ESTADO DEL ARTE DE HERRAMIENTAS DE HACKING Y SU IMPACTO EN EL SISTEMA OPERATIVO GNU/LINUX

DORIS JANETH RINCON BERNAL
OSMAN GUTIERREZ DIAZ

UNIVERSIDAD AUTONOMA DE BUCARAMANGA
FACULTAD DE INGENIERIA DE SISTEMAS
LINEA DE SISTEMAS DE INFORMACION
BUCARAMANGA
2004

ESTADO DEL ARTE DE HERRAMIENTAS DE HACKING Y SU IMPACTO EN EL SISTEMA OPERATIVO GNU/LINUX

DORIS JANETH RINCON BERNAL
OSMAN GUTIERREZ DIAZ

Proyecto de Grado para optar al titulo de
Ingeniero de Sistemas

Director:
ROBERTO CARVAJAL SALAMANCA
Ingeniero de Sistemas

UNIVERSIDAD AUTONOMA DE BUCARAMANGA
FACULTAD DE INGENIERIA DE SISTEMAS
LINEA DE SISTEMAS DE INFORMACION
BUCARAMANGA
2004

Nota de aceptación

Coordinador Jurado

Jurado 1

Jurado 2

Bucaramanga, Mayo de 2004

A Dios, por darme la vida, las fuerzas para seguir adelante en los momentos mas difíciles y la posibilidad de disfrutar lo que he construido hasta hoy.

A mis Padres Luis Armando y Doris leonor que me demuestran diariamente que todo en la vida se puede realizar, y que el gozo mas grande se da, cuando se obtiene un logro con esfuerzo y dedicación. Sus valiosos consejos han sido una luz en mi vida.

A mi hija Camila Andrea sin ella mi vida no hubiese sido la misma; sin su sonrisa, su voz de aliento y sobre todo su amor.

A mis hermanos Claudia y Javier que me dieron la mano en todo momento y me impulsaron a lograr este objetivo.

A mis familiares y amigos, que llenan mi vida de alegría, caminan junto a mi y me incitan a luchar con tenacidad.

JANETH.

AGRADECIMIENTOS

Los autores de este proyecto expresan sus agradecimientos a:

A la Facultad de Ingeniería de Sistemas, por su valioso aporte a nuestra formación moral e intelectual.

Ingeniero Roberto Carvajal Salamanca, Director de nuestro proyecto y Coordinador de la Facultad de Ingeniería de Sistemas, por sus valiosas orientaciones, sus aportes y colaboración que nos permitieron alcanzar los objetivos propuestos.

A los profesores de la Facultad de Ingeniería de Sistemas, por transmitirnos sus conocimientos.

A nuestros compañeros y amigos, por sus valiosas palabras de apoyo cuando mas las necesitábamos.

CONTENIDO

Pag

1. INTRODUCCION 9

2. RESUMEN 13

3. OBJETIVOS 19

3.1. OBJETIVO GENERAL 19

3.2. OBJETIVOS ESPECIFICOS 19

4. MARCO TEORICO..... 20

4.1. SISTEMAS OPERATIVOS 20
4.1.1. Qué es un Sistema Operativo 20
4.1.2. Seguridad. 20

4.2. LINUX 28

4.3. TIPOS DE INTRUSOS 28

4.4. VIRUS 32

4.5. CONTROL DE ACCESO 34

4.6 DENEGACIÓN DE SERVICIO 39

5. DESARROLLO DE LA INVESTIGACION..... 52

5.1. Listado de Software recopilado 52
5.1.1 Hacking y desencripcion..... 52
5.1.2. Keyloggers. 55
5.1.3 Sniffers 57
5.1.4. Crackeadores 58
5.1.5. Crackeadores de BIOS..... 59
5.1.6. Scanners. 60
5.1.7. Troyanos. 63
5.1.8. Mails Masivos 66

5.1.9. Utilidades y otros 67

5.2 DOCUMENTACIÓN DE ALGUNOS DE LOS PROGRAMAS ENCONTRADOS 69

6. CONCLUSIONES 83

7. RECOMENDACIONES 85

8. BIBLIOGRAFIA 87

ANEXOS 92

LISTA DE FIGURAS

Figura 1 Flujo de Informacion 25

Figura 2 Tipos de Ataques 26

Figura 3 Funcionamiento de una red Normalmente 40

Figura 4 Descripcion de un ataque sufrido 1 40

Figura 5 Descripción de ataque sufrido 2 41

Figura 6 Descripción de ataque sufrido 3 41

Figura 7 Descripción de ataque sufrido 4 42

Figura 8 características de un ataque de Denegación de Servicio 42

Figura 9 Red haciendo un ataque 49

Figura 10 Ejemplo del Comando ping 49

Figura 11 Generalidades de Instalacion de software Investigado 69

Figura 12 Aspecto de un diccionario de palabras 72

LISTA DE TABLAS

Tabla 1 Software de Hacking Y desencripcion de Archivos 52

Tabla 2 Key Loggers 55

Tabla 3 Sniffers 57

Tabla 4 Crackeadores 58

Tabla 5 Crackeadores de BIOS 59

Tabla 6 Scanners 60

Tabla 7 Troyanos 63

Tabla 8 Mails Masivos 66

Tabla 9 Utilidades y Otros 67

LISTA DE ANEXOS

Anexo A Gua de Control de Acceso 92

Anexo B Guia De Denegacion de Servicio 130

Anexo C Entrevistas 135

INTRODUCCION

En este documento se dan a conocer los fenómenos informaticos conocidos como intrusión logica y denegacion de servicio, mas específicamente en equipos con sistemas operativos GNU/LINUX. Esto sucede en maquinas conectadas a redes, las cuales son susceptibles a ataques de intrusos o personas maliciosas. Dichas maquinas tienen sistemas operativos los cuales tienen ciertas vulnerabilidades, las cuales son excelentemente aprovechadas por los cibernautas maliciosos. El objeto de estos ataques puede ser sabotaje corporativo, espionaje de información empresarial o gubernamental, manipulación de datos, vandalismo al azar, casualidad o simplemente curiosidad y reconocimiento por parte de la comunidad hacker. Esta comunidad la cual se esconde dia tras dia en la red mantiene las identidades de sus integrantes en reserva gracias a un seudonimo o mas conocido como Nick, el cual identifica a los cibernautas, haciendo la búsqueda de intruso una tarea realmente complicada por parte de las autoridades. Aunque hoy dia es relativamente sencillo conocer el origen de un ataque por medio de direccionamiento IP o direcionamiento MAC, tambien es realmente facil falcificar estas direcciones, haciendo el trabajo investigativo una tarea de real ingenieria. [1]

El primer tema a tratar consiste en controlar el acceso a los usuarios legitimos de un sistema determinado, esto conlleva a aun serie de procesos como mantener a las maquinas al tanto del estado de usuarios, contraseñas y permisos que tienen acceso al sistema. En muchos casos este control es perfectamente bien efectuado por el sistema operativo, el cual autentica el acceso de usuarios, y entrega permisos para poder acceder a la información y modificarla si es el caso. Sin embargo existen algunas trampas realizadas por los hackers para interceptar esta información, la cual viaja por la red, haciendo imposible al sistema reconocer un usuario legítimo a un intruso. En la actualidad existen algoritmos y metodos muy eficaces los cuales evitan dicha interceptacion de información, estos metodos,

explicados mas adelante, en muchos casos son infalibles o podria decirse inviolables, pero la astucia de un intruso no se limita a el ingenio detrás de un monitor. Existen muchas maneras de conseguir una clave de usuario sin necesidad de interceptar dicha información por la red, entre ellas esta la famosa ingenieria social, el comercio por internet y las claves por defecto que traen los sistemas.

El otro gran problema es el causado por cibernautas maliciosos los cuales se encargan de saturar los sistemas con peticiones de recursos inecesarias, haciendo imposible a los verdaderos solicitantes del servicio acceder a dicho recurso. Entre estos ataques estan los conocidos correos masivos, anonimos o con datos ajuntos excesivamente grandes.

Existen muchas maneras de contrarrestar estos ataques, sin embargo no son suficientes ya que en muchos de los casos son casi imposibles de detectar. En el caso de las versiones mas recientes de los sistemas GNU/LINUX las seguridades ante ataques de denegacion de servicio (DoS) son bastante efectivas, haciendo de este sistema uno de los mas avanzados en materia de proteccion contra DoS.

En la mayoria de casos estos ataques son realizados por vandalos o jóvenes cibernautas que logran crear algunas rutinas de codigo (Scripts) las cuales tienen la capacidad de autoenviarse y autoejecutarse en las maquinas de otros usuarios de manera tal que el rastreo de uno de estos ataques es imposible, ya que proviene de cientos, miles y a veces millones de usuarios, los cuales son completamente inocentes de sus acciones. Por otra parte la falcificacion de direccines IP y MAC hace el rastreo de un ataque total mente inútil. [1],[5],[6]

2. RESUMEN

Debido a la creciente acogida del sistema Operativo GNU/LINUX y el acelerado crecimiento de Internet y la importancia de la información nace con ellos un gran problema el cual es evitar los ataques de ínter nautas maliciosos.

En la actualidad el manejo de la información es más importante que tener grandes cantidades de riquezas o de poder sobre otros. Se dice que aquel que maneje la información maneja el mundo, es por ello que cada dato puede hacer la diferencia entre el éxito y el fracaso. Mantener esta información accesible a sus dueños, a salvo y lejos de intrusos se convierte en la clave del éxito. Sin embargo en términos de sistemas nunca se está lo suficientemente asegurado, y nunca se puede asegurar que la información esta 100 por ciento segura. Dado que el software es susceptible a errores no podemos asegurar que un sistema es completamente seguro, no porque desconozcan las técnicas a la hora de escribir código seguro sino porque es prácticamente imposible no equivocarse en miles de líneas de código. Por otra parte el ingenio de aquellos personajes para violar las seguridades o para evitar que los datos puedan llegar a tiempo a sus verdaderos usuarios es cada vez más difícil de controlar. Es el caso de algunos tipos de Denegación de servicio en donde los ataques parecen peticiones de información totalmente legales. Para solucionar problemas como estos se propone una especie de identificador, el cual tome la decisión de no aceptar paquetes desde ciertas direcciones IP si estas envían repetidamente solicitudes o paquetes de información. Es lógico que un usuario legítimo no vaya a solicitar un servicio más de tres o cuatro veces durante un tiempo determinado, dándonos así una posible solución a este problema. [4]

En el caso de los controles de acceso lo mas útil son las contraseñas o claves de usuario. Sin embargo estas algunas veces son violadas o fáciles de adivinar. Aprovechando la arquitectura de LINUX podemos restringir el acceso no solo por nombre de usuario y contraseña, sino también por direccionamiento IP. Aunque al parecer estas direcciones IP pueden ser falsificadas de manera tal que la victima dará acceso al intruso pensando que es la máquina conocida

En esta investigación se encuentra la información acerca de los fenómenos informáticos conocidos como control de acceso y denegación de servicio. Este documento esta dividido en cuatro secciones.

En la primera sección se habla de las definiciones de estos fenómenos, así como las definiciones, semejanzas y diferencias de distintos tipos de intrusos. Como primera parte esta el control de acceso, el cual se constituye en una herramienta para proteger la entrada a un sistema operativo, un Web, una Base de datos o a cualquier archivo se tenga compartido con otros usuarios. Este control consta generalmente de dos pasos:

• En primer lugar, la autenticación, que identifica al usuario o a la máquina que trata de acceder a los recursos, protegidos o no.

• En segundo lugar, procede la sesión de derechos, es decir, la autorización, que dota al usuario de privilegios para poder efectuar ciertas operaciones con los datos protegidos, tales como leerlos, modificarlos, crearlos, etc.

La forma más fácil de denegar el acceso a un servicio es desactivándolo. En GNU/LINUX tanto los servicios administrados con xinetd y los servicios en la jerarquía /etc/rc.d.

Otra forma de administrar el acceso a los servicios del sistema GNU/LINUX es mediante el uso de iptables para configurar un firewall IP. Si se es un administrador nuevo de LINUX, hay que tener en cuenta que iptables puede que no sea la mejor solución. La configuración de iptables puede ser complicada y es mejor que la realicen administradores de sistemas LINUX experimentados.

Debido a que no se puede evitar que se intercepte la información en una red, es necesaria la utilización de conexiones seguras como SSH y SSL, las cuales son de gran ayuda en el momento de transferencias de claves y contraseñas. Para la transferencia de datos se encuentra una gran utilidad, conocida como llaves personales, las cuales se dividen en dos (Publica y privada) haciendo confiable el envió y recepción de información sin que otra persona la entienda

Por otra parte se encuentra La denegación de servicio. La cual consiste en saturar de peticiones y demandas a los servicios de una máquina o una red, pero también podría tratarse de una impresora o una terminal, con el objetivo que no pueda atender total o parcialmente las peticiones a sus usuarios legítimos.
Estos ataques pueden ser realizados al nivel de red enviando datagramas cuidadosamente preparados y malintencionados de tal forma que puedan causar que las conexiones de red fallen. También pueden realizarse a nivel de aplicación, donde órdenes cuidadosamente construidas se envían contra un programa para tratar que se vuelva muy ocupado o que pare su funcionamiento, dejando de prestar los servicios.
También se tratan temas como los distintos tipos de software que requiere un hacker para introducirse ilícitamente en un sistema, así como los conceptos de conexiones remostas, servicios de red, y definiciones de protocolos de comunicación. [1],[3],[4]

En la segunda sección se encuentra un listado general de los distintos tipos de software que se utilizan para atacar sistemas GNU/LINUX. Cabe decir que

muchos de estos programas funcionan en distintas plataformas. Esta recopilación de distintos programas que funcionan en distintas plataformas es hecha dado que en el momento en que un atacante desea hachear un sistema GNU/LINUX no debe hacerlo desde el mismo LINUX, puede hacerlos desde un sistema como DOS, MAC o UNIX. Sin embargo la documentación de estos programas se limita a aquellos que funcionan en plataformas LINUX más exactamente en su distribución RED HAT 7.1 con kernel 2.4.2-2

Como complemento de esta sección hay un listado general de estos programas, con su clasificación y dirección url en donde ese pueden encontrar (Puede encontrar este software en el disco compacto que se adjunta a este documento.)

La tercera sección incluye dos completas guías que pueden ayudar a los administradores lINUX a proteger sus sistemas de ataques como la denegación de servicio y la intrusión ilícita (lógica) a sus sistemas.

En el campo de la intrusión lógica se muestran soluciones las cuales han dado muy buenos resultados hasta el momento. Sin embargo gracias a las entrevistas realizadas en esta investigación, se puede deducir que el problema a la intrusión ilícita a los distintos sistemas no proviene de errores de software, inclusive no de la información que viaja en la red, ya que muchas veces viaja cifrada, y no hay posibilidad de que sea legible sin una llave. El problema proviene de la falta de conciencia de los usuarios de un sistema, la ingeniería social es el mayor método para conseguir claves o contraseñas de los sistemas. Siguen los usuarios del sistema como empleados, y ex-empleados que se encuentran en descontento con sus condiciones salariales. Otro factor, aunque en muy baja proporción es el intercambio de información por Internet. En Internet se cambia un video porno por la clave de root de un banco y cosas así.

En la parte de denegación de servicio los resultados de la investigación no son muy alentadores, ya que aun no se encuentran soluciones completas o de raíz a este problema. Ya que las denegaciones de servicio consisten en peticiones legales que hacen varios equipos a un solo servidor, o que hace un solo equipo de manera tal que termina bloqueándose, no se puede tener una solución definitiva al problema. Una opción era hacer que el sistema remoto al cual se le hace la petición, tuviese una especie de identificador de direcciones IP o MAC que supiera si un equipo esta haciendo un petición demasiadas veces, sin embargo esto no es una solución total, ya que cuando son mas de 400 equipos los que están atacando el servidor queda imposibilitado para manejar listas de control de acceso y estarlas revisando mas de 100 veces por segundo. Por otra parte algunas redes manejan direccionamiento privado, en donde quien hace la petición del servicio no es el quipo donde esta situado físicamente el usuario sino el servidor Proxy. Y cuando son mas de 1000 equipos donde muchos están haciendo peticiones 100% legales, harán creer al servidor victima que se trata de un ataque de denegación de servicio, cuando en realidad son solo un gran numero de usuarios queriendo acceder a su información.

En la cuarta y última sección se encuentran algunas entrevistas realizadas por los autores de esta investigación y otras entrevistas recopiladas de algunos de los hackers más famosos.

Como conclusión a estas entrevistas se logro deducir que el problema de intrusiones a un sistema no esta en la parte de software sino en la parte de hardware. Muchas veces se preguntan las personas. Y como hace el hacker para entrar a una maquina si se usan conexiones seguras, encriptadas, se bloquean al máximo los puertos por donde se pueda ingresar, e inclusive a veces no hay conexión a ningún otra red. La respuesta a esto la da el señor Kevin Mintick en una entrevista dada días después de pagar una condena por ingresar a un sistema y robar el archivo de contraseñas. Kevin Mintick narra en esta entrevista

la manera en que se conseguían las claves para entrar como un usuario total mente normal. Muchas veces la ingeniería social daba un excelente resultado, como preguntar la clave para hacer un mantenimiento de sistema o para hacer una inocente consulta.

3. OBJETIVOS

3.1. OBJETIVO *GENERAL*

Investigar el estado del arte del hacking, en lo referente a la parte de ataques por falsificación de acceso y negación de servicio, en sistema operativo GNU/LINUX, estableciendo posibles soluciones y recomendaciones para contrarrestar dicho fenómeno.

3.2. OBJETIVOS ESPECIFICOS

Definir mediante contactos con expertos en el tema y búsquedas en Internet, las diferencias entre los distintos tipos de intrusos, con el propósito de identificar y caracterizar los posibles ataques realizados por estos individuos a los sistemas de cómputo.

Recopilar herramientas o programas de violación y ataques por negación de servicio en sistemas GNU/LINUX ya usados por otros intrusos para establecer niveles de vulnerabilidad en el sistema operativo GNU/LINUX

Ejecutar dichos programas encontrados a fin de establecer una taxonomía o clasificación de los mismos.

Basados en los resultados obtenidos, proporcionar a los Administradores de los sistemas operativos GNU/LINUX, un documento guía con posibles soluciones y alternativas para contrarrestar el ingreso de intrusos y ataques por negación de servicio

4. MARCO TEORICO

4.1. SISTEMAS OPERATIVOS

4.1.1. Qué es un Sistema Operativo Un Sistema Operativo es un grupo de programas de proceso con las rutinas de control necesarias para mantener continuamente operaciones de dichos programas, dependiendo de su función. [1]

Es un programa que controla la ejecución de los programas de aplicación y que actúa como interfaz entre las aplicaciones del usuario y el hardware de un computador.

4.1.2. Seguridad El campo de la seguridad es bastante amplio y abarca controles físicos y administrativos así como controles automatizados. Sin embargo todo sistema de seguridad exige ciertos niveles de confiabilidad de información para que se pueda garantizar su seguridad. [2],[7],[9]

Secreto: Consiste en exigir que la información sea suministrada únicamente a quienes tienen permisos. Este tipo de acceso incluye la visualización, impresión y otras formas de revelación de los datos, incluyendo la existencia de los mismos.

Integridad: Incluye toda la parte de edición de la información así como la inserción y eliminación de la misma.

Disponibilidad: Trata de los permisos que se tienen en un sistema de computadores. Es decir, exige que los elementos de un sistema estén disponibles para las partes autorizadas.

Autenticidad: Exige que un sistema sea capaz de verificar la identidad de un usuario.

Seguridad lógica La seguridad lógica es la que se debe tener mas en cuenta, ya que al estar conectados con la red la mayoría de ataques que se reciben Irán hacia el software del computador. Para una buena seguridad lógica se tienen que tener en cuenta muchos factores, pero principalmente factores que dependen de los usuarios, y no del equipo en si. [2],[5]

Una buena contraseña: Fijar una buena contraseña es una de las cosas más importantes a tener en cuenta a la hora de empezar con la seguridad, permitir que los usuarios se pongan contraseñas fácilmente adivinables. Por ejemplo un usuario llamado "pepe" no puede tener una contraseña que sea "pepito" ni el nombre del perro, ninguna data conocida, etc... Tendría que ser algo que no tuviese nada que ver con ese usuario. Por eso es muy importante a la hora que los usuarios pongan contraseñas crear una política de seguridad fuerte que no permita, por ejemplo, una palabra con solo letras y obligue a meter números, una palabra que tenga mas de ocho caracteres, etc... Aunque también es bueno no dejar al abaste de todos esos guiones a seguir por las contraseñas, ya que si un atacante sabe que tienen que haber números, al menos ocho caracteres, máximo 12, etc., son demasiadas pistar para el crackeador de claves (en caso de que consiguiese alguna) Para meter esas políticas en el archivo de claves tendrá que configurar debidamente el archivo “login.defs” ubicado en /etc/.

IDS: Para tener una buena seguridad del sistema es muy recomendado tener IDS (Introducer Detection System) y NIDS (Network Introducer Detection System) ya que pueden dar muchas pruebas sobre los ataques y pueden informar [3],[5]

rápidamente sobre los ataques que se están cometiendo. Existen muchos IDS que van aprendiendo automáticamente, por ejemplo si ven que desde una IP se están realizando muchos intentos de meter una contraseña y va fallando, es posible que sea algún hacker/cracker usando métodos de fuerza bruta, cosa que por supuesto no se quiere, por lo que el IDS bloquea todas las conexiones que lleguen de esa ip hasta que el administrador no diga lo contrario. También pueden encontrar IDS que están configurados para mandar e-mails a los administradores de la red, así como (en redes muy, muy avanzadas) manden un sms al móvil del administrador o a su busca.

Permisos: Se tiene que ir con cuidado con todo lo que tiene que ver con los permisos sobre los archivos. Dejar todos los comandos innecesarios para los usuarios normales inhabilitados, ya que algunos comandos pueden traer problemas. Mrar bien los permisos que se le dan a los archivos haciendo referencia a permisos con los de escritura (w) lectura (r) y ejecución (x). En un sistema linux esto es fácil de hacer. [1],[2],[3]

Periodos: También se tiene que realizar cambios en la política de seguridad periódicamente, por ejemplo obligar a los usuarios a cambiar su contraseña cada X tiempo, dificultando así la tarea de un atacante para averiguar las contraseñas. También es recomendable, en caso de hacer esto de las contraseñas, cambiar los guiones para establecer las contraseñas, por ejemplo si la primera vez tenia que ser de mas de 4 caracteres, la segunda vez puede ser de mas de 6, y la tercera de mas de 8, etc. [1]

Para poder brindar seguridad a un Sistema Operativo primero debemos conocer las amenazas que puede tener nuestro sistema. Los tipos de amenazas se pueden caracterizar mejor por la función del sistema como un suministrador de información. En donde existe un flujo de datos los cuales pueden sufrir anomalías que pueden no ser muy fáciles de detectar.

Interrupción: Es cuando se destruye la información o se hace inaccesible. Generando un ataque a la disponibilidad de la información. Ejemplos de este ataque son los Nukes, que causan que los equipos queden fuera de servicio. También la destrucción o sabotaje de un elemento hardware, o cortar una línea de comunicación.
Interceptación: Una entidad no autorizada consigue acceso a la información. Éste es un ataque contra la confidencialidad., este ataque se hace en secreto, de tal manera que el usuario no se da cuenta. Ejemplos de este ataque son la obtención de datos mediante el empleo de programas troyanos o la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes de datos para desvelar la identidad de uno o más de los usuarios mediante el Spoofing o engaño implicados en la comunicación intervenida (intercepción de identidad).

Modificación: Una entidad no autorizada no sólo consigue acceder a la información de una manera no autorizada, si no que es capaz de manipularlo. Virus y troyanos poseen esa capacidad. Éste es un ataque contra la integridad. Ejemplos de este ataque son la modificación de cualquier tipo en archivos de datos, alterar un programa para que funcione de forma distinta y modificar el contenido de información que esté siendo transferida por la red. Pero en este caso es más fácil que se detecte una intrusión. [1]

Fabricación: Una entidad no autorizada inserta objetos falsificados en el sistema. Éste es un ataque contra la autenticidad. Ejemplos de este ataque son la

inserción de mensajes falsos en una red o añadir datos a un archivo. Asimismo estos ataques se pueden clasificar en términos de ataques pasivos y ataques activos.

Ataques activos: Estos ataques implican algún tipo de modificación de los datos o la creación de falsos datos: Suplantación de identidad, Modificación de mensajes, Web Spoofing Etc. [2]

Suplantación de identidad: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.
Reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B". [2]

Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes imitados. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

Ataques pasivos: En los ataques pasivos el atacante no altera la comunicación, si no que únicamente la escucha o monitoriza, para obtener de esta manera la información que está siendo transmitida. .Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos.
Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:
- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad. Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. El ejemplo de la figura 1 muestra el cambio de información generado por una ataque y en la fugura 2 estan las generalidades de los distiontod problemas al flujo de información, en algunos casos estos problemas son detectados por la victima, en otros no. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

Figura 1 Flujo de Informacion

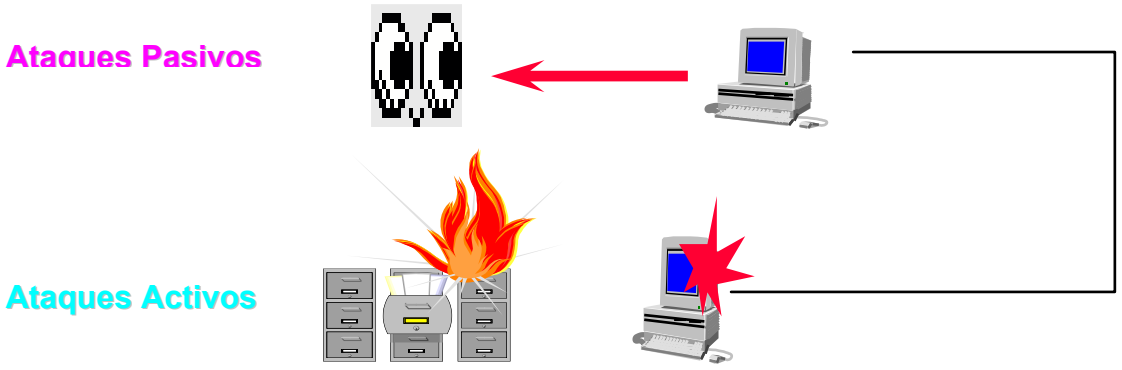
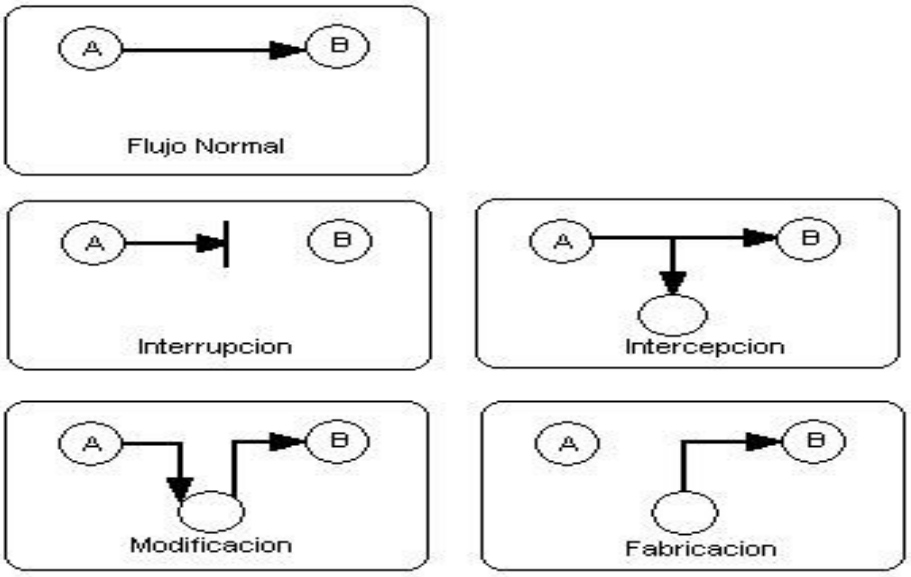


Figura 2 Tipos de Ataques



Proteccion: El hecho de compartir recursos e información compromete no solo al procesador sino también a la Memoria, los dispositivos de la maquina, los programas y los datos. Para ello se pueden tener distintos niveles de protección.
Ninguna: Es apropiada para cuando no se tiene amenaza de destrucción de los datos o sistemas de cómputo. Además es lo más sencillo que se puede realizar.
Aislamiento: Esto implica que cada proceso opere separadamente de los demás. De manera tal que cada proceso tiene su propio espacio de memoria, archivos y otros objetos. [2]

Compartir todo o nada: Esto quiere decir que el propietario de la información permite que cualquier otro usuario pueda acceder a la información. De lo contrario, únicamente los procesos del propietario de la información pueden hacer uso de esta.

Compartir por limitación de acceso: Es como entregar contraseñas a los usuarios autorizados. De manera tal que el sistema actúa como un portero que permite el paso a quienes conoce únicamente.

Compartir por capacidades dinámicas: Consiste en permitir el acceso a los datos por medio de contraseñas y también en dar permisos por partes de la lectura, modificación e impresión de los datos.

En el caso de la Memoria principal, la protección es fundamental. Ya sea a que nadie pueda modificar el contenido de la misma. Si algún proceso llegase a ser modificado en la memoria, nunca seria posible terminar satisfactoriamente dicho proceso. Si se consigue la segmentación y paginación de la memoria, el sistema solo debe asegurarse de que cada proceso acceda a cada página que ha sido asignada.

Software Maligno Tal vez los ataques mas sofisticados a los sistemas son los presentados por los programas que aprovechan los puntos vulnerables de los mismos. Comúnmente estos programas están camuflados dentro de los archivos de editores de texto o compiladores, de tal manera que el usuario los utiliza sin saber el trasfondo que tienen los datos. Estos programas malignos se pueden clasificar en dependientes e independientes. [2]

Trampillas: Es un punto de entrada secreto a un programa que permite a alguien que la conoce conseguir el acceso sin pasar por los procedimientos usuales de seguridad. La trampilla es un código que reconoce alguna secuencia de entrada especial o que se activa al ser ejecutado por un cierto identificador de usuario o mediante una secuencia improbable de sucesos. [2]

Bombas lógicas: Comúnmente están hechas por lo programadores que distribuyen sus aplicaciones de forma legal. Este software estalla en algún momento determinado que ya haya sido programado por el diseñador del sistema.

Caballos de Troya: Son programas o procedimientos útil o aparentemente útil que contiene un código oculto que al invocarse lleva a cabo una función no

deseada. Un caballo de Troya seria imposible de descifrar si fuese hecho por un compilador. Esto seria si al compilar un código, el compilador agrega un código aparte que genere puertas traseras o accesos a la información. [2]

Virus: Es un programa que infecta datos o programas alterando su funcionamiento. Esto también incluye la copia del virus de tal manera que se reproduzca infinitas veces.

Gusanos: Son programas con características de ejecución remota. Los gusanos se propagan a través de redes, en correo electrónico o desde otros equipos. Después de ingresar a la maquina victima se comportan igual que un virus o un caballo de Troya. Además tienen la capacidad de auto transmitirse a otros equipos y auto ejecutarse en su destino.

4.2. LINUX

En líneas generales podemos decir que LINUX dispone de varios tipos de sistema de archivos para poder acceder a archivos en otras plataformas. Incluye un entorno gráfico X Windows (Interface gráfico estándar para máquinas UNIX). Está orientado al trabajo en red, con todo tipo de facilidades como correy web entre otros. [8],[9]

4.3. TIPOS DE INTRUSOS

4.3.1. Hackers Un Hacker es una persona dedicada a su arte, alguien que sigue el conocimiento hacia donde este se dirija, alguien que se apega a la tecnología para explorarla, observarla, analizarla y modificar su funcionamiento, es alguien que es capaz de hacer algo raro con cualquier aparato electrónico y lo hace actuar

distinto, alguien que no tiene límites para la imaginación y busca información para después compartirla, es alguien al que no le interesa el dinero con lo que hace, solo le importa las bellezas que pueda crear con su cerebro, devorando todo lo que le produzca satisfacción y estimulación mental. Un hacker es aquel que piensa distinto y hace de ese pensamiento una realidad con diversos métodos. Es aquel que le interesa lo nuevo y que quiere aprender a fondo lo que le interesa.

4.3.2. Crackers Obviamente que antes que llegar a ser un cracker se debe ser un buen hacker. Asimismo se debe mencionar que no todos los hackers se convierten en crackers. [8],[9]

Un cracker también puede ser el que se dedica a realizar esos pequeños programas que destruyen los datos de las PC.
Los mismos crackers, pueden usar herramientas (programas) hechas por ellos mismos o por otros crackers, que les sirven para des-encriptar información, "romper" los passwords de las PC, e incluso de los programas y compresores de archivos; aunque si estos programas no son manejados por malas manos, pueden ser muy útiles para los técnicos o para uno mismo; claro con los archivos y computadores de cada quien.

4.3.3. Phreacker El phreaker es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello. En Internet se distribuyen planos con las instrucciones y nomenclaturas de los componentes para construir diversos modelos de estos aparatos. [8],[9]

4.3.4. Lamer

Un Lamer es simple y sencillamente un tonto de la informática, una persona que se siente Hacker por haber bajado de Internet el Netbus, alguien a quien le guste bajar virus de la red e instalarlos en la PC de sus amigos, aunque mas bien podría decírsele como un Cracker de pésima calidad; en general alguien que cree que tiene muchos conocimientos de informática y programación, pero no tiene ni la más mínima idea de ello. [8],[9]

4.3.5. Relación entre ellos Un Cracker es parecido al Hacker en cuanto a que el cracker, también puede tener la habilidad de entrar en sistemas ajenos, solo que el cracker destruye la información que encuentra e inclusive la vende.

Un Lamer, pretende ser Hacker, haciendo cosas que los Crackers ya pasaron.

Un Phreacker solo tiene similitud entre estos en que ocupan programas para generar tarjetas de crédito, en lo demás son totalmente diferentes.

Por último, cuando se escuche o lea la palabra Hacker, solo hay que pensar en que es una persona que solo busca información para su uso personal, y no es como el cracker que se dedica a destruir, aunque esto no quiere decir que los hackers no puedan destruir la información, solo que no lo hacen por ética. [8],[9]

4.3.6. SON LOS INTRUSOS

Personal desprevenido Debido a que los empleados se concentran en sus obligaciones laborales específicas, generalmente suelen descuidar reglas estándar relacionadas con la seguridad de la red. Por ejemplo, pueden elegir contraseñas que son fáciles de recordar para poder conectarse a las redes fácilmente. No obstante, los hackers pueden adivinar o craquear fácilmente estas contraseñas usando el sentido común o con un programa de craqueo de contraseñas. Los empleados pueden inconscientemente ocasionar otras violaciones a la seguridad, incluyendo la exposición y difusión accidental de virus

informáticos. Una de las formas más comunes de contraer un virus es a través de un disco flexible o de la descarga de archivos de Internet.

Los empleados que usan discos flexibles para transferir información pueden involuntariamente infectar las redes de la empresa con virus contraídos de computadoras de bibliotecas o centros de copiado. Es probable que ni siquiera ellos mismos sepan que los virus se encuentran en sus PC. Las empresas también se enfrentan al riesgo de infección cuando los empleados descargan archivos de Internet, como presentaciones de PowerPoint.

Las empresas también deben estar alertas ante errores humanos. Los empleados, ya sean principiantes o expertos en computación, pueden cometer errores tales como instalar equivocadamente un software de protección antivirus o accidentalmente pasar por alto advertencias relacionadas con las amenazas a la seguridad.

Personal descontento Mucho más perturbadora que la probabilidad de un error por parte de un empleado que pudiera afectar la red, es la posibilidad de que un miembro del personal esté enojado o quiera vengarse e inflija un daño. Los empleados disgustados, generalmente porque fueron reprendidos, suspendidos o despedidos del trabajo, pueden vengarse infectando las redes de la empresa con virus o intencionalmente eliminar archivos importantes. Este grupo es especialmente peligroso porque en general tiene más conocimiento de la red, de la importancia del contenido de la información, de la ubicación estratégica de la información considerada de alta prioridad y los resguardos establecidos para protegerla.

Curiosos Algunos empleados, tanto conformes como descontentos, también pueden ser curiosos o traviesos. Los empleados identificados como “curiosos” participan en espionajes de la empresa, accediendo sin autorización a datos

confidenciales a fin de facilitar a la competencia información que de otra forma sería inaccesible.

Otros empleados simplemente satisfacen su curiosidad personal accediendo a información personal y privada, como datos financieros, mensajes amorosos de correo electrónico entre compañeros de trabajo o el sueldo de un compañero de trabajo. Algunas de estas actividades pueden resultar relativamente inofensivas pero otras, como revisar datos financieros, el historial de un paciente o información de recursos humanos, son mucho más graves, pueden ser perjudiciales para las reputaciones y generar una responsabilidad económica por parte de la empresa.

4.4. VIRUS

Son programas creados con distintos lenguajes de programación o código de máquina (es el lenguaje más elemental que el computador es capaz de interpretar). Cuando se activa (previamente el usuario a ejecutado dicho virus, en forma de archivo con distintas extensiones ejecutables) el virus comienza su infección, entra en acción el código, que dependiendo, de su programación, será más o menos destructivo, provocando problemas al sistema informático del usuario. Se comportan a veces de forma similar a los biológicos, aunque hay una diferencia muy clara. Los virus informáticos siempre se introducen en el sistema cuando el usuario los ejecuta. Por lo tanto si tenemos un antivirus actualizado y NO ejecutamos archivos de procedencia sospechosa, desconocida, podemos estar a salvo de estos virus con un porcentaje muy alto. Los biológicos es distinto, todos sabemos que nos podemos cuidar perfectamente y por el simple echo de respirar un aire acondicionado contaminado nos puede entrar un virus. Pero creadores de estos programas informáticos víricos en ocasiones, podemos encontrar obras de "ingeniería social" que da lugar a que el usuario ejecute un virus sin prácticamente darse cuenta. [8],[9]

4.4.1. Virus en la Red ¿Qué son los troyanos? No son virus como tales, pero pueden realizar acciones destructivas como algunos virus. Los más peligrosos constan de dos programas, un servidor y un cliente. El servidor es por ejemplo nuestro computador y el cliente es el usuario que intenta "entrar" en nuestra máquina, una vez que ha entrado, en función de las características de dicho troyano, puede borrar archivos de nuestro disco duro, formatearlo, abrir la unidad de cd-rom, realizar capturas de nuestro escritorio, de lo que tecleamos, hay troyanos que "copian" el archivo .PWL que es donde el sistema Windows guarda las contraseñas y las envía a una dirección de correo_electrónico.

4.4.2. Proceso de infección El virus puede estar en cualquier sitio. En ese disquette que nos deja un amigo, en el último archivo descargado de Internet, etc.

Dependiendo del tipo de virus el proceso de infección varía sensiblemente. Puede que el disco contaminado tenga un virus de archivo, en el ARCHIVO.EXE por ejemplo. El usuario introduce el disco en la máquina (por supuesto no lo escanea con un antivirus o si lo hace es con un antivirus desactualizado) y mira el contenido del disco: unos archivos de texto, unas .dll's, un .ini ... ah, ahí esta, un ejecutable. Vamos a ver que tiene. El usuario ejecuta el programa. En ese preciso momento las instrucciones del programa son leídas por el computador y procesadas, pero también procesa otras instrucciones que no deberían estar ahí. El virus comprueba si ya se ha instalado en la memoria. Si ve que todavía no está contaminada pasa a esta y puede que se quede residente en ella. A partir de ese momento todo programa que se ejecute será contaminado. El virus ejecutará todos los programas, pero después se copiará a sí mismo y se "pegará" al programa ejecutado "engordándolo" unos cuantos bytes. Para evitar que usuarios avanzados se den cuenta de la infección ocultan esos bytes de más para que parezca que siguen teniendo el mismo tamaño. El virus contaminará rápidamente los archivos del sistema, aquellos que están en uso en ese momento y que son los

primeros en ejecutarse al arrancar el computador. Así, cuando el usuario vuelva a arrancar la máquina el virus se volverá a cargar en la memoria cuando se ejecuten los archivos de arranque del sistema contaminados y tomará otra vez el control del mismo, contaminando todos los archivos que se encuentre a su paso.

Puede que el virus sea también de "Sector de arranque". En ese caso el código del virus se copiará en el primer sector del disco duro que el computador lee al arrancar. Puede que sobrescriba el sector original o que se quede una copia del mismo para evitar ser detectado. Los virus de sector de arranque se aseguran de ser los primeros en entrar en el sistema, pero tienen un claro defecto. Si el usuario arranca la máquina con un disquete "limpio" el virus no podrá cargarse en memoria y no tendrá el control.

Un caso menos probable es que el virus sea de "Tabla de partición". El mecanismo es muy parecido al de los de sector de arranque solo que el truco de arrancar con un disquete limpio no funciona con estos. En el peor de los casos nos encontraremos con un virus multipartita, que contaminará todo lo que pueda, archivos, sector de arranque, entre otros.

4.5. CONTROL DE ACCESO

El control de acceso constituye en una herramienta para proteger la entrada a un sistema operativo, un Web, una Base de datos o a cualquier archivo se tenga compartido con otros usuarios. Este control consta generalmente de dos pasos:

- En primer lugar, la autenticación, que identifica al usuario o a la máquina que trata de acceder a los recursos, protegidos o no.

- En segundo lugar, procede la sesión de derechos, es decir, la autorización, que dota al usuario de privilegios para poder efectuar ciertas operaciones con los datos protegidos, tales como leerlos, modificarlos, crearlos, etc.

La forma más fácil de denegar el acceso a un servicio es desactivándolo. Tanto los servicios administrados con xinetd y los servicios en la jerarquía /etc/rc.d. [4][7]

Otra forma de administrar el acceso a los servicios del sistema es mediante el uso de iptables para configurar un firewall IP. Si se es un administrador nuevo de LINUX, hay que tener en cuenta que iptables puede que no sea la mejor solución. La configuración de iptables puede ser complicada y es mejor que la realicen administradores de sistemas LINUX experimentados.

Por otro lado, la ventaja de utilizar iptables es flexibilidad. Por ejemplo, si necesita una solución personalizada que proporcione a determinados hosts el acceso a servicios concretos, iptables puede ser una herramienta muy útil.

Para poder construir un cortafuego IP con Linux, es necesario disponer de un núcleo compilado con soporte de cortafuegos de IP y de la utilidad de configuración adecuada. En todos los núcleos anteriores a la serie 2.2 se usaba la utilidad ipfwadm. Los núcleos 2.2.x supusieron el lanzamiento de la tercera generación de cortafuegos de IP para Linux que se denominó 'IP Chains'. 'IP chains' utiliza un programa similar a ipfwadm que se llama ipchains. Los núcleos de Linux 2.3.15 y siguientes soportan la cuarta generación de cortafuegos de IP de Linux que se denomina netfilter. El código de netfilter es el resultado de un gran rediseño del flujo en el manejo de paquetes en Linux. Netfilter es una criatura con múltiples caras, pues proporciona un soporte compatible hacia atrás tanto con ipfwadm como con ipchains además de una nueva orden alternativa que se llama iptables.

Alternativamente, si se está buscando una utilidad que establezca reglas de acceso generales para su máquina, y/o es un nuevo usuario de LINUX, pruebe con GNOME Lokkit. GNOME Lokkit es una aplicación tipo GUI que hace preguntas sobre cómo desea usar el equipo. Basado en las respuestas proporcionadas, configurará un cortafuego sencillo para la máquina. También se puede usar la Herramienta de configuración de nivel de seguridad (redhat-config-securitylevel), la cual permite seleccionar el nivel de seguridad para el sistema, similar a la pantalla de Nivel de seguridad en el programa de instalación de Linux.

4.5.1. Autenticación Se denomina autentificación a la comprobación de la identidad de una persona o de un objeto. Hay muchos sistemas que pueden servir para la autentificación de servidores, de mensajes de remitentes y destinatarios. Pero esto deja pendiente un problema. Las claves privadas suelen estar alojadas en máquinas clientes y cualquiera que tenga acceso a estas máquinas puede utilizar las claves que tenga instaladas y suplantar la identidad de su legítimo usuario. [4]

Por tanto es necesario que los usuarios adopten medidas de seguridad y utilicen los medios de autentificación de usuario de los que disponen sus computadores personales. Hay tres sistemas de identificación de usuario, mediante contraseña, mediante dispositivo y mediante dispositivo biométrico.

La autentificación mediante contraseña es el sistema más común ya que viene incorporado en los sistemas operativos modernos de todos los computadores. Los computadores que estén preparados para la autentificación mediante dispositivo sólo reconocerá al usuario mientras mantenga introducida una “llave”, normalmente una tarjeta con chip. Hay sistemas de generación de claves asimétricas que introducen la clave privada en el chip de una tarjeta inteligente.

Los dispositivos biométricos son un caso especial del anterior, en los que la “llave” es una parte del cuerpo del usuario, huella dactilar, voz, pupila o iris. Existen ya en el mercado a precios relativamente económicos ratones que llevan incorporado un lector de huellas dactilares.

4.5.2. Contraseñas En todo sistema operativo tipo UNIX se dan varias constantes, y una de ellas es el archivo /etc/passwd y la forma en que funciona. Para que la autentificación de usuario funcione correctamente se necesitan (como mínimo) algún tipo de archivo(s) con UID (Numero que identifica al usuario) a mapas de nombres de usuarios, GID (Numero que identifica al grupo que identifica el grupo al que pertenece el usuario) a mapas de nombres de grupos, contraseñas para todos los usuarios y demás información variada. El problema es que todo el mundo necesita acceso al archivo de contraseñas, cada vez que se hace un ls, se verifica el archivo de contraseñas, de modo que ¿cómo se consigue almacenar todas las contraseñas con seguridad y a la vez mantenerlas legibles por el mundo? Durante muchos años, la solución ha sido bastante simple y efectiva, simplemente, haga un hash de las contraseñas y guarde el hash, cuando un usuario necesite autentificar, tome la contraseña que introduce, pásela por el hash y si coincide, evidentemente se trataba de la misma contraseña. El problema que tiene esto es que la potencia computacional ha crecido enormemente, y ahora se puede coger una copia del archivo de contraseñas e intentar abrirlo mediante fuerza bruta en una cantidad de tiempo razonable. Para resolver esto hay varias soluciones: [4]

Utilice un algoritmo de hashing "mejor", como MD5. El problema que puede encontrar, es que se pueden dañar algunas cosas en las aplicaciones de los usuarios.

Almacene las contraseñas en alguna otra parte. Problema: el sistema/usuarios siguen necesitando tener acceso a ellas, y podría hacer que fallasen algunos programas si no están configurados de esta forma.

Varios Sistemas Operativos han escogido la primera opción, Linux ha implementado la segunda opción desde hace tiempo, se llama contraseñas con shadow. En el archivo de contraseñas, se reemplaza la contraseña por una 'x', lo cual le indica al sistema que verifique su contraseña contra el archivo shadow (se hace lo mismo con el archivo de grupos y sus contraseñas). Parece lo suficientemente simple, pero hasta hace bien poco, implementar el shadow era una ardua tarea. Había que recompilar todos los programas que verificasen la contraseña (login, ftpd, etc, etc.) y esto, por supuesto, implica una considerable cantidad de esfuerzo. Es aquí donde brilla Red Hat, con su confianza en PAM.

Para implementar contraseñas con shadow hay que hacer dos cosas. La primera es relativamente simple, cambiar el archivo de contraseñas, pero la segunda puede ser un calvario. Hay que asegurarse que todos sus programas tienen soporte para contraseñas con shadow, lo cual puede ser bastante penoso en algunos casos (esta es una más que importante razón por la cual un mayor número de distribuciones deberían venir con PAM).

Debido a la confianza de Red Hat en PAM para la autentificación, para implementar un esquema nuevo de autentificación todo lo que se necesita es añadir un módulo PAM que lo entienda y editar el archivo de configuración para cualquier programa (digamos el login) permitiéndole que use ese módulo para hacer la autentificación. No hace falta recompilar, Desde el Red Hat 6.0, durante la instalación se le da la opción al usuario de elegir contraseñas con shadow, o puede implementarlas más tarde vía las utilidades pwconv y grpconv que vienen con el paquete de utilidades shadow. La mayoría del resto de distribuciones también tienen soporte para contraseñas con shadow, y la dificultad de

implementación varía de un modo u otro. Ahora, para que un atacante mire las contraseñas con hash, tiene que esforzarse un poco más que simplemente copiar el archivo /etc/passwd. También el administrador debe asegurarse de ejecutar cada cierto tiempo pwconv, para tener la certeza de que todas las contraseñas efectivamente tienen shadow. Hay veces que las contraseñas se quedan en /etc/passwd en lugar de enviarse a /etc/shadow como deberían, lo cual hacen algunas utilidades que editan el archivo de contraseñas.

4.6 DENEGACIÓN DE SERVICIO

La denegación de servicio consiste en saturar de peticiones y demandas a los servicios de una máquina o una red, pero también podría tratarse de una impresora o una terminal, con el objetivo que no pueda atender total o parcialmente las peticiones a sus usuarios legítimos.

Estos ataques pueden ser realizados al nivel de red enviando datagramas cuidadosamente preparados y malintencionados de tal forma que puedan causar que las conexiones de red fallen. Asi se muestran el proceso de un ataque, desde la figuras 3 a la figura 7. También pueden realizarse a nivel de aplicación, donde órdenes cuidadosamente construidas se envían contra un programa para tratar que se vuelva muy ocupado o que pare su funcionamiento, dejando de prestar los servicios.

Figura 3 Funcionamiento de una red Normalmente

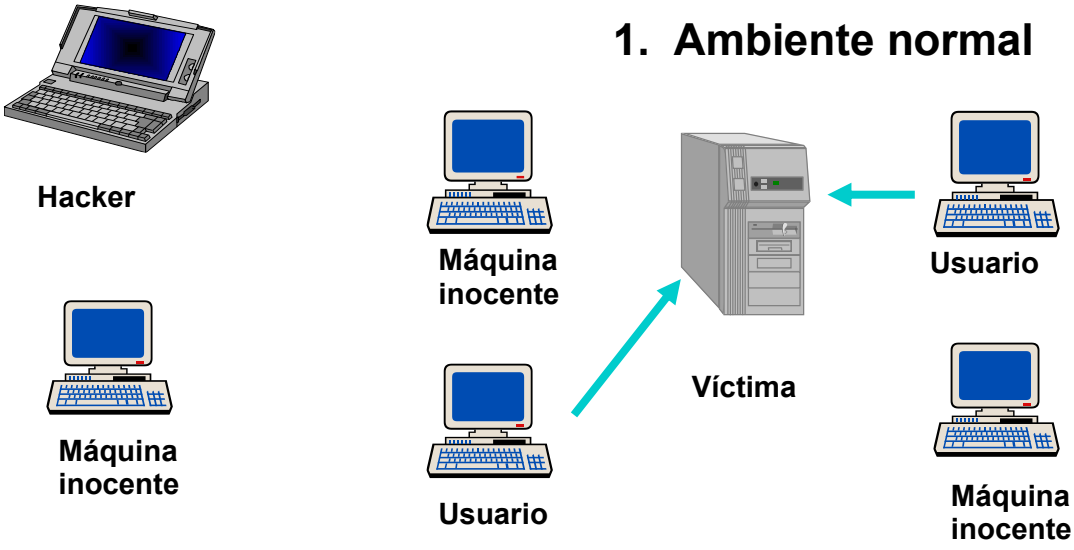


Figura 4 Descripcion de un ataque sufrido 1

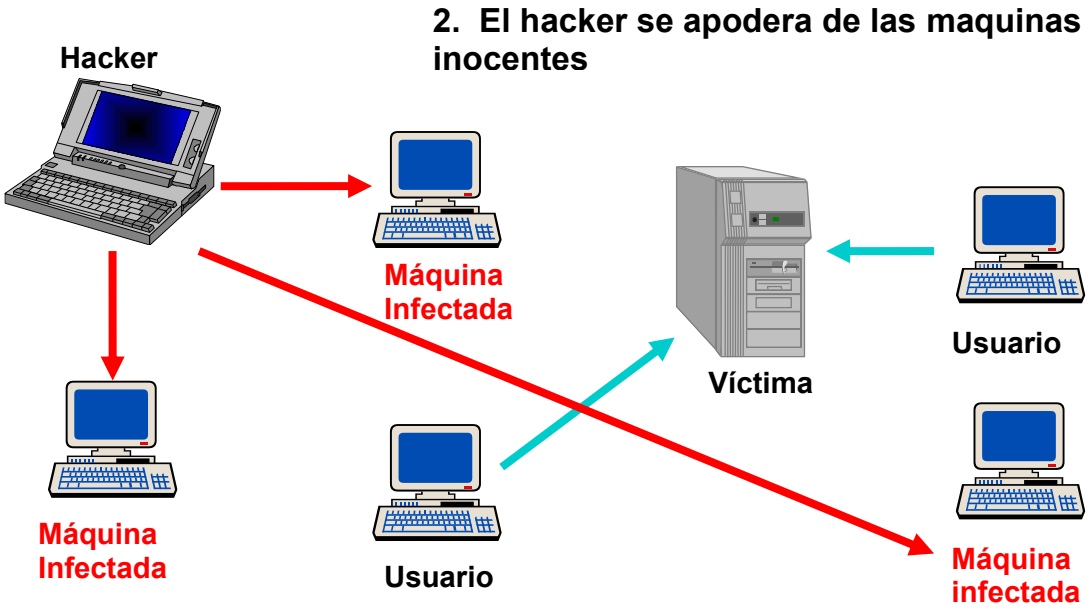


Figura 5 Descripción de ataque sufrido 2

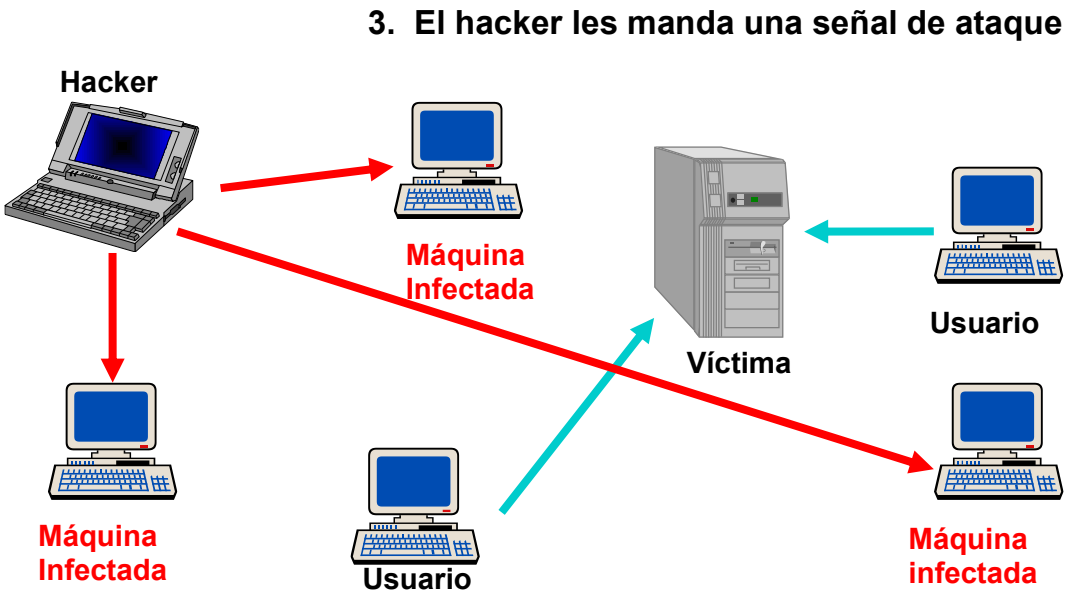


Figura 6 Descripción de ataque sufrido 3

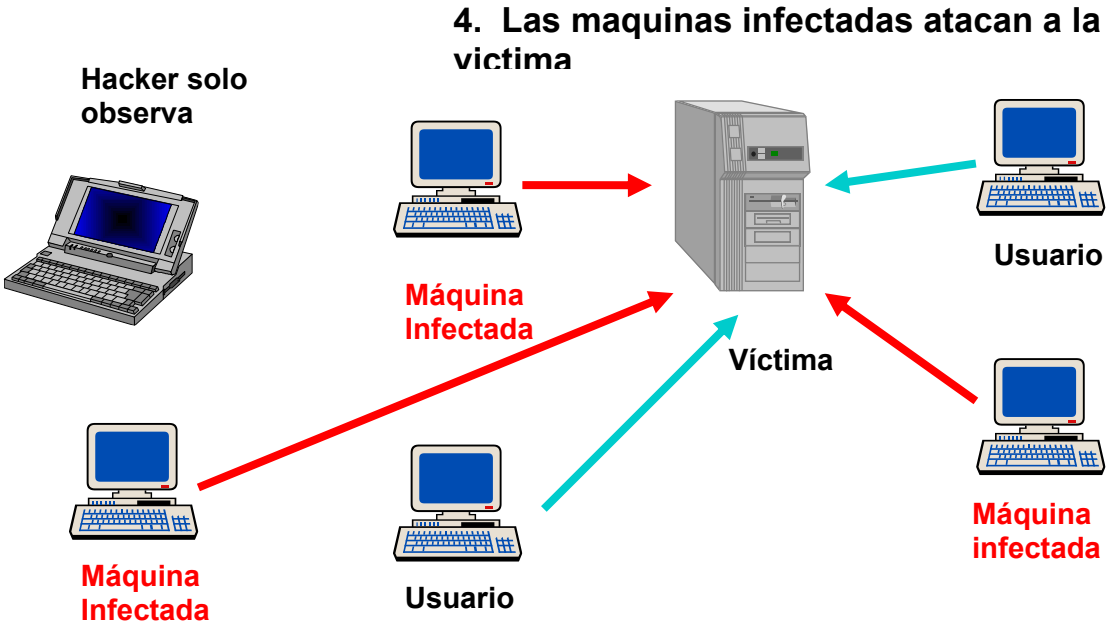
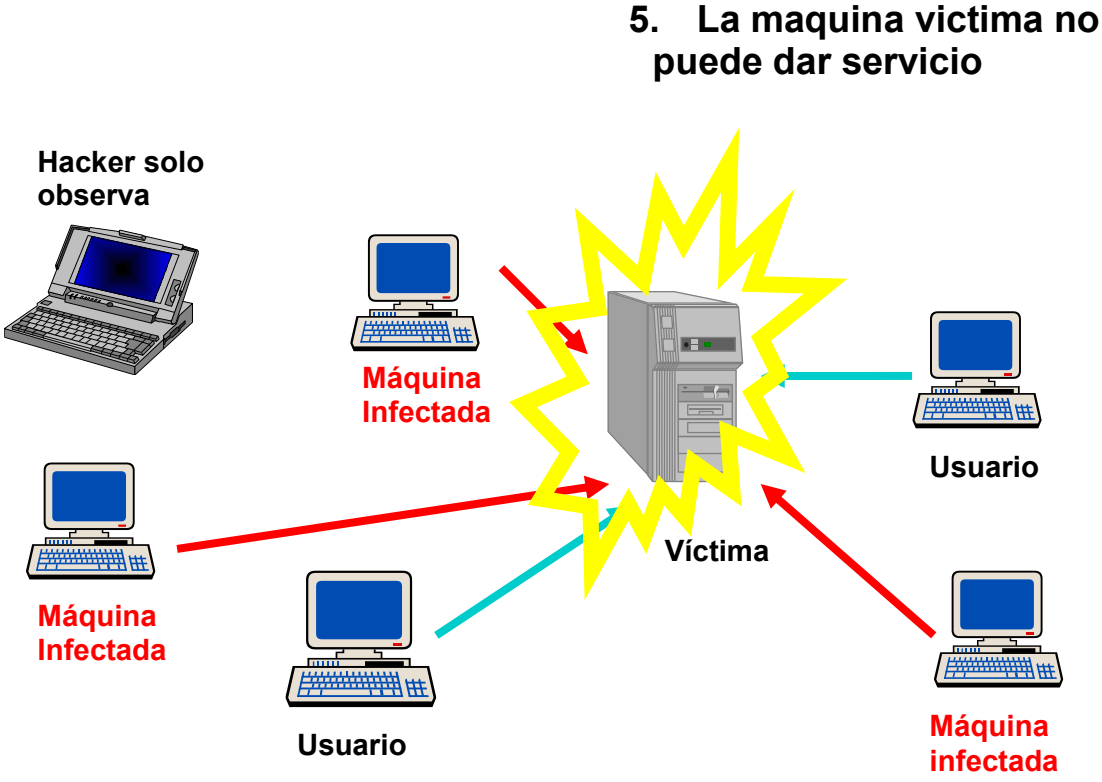


Figura 7 Descripción de ataque sufrido 4



4.6.1. Características: Durante el análisis se simula un atacante externo con intenciones maliciosas, lanzando ataques de Denegación de Servicio frente a componentes de red, sistemas operativos y aplicaciones.

En la figura 17 se muestran algunas pruebas de las caracteristicas mas comunes:

Figura 8 características de un ataque de Denegación de Servicio

- Envió de paquetes TCP incompletos.- Land
- Fragmentos ICMP- Smurff
- Teardrop- CPU Hog
- OOB DoS- Win Nukes
- SYN Flood- Jolt2
- Ping of Death- Bubonic
- SSPing - Otros

* La prueba de Denegación de servicio se realiza fuera del horario habitual de su empresa, para reducir el impacto de este tipo de ataques frente a usuarios legítimos.

En los casos que se presenta este tipo de ataque es:
Inundando la red, de esta forma impide el tráfico en ella, haciendo más lento el transporte de datos.

Rompiendo la conexión entre dos computadores, impidiendo el acceso a determinados servicios.

Impidiendo el acceso de usuarios individuales a un servicio.

Rompiendo los servicios a un sistema especifico,

En este ataque se encuentran involucrados usuarios u organizaciones víctimas que son privadas de utilizar sus propios recursos. Este ataque puede deshabilitar cualquier equipo o red y dependiendo del sistema; este ataque puede llegar a deshabilitar organizaciones completas. Esto se ve en las páginas Web a las cuales ingresan millones de personas, privándolas temporalmente de realizar sus operaciones.

Los ataques de Denegación no siempre son ejecutados por atacantes externos o internos sino que también suceden accidentalmente. De cualquiera de las dos formas que se presente este tipo de ataques siempre trae consecuencias de perdida de tiempo y dinero.

Ejemplos de este tipo de ataque son:
El consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio.

El consumo de ciclos de CPU, de forma que el resto de procesos que corren en la misma máquina apenas dispongan de tiempo de ejecución, por lo que su rendimiento decae rápidamente.

La apertura de cientos o miles de ventanas, con el fin de que se pierda el dominio del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada.

El monopolio de algún periférico, de manera que nadie más pueda acceder a él, obligando así a desconectarlo o a terminar con alguno de los procesos que corren en la máquina.

Se pueden realizar también a nivel de aplicación, donde órdenes que se han construido cuidadosamente se envíen contra un programa para tratar que se vuelva muy ocupado o que pare su funcionamiento.

Impedir que el tráfico de red sospechoso alcance las máquinas y que lleguen órdenes y peticiones de programa sospechosos son las mejores formas de minimizar el riesgo de un ataque de denegación de servicio.

4.6.2. Tipos de ataques por denegación de servicio: Los ataques por denegacion de servicio mas utilizados son:

Consumo de recursos, limitados o no renovables: Los computadores y redes necesitan ciertas cosas para tener un buen funcionamiento: ancho de banda para la red y espacio de disco, tiempo de CPU, estructuras de datos, acceso a otros equipos y redes y recursos de entorno como potencia y aire frío.

Conectividad entre redes: los ataques son frecuentes contra la capacidad de conectividad entre redes. Es necesario evitar que los equipos o las subredes se comuniquen con el resto de la red. El ataque inicia por el proceso de establecimiento de conexión de la máquina víctima, la culminación del ataque llