin embargo, no es ni necesario crackear las contraseñas para entrar en una computadora con Windows 9x reiniciándola en MS-DOS y renombrando el fichero de contraseñas. Este sistema le permite al cracker introducir cualquier contraseña nueva para registrarse en el sistema. La contraseña del refrescador de pantalla de Windows 9x se almacena en el fichero de Registro nombrado `user.dat`, que se ubica en `<driveletter>\windows\profiles\<username>`. La contraseña es una cadena de valores hexadecimales con cada valor hex de dos dígitos representando un carácter ASCII. Para crackear la contraseña, Usted tiene que decodificar los valores hex y llevarlos a ASCII.

Los sistemas operativos de Windows basados en NT son mucho más seguros. Al igual que UNIX, ellos almacenan un código de la contraseña en el Registro. Esta información está contenida en la base de datos SAM (Administrador de Cuentas de Seguridad), la cual los hackers a veces pueden obtener del directorio de reparación `\<systemroot>` que se crea cuando está corriendo la utilidad del rdisco con el conmutador `/s` para hacer una copia de seguridad de la información de configuración del sistema en un disquete.

Windows 2000 usa autenticación Kerberos que es generalmente reconocida como más segura que la NTLM. Sin embargo, Kerberos también tiene vulnerabilidades. Los crackers pueden usar el software rastreador para capturar el tráfico de registro en la red y usar los datos de pre-autenticación usados por Kerberos para verificar las credenciales del usuario. En el sitio Web www.brd.ie/papers/w2kkrb/feasibility_of_w2k_kerberos_attack.htm Usted encontrará un análisis sobre cómo esto se hace. En numerosos sitios Web, listas de correos y grupos de noticias se puede encontrar información sobre el crackeo en NT y Windows 2000.

¿Por qué esto le concierne al investigador? El conocimiento de un investigador sobre cómo los diferentes sistemas operativos almacenan contraseñas se puede utilizar, en algunos casos, para rastrear actos de criminales. Si la auditoria de seguridad está debidamente configurada, los investigadores podrán decir si y cuándo hubo acceso a diferentes ficheros. Los registros que guardan el acceso a ficheros de contraseñas podrían indicar que las mismas han sido o serán comprometidas.

Intercepción de Contraseñas

Los crackers no siempre tienen que acceder a los ficheros de contraseñas o recurrir a adivinar mediante fuerza bruta las contraseñas utilizables. Cuando las contraseñas se envían a través de la red mediante conexiones de acceso local o remoto en forma de texto plano, pueden ser interceptadas, como lo pueden ser otros datos que viajan a través de la red, usando un software rastreador. Las sesiones Telnet para computadoras UNIX pueden ser interceptadas y la contraseña de texto plano extrapolada si no se toman medidas de seguridad. El uso de protocolos de autenticación no seguros como el PAP (Protocolo de Autenticación de Contraseñas) para acceso remoto trae como resultado el envío de contraseñas de texto plano a través del enlace, lo que debería evitarse en la medida de lo posible. (Analizaremos más detalladamente los protocolos de autenticación en el Capítulo 7).

Otra forma de interceptar contraseñas es usando un *registrador de teclados*. Como analizamos anteriormente en este capítulo, este es un dispositivo de hardware o programa de software que captura y registra cada carácter que se tecléa – incluyendo las contraseñas.

A menudo es posible detectar un rastreador de paquetes no autorizado en la red usando un dispositivo denominado reflectómetro óptico en el dominio del tiempo (TDR), el que envía un pulso hacia el cable y crea un gráfico de las reflexiones que regresan. Los usuarios que saben cómo leer el gráfico pueden decir si y dónde existen dispositivos no autorizados conectados al cable.

Otras formas de detectar conexiones no autorizadas incluyen el monitoreo del concentrador o de las luces del conmutador, usando gestores SNMP que registren las conexiones y desconexiones, o el uso de una de las muchas herramientas diseñadas con el propósito específico de detectar rastreadores en la red.

Además, varias técnicas que usan PING, ARP y DNS podrían ayudar a capturar a rastreadores no autorizados. El empleo de esas técnicas va más allá del alcance de este libro, pero Usted puede encontrar instrucciones para utilizarlas (y mucha más información excelente sobre el rastreo de paquetes) en la sección dedicada a las Preguntas Realizadas con más Frecuencia de Robert Gram. en www.secinf.net/info/misc/sniffingfaq.html.

Software de Decodificación de Contraseñas

La mayoría de los programas de crackeo de contraseñas realmente no decodifican nada. Sin embargo, si el algoritmo de encriptación es débil o está implementado incorrectamente, a veces es posible usar una técnica llamada *parqueo de un byte*, la cual es capaz de decodificar la contraseña cambiando un byte en el programa. Otra técnica empleada con algoritmos débiles requiere que el cracker ya haya obtenido uno o más ficheros en forma decodificada; entonces estos se pueden usar para decodificar otros que usen el mismo algoritmo. Esto es a lo que llaman el *conocido método del texto plano*. Esta técnica es popular como un ataque contra los ficheros protegidos con contraseñas .zip, .rar y .arj. Todas esas son extensiones usadas para ficheros de archivos compactados.

Cuando se emplea una encriptación poderosa y se escogen contraseñas complejas, resulta mucho más difícil usar decodificación directa. En esos casos, un ataque de diccionario o de fuerza bruta resulta más exitoso. Los “decodificadores” PDF como el Decodificador PDF Garantizado/Eliminador de Restricciones (GuaPDF) usa un tipo de fuerza bruta que prueba todas las claves posibles.

En la escena...

El Debate sobre la Encriptación Débil

Muchos expertos en seguridad sienten que la encriptación débil y fácil de romper es peor que no tener ninguna, porque esta le da a los usuarios un falso sentido de seguridad, conduciéndolos a ser descuidados con datos sensibles porque creen que están protegidos. Otros arguyen que la encriptación débil es mejor que no tener ninguna porque, al menos, mantiene alejados a los “fisgones” casuales, meramente curiosos o no sofisticados desde el punto de vista técnico. La verdad, como es usual, radica entre ambos extremos. La encriptación débil podría resultar beneficiosa en algunas situaciones, - por ejemplo, en el caso de un documento no crítico como un diario personal que un usuario quiere proteger de otros usuarios no técnicos que comparten la computadora. Por otra parte, la seguridad débil puede ser desastrosa en el caso de informaciones de vital importancia tales como secretos comerciales o datos militares que son más propensos a ser blancos de crackers técnicamente sofisticados. En esta situación, la encriptación débil realmente puede ser peor que no tener ninguna porque el hecho de que el fichero esté encriptado atrae la atención del cracker, quien quizás, de otro modo, lo hubiese ignorado.

Ingeniería Social

A diferencia de los otros tipos de ataques, la *ingeniería social* no se refiere a una manipulación tecnológica del hardware de la computadora o de las vulnerabilidades de los softwares y no requiere de muchos conocimientos técnicos. En su lugar, este tipo de ataque explota las *debilidades humanas* – tales como la despreocupación o el deseo de ser cooperativo – para obtener el acceso a credenciales legítimas de la red. Los talentos que le son más útiles al intruso que se basa en técnicas de ingeniería social son las llamadas “aptitudes de las personas” como tener una personalidad encantadora o persuasiva o una presencia autoritaria e imperiosa.

La *ingeniería social* se define como la obtención de información confidencial mediante la interacción humana (Business Wire, 4 de Agosto de 1998). Usted puede imaginarse a este tipo de atacantes como estafadores especializados. Ellos se ganan la confianza de los usuarios (o, aún mejor, la de los administradores) y entonces se aprovechan de la relación para averiguar nombres de cuenta de usuarios y contraseñas o hacer que los usuarios confiados los validen en el sistema. Como esta se basa en convencer a un usuario válido de la red para “abrir la puerta”, la ingeniería social puede introducir exitosamente a un intruso en una red protegida con medidas de alta seguridad como son los escáners biométricos.

La ingeniería social es, en muchos casos, el modo más fácil de obtener acceso no autorizado a una red de computadoras. La Competencia de Ingeniería Social que tuvo lugar en Las Vegas, en la convención anual de hackers Defcon, atrajo a cientos de participantes ansiosos de poner en práctica sus técnicas manipuladoras. Incluso hackers famosos por sus habilidades técnicas saben que las *personas* constituyen la mayor vulnerabilidad de la seguridad en la mayoría de las redes. Kevin Mitnick, condenado por graves crímenes por ordenador y una celebridad extraordinaria en el mundo de los hackers, cuenta en sus lecturas cómo durante su carrera de hacker solía usar la ingeniería social para obtener acceso a sistemas.

Nota

Para más información sobre las lecturas de Mitnick, véase *Mitnick Enseña Ingeniería Social* en www.zdnet.com/filters/printerfriendly/0,6061,2604480-2,00.html.

Estos “ingenieros”, a menudo, se hacen pasar por personal de soporte técnico – simulando trabajar como parte del equipo interno o para entidades externas como la compañía de teléfonos, un ISP, como vendedores de hardware para redes o, incluso, como trabajadores del gobierno. A veces contactan a sus víctimas por teléfono y generalmente les cuentan una historia compleja y convincente de por qué ellos necesitan que los usuarios divulguen sus contraseñas u otra información (como la dirección IP de la máquina del usuario o el nombre de la computadora del servidor de autenticación de la red).

Nota

Para más información sobre la ingeniería social y qué decir cuando alguien trate de aplicarla, véase el capítulo previo, *Todo lo que Quería Saber sobre Ingeniería Social – Pero Temía Preguntar*, en el sitio Web del Hacker Feliz: www.happyhacker.org/uberhacker.se.shtml.

Prevención y Respuesta

Ya que las contraseñas son la primera – y en algunas redes, la única – línea de defensa para proteger una red contra intrusos, resulta extremadamente importante que se tomen medidas para asegurar la integridad de las contraseñas de todos los usuarios. Analizaremos más detalladamente las políticas de contraseñas en el Capítulo 7. Las secciones siguientes

brindan algunas pautas generales sobre la protección de contraseñas y cómo lidiar con los llamados ingenieros sociales.

Medidas Generales de Protección de Contraseñas

Los administradores de redes y los usuarios pueden tomar una serie de medidas para proteger las contraseñas, incluyendo las siguientes:

- Seguir las pautas para crear contraseñas poderosas, analizadas detalladamente en el Capítulo 7 en la sección sobre políticas de contraseñas.
- Configurar de modo que las cuentas de usuarios se inhabiliten o se bloqueen después de una cantidad razonable de intentos incorrectos de introducir la contraseña.
- Usar EFS en computadoras con Windows 2000/XP/.NET para encriptar ficheros.
- Almacenar datos críticos en servidores de redes en lugar de en máquinas locales.
- No confiarse de la protección de contraseñas incluida en la mayoría de las aplicaciones.
- Habilitar la contraseña fantasma en sistemas UNIX/Linux.
- Deshabilitar la Autenticación de Administración de la LAN en redes de Windows. (NTLMv2 o Kerberos son mucho más seguras).
- Asegurar que las contraseñas no se envíen jamás a través de la red en formato de texto plano.
- Usar softwares anti-rastreadores y técnicas de detección de rastreadores para protegerse de los crackers que tratan de interceptar las contraseñas que viajan a través de la red.

Protegiendo la Red contra los Ingenieros Sociales

Los administradores consideran un reto especial el protegerse contra los ataques de ingeniería social. Adoptar políticas verbales que prohíban la divulgación de contraseñas y otras informaciones sobre la red a cualquiera a través del teléfono y educar a los usuarios sobre este fenómeno son pasos obvios que los administradores pueden dar para reducir la probabilidad de este tipo de ruptura de la seguridad. Sin embargo, debido a la naturaleza del ser humano, algunos usuarios en todas las redes serán siempre vulnerables al engaño de los ingenieros sociales. Un ingeniero social talentoso es un maestro en hacer que los usuarios duden de sus propias dudas acerca de su legitimidad.

