Seguridad Informática

Tema: 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 2000, 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.

El avance de la era informatica ha introducido nuevos terminos en el vocabulario de cada dia. Una de estas palabras, hacker, tiene que ver con los delitos informaticos. Todos estamos familiarizados con las historias de aquellos que consiguen entrar en las corporaciones informatizadas. Pero tenemos la impresion de que el termino "hacker" es uno de los peor entendidos, aplicados y, por tanto, usados en la era informatica.

La cultura popular define a los hackers como aquellos que, con ayuda de sus conocimientos informaticos consiguen acceder a los ordenadores de los bancos y de los negociados del gobierno. Bucean por informacion que no les pertenece, roban software caro y realizan transacciones de una cuenta bancaria a otra. Los criminologos, por otra parte, describen a los hackers en terminos menos halagadores. Donn Parker los denomina "violadores electronicos" y August Bequai los describe como "vandalos electronicos". Ambos, aunque aseveran que las actividades de los hackers son ilegales, eluden habilmente llamarlos "criminales informaticos". Hacen una clara distincion entre el hacker que realiza sus actividades por diversion y el empleado que de repente decide hacer algo malo. Por tanto, parece que tenemos una definicion en la que caben dos extremos: por un lado, el moderno ladron de bancos y por otro el inquieto. Ambas actividades (y todas las intermedias) son calificadas con el mismo termino. Dificilmente se podria considerar esto como un ejemplo de conceptualizacion precisa. Una gran parte de esta ambigüedad puede seguirse desde el origen durante estos aproximadamente 20 años de vida del mencionado termino. El termino comenzo a usarse

aplicandolo a un grupo de pioneros de la informatica del MIT, a principios de la decada de 1960. Desde entonces, y casi hasta finales de la decada de 1970, un hacker era una persona obsesionada por conocer lo mas posible sobre los sistemas informaticos. Los diseñadores del ordenador Apple, Jobs y Wozniack, pueden considerarse hackers en este sentido de la palabra. Pero a principios de la decada de 1980, influenciados por la difusion de la pelicula 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 jovenes capaces de violar sistemas informaticos de grandes empresas y del gobierno. Desgraciadamente, los medios de informacion y la comunidad cientifica social no ha puesto mucho esfuerzo por variar esta definicion. El problema para llegar a una definicion mas precisa radica, tanto en la poca informacion 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 definicion legal que sea aplicable a los hackers, ni todas sus actividades conllevan la violacion 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 raiz 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 informaticas. Parker y Bequai, dos lideres en el estudio de los delitos informaticos, utilizan el termino "hacker" de formas ligeramente diferentes. Parker reconoce que hacking no abarca todo el rango de actividades asociadas a la violacion de los sistemas informaticos, 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 credito telefonico 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 informaticas inusuales.

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

En primer lugar, el area de los hackers. En la tradicion de esta comunidad informatica, el hacker puede realizar dos tipos de actividades: bien acceder a un sistema informatico, o bien algo mas general, como explorar y aprender a utilizar un sistema informatico. En la primera connotacion, el termino lleva asociados las herramientas y trucos para obtener cuentas de usuarios validos de un sistema informatico, que de otra forma serian inaccesibles para los hackers. Se podria pensar que esta palabra esta intimamente relacionada con la naturaleza repetitiva de los intentos de acceso. Ademas, una vez que se ha conseguido acceder, las cuentas ilicitas a veces compartidas con otros asociados, denominandolas "frescas". He aqui la vision estereotipada de los medios de comunicacion de los hackers un joven de menos de veinte años, con conocimientos de informatica, pegado al teclado de su ordenador, siempre en busca de una cuenta no usada o un punto debil en el sistema de seguridad. Aunque esta vision no es muy precisa, representa bastante bien el aspecto del termino. La segunda dimension 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 autorizacion, el hacker no suele tener, el terminos generales, acceso a los manuales de operacion y otros recursos disponibles para los usuarios legitimos del sistema. Por tanto, el usuario experimenta con estructuras de comandos y explora ficheros para conocer el uso que se da al sistema. En oposicion con el primer aspecto del termino, aqui no se trata solo de acceder al sistema (aunque alguno podria estar buscando niveles de acceso mas restringidos), sino de aprender mas sobre la operacion general del sistema. Contrariamente a lo que piensan los medios de comunicacion, la mayoria de los hackers no destruyen y no dañan deliberadamente los datos. El hacerlo iria en contra de su intencion de mezclarse con el usuario normal y atraeria la atencion sobre su presencia, haciendo que la cuenta usada sea borrada. Despues de gastar un tiempo sustancioso en conseguir la cuenta, el hacker pone una alta prioridad para que su uso no sea descubierto. Ademas de la obvia relacion 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 informatico. El mero hecho de conseguir el acceso (adivinando la clave de acceso) no es suficiente para conseguir la denominacion. Debe haber un deseo de liderar, explotar y usar el sistema despues de haber accedido a él. Esta distincion parece

logica, ya que no todos los intrusos mantienen el interes una vez que han logrado acceder al sistema. En el submundo informatico, las claves de acceso y las cuentas suelen intercambiarse y ponerse a disposicion del uso general. Por tanto, el hecho de conseguir el acceso puede considerarse como la parte "facil", 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 telefonicos. Se convirtio en una actividad de uso comun 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 facturacion de las compañías telefonicas. Permite llamar a de cualquier parte del mundo sin costo practicamente. En muchos casos, tambien evita, o al menos inhibe, la posibilidad de que se pueda trazar el camino de la llamada hasta su origen, evitando asi la posibilidad de ser atrapado. Par la mayor parte de los miembros del submundo informatico, 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 telefonico. La mayoria de la gente, aunque usa el telefono, sabe muy poco acerca de él. Los phreakers, por otra parte, quieren aprender mucho sobre el. Este deseo de conocimiento lo resume asi un phreaker activo: "El sistema telefonico es la cosa mas interesante y fascinante que conozco. Hay tantas cosas que aprender. Incluso los phreakers tienen diferentes areas 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 informacion. Yo mismo quisiera trabajar para una empresa de telecomunicaciones, haciendo algo interesante, como programar una central de conmutacion. 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 mayoria de la gente del submundo no se acerca al sistema telefonico con esa pasion. Solo estan interesados en explorar sus debilidades para otros fines. En este caso, el sistema telefonico 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 informatico, la posibilidad de actuar asi se agradece, luego llego el uso de la tarjeta telefonica. Estas tarjetas abrieron la puerta para realizar este tipo de actividades a gran escala. Hoy en dia no hace falta ningun equipo especial. Solo un telefono con marcacion 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 motivacion son llamados hackers, aquellos que desean conocer el sistema telefonico 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 distincion. Finalmente llegamos a la "telepirateria" del software. Consiste en la distribucion ilegal de software protegido por los derechos de autor. No nos refiererimos 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 traves de un modem telefonico, 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. Asi, por el precio de una sola llamada telefonica, uno puede amontonar una gran cantidad de paquetes de software. En muchas ocasiones, incluso se evita pagar la llamada telefonica. Notese que al contrario que las dos actividades de hacker y phreaker, no hay ninguna consideracion al margen de "prestigio" o "motivacion" en la telepirateria. En este caso, el cometer los actos basta para "merecer" el titulo. 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 modem y algun 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 ningun tipo de admiracion o prestigio en el submundo informatico. (Una posible excepcion la constituyen aquellos que son capaces de quitar la proteccion del software comercial.) Aunque los hackers y los phreakers de la informatica probablemente no desaprueben la pirateria, 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 mayoria de los telepiratas carecen de conocimientos informaticos especiales, y por tanto son conocidos por abusar en exceso de la red telefonica para conseguir el ultimo programa de juegos. Un hacker mantiene la teoria de que son estos piratas

los culpables de la mayoria de los fraudes con tarjetas de credito telefonicas. "Los medios de comunicacion afirman que son unicamente 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 codigos en la calle." Otro hacker explica que el proceso de intercambiar grandes programas comerciales por modem normalmente lleva varias horas, y son estas llamadas, y no las que realizan los "entusiastas de telecomunicaciones", las que preocupan a las compañias telefonicas. Pero sin considerar la ausencia de conocimientos especiales, por la fama de abusar de la red, o por alguna otra razon, parece haber algun tipo de division entre los hackers / phreakers y los telepiratas. Despues de haber descrito los tres papeles del submundo informatico, podemos ver que la definicion presentada al principio, segun la cual un hacker era alguien que usaba una tarjeta de credito telefonico robada para cargar alguno de los ultimos juegos, no refleja las definiciones dadas en el propio submundo informatico. Obviamente, corresponde a la descripcion 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 impresion de que un individuo es un hacker, un phreaker o un telepirata exclusivamente. Estas categorias 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. Recuerdese 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 telefonica no explica sobre su red y el objetivo de un telepirata es obtener una copia del software mas moderno para su ordenador. Asi, aunque un individuo tenga un conocimiento especial sobre los sistemas telefonicos, 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 semantico. Independientemente de que a un hacker se le etiquete erroneamente como telepirata, los accesos ilegales y las copias no autorizadas de software comercial van a seguir produciendose. Pero si queremos conocer los nuevos desarrollos de la era informatica, 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 habra alguien que este en desacuerdo con las diferencias que se han descrito entre los grupos. En el desarrollo de esta investigacion, quedo de manifiesto que los individuos que realizan actualmente estas actividades no se ponen de acuerdo en cuanto a donde estan las fronteras. Las categorias y papeles, como se ha indicado previamente, no son mutuamente exclusivos. En particular, el mundo de los hackers y los phreakers estan muy relacionados.

Pero, de la misma forma que no debemos agrupar toda la actividad del submundo informatico bajo la acepcion de hacker, tampoco debemos insistir en que nuestras definiciones sean exclusivas hasta el punto de ignorar lo que representan. Las tipologias que he presentado son amplias y necesitan ser depuradas. Pero representan un paso mas en la representacion precisa, especificacion e identificacion de las actividades que se dan en el submundo de la informatica.

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.

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.

MÉTODOS Y HERRAMIENTAS DE ATAQUE

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.

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 estan direccionados a la computadora donde estan instalados. El sniffer puede ser colocado tanto en una estacion 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 deliverada. 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 informacion 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 examenes, 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 comun 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 identificacion 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 estan 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 examenes 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 recusos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, asi 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 conección. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (o sea que este ataque involucra tambien spoofing). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conecciones abiertas, no dejando lugar a las conecciones 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 contínua, 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 destruira, 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 rapidamente, 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 traves de cualquier red o Internet. Y ademas son multiplataforma, es decir, no estan 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 rapidamente 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 algun virus en los últimos 5 años.

EXPLOTACIÓN DE ERRORES DE DISEÑO, IMPLEMENTACIÓN U OPERACIÓN

Muchos sistemas estan expuestos a agujeros de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de puertas invisibles han sido descubiertas en aplicaciones de software, sistemas operativos, protocolos de red, browsers de Internet, correo electronico y todas clase de servicios en LAN o WANs.

Sistemas operativos abiertos como Unix tienen agujeros mas conocidos y controlados que aquellos que existen en sistemas operativos cerrados, como Windows NT. Constantemente encontramos en Internet avisos de nuevos descubrimientos de problemas de seguridad (y herramientas de hacking que los explotan), por lo que hoy tambien se hace indispenable contar con productos que conocen esas debilidades y pueden diagnosticar un servidor, actualizando su base de datos de tests periodicamente.

Ademas de normas y procedimientos de seguridad en los procesos de diseño e implementacion de proyectos de informática.

