hackers

INTRODUCCIÓN

Los piratas ya no tienen un parche en su ojo ni un garfio en reemplazo de la mano. Tampoco existen los barcos ni los tesoros escondidos debajo del mar. Llegando al año 2001, los piratas se presentan con un cerebro desarrollado, curioso y con muy pocas armas: una simple computadora y una línea telefónica. **Hackers**. Una palabra que aún no se encuentra en los diccionarios pero que ya suena en todas las personas que alguna vez se interesaron por la informática o leyeron algún diario. Proviene de "hack", el sonido que hacían los técnicos de las empresas telefónicas al golpear los aparatos para que funcionen. Hoy es una palabra temida por empresarios, legisladores y autoridades que desean controlar a quienes se divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información indebida.

Sólo basta con repasar unas pocas estadísticas. Durante 1997, el 54 por ciento de las empresas norteamericanas sufrieron ataques de Hackers en sus sistemas. Las incursiones de los piratas informáticos, ocasionaron pérdidas totales de 137 millones de dólares en ese mismo año. El Pentágono, la CIA, UNICEF, la ONU y demás organismos mundiales han sido víctimas de intromisiones por parte de estas personas que tienen muchos conocimientos en la materia y también una gran capacidad para resolver los obstáculos que se les presentan. Un hacker puede tardar meses en vulnerar un sistema ya que son cada vez más sofisticados. Pero el lema es viejo: hecha la ley, hecha la trampa.

Los medios de comunicación masivos prefieren tildarlos de delincuentes que interceptan códigos de tarjetas de crédito y los utilizan para beneficio propio. También están los que se intrometen en los sistemas de aeropuertos produciendo un caos en los vuelos y en los horarios de los aviones. Pero he aquí la gran diferencia en cuestión. Los **crackers** (crack=destruir) son aquellas personas que siempre buscan molestar a otros, piratear software protegido por leyes, destruir sistemas muy complejos mediante la transmisión de poderosos virus, etc. Esos son los crackers. Adolescentes inquietos que aprenden rápidamente este complejo oficio. Se diferencian con los Hackers porque no poseen ningún tipo de ideología cuando realizan sus "trabajos". En cambio, el principal objetivo de los Hackers no es convertirse en delincuentes sino "pelear contra un sistema injusto" utilizando como arma al propio sistema. Su guerra es silenciosa pero muy convincente.

La cultura popular define a los hackers como aquellos que, con ayuda de sus conocimientos informáticos consiguen acceder a los ordenadores de los bancos y de los negociados del gobierno. Bucean por información que no les pertenece, roban software caro y realizan transacciones de una cuenta bancaria a otra. Los criminólogos, por otra parte, describen a los hackers en términos menos halagadores. Donn Parker los denomina "violadores electrónicos" y August Bequai los describe como "vándalos electrónicos". Ambos, aunque aseveran que las actividades de los hackers son ilegales, eluden hábilmente llamarlos "criminales informáticos". Hacen una clara distinción entre el hacker que realiza sus actividades por diversión y el empleado que de repente decide hacer algo malo. Por tanto, parece que tenemos una definición en la que caben dos extremos: por un lado, el moderno ladrón de bancos y por otro el inquieto. Ambas actividades (y todas las intermedias) son calificadas con el mismo termino. Difícilmente se podría considerar esto como un ejemplo de conceptualización precisa. Una gran parte de esta ambigüedad puede seguirse desde el origen durante estos aproximadamente 20 años de vida del mencionado termino. El termino comenzó a usarse aplicándolo a un grupo de pioneros de la informática del MIT, a principios de la década de 1960. Desde entonces, y casi hasta finales de la década de 1970, un hacker era una persona obsesionada por conocer lo mas posible sobre los sistemas informáticos. Los diseñadores del ordenador Apple, Jobs y Wozniack, pueden considerarse hackers en este sentido de la palabra. Pero a principios de la década de 1980, influenciados por la difusión de la película Juegos de Guerra, y el ampliamente publicado arresto de una "banda de hackers" conocida como la 414, los hackers pasaron a ser considerados como chicos jóvenes capaces de violar sistemas informáticos de grandes empresas y del gobierno. Desgraciadamente, los medios de información y la

comunidad científica social no ha puesto mucho esfuerzo por variar esta definición. El problema para llegar a una definición mas precisa radica, tanto en la poca información que hay sobre sus actividades diarias, como en el hecho de que lo que se conoce de ellos no siempre cabe bajo las etiquetas de los delitos conocidos. Es decir, no hay una definición legal que sea aplicable a los hackers, ni todas sus actividades conllevan la violación de las leyes. Esto lleva a que la aplicacion del termino varie segun los casos, dependiendo de los cargos que se puedan imputar y no a raíz de un claro entendimiento de lo que el termino significa. Este problema, y la falta de entendimiento de lo que significa ser un hacker, convierte a esta en una etiqueta excesivamente utilizada para aplicar a muchos tipos de intrusiones informáticas. Parker y Bequai, dos lideres en el estudio de los delitos informáticos, utilizan el termino "hacker" de formas ligeramente diferentes. Parker reconoce que hacking no abarca todo el rango de actividades asociadas a la violación de los sistemas informáticos, pero lo prefiere al termino "phreaking", que considera muy oscuro. Por otra parte, Bequai no rechaza el termino "phreaking" y a menudo lo aplica a hechos que Parker califica como de hacker. Bequai confunde aun mas el termino al definir al hacker como alguien que utiliza ilegalmente las tarjetas de crédito telefónico para acceder a sistemas que distribuyen software comercial ilegalmente. Veremos que esto tiene poco que ver con las actuaciones propias de los hackers, pero es ilustrativa de otros tipos de actividades informáticas inusuales.

Los términos, "hacker", "phreaker" y "pirata" se presentan y definen tal y como los entienden aquellos que se identifican con estos papeles.

DESARROLLO

CARACTERÍSTICAS DE LOS HACKERS Y DE LOS PHREAKERS

En primer lugar, el área de los hackers. En la tradición de esta comunidad informática, el hacker puede realizar dos tipos de actividades: bien acceder a un sistema informático, o bien algo mas general, como explorar y aprender a utilizar un sistema informático. En la primera connotación, el termino lleva asociados las herramientas y trucos para obtener cuentas de usuarios validos de un sistema informático, que de otra forma serian inaccesibles para los hackers. Se podría pensar que esta palabra esta intimamente relacionada con la naturaleza repetitiva de los intentos de acceso. Además, una vez que se ha conseguido acceder, las cuentas ilícitas a veces compartidas con otros asociados, denominándolas "frescas". He aquí la visión estereotipada de los medios de comunicación de los hackers un joven de menos de veinte años, con conocimientos de informática, pegado al teclado de su ordenador, siempre en busca de una cuenta no usada o un punto débil en el sistema de seguridad. Aunque esta visión no es muy precisa, representa bastante bien el aspecto del termino. La segunda dimensión del mencionado termino se ocupa de lo que sucede una vez que se ha conseguido acceder al sistema cuando se ha conseguido una clave de acceso. Como el sistema esta siendo utilizado sin autorización, el hacker no suele tener, en términos generales, acceso a los manuales de operación y otros recursos disponibles para los usuarios legítimos del sistema. Por tanto, el usuario experimenta con estructuras de comandos y explora ficheros para conocer el uso que se da al sistema. En oposición con el primer aspecto del termino, aquí no se trata solo de acceder al sistema (aunque alguno podría estar buscando niveles de acceso mas restringidos), sino de aprender mas sobre la operación general del sistema. Contrariamente a lo que piensan los medios de comunicación, la mayoría de los hackers no destruyen y no dañan deliberadamente los datos. El hacerlo iría en contra de su intención de mezclarse con el usuario normal y atraería la atención sobre su presencia, haciendo que la cuenta usada sea borrada. Después de gastar un tiempo sustancioso en conseguir la cuenta, el hacker pone una alta prioridad para que su uso no sea descubierto. Además de la obvia relación entre las dos acepciones, la palabra "hacker" se reserva generalmente a aquellos que se dedican al segundo tipo. En otras palabras, un hacker es una persona que tiene el conocimiento, habilidad y deseo de explorar completamente un sistema informático. El mero hecho de conseguir el acceso (adivinando la clave de acceso) no es suficiente para conseguir la denominación. Debe haber un deseo de liderar, explotar y usar el sistema después de haber accedido a él. Esta distinción parece lógica, ya que no todos los intrusos mantienen el interés una vez que han logrado acceder al sistema. En el submundo informático, las claves de acceso y las cuentas suelen intercambiarse y ponerse a disposición del uso general. Por tanto, el hecho de conseguir el acceso puede considerarse como la parte "fácil", por lo que