El intruso “principiante” quizás le haga al usuario historias tristes sobre el costo extra en que incurriría la compañía si él o ella invierte tiempo en verificar su identidad. Él podría hacerse pasar por un miembro de la alta dirección de la compañía y asumir un enfoque severo amenazando al empleado con una medida disciplinaria o incluso la pérdida del empleo si no obtiene la cooperación de los usuarios. O el ingeniero social podría tratar de hacer que el empleado se sienta culpable fingiendo ser un empleado de bajo nivel que sólo está tratando de hacer su trabajo y que será despedido si no accede a la red y se ocupa del problema inmediatamente. Un buen ingeniero social es paciente y metódico. Él hará su tarea y sabrá suficiente sobre la compañía objetivo o la organización que dice representar para sonar convincente.

Debido a que la ingeniería social es un problema humano, no técnico, la prevención debe venir fundamentalmente a través de la educación en lugar de mediante soluciones técnicas.

Comprendiendo las Explotaciones Técnicas

Un ladrón que no es capaz de falsificar una tarjeta de identificación de un empleado para entrar por la puerta delantera de una compañía, puede, sin embargo, regresar por la noche y forzar las cerraduras de la puerta trasera para entrar. Así mismo, si un intruso cibernético o un atacante es incapaz de venir con contraseñas para entrar en la red haciéndose pasar por un usuario legítimo, él o ella tiene numerosos métodos para entrar sin credenciales.

Generalmente, estos métodos explotan las características de los protocolos, del sistema operativo, o de los softwares de aplicación usados en el sistema o la red objetivo, del mismo modo que un ladrón maestro podría explotar el hecho de que un edificio tenga salidas de ventilación y las utilice para entrar al lugar. En las siguientes secciones analizaremos algunas explotaciones técnicas populares que los hackers emplean para acceder o interrumpir comunicaciones en las redes. Los investigadores deberían tener un conocimiento básico acerca de cómo funcionan esas técnicas, por las mismas razones por las que necesitan saber los aspectos técnicos del crackeo de contraseñas: El conocimiento de cómo un criminal cibernético comete el crimen, a menudo, brinda una información valiosa para crear el perfil que conduce a la aprehensión.

Explotaciones de Protocolos

Las explotaciones de protocolos usan las características de un protocolo tales como las que utiliza el método de “intercambio” TCP para establecer una sesión de comunicaciones, con el fin de obtener un resultado nunca previsto – por ejemplo, sobrecargar el sistema objetivo al punto donde este es incapaz de comunicarse con los usuarios legítimos. Existen muchas maneras en las que se puede manipular el comportamiento normal de los protocolos de redes para congestionar la red o el servidor al punto donde no se puedan establecer comunicaciones legítimas. En esta sección, analizaremos en detalles qué es un ataque DoS y las muchas formas en que las características del TCP/IP pueden usarse para lanzar ataques DoS. También analizaremos los ataques de enrutamiento fuente y otras explotaciones de protocolos.

Ataques DoS que Explotan el TCP/IP

Los ataques DoS, mencionados previamente en este capítulo, son una de las variantes más populares de los hackers de Internet que quieren afectar las operaciones de una red. En Febrero de 2000, ataques DoS masivos echaron abajo varios de los mayores sitios Web mundiales, incluyendo Yahoo.com y Buy.com. Muchos de estos ataques explotan varias características de la suite de protocolo TCP/IP. Esta sección detalla cómo funcionan los diferentes ataques DoS. Los tipos de ataques que analizaremos incluyen:

- Ataques DoS al DNS que explotan los protocolos del Sistema de Nombre de Dominio
- Ataques SYN/LAND que explotan el modo en que funciona el proceso de intercambio TCP
- El Ping de la Muerte, que usa un “paquete asesino” para sobrecargar un sistema
- Los ataques Ping flood, fraggle y smurf que emplean varios métodos para “inundar” la red o el servidor
- La bomba UDP y el snork UDP que explotan el Protocolo de Datagramas del Usuario
- Los ataques Teardrop que explotan los campos de encabezamiento de los paquetes IP
- Explotaciones del SNMP que está incluido en la mayoría de las implementaciones del TCP/IP

¿Qué es la Denegación del Servicio?

Aunque ellos no destruyen o roban datos como otros tipos de ataques, los atacantes DoS tienen un objetivo al echar abajo una red, denegándole el servicio a sus legítimos usuarios. Los ataques DoS son fáciles de iniciar, el software se puede conseguir fácilmente en los sitios Web de los hackers y los grupos de noticias warez. Este le permite a cualquiera con poca o ninguna pericia lanzar un ataque DoS.

El propósito de un ataque DoS es tornar inaccesible una red generando un tipo o una cantidad de tráfico en la red que colapse los servidores, sobrecargue los enrutadores o impida que los dispositivos de red funcionen apropiadamente. El DoS se puede conseguir paralizando los recursos del servidor, por ejemplo, sobrecargando la CPU y los recursos de memoria. En otros casos, un usuario o una máquina en particular puede ser blanco de ataques DoS que bloqueen la máquina del cliente, siendo necesario reiniciarla.

Los DoS Distribuidos o ataques *DDoS* utilizan computadoras intermediarias, llamadas *agentes*, en las que han sido instalados previa y furtivamente programas llamados *zombies*. El hacker activa estos programas zombies desde un puesto remoto, haciendo que las computadoras intermediarias (que pueden ser cientos o incluso miles) lancen simultáneamente el ataque real. Debido a que el ataque proviene de computadoras corriendo los programas zombies, las que pueden estar en redes de cualquier lugar del mundo, el hacker puede ocultar el verdadero origen del ataque.

Ejemplos de las herramientas que emplean los hackers para lanzar el DDoS son Tribe FloodNet (TFN), TFN2K, Trinoo y Stacheldraht (en alemán *alambre de púa*). Las primeras versiones de las herramientas del DDoS tenían como blancos los sistemas UNIX y Solaris, pero TFN2K puede correr en ambos sistemas: UNIX y Windows.

Ya que los ataques DDoS son tan populares, se han creado muchas herramientas para ayudarle a detectarlos, eliminarlos y analizar el software DDoS que podría estar instalado en su red. Es importante destacar que los ataques DDoS constituyen una amenaza de dos capas. No sólo su red podría ser un blanco de un ataque DoS que colapse sus servidores e impida el tráfico entrante y saliente, sino que sus computadoras podrían ser utilizadas como el “intermediario inocente” para lanzar un ataque DDoS contra otra red u otro sitio.

Los ataques DoS/DDoS se pueden llevar a cabo de varias formas. Las explotaciones de las aplicaciones, del sistema operativo y de los protocolos se pueden usar para sobrecargar los sistemas y crear una denegación del servicio. En las siguientes secciones, abordaremos tipos específicos de ataques DoS y DDoS y explicaremos cómo funcionan.

En la escena....

El DoS como un Arma de la Guerra Cibernética

En Noviembre de 2000, Lucent Technologies anunció que un grupo pro-Palestina llamado Unidad había atacado su sitio Web empleando una herramienta llamada Defiende que crea un flujo de mensajes diseñado para sobrecargar el sistema y crear una denegación del servicio. A Lucent le dijeron que fue atacada por haber hecho negocios en Israel.

DoS al DNS

El ataque DoS al DNS explota la diferencia de tamaño entre una pregunta DNS y una respuesta DNS, en el que todo el ancho de banda de la red está paralizado por falsas preguntas DNS. El atacante usa los servidores DNS como “amplificadores” para multiplicar el tráfico DNS.

El atacante comienza enviando a cada servidor DNS pequeñas preguntas DNS que contienen la dirección IP falsa de la futura víctima (véase el análisis del Spoofing del IP realizado anteriormente en este capítulo). Las respuestas a las pequeñas preguntas son mucho más largas, de modo que si regresa una gran cantidad de respuestas al mismo tiempo, el enlace se congestiona y tiene lugar la denegación del servicio.

Una solución a este problema es que los administradores configuren los servidores DNS para que cuando reciban preguntas DNS de fuentes sospechosas o inesperadas respondan con una “negación”, que es mucho más pequeña que una respuesta de resolución de nombre.

Ataques SYN/LAND

Los ataques SYN explotan el “intercambio TCP de tres pasos”, proceso mediante el cual se establece una sesión de comunicaciones entre dos computadoras. Como el TCP (a diferencia del UDP) está orientado a la conexión, se debe crear, antes del envío de datos, una *sesión* o un enlace directo de comunicación uno a uno. La computadora cliente inicia la comunicación con el servidor (la computadora a cuyos recursos esta quiere acceder).

El “intercambio” incluye los siguientes pasos:

- 1.La máquina cliente envía un segmento (SYN) de solicitud de sincronización.
- 2.El servidor envía un mensaje de reconocimiento (ACK) y un SYN, que reconoce la solicitud de la máquina cliente enviada en el paso 1 y le envía al cliente una solicitud de sincronización para ella. Las máquinas cliente y servidor deben sincronizar los números de secuencias de cada una.

3.El cliente envía de regreso al servidor un ACK, reconociendo la solicitud de sincronización del servidor. Cuando ambas máquinas han reconocido mutuamente las solicitudes, el intercambio se completa exitosamente y se establece una conexión entre las dos computadoras.

La Figura 6.3 ilustra el funcionamiento del proceso.

Figure 6.3 TCP uses a “three-way handshake” to establish a connection.

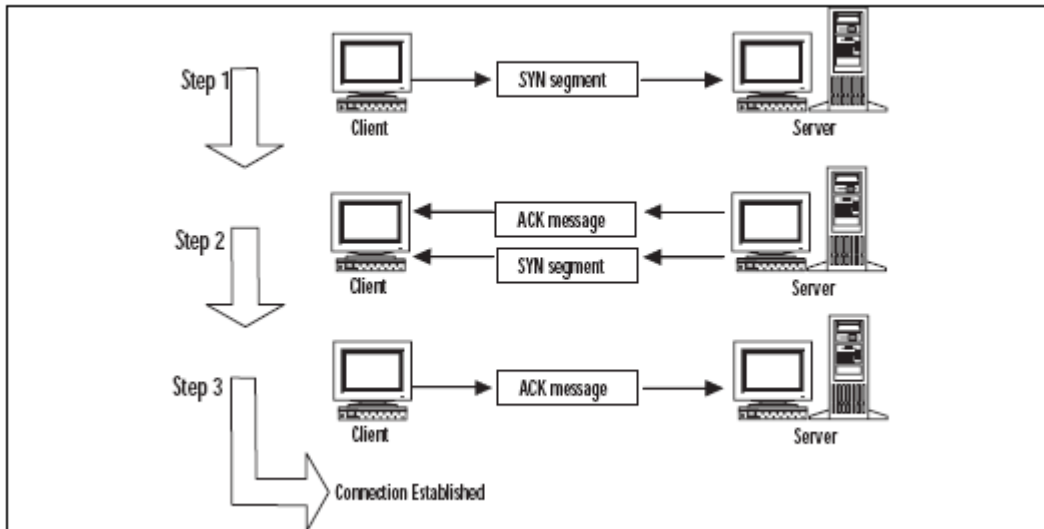


Figura 6.3 El TCP usa un “intercambio de tres pasos” para establecer una conexión.

Paso 1	Cliente	Segmento SYN	Servidor
Paso 2	Cliente	Mensaje ACK Segmento SYN	Servidor
Paso 3	Cliente	Mensaje ACK	Servidor

Conexión establecida

Un ataque SYN usa este proceso para inundar el sistema objetivo como la víctima del ataque con paquetes SYN múltiples que tienen direcciones IP de mala procedencia. Esto ocasiona que el sistema responda con mensajes SYN/ACK. El problema surge cuando el sistema, esperando por el mensaje ACK del cliente que normalmente viene en respuesta a su SYN/ACK, pone los mensajes de espera SYN/ACK en cola. Esto constituye un problema porque la cola sólo puede manejar un número limitado de mensajes. Cuando la cola se llena, los paquetes SYN que llegan después serán ignorados. Para que un SYN/ACK sea eliminado de la cola, un ACK debe retornar del cliente o un temporizador de intervalo debe detenerse y terminar el proceso de intercambio de tres pasos.