OBTENCIÓN DE PASSWORDS, CÓDIGOS Y CLAVES

Este método (usualmente denominado cracking), comprende la obtencion 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 algun 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 enfasis en la parte humana con politicas claras (como se define una password?, a quien se esta autorizado a revelarla?) y una administracion eficiente (cada cuanto se estan cambiando?)

No muchas organizaciones estan 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?.

ELIMINAR EL BLANCO

Ping mortal. Algunos ataques eliminan el blanco en lugar de inundarlo con trabajo. Un ejemplo de este tipo es el ping mortal, un paquete ping ilícitamente enorme, que hace que el equipo de destino se cuelgue. Muchas implementaciones de routers, la mayoría de los Unix y todas las versiones de Windows se mostraron vulnerables a este ataque cuando se lo descubrió por primera vez hace un par de años. A pesar de que los vendedores lanzaron parches de inmediato, hay todavía cantidades significativas de hosts "no corregidos" en las redes de producción (en especial, las que corren bajo el Windows 95).

TCP/IP permite un tamaño máximo de paquete de 64 kilobytes (KB, este máximo está dividido en piezas mucho más pequeñas a través de protocolos de capas más bajas, como Ethernet o token ring, pero dentro de una computadora, paquetes mucho más grandes son posibles). Para lidiar con un paquete de 64 KB, la cola TCP/IP asigna un buffer en memoria de 64 KB. Al recibir una cantidad ilícitamente grande de información, como un ping mortal, el buffer del equipo de destino se desborda y el sistema se puede colgar. Todos los IDS que se probaron detectaron paquetes de ping mortal en nuestro test.

OTRA FORMA DE "COLGAR" UN EQUIPO

Land. Otro método para colgar un equipo es el denomindo Land attack, en el que se genera un paquete con direcciones IP y puertos de fuente y destino idénticos. Existen diferentes variantes para este ataque. Una de ellas usa idénticas direcciones IP de fuente y destino, pero no números de puertos.

Fue esta variación la que utilizó NSTL contra el primer par de productos testeados y los dos identificaron el tráfico como un land attack. El tercer producto que se probó, el Netranger, de Cisco, identificó a un land attack solamente (y correctamente) cuando ambas direcciones y números de puerto eran idénticos. El ingeniero de Cisco agregó enseguida una nueva regla, que detectaba a los paquetes con direcciones idénticas nada más. Una vez más, esto pone de manifiesto la importancia de saber qué es lo que se debe buscar.

Supernuke. Un ataque característico de los equipos con Windows es el Supernuke (llamado también a veces Winnuke), que hace que los equipos que escuchan por el puerto UDP 139 se cuelguen. Netbios es un protocolo integral para todas las versiones en red de Windows. Para transportar Netbios por IP, Microsoft ideó el Windows Networking (Wins), un esquema que enlaza el tráfico Netbios a puertos TCP y UDP 137, 138 y 139. Al enviar a estos puertos fragmentos UDP, se pueden arruinar equipos Windows que no estén arreglados o disminuir la velocidad del equipo durante un largo tiempo.

En cuanto a la inundación ICMP, todos los IDS reconocieron a los ataques Supernuke.

Teardrop 2. El ataque más reciente a nuestra base de datos, el Teardrop 2, data de fines de 1997. Al igual que el Supernuke, los ataques Teardrop 1 y Teardrop 2 afectan a fragmentos de paquetes. Algunas implementaciones de colas IP no vuelven a armar correctamente los fragmentos que se superponen, haciendo que el sistema se cuelgue. Windows NT 4.0 de Microsoft es especialmente vulnerable a este ataque, aun cuando se ha aplicado el Service Pack 3. La empresa hizo un parche del Teardrop 1 en mayo de 1997, pero se mostró vulnerable al Teardrop 2, que supuso colocar una bandera de "urgente" en la cabecera de un fragmento TCP. Hasta el lanzamiento de un hot fix en enero de 1998.

En cuanto al ataque Dig, el actual lanzamiento del Realsecure, de ISS no vio el ataque del Teardrop 2. Sí lo vio el lanzamiento beta de la versión 2.5.

¿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".

BUSCADORES DE AGUJEROS

En la Argentina existe un grupo de laboratorios y consultoras dedicado a buscar "agujeros" en los sistemas de seguridad. Core SDI tiene sus propios laboratorios, donde se investigan y evalúan las distintas tecnologías de seguridad informática para desarrollar otras en función de los resultados que obtienen.

Además de proveer software, Zampatti, Maida & Asociados ofrece servicios de consultoría, soporte técnico y capacitación. También envía por e−mail un resumen con las últimas noticias acerca de nuevos virus y problemas de seguridad en programas de encriptación.

Por su parte, la empresa GIF tiene servicios de seguridad informática, controla fraudes y desarrolla software para proteger la información, como Firewalls (barreras de seguridad entre una red interna conectada a Internet o a una intranet) y sistemas de encriptación.

Todas tienen el mismo objetivo: investigar las tecnologías de seguridad informática y adaptarlas (si se puede) a las necesidades argentinas.

Hoy, en muchas corporaciones, un hambre de información perpetuo e insaciable ha generado temas de seguridad graves y difíciles de solucionar. El crecimiento de Internet ha generado un aumento en las posibilidades de intrusión electrónica desde adentro y desde afuera de las empresas.

No cabe duda de que los gerentes de sistemas y de redes necesitan contar con métodos y mecanismos efectivos, capaces de detectar ataques y disminuir el riesgo de robo de información, sabotaje y todo acceso no deseado a datos de la empresa.

A pesar de que los "net management systems" (sistemas de administración de redes), los "routers" y los "firewalls" son capaces de registrar problemas de la red predefinidos, un nuevo tipo de software llamado intrusion detection system (IDS) (sistema de detección de intrusos) los supera en términos de qué es lo que detectan y cómo denuncian los problemas potenciales a los gerentes de redes.

Los productos IDS no eliminan todos los problemas de seguridad, pero ofrecen beneficios que los convierten en una opción que vale la pena considerar.

Para observar la conducta real de los IDS, NSTL Inc. (Conshohocken, PA) revisó de forma sistemática y

probó cinco productos IDS de primera línea, fabricados por Anzen, Cisco, ISS e Internet Tools Inc. Estas pruebas proveen a los gerentes de redes de toda la información que necesitan para determinar de qué forma los productos IDS pueden servir a sus necesidades de protección de la red.

Los resultados de la prueba de NSTL permiten también a los gerentes de redes tomar prudentes decisiones de compra, basadas en "rated management capabilities" (capacidades nominales de administración) y "benchmarked performance" (performance de pruebas).

CARACTERÍSTICAS DE LOS IDS

Varias cualidades importantes de los IDS los ubican bastante más allá de los "network management systems", los "routers", los "firewalls" y otros medios de protección de redes.

Todos los productos, con excepción del Sessionwall−3, de Abirnet Inc. (Dallas), constan de un monitor y una "management station" (estación de administración) que recoge información de monitores (Sessionwall−3 es manejado de forma local).

A diferencia de los productos de monitoreo remoto (RMON), los IDS no usan SNMP −que en estos momentos carece de rasgos de seguridad claves− para transmitir información del monitor al gerente. En lugar de ello, los IDS utilizan diversos medios de autenticación y codificado. Todas las interfases de monitoreo de los productos, con excepción de ID−Trak, de Internet Tools Inc. (Fremont, California) son pasivas, de forma tal de que los agresores no estarán en condiciones de detectar nada si hay un IDS escuchando.

Los productos IDS que se probaron incluyen también rutinas predefinidas para detectar ataques específicos, y permiten a vendedores y usuarios agregar rutinas que detectan ataques nuevos apenas se

los descubre. De todas maneras, existen grandes diferencias en cuanto a qué tipo de definiciones están disponibles para los usuarios.

LAS REDES NECESITAN CENTINELAS CADA VEZ MÁS ATENTOS

Atender de manera eficiente la seguridad de una red se hace cada vez más difícil. A pesar de que las herramientas se mejoran día a día, los hackers también aumentan su nivel de conocimientos técnicos y de sofisticación. En general, las empresas y las organizaciones son cada vez más conscientes de los riesgos y permanentemente tratan de aumentar los niveles de protección. Pero la lucha, como dice el tango, "es cruel y es mucha".

VULNERAR PARA PROTEGER

Los hackers utilizan diversas técnicas para quebrar los sistemas de seguridad de una red. Básicamemte buscan los puntos débiles del sistema para poder colarse en ella. El trabajo de los testers no difiere mucho de esto. En lo que sí se diferencia, y por completo, es en los objetivos.

Mientras que los hackers penetran en las redes para dañar o robar información, un testers lo hace para poder mejorar los sistemas de seguridad.

Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se lo conoce como Penetration Testing, uno de los recursos más poderosos con los que se cuenta hoy para generar barreras cada vez más eficaces.

En cuanto a las barreras de seguridad, un testers explica: "Están totalmente relacionadas con el tipo de información que se maneja en cada organización. Por consiguiente, según la información que deba ser

protegida, se determinan la estructura y las herramientas de seguridad. No a la inversa".

Pero las herramientas no son sólo técnicas. El soft y el hard utilizados son una parte importante, pero no la única. A ella se agrega lo que se denomina "políticas de seguridad internas", que cada empresa u organización debe generar.

La explicación del porqué viene de un dato de la realidad. Según un reciente informe de la publicación estadounidense InformationWeek, un porcentaje sustancial de intrusiones en las redes de las empresas (ya sean chicas, medianas o grandes) proviene de ataques internos. Es decir, los mismos empleados hackean a su propia organización. Y aquí es donde cobran especial importancia las políticas de seguridad que se establezcan, además del aspecto técnico.

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 prestén 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 dolares anuales solo en los EEUU"

En la era de la informacion, 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 comercializacion y diseño de productos.

Cuanto valen ellos para su organizacion?

Cuan importante es esta informacion para el exito de su empresa?

En su estado actual, la informacion que esta almacenda en su red no es utilizada con comodidad si la misma no es de facil acceso e intercambio. Esto significa, que usted debe elegir entre accesibilidad sobre seguridad?. Muchas companias piensan que ellos deben dejar que la informacion 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 informacion 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 funcion del firewall es ser una solida 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 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 intromision a su red.

Estas son algunas de sus carateristicas tecnicas:

· Dos tipos de configuracion, local y remota.

· Configuracion remota por medio de una interface grafica que corre sobre sistema operativo Windows 95/NT.

· Configuracion 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 tasacion de tiempos de coneccion y uso de servicios.

· Soporta el uso de proxy−server para la configuracion de su red interna.

· Conexiones de todos los servicios comunes de TCP/IP atraves 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 configuracion de servidores que proveen servicios hacia el exterior de la red interna por medio de normas de seguridad.

· Multiples alarmas de intentos de ingreso fallidos hacia la red.

· Sistema de alarmas configurable que permite el envio de avisos por medio de FAX, Pager, Mail, Voice Mail y advertencia visuales.

· Filtro de acceso de conecciones permitidas por interfaces no permitidas, este filtro es importante para contrarestar tecnicas IP−SPOOFING.

· La configuracion del firewall se puede hacer mediante el mismo server o desde un servidor remoto corriendo un sistema de administracion especifico que utiliza para esta tarea una interface dedicada o TUNNELING (comunicacion 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 comunicacion se encuentren dos FIREWALL tambien se puede efectuar la conexion 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 modulos de alarmas corren tanto dentro del FIREWALL (centralizador de alarmas) como tambien en los servidores de su red para poder brindar detalles mas especificos.

El sistema de configuracion permite agregar servicios no estandar a su red y usar estos con el modulo de TUNNELING (comunicacion 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 auditorías 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 auditoría; 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 desifrables, 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.

SEGURIDAD INFORMÁTICA

Toda organización debe estar a la vanguardia de los procesos de cambio. Donde disponer de información continua, confiable y en tiempo, constituye una ventaja fundamental.

Donde tener información es tener poder.

Donde la información se reconoce como:

· Crítica, indispensable para garantizar la continuidad operativa de la organización.

· Valiosa, es un activo corporativo que tiene valor en sí mismo.

· Sensitiva, debe ser conocida por las personas que necesitan los datos.

Donde identificar los riesgos de la información es de vital importancia.

La seguridad informática debe garantizar:

· La Disponibilidad de los sistemas de información.

· El Recupero rápido y completo de los sistemas de información

· La Integridad de la información.

· La Confidencialidad de la información.

Nuestra Propuesta

· Implementación de políticas de Seguridad Informática.

· Identificación de problemas.

· Desarrollo del Plan de Seguridad Informática.

· Análisis de la seguridad en los equipos de computación.

· Auditoría y revisión de sistemas.

HACKING EN WINDOWS95

ACCEDIENDO AL MS−DOS

Es de real importancia aclarar que realizar actividades de Hackeo en Windows es una tarea que principalmente es realizada por los que recién comienzan. Por cuestiones de conocimiento nos restringiremos a abarcar solamente Windows ya que la ejemplificación en otros sistemas operativos como UNIX serían de real complejidad.

Windows95 realmente no es un sistema operativo. Trabaja sobre el MS−DOS, que sí lo es, pero que a su vez no proporciona ninguna seguridad.

Ej. Desde el prompt del MS−DOS cualquier persona con solo ejecutar el comando format puede destruir todo el disco rígido y el sistema no lo impedirá.

Sin embargo, en Windows95 el sistema comprueba siempre las restricciones aplicadas a los usuarios por el administrador. ¿Qué quiere decir esto? Que se tiene acceso al MS−DOS, la computadora es vulnerable.

Pero ahora se plantea un problema: Muchos administradores de sistemas "prohiben" la entrada en MS−DOS de sus usuarios. ¿Cómo entrar entonces?

Primero: A través del menú ejecutar.

Pulsar sobre Inicio, luego Ejecutar, escribir "Command" (sin comillas) y pulsar enter.

Segundo: A través de la ayuda

Con un editor de textos hexadecimal como WordPad (no el block de notas) abrir el archivo "COMMAND.COM", luego ir a la opción "Guardar como..." normalmente en el menú "Archivo" y guardarlo, en el directorio dónde esté instalado Windows95 con el nombre de "WINHLP32.EXE". Ahora, cada vez que se pulse la tecla F1, tendrá un prompt del MS−DOS

Tercero: Saltándose el inicio de Windows95

Al encender el sistema. Pulsando F8 cuando aparece el mensaje "Iniciando Windows95" y seleccionando después "Sólo símbolo de MS−DOS" accederá al mismo. Un método no muy bueno, pues muchos

administradores desactivan el teclado en el inicio del Windows95.

Cuarto: A través de la pantalla "Ahora puede apagar el equipo"

Lo que sucede realmente al apagar el sistema es que Windows95 se descarga de memoria y presenta el famoso dibujito en la pantalla. Pero he aquí lo importante: Nos deja sobre MS−DOS. Probar escribir "CLS". La pantalla se borrará y aparecerá el prompt del MS−DOS, en un modo gráfico un tanto peculiar. Para ver el prompt en modo de texto, escribir "MODE 80".

PASSWORDS

Paso uno: Arrancar la computadora.

Paso dos: Cuando aparezca la pantalla de "Iniciando el sistema" o "Configuración del sistema" (depende de las versiones), pulsar la tecla "F5", si el ordenador no muestra esa pantalla, simplemente tocar la tecla "F5" todo el tiempo.

Si Windows95 tiene la configuración correcta, la tecla F5 permitirá arrancar en "modo de a prueba de fallos". Una vez cargado el sistema todo va parecer extraño, pero no será necesario dar un password y aún así se podrá utilizar los programas.

Otra manera de saltar el password.

Paso uno: Arrancar la computadora.

Paso dos: cuando aparezca la pantalla "configuración del sistema", pulsar F8.

Accediendo al Menú de Inicio de Microsoft Windows 95.

Paso tres: Elegir la opción 7, modo MS−DOS. En el prompt, teclear el comando " rename c: \windows*. pwl c: \windows*. zzz "

Nota: MS−DOS significa Microsoft Disk Operating System, un antiguo sistema operativo que data de 1981. Es un sistema operativo de línea de comandos, lo que significa que aparece un prompt (probablemente c: \>) tras el cual es posible teclear un comando y pulsar la tecla Enter. MS−DOS se suele abreviar por DOS. Es un poco parecido a UNIX, y de hecho en su primera versión incorporaba miles de líneas de código UNIX.

Paso cuatro: reiniciar. De esta forma se obtendrá el cuadro de diálogo de password. Entonces

Puede ingresarse cualquier password que se nos ocurra. Posteriormente pedirá nuevamente el ingreso del password para confirmar el cambio.

Paso cinco: Para no dejar rastros de la violación del password podrá utilizarse cualquier herramienta que se desee, Administrador de Archivos, Explorador o MS−DOS para renombrar *. zzz otra vez a *.pwl.

Paso seis: reiniciar y comprobar el funcionamiento del viejo password.

Si alguien estuviese husmeando en el ordenador con Windows95 de otra persona, usando esta técnica, el único modo en que la víctima se podría dar cuenta de que hubo un intruso en el sistema es comprobar los archivos recientemente modificados y descubrir que los archivos *. pwl han sido toqueteados.

Consejo: A menos que en el archivo msdos.sys la opción bootkeys=0 esté activada, las teclas que pueden

hacer algo durante el arranque son F4, F5, F6, F8, Shift+F5, Control+F5 y Shift+F8.

Ahora supongamos que se descubrió que Windows95 no responde a las teclas de arranque. Todavía es posible entrar.

Si la computadora permite el uso de las teclas de arranque, puede que se desee desactivarlas para contar con un poco más de seguridad.

El modo más fácil pero a su vez más lento para desactivar las teclas de arranque es configurarlas adecuadamente mientras se instala el Windows95. Pero la forma más rápida para hacerlo es la siguiente.

Editando el archivo msdos.sys de Windows95, que controla la secuencia de arranque.

El modo fácil de editar el archivo Msdos.sys es:

Paso cero: Hacer una copia del disco rígido entero, especialmente de los archivos de sistema. Asegurarse que se tiene un disco de arranque de Windows95. Estamos a punto de jugar con fuego! Si se está haciendo esto en el ordenador de otra persona, esperemos que se cuente con el permiso para destruir el sistema operativo.

Nota: En el caso de no contar con un disco de arranque se necesitará un disco vacío y los discos de instalación de Windows95. Hacer click en Inicio, luego en Configuración, Panel de

Control, en Agregar/Quitar Programas y finalmente entonces en Disco de Inicio.

Desde ahí simplemente seguir las instrucciones.

Paso uno: Encontrar el archivo msdos.sys. Se encuentra en el directorio raíz (normalmente c: \). Como este es un archivo oculto de sistema, la manera más fácil de encontrarlo es hacer click en Mi PC, hacer click con el botón derecho en el icono del disco rígido (normalmente C:), hacer click en Explorar, y entonces navegar por la unidad hasta encontrar el archivo "msdos.sys".

Paso dos: Hacer que se pueda escribir en el archivo msdos.sys (darle permiso de escritura). Para hacer esto, clickear con el botón derecho en msdos.sys, y entonces hacer click en "propiedades". Esto trae una pantalla en la que se tiene que desactivar las opciones "sólo lectura" y "oculto". Ahora se debe editar este archivo con tu procesador de textos.

Paso tres: Abrir WordPad y el archivo msdos.sys. Es muy importante usar WordPad y no NotePad (bloc de notas) o cualquier otro programa de edición de textos.

Paso cuatro: Ahora estamos preparados para editar. Ahora que se tiene WordPad abierto con el archivo msdos.sys abierto también se verá algo similar a esto:

[Paths]

WinDir=C:\WINDOWS

WinBootDir=C:\WINDOWS

HostWinBootDrv=C

[Options]

BootGUI=1

Network=1

;

;The following lines are required for compatibility with other programs.

;Do not remove them (MSDOS>SYS needs to be >1024 bytes).

Para desactivar las teclas de función durante el arranque, directamente debajo de [Options] se tiene que insertar el comando "BootKeys=0." .

Otra manera de desactivar dichas teclas de arranque, es insertar el comando BootDelay=0. Guardar msdos.sys.

Paso cinco: ya que msdos.sys es absolutamente esencial para la computadora, mejor sería que se protegiese contra escritura ahora (es decir, dejarlo como estaba antes de que se editase). Hacer click en Mi PC, entonces en Explorar, luego clickear en el icono del disco rígido (normalmente C:), entonces encuentra el archivo msdos.sys. Hacer click en y luego en propiedades. Esto vuelve a traer esa pantalla con las opciones de "sólo lectura" y "oculto". Activar la opción de "sólo lectura".

Paso seis: reiniciar la computadora

Nota: evitar correr antivirus!

Modo más Difícil de Editar al archivo Msdos.sys.

Paso cero: Esto es una útil práctica para poder usar MS−DOS algún día en WindowsNT LANs, y servidores de Internet o Webs. Poner un disco de inicio de Windows95 en la unidad a: . Reiniciar.

Esto nos regresará prompt A: \.

Paso uno: Otorgar permiso de escritura a msdos.sys. Correr comando "attrib −h −r −s c: \msdos.sys" (Se da por hecho que la unidad c: es el disco duro.)

Paso dos: Entrar el comando "edit msdos.sys". Esto trae este archivo al procesador de textos.

Paso tres: Utilizar el programa Edit para alterar msdos.sys. Guardar. Salir del programa Edit.

Paso cuatro: En el prompt del MS−DOS, introducir el comando "attrib +r +h +s c: \msdos.sys" para volver a dejar el archivo en su estado original (oculto, de sistema, sólo lectura).

Ahora las teclas de inicio de la computadora están desactivadas. Significa esto que nadie puede entrar en el sistema?

Como seguramente habrá deducido de "Modo más Difícil de Editar Msdos.sys", la siguiente opción para acceder a Windows95 es usar un disco de inicio que vaya en la unidad a: .

Cómo Acceder al Sistema de Win95 Usando un Disco de Inicio

Paso uno: apagar la computadora.

Paso dos: poner el disco en la unidad A: .

Paso tres: encender la computadora.

Paso cuatro: en el prompt de A: , teclear el comando:

"rename c:\windows*.pwl c:\windows*.zzz".

Paso cinco: reiniciar otra vez. Puede introducir lo que sea o nada en la ventana del password y entrar.

Paso seis: Cubrir huellas renombrando los archivos de passwords otra vez a como estaban al principio.

Este es un truco común en LANs en las que el administrador de red no quiere tener que ocuparse de la gente que va curioseando en los ordenadores de otras personas. La respuesta (no es una respuesta demasiado buena) es usar un password del CMOS.

Cómo Jugar con el CMOS

Las configuraciones básicas en la computadora como por ejemplo cuántos y de qué clase son las unidades de disco que posee y cuáles de ellas son usadas en el arranque están controladas en un chip del CMOS en la placa base. Una diminuta batería mantiene este chip funcionando siempre para que en cualquier momento que enciendas de nuevo la computadora, recuerde cuál es la primera unidad que debe revisar para recibir instrucciones de inicio. En una PC de hogareña normalmente se lee primero la unidad A: . Si la unidad A: está vacía, a continuación mirar en la unidad C: .

Si deseo cambiar la configuración del CMOS deberé pulsar la tecla "delete" al principio de la secuencia de inicio. Entonces configuro el CMOS para que pida password de acceso, tengo que teclear el password para entrar y realizar los cambios que desee.

Si yo no quiero que nadie arranque la computadora desde la unidad A: y juegue con el archivo de passwords, puedo configurarlo para que arranque únicamente desde la unidad C: . O incluso que sólo arranque desde una unidad remota en una LAN.

Entonces, existe alguna manera de penetrar en un sistema de Windows95 que no arranque por la unidad A: ? Absolutamente sí, pero antes de probarlo, debe asegurarse de anotar la configuración *COMPLETA* del CMOS. Y estar preparado para un naufragio total de la computadora. Hackear las configuraciones de las CMOS es incluso más destructivo que hackear archivos de sistema.

Paso uno: conseguir un destornillador de precisión y el material necesario para soldadura de componentes electrónicos.

Paso dos: abrir la computadora.

Paso tres: quitar la batería.

Paso cuatro: volver a enchufar la batería.

Paso alternativo al tres: muchas placas base poseen un jumper de 3 pins para reiniciar la CMOS a su configuración por defecto. Buscar un jumper situado cerca de la batería o mirar en el manual si tiene uno. Por ejemplo, podría encontrar un dispositivo de 3 pins con los pins 1 y 2 conectados. Si quita los puentes de los pins 1 y 2 y lo deja así durante unos cinco segundos, puedes reiniciar la CMOS.

Advertencia: esto puede no funcionar en todas las computadoras!

Paso cinco: la computadora tiene ahora la CMOS con su configuración por defecto. Poner todo como estaba al principio, con la excepción de decirle que compruebe primero la unidad A: durante el arranque.

Advertencia: esto no es recomendable si utiliza la computadora del trabajo

Paso seis: proceder con las instrucciones de acceso a través de la unidad A: durante el arranque explicadas antes.

Cómo Jugar con el CMOS 2:

Hay una solución fácil Al problema del password de CMOS. Es un programa llamado KillCMOS que puede bajarse de http: //www.koasp.com

Ahora supongamos que le gusta navegar por la WWW pero Windows95 tiene instalado alguna clase de programa que te restringe el acceso a sitios que realmente te gustaría visitar. Significa esto que está realmente restringido a él?. Claro que no.

Hay varios modos de saltarse esos programas que censuran los Web sites que se desea visitar.

Esto no tiene como objetivo fomentar la pornografía infantil. El hecho lamentable es que estos programas de censura de la Red no tienen posibilidad de analizar todo el contenido de una Web. Lo que hacen es sólo permitir el acceso a un pequeño número de Webs.

La primera táctica a usar con un programa censor de WWW es pulsar ctrl−alt−supr. Esto hace aparecer la lista de tareas. Si el programa de censura está en la lista, podrá apagarse.

La segunda táctica es editar el archivo autoexec.bat para borrar cualquier cosa relacionada con el programa de censura. Esto evita que sea cargado al principio.

Pero qué pasa si existe un control sobre dónde ha estado navegando? Tiene que deshacerse de esos comprometedores registros que almacenan los lugares que has visitado!

Es fácil arreglarlo en Netscape. Abra Netscape.ini con Notepad (block de notas) o WordPad. Probablemente estará en el directorio C: \Netscape\Netscape.ini. Cerca de la parte final encontrará el historial de URLs visitadas. Ahora podrá Borrar esas líneas.

En Internet Explorer solo tiene que editarse el Registro y eliminar la característica de censura del Internet Explorer.

Nota: Cualquiera que controle el Registro de un servidor de red controla la red, totalmente. Cualquiera que controle el Registro de un Windows95 o NT controla ese ordenador, totalmente. La habilidad para editar el Registro es comparable a obtener acceso de root en un sistema UNIX.

Paso cero: Hacer una copia de seguridad de todos los archivos. Tener un disco de inicio a mano. Si se modifica el Registro de forma incorrecta se tendrá que reinstalar el sistema operativo.

Advertencia: Si edita el Registro de una computadora en el trabajo, puede traerle muchos problemas

Paso uno: Encuentre el Registro. Esto no es sencillo, porque la teoría de Microsoft es "Lo que no se conoce, no se daña". Por tanto la idea es mantener el Registro fuera del alcance de los novatos. Así que se deberá

clickear en Inicio, luego en Programas y a continuación en Explorador de Windows, luego hacer click en el directorio Windows y buscar un archivo llamado "Regedit.exe".

Paso dos: arrancar Regedit clickeando sobre el mismo. Esto hará aparecer varias carpetas:

HKEY_CLASSES_ROOT

HKEY_CURRENT_USER

HKEY_LOCAL_MACHINE

HKEY_USERS

HKEY_CURRENT_CONFIG

HKEY_DYN_DATA

Lo que se debe buscar es alguna clase de archivo de passwords. Esto controla todas las configuraciones, la apariencia del escritorio, qué accesos directos se están usando, a qué archivos se te permite acceder, etc. Si se está acostumbrado a usar UNIX, va haber que repasar cómo ver los permisos de los archivos y los passwords.

Nota: Se puede usar Regedit desde el MS−DOS desde un disco de inicio. Esto es muy útil en ciertas situaciones.

Paso tres: Entrar en una de las carpetas HKEY. Comprobar CURRENT_USER haciendo click en el signo + que hay a la izquierda. El Regedit da opciones en diversos menús para escoger nuevas configuraciones. Todo lo que verá son dibujos sin ninguna pista de cuál es la apariencia de estos archivos en MS−DOS. Esto se llama "seguridad por oscuridad".

Paso cuatro: Ahora empezaremos a actuar como verdaderos hackers. Vamos a poner parte del archivo en un lugar donde podamos verlo y modificarlo. Primero hacer click en KEY_CLASSES_ROOT para que aparezca resaltada. Luego ir a la barra de menú de Regedit y clickear en la primera opción, "Registro", y entonces elegir "Exportar archivo del registro". Poner el nombre que quiera, pero asegúrese de que acaba con ".reg".

Paso cinco: Abrir esa parte del registro en el WordPad. Es importante el usar ese programa y no otros como por ejemplo el Bloc de notas.

Advertencia: si se clickea normal en (con el botón izquierdo del ratón), automáticamente será importado de vuelta al Registro y accidentalmente puede dañarse la computadora durante bastante tiempo.

Paso seis: Ahora es posible leer todo lo que siempre Windows y Microsoft temió que descubriera sobre seguridad. Cosas como por ejemplo:

[HKEY_CLASSES_ROOT\htmlctl.PasswordCtl\CurVer]

@="htmlctl.PasswordCtl.l"

[HKEY_CLASSES_ROOT\htmlctl.PasswordCtl.1]

@="PasswordCtl Object"

[HKEY_CLASSES_ROOT\htmlctl.PasswordCtl.1\CLSID]

@="{EE230860−5A5F−11CF−8B11−00AA00C00903}"

Lo que hay entre las llaves en esta última línea es un password encriptado que controla el acceso a un programa o las características de un programa como el de censura de red que posee el Internet Explorer. La función es encriptar el archivo cuando se teclea, y entonces compararlo con la versión desencriptada que posee en el archivo.

Paso siete: No es realmente obvio qué password corresponde con qué programa. Lo que se recomienda es... borrarlos todos!. Por supuesto esto significa que los passwords almacenados para acceder por ejemplo al ISP pueden desaparecer. También, Internet Explorer hará aparecer un mensaje como "La configuración del controlador de contenidos se ha perdido. Alguien puede haber intentado modificarla".

Es una buena idea empezar a conocer cómo usar el disco de inicio para reinstalar Windows95 por si algo sale mal.

Paso ocho (opcional): Se quiere borrar los registros de sitios visitados?

En el Internet Explorer tendrá que editar HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE y HKEY_USERS. También puede borrar los archivos c: \windows\cookies\mm2048.dat y c: \windows\cookies\mm256.dat, ya que estos archivos también almacenan datos sobre URLs.

Paso nueve: Importar los archivos .reg de regreso al Registro. Hacer click en los archivos .reg en el Explorador o usar la herramienta "Importar" que se encuentra a continuación de la "Exportar" que usaste en Regedit. Esto sólo funciona si se nombraron con la extensión .reg.

Paso diez: Internet Explorer hará un estridente ruido la primera que se encienda y a continuación aparecerá un mensaje con una gran "X" roja y brillante que dice que he modificado el vigilante de contenidos!

No está todo perdido. Borrar el Registro y sus backups. Están en cuatro archivos: system.dat, user.dat, y sus backups, system.da0 y user.da0. El sistema operativo inmediatamente colapsará. (Esto fue un test realmente excitante) Pero es importante saber que la Papelera de Reciclaje todavía funciona aún después de haber eliminado los archivos del Registro, por lo que se puede restaurarlos y la computadora volverá a ser la misma de antes. Luego cargar esos archivos y apagarla.

Entonces usar el disco de inicio de Windows95 para resucitar la computadora. Reinstalar Win95.

Entonces por qué en vez de tener que editar el Registro, no recomendamos simplemente se borrase esos archivos y se reinstale Windoes95?

Porque es importante aprender cómo editar el Registro de un ordenador WindowsNT. Sólo se ha probado un poco de cómo sería en uno de esos sistemas.

No se ha analizado todas las maneras de penetración remota en un sistema con Win95, pero existen multitud de maneras. Cualquier sistema con Windows95 que está conectado a una red es vulnerable, a menos que se encripte la información.

QUE PUEDE HACERSE CON UNA CONEXIÓN Y WINDOWS 95?

Esta sección esta destinada a informar que tipos de Hacking se pueden realizar utilizando dos herramientas de las más típicas, el sistema Operativo Windows 95 y un servicio de Internet básico.

En esta lección especificará como:

− Usar comandos del Windows95 y MS−DOS secretos para escanear y navegar por puertos de las computadoras usadas por proveedores de servicios de Internet (ISP).

− Hacer telnet a ordenadores que permitan usar las valiosas herramientas.

− Bajar herramientas como por ejemplo escaneadores de puertos y crackeadores de passwords diseñados para su uso en Windows.

− Usar Internet Explorer para saltar las restricciones en esos programas que pueden utilizarse en el colegio, la facultad o el trabajo.

Pero actualmente existe una buena razón para aprender a hackear desde Windows.

Algunas de las mejores herramientas para probar y manipular redes Windows se encuentran sólo en WindowsNT. Además, con Windows95 es posible practicar el Hacking del Registro, que es importante para conseguir objetivos en Servidores WindowsNT y las redes que estos administran.

De echo, es muy importante en ciertas ocasiones conocer Windows, esto es porque WindowsNT es más rápido para acceder a Internet que UNIX.

Hacia el año 2000, el porcentaje de servidores WindowsNT crecerá un 32%. Este débil futuro para los servidores UNIX se ve con más claridad gracias a un estudio que refleja que el porcentaje de sistemas UNIX está disminuyendo actualmente a un ritmo del 17% anual, mientras el de Windows NT aumenta en un 20% por año. (Mark Winther, "The Global Market for Public and

Private Internet Server Software" Abril 1996).

Por lo tanto es una herramienta fuerte es dominar perfectamente Windows.

El secreto para realizar actividades de Hackeo desde Windows95 (o desde cualquier otro ISP que de acceso a World Wide Web) está escondido en el MS−DOS de Windows95 (MS−DOS 7.0).

MS−DOS 7.0 ofrece varias herramientas de Internet, ninguna de las cuales llevan incluidas documentos de instrucciones ni en la ayuda de Windows ni la de MS−DOS.

Para comenzar

Realizar una conexión a través de un ISP a la WWW. A continuación minimizar la ventana y cargar el MS−DOS (INICIO, PROGRAMAS, MS−DOS)

De esta forma es más fácil utilizar los comandos cortar y copiar y a su vez pasar desde las ventanas de programas de Windows a las de MS−DOS y viceversa. Si el MS−DOS aparece en la pantalla completa, se debe pulsar ALT+Enter (Ventana) . En el caso de no poder ver la barra de tareas, se deberá hacer un click en el icono de sistema de la esquina superior izquierda de la ventana y seleccionar Barra de Herramientas.

Ahora es posible elegir entre ocho utilidades de TCP/IP con las cual trabajar:

telnet, arp, ftp, nbtstat, netstat, ping, route, y tracert.

Telnet es la más importante, es posible también acceder al programa de Telnet directamente desde Windows, pero mientras se está hackeando pueden llegar a necesitarse otras utilidades que sólo pueden ser usadas desde MS−DOS, por ello esta metodología de trabajo.

Con el telnet de MS−DOS es posible navegar por los puertos casi como lo harías si se usara el telnet de UNIX. Pero existen varios trucos que se necesitan conocer para hacer este trabajo.

Primero, probaremos a hacer Login a cualquier ordenador desconocido, para hacer esto debe verse el prompt de MS−DOS, C:\WINDOWS> e introducirse el comando "telnet". Esto hace aparecer una pantalla de telnet, clickear en conectar y entonces en Sistema Remoto.

Esto hace aparecer un cuadro que pide "Nombre de Host", teclear "whois.internic.net" en este cuadro. Debajo pide "Puerto" y tiene el valor por defecto de "telnet". Dejar "telnet" como puerto seleccionado. Debajo hay otro cuadro que pregunta por "Tipo de terminal". Escoger VT100.

Lo primero que puede hacerse para asustar a los vecinos e impresionar a sus amigos es un "whois". Hacer click en Conectar y pronto aparecer un prompt como este:

[vt100]InterNIC>

Entonces pregúntale a tu vecino o a tu amigo su dirección de e−mail. Luego introduce las últimas dos partes de esa dirección de e−mail. Por ejemplo, si la dirección es "luser@aol.com", teclea "aol.com".

En AOL conseguimos esta respuesta:

[vt100]InterNIC>whois aol.com

Connecting to the rs Database. . . . .

Connected to the rs Database

AOL

12100 Sunrise Valley Drive

Reston, Virginia 22091

USA

Nombre de Dominio: AOL.COM

Contacto Administrativo:

OïDonell, David B (DBO 3) PMDAtropos@AOL.COM

703/453−4255 (FAX) 703/453−4102

Contacto Técnico, contacto regional:

AOL Nombre trouble@isp.net

703/453−5862

Contacto de Facturación:

Barrett, Joe (JB4302) BarrettJG@AOL.COM

703−453−4160 (FAX) 703−453−4001

Record Last Updated on 13−Mar−97

Record Created on 22−Jun−95

Domain Servers in listed order:

DNS−01.AOL.COM 152.163.199.42

DNS−02.AOL.COM 152.163.199.56

DNS−AOL.ANS.NET 198.83.210.28

Las últimas tres líneas nos dan los nombres de algunos de los ordenadores que trabajan para el AOL. Si queremos hackear el AOL, son un buen sitio para empezar.

Nota: Simplemente obtuvimos información de tres "nombres de dominio" del AOL. "aol.com" es el nombre de dominio de AOL, y los servidores de dominio son los ordenadores que controlan la información que le dice al resto de Internet cómo mandar mensajes a ordenadores AOL y direcciones de e−mail.

Nota: Usando Windows95 y una conexión a Internet es posible utilizar el comando whois desde otros muchos ordenadores también. Al hacer telnet al puerto 43 del ordenador objetivo y en caso que pueda pasarse podrá hacerse cualquier petición.

Ejemplo: Hacer telnet a nic.ddn.mil, puerto 43. Una vez que se esté conectado, teclear "whois DNS−01.AOL.COM", o cualquier otro nombre que se desee probar. Sin embargo, esto sólo funciona en ordenadores que tengan activo el servicio whois en el puerto 43.

Advertencia: Simplemente se accede a un ordenador del ejército de los EEUU, pero no hay de que preocuparse, nic.ddn.mil esta abierto al público en muchos de sus puertos. Puede también conectarse a su Web en www.nic.ddn.mil y también a su Server de ftp.

A continuación probar navegar por los puertos (port surfing) de DNS−01.AOL.COM pero es posible no encontrar ninguno abierto. Por tanto seguramente lo que ocurre es que este ordenador se encuentra tras el Firewall del AOL.

Nota : port surfing significa intentar acceder a un ordenador a través de diferentes puertos. Un puerto es cualquier camino por el que la información entra o sale de un ordenador. Por ejemplo, el puerto 23 es el que normalmente se utiliza para hacer Login en una cuenta shell. El puerto 25 se

usa para enviar e−mail. El puerto 80 se utiliza para las Webs. Existen miles de puertos disponibles, pero normalmente un ordenador sólo tendrá activados tres o cuatro de sus puertos. En una computadora común los puertos incluyen el monitor, el teclado y el módem.

A continuación cerrar el programa de telnet y regresar a la ventana del MS−DOS. En el prompt del MS−DOS se deberá teclear el comando "tracert 152.163.199.42", o igual sería teclear "tracert DNS−01.AOL.COM". Con cualquier opción que se escoja se obtendrá el mismo resultado. Este comando

tracert da la ruta que toma un mensaje, de un ordenador hasta otro, desde que viaja desde mi ordenador hasta ese servidor de dominio del ISP. Aquí está lo que obtendremos:

C:\WINDOWS>tracert 152.162.199.42

Tracing route to dns−01.aol.com [152.162.199.42]

over a maximum of 30 hops:

1 * * * Request timed out.

2 150 ms 144 ms 138 ms 204.134.78.201

3 375 ms 299 ms 196 ms glory−cyberport.nm.westnet.net [204.134.78.33]

4 271 ms * 201 ms enss365.nm.org [129.121.1.3]

5 229 ms 216 ms 213 ms h4−0.cnss116.Albuquerque.t3.ans.net [192.103.74.45]

6 223 ms 236 ms 229 ms f2.t112−0.Albuquerque.t3.ans.net [140.222.112.221]

7 248 ms 269 ms 257 ms hl4.t64−0.Houston.t3.ans.net [140.223.65.9]

8 178 ms 212 ms 196 ms hl4.t80−1.St−Louis.t3.ans.net [140.223.65.14]

9 316 ms * 298 ms hl2.t60−0.Reston.t3.ans.net [140.223.61.9]

10 315 ms 333 ms 331 ms 207.25.134.189

11 * * * Request timed out.

12 * * * Request timed out.

13 207.25.134.189 reports: Destination net unreachable.

Qué es todo esto? El número a la izquierda es el número de ordenador cuya ruta se ha traceado.

A continuación, "150 ms" es el tiempo, en milésimas de segundo, que se tarda en enviar un mensaje a/y desde ese ordenador. Como el mensaje puede tomar una distinta cantidad de tiempo cada vez que se manda, tracert mide el tiempo del "viaje" tres veces. Los "*" significan que el viaje duró demasiado. Después de la información del cronometraje viene el nombre del ordenador al que llegó el mensaje, primero en un modo que es fácil de recordar para los humanos, y luego en otra forma (direcciones IP) que es la que prefieren las computadoras.

"Destination net unreachable" (Red de Destino no alcanzable) probablemente significa que nos topamos con un Firewall.

Probemos el segundo nombre de dominio del AOL.

C:\WINDOWS>tracert 152.163.199.56

Tracing route to dns−02.aol.com [152.163.199.56]

over a maximum of 30 hops:

1 * * * Request timed out.

2 142 ms 140 ms 137 ms 204.134.78.201

3 246 ms 194 ms 241 ms glory−cyberport.nm.westnet.net [204.134.78.33]

4 154 ms 185 ms 247 ms enss365.nm.org [129.121.1.3]

5 475 ms 278 ms 325 ms h4−0.cnss116.Albuquerque.t3.ans.net [192.103.74.45]

6 181 ms 187 ms 290 ms f2.t112−0.Albuquerque.t3.ans.net [140.222.112.221]

7 162 ms 217 ms 199 ms h14.t64−0.Houston.t3.ans.net [140.223.65.9]

8 210 ms 212 ms 248 ms h14.t80−1.St−Louis.t3.ans.net [140.223.65.14]

9 207 ms * 208 ms h12.t60−0.Reston.t3.ans.net [140.223.61.9]

10 338 ms 518 ms 381 ms 207.25.134.189

11 * * * Request timed out.

12 * * * Request timed out.

13 207.25.134.189 reports: Destination net unreachable.

Nota: Darse cuenta de que ambos tracerts terminan en el mismo ordenador llamado h12.t60−0.Reston.t3.ans.net. Como el AOL tiene su "central" en Reston, Virginia, seguramente este debe ser un ordenador que envía información directamente a AOL. Pero nos damos cuenta de que h12.t60−0.Reston.t3.ans.net, h14.t80−1.St−Louis.t3.ans.net, h14.t64−0.Houston.t3.ans.net y Albuquerque.t3.ans.net, todos tienen nombres numéricos que comienzan con 140, y nombres que acaban con "ans.net". Por tanto es seguro que todos ellos pertenecen a la misma compañía. Además, el "t3" en cada nombre sugiere que estos ordenadores son Routers de un backbone (red principal) de comunicaciones en Internet.

Ahora probemos con el último de esos nombres de dominio:

C:\WINDOWS>tracert 198.83.210.28

Tracing route to dns−aol.ans.net [198.83.210.28]

over a maximum of 30 hops:

1 * * * Request timed out.

2 138 ms 145 ms 135 ms 204.134.78.201

3 212 ms 191 ms 181 ms glory−cyberport.nm.westnet.net [204.134.78.33]

4 166 ms 228 ms 189 ms enss365.nm.org [129.121.1.3]

5 148 ms 138 ms 177 ms h4−0.cnss116.Albuquerque.t3.ans.net [192.103.74.45]

6 284 ms 296 ms 178 ms f2.t112−0.Albuquerque.t3.ans.net [140.222.112.221]

7 298 ms 279 ms 277 ms h14.t64−0.Houston.t3.ans.net [140.223.65.9]

8 238 ms 234 ms 263 ms h14.t104−0.Atlanta.t3.ans.net [140.223.65.18]

9 301 ms 257 ms 250 ms dns−aol.ans.net [198.83.210.28]

Trace complete.

Al final conseguimos el trazado completo llegando a lo que seguramente es un ordenador de AOL, y parece como si estuviera fuera del Firewall! Pero nótese cómo tracert tomó una ruta diferente esta vez, yendo por Atlanta en vez de por St. Louis y Reston. Pero este, el igual que los otros, posee en su dirección el "ans.net" junto con los "t3", por lo que este último nombre de dominio está usando la misma red que los anteriores.

Ahora, que podemos intentar acceder a la cuenta de luser@aol.com. Vamos a hacer port surfing en este último servidor de AOL, pero para hacer esto necesitaremos modificar un poco nuestra configuración de telnet.

Clickear en Terminal, y luego en Preferencias. En el cuadro de preferencias se debe seleccionar "Eco Local". Debe hacerse esto para ver las cosas que lleguen cuando se está haciendo el port surfing. Por alguna razón, algunos de los mensajes que un ordenador remoto envía no aparecen en la pantalla de Windows95 (telnet) a menos que se active la opción de eco local. Sin embargo, debe tenerse cuidado, porque en algunas situaciones todo lo que se teclee aparecerá duplicado. Por ejemplo, si se teclea "hello" la pantalla de telnet puede mostrar "heh lelllo o". Esto no significa que haya errores de tecleado, sino que lo que se escribe sufre un eco de regreso a intervalos variables.

Ahora clickear en Conectar, luego en Sistema Remoto. A continuación introducir el nombre de ese último Server de AOL, dns−aol.ans.net. Debajo de eso, en Puerto, escribir "Daytime". Esto hará que el Server envíe el día de la semana, la fecha y la hora de su región geográfica.

Sabemos ahora que dns−aol.ans.net está expuesto al mundo, con al menos un puerto abierto

Esto nos da ánimos para seguir con el port surfing.

Advertencia: Si todo el mundo que lea esto hace telnet al puerto de fecha de este ordenador, el sysadmin dirá "Whow, estoy siendo atacado por hackers!!! Será que existe alguna clase de exploit para el servicio de fechas! Cerrar este puerto rápidamente!".

Ahora probaremos el ordenador de Reston. Seleccionar Host Remoto otra vez y escribir el nombre h12.t60−0.Reston.t3.ans.net.

Si no se consigue nada al hacer port surfing:

Primero desactivar la opción de "Eco local" y entonces volver a hacer telnet a whois.internic. Preguntamos por este sistema (ans.net) que ofrece links a AOL:

[vt100] InterNIC > whois ans.net

Connecting to the rs Database . . . . . .

Connected to the rs Database

ANS CO+RE Systems, Inc. (ANS−DOM)

100 Clearbrook Road

Elmsford, NY 10523

Domain Name: ANS.NET

Administrative Contact:

Hershman, Ittai (IH4) ittai@ANS.NET

(914) 789−5337

Technical Contact:

ANS Network Operations Center (ANS−NOC) noc@ans.net

1−800−456−6300

Zone Contact:

ANS Hostmaster (AH−ORG) hostmaster@ANS.NET

(800)456−6300 fax: (914)789−5310

Record last updated on 03−Jan−97.

Record created on 27−Sep−90.

Domain servers in listed order:

NS.ANS.NET 192.103.63.100

NIS.ANS.NET 147.225.1.2

Ahora si realmente se desea ser un hacker ingenioso podría llamarse a esos teléfonos 800 y probar mediante ingeniería social a sacar un password a alguien que trabaje en esa red. Pero eso no estaría bien y no hay nada legal que pueda hacerse para conocer los passwords.

Esta es una de las formas de cómo se puede hackear utilizando información que lleve a los servidores que controlan e−mail.

QUE MÁS SE PUEDE HACERSE CON UNA CONEXIÓN Y WINDOWS 95?

El ping de la muerte

Es una manera rápida de perder el trabajo. Se hace desde el prompt de Windows (MS−DOS). Afortunadamente muchos administradores de sistema han actualizado y reparado las cosas actualmente para que el ping de la muerte no funcione. Pero para el caso de que tu ISP o LAN en el trabajo o en el colegio no esté protegida, no lo pruebes sin el consentimiento de tu administrador de sistemas.

La utilidad Ping sirve principalmente para saber si un servidor esta activo y además para poder calcular el trafico en la red según el tiempo de su respuesta. Básicamente se le envía un paquete a un servidor y este nos contesta, solo que si se le envía un paquete muy grande puede llegar desordenado, por lo que el servidor pide al origen que le vuelva a enviar una parte o la totalidad del paquete, por lo que se produce un datagrama del ping muy grande y producirá su caída. Para ejecutar este ataque solo tenemos que escribir:

c:\>ping −l 65510 victima.com

También existe el ping ordinario, que también se realiza desde MS−DOS. Es como una clase de tracert, pero todo lo que hace es medir el tiempo que tarda un mensaje en ir de un ordenador a otro, sin decirte nada sobre los ordenadores que se encuentran entre el tuyo y el otro (al que se le hace el ping).

Otros comandos TCP/IP ocultos de MS−DOS son:

ARP Tablas de traducción de direcciones IP a físicas.

FTP File Transfer Protocol (Protocolo de Transferencia de Archivos).

Nbtstat Visualiza información sobre la red actual, maravilloso para ser usado en tu propio . ISP.

Netstat Similar a Nbtstat

Route Controla las tablas de Routers (enrutado). El Hacking de Routers

está considerado de extra elite.

Al ser comandos semi−secretos, no se puede conseguir detalles sobre su funcionamiento en el menú de ayuda del MS−DOS.

Para conseguir ayuda simplemente teclea el comando arp, nbtstat, ping y route, y pulsa enter.

Para obtener ayuda para el comando netstat debe ponerse el comando "netstat ?" .

Telnet tiene también una opción de ayuda en la barra de tareas.

Ahora supongamos que se quiere realizar un Hacking serio, y se necesita conocer otros comandos además de los que acabamos de ver, pero sin usar UNIX.

Por tanto cuál es la siguiente opción para hacer Hacking serio desde Windows?

Crackear passwords de servidores Windows NT?

Al programa freeware NTLocksmith para Windows95, añadirle el NTRecover que permite el cambio de passwords en sistemas donde el password administrativo se ha perdido. Funciona el 100% de las veces. Consigue NTLocksmith y NTRecover (y montones más de herramientas para el hacker gratis) en http://www.ntinternals.com.

Advertencia :Puede Ir a la Cárcel. Si usa NTRecover para acceder a un sistema ajeno, está pidiendo a gritos ser atrapado.

Cuánto le gustaría hacer creer a la gente que el sistema NT se ha colgado cuando realmente no lo ha echo? Este programa tan bromista puede conseguirlo en http://www.osr.com/insider/insdrcod.htm.

Pero de dónde puede conseguirse la herramienta de Hacking más mortífera que funcione en Windows?

http://home.microsoft.com

Este programa mortífero es el Internet Explorer 3.0. Desdichadamente, lo que mejor hace este programa es dejar a otros hackers introducirse en su sistema y hacer cosas como por ejemplo obligar a su programa de planilla de cálculo (por ej. Quicken) a transferir los registros de los ahorros de toda tu vida a alguien en Afganistán.

Internet Explorer es realmente un shell de Windows alternativo que opera muy similarmente al

Administrador de Archivos o al Explorador que viene con los sistemas operativos Windows 95 y Windows NT.

Desde Internet Explorer puede utilizar cualquier programa de su ordenador. O cualquier programa al que tenga acceso a través de su LAN.

Nota: Un shell es un programa que se encuentra entre el sistema operativo y el usuario. Lo mejor de que Internet Explorer sea un shell de Windows es que Microsoft nunca le dijo a nadie que efectivamente fuese un shell. Los problemas de seguridad que están acosando como una plaga a

Internet Explorer son la mayoría, consecuencia de que resulte ser un shell. Por el contrario, los

navegadores Netscape y Mosaic no son shells. También son mucho más seguros de usar que el anterior.

Para usar Internet Explorer como un shell de Windows, enciéndalo justo como si fuese a utilizarlo para navegar normalmente. Impide el intento del programa de establecer una conexión de Internet.

Entonces en el espacio donde normalmente tecleará la URL a la que quiere ir, escriba c: en su lugar.

Todas esas carpetas que aparecen en la pantalla. Le resultan familiares? Es lo mismo que te mostraría el Explorador. Ahora, por diversión, haga click en "Archivos de Programa" , luego en "Accesorios" y finalmente en "MSPaint". Entonces arrancar el MSPaint.

Por tanto, se puede utilizar Internet Explorer como herramienta de Hacking?

Una manera es si está usando un ordenador que restringe la utilización de otros programas en una LAN, por ejemplo. La próxima vez que acabe frustrado en el ordenador del trabajo o el de la biblioteca, compruebe si tiene el Internet Explorer. Si lo tiene, haga funcionar el programa e intente escribir letras de unidades de disco. Mientras que en su ordenador C: es una unidad corriente, en una LAN puede obtener resultados poniendo R: o Z: o cualquier otra letra del alfabeto.

Ahora supongamos que desea acceder al archivo de sistema NTFS que Windows NT usa desde su Windows95 o incluso desde la plataforma de MS−DOS. Esto puede ser útil si quiere usar Windows95 como una plataforma para hackear un sistema de Windows NT. http://www.ntinternals.com/ntfsdos ofrece un programa que permite a Windows95 y a MS−DOS reconocer y hacer funcionar unidades NTFS para acceso transparente.

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 International Business Machines 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 todavia 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. ¿Quién le asegura al comprador que sus datos no se almacenarán a la ligera, siendo accesibles fácilmente por un hacker o un empleado desleal? ¿Cómo saber que no se revenden a terceros?

2)− La autenticación (56%), que inquieta a los usuarios, quienes dudan si la persona con la que se comunican es verdaderamente quien dice ser. Sin embargo, dada la relativa facilidad de falsificar una página web e incluso un sitio web completo, ¿cómo asegurarse de que se está comprando en una tienda virtual o en una imitación fiel?

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, ofrecen 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. Otro asunto es si asegura o no la confidencialidad, cuestión más que dudosa, si se tiene en cuenta que una clave de 40 bits se rompe en cuestión de horas, con lo que los datos por ella protegidos quedan al descubierto rápidamente. 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. Su mecanismo de firma dual garantiza además que el comerciante no conocerá los datos de pago (número de tarjeta de crédito), eliminando así la posibilidad de fraude por su parte. Esto garantiza así que el comerciante cobra por la venta y que el comprador no es estafado por el comerciante ni por hackers.

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.

MICROSOFT DESAFÍA A HACKERS

(05.08.99): Microsoft le invita a probar sus habilidades como hacker mediante un sitio Web operado en un ambiente Windows 2000 y desprovisto de software Cortafuegos (Firewall). Con ello, los interesados tienen la posibilidad de irrumpir en un servidor sin ser perseguidos luego por la justicia.

La compañía informa que en todo momento el servidor tendrá instalada la última versión beta del sistema operativo Windows 2000. El desafío forma parte de las pruebas de seguridad que Microsoft realiza con el sistema operativo, que según las intenciones de la compañía ha de convertirse "en el más seguro que haya existido".

En su lista de condiciones para participar en el Hacking autorizado, la compañía sugiere a quienes logren ingresar al servidor "cambiar archivos o contenidos, aunque evitando los comentarios insolentes o groseros". De igual modo, indica que el servidor contiene una serie de mensajes ocultos, que invita a encontrar. Bajo el subtítulo "Hágalo Interesante", la compañía precisa que filtrará aquellos intentos de Hacking simple, tales como el bombardeo de paquetes tendientes a doblegar al servidor desbordando su capacidad de respuesta.

Por último, Microsoft precisa que la invitación se refiere única y exclusivamente al sitio de prueba.

· http://www.windows2000test.com/"

AHORA LINUX DESAFÍA A HACKERS

(06.08.99): Luego del desafío planteado por Microsoft a hackers interesados en poner a prueba la seguridad y presunta impenetrabilidad de Windows 2000, la compañía Linux PPC lanzó una oferta similar. El premio para quien logre violar la seguridad del servidor es el servidor.

Para el caso de Linux PPC, se trata de un servidor operado con la instalación estándar, incluyendo Telnet y el servidor Web Apache. Desde su instalación, el martes 3, a la fecha, el servidor ha registrado 11.294 intentos infructuosos de irrupción.

El hacker que logre penetrar el servidor se llevará la máquina como premio, informa Linux PPC. La única condición será reproducir exactamente, paso a paso, el procedimiento seguido.

En la página Web creada para el concurso, J. Carr, administrador del sistema, "felicita" a los 87 habilidosos que hasta ahora han intentado realizar una conexión telnet a la máquina pretendiendo ser el propio Carr.

El sitio del caso se encuentra en:

· http://crack.linuxppc.org/

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. Seguramente por eso, el presidente Bill Clinton, el principal mentor de intentar ponerle restricciones a la red mundial, es parodiado constantemente con fotos trucadas que hacen alusión al sexgate desatado tiempo atrás.

Estos personajes suelen ingresar también a un sistema dejando "evidencias" de que ellos estuvieron allí con el objetivo de que los encargados de la seguridad de la empresa sepan que pueden volver y destruir lo que se les

plazca en el momento menos pensado. 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, Ardita tiene, a modo de homenaje y admiración, cientos de páginas en Internet construidas por personas de diferentes países donde se pueden ver sus fotos y datos personales.

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 hinóspitos. No son muy sociables y les causa mucho placer sentir que transgreden.

HACKERS VULNERARON RED DEL PENTÁGONO

(27.02.98): Durante las dos últimas semanas, la red informática del Pentágono ha estado expuesta a intensas irrupciones de grupo de hackers.

El Subsecretario estadounidense de Defensa, declaró a los medios que "se trata del ataque más organizado y sistemático experimentado por el Pentágono". Según Hamre, nada hace suponer que el asunto tenga alguna relación con la crisis iraquí.

La Secretaría de Defensa de Estados Unidos no desea proporcionar detalles del asunto a fin de no perjudicar las investigaciones correspondientes, que han sido encargadas al FBI. En tal sentido, se limitó a señalar que los hackers en ningún momento tuvieron acceso a información clasificada, sino "sólo" a los registros de personal y sueldos.

El ataque contra el Pentáfono no es el primero realizado contra computadoras del gobierno y la defensa de Estados Unidos. En diciembre pasado, el sitio web de la fuerza aérea de ese país también fue alterado por hackers, que incorporaron a la página de inicio una imagen pornográfica. En septiembre fue el turno de la CIA (Central Intelligence Agency), que vio su nombre modificado a Central Stupidity Agency.

(19.07.99): Personas de todo el mundo podrán tener acceso a botines multimillonarios gracias a la falla del milenio, según consultora.

En un informe elaborado por la consultora Gartner Group, se advierte contra las actividades de estafadores sofisticados que aprovecharán los errores en sistemas de seguridad el 31 de diciembre, para apoderarse de dinero ajeno mediante procedimientos electrónicos.

En el informe, que se basa en información recabada entre 1.000 de sus clientes, la consultora indica que no le sorprendería si al menos un robo electrónico excede los mil millones de dólares.

En el documento se pone de relieve que uno de los mayores factores de riesgo es que empleados y contratistas encargados de compatibilizar sistemas "dejen una puerta trasera abierta", que posteriormente pueda ser utilizada por ellos mismos o por terceros para ingresar ilícitamente.

Al respecto, Joe Pucciarelli, autor del informe de Gartner Group, declaró a USA Today que "hemos abiertos todos nuestros sistemas a personas a quienes no necesariamente conocemos bien". En tal contexto, precisó que varias compañías han descubierto "entradas traseras" en sus sistemas informáticos, dejadas ahí sin autorización con el fin evidente de obtener acceso posterior al sistema.

HACKERS ATACAN SITIO DE HILLARY CLINTON

(28.07.99): 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" −simpatizantes de Rudolph Giuliani− 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 (Domain Name Server), haciendo que al escribir una dirección en la web los usuarios sean llevados a una dirección distinta.

Los autores de la página web sobre Giuliani desmienten categóricamente ser los autores del sabotaje de la página de Hillary Clinton.

A la fecha, el problema no ha sido solucionado, por lo que la página de la candidata sólo presenta un mensaje en numerosos idiomas, con el texto "en construcción".

100 HACKERS PREPARAN ATAQUE CONTRA INDONESIA

(23.08.99): José Ramos Horta, quien en 1996 fuese galardonado con el Premio Nobel 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.

Temiendo que el plebiscito de independencia de Timor del Este se transforme en el mayor fraude electoral de la historia, José Ramos Horta advirtió al gobierno que 100 hackers europeos y estadounidenses han preparado un arsenal cibernético consistente de una docena de virus y modalidades de ataque diseñadas para causar un colapso del sistema financiero indonesio, escribe BBC News.

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

(02.03.99): 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.

HACKERS VULNERAN SITIO DE SYMANTEC

(03.08.99): El sitio web de Symantec fue alterado ayer por hackers. La noticia está causando revuelo en círculos informáticos, toda vez que la compañía es uno de los principales proveedores mundiales de software de seguridad y antivirus.

Como parte de su irrupción contra los servidores de Symantec, los hackers cambiaron la portada del sitio web corporativo con un texto procaz en que su acción es reivindicada como una victoria (" we own your ass, Symantec").

Según BBC News, los piratas informáticos también lograron infiltrar los servidores de Symantec con un programa tipo "gusano", que automáticamente se propaga por sistemas interconectados y que está en condiciones de causar daños similares a los virus.

Consultado por BBC, un portavoz de Symantec confirmó la alteración del sitio web, aunque desmintió que los hackers hubieran logrado instalar un "gusano" en sus sistemas.

El portavoz intentó quitar importancia a la situación, señalando que siempre existe el riesgo de que una compañía se vea afectada por tales ataques y que lo importante es corregir el daño con prontitud y restablecer el sitio web original.

A juicio del portavoz, el prestigio de Symantec no se verá alterado por el ataque, a pesar de ser una compañía líder del rubro de la seguridad informática.

Symantec denunció el hecho al FBI, que inició de inmediato las investigaciones correspondientes.

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.

Mayor información en:

http://www.gtri.gatech.edu/res−news/rchnews.html

PROGRAMAS UTILIZADOS PARA HACKEAR

NOMBRE DEL PROGRAMA

DESCRIPCIÓN S.O.

Cracker Jack 1.4

Descodificador de Passwords de Unix. Inglés.

Dos

Brute Forece 1.1

Descodificar de passwords Unix. Inglés.

Dos

John the Ripper 1.4

Posiblemente el mejor descodificador de password Unix.

Dos

Star Cracker 1.0

Otro descodificador de pass. Unix. Ing.

Dos

Hack486

Más descodificadores de pass. Éste incluye un fichero de password para probar. Muy rápido. Ing.

Dos

[Xit]v2.0

Más descodificadores..... Ing.

Dos

Crack v5.0

Otro descodificador pero de passwords ffb X. Ing.

Unix

Magic Cracker

Otro descodificador de passwords Unix. Ing.

Win95/NT

Jill20

Complemento para el Cracker Jack.Ing.

Dos

Unix Password analizer

Busca personas bastante importantes en un fichero password de Unix. Ing.

Dos

VMS crack 1.0

Descodificador password de sistemas VMS.

–

Crack CNX

Descodifica ficheros cnx del software de infovía para Win3.x. Ing.

Dos

Glide

Dicen que descodifica los passwords .PWL de W95. No es compatible con la versión OSR2. Ing.

Dos

PWL Viewer

Visualizador de los ficheros .PWL. Ing.

Dos/W95

PWL Tools

Como el anterior pero todo el kit, crackeador, y visualizador. La velocidad del cual está limitada por el mal uso que se pueda hacer. Ing.

Dos/W95

PopCrack v1.0

Cracker del Popmail Password. Ing.

Dos

Toneloc 1.10

Uno de los mejores War−Dialers de todos. Ing.

Dos

Phonetag v1.3

Otro escaneador de telefonos. Ing.

Windows

THC scan v1.0

El mejor de todos. Sin ninguna duda. Pese a que es un poco dificil de configurar. Ing.

Dos

Keylog 95

Capturador de teclado. En el archivo figuran todas las teclas pulsadas. Ing.

Dos/Win95

Keylog v2.0 95/NT

Como el anterior pero mejorado. Ing.

Win95/NT

Passgrab 1.0

Otro capturador de teclado.

–

Password Thief v1.0

Un buen capturador de teclado. Sharewar.

W95

Passbios

Este programa engaña al usuario para pillar la clave de la Bios. Se simula la Bios del ordenador para engañar. Esp.

W95

L0phtCrack 2.01

Pillar passwords en NT. Ing.

W95/NT

PortScan

Escanea los puertos abiertos de un ordenador remoto. Ing.

Dos

Winsock spy v0.91

Substituye el ficher wsock32.dll para espiar las comunicacioens de u Pc. W95. Ing.

–

Satan v1.1.1

Herramienta muy util para detectar posibles agujeros de seguridad. Ing.

UNIX

Netcat v1.1.0

Herramienta que escribe y lee datos de conexiones TCP/IP. w95/NT. Ing.Versión Unix

W95/UNIX

Netpack v2.0

Conjunto de utilidades. Ing.

W95/NT

Hacker's Utility

Muchas utilidades y descodificadores de pass. Ing. o Ital.

Win95/NT

Date Dictionary Creator

Generador de listas, o diccionarios para los crackeadores de passwords. Ing.

Dos

Wordlist Maker

Creador de listas de palabras de Ing.

Win3.x.

Diccionario

Un diccionario grande para utilizarlo para los crackeadores de passwords. .

Dos

Super Diccionario

Uno de los diccionarios más grandes. !!!!3'8Mb.¡¡¡

–

Manipulador de Passwords

Descodifica y modifica el fichero /etc/passwd. Esp.

Dos

NETLAB95

Conjunto de utilidades para chequer Redes, funciones finger, ping, etc...

W95

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".

LA INFORMACIÓN FUE EXTRAÍDA DE LOS SIGUIENTES SITIOS WEB

http://cultdeadcow.com

http://diarioit.com

ftp://ftp.cdrom.com

ftp://ftp.coast.net

http://hertz.njit.edu/%7ebxg3442/temp.html

http://www.alpworld.com/infinity/void−neo.html

http://www.danworld.com/nettools.html

http://www.eskimo.com/~nwps/index.html

http://www.geocities.com/siliconvalley/park/2613/links.html

http://www.ilf.net/Toast/

http://www.islandnet.com/~cliffmcc

http://www.simtel.net/simtel.net

http://www.supernet.net/cwsapps/cwsa.html

http://www.trytel.com/hack/

http://www.tucows.com

http://www.windows95.com/apps/

http://www2.southwind.net/%7emiker/hack.html

Back Orifice

Sistema de administracion remota

v1.20 (30−7−1998)

Back Orifice es una aplicacion cliente−servidor que permite al software cliente monitorizar , administrar , y realizar otras acciones de red y multimedia en la maquina que esta ejecutando el servidor. Para comunicarse con el servidor , tanto el cliente basado en texto como en graficos pueden ejecutarse en cualquier maquina con Microsoft windows. El servidor solo funciona actualmente en Windows 95/98.

Este paquete contiene:

bo.txt (documentacion)

bo_esp.txt (Este documento)

Plugin.txt (documentacion de programacion de extensiones para el servidor)

boserve.exe (Servidor Auto−Instalable de Back Orifice)

bogui.exe (Cliente grafico para BO)

bocliente (cliente en modo texto),

boconfig.exe (utilidad para configurar el nombre del ejecutable , el puerto,el password y la extension predeterminada para el servidor BO)

melt.exe (un descompresor)

frezze.exe (un compresor)

Para instalar el servidor , este tan solo necesita ser ejecutado. Cuando el ejecutable del servidor se ejecuta , se instala a si mismo , y se borra.

Esto es util en entornos de red, donde el servidor puede ser instalado en una maquina , simplemente copiando el ejecutable del servidor en el directorio Startup (o Inicio, en el caso español) , donde sera instalado y luego borrado. Una vez que el servidor esta instalado en una maquina, se iniciara cada vez que la maquina re−arranque.

Para actualizar una copia de BO de forma remota , simplemente manda la nueva version del servidor al host remoto, y usa el comando Process spawn para ejecutarlo. Cuando se ejecuta, el servidor automaticamente mata cualquier proceso que se llame como el programa a instalar, e intenta instalarse sobre la vieja version, se autoejecuta desde su posicion de instalacion, y borra el .exe que acaba de ejecutar.

Antes de la instalacion , algunos de los aspectos del servidor pueden ser configurados. El nombre de fichero que usa el BO para instalarse a si mismo, el puerto en el que estara escuchando el servidor, y la password usada para encriptar pueden ser configurados con la utilidad boconf.exe. Si el servidor no se configura , usara el puerto 31337, sin password (aunque las comunicaciones siguen estando encriptadas), y se instala a si mismo como ".exe" (espacio punto exe)

El cliente se comunica con el servidor via paquetes UDP encriptados. Para una comunicacion con exito , el cliente necesita mandar al mismo puerto al que esta escuchando el servidor , y la password del cliente debe ser la misma con la que esta configurado el servidor.

El puerto al que el cliente manda sus paquetes puede ser establecido con la opcion −p tanto en el cliente grafico como en el de texto. Si los paquetes estan siendo filtrados o existe un firewall , puede ser necesario mandar desde un puerto que no sea filtrado y/o bloqueado. Ya que las comunicaciones por UDP son sin conexion , los paquetes pueden ser bloqueados tanto en su camino hacia el servidor como en la vuelta hacia el cliente.

Las acciones son realizadas en el servidor mandando comandos desde el cliente a una direccion ip especifica. Si la maquina servidora no esta en una direccion IP fija (caso habitual si se accede a traves de Infobirria), puedes localizarla utilizando el barrido o los comandos de barrido (sweep) en los cliente usando el dialogo "ping..." o poniendo una direccion IP destino del tipo "1.2.3.*". Si se barre una lista de subredes , cuando una maquina con el servidor instalado responde , el cliente mirara en el mismo directorio que contiene la lista de subredes y mostrara la primera linea del primer archivo que encuentre con el nombre de archivo de la subred.

Las ordenes actualmente implementadas en BO se listan abajo. Algunos de los nombres pueden ser diferentes entre la version texto y grafica de los clientes, pero la sintanxis es la misma para practicamente todos los comandos. Mas informacion sobre cualquier orden se puede conseguir usando el comando "help ". El cliente

grafico pone las etiquetas de los dos campos parametro con una descripcion de los argumentos que cada orden acepta, cuando se selecciona ese comando de la lista de ordenes(Command List)

Si parte de la informacion requerida no se proporciona con la orden , el servidor devolvera el error "Missing data". Las ordenes de BO son:

(Cliente Grafico/Cliente Texto)

App add/appadd

Lanza una aplicacion basada en texto en un puerto tcp. Esto permite que tengas el control de una aplicacion de texto o MS−DOS desde una sesion de telnet (por ejemplo , command.com)

App del/appdel

Hace que una aplicacion deje de esperar conexiones

Directory create/md

Crea un directorio

Directory list/dir

Lista los ficheros y directorios. Debes especificar un comodin si quieres que mas de un fichero sea listado.

Directory remove/rd

Borra un directorio.

Export add/shareadd

Crea una comparticion en el servidor. El icono de directorio o unidad exportado no se ve modificado por la el icono de la mano.

Export delete/sharedel

Borra una comparticion.

Exports list/sharelist

Lista los nombres de las comparticiones actuales, la unidad o directorio que esta siendo compartido , el acceso para esta comparticion , y el password para esta comparticion.

File copy/copy

Copia un fichero

File delete/del

Borra un fichero

File find/find

Busca en un arbol de directorios los ficheros que correspondan con los comodines especificados.

File freeze/freeze

Comprime un fichero

File melt/melt

Descomprime un fichero

File view/view

Ver el contenido de un fichero de texto.

HTTP Disable/httpoff

Deshabilita el servidor HTTP.

HTTP Enable/httpon

Habilita el servidor HTTP

Keylog begin/keylog

Graba las pulsaciones de tecla en la maquina servidora a un fichero de texto. El log muestra el nombre de la ventana en la que fue introducido el texto.

Keylog end

Parar la captura de teclado. Para terminar la captura desde el cliente texto, usa "keylog stop".

MM Capture avi/capavi

Captura video y audio (si se puede) desde cualquier dispoditivo de captura de video disponible a un fichero avi.

MM Capture frame/capframe

Captura un fotograma de video y lo graba en un fichero bmp

MM Capture screen/capscreen

Captura una imagen de la pantalla de la maquina servidora en un fichero bmp

MM List capture devices/listcaps

Muestra una lista de los dispositivo de captura de video.

MM Play sound/sound

Toca un fichero wav

Net connections/netlist

Muestra las conexiones de entrada y salidas a la red

Net delete/netdisconnect

Desconecta la maquina servidora de un recurso de red.

Net use/netconnect

Conecta la maquina servidora a un recurso de red.

Net view/netview

Ve todos los interfaces de red , dominios , servidores , y comparticiones accesibles desde la maquina servidora.

Ping host/ping

Ping a la maquina. Devuelve el nombre de la maquina y el numero de version del BO que tiene instalado.

Plugin execute/pluginexec

Ejecuta una extension BO. Ejecutar funciones que no se ajusten al interfaz de extensiones de BO ,causara el cuelgue del servidor.

Plugin kill/pluginkill

Le dice a una extension que pare y se retire.

Plugins list/pluginlist

Lista las extensiones activas o el valor de retorno de una extension que ha salido (terminado)

Process kill/prockill

Terminar un proceso.

Process list/proclist

Muestra los procesos en ejecucion.

Process spawn/procspawn

Ejecuta un programa. Desde el gui, si el segundo parametro se especifica,el proceso sera ejecutado como un proceso normal , visible. Si no , sera ejecutado escondido o camuflado

Redir add/rediradd

Redirecciona las conexiones tcp entrantes o paquetes udp a otra direccion IP.

Redir del/redirdel

Para la redireccion de puerto.

Redir list/redirlist

Lista todas las redirecciones de puerto.

Reg create key/regmakekey

Crea una clave en el registro. NOTA; Para todos los comandos de registro, no especificar los \\ del final para los valores del registro.

Reg delete key/regdelkey

Borra una clave del registro.

Reg delete value/regdelval

Borra un valor del registro.

Reg list keys/reglistkeys

Lista las subclaves de una clave del registro.

Reg list values/reglistvals

Lista los valores de una clave de registro.

Reg set value/regsetval

Establece un valor para una clave de registro. Los valores son especificados como un tipo seguidos de una coma , y despues el dato del valor. Para valores binarios (Tipo B) el valor es una serie de dos digitos con valores hexadecimales. Para valores DWORD (tipo D) el valor es un numero decimal.Para valores de cadena (tipo S) el valor es una cadena de texto.

Resolve host/resolve

Resuelve la direccion IP de una maquina relativa a la maquina servidor. El nombre de la maquina puede ser un nombre internet o de red local.

System dialogbox/dialog

Crea una caja de dialogo en la maquina con el texto especificado , y un boton "ok". Puedes crear tantas cajas de dialogo como quieras, ellas sencillamente iran en cascada frente a la caja anterior.

System info/info

Muestra informacion del sistema de la maquina servidora. La informacion mostrada incluye el nombre de la maquina , usuario actual , tipo de CPU,memoria total y disponible, informacion de la version de windows , e informacion sobre las unidades (fijas , CD−rom, removible,remota) , y para las unidades fijas , el tamaño y espacio libre.

System lockup/lockup

Bloquea la maquina servidora.

System passwords/passes

Muestra las passwors en cache para el usuario actual y la password de su salvapantallas. Pueden tener basura enganchada al final.

System reboot/reboot

Apaga la maquina y la reinicia.

TCP file receive/tcprecv

Conecta el servidor a una direccion IP/Puerto y guarda cualquier dato recibido de esa coinexion al fichero especificado.

TCP file send/tcpsend

Conecta la maquina servidora a una IP/Puerto especifico y manda el contenido de un fichero especifico , luego desconecta.

NOTA: Para transferecias TCP de ficheros , la direccion IP y el puerto deben estar escuchando antes de que el comando de fichero tcp sea mandado , o fallara. Un utilidad para trasnferencias de este tipo es netcat , que esta disponible tanto para Unix como para Win32 Los ficheros pueden ser transferidos DESDE el servidor usando el comando tcp dile send , y netcat con una sentencia del tipo : netcat −l −p 666 > fichero.

Los ficheros pueden ser transferidos AL servidor usando el comando tcp file receive command y netcat con una sentencia del tipo : netcat −l −p 666 < fichero.

NOTA: la version win32 de netcat no desconecta ni sale cuando encuentra el fin del fichero de entrada. Despues de que el contenido del fichero ha sido transferido , termina el netcat con ctrl−c o ctrl−break.

BOConfig:

BOConfig.exe te permite configurar las opciones para un servidor BO antes de que se instale. Te pregunta el nombre del ejecutable , cual es el nombre que BO usara para instalarse en el directorio del sistema. No tiene porque terminar en .exe , pero no agregara .exe si no le das una extension de fichero. Despues te pregunta por una descripcion del fichero .exe si no le das una extension exe que describira el exe en el registro donde sera iniciado durante el arranque. Entonces pregunta por el puerto por donde el servidor esperara los paquetes, y una password para la encriptacion. Para comunicarse el servidor con el cliente , el cliente debe tener la misma password. Puede ser nula. Despues pregunta por la extension para ejecutar al iniciar. Esto es una DLL y nombre de funcion , del tipo "DLL:_Funcion" de una extension de BO que se ejecutara automaticamente cuando el servidor se inicie. Puede ser nula. Entonces , te permite entrar cualquier argumento que quieras pasarle a la extension en arranque. Tambien puede ser nula. Y finalmente , te pregunta por la localizacion del fichero que sera unido al servidor , que sera escrito al directorio del sistema cuando el servidor se inicie. Este puede ser una extension del BO que se ejecute automaticamente. El servidor funcionara sin ser configurado. Por defecto , comunica al puerto 31337 sin password , e instalandose como " .exe"

(TRADUCCION : Cthulhu)

Back Orifice Eliminator

Que le servirá para eliminar el Back Orifice de su computador.

Instalación: Para instalar el Back Orifice Eliminator, baje y ejecute este archivo que es ejecutable y autodescomprimible (boe.exe). Este extrae el Back Orifice Eliminator a su disco duro (usted puede especificar donde), y la aplicación será ejecutada automáticamente y verá la documentación o guía. A partir de este momento, el Back Orifice Eliminator se ejecutará automáticamente cada vez que usted inicie su computador. El programa puede ser habilitado o deshabilitado a opción suya en cualquier momento usando el menú.

Back Orifice Eradicator 1.00

Para limpiar el Back Orifice con un simple click. Al hacer click en Memory Scan para ver si el server está corriendo en su computador. Si es así, el mismo será removido y detenido de inmediato.

Codetel recomienda revisar de inmediato la revisión en su sistema y proceder a eliminarlo si existe.

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.

−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.

1

21