aquellos que utilizan y exploran los sistemas son los que tienen un mayor prestigio. La segunda actividad es la de los phreakers telefónicos. Se convirtió en una actividad de uso común cuando se publicaron las aventuras de John Draper, en un articulo de la revista Esquire, en 1971. Se trata de una forma de evitar los mecanismos de facturación de las compañías telefónicas. Permite llamar a de cualquier parte del mundo sin costo prácticamente. En muchos casos, también evita, o al menos inhibe, la posibilidad de que se pueda trazar el camino de la llamada hasta su origen, evitando así la posibilidad de ser atrapado. Para la mayor parte de los miembros del submundo informático, esta es simplemente una herramienta para poder realizar llamadas de larga distancia sin tener que pagar enormes facturas. La cantidad de personas que se consideran phreakers, contrariamente a lo que sucede con los hackers, es relativamente pequeña. Pero aquellos que si se consideran phreakers lo hacen para explorar el sistema telefónico. La mayoría de la gente, aunque usa el teléfono, sabe muy poco acerca de él. Los phreakers, por otra parte, quieren aprender mucho sobre el. Este deseo de conocimiento lo resume así un phreaker activo: "El sistema telefónico es la cosa mas interesante y fascinante que conozco. Hay tantas cosas que aprender. Incluso los phreakers tienen diferentes áreas de conocimiento. Hay tantas cosas que se pueden conocer que en una tentativa puede aprenderse algo muy importante y en la siguiente no. O puede suceder lo contrario. Todo depende de como y donde obtener la información. Yo mismo quisiera trabajar para una empresa de telecomunicaciones, haciendo algo interesante, como programar una central de conmutación. Algo que no sea una tarea esclavizadora e insignificante. Algo que sea divertido. Pero hay que correr el riesgo para participar, a no ser que tengas la fortuna de trabajar para una de estas compañías. El tener acceso a las cosas de estas empresas, como manuales, etc., debe ser grandioso". La mayoría de la gente del submundo no se acerca al sistema telefónico con esa pasión. Solo están interesados en explorar sus debilidades para otros fines. En este caso, el sistema telefónico es un fin en si mismo. Otro entrevistado que se identificaba a si mismo como hacker, explicaba: "Se muy poco sobre teléfonos simplemente soy un hacker. Mucha gente hace lo mismo. En mi caso, hacer de phreaker es una herramienta, muy utilizada, pero una herramienta al fin y al cabo". En el submundo informático, la posibilidad de actuar así se agradece, luego llego el uso de la tarjeta telefónica. Estas tarjetas abrieron la puerta para realizar este tipo de actividades a gran escala. Hoy en día no hace falta ningún equipo especial. Solo un teléfono con marcación por tonos y un numero de una de esas tarjetas, y con eso se puede llamar a cualquier parte del mundo. De igual forma que los participantes con mas conocimientos y motivación son llamados hackers, aquellos que desean conocer el sistema telefónico son denominados phreakers. El uso de las herramientas que les son propias no esta limitada a los phreakers, pero no es suficiente para merecer la distinción. Finalmente llegamos a la "telepirateria" del software. Consiste en la distribución ilegal de software protegido por los derechos de autor. No nos referimos a la copia e intercambio de diskettes que se produce entre conocidos (que es igualmente ilegal), sino a la actividad que se realiza alrededor de los sistemas BBS que se especializan en este tipo de trafico. El acceso a este tipo de servicios se consigue contribuyendo, a través de un módem telefónico, con una copia de un programa comercial. Este acto delictivo permite a los usuarios copiar, o "cargar", de tres a seis programas que otros hayan aportado. Así, por el precio de una sola llamada telefónica, uno puede amontonar una gran cantidad de paquetes de software. En muchas ocasiones, incluso se evita pagar la llamada telefónica. Notese que al contrario que las dos actividades de hacker y phreaker, no hay ninguna consideración al margen de "prestigio" o "motivación" en la telepirateria. En este caso, el cometer los actos basta para "merecer" el título. La telepirateria esta hecha para las masas. Al contrario de lo que sucede con los hackers y los phreakers, no requiere ninguna habilidad especial. Cualquiera que tenga un ordenador con módem y algún software dispone de los elementos necesarios para entrar en el mundo de la telepirateria. Debido a que la telepirateria no requiere conocimientos especiales, el papel de los piratas no inspira ningún tipo de admiración o prestigio en el submundo informático. (Una posible excepción la constituyen aquellos que son capaces de quitar la protección del software comercial.) Aunque los hackers y los phreakers de la informática probablemente no desaprueben la piratería, y sin duda participen individualmente de alguna forma, son menos activos (o menos visibles) en los BBS que se dedican a la telepirateria. Tienden a evitarlos porque la mayoría de los telepiratas carecen de conocimientos informáticos especiales, y por tanto son conocidos por abusar en exceso de la red telefónica para conseguir el ultimo programa de juegos. Un hacker mantiene la teoría de que son estos piratas los culpables de la mayoría de los fraudes con tarjetas de crédito telefónicas. "Los medios de comunicación afirman que son únicamente los hackers los responsables de las perdidas de las grandes compañías de telecomunicaciones y de los servicios de larga distancia. Este no es el caso. Los hackers representan solo una

pequeña parte de estas perdidas. El resto esta causado por "los piratas y ladrones que venden estos códigos en la calle." Otro hacker explica que el proceso de intercambiar grandes programas comerciales por módem normalmente lleva varias horas, y son estas llamadas, y no las que realizan los "entusiastas de telecomunicaciones", las que preocupan a las compañías telefónicas. Pero sin considerar la ausencia de conocimientos especiales, por la fama de abusar de la red, o por alguna otra razón, parece haber algún tipo de división entre los hackers / phreakers y los telepiratas. Después de haber descrito los tres papeles del submundo informático, podemos ver que la definición presentada al principio, según la cual un hacker era alguien que usaba una tarjeta de crédito telefónico robada para cargar alguno de los últimos juegos, no refleja las definiciones dadas en el propio submundo informático. Obviamente, corresponde a la descripción de un telepirata y no a las acciones propias de un hacker o un phreaker. En todo esto hay una serie de avisos. No se quiere dar la impresión de que un individuo es un hacker, un phreaker o un telepirata exclusivamente. Estas categorías no son mutuamente excluyentes. De hecho, muchos individuos son capaces de actuar en mas de uno de estos papeles. Se cree que la respuesta se encuentra en buscar los objetivos que se han expuesto previamente. Recuérdese que el objetivo de un hacker no es entrar en un sistema, sino aprender como funciona. El objetivo de un phreaker no es realizar llamadas de larga distancia gratis, sino descubrir lo que la compañía telefónica no explica sobre su red y el objetivo de un telepirata es obtener una copia del software mas moderno para su ordenador. Así, aunque un individuo tenga un conocimiento especial sobre los sistemas telefónicos, cuando realiza una llamada de larga distancia gratis para cargar un juego, esta actuando como un telepirata. En cierto modo, esto es un puro argumento semántica. Independientemente de que a un hacker se le etiquete erróneamente como telepirata, los accesos ilegales y las copias no autorizadas de software comercial van a seguir produciéndose. Pero si queremos conocer los nuevos desarrollos de la era informática, debemos identificar y reconocer los tres tipos de actividades con que nos podemos encontrar. El agrupar los tres tipos bajo una sola etiqueta es mas que impreciso, ignora las relaciones funcionales y diferencias entre ellos. Hay que admitir, de todas formas, que siempre habrá alguien que este en desacuerdo con las diferencias que se han descrito entre los grupos. En el desarrollo de esta investigación, quedo de manifiesto que los individuos que realizan actualmente estas actividades no se ponen de acuerdo en cuanto a donde están las fronteras. Las categorías y papeles, como se ha indicado previamente, no son mutuamente exclusivos. En particular, el mundo de los hackers y los phreakers están muy relacionados.

Pero, de la misma forma que no debemos agrupar toda la actividad del submundo informático bajo la acepción de hacker, tampoco debemos insistir en que nuestras definiciones sean exclusivas hasta el punto de ignorar lo que representan. Las tipologías que he presentado son amplias y necesitan ser depuradas. Pero representan un paso mas en la representación precisa, especificación e identificación de las actividades que se dan en el submundo de la informática.

¿QUE SE NESECITA PARA SER UN HACKER?

Uno puede estar preguntándose ahora mismo si los hackers necesitan caros equipos informáticos y una estantería rellena de manuales técnicos. La respuesta es NO! ,Hackear puede ser sorprendentemente fácil, mejor todavía, si se sabe cómo explorar el World Wide Web, se puede encontrar casi cualquier información relacionada totalmente gratis.

De hecho, hackear es tan fácil que si se tiene un servicio on−line y se sabe cómo enviar y leer un e−mail, se puede comenzar a hackear inmediatamente. A continuación se podrá encontrar una guía dónde puede bajarse programas especialmente apropiados para el hacker sobre Windows y que son totalmente gratis. Y trataremos también de explicar algunos trucos de hacker sencillos que puedan usarse sin provocar daños intencionales.

LOS DIEZ MANDAMIENTOS DEL HACKER

I. Nunca destroces nada intencionalmente en la Computadora que estés crackeando.

II. Modifica solo los archivos que hagan falta para evitar tu detección y asegurar tu acceso futuro al sistema.

III. Nunca dejes tu dirección real, tu nombre o tu teléfono en ningún sistema.

IV. Ten cuidado a quien le pasas información. A ser posible no pases nada a nadie que no conozcas su voz, número de teléfono y nombre real.

V. Nunca dejes tus datos reales en un BBS, si no conoces al sysop, déjale un mensaje con una lista de gente que pueda responder de ti.

VI. Nunca hackees en computadoras del gobierno. El gobierno puede permitirse gastar fondos en buscarte mientras que las universidades y las empresas particulares no.

VII. No uses BlueBox a menos que no tengas un servicio local o un 0610 al que conectarte. Si se abusa de la bluebox, puedes ser cazado.

VIII. No dejes en ningún BBS mucha información del sistema que estas crackeando. Di sencillamente "estoy trabajando en un UNIX o en un COSMOS...." pero no digas a quien pertenece ni el teléfono.

IX. No te preocupes en preguntar, nadie te contestara, piensa que por responderte a una pregunta, pueden cazarte a ti, al que te contesta o a ambos.

X. Punto final. Puedes pasearte todo lo que quieras por la WEB, y mil cosas mas, pero hasta que no estés realmente hackeando, no sabrás lo que es.

PASOS PARA HACKEAR

1.Introducirse en el sistema que tengamos como objetivo.

2.Una vez conseguido el acceso, obtener privilegios de root (superusuario).

3.Borrar las huellas.

4.Poner un sniffer para conseguir logins de otras personas.

MÉTODOS PARA HACKEAR

En los primeros años, los ataques involucraban poca sofisticación técnica. Los insiders (empleados disconformes o personas externas con acceso a sistemas dentro de la empresa) utilizaban sus permisos para alterar archivos o registros. Los outsiders (personas que atacan desde afuera de la ubicación física de la organización) ingresaban a la red simplemente averiguando una password válida.
A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar

"agujeros" en el diseño, configuración y operación de los sistemas. Esto permitó a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevo a la

desaparición de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica (bancos, servicios automatizados, etc).

Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita conocimiento técnico básico para realizarlos. El aprendiz de intruso tiene acceso ahora a numerosos programas y scripts de numerosos "hacker" bulletin boards y web sites, donde además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

Los métodos de ataque descriptos a continuación están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras. Por ejemplo: después de crackear una password, un intruso realiza un login como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente también, el atacante puede adquirir derechos a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de huir.

ATAQUES A NUESTRA INFORMACIÓN, ¿ CUALES SON LAS AMENAZAS ?

El objetivo es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar (y desde donde), es tan importante como saber con que soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo. Sin olvidar que éstas últimas siempre son una combinación de herramientas que tienen que ver con tecnología y recursos humanos (políticas, capacitación).
Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

A esta altura del desarrollo de la "sociedad de la información" y de las tecnologías computacionales, los piratas informáticos ya no son novedad. Los hay prácticamente desde que surgieron las redes digitales, hace ya unos buenos años. Sin duda a medida que el acceso a las redes de comunicación electrónica se fue generalizando, también se fue multiplicando el número de quienes ingresan "ilegalmente" a ellas, con distintos fines. Los piratas de la era cibernética que se consideran como una suerte de Robin Hood modernos y reclaman un acceso libre e irrestricto a los medios de comunicación electrónicos.

Genios informáticos, por lo general veinteañeros, se lanzan desafíos para quebrar tal o cual programa de seguridad, captar las claves de acceso a computadoras remotas y utilizar sus cuentas para viajar por el

ciberespacio, ingresar a redes de datos, sistemas de reservas aéreas, bancos, o cualquier otra "cueva" más o menos peligrosa.

Como los administradores de todos los sistemas, disponen de herramientas para controlar que "todo vaya bien", si los procesos son los normales o si hay movimientos sospechosos, por ejemplo que un usuario esté recurriendo a vías de acceso para las cuales no está autorizado o que alguien intente ingresar repetidas veces con claves erróneas que esté probando. Todos los movimientos del sistema son registrados en archivos, que los operadores revisan diariamente.

TIPOS DE ATAQUES:

EAVESDROPPING Y PACKET SNIFFING

Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras

vías. Existen kits disponibles para facilitar su instalación.

Este método es muy utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e−mail entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

SNOOPING Y DOWNLOADING

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e−mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos mas resonantes de este tipo de ataques fueron : el robo de un archivo con mas de 1700 números de tarjetas de crédito desde una compañía de música

mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

TAMPERING O DATA DIDDLING

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por insiders o outsiders, generalmente con el propósito de fraude o dejar fuera de servicio un competidor.

Son innumerables los casos de este tipo como empleados (o externos) bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule la deuda por impuestos en el sistema municipal.

Múltiples web sites han sido víctimas del cambio de sus home page por imágenes terroristas o humorísticas, o el reemplazo de versiones de software para download por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos).

La utilización de programas troyanos esta dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet como el caso de Back Orifice y NetBus, de reciente aparición.

SPOOFING

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering. Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e−mails.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y en otro. Este proceso, llamado Looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener

muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad estan seguramente siendo atacado por un insider, o por un estudiante a miles de Km. de distancia, pero que ha tomado la identidad de otros.

El looping hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones.
Los protocolos de red también son vulnerables al spoofing. Con el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete.

El envío de falsos e−mails es otra forma de spoofing permitida por las redes. Aquí el atacante envía a nombre de otra persona e−mails con otros objetivos. Tal fue el caso de una universidad en USA que en 1998 debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina (163 estudiantes).
Muchos ataques de este tipo comienzan con ingeniería social, y la falta de cultura por parte de los usuarios para facilitar a extraños sus identificaciones dentro del sistema. Esta primera información es usualmente conseguida a través de una simple llamada telefónica.

JAMMING o FLOODING

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (o sea que este ataque involucra también spoofing). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conecciones abiertas, no dejando lugar a las conexiones legítimas.

Muchos host de Internet han sido dados de baja por el "ping de la muerte", una versión−trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el reboot o el apagado instantáneo del equipo.

Otra acción común es la de enviar millares de e−mails sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servers destino.

CABALLOS DE TROYA

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto (P.ej. Formatear el disco duro, modificar un fichero, sacar un mensaje, etc.).

BOMBAS LOGICAS

Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificara la información o provocara el cuelgue del sistema.

INGENIERA SOCIAL

Básicamente convencer a la gente de que haga lo que en realidad no debería. Por ejemplo llamar a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa convincente. Esto es común cuando en el Centro de Computo los administradores son amigos o conocidos.

DIFUSION DE VIRUS

Si bien es un ataque de tipo tampering, difiere de este porque puede ser ingresado al sistema por un dispositivo externo (diskettes) o través de la red (e−mails u otros protocolos) sin intervención directa del atacante. Dado que el virus tiene como característica propia su autoreproducción, no necesita de mucha ayuda para propagarse a traves de una LAN o WAN rápidamente, si es que no esta instalada una protección antivirus en los servidores, estaciones de trabajo, y los servidores de e−mail.
Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe, .com, .bat, etc) y los sectores de boot−particion de discos y diskettes, pero aquellos que causan en estos tiempos mas problemas son los macro−virus, que están ocultos en simples documentos o planilla de cálculo, aplicaciones que utiliza cualquier usuario de PC, y cuya difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet. Y además son multiplataforma, es decir, no están atados a un sistema operativo en particular, ya que un documento de MS−Word puede ser procesado tanto en un equipo Windows 3.x/95/98 , como en una Macintosh u otras.
Cientos de virus son descubiertos mes a mes, y técnicas más complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puertas de entrada. Por eso es indispensable contar con una herramienta antivirus actualizada y que pueda responder rápidamente ante cada nueva amenaza.

El ataque de virus es el más común para la mayoría de las empresas, que en un gran porcentaje responden afirmativamente cuando se les pregunta si han sido víctimas de algún virus en los últimos 5 años.

OBTENCIÓN DE PASSWORDS, CÓDIGOS Y CLAVES

Este método (usualmente denominado cracking), comprende la obtención "por fuerza bruta" de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En esta caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.
Es muy frecuente crackear una password explotando agujeros en los algoritmos de encriptación utilizados, o en la administracion de las claves por parte la empresa.

Por ser el uso de passwords la herramienta de seguridad mas cercana a los usuarios, es aquí donde hay que poner énfasis en la parte "humana" con políticas claras (como se define una password?, a quien se esta autorizado a revelarla?) y una administración eficiente (cada cuanto se están cambiando?)
No muchas organizaciones están exentas de mostrar passwords escritas y pegadas en la base del monitor de sus usuarios, u obtenerlas simplemente preguntando al responsable de cualquier PC, cual es su password?.

ATAQUES DE HACKERS: HECHOS DESTACABLES

En 1996, la página Web de Kriesgman (http://www.kriesgam.com/), una de las principales fábricas de pieles de Estados Unidos fue hackeada por unos chicos que pusieron carteles y frases en defensa del animal y la ecología. También en noviembre de 1996 fue asaltada la página de la Agencia Central de Inteligencia de los EE. UU (CIA) (http://www.odci.gov/cia) y en su lugar ubicaron la frase "Welcome to the Central Stupidity Agency". Las famosas cantantes inglesas de Spice Gilrs (http://www.spicegirls.com/) tampoco salieron

indemnes de esta cruzada ideológica cuando en 1997 fue modificado su site para protestar contra "la cultura pop y el uso masivo de Internet". Sin ir tan lejos, la Web principal del Ministerio de justicia local fue intervenida por el grupo **x−team**, colocando una fotografía de José Luis Cabezas el mismo día que se cumplía un año de su cruel asesinato. Debajo, se encontraba un texto donde supuestamente los funcionarios le pedían perdón al pueblo por trabar constantemente el esclarecimiento del caso. La pantalla, con la tristemente famosa mirada de Cabezas, permaneció allí 24 horas hasta que la removieron. Consultados los autores de ese hackeo dijeron que ellos "golpearon las puertas cibernéticas de la justicia".

Los Hackers pretenden que Internet sea un espacio de comunicación libre de toda censura y restricción conspirando contra todo medio contrario a ese pensamiento. En ocasiones, muchos fueron contratados bajo altísimos sueldos por las empresas que fueron hackeadas para que ellos mismos construyan un sistema más seguro. Tienen mucho poder y lo saben. Por eso son perseguidos constantemente.

El gobierno de los Estados Unidos, en defensa de sus empresarios, ha decidido hace unos años tomar cartas en el asunto personalmente. Se creó una división especial en el FBI llamada National Computer

Crime Squad que protege a las computadoras gubernamentales, financieras, de instituciones médicas, etc. Ya existen leyes que penalizan el accionar estos delitos a diferencia de nuestro país, donde la legislación al respecto es nula. En 1996, el argentino Julio César Ardita penetró ilegalmente a la red del Pentágono de Estados Unidos mediante Internet y provocó el enojo de más de uno en el país del norte. Fue condenado allí a cinco años de prisión en suspenso y debió pagar una multa de 5000 dólares. A pesar de la sanción.

Los hackers poseen su propia ética, su propio vocabulario y son por demás utópicos. Tienen niveles de aprendizaje y detestan a aquellos que se animan a prejuzgarlos. Son solidarios entre sí y, cuando no están sentados frente a sus máquinas, estudian nuevas formas para penetrar en lugares inhóspitos. No son muy sociables y les causa mucho placer sentir que transgreden.

HACKERS ATACAN SITIO DE HILLARY CLINTON

Como es sabido, la primera dama estadounidense, Hillary Clinton, aspira a convertirse en senadora por Nueva York. Como parte de su campaña, su equipo creó un sitio web (http://www.hillary2000.com), que ya ha sido asaltado por piratas informáticos.

La intervención realizada por los hackers fue relativamente leve, ya que sólo implicó un redireccionamiento del URL, que hizo que quienes intentaran acceder al sitio web de la candidata fuesen llevados a una página web creada por "Los Amigos de Guiliani" también candidato a una senaturía por Nueva York.

Jerry Irvine, experto consultado por CNN, señaló que lo más probable es que los hackers hayan recurrido a un truco conocido como *DNS poisoning*; es decir un "envenenamiento" del sistema de nombres de dominios, haciendo que al escribir una dirección en la web los usuarios sean llevados a una dirección distinta.

100 HACKERS PREPARAN ATAQUE CONTRA INDONESIA

José Ramos Horta, quien en 1996 fuese galardonado con el Premio Nóbel de la Paz junto al obispo Carlos Belo, advirtió al gobierno de Indonesia que un grupo de 100 hackers se dispone a atacar el sistema bancario del país en caso de que adultere el resultado del plebiscito de fin de mes.

El día 30 de agosto, los ciudadanos de Timor del Este concurrirán a las urnas para decidir si desean o no independizarse de Indonesia. Hasta ahora, la "campaña" del gobierno de Yacarta ha resultado en más de 1.000 muertos y el desplazamiento forzado y relegación interna de más de 80.000 personas.

En caso de conseguir su objetivo, las pérdidas serían de "varios cientos de millones de dólares", lo que tendría efectos catastróficos para la economía de Indonesia, en palabras del propio Horta. A juicio del galardonado con el Premio Nobel de la Paz, un ataque informático contra Indonesia es plenamente justificable, especialmente al considerar que no se perderían vidas humanas.

HACKERS CONTROLAN SATÉLITE MILITAR BRITÁNICO

Satélite militar de comunicaciones está siendo controlado por piratas informáticos. El satélite sería usado para la defensa de Gran Bretaña en caso de un ataque nuclear.

Según el diario inglés Sunday Business, desconocidos alteraron el rumbo del satélite hace dos semanas, luego de lo cual las autoridades responsables recibieron una extorsión según la cual los hackers dejarían en paz el satélite a cambio de una fuerte suma de dinero en efectivo.

Expertos en seguridad y estrategas militares toman en serio la amenaza, recalcando que sería muy natural que enemigos interesados en atacar a Gran Bretaña con armas atómicas primero intentasen dejar fuera de servicio a los sistemas de comunicación.

Una fuente militar consultada por Sunday Business destacó el grave riesgo para la seguridad del país que implica que desconocidos logren apoderarse del control de un satélite. El hecho de que se trate de una extorsión agrava aún más las cosas, señaló.

Por el momento, tanto la policía británica como el Ministerio de Defensa se niegan a comentar los hechos.

QUE PASARÁ MAS ADELANTE.....

La incorporación de las denominadas "redes inteligentes" podría dificultar considerablemente las actividades de los Hackers.

El Instituto Tecnológico de Georgia, EEUU, trabaja en un proyecto de desarrollo de redes neurológicas, que probablemente aumentarán la seguridad del tráfico digital.

El nombre "red neurológica" se basa en las neuronas del cerebro humano, que aprenden de la experiencia, creando conexiones entre las distintas áreas del cerebro. Con todo, cabe precisar que no se trata de redes que estén en condiciones de pensar, sino de sistemas capaces de identificar patrones en el flujo digital y aprender de los intentos de intrusión.

Hoy en día, los administradores de sistemas deben actualizar manualmente los sistemas de protección de las redes contra las embestidas de los sagaces piratas informáticos. Con la incorporación de redes inteligentes se hará más previsible y fácil la contención de los intrusos, según escribe James Cannady, experto en el tema, en un artículo en Netsys.com.

Según Cannady, tales redes estarán incluso en condiciones de detectar máquinas que monitorizan ilegalmente el tráfico de la red para captar y apoderarse de información tal como números de tarjetas de crédito, contraseñas y otros datos confidenciales. La novedad es que las redes neurológicas detectarán ese tipo de máquinas sin que sus operadores se percaten.SEGURIDAD INFORMÁTICA

¿SON SEGUROS LOS SOFT DE ENCRIPTACIÓN DE DATOS?

Según expertos argentinos, el software que importan algunas empresas argentinas desde los Estados Unidos

para proteger sus datos confidenciales no tiene los niveles de seguridad esperados. Para Ariel Futoransky, del laboratorio de seguridad informática argentino Core SDI, por ejemplo, los programas de encriptación de datos que se importan de ese país pueden ser fácilmente violados.

"Esto es así porque en los Estados Unidos hay grandes restricciones para exportar este tipo de software. Tienen miedo de que en todo el mundo se usen los mismos programas que utilizan ellos y de este modo se puedan desarrollar métodos para interferir organismos oficiales clave, como los de inteligencia o seguridad".

La encriptación usa una técnica −la criptografía− que modifica un mensaje original mediante una o varias claves, de manera que resulte totalmente ilegible para cualquier persona. Y solamente lo pueda leer quien posea la clave correspondiente para descifrar el mensaje. Junto con la firma digital y las marcas de

aguas digitales (digital watermark), la encriptación es una de las posibles soluciones para proteger datos cuando son enviados a través de redes como Internet.

La preocupación que tienen en los Estados Unidos por el uso indebido de estos programas es muy fuerte. El software de encriptación tiene las mismas restricciones de exportación que los planos de armas nucleares.

Con este panorama, no es alocado sospechar de la calidad de los programas que, a pesar de todas las restricciones, logran salir de los Estados Unidos. Porque si en ese país son tan celosos de su seguridad, se puede pensar que sólo exportarán los programas menos poderosos.

"Nosotros creemos que si el software salió de los Estados Unidos no es seguro. Si lo que se busca es proteger información importante, las empresas tienen que buscar otras estrategias de seguridad", agregó Futoransky.

OTRAS OPCIONES

La seguridad no es patrimonio exclusivo del gran país del Norte. Pruebas al canto: una universidad de Finlandia desarrolló el Secure Shell (SSH) que sirve para establecer comunicaciones encriptadas a través de Internet o de intranets, las redes internas de las empresas que usan el mismo lenguaje de Internet y así "transportan" información valiosa.

Este software, que goza de buena reputación entre las empresas de ese país, fue pedido por compañías de Europa y de los Estados Unidos para ser incluido a su vez en otros programas de seguridad.

Sin embargo, Core SDI encontró agujeros en la seguridad de este software, aparentemente infalible: descubrió que permitía que, a través de una serie de instrucciones y comandos, un extraño manejara en forma remota una computadora dentro de una intranet.

Esta empresa no solucionó el problema de seguridad del programa, sino que puso un "parche" que detecta cualquier ataque de intrusos en la red, activa una alarma y hace que enseguida se corten todas las conexiones. Ese parche ahora se puede bajar gratis de su sitio en la Web.

Para las empresas es muy importante contar con un software de protección confiable porque cada vez utilizan más las redes del tipo intranet, Internet y el correo electrónico para transmitir información.

Juan Carlos Maida, de la consultora Zampatti & Maida, coincide en la "inseguridad" de los programas de seguridad estadounidenses. "Sabemos que ahora en los Estados Unidos las reglas para la exportación de este tipo de software tienden a ser más flexibles. Pero, de todas maneras, existen productos de origen israelí o inglés con niveles de seguridad más altos que los estadounidenses. De todas formas, en la Argentina todavía no hay mucha conciencia sobre la necesidad de proteger datos importantes. Acá no se va más allá de los

antivirus".

Para este consultor, hay algunas señales claras que apuntan a mejorar esta cuestión, como la decisión del Banco Central argentino de exigir a todos los bancos que usen programas de encriptación de datos. Pero "lamentablemente, todavía son pocos los bancos que usan este tipo de software".

LOS MALOS TAMBIÉN SABEN MUCHO

El nivel de importancia que se le da a la cuestión de la seguridad se generalizó en los últimos años. Esto significa que las empresas son cada vez más conscientes del tema y no escatiman esfuerzos para evitar ser vulneradas.

Esta conclusión lleva a pensar que la seguridad creció. Pero esto no es así, porque simultáneamente aumentó y se difundieron la tecnología y los conocimientos para hackear. Por lo tanto, el nivel de inseguridad aumentó.

"En el año 1995, con la ejecución de algunas herramientas específicas de ataque y penetración, se hallaron 150 puntos vulnerables en diversos sistemas de red. En el último año, las mismas herramientas fueron utilizadas sobre las nuevas versiones de los sistemas operativos y el resultado fue peor: se encontraron 450 puntos débiles, pese a los avances y la mejora tecnológica de los softwares".

Esto hace que las compañías de software presten cada vez más atención al problema. "El Windows 2000, por ejemplo, que aún no salió al mercado, ya fue sometido a pruebas de este tipo y se le detectaron problemas de seguridad".

LA INVERSIÓN

Los costos de las diferentes herramientas de protección se están haciendo accesibles, en general, incluso para las organizaciones más pequeñas. Esto hace que la implementación de mecanismos de seguridad se dé prácticamente en todos los niveles. Empresas grandes, medianas, chicas y las multinacionales más grandes. Todas pueden acceder a las herramientas que necesitan y los costos (la inversión que cada empresa debe realizar) van de acuerdo con la empresa.

"Pero no es sólo una cuestión de costos, Los constantes cambios de la tecnología hacen que para mantener un nivel parejo de seguridad cada empresa deba actualizar permanentemente las herramientas con las que cuenta. Como los hackers mejoran sus armas y metodologías de penetración de forma incesante, el recambio y la revisión constantes en los mecanismos de seguridad se convierten en imprescindibles. Y éste es un verdadero punto crítico".

Según testers, "esto es tan importante como el tipo de elementos que se usen". Sin duda, éstos deben ser las que mejor se adapten al tipo de organización. Pero tan importante como eso es el hecho de conocer exactamente cómo funcionan y qué se puede hacer con ellos. "Es prioritario saber los riesgos que una nueva tecnología trae aparejados".

LAS REGULACIONES

Una de las herramientas de seguridad que se utiliza en la actualidad es la encriptación, pero esta técnica no es perfecta. En los Estados Unidos una serie de regulaciones le ponen un techo al nivel de encriptación.

El máximo nivel permitido hasta hace algunos meses (64 bits) perdió confiabilidad desde que se logró vulnerarlo.

En los Estados Unidos se está buscando un algoritmo de encriptación que permita unos diez años de tranquilidad. Es decir, que durante ese tiempo nadie logre tener los medios tecnológicos que le posibiliten descifrarlo. Además se está tratando de integrar a las empresas proveedoras de softwares con las compañías que los utilizan, o sea, unir a clientes y proveedores para encontrar opciones más seguras.

LA SEGURIDAD TOTAL ES MUY CARA

Hoy es imposible hablar de un sistema ciento por ciento seguro, sencillamente porque el costo de la seguridad total es muy alto. "Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas. La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios", "Si un hacker quiere gastar cien mil dólares en equipos para descifrar una encriptación, lo puede hacer porque es imposible de controlarlo. Y en tratar de evitarlo se podrían gastar millones de dólares".

La solución a medias, entonces, sería acotar todo el espectro de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total. Y esto significa ni más ni menos que un gran avance con respecto a unos años atrás.

FIREWALLS

"Los ataques a maquinas conectadas a Internet se incrementaron en un 260% desde 1994, se calcula una perdida de 1.290 millones de dólares anuales solo en los EEUU"

En la era de la información, las ideas, datos y archivos en su red son probablemente lo mas valioso que su empresa posee. Piense acerca de sus listas de clientes y registros de accionistas, transacciones comerciales y material de marketing, estrategias de comercialización y diseño de productos.

Cuanto valen ellos para su organización?

Cuan importante es esta información para el éxito de su empresa?

En su estado actual, la información que esta almacenada en su red no es utilizada con comodidad si la misma no es de fácil acceso e intercambio. Esto significa, que usted debe elegir entre accesibilidad sobre seguridad?. Muchas compañías piensan que ellos deben dejar que la información fluya libremente en su red. pero no piensan lo mismo sobre su dinero cuando lo depositan en el banco.

El Firewall logra el balance optimo entre seguridad y accesibilidad, de esta manera su empresa puede obtener todas las ventajas que ofrece el libre manejo de su información sabiendo que esta se encuentra completamente protegida.

Si su empresa tiene una red interna conectada a Internet o a una intranet corporativa usted necesita un firewall para mantenerlas normas de seguridad entre ellas . El firewall mantiene separada su red interna (de la cual usted tiene control) de diferentes tipos de redes externas (de las cual usted NO tiene control). El firewall controla la entrada y salida de trafico protegiendo su red de intromisiones indeseadas.

La función del firewall es ser una sólida barrera entre su red y el mundo exterior. Este permite habilitar el acceso a usuarios y servicios aprobados.

Algunos de las prestaciones que le brindan son:

- Previene que usuarios no autorizados obtengan acceso a su red.
- Provee acceso transparente hacia Internet a los usuarios habilitados.
- Asegura que los datos privados sean transferidos en forma segura por la red publica.
- Ayuda a sus administradores a buscar y reparar problemas de seguridad.
- Provee un amplio sistema de alarmas advirtiendo intentos de intromisión a su red.

Estas son algunas de sus características técnicas:

- Dos tipos de configuración, local y remota.
- Configuración remota por medio de una interface grafica que corre sobre sistema operativo Windows 95/NT.
- Configuración local por medio de una interface "ncurses" la cual se utiliza desde la consola del firewall.
- Permite el uso de aplicaciones basados en servicios tales como RADIUS y TACACS+ los cuales se utilizan en tasación de tiempos de conexión y uso de servicios.
- Soporta el uso de proxy−server para la configuración de su red interna.
- Conexiones de todos los servicios comunes de TCP/IP a través del firewall de manera totalmente transparente.
- Soporta servicios multimedia, incluyendo Real Audio, CuSeeMe, Internet Relay Chat, etc..
- Amplio sistema de logeo de conexiones entrantes / salientes totalmente configurable.
- Auto configuración de servidores que proveen servicios hacia el exterior de la red interna por medio de normas de seguridad.
- Múltiples alarmas de intentos de ingreso fallidos hacia la red.
- Sistema de alarmas configurable que permite el envió de avisos por medio de FAX, Pager, Mail, Voice Mail y advertencia visuales.
- Filtro de acceso de conexiones permitidas por interfaces no permitidas, este filtro es importante para contrarrestar técnicas IP−SPOOFING.
- La configuración del firewall se puede hacer mediante el mismo server o desde un servidor remoto corriendo un sistema de administración especifico que utiliza para esta tarea una interface dedicada o TUNNELING (comunicación encriptada).
- Soporte de comunicaciones encriptadas entre dos FIREWALL (tunneling) en forma totalmente transparente usando algoritmo IDEA/3DES, no es necesario que entre las dos puntas de la comunicación se encuentren dos FIREWALL tambien se puede efectuar la conexión con cualquier servidor corriendo sistema operativo de tipo BSD, SunOS, Solaris, etc por medio de un daemon que el Firewall provee para cada sistema operativo.
- Los módulos de alarmas corren tanto dentro del FIREWALL (centralizador de alarmas) como también en los servidores de su red para poder brindar detalles mas específicos.

El sistema de configuración permite agregar servicios no estándar a su red y usar estos con el modulo de TUNNELING (comunicación encriptada) para aumentar su seguridad.

¿ES LA SEGURIDAD EN LA RED PROBLEMA CULTURAL MÁS QUE TECNOLÓGICO?

Panelistas participantes de una reunión mensual, coinciden en que el 80 por ciento de las violaciones a la información se da dentro de las organizaciones.

A medida que el comercio de las empresas vía Internet se hace más generalizado, la inseguridad en las transacciones comerciales se vuelve un problema crucial y en constante crecimiento que debe ser contemplado por la alta gerencia en la toma de decisiones y en la implementación de soluciones.

Al hablar sobre la "Seguridad en Internet" nos referimos al gran índice de inseguridad interna de la infraestructura informática de las empresas, así como la falta de una cultura informática necesaria para contemplar estos problemas.

El alto grado de vulnerabilidad de la información transferida por la Internet y la facilidad de ataques externos e internos que se traducen en pérdidas que ascienden hasta miles de dólares en términos de información alterada, robada o perdida.

Según una investigación realizada en 1700 empresas por la empresa, el 75 por ciento de estas han tenido algún problema de seguridad. De éstas el 40 por ciento ha enfrentado problemas de seguridad debido a la falta de apoyo de la alta dirección para invertir en medidas y herramientas de seguridad y sólo el 38 por ciento se debió a la falta de herramientas adecuadas.

Una alternativa es el uso de una llave pública y una privada mediante el protocolo de seguridad Securet Socket Layer (SSL) que autentifica tanto al usuario que envía como al que recibe la información, porque es durante este proceso de transmisión que ocurren la mayor parte de las violaciones en la seguridad.

Más que un problema de tecnología, la seguridad en la transmisión de la información por la Red se debe a la falta de cultura de las organizaciones y de las personas que la integran.

El eslabón más débil de esta cadena en la seguridad la constituye el humano y no el tecnológico, lo cual destaca la importancia de tener una cultura de seguridad, porque no existe en muchas empresas un responsable de la seguridad.

A todos los usuarios se les debe divulgar las políticas de seguridad, además de hacer constantes auditorias para controlar que sean las adecuadas al momento que vive la empresa.

Lo que se necesita no es solamente prevenir un ataque en la seguridad, sino ser capaces de detectar y responder a esta agresión mientras ocurre y reaccionar ante la misma.

Es importante destacar que no existe un control de seguridad único, sino que las empresas deben contar con diversas capas de seguridad en todos los niveles de su información para poder así detectar el problema en algunos de estos puntos antes de que llegue a la información crucial.

LA SEGURIDAD EN LAS REDES : HACKERS, CRACKERS Y PIRATAS

Junto a los avances de la informática y las comunicaciones en los últimos años, ha surgido una hueste de apasionados de estas tecnologías, que armados con sus ordenadores y conexiones a redes como Internet, ha logrado humillar a instituciones tan potencialmente seguras como el Pentágono y la NASA. La notoriedad de sus hazañas, su juventud y la capacidad de dejar en evidencia a instituciones muy poderosas, les hace aparecer ante la opinión pública rodeados de un halo de romanticismo. Pero, ¿quiénes son?, ¿son peligrosos para la sociedad?, ¿deben ser perseguidos?

Podemos encontrarnos con diferentes términos para definir a estos personajes: *hackers*, *crackers*, piratas, etc., estando normalmente condicionado el calificativo a los objetivos y a los efectos de sus ataques a los sistemas. El término **hacker**, por ejemplo, se utiliza normalmente para identificar a los que únicamente acceden a un sistema protegido como si se tratara de un reto personal, sin intentar causar daños. Los **crackers,** en cambio, tienen como principal objetivo producir daños que en muchos casos suponen un problema de extrema gravedad para el administrador del sistema. En cuanto a los piratas, su actividad se centra en la obtención de información confidencial y *software* de manera ilícita.

Es muy difícil establecer perfiles de estas personas, porque salvo en los casos en que han saltado a la luz

pública como resultado de sus actividades, en su conjunto forman un círculo cerrado e impenetrable. Una aproximación podría ser la de un joven, bastante inteligente, con necesidad de notoriedad, inclinaciones sectarias, y en muchos casos, algo de inadaptación social. Su principal motivación es la de acceder a sistemas protegidos de forma fraudulenta, en una escala que va desde la mera constancia de su éxito, hasta la destrucción de datos, obtención de información confidencial, colapso del sistema, etc. Normalmente los objetivos más apetecibles son los sistemas relacionados con la seguridad nacional, defensa e instituciones financieras, pero ante las posibles consecuencias legales de estos actos optan por otros organismos públicos, las universidades y las empresas.

Existe una serie de grupos que tienen un carácter supranacional, y que se extiende a través de su hábitat natural: Internet. A través de este medio intercambian información y experiencias, al mismo tiempo que logran un cierto grado de organización. Esto ha disparado la alarma en algunos ámbitos gubernamentales, dado que una acción coordinada que afectara a varios sistemas estratégicos de un país puede ser igual de desestabilizadora que las actividades terroristas. En España tenemos ejemplos recientes, como es el caso de *Hispahack*, que realizó ataques a varios sistemas, incluidos los de algunas universidades. También se ha creado en la Guardia Civil un grupo especializado en todo tipo de delitos informáticos para identificar e investigar a estos modernos delincuentes.

En la ULL, en cambio, hasta este momento no ha existido un riesgo importante ya que, por una parte, había un gran retraso tecnológico en nuestras infraestructuras y, por otro, los sistemas formaban parte de redes que por sus características eran impermeables a dichos ataques. Pero la situación ha cambiado: la ejecución del Plan Integral de Comunicaciones ha elevado tanto nuestras posibilidades que nos permite la integración en una única red de todos nuestros sistemas informáticos, con lo que conlleva a la hora de prestar servicios a los usuarios. Esto tiene su contrapartida, y es que el número de servicios que se ofrecen es directamente proporcional a los riesgos que se asumen, y sobre todo porque el primer enemigo al que habría que considerar podrían ser los propios usuarios.

De todas formas, el exceso de prudencia es contrario a la innovación y, por tanto, se están adoptando medidas que garanticen una cobertura suficiente: la adquisición de herramientas de *software* para la

gestión de red, *firewalls* (cortafuegos, programas especializados en la protección de redes y sistemas), y *software* de auditoria; la elaboración de planes de seguridad tanto física como lógica y de las políticas correspondientes; y, por último, la mentalización de los usuarios para el correcto uso de los servicios que se prestan. De todas formas, la total seguridad nunca se podrá alcanzar, a menos que coloquemos los sistemas detrás de un muro infranqueable. Pero entonces nos encontraríamos con una red que es una auténtica autopista, pero por la que sólo circularían el correo electrónico y las páginas *web*.

Además, esto significa un incentivo para que los administradores de los sistemas y responsables de seguridad seamos mejores en nuestro trabajo, ya que cada ataque con éxito pone en evidencia nuestras deficiencias.

RESTRICCIONES LEGALES.

En algunos países existen muchas restricciones legales para el comercio electrónico, y esto impide la evolución del desarrollo de las aplicaciones y la implementación de software de seguridad para los negocios en línea.

Desgraciadamente, no sólo se enfrenta el problema técnico sino el legal porque cuando se utiliza una firma electrónica autorizada por las empresas involucradas en una transacción, por ejemplo, no se puede probar en un juicio que esta firma es auténtica. No existe una autoridad certificadora, éste es uno de los problemas más serios.

No se puede considerar que la seguridad sea cuestión de una sola cosa, ya que hay muchos elementos y soluciones en la infraestructura de informática de una empresa.

Por ejemplo, muchas de las claves en la criptología son fácilmente descifrables, debemos ver otras alternativas de tecnología de otros países de Europa, Israel, Rusia y no sólo en las soluciones americanas que presentan también muchas restricciones legales para su importación.

Algunas medidas para hacer frente al creciente problema de la falta de seguridad son: entre ellas la importancia de evaluar su vulnerabilidad interna y hacerse conscientes de que si bien existen muchas violaciones externas y muchas soluciones tecnológicas, existe un porcentaje muy alto de inseguridad interna como resultado de problemas organizacionales.

Esto enmarca la importancia de contar con políticas internas específicas que cuenten con el apoyo de los altos directivos, así como la existencia de un responsable en la seguridad interna cuyas decisiones de protección se realicen en función de problemáticas específicas y no sujetas a ajustes económicos.

HACK&BUSINESS (LAS EMPRESAS Y LOS ASESORES)

Para la mayoría de las empresas, las grandes oportunidades de ganar dinero en Internet todavía puede que estén lejos, pero las empresas de seguridad informática ya están viendo cómo sus arcas se llenan. Internet, que al principio no era nada más que una modesta asociación de redes informáticas utilizada por investigadores para el intercambio de información, no fue concebida para servir de autopista al comercio mundial. En los primeros tiempos, la comunidad Internet era una especie de pequeño pueblo de gentes con ideas afines, donde todos se conocían y donde todos confiaban en los demás. Inevitablemente, el carácter de Internet ha cambiado ahora que están conectadas millones de personas en todo el mundo. Con la irrupción de las empresas en Internet, éstas se aprovechan de una mejor relación con clientes, proveedores y empleados en oficinas remotas pero, al mismo tiempo, se arriesgan más a que sus sistemas informáticos puedan ser violados por personas ajenas con intenciones delictivas. Así se explica que el sector de la seguridad informática, antaño una especialidad misteriosa, se haya convertido en un negocio en boga.

Los peligros de un mundo conectado han hecho que corran buenos tiempos para los asesores de seguridad informática, auditores, criptógrafos y otros profesionales. La gran demanda de profesionales especializados ha hecho que los salarios suban rápidamente, a veces doblándolos o triplicándolos en los últimos cinco años, y algunos expertos en seguridad informática ganan actualmente sueldos de unos 120.000 dólares anuales. La búsqueda de talentos en seguridad informática se extiende por el mundo entero. Wletse Venema, científico informático de la universidad holandesa de Eindhoven, es coautor de Satán, un atractivo programa de software diseñado para detectar fallos de seguridad en cualquier sistema informático conectado a Internet. A finales del año pasado, fue requerido por varias empresas internacionales, antes de que se decidiera por el laboratorio de investigación de IBM en las afueras de la ciudad de Nueva York. "Ahora hay una gran demanda para mis conocimientos", comenta jocosamente. Resulta difícil precisar las cifras del gasto destinado a seguridad informática. Muchas empresas tratan esta partida de sus presupuestos como información confidencial. Dataquest, empresa dedicada a investigaciones de mercado, calcula que las empresas en todo el mundo invertirán este año 6.300 millones de dólares en seguridad de las redes informáticas. El cálcalo de Dataquest, no obstante, abarca sólo servicios suministrados por contratistas ajenos a la empresa, de modo que no incluye los gastos en personal fijo y soporte físico. Aún así, incluso tomando en cuenta sólo a los contratistas, Dataquest prevé que la facturación en el ámbito de seguridad se duplicará con creces a lo largo de los tres próximos años hasta llegar a los 12.900 millones de dólares. Aproximadamente una tercera parte de ese gasto se realizará en Estados Unidos, mientras que el resto corresponde principalmente a Europa y Asia.

La industria de seguridad informática comprende a miles de empresas en todo el mundo, pasando por toda la gama, desde multinacionales gigantes como **I**nternational **B**usiness **M**achines Corporation o Science Applications International Corporation, hasta las más pequeñas integradas por una sola persona. Por supuesto,

es el miedo lo que impulsa este aumento de los gastos en seguridad informática. Los temores empresariales aumentan con cada noticia de piratas informáticos que irrumpen en sitios de renombre en la Red, como el ataque a principios de año a la página de la CIA. Las autoridades policiales afirman que las intrusiones en los sistemas informáticos de las empresas que denuncian son muy pocas, como mucho un 15%.

Pero las pocas que si se denuncian, como el caso de los saboteadores informáticos que en 1994 se colaron en el Citibank y consiguieron obtener diez millones de dólares en transferencias de fondos ilegales (de las cuales solamente se recuperaron 400.000 dólares), tienden a sembrar la alarma. "La cuestión no es tanto la seguridad de la Red, sino su inseguridad", afirmó Alice Murphy, analista de Dataquest. Hay mucha ansiedad en el ambiente.

El grado de ansiedad de las empresas y el importe que deben invertir en seguridad informática son objeto de un acalorado debate. Y ese debate refleja en parte una división en la cultura de Internet entre el genio pirata del pasado, cuando el estado subvencionaba la Red y la información se intercambiaba libremente, y el genio comercial de la Internet de hoy. También es cierto que la motivación de muchos piratas es la emoción y el desafío intelectual. Ellos componen gran parte del público internacional se calcula que existen unos 1900 sitios en la Web donde se proporcionan trucos y herramientas para el pirateo y docenas de publicaciones como Phrack y 2600, Revista trimestral sobre piratería informática. No obstante, existe un animado mercado ilegal en esta materia, según expertos en seguridad, con una gama de precios para sabotear una página de Internet que oscila entre 6300 y 7000 dólares. Por lo general se exigen pagos adicionales por el hurto de secretos comerciales o por infligir daño en el sistema informático de una empresa de la competencia. En todo caso, como señalan algunos analistas, existe una considerable diferencia entre la vulnerabilidad potencial de los sistemas informáticos de las empresas y el riesgo real que corren. "El riesgo existe, pero se tiende a exagerar la amenaza", comenta George Colony, presidente de Forrester Research Inc., empresa asesora de Cambridge, Massachusetts.

Forrester calcula que las pérdidas por fraude en el comercio de Internet probablemente ronda un dólar cada mil.

Para hacernos una idea, según Forrester, las pérdidas por fraude en el servicio de telefonía celular son de unos 19 dólares por cada mil aproximadamente, mientras que las pérdidas por transacciones electrónicas con tarjetas de crédito se aproximan a los 2 dólares por cada mil de productos cobrados.
No obstante, hasta los escépticos como Colony, de Forrester, están de acuerdo en que la seguridad informática es algo que precisa atención continua. "Supone un riesgo controlable que no debería desanimar a las empresas a la hora de lanzarse al comercio en Internet", comenta Colony, "pero también digo a nuestros clientes que piensen en la seguridad electrónica como una guerra de guerrillas que durará eternamente". Esta guerra de guerrillas se está desarrollando de diferentes maneras en cada país. Las empresas norteamericanas, por ejemplo, son más propensas a contratar expertos de seguridad informática en calidad de empleados fijos, como ha hecho ya el 78%, según una encuesta realizada por la firma contable Ernst & Young y la revista comercial Information Week entre 4.200 ejecutivos de servicios información, en 24 países.

SEGURIDAD : BARRERA AL COMERCIO ELECTRÓNICO

Recientemente ha aparecido publicada una encuesta sobre las barreras al comercio electrónico, llevada a cabo por ITAA (Information Technology Association of America) y la consultora Ernst & Young.

Es un hecho que el comercio electrónico no ha experimentado todavía el crecimiento ni la aceptación que el entusiasmo inicial pronosticaba para el futuro inmediato.

La encuesta tenía por cometido el analizar cuáles eran los mayores factores que actúan de freno a la expansión

de la actividad comercial en Internet y de acuerdo con los resultados obtenidos, la barrera más importante es, obviamente, la falta de confianza (señalada por el 62% de los encuestados).

Esta desconfianza hacia las nuevas tecnologías se articula en torno a tres temores fundamentales:

1)− La privacidad (60%), que los usuarios finales sienten amenazada en la medida en que desconocen hasta qué punto los datos personales que suministran a un servidor de comercio electrónico serán tratados de forma confidencial.

2)− La autenticación (56%), que inquieta a los usuarios, quienes dudan si la persona con la que se comunican es verdaderamente quien dice ser.

3)− La seguridad global (56%), que preocupa a los usuarios, pues temen que la tecnología no sea suficientemente robusta para protegerlos frente a ataques y apropiaciones indebidas de información confidencial, especialmente en lo que respecta a los medios de pago.

Es interesante el hecho de que de toda la actividad de compra, lo que más sigue preocupando es la operación de pago, es decir, el momento en el que el comprador se enfrenta a la ventana donde han introducido su número de tarjeta de crédito y duda a la hora de pulsar el botón de "Enviar". "¿Me robarán?, ¿seré víctima de un fraude?", se pregunta el usuario en el último momento.

Estos temores, qué duda cabe, tienen su fundamento real y su solución no resulta trivial. En el primer caso, la tecnología, y en concreto la criptografía, ofrece las herramientas necesarias para la protección férrea de la información almacenada en las bases de datos corporativas, información como listas de clientes, sus datos personales y de pago, listas de pedidos, etc. Existen muchas técnicas de control de acceso que hábilmente implantadas garantizan el acceso a la información confidencial exclusivamente a aquellos usuarios autorizados para ello. Ahora bien, se han producido incidentes de servidores de comercio que almacenaron esta clase de información sensible ¡en archivos accesibles vía web por cualquier navegante! Por lo tanto, aunque la criptografía provee de medios aptos, depende en última instancia de la empresa el nivel de compromiso que adopte respecto a la seguridad de los datos que conserva en sus ficheros y su política de control de acceso. Así pues, éste es un temor bien presente y sin fácil respuesta. La tecnología nada tiene que decir si un comerciante decide vender su información a terceros. La delgada línea que protege la privacidad del usuario está constituida en este caso por la integridad moral de la empresa.

En el segundo caso, la solución inmediata que ofrece la criptografía viene de la mano de los certificados digitales. La tecnología de certificación está suficientemente madura como para autenticar adecuadamente a las partes involucradas en una transacción. La más comúnmente utilizada es SSL y a pesar de la tan vapuleada limitación criptográfica fuera de Norteamérica de claves débiles de 40 bits, lo

cierto es que a la hora de autenticar a las partes, principalmente al servidor, SSL funciona satisfactoriamente. Otras tecnologías emergentes, ofrecen mucha mayor confianza en este campo y, de paso, dan solución al primer problema de la privacidad, ya que permite autenticar a las partes involucradas en la transacción de manera completamente segura, sin restricciones criptográficas debidas a absurdas leyes de exportación.

En cuanto al tercer temor, nuevamente la criptografía y los productos de seguridad proporcionan las soluciones a los problemas.

Otra cuestión es: ¿incorporan los servidores de comercio todas las medidas necesarias para asegurar las transacciones con el usuario?. Las herramientas ofrecen solución tecnológica a los retos que se le presentan a la seguridad en el comercio electrónico, pero ¿se usa correctamente? ¿Se usa en absoluto?
Por lo que parece, las verdaderas barreras al comercio electrónico no son tanto tecnológicas como humanas.

Una vez más, el eslabón más débil de la cadena es de índole personal, no tecnológico.

GLOSARIO

Administrador: Persona que se encarga de todas las tareas de mantenimiento de un sistema informático.

Backdoor: Puerta de entrada trasera a una computadora, programa o sistema en general. Sirve para acceder sin usar un procedimiento normal

Bajar o Download: Extraer un programa de un BBS vía módem.

Black Box: Aparato que engaña a la central telefónica haciéndole creer que no se levantó el teléfono cuando en realidad se está produciendo una comunicación

Blue Box: Aparato (o programa de computadora) que emite tonos multifrecuencias que permite controlar las centrales telefónicas. Se utiliza para lograr comunicaciones gratuitas, entre otras cosas.

Boxes: Circuitos preparados para realizar phreaking. Destacan:

- Bluebox => Para llamar gratis
- Redbox => Emula la introducción de monedas en teléfonos públicos
- Blackbox => El que llame a un teléfono con este dispositivo no pagará la llamada.

Bug: Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otra cosa.

Bustear: Precinto o incubación de un BBS por parte de la policía.

Calling Card: Tarjeta de crédito emitida por una compañía telefónica que permite hacer llamadas y pagarlas después.

Carding: Uso de tarjetas de crédito de otras personas, generación de nuevas tarjetas de crédito para realizar pagos a sistemas de compra a distancia (principalmente). En general, cualquier actividad fraudulenta que tenga que ver con las tarjetas de crédito.

Crack: Desprotección de un juego o programa.

Cracking: Modificar un programa para obtener beneficios. Normalmente se basa en quitar pantallas introductorias, protecciones o, como en unas modificaciones de cierto programa de comunicaciones, conseguir nuevos passwords de acceso a sistemas...

Cortafuegos (Firewall): Computadora que registra todos los paquetes de información que entran en una compañía para, una vez verificados, derivarlos a otra que tiene conexión interna y no recibe archivos que no provengan de aquella. Es como un embudo que mira si la información que desea entrar a un servidor tiene permiso para ello o no. Los hackers deben contar con gran creatividad para entrar ya sea buscando un bug (error de diseño) o mediante algún programa que le permita encontrar alguna clave válida.

Cyberpunk: Corriente literaria dentro de la ciencia−ficción que, entre otras cosas, se destaca por incorporar a sus argumentos el uso de la tecnología de las redes de computadoras.

Dial−up: Línea de datos que permite a un usuario acceder por módem a una red o a una computadora.

Facke: Todas aquellas versiones de programas que han sido manipuladas de tal manera que figuran como versiones superiores a la original sin serlo.

Guest: Cuenta pública de un sistema, para que la use alguien que no tiene cuenta propia.

Gusano: Programa que se reproduce, sin infectar a otros en el intento.

Group: Grupos de personas que unen sus fuerzas para `suplier' juegos o programas.

Hacking: Acto de hackear. Básicamente consiste en entrar de forma ilegal en un sistema, para obtener información. No conlleva la destrucción de datos ni la instalación de virus, pero pueden instalarse troyanos que proporcionen passwords nuevos. También consiste en llevar una vida acorde con el hackmode.

Hackmode: Modo de actuar del hacker. No tiene por qué estar relacionado con las computadoras, es más bien un modo de interpretar la vida. Consiste en:

- No pagar lo que no es estrictamente necesario o pagar de forma "poco corriente".
- Ser un poco "paranoico".
- Actuar acorde con costumbres rigurosamente calculadas.

Handle: Seudónimo usado en vez del nombre verdadero.

Ingeniería social: Arte de convencer a la gente de entregar información que no corresponde.

Lamer: Tonto, persona con pocos conocimientos. Principiante

Login: Procedimiento de identificarse frente a un sistema para luego usarlo. Este identificativo más el

password o clave te permite acceder a información restringida.

Loops: Circuitos. Un loop (o bucle) de teléfonos son dos teléfonos que se comunican entre sí.

Operador: Persona que usa una computadora. A menudo se llama 'operador' al administrador del sistema.

Nukear: Anular un programa de un BBS recién `subido', por ser antiguo y carecer de interés.

Outdial: Modem de salida dentro de una misma red, que permite a un usuario de la misma salir a la red telefónica convencional. Los que permiten hacer llamadas a larga distancia se llaman 'global Outdial' (Outdial globales) o GOD.

Packet switching: Conmutación de paquetes.

Password: Clave. Palabra que sirve para verificar que un usuario es realmente quien dice ser. Por eso mismo, el único que debe conocerla es ese mismo usuario.

PBX: Private Branch Exchange. Centrales telefónicas internas de empresas

Patch o Parche: Modificación de un programa ejecutable para solucionar un problema o para cambiar su comportamiento.

Petar: Anular. Este término se utiliza en el supuesto de que los sistemas utilizados para `tracear' de un BBS, se hayan anulado o caducado.

Payload: Efecto visible de un software maligno.

Phreaking: Acto de llamar por teléfono gratuitamente y la realización de modificaciones a los aparatos telefónicos con el fin de obtener algún tipo de beneficio.

Subir o Upload: Enviar un programa a un BBS vía módem.

Tracear: Seguimiento exhaustivo. Se utiliza cuando se intenta desproteger un programa y se tiene instalado un Debugger. Este término también es utilizado en caso de que la línea telefónica esté pinchada por la policía.

Trader: Persona que `sube' y `baja' continuamente programas y juegos de BBS.

Virii: Suele encontrarse en textos en inglés. Es la acción de crear virus.

Warez: Programas comerciales ofrecidos gratuitamente. Lo que se conoce popularmente como "pirateo".

ENTREVISTAS A HACKERS

DANIEL SENTINELLI

El FBI llegó a mandar a Buenos Aires a uno de sus agentes de su central regional instalada en Montevideo. Uno de los más conocidos hackers argentinos, apodado El Chacal, aceptó revelar su identidad (se llama Daniel Sentinelli) para realizar una demostración pública, en un cybercafé del barrio de Belgrano, de lo fácil que puede resultar a un conocedor en informática llegar a redes supuestamente secretas de gobiernos como el estadounidense. "Estas redes (como la mayoría de las que están en Internet) tienen un sector público (de acceso directo e irrestricto) y uno privado (sólo para usuarios autorizados).

Como ambos deben estar disponibles hay una brecha entre ellos que permite aprovechar los errores propios de los programas que usan". Si este asesor en informática de 30 años que en 1986 estuviera entre los fundadores de Piratas Unidos Argentinos decidió darse a conocer es porque cree que "se ha desatado una paranoia generalizada que puede derivar en una caza de brujas". Detrás de los hackers, dice, "no hay ninguna clase de criminales. En todo caso respondemos a una curiosidad: la tecnología está ahí, al alcance de la mano y probar qué se puede hacer con ella es irresistible".

"Hay quienes intentan meter miedo, como un periodista argentino que cuando salió a luz el caso del muchacho que entró a la red de la Marina estadounidense clamó poco menos que el mundo está en poder de los hackers y que cualquiera puede ahora entrar a redes ultrasecretas y disponer el envío de misiles nucleares." Sentinelli remata: "Internet no es segura porque en ella habitan los hackers. Nada de lo que usamos habitualmente es seguro: los autos, el sistema de gas, el de electricidad tienen fallas, pero no por eso dejamos de usarlos. Tratamos de informarnos de los riesgos de esas fallas. Con Internet debemos hacer lo mismo".

ENTREVISTA A EX−HACKER

−¿Qué es un hacker?

Un hacker es una persona que investiga la tecnología de una forma no convencional. Lo que pasa es que a raíz de eso muchas veces, y ésta es la imagen que suele tener la gente de un hacker, por investigar la tecnología de una forma distinta termina metiéndose en lugares donde no estaba previsto que entrara y termina violando la seguridad de algunos sistemas. La definición más popular de hacker: "señor que viola sistemas de computadoras".

−¿Quién NO es hacker?

Todos lo demás. El que no viola los sistemas de seguridad.

El hacker tiene una actitud diferente hacia la tecnología, mira la tecnología de una forma diferente, no se conforma con leer el manual y usarla como se debe. El pibe que desde chico empieza a desarmar el autito, es un hackercito. A ese hay que cuidarlo, no se conforma en jugar como se debe.

−¿Así empieza un hacker? desarmando autitos? ¿Cómo llega uno a ser hacker?

Yo me acuerdo de algunos relojes despertadores que desarmé de chico y nunca pude volver a armar, supongo que podemos considerar que eran mis primeros pasos como hacker. En mi caso y en la mayoría de la gente de mi generación empezamos así, porque nos llamaba la atención la tecnología; hace 15 o 20 años atrás no había mucha información disponible sobre computadoras entonces tenías que buscarla vos, y vos meterte y vos analizar y programar e investigar y porque queríamos empezar a comunicarnos empezó a surgir el tema de las comunicaciones de los modems, en esa época 300 baudios con acopladores acústicos, una cosa bien primitiva y no había muchas cosas disponibles para la gente inclusive lo poco que había era solamente para empresas, entonces vos querías jugar con eso y la única alternativa que te quedaba era usar esos canales que no estaban disponibles para vos y tenías que hackear.

−¿Y cuál fue tu primer hackeo?

No es tan claro, vos te ponés a probar cosas y lo que estás hackeando es tecnología, después si eso de casualidad tiene que ver con una empresa o "disparaste una guerra nuclear" o algo así, es como un accidente; pero uno trata de evitarlo.

La actitud es ésa, en verdad lo que estás haciendo es divirtiéndote con la tecnología −por lo menos apriori− después vas encontrando cosas y a partir de ahí seguís jugando.

−Lo que muestran las películas, chicos o grandes entrando en sistemas que no deben, como la red,¿ son pura fantasía o tienen algo de real?

Yo, si tengo que elegirte una película que muestra un poquito mejor la actitud de un hacker y un poquito más cerca de la realidad y las cosas que hace, elijo "Hackers". Es muy difícil mostrar en una película lo que hace un hacker, sería muy aburrido mostrarlo porque es estar delante de una pantalla durante cuatro horas mirando un montón de números. La única película que muestra mejor el background o underground de lo que hace un

hacker, mejor que "la red", es "Hackers". En La Red se muestra a Sandra Bulloc que es "buena", los hackers son "malos" y los del gobierno son "tontos". A mí particularmente no me parece así... me parece que es una campaña de prensa más que nada para decir: "los hackers son malos". Lo que te diría es que inclusive ahí muestran a las agencias del gobierno norteamericano como tontas cuando te diría que por ahí ellos son el peor hacker y ellos tienen licencia para ser hackers ¿o no?

−Entonces ¿hay hackers buenos y hackers malos?

No sé, yo te diría que tendríamos que separar los tantos, en función de la intención. Eso es lo mismo que si vos decís que un tipo se mete en medio de la selva porque está explorando, es lo mismo que un grupo de guerrilleros que se mete en medio de la selva. Son actitudes distintas.

−Que los gobiernos en sus departamentos de defensa ya tienen hackers profesionales, es bastante público...

Claro, yo insisto, para mí hackear es un hobby, una diversión, algo que hago porque me gusta. Cuando vienen y me dicen *"bueno, y por qué no te ponés a robar bancos"*, pero eso es trabajar!; eso sería ser hacker con un objetivo en mente, entonces ahí estás laburando. Yo para laburar, doy consultoría. Es mucho más cómodo, es legal y gano también mucha plata, entonces, el tipo que está hackeando con un objetivo en mente, yo no sé si está hackeando. Está haciendo otra cosa y está usando el hacking como medio para llegar a otra cosa.

−Y vos qué has hecho, ¿por qué se te conoce?

Por qué se me conoce... y... porque estoy hace muchos años con esto, y porque fui el primero que se animó a hablar del tema...

−Pero escuchame, has viajado gratis, has aumentado un cero en tu cuenta...

No, no, no, eso... lo hago trabajando, como corresponde. Laburo en lo que me gusta y la gente me paga.

−¿Un hacker trabaja de conferencista, de consultor y nada más?¿ o a veces lo contratan esas empresas o esos sistemas de inteligencia para hacer alguna cosa especial?

No, bueno, yo asesoro empresas. Mi trabajo es asesorar empresas, esto de los seminarios es una cosa que organizó la gente del Programa Enlace, es más, es algo que no deja un rédito económico significativo, es algo más de difusión de la actividad y de tratar de transmitir una imagen más real de lo que es un hacker, tratar de cortar un poquito con el mito que están creando de los hackers malos y todo esa historia porque sino un día de éstos va a venir "un astuto" que se va a querer ganar un par de galones y ya veo que me van a querer agarrar de las pestañas a mí acusándome de... no sé, de cualquier cosa. Mi trabajo es... yo soy consultor en informática en la parte de redes, doy consultoría sobre seguridad, asesoro a empresas, a organismos... ése es mi trabajo.

−A los asistentes a los seminarios, en general, ¿qué es lo que más les interesa, lo que más preguntan, qué quieren saber?

Justamente, el temario que se armó para estos seminarios está en función de unas encuestas que hizo la gente de Enlace por e−mail tratando de ver qué es lo que le interesaba a la gente, y lo que más le llama la atención es lo de la telefonía celeular, todo lo que se puede hacer sobre telefonía celular. No saben que

se pueden pinchar, no saben cuán fácilmente, es más, conocemos que muchos políticos tampoco lo saben, si no no dirían las cosas que han dicho por celular, a pesar de que lo venimos mostrando en los medios desde hace años.

Hay gente que obviamente le interesa mucho el tema internet, evidentemente...

−¿Y el comercio electrónico?

Si, lo que pasa es que yo en los seminarios hablo mucho sobre criptografía, porque la idea también es, ya que estamos mostrando lo vulnerable que es la tecnología, la idea es mostrar cómo podés hacer vos individualmente para mantener tu privacidad; entonces tratamos de hablar de eso.

−¿Existe la posibilidad de mantener esa privacidad?

Sí, por supuesto que existe, a través del uso de criptografía; lo que pasa es que tenés que saber lo que estás haciendo, tenés que tener nociones claras de cómo funciona y esto es más complejo que mandar un mail simple con los datos y ya está, un poquito más de trabajo. La seguridad es costosa y la seguridad implica un poquito de trabajo, en todo sentido.

−¿Y tenés alguna presión de empresas, te siguen, te molestan, has tenido problemas con la justicia?

No al contrario, yo he asesorado a la justicia en algunos casos; algunos jueces me han llamado para que los ayude a entender algunos problemas técnicos, hay veces en que a los jueces le llegan causas por temas de tecnología y me han llamado para que les de una mano.

−¿Seguís "pagando el teléfono"?

Sí, yo pago el teléfono para mi uso normal, si bien hemos investigado tecnología para no hacerlo; lo que pasa es que, bueno...

−Para ir terminando, ¿qué hace que un hacker sea mejor que otro hacker?

Mirá, creo que es algo que se define en función de las cosas que hacés y de cómo las hacés, lo que pasa es que no hay un organismo central de calificación de hackers que designe puntaje, pero hay una cosa tácita de que la gente se conocen entre sí y obviamente existen ciertas rivalidades... no muchas veces, así un poco simpáticas, en joda. Pero a mí me llama la atención un tipo cuando hace algo de manera distinta más que qué hace, es la forma en que lo hace lo que te llama la atención, porque se le ocurrió una idea brillante, una forma brillante de hacer, aunque sea una pavada; pero un uso brillante de una tecnología, un uso novedoso, un uso que a nadie se le hubiera ocurrido, ése es un hacker admirable.

−¿Y de ésas has hecho algunas?

Y bueno, man, te imaginás que en los quince años que venimos haciendo cosas, acordate que empezamos cuando vos le hablabas a alguien de que tenías una computadora en tu casa y te miraban y te decían qué, ¿está llena de lucecitas y de cintas?. Empezamos ahí a hacer cosas, muchos... así que tenemos un historial...

CONCLUSIÓN

Después de realizar este trabajo nos dimos cuenta que ser un hacker no es como te muestran en las películas o como lo definen sino implica muchas mas cosas como por ejemplo, aprender a programar, conocer sobre redes, sistemas, etc. para luego poder ponerlo en practica cuando se busque algún tipo de información.
Un hacker no es más que alguien que quiere conocer la verdad y aprende para ello. También un hacker pone a prueba sus conocimientos, intentando entrar en sitios a los que no ha sido invitado. Y también intenta mejorar a los demás poniendo en conocimiento de todos, los fallos y las virtudes que ha encontrado en los sistemas y redes.

BIBLIOGRAFÍA

- Enciclopedia Encarta
- Internet: www.altavista.com
- Suplemento de Informática−Diario Clarín.
- Suplemento de Informática−Diario La Nación.

ÍNDICE

31