Como las direcciones IP fuentes de los paquetes SYN enviados por el atacante no son buenas, las ACK que el servidor espera nunca llegan. La cola se mantiene llena y no hay

espacio para que las solicitudes SYN válidas sean procesadas. Por ende, el servicio se le deniega a los clientes legítimos que intentan establecer comunicaciones con el servidor.

El ataque LAND es una variación del ataque SYN. En el ataque LAND, en lugar de enviar paquetes SYN con direcciones IP que no existen, el flujo de paquetes SYN tiene la misma dirección IP falsa – la de la computadora objetivo.

El ataque LAND se puede evitar filtrando los paquetes en arribo cuyas direcciones IP fuentes parezcan ser de computadoras de la red interna.

El Ping de la Muerte

Otro tipo de ataque DoS es el llamado *Ping de la Muerte* (también conocido como el *ping de paquete grande*). El ataque Ping de la Muerte se lanza creando un paquete IP mayor de 65,536 bytes que es el máximo permitido por la especificación IP (a veces referido como un *paquete asesino*). Este paquete puede ocasionar que el sistema objetivo colapse, se bloquee o se reinicie.

Ping Flood/Fraggle/Smurf

El *pingflood* o *flood ICMP* es un medio de paralizar una máquina cliente específica. Esto es ocasionado por un atacante que envía un gran número de paquetes ping (paquetes de solicitud eco ICMP) al Winsock o al software de marcación. Este torrente impide que el software responda a las solicitudes de actividad ping del servidor, lo que ocasiona que el servidor eventualmente finalice la conexión. Un síntoma de un ping flood es una gran cantidad de actividad en el módem, indicada por sus luces. Este tipo de ataque es también referido como una *tormenta de ping*.

El *ataque fraggle* se relaciona con la tormenta de ping. Utilizando una dirección IP falsa (la dirección de la víctima), un atacante envía paquetes ping a una subred, ocasionando que todas las computadoras de la subred respondan a la dirección falsa y la inunden con mensajes de respuesta eco.

En la escena...

Ataques Fraggle en Acción

Durante la crisis de Kosovo, los hackers pro-Serbia usaban frecuentemente el ataque fraggle contra los sitios de los Estados Unidos y la OTAN para sobrecargarlos y echarlos abajo.

El ataque *smurf* es una forma de ataque de fuerza bruta que emplea el mismo método del torrente de ping, pero dirige el torrente de paquetes de solicitud eco ICMP hacia el enrutador de la red. La dirección de destino de los paquetes ping es la dirección broadcast de la red, lo que ocasiona que el enrutador broadcast el paquete hacia todas las computadoras en la red o en el segmento. Esto puede resultar en un gran tráfico dentro de

la red si hay muchas computadoras anfitrionas y puede crear una congestión que ocasione una denegación del servicio a los legítimos usuarios.

Nota

La dirección broadcast está representada normalmente por todos los uno (1) en el ID de la máquina (en la forma binaria de la dirección). Esto significa, por ejemplo, que en la red Clase C 192.168.1.0, la dirección broadcast sería 192.168.1.255. El número 255 en decimal representa 11111111 en binario, y en una red Clase C, el último octeto o z representa el ID de la máquina. Un mensaje enviado a la dirección broadcast es enviado simultáneamente a todas las máquinas de la red.

En su forma más insidiosa, el atacante smurf falsifica la dirección IP fuente del paquete ping. Entonces ambas, la red hacia la que se envía el paquete y la red de la dirección IP fuente falsa se sobrecargarán con el tráfico. La red a la que pertenece la dirección fuente falsa se inundará con respuestas al ping, pues todas las máquinas a las que se les envió el ping responden a la pregunta eco con una respuesta eco.

Los ataques smurf, generalmente, pueden hacer más daño que otras formas de DoS como los torrentes SYN. El torrente SYN afecta solamente la capacidad de otras computadoras de establecer una conexión TCP con el servidor inundado, pero un ataque smurf puede derribar todo un ISP por minutos u horas. Esto se debe a que un solo atacante puede enviar fácilmente entre 40 y 50 paquetes ping por segundo, aún usando una conexión lenta. Como cada paquete es emitido a todas las computadoras de la red de destino, el número de respuestas por segundo es 40 o 50 veces el número de computadoras en la red – que podrían ser cientos o miles. Esto son suficientes datos como para congestionar incluso un enlace T-1.

Una forma de evitar que un ataque smurf use una red como blanco de emisión es cancelando la capacidad de transmitir tráfico broadcast en el enrutador. La mayoría de los enrutadores le permiten hacerlo. Para evitar que la red sea víctima de la dirección IP falsa, el muro de fuego debe estar configurado para filtrar los paquetes ping en arribo.

Bomba UDP/ Snork UDP

Un atacante puede usar el Protocolo de Datagramas del Usuario (UDP) y uno de los varios servicios que sirven de eco a los paquetes en recepción para crear una congestión en la red que ocasione una denegación del servicio al generar un torrente de paquetes UDP entre los dos sistemas objetivos. Por ejemplo, el servicio UDP Chargen en la primera computadora, que es una herramienta de prueba que genera una serie de caracteres por cada paquete que recibe, envía paquetes al servicio de eco UDP de otro sistema, que sirve de eco a cada carácter que recibe. El UDP Chargen se encuentra en el puerto 19. Explotando estas herramientas de prueba, un interminable flujo de ecos va y viene entre los dos sistemas, congestionando la red. A veces esto se denomina *tormenta de paquetes UDP* o *bomba UDP*.

Además del puerto 7, el puerto eco, un atacante puede usar el puerto 17, la cuota del servicio diario (quotd) o el servicio de tiempo en un día en el puerto 13. Estos servicios también sirven de eco a los paquetes que reciben. El deshabilitar en cada computadora los servicios UDP innecesarios (especialmente aquellos mencionados anteriormente) o utilizar un muro de fuego para filtrar esos puertos o servicios lo protege a Usted de este tipo de ataque.

El *ataque snork* es similar a la bomba UDP. Emplea una trama UDP que tiene un puerto fuente, el 7 (eco) o el 9 (chargen) con un puerto de destinación 135 (servicio de locación de Microsoft). El resultado es el mismo de la bomba UDP – un torrente de transmisiones innecesarias que pueden disminuir el rendimiento o colapsar los sistemas involucrados.

Ataques Teardrop

El *ataque Teardrop* funciona un tanto diferente al del Ping de la Muerte, pero con resultados similares. El programa teardrop crea fragmentos IP, que son pedazos de un paquete IP en los que un paquete original se puede dividir a medida que viaja a través de Internet. El problema es que los campos offset de estos fragmentos, que se supone indiquen la porción (en bytes) del paquete original contenido en el fragmento, coinciden.

Por ejemplo, normalmente dos campos offset de los fragmentos podrían aparecer como se muestra seguidamente:

Fragmento 1: (offset) 100 – 300
Fragmento 2: (offset) 301 – 600

Eso indica que el primer fragmento contiene del byte 100 al 300 del paquete original y el segundo fragmento contiene del 301 al 600.

Los campos offset coincidentes se asemejan a esto:

Fragmento 1: (offset) 100 – 300
Fragmento 2: (offset) 200 – 400

Cuando la computadora destino trata de reensamblar estos paquetes, es incapaz de hacerlo y podría colapsar, bloquearse o reiniciarse.

Las variaciones incluyen:

- NewTear
- Teardrop2
- SynDrop
- Boink

Todos esos programas generan alguna suerte de coincidencia de fragmentos.

Para más información sobre estas variaciones, véase *Un Análisis de Ataques de Fragmentación*, por Jason Anderson, en rr.sans.org/tretas/frag_attacks.php.

Explotaciones SNMP

El SNMP se usa para monitorear los dispositivos de redes y administrar redes. Es un conjunto de protocolos que utiliza mensajes llamados *Unidades de Datos de Protocolo* (PDU) a través de la red hacia varias máquinas o dispositivos que tienen instalado el software *agente* SNMP. Estos agentes mantienen las Bases de Información de Gestión (MIB) que contienen información sobre el dispositivo. Cuando los agentes reciben los PDU, responden con información del MIB.

Se han descubierto vulnerabilidades en algunas implementaciones del SNMP que le dan a los atacantes la posibilidad de deshabilitar los dispositivos o crear un DoS.

Nota

Para más información sobre las explotaciones SNMP, véase los siguientes artículos:

- Vulnerabilidad del SNMP Representa una Amenaza Importante (www.vnunet.com/news/1129218)
- Alerta SNMP 2002: ¿De qué se trata? (http://rr.sans.org/protocols/SNMP_alert.php)

Ataques de Enrutamiento Fuente

El TCP/IP soporta el *enrutamiento fuente* que es un medio de permitir que el remitente de datos de la red enrute los paquetes a través de un punto específico en la red. Existen dos tipos de enrutamiento fuente:

- **Enrutamiento fuente estricto** El remitente de los datos puede especificar la ruta exacta (raramente utilizado)
- **Ruta record de fuente flexible (LSRR)** El remitente puede especificar ciertas rutas (saltos) a través de las cuales debe pasar el paquete.

La ruta fuente es una opción en el encabezado IP que le permite al remitente anular decisiones de enrutamiento que normalmente son tomadas por los enrutadores entre las máquinas fuente y de destino. Los administradores de redes usan el enrutamiento fuente para trazar la red o para resolver problemas de enrutamiento y comunicaciones. También se puede utilizar para forzar el tráfico a través de una ruta que proporcionará el mejor rendimiento. Desafortunadamente, el enrutamiento fuente puede ser explotado por los hackers.

Si el sistema permite el enrutamiento fuente, un intruso puede usarlo para acceder a direcciones internas privadas en la LAN que normalmente no serían accesibles desde Internet, enrutando el tráfico a través de otra máquina que es accesible desde Internet y desde la máquina interna. El enrutamiento fuente se puede deshabilitar en la mayoría de los enrutadores para prevenir este tipo de ataque.

Otras Explotaciones de Protocolos

Los ataques que hemos analizado hasta ahora incluyen la explotación de algunas características o debilidades de los protocolos TCP/IP. Los hackers también pueden explotar las vulnerabilidades de otros protocolos comunes como HTTP, DNS, Pasarela de Interfaz Común (CGI) y otros protocolos comúnmente empleados.

Explotaciones de Aplicaciones

Las *explotaciones de softwares de aplicaciones* son aquellas que se aprovechan de las debilidades de programas de aplicaciones específicos. Estas debilidades se denominan a menudo *fallas*. Al igual que las explotaciones de protocolos, los intrusos utilizan las explotaciones de aplicaciones para obtener acceso no autorizado a computadoras o redes o para colapsar o bloquear los sistemas con el fin de denegarle el servicio a otros.

Explotaciones de las Fallas

Las “fallas” comunes se pueden dividir en las siguientes categorías:

- **Inundaciones del Buffer** Muchas de las lagunas de seguridad comunes se basan en problemas de inundación del buffer. Esto ocurre cuando el número de bytes o entrada de caracteres excede el máximo permitido por el programa.
- **Entrada inesperada** Los programadores podrían no tomar medidas para definir qué pasa si ocurre una entrada no válida (una entrada que no se corresponde con las especificaciones del programa). Esto podría ocasionar que el programa colapse o abra una vía hacia el sistema.
- **Fallas de configuración** En realidad estas no son “fallas” en sí, sino modos de configurar el software dejándolo vulnerable a la penetración.

Softwares populares como Microsoft Internet Information Server (IIS), Internet Explorer (MSIE) y Outlook Express (MSOE) son los blancos favoritos de los hackers que buscan lagunas de seguridad en softwares para explotarlas. Los controles de ActiveX, JavaScript y VBScript se pueden usar para adicionar animaciones o applets a sitios Web o mensajes electrónicos, pero los hackers pueden explotar estas características para escribir controles o guiones que les permitan, desde un puesto remoto, plantar virus, acceder a datos, cambiar o borrar ficheros en el disco duro de usuarios ingenuos que visiten la página o abran el correo electrónico y corran el guión.

Los vendedores de softwares importantes sacan regularmente al mercado parches de seguridad para solucionar el problema de las fallas explotables. Resulta muy importante para los administradores de redes mantenerse actualizados en la aplicación de estas soluciones para asegurar que sus sistemas estén lo más seguros posible. Las siguientes secciones se acercan a algunos de los ataques populares que explotan los softwares de aplicaciones.

Bombas de correo

Una *bomba de correo* es una forma de sobrecargar un servidor de correo, ocasionando que este deje de funcionar y por ende, deniegue el servicio a los usuarios. Una bomba de correo es una forma relativamente simple de ataque realizado al enviar una cantidad masiva de correos a un usuario o sistema específico. Programas disponibles en los sitios de hackeo en Internet le permiten a un usuario lanzar fácilmente un ataque de bomba de correo, mandando automáticamente torrentes de correos a una dirección específica mientras protege la identidad del atacante. Varios tipos de técnicas de bombardeo de correo se pueden usar contra el popular programa Sendmail, incluyendo bombas en cadena, bombas de mensajes de error, canales de distribución encubiertos y abuso de bombarderos de correo. Para explicaciones técnicas detalladas sobre estas técnicas, véase www.silkroad.com/papers/html/bomb.

Una variación en la bomba de correo subscribe automáticamente al usuario víctima a cientos o miles de listas de correo de gran volumen en Internet, lo que llena la carpeta de entrada y/o el servidor de correo del usuario. Los bombarderos denominan este ataque *list linking* (vinculación a listas). Ejemplos de estos programas de bombas de correo incluyen Unabomber, Extreme Mail, Avalanche, Voodoo y Kaboom.

La solución para los ataques de bomba de correo repetidos es bloquear el tráfico de la red que los origina usando filtros de paquetes. Desafortunadamente, esta solución no funciona con la vinculación a listas porque la dirección del que la origina está encubierta. La avalancha de tráfico proviene de las listas de correo a las que la víctima ha sido inconscientemente suscrito.

Explotaciones del Visualizador

Los visualizadores Web son programas de softwares clientes como el MSIE, Netscape y Opera que se conectan a servidores que corren softwares de servidores Web como el IIS o Apache y solicitan páginas Web a través de un URL que es una dirección “amistosa” que representa una dirección IP y ficheros específicos del servidor en esa dirección. El visualizador recibe ficheros que están codificados (generalmente en HTML) y debe interpretar el código o “marca” que determina cómo se visualizará la página en el monitor del usuario. Los visualizadores están abiertos a varios tipos de ataque.

Características del Visualizador Explotable

Los primeros programas de visualización eran bastante simples, pero los visualizadores actuales son complejos. Ellos son capaces no sólo de visualizar textos y gráficos, sino también de reproducir ficheros de sonido, películas y correr códigos ejecutables. El software visualizador, generalmente, también almacena información acerca de la computadora en la cual está instalado e incluso acerca del usuario (datos almacenados como cookies en el disco duro local) que pueden ser transferidos a servidores Web – deliberadamente por el usuario o en respuesta al código de un sitio Web.

Todas estas características sirven a propósitos útiles. El soporte para correr códigos (en calidad de “contenido activo” tales como Java, Javascript y ActiveX) le permite a los diseñadores Web crear páginas que interactúen con los usuarios en modos sofisticados. Las cookies les permiten a los usuarios establecer preferencias en sitios que permanecerán la próxima vez que ellos los visiten. Sin embargo, los hackers pueden explotar estas características de muchas maneras. Por ejemplo, un hacker puede programar un sitio Web para que corra códigos que transfieran un virus a la computadora cliente a través del visualizador, que borren ficheros claves del sistema, o planten un programa de “puerta trasera” que le permita al hacker tomar el control del sistema del usuario. El Capítulo 8 “Implementando el Sistema de Seguridad” analiza el contenido activo y otros temas sobre la seguridad del visualizador, y ofrece consejos sobre cómo deshabilitar estas opciones cuando no son necesarias y hacer más seguros los visualizadores populares.

Spoofing de la Web

Es una forma mediante la cual un atacante es capaz de ver e incluso hacer cambios a páginas Web que se transmiten hacia o desde otra computadora (la máquina objetivo). Estas páginas incluyen información confidencial como números de tarjetas de crédito introducidos en formularios comerciales en línea y contraseñas que se usan para acceder a sitios Web restringidos. Javascript se puede emplear para enrutar páginas Web e información a través de la computadora del atacante, que se hace pasar por el servidor Web de destino. El atacante le puede enviar a la víctima correos electrónicos que contengan un enlace con la página falsa, o poner un enlace en un popular motor de búsqueda. El SSL no necesariamente previene esta suerte de ataque de “hombre por el medio”. La conexión aparenta ser segura para el usuario víctima porque *es segura*. El problema es que la conexión segura es con otro sitio, no con el que la víctima piensa que se está conectando. La *falsificación de hipervínculos* explota el hecho de que el SSL no verifica los hipervínculos que sigue el usuario, de modo que si un usuario llega a un sitio siguiendo un enlace, el usuario puede ser enviado a un sitio falso que aparenta ser legítimo.

La falsificación de la Web o spoofing de la Web es una variante altamente tecnológica del arte de estafar. El objetivo de la estafa es engañar al usuario para que le dé información confidencial como números de tarjetas de crédito, números de cuentas bancarias o números de Seguridad Social a una entidad que el usuario cree legítima y entonces usar esa información con fines criminales como el robo de identidad o el fraude con tarjetas de crédito. La única diferencia entre este estafador y el del “mundo real” que toca a la puerta de la víctima y simula ser del banco pidiendo información de la cuenta, radica en la tecnología utilizada para llevarla a cabo.

Nota

Para más detalles técnicos acerca de la falsificación de la Web y de hipervínculos, véase el documento de Frank O'Dwyer en www.brd.ie/papers/sslpaper/sslpaper.html

y el de Felten, Balfanz, Dean y Wallach en www.cs.princeton.edu/sip/pub/spoofing.pdf.

Podrían existir pistas que le podrían indicar a una víctima observadora que un sitio Web no es lo que aparenta ser, como el URL o la línea de estado del visualizador. Sin embargo, el atacante puede usar Javascript para cubrir sus trazas modificando esos elementos. Un atacante puede incluso llegar tan lejos como para usar Javascript con el fin de reemplazar la barra de menú del visualizador por una que parezca la misma, pero que reemplace funciones que den pistas para la invalidación de la página tales como la visualización del código fuente de la página.

Versiones posteriores de los softwares de visualización han sido modificadas para dificultar la falsificación de la Web. Sin embargo, muchas personas del mundo comercial continúan usando la versión 3 de MSIE o Netscape que son altamente vulnerables a este tipo de ataque.

Explotaciones del Servidor Web

Los servidores Web hospedan páginas Web disponibles para otros a través de Internet o de una red interna. Los servidores Web públicos (aquellos accesibles desde Internet) representan siempre un riesgo de seguridad inherente porque ellos deben estar disponibles en Internet a fin de hacer lo que se supone que hagan. Los clientes (softwares de visualización de la Web) deben ser capaces de enviar transmisiones al servidor Web con el propósito de solicitar páginas Web. Sin embargo, permitir que las transmisiones entren a la red y vayan al servidor Web torna al sistema – y a toda la red, a menos que se hayan tomado medidas para aislar el servidor Web del resto de la red interna – vulnerable a los atacantes.

Las aplicaciones del servidor Web, al igual que otros softwares, pueden contener fallas que se pueden explotar. Por ejemplo, en el año 2001, se descubrió un error en el software IIS de Microsoft (incluido en Windows NT, 2000 y XP) que explotaba el código usado para indexar. El componente fue instalado por defecto. Cuando corría, los hackers podían crear inundaciones del buffer para tomar control del servidor Web y cambiar páginas Web o atacar al sistema para derrumbarlo. Rápidamente, Microsoft sacó parches de seguridad con el objetivo de solucionar el problema, pero muchas compañías no mejoraron su software o no lo actualizaron con soluciones disponibles y se siguieron encontrando lagunas de seguridad nuevas y diferentes en todos los programas importantes del servidor Web. Se encontraron fallas significativas en el lenguaje de guiones PHP de los servidores Web Apache que explotadas por un atacante, podían traer como resultado que el atacante corriera el código arbitrario en el sistema. Existen parches de seguridad para solucionar este tema. Estos son solo unos pocos ejemplos de cómo los servidores Web pueden ser explotados, por eso resulta de vital importancia que esas máquinas estén seguras.

Analizaremos más detalladamente en el Capítulo 8 la implementación de la seguridad en los servidores Web.

Inundaciones del Buffer

Un *buffer* es una especie de área de almacenamiento de datos. Para acelerar el procesamiento, muchos programas de software usan un buffer de memoria para almacenar los cambios a los datos, entonces la información en el buffer se copia en el disco. Cuando se introduce más información en el buffer de la que es capaz de manejar, ocurre *una inundación del buffer*. Las inundaciones pueden ser causadas deliberadamente por hackers y después explotadas para correr códigos maliciosos.

Existen dos tipos de inundaciones: *inundaciones de la pila* e *inundaciones del heap* (*área de memoria dinámicamente reservada por la aplicación*). La pila y el heap son dos áreas de la estructura de la memoria que se asignan cuando corre un programa. Las llamadas de función se almacenan en la pila y las variables asignadas dinámicamente se almacenan en el heap. Una cantidad específica de memoria se le asigna al buffer. Los atacantes pueden usar las inundaciones del buffer en el heap para sobrescribir una contraseña, el nombre de un fichero u otros datos. Si se sobrescribe el nombre de un fichero, se abrirá un fichero diferente. Si se trata de un fichero ejecutable, correrán códigos que no tenían que correr. En sistemas UNIX, el código del programa substituido es generalmente el intérprete de comandos que le permite al atacante ejecutar comandos con privilegios de Súper usuario. En sistemas Windows, el código de inundación se puede usar para enviar una solicitud HTTP para descargar códigos maliciosos que elija el atacante.

Las inundaciones del buffer se basan en la forma en que funciona el lenguaje de programación C. Muchas llamadas de funciones no verifican para asegurarse de que el buffer sea lo suficientemente grande como para soportar los datos copiados en él. Los programadores pueden usar llamadas que hagan esta verificación con el objetivo de evitar inundaciones, pero muchos no lo hacen.

Crear un ataque de inundación del buffer requiere que el hacker comprenda el lenguaje ensamblador, así como los detalles técnicos acerca del sistema operativo para poder escribir el código de reemplazo en la pila. Sin embargo, el código para estos ataques se publica a menudo, de modo que otros con menos conocimientos técnicos pueden utilizarlo. Algunos tipos de muro de fuego, denominados muros de fuego de *inspección del estado*, dejan pasar ataques de inundación del buffer, mientras que las *puertas de enlace de aplicaciones* (debidamente configuradas) pueden filtrar la mayoría de los ataques de inundación. Analizaremos detalladamente los muros de fuego en el Capítulo 7 “Comprendiendo la Prevención del Crimen Cibernético”.

Explotaciones del Sistema Operativo

Algunas explotaciones son únicas para un sistema operativo o una familia de sistemas operativos en particular. Estos hackeos explotan características específicas del código del sistema operativo para llevar a cabo el ataque. Todos los sistemas operativos tienen sus propias vulnerabilidades.

El Ataque WinNuke Fuera de Banda

El *ataque fuera de banda (OOB)* es uno que explota una vulnerabilidad en algunas redes Microsoft, así que a veces es denominado la *falla OOB de Windows*. El programa WinNuke y variaciones como Sinnerz y Muerte crean una transmisión de datos OOB que colapsa la máquina a la que son enviados. Funciona así: Se establece una conexión TCP/IP con la dirección IP objetivo, usando el puerto 139 (el puerto NetBIOS). Entonces el programa envía datos usando un indicador llamado MSG_OOB (o Urgente) en el encabezado del paquete. Este indicador instruye al Winsock de la computadora para que envíe datos llamados *datos fuera de banda*. Al recibir este indicador, el servidor de Windows objetivo espera un puntero en el lugar del paquete donde terminan los datos Urgentes a los que le siguen datos normales, pero el puntero OOB en el paquete creado por WinNuke apunta al final de la trama, sin que le sigan más datos.

La máquina Windows no sabe cómo manejar esta situación y cesa las comunicaciones en la red. Se le deniega el servicio a todos los usuarios que después de eso traten de comunicarse con ella. Un ataque WinNuke generalmente requiere que se reinicie el sistema afectado para restablecer las comunicaciones de la red.

Windows 95 y NT 3.51 y 4.0 son vulnerables a la explotación WinNuke, a menos que se hayan instalado las soluciones de Microsoft. Windows 98/ME y Windows 2000/XP no son vulnerables al WinNuke. Desafortunadamente, muchas redes aún usan los antiguos sistemas operativos de Microsoft, a veces sin actualizar los parches y paquetes de servicios.

Ataques al Registro de Windows

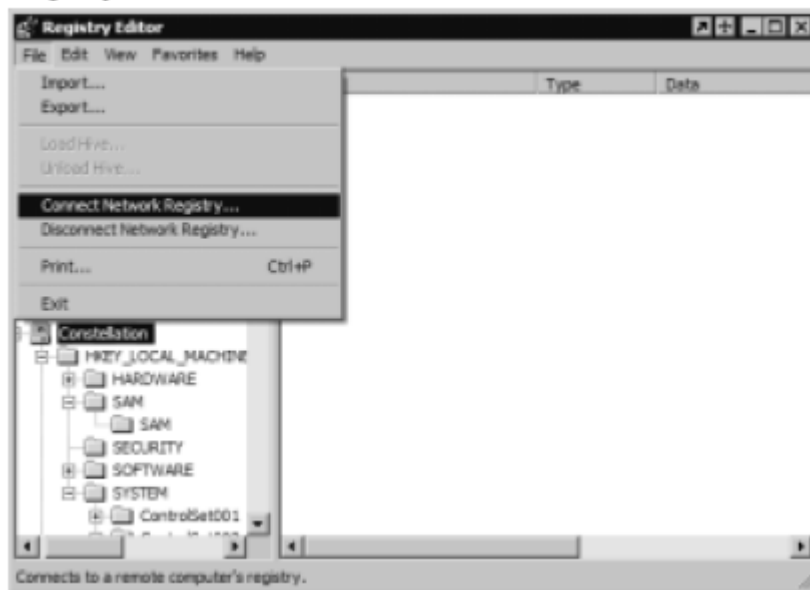
El Registro de Windows en Windows 9x/ME y NT/2000/XP (o sea, todos los sistemas operativos posteriores a Windows 3.x) es una base de datos en la que se almacena la información de inicialización y la configuración del sistema y de las aplicaciones más importantes. Tener esta información centralizada en un lugar en vez de esparcida en múltiples ficheros de configuración e inicialización ofrece muchos beneficios, pero también hace que el Registro sea vulnerable a hackers y atacantes.

Las herramientas Regedit y Regedt32 le permiten al usuario conectarse al Registro en un sistema remoto a través de la red y hacer cambios a la configuración del mismo, como se muestra en la Figura 6.4. Un hacker puede explotar esta posibilidad y alterar informaciones importantes que podrían echar abajo el sistema. Se necesitan privilegios administrativos para editar registros remotos y Usted no puede editar el Registro de una computadora con Windows 95/98 a menos que se le haya habilitado explícitamente la administración remota, instalando el servicio de Registro remoto. Esto lo pueden hacer los administradores usando un fichero por lotes durante la aparición de una gran cantidad de máquinas Windows 9x.

Puede resultar difícil detectar ataques al registro, porque el sistema accede al registro muy a menudo, complicando el proceso de monitoreo. Sin embargo, utilidades como RegMon se pueden utilizar para rastrear datos de acceso al registro, los que se pueden comparar con modelos comunes de ataques.

Figura 6.4 La utilidad Regedit se puede utilizar para conectarse y editar el Registro de un sistema remoto.

Figure 6.4 The Regedit utility can be used to connect to and edit a remote system's Registry.



Otras Explotaciones de Windows

Se han descubierto muchas vulnerabilidades en los sistemas operativos de Windows. Microsoft es, por lo general, rápida en hacer parches para esas vulnerabilidades, una vez conocidas. Muchas de las vulnerabilidades del sistema operativo son causadas por inundaciones del buffer en aplicaciones implícitas como Monitor de Red, el servicio SNMP y el servicio Universal Plug and Play (UPnP). Otras se crean al instalar programas de software específicos en Windows o provienen de fallas de seguridad en el visualizador Web MSIE. Aquí tienen algunas de las fallas de seguridad más interesantes que se han descubierto en Windows 2000:

- Al renombrar la torre de CD-ROM u otra unidad desmontable se crea automáticamente una correspondencia administrativa para la nueva torre. Aunque esta correspondencia no es visible en el visualizador de la red, no se requiere de una contraseña para acceder a ella si su nombre es conocido. El problema fue solucionado en Service Pack 2, pero los usuarios de Windows 2000 que no tengan este paquete de servicios son vulnerables.
- El servicio de Protocolo de Transferencia de Noticias (NNTP) en Windows NT 4.0 y 2000 tiene una falla de programación que ocasiona un escape de memoria que un atacante puede explotar para agotar toda la memoria del servidor y crear un DoS. Microsoft sacó al mercado un parche para solucionar este problema.
- Una falla de programación le permitía a los hackers comenzar un proceso de autenticación NTLM con un servidor Telnet remoto, causando que las credenciales del

usuario fueran enviadas a través de la red cuando un usuario hacía clic en un enlace de un documento HTML. Se sacó al mercado un parche para solucionar este problema.

Nota

Para una buena lista de las conocidas vulnerabilidades de seguridad de Windows 2000, véase el sitio Web www.labmice.net/articles/win2000securityholes.htm. Para listados de explotaciones que se pueden usar con Linux, Macintosh y varias versiones de UNIX (así como Windows), véase el sitio Web El Mundo de las Explotaciones: www.insecure.org/sploits.html.

Explotaciones UNIX

Muchas explotaciones de UNIX/Linux apuntan a obtener acceso raíz. En UNIX, la cuenta raíz es el equivalente de la cuenta del Administrador en un sistema de Windows. Un usuario que se valide con la cuenta raíz tiene control total sobre el sistema y puede borrar los registros para cubrir sus trazas. “Llegar a la raíz” se trata a menudo de encontrar un fichero que tenga permisos de Súper usuario (SUID) y correr un guión (que se puede descargar de sitios de hackers en la Web) o explotar fallas en Sendmail o algún otro servicio.

Ataques a la cuenta raíz

A pesar de su nombre, un *ataque a la cuenta raíz* no es un método de obtener privilegios de cuenta raíz – al menos, no directamente. Es un grupo de programas que instalan un sustituto de validación Troyano con una puerta trasera, junto a un rastreador de paquetes en carpetas UNIX. El rastreador puede usarse para capturar el tráfico de la red, incluyendo las credenciales de usuarios, dándole al usuario acceso a la cuenta raíz al validarse con credenciales legítimas. Se encuentran disponibles softwares como Rkdet para detectar la instalación de dichos programas o de rastreadores de paquetes corriendo en un sistema UNIX.

Explotaciones del NFS

El Sistema de Ficheros de la Red (NFS) le permite a los usuarios, desde un puesto remoto, montar discos en otras computadoras en aras de acceder a ficheros del sistema remoto. Esto torna disponibles a los ficheros del disco remoto a través de la red. Un programa llamado nfsbug se puede utilizar para probar diferentes métodos de montar un disco NFS con el objetivo de determinar si la computadora remota está configurada de modo que permita el montaje remoto. Si funciona, esto le permite al atacante el acceso pleno al sistema de ficheros remoto. Entonces el atacante puede leer o escribir en todos los ficheros.

Otras Explotaciones UNIX

Los sistemas operativos *nix, al igual que sus primos Windows, son vulnerables a una variedad de explotaciones de inundación del buffer, configuraciones implícitas inseguras y fallas de programación que los hackers pueden usar para comprometer los sistemas y las redes. Para una lista de vulnerabilidades en distribuciones específicas de UNIX y Linux, incompleta, pero bastante abarcadora, véase el sitio Web de seguridad de UNIX: www.cs.iastate.edu/%7eghelfer/unixsecurity/unix_vuln.html.

Explotaciones del Enrutador

Ahora muchos hackers escogen para sus ataques a los enrutadores en lugar de a las computadoras. La creciente popularidad de DSL y de la conectividad a Internet por cable han traído a los enrutadores hacia las redes caseras, así como hacia las comerciales. Esto, a su vez, ha creado un nuevo punto de vulnerabilidad.

Muchos de los nuevos y relativamente no costosos enrutadores diseñados para conexiones de banda ancha vienen con contraseñas de administrador implícitas que se pueden usar en cualquiera de los dispositivos del vendedor si el administrador no las cambia. Esto significa que un hacker con conocimiento de la contraseña implícita podría validarse y hacerle cambios a la tabla de enrutamiento o a la configuración del enrutador, y difiere de la mayoría de los sistemas operativos que no vienen con una contraseña implícita, sino que requieren que el usuario cree una durante la instalación. Además de la contraseña del administrador, algunos vendedores de enrutadores han creado contraseñas especiales de “puerta trasera” para sus sistemas, concebidas para ser usadas por el personal de apoyo técnico de los vendedores; en caso de que un administrador se olvide de la contraseña de administración, el vendedor puede ayudar al administrador a entrar. Por supuesto, este sistema también puede ser explotado por hackers con conocimiento de la contraseña “maestra” secreta.

Los hackers también pueden obtener las contraseñas de los enrutadores del mismo modo en que obtienen las de las computadoras: empleando un software rastreador o espía, ataques de fuerza bruta, o tácticas de ingeniería social. Cualquiera que sea el método que utilice el hacker para acceder al enrutador, él o ella puede crear ataques DoS al cambiar las entradas de la tabla de enrutamiento para enviar todos los mensajes a un mismo destino. De hecho, si el enrutador usa el Protocolo de Información de Enrutamiento para actualizar dinámicamente sus tablas de enrutamiento, al atacante puede enviar mensajes RIP falsos con el fin de hacerle los cambios a la tabla de enrutamiento sin necesitar siquiera acceder directamente al enrutador.

Los ataques DoS también pueden estar dirigidos a los enrutadores. Al apagar el enrutador se detiene la comunicación entre la subred y el mundo exterior. Cisco anunció en el 2001 que sus 12000 enrutadores serie eran vulnerables a ataques DoS.

Para más información acerca de la creciente popularidad de las explotaciones de enrutadores, véase www.vnunet.com/News/1126398.

Prevención y Respuesta

Los administradores pueden tomar una serie de medidas para ayudar a prevenir explotaciones de protocolos, aplicaciones y sistemas operativos, incluyendo las siguientes:

- Asegurar que todos los sistemas tengan los parches de seguridad más recientes. Aplicar estos parches protege de muchos ataques DoS que se basan en “fallas” de los protocolos o de los sistemas operativos.
- Los sistemas Linux pueden protegerse de los ataques SYN construyendo el corazón con cookies SYN. Algunas versiones de UNIX (como Solaris 2.6 y posteriores) tienen incluida una protección contra ataques SYN. En Windows 2000, se puede editar el Registro para protegerse contra este ataque. Para información e instrucciones, véase <http://security.uchicago.edu/seminars/DDoS/netprot.shtml>.
- Los enrutadores se pueden configurar para responder a broadcasts dirigidos en lugar de pasarlos a la subred para protegerse de los ataques smurf.
- Los servidores DNS se pueden configurar para que respondan con una respuesta “de negación” cuando reciben preguntas DNS de fuentes sospechosas o inesperadas para protegerse de ataques DoS al DNS.
- El enrutador se puede configurar para filtrar paquetes en arribo con una dirección IP fuente que parezca ser de la red local.
- Configurar el sistema para ignorar redirecciones del enrutador.
- Deshabilitar el SNMP, si no es necesario, protege contra explotaciones que se basan en el protocolo.
- Deshabilitar Java, Javascript, ActiveX y otro contenido activo en el visualizador Web frustra explotaciones comunes del visualizador.
- Usar muros de fuego en la puerta de enlace de las aplicaciones para protegerse contra ataques de inundación del buffer.
- Cambiar las contraseñas implícitas en los enrutadores y deshabilitar las contraseñas de “puerta trasera”.

Atacando con Troyanos, Virus y Gusanos

Los intrusos que acceden a las redes y los sistemas sin autorización o los atacantes internos con motivos maliciosos pueden plantar varios tipos de programas para causarle daño a la red. Estos programas – a menudo agrupados bajo el término general *virus*, aunque existen otras variedades – les han costado a compañías e individuos billones de dólares por concepto de pérdida de datos, productividad, del tiempo y el gasto de la recuperación. Algunos de los ejemplos más destructivos de códigos maliciosos, a veces también referidos como *malware* (*softwares maliciosos*), en la última década son:

- **CIH/Chernobyl** A finales de los 90, este virus le causó un gran daño a usuarios de computadoras caseras y comerciales. Infectaba ficheros ejecutables y se esparcía al correr un fichero infectado en una máquina de Windows 95/98. Existían varias variantes del CIH. Estos eran virus “bomba de tiempo” que se activaban en una fecha predefinida (el 26 de abril – Aniversario del Desastre de Chernobyl – o el 26 de cada mes). Hasta la fecha

prevista, el virus permanecía dormido. Una vez que el reloj interno de la computadora indicaba la fecha de activación, el virus sobrescribía los primeros 2048 sectores de todos los discos duros de la computadora, borrando la tabla de ubicación de ficheros y ocasionando que el disco duro apareciese como borrado. Sin embargo, los datos en el resto del disco se podían recuperar usando el software de recuperación de datos. Muchos usuarios ignoraban esta posibilidad. El virus también intentaba escribir el bloque de inicio del BIOS, dejando a la computadora incapaz de reiniciarse. (Esto no funcionaba en computadoras configuradas para prevenir la escritura en el BIOS). Este virus comenzó a aparecer nuevamente en la primavera del 2002, a costas del virus Klez que se describirá posteriormente en esta lista.

- **Melissa** Este fue el primer virus que se diseminó ampliamente a través del correo electrónico, a partir de Marzo de 1999. Es un virus macro, escrito en Visual Basic para Aplicaciones (VBA) e incrustado en un documento de Microsoft Word 97/2000. Cuando se abre el documento infectado, el macro se ejecuta (a menos que Word no esté configurado para correr macros), enviándose a sí mismo a las primeras 50 entradas de cada libreta de direcciones MAPI de Microsoft Outlook. Esto incluye las direcciones de la lista de correos, lo que podía traer como resultado una rápida propagación del virus. El virus también le hacía cambios a la plantilla Normal.dot, lo que causaba que se infectaran los documentos Word creados recientemente. Debido al enorme volumen de correos que este producía, el virus causaba una denegación del servicio en algunos servidores de correo electrónico. El autor confeso del virus, David Smith, fue sentenciado a 20 meses en una prisión federal y multado con \$5,000usd.

- **Código Rojo** En el verano del 2001, el gusano de auto-propagación comenzó a infectar servidores Web que corrían IIS (Servidor de Información de Internet). En varias fechas de activación, la máquina infectada trataría de conectarse al puerto 80 TCP (usado para los servicios Web) en computadoras con direcciones IP seleccionadas al azar. Si lo lograba, trataba de infectar los sistemas remotos. Algunas variaciones también desfiguraban páginas Web almacenadas en el servidor. En otras fechas, la máquina infectada lanzaría ataques DoS contra una dirección IP específica incrustada en el código. CERT reportó que el Código Rojo infectó a más de 250,000 sistemas en el curso de 9 horas el 19 de julio de 2001.

- **Nimda** A finales del verano del 2001, el gusano Nimda infectó a numerosas computadoras que corrían Windows 95/98/ME, NT y 2000. El gusano hacía cambios a documentos Web y ficheros ejecutables en los sistemas infectados y creaba múltiples copias de sí mismo. Se expandía vía correo electrónico, a través del compartimiento en la red y a través del acceso a sitios Web infectados. También explotaba vulnerabilidades en las versiones 4 y 5 del IIS y se diseminaba de las máquinas clientes hacia los servidores Web a través de las puertas traseras dejadas por el gusano Código Rojo II. Nimda le permitía a los atacantes ejecutar comandos arbitrarios en máquinas IIS que no habían sido parcheadas y se producía una denegación del servicio por causa de las actividades del gusano.

- **Klez** A finales del 2001 y principios del 2002, este gusano de correo electrónico se disemina a través de Internet. Se propaga a través de correos masivos y explota

vulnerabilidades en las versiones no parcheadas de clientes de correo Outlook y Outlook Express, intentando correr cuando se hace una vista previa del mensaje que lo contiene. Cuando corre, se copia a sí mismo en la carpeta Sistema o Sistema32 en el directorio raíz del sistema y modifica una clave del Registro para provocar ser ejecutado al iniciarse Windows. También trata de deshabilitar cualquier escáner de virus y envía copia de sí mismo a direcciones en la libreta de direcciones de Windows en forma de nombre de fichero aleatorio con una extensión doble (por ejemplo, file.doc.exe). La carga explosiva se ejecuta el día 13 un mes sí y otro no, a partir de Enero, trayendo como resultado que los ficheros de las torres locales y mapeadas tengan 0 bytes de longitud.

Estos son sólo unos ejemplos del daño y de los inconvenientes causados por varias formas de códigos maliciosos. Existen tres categorías amplias de este tipo de código identificado como *Troyanos* o *programas de caballo Troyano*, *virus* y *gusanos*. En las siguientes secciones analizaremos brevemente estos tipos de ataques.

Troyanos

El nombre *Troyano* es la abreviatura de *caballo Troyano* y se refiere a un programa de software que simula realizar una función útil, pero que, en realidad, realiza acciones no concebidas o ignoradas por el usuario del programa. Los caballos Troyanos son escritos a menudo por hackers para eludir la seguridad de un sistema. Una vez instalado el Troyano, el hacker puede explotar las lagunas de seguridad que este crea para obtener acceso no autorizado, o el programa Troyano podría realizar alguna acción como:

- Borrar o modificar ficheros
- Transmitir ficheros al intruso a través de la red
- Instalar otros programas o virus

Básicamente, el Troyano puede realizar cualquier acción que el usuario con privilegios y permisos pueda hacer en el sistema. Esto significa que un Troyano es especialmente peligroso si el usuario ingenuo que lo instala es un administrador y tiene acceso a ficheros del sistema.

¡Atención!

Aunque los documentos de Microsoft Office no son por sí mismos ficheros ejecutables, pueden contener *macros*, que son pequeños programas incrustados en los documentos y que se pueden usar para expandir códigos maliciosos. Por ende, los documentos de Office deben ser tratados como si fueran ejecutables, a menos que la opción de correr macros esté deshabilitada en el programa de Office.

Los Troyanos pueden ser disfrazados muy inteligentemente como programas inocuos, utilidades o protectores de pantalla. Un Troyano también puede ser instalado por un guión ejecutable (JavaScript, un applet de Java, control ActiveX, etc.) en un sitio Web. Al acceder al sitio, se puede iniciar la instalación del programa si el visualizador Web está configurado para permitir que los guiones corran automáticamente. Los Troyanos pueden usar el comportamiento implícito de Windows para disfrazar su verdadera naturaleza.

Como la extensión del fichero (los caracteres que aparecen después del último punto en un nombre de fichero) está oculta por defecto, un hacker puede nombrar un fichero, por ejemplo, vacation.jpg.exe y en el Explorador de Windows aparecerá como vacation.jpg, simulando ser un fichero de gráficos inocente cuando, en realidad, es un programa ejecutable.

Por supuesto, al dar doble clic para abrir la “imagen”, el programa correrá. Los Troyanos que están diseñados para permitir que un hacker obtenga acceso no autorizado a través de la red (tales como Back Orifice y NetBus) se denominan, en ocasiones, *Troyanos de acceso remoto* o *RATs*.

Para más información sobre los Troyanos en general y vínculos a soluciones específicas para contrarrestar el ataque de Troyanos, véase www.irchelp.org/irchelp/security/trojan.html.

Virus

Los *virus* son programas que, generalmente, son instalados sin el conocimiento del usuario y realizan acciones indeseadas que, a menudo, son dañinas, aunque a veces sólo son fastidiosas. Los virus se pueden reproducir por sí mismos, infectando a otros sistemas al escribirse a sí mismos en cualquier disquete que se use en la computadora o enviándose a través de la red. Los virus, a menudo, se distribuyen como anexos a correos electrónicos o como macros en documentos de procesamiento de texto. Algunos se activan inmediatamente con la instalación y otros permanecen dormidos hasta una fecha u hora específica o un evento en particular del sistema que los hace estallar. Para más información, véase el artículo *Cómo Funcionan los Virus de Computadora* en www.howstuffworks.com/virus.htm.

Los virus vienen en miles de variedades. Ellos pueden hacer cualquier cosa, desde aparecer un mensaje que diga ¡Hola! hasta borrar todo el contenido del disco duro de una computadora. La proliferación de virus de computadora ha conducido también al fenómeno de las *bromas sobre virus*, que es una advertencia – generalmente circulada a través del correo electrónico o sitios Web – acerca de un virus que no existe o que no hace lo que la advertencia dice que hará.

Sin embargo, los virus reales representan una verdadera amenaza para Su red. Compañías como Symantec y McAfee desarrollan softwares antivirus dirigidos a detectar y borrar programas de virus. Como se crean virus diariamente, es importante descargar regularmente nuevos *ficheros de definición de virus*, que contienen la información requerida para detectar todos los tipos de virus, a fin de asegurarse de que Su protección contra virus esté actualizada.

Los tipos de virus incluyen:

- **Virus del sector de inicio** Estos son transmitidos, a menudo, a través de un disquete. El virus es escrito en el archivo maestro de inicio en el disco duro, de donde se carga hacia la memoria de la computadora cada vez que se inicia el sistema.
- **Virus de programas o aplicaciones** Estos son programas ejecutables que al correr infectan Su sistema. Los virus también se pueden anexar a otros programas inocuos e instalarse a la misma vez que se instala el programa deseado.
- **Virus macros** Estos están incrustados en documentos (tales como documentos de Microsoft Word) que pueden usar macros, pequeñas aplicaciones o “applets” que automatizan la ejecución de alguna tarea o secuencia.

En la escena....

Comprendiendo la Amenaza que representan los Virus

El aspecto más peligroso de los virus de computadora (como sucede con sus equivalentes biológicos) es su capacidad de “mutar” y convertirse en otra cosa. Por supuesto, esta mutación no ocurre espontáneamente, sino que los escritores de virus se basan en el código de otros para hacer de virus relativamente benignos otros más destructivos – y evitar la detección por softwares antivirus.

Virus que están programados para “estallar” (activarse y destruir datos o ficheros) en una fecha determinada se denominan *bombas de tiempo* o *bombas lógicas*. Uno de los primeros de este tipo en atraer la atención mundial fue el virus Michelangelo a principios de los 90, que intentaba borrar los discos duros de PC infectadas el 6 de marzo, el cumpleaños del famoso pintor. Pocos años después, un antiguo empleado descontento de Omega Engineering plantó un virus bomba de tiempo en la red de la compañía que trajo como resultado aproximadamente 10 millones de dólares por concepto de pérdidas y daños. Fue acusado y sentenciado a 41 meses en prisión.

Gusanos

Un *gusano* es un programa que puede viajar a través de una red de una computadora a otra. A veces, partes diferentes de un gusano corren en diferentes computadoras. Los gusanos hacen copias múltiples de sí mismos y se diseminan a través de una red. La diferencia entre los virus y los gusanos se ha tornado borrosa. Originalmente el término *gusano* se usaba para describir códigos que atacaban a sistemas multiusuarios (redes), mientras que *virus* describía a programas que se multiplicaban en computadoras individuales.

El propósito primario de un gusano es reproducirse. Estos programas fueron usados inicialmente con fines legítimos para llevar a cabo tareas de administración de redes, pero su capacidad de multiplicarse rápidamente ha sido explotada por los hackers que crean

gusanos maliciosos que se reproducen indiscriminadamente y que pueden explotar las debilidades de los sistemas operativos y realizar otras acciones dañinas.

Nota

Uno de los primeros programas gusano ampliamente diseminado fue el Gusano de Internet de 1988, que prácticamente apagó toda la Internet. Para un documento detallado sobre cómo sucedió esto, véase *Un Tour alrededor de El Gusano* en <http://world.std.com/~frank/worm.html>.

Prevención y Respuesta

Proteger sistemas y redes del daño causado por Troyanos, virus y gusanos es principalmente un asunto de sentido común. Prácticas que pueden ayudar a prevenir la infección incluyen estas:

- No correr ficheros ejecutables (.exe) procedentes de fuentes desconocidas, incluyendo aquellos anexados a correos electrónicos o descargados de sitios Web.
- Deshabilitar las opciones de Vista Previa y/o HTML en Su programa cliente de correo electrónico.
- No abrir documentos de Microsoft Office procedentes de fuentes desconocidas sin deshabilitar previamente las macros.
- Ser cuidadosos en el uso de disquetes que han sido usados en otras computadoras.
- Instalar y emplear softwares de muro de fuego.
- Instalar softwares antivirus, configurándolos para que corran automáticamente cada cierto tiempo y actualicen regularmente los ficheros de definición.
- Usar herramientas de prevención contra intrusos llamadas *bloqueadoras de comportamiento* que le deniegan a los programas la posibilidad de ejecutar operaciones que no han sido permitidas explícitamente.
- Usar soluciones de *detección de comportamiento* como SurfinGate de Finjan y SurfinShield que pueden utilizar técnicas heurísticas para analizar ficheros ejecutables y evaluar si estos podrían ser hostiles.
- Utilizar softwares *analizadores de integridad* (como Tripwire) para escanear el sistema en busca de cambios.

Reconocer la presencia de códigos maliciosos es el primer paso – respuesta si el sistema resulta infectado. Los administradores y usuarios necesitan estar alertas a indicaciones comunes de la existencia de un virus, como por ejemplo, ficheros o programas faltantes, cambios inexplicables a la configuración del sistema, visualizaciones, mensajes o sonidos inesperados e inexplicables, ficheros o programas nuevos que aparecen de repente sin explicación, “escapes” de memoria (menos disponibilidad de la memoria del sistema de lo normal), o el uso inexplicable de espacio en disco y cualquier otro comportamiento extraño de programas o del sistema operativo. Si se sospecha que es un virus, se debe instalar un buen programa antivirus y correrlo para escanear el sistema en busca de virus e intentar borrar o poner en cuarentena los que se encuentren. Finalmente, se debe hacer regularmente una copia de seguridad de todos los datos importantes o irremplazables para el caso en que todas estas medidas fallen.

Algunos escritores de virus crean virus de “prueba de concepto” que no causan daños y que están diseñados meramente para demostrar que se puede escribir un tipo particular de virus. Por ejemplo, una vez se pensó que los virus no se podían diseminar con sólo leer un correo electrónico. Se les dijo a los usuarios que mientras no abrieran los anexos, estarían seguros. Los primeros virus en explotar los correos HTML para correr e infectar sistemas cuando un usuario abría el mensaje de correo (no un anexo) demostraron el concepto de un virus que podía diseminarse también a través del mensaje de correo electrónico. En Junio del 2002, los investigadores de McAfee recibieron un virus de prueba de concepto denominado Perrun que se decía estar incrustado en un fichero imagen JPEG. De ser genuino, este fue el primer caso conocido de un virus incrustado en un fichero imagen que corre automáticamente cuando se visualiza el gráfico. Ese mismo mes, Symantec reportó el primer virus de plataforma en cruz que podía infectar a ambos sistemas: Linux y Windows.

Algunos comentaristas técnicos han puesto en duda la veracidad de estos nuevos virus, pero muchos técnicos una vez también le aseguraron a los usuarios que los virus no podían diseminarse a través del correo electrónico. La moraleja de la historia es que los escritores de virus son un grupo creativo y persistente que continuará apareciéndose con nuevas formas de hacer lo “imposible” para que los usuarios de computadoras nunca asuman que un tipo de fichero en particular o un sistema operativo es inmune a códigos maliciosos. El único modo seguro de protegerse contra virus es apagar la computadora y dejarla apagada.

Nota

En www.symantec.com y www.mcafee.com podrá encontrar información acerca de virus específicos e instrucciones sobre cómo limpiar un sistema infectado. Ambos vendedores de antivirus ofrecen bases de datos detalladas que enumeran y describen virus conocidos.

Hackeando para los No Técnicos

Como hemos mencionado, las personas que quieren entrar en sistemas de computadoras y redes ya no necesitan tener habilidades técnicas altamente desarrolladas para ello. Algunos dicen que el hackeo fue, originalmente, un arte que requería un gran talento, después sólo un poco de habilidades y hoy día lo puede hacer cualquiera que tenga suficiente coordinación mano/ojo como para hacer clic con el ratón. Para decirlo de un modo más elocuente: “El Hackeo pasó de ser una labor de amor a una labor no especializada”. Este proceso de deterioro comenzó con el fenómeno de los *script kiddies*.

El Fenómeno de los Script Kiddies

Usted encontrará una docena de definiciones de *script kiddie*, en dependencia de la fuente que consulte. Webopedia (www.webopedia.com) define el término como alguien que “al azar busca una debilidad específica en Internet con el fin de obtener acceso raíz a un sistema sin comprender realmente qué es lo que él o ella está explotando, porque la debilidad fue descubierta por otra persona”. El Jargo Lexicon en

www.tuxedo.org/~esr/jargon es un poco más sentencioso: “La forma más baja del cracker Personas que no pueden programar pero que crean páginas HTML de mal gusto copiando rutinas Javascript de otras páginas HTML de mal gusto”.

Sin tener en cuenta una definición precisa, la mayoría concuerda en una cosa: Los script kiddies no tienen mucha pericia técnica, pero usan códigos escritos por otros para causar estragos. En la cultura de los hackers, ellos son vistos, por lo general, con desdén o, al menos, con poco respeto. Sin embargo, los hackers que sí entienden de tecnología continúan distribuyendo guiones y programas que los script kiddies utilizan para hacer su trabajo sucio.

De acuerdo con el Instituto SANS (<http://rr.sans.org/hackers/monkeys.php>), los script kiddies y sus primos, los *monos de paquetes* (definidos como personas que lanzan ataques DoS contra sitios Web sin “razón aparente”), son la nueva generación de hackers responsable de muchos de los ataques DDoS de gran escala en los años recientes, incluyendo aquellos que derrumbaron Yahoo!, eBay, ZDNet y CNN. El ataque a Yahoo! fue lanzado por un adolescente canadiense llamado “Chico de la Mafia” que usó una utilidad denominada Stacheldraht, escrita por un hacker alemán.

Los hackers “reales” pasan años jugando con sistemas de computadoras y conociendo las interioridades de los complejos sistemas operativos; a menudo prefieren trabajar con UNIX. Ellos se enorgullecen de sus conocimientos y de la “elegancia” de sus ataques. Ven a los script kiddies, que se basan en guiones escritos por otros e incluso se rebajan a usar herramientas de hackeo con interfaces gráficas, casi de la misma manera en un maestro del robo de joyas ve a un matón callejero. Como los script kiddies no son calificados (y, por ende, menos capaces de cubrir sus trazas) y como tienden a ansiar atención (mientras que la mayoría de los hackers calificados se enorgullecen de ser capaces de invadir furtivamente un sistema y salir sin que nadie lo sepa), los script kiddies conforman una gran proporción de los intrusos de redes y atacantes que son capturados y procesados.

A pesar de su irrespetuoso apodo y del bajo nivel de consideración que se les tiene dentro de la comunidad de los hackers, los script kiddies pueden hacer mucho daño y el orden aleatorio de sus ataques los hace especialmente peligrosos. Como sucede con los disparos procedentes de vehículos en movimiento que alcanzan víctimas al azar, las acciones de los script kiddies son imposibles de predecir y ponen en riesgo a todos.

El Hacker que “Señala y Hace Clic”

Tan poco sofisticados como son los script kiddies, otra variedad de hackers “principiantes” es aún menos calificada desde el punto de vista técnico. Al menos el script kiddie promedio conoce lo suficiente como para teclear algunos comandos a fin de lanzar el guión que él o ella obtuvo de otro. La más nueva encarnación de los atacantes “por la vía fácil” es demasiado ignorante – o demasiado perezosa – incluso para hacer eso. En su lugar, esta nueva generación usa utilidades de “señala y haz clic” con bellas interfaces gráficas o sitios Web con “completa los espacios en blanco” que sirven de fachada para lanzar el o los

ataques escogidos contra objetivos específicos sin que el así llamado hacker necesite saber siquiera cómo descargar un fichero.

David Rhoades de Maven Security se apareció con el término *clic kiddies* para describir a estos “rebeldes sin causa”. Rhoades viaja por todo el mundo y se presenta en conferencias sobre seguridad informática con su trabajo “Hackeando para las Masas”. En su exposición, él subraya cuán fácil es, literalmente, para cualquiera cometer allanamiento en línea – y mucho peor – con herramientas fáciles de conseguir que, parafraseando a Rhoades, son tan fáciles de usar por el usuario que incluso Su abuela podría echar abajo varios servidores antes de la cena.

El uso de las herramientas de ataque con base en la Web, favorables para los script kiddies, también dificulta el rastreo del origen del ataque, ya que el ataque procede de un intermediario (el sitio Web que ofrece la herramienta) en lugar de venir directamente del atacante.

Nota

Una versión en línea de la presentación de Rhoades “Hackeando para las Masas”, que incluye ejemplos de las herramientas con base en la Web que él analiza, está disponible para visualizar o descargar en su sitio Web: <http://www.clickkiddie.net>.

Prevención y Respuesta

Las mismas medidas de seguridad que ya hemos analizado aplican para proteger una red contra hackers no calificados técnicamente. Además, los script kiddies pueden, a veces, ser atraídos y capturados colocándoles un *tarro de miel*, que es un sistema diseñado específicamente para atrapar atacantes. El tarro de miel es un sistema o una red que actúa como una “invitación abierta” para los hackers. Está conectado a Internet con protección mínima, corriendo sistemas operativos no parcheados y softwares de aplicación que se pueden explotar fácilmente. Los sistemas son constantemente monitoreados, de modo que el atacante puede ser identificado y rastreado antes de que él o ella tenga la oportunidad de destruir la evidencia.

Analizaremos más detalladamente los tarros de miel en el Capítulo 9 “Implementando Técnicas de Detección de Crímenes Cibernéticos”.

Resumen

La gran cantidad de formas en que un hacker puede entrar o atacar a una red puede ser abrumadora. Tan pronto como se elimina una “laguna” de seguridad, se descubren o se crean docenas más de ellas. Algunos de esos métodos son tan sutiles que nadie se percataría nunca de que la seguridad de la red ha estado comprometida. Otros son tan obvios que *cualquiera* lo sabría al instante.

Los atacantes abarcan desde personas encantadoras con muchas “aptitudes humanas” que pueden persuadir a los usuarios legítimos para que les den las credenciales que ellos

necesitan a fin de entrar en el sistema, hasta “niños prodigio” desde el punto de vista técnico que pueden explotar las características de protocolos de redes, aplicaciones y sistemas operativos y hackers “principiantes” técnicamente no sofisticados que usan guiones, herramientas GUI y sitios Web creados por otros para llevar a cabo sus ataques. Los ataques pueden abarcar desde la denegación del servicio que interrumpe las comunicaciones en toda la red hasta virus “benignos” que no hacen más que sacar una ventana con un mensaje fastidioso. En muchos casos, el objetivo de un ataque es plantar una “puerta trasera” en el sistema que le permita al hacker entrar nuevamente cuando quiera.

La buena noticia es que los profesionales de las redes pueden tomar muchas medidas para prevenir explotaciones técnicas en sus sistemas. De hecho, aplicar todos los parches, soluciones, paquetes de servicio y otras mejoras actuales y correr buenos softwares antivirus con definiciones de fichero de virus actualizadas los ayudará a mantener a raya a los intrusos y atacantes. La mala noticia es que los administradores deben estar siempre vigilantes para protegerse de las nuevas amenazas que aparecen diariamente. El estado del hackeo ha alcanzado el punto en que cualquiera que quiera lanzar un ataque puede hacerlo y la incidencia del “hackeo de pasada” se ha incrementado con la llegada de herramientas de hackeo fáciles de usar.

Preguntas Realizadas con Frecuencia

Las siguientes preguntas realizadas con frecuencia, respondidas por los autores de este libro, están diseñadas para medir su comprensión de los conceptos presentados en este capítulo y para ayudarle con la implementación de estos conceptos en la vida real. Para hacer que el autor conteste a sus preguntas, visite www.syngress.com/solutions y haga clic en el formulario “**Pregúntale al autor**”.

P: ¿Por qué las herramientas descritas en este capítulo – utilidades de escaneo de puertos, rastreadores de paquetes, dispositivos de registro de tecleos, etc. – no son ilegales para crear o descargar?

R: Muchas de estas herramientas tienen usos legítimos. Resulta especialmente importante para los administradores de la red y asesores de seguridad ser capaces de usar las herramientas de escaneo para determinar dónde están las vulnerabilidades en sus propias redes o en las redes de sus clientes en aras de tomar las medidas apropiadas para “fortalecer” los sistemas. Después de todo, si las herramientas de escaneo fueran ilegales, sólo los bandidos tendrían herramientas de escaneo.

Esas utilidades – al igual que muchas otras cosas – pueden usarse de forma ofensiva o defensiva. Los dispositivos de registro de tecleos y otros “espías” pueden ser útiles en situaciones en las que el monitoreo de las actividades del usuario es legal y apropiado – por ejemplo, para que los empleadores lleven cuenta de lo que los empleados están haciendo en la red (especialmente si el empleador pudiera ser visto como responsable de esas actividades) y para que los padres ejerzan control sobre las actividades en línea de sus hijos.

P: ¿Si una compañía tiene instalado un buen muro de fuego, eso no la protegerá de todos esos ataques?

R: No, los productos de muro de fuego son muy útiles para controlar qué entra o sale de una red. Pero un muro de fuego es como una computadora (en muchos casos, un muro de fuego es una computadora especializada). Sólo hace lo que la persona que lo configura le dice que haga. Algunos tipos de ataques son reconocidos y no pueden ser detenidos por muros de fuego, pero otros explotan las características de los protocolos comúnmente usadas para comunicaciones legítimas de la red, y los paquetes podrían parecer sólo un bit benigno de datos destinado para una computadora en la red interna. Troyanos, virus y gusanos entran a la red como anexos de correos electrónicos o a través del compartimiento remoto de ficheros. Los muros de fuego no los capturarán, pero un buen programa antivirus, actualizado con frecuencia y configurado para escanear todos los correos en arribo, podría ser capaz de hacerlo. Muchas compañías parecen operar bajo la asunción de que instalar un muro de fuego es casi como invocar un conjuro mágico que emite un campo de fuerza de protección alrededor de sus redes, dejándolas completamente inmunes al ataque. Incluso el mejor muro de fuego no protegerá contra ataques de ingeniería social, tampoco hará ningún bien contra atacantes internos que tengan acceso físico a la red. Estudios han mostrado que un gran número de crímenes relacionados con redes son en realidad “trabajos internos”. En el próximo capítulo, Usted verá en detalles cómo funcionan los muros de fuego, lo que hará más fácil comprender porqué no son la solución “panacea” para la seguridad de la red que a veces piensan que es.

P: ¿Cómo funciona exactamente la ingeniería social? ¿Por qué alguien revelaría su contraseña a un extraño? ¿Esto sucede realmente?

R: Sí, realmente sucede – y más seguido de lo que Usted podría pensar. Los ingenieros sociales calificados son buenos estafadores; son maestros en hacer que otras personas confíen en ellos. En grandes compañías, los empleados a menudo no están personalmente familiarizados con los otros empleados, de modo que resulta relativamente fácil para el ingeniero social entrar paseándose o incluso llamar por teléfono y persuadir a un usuario de que él o ella es un miembro del Departamento Informático y que necesita la contraseña de usuario. El ingeniero social podría tener una historia convincente, diciendo, por ejemplo, que un hacker entró al sistema y descubrió todos los ficheros de contraseñas y que ahora el Departamento Informático necesita conocer las contraseñas antiguas para reponerlas y suministrar nuevas a fin de protegerse contra el hacker. Al igual que los estafadores, el ingeniero social generalmente juega con las emociones humanas comunes. Por ejemplo, el ingeniero exagerará el peligro, dirá que el hacker puede acceder y destruir todos los datos de los usuarios si el “informático” no obtiene inmediatamente la contraseña y hace el cambio. En otros casos, el ingeniero podría explotar otras emociones, como el deseo natural de las personas de ayudar al decirles que el “informático” tendrá problemas con el “gran jefe”, quizás incluso pierda el trabajo si él o ella no es capaz de obtener la información requerida sobre las contraseñas. Los ingenieros sociales son muy capaces de apelar al ego del usuario o simular interés sexual/romántico en el usuario para obtener la contraseña. Aunque algunos no la clasificarían como ingeniería social, existe otra técnica que se trata sencillamente de espiar al usuario para obtener la contraseña (“surfeando sobre su hombro” o mirar por encima del hombro del usuario mientras este la teclea) o revisar los

documentos del usuario para encontrar la contraseña. Un hacker de triste fama, Kevin Mitnik dijo: “Usted puede tener la mejor tecnología, muros de fuego, sistemas de detección de intrusos, dispositivos biométricos. Todo lo que se necesita es llamar a una empleada ingenua y tendrás todo lo que escribió, bebé. Ellas lo consiguen todo.” Visite http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci771517,00.html para tener más información sobre este tópico.

P: Creo entender las diferencias entre un virus, un Troyano y un gusano. Pero, ¿qué son todos esos otros tipos de virus de los que he oído hablar: virus furtivos, virus polimorfos, virus blindados y virus de cavidad?

R: Los *virus furtivos* son capaces de ocultar los cambios que les hacen a los ficheros, registros de inicio y similares de los programas antivirus. Esto lo hacen falsificando los resultados de un intento del programa de leer los ficheros infectados. Un *virus polimorfo* hace copias de sí mismo para expandirse, al igual que otros virus, pero las copias no son exactamente como el original. El virus “se metamorfosea” en algo ligeramente diferente, en un esfuerzo por evitar la detección por un software antivirus que quizás no tenga definiciones para todas las variaciones. Los virus pueden usar un “motor de mutación” para crear esas variaciones en ellos mismos. Un *virus blindado* usa una técnica que dificulta la comprensión del código del virus. Un *virus de cavidad* es capaz de sobrescribir parte del fichero (de la máquina) infectada, pero no incrementa la longitud del fichero, lo que sería un indicio claro de que un virus ha infectado al fichero. Todas estas y más clasificaciones de virus se describen en la sección Preguntas Realizadas con Mayor Frecuencia sobre Virus de Nick FitzGerald localizada en www.safetynet.com/support/kbvfaq.asp#SB. Aunque algo desactualizado en relación con virus específicos, este sitio contiene alguna información básica buena que conforma una base para estudios modernos sobre virus.

Referencias

- *Estrategias para Combatir Ataques Distribuidos*
<http://razor.bindview.com/publish/papers/strategies.html>
- *CERT Advertencias sobre Ataques Automatizados*
www.vnunet.com/News/1130755
- *La PaSsWord Rusa de los Crackers: ejemplos de softwares gratis de crackeo*
www.password-crackers.com/crack.html
- *Todo lo que Usted Quería Saber sobre La Ingeniería Social – Pero que Temía Preguntar*
www.happyhacker.org/uberhacker/se.html
- *Sección FAQ sobre el Hackeo no Oficial de redes Netware*
http://nmrc.org/faqs/netware/nw_sec02.html#02-1
- *Spoofing de la Web: Un Engaño en Internet (el documento Princenton)*

www.cs.princeton.edu/sip/pub/spoofing.pdf

- *Instituto SANS: Panorámica sobre el DNS con Análisis del Spoofing del DNS*
<http://rr.sans.org/DNS/DNS.php>
- *Escaneo de Puertos: Ya No Es Sólo Una Herramienta Ofensiva*, por Gary Kessler
www.garykessler.net/library/is_tools_scan.html
- *Principios Éticos y Legalidad del Escaneo de Puertos*, por Shaun Jamieson
<http://rr.sans.org/audit/ethics.php>
- *Encontrando Cercas en el Ciberespacio: Privacidad, Propiedad y Acceso Abierto en Internet*, por Ethan Preston
<http://grove.ufl.edu/~techlaw/vol6/Preston.html>
- *Principios Básicos del Orificio Trasero*
www.nwinternet.com/~pchelp/bo/bobasics.htm
- *Bombas de Correo Electrónico y Medidas de Contención: Ataques Cibernéticos Disponibles y Daños a la Integridad*
www.silkroad.com/papers/html/bomb
- *Conocidas Vulnerabilidades de Seguridad de Windows 2000*
www.labmice.net/articles/win2000securityholes.htm
- *El Mundo de las Explotaciones: Explotaciones para varios sistemas operativos*
www.insecure.org/sploits.html
- *Servidores con Enrutadores Surpass para Ataques de Hackers*, por James Middleton
www.vnunet.com/News/1126398
- *Cómo funcionan los Virus Informáticos*, por Marshall Brain
www.howstuffworks.com/virus.htm
- *El Gusano de Internet de 1988: Un Tour alrededor del Gusano*
<http://world.std.com/~franl/worm.html>
- *Script Kiddies y Monos de Paquete – La Nueva Generación de “Hackers”*, por Denis Dion
<http://rr.sans.org/hackers/monkeys.php>
- *Conoce a tu Enemigo: Las Herramientas y Metodologías del Script Kiddie*, del Proyecto Honeynet (red de miel)
<http://project.honeynet.org/papers/enemy>
- *Hackeando para las Masas*, presentación realizada por David Rhoades, Maven Security
www.clickkiddie.net

- *Script Kiddies: Quiénes son y Qué están Haciendo?*, por Andrew Stephens
<http://rr.sans.org/hackers/kiddies.php>
- *UNIX, Técnicas Forenses para Respuestas ante Incidentes*
www.incident-response.org
- *Ciencia Forense aplicada a la Computación: Introducción a Respuestas ante incidentes e Investigación de Windows NT/2000*
http://rr.sans.org/incident/comp_forensics3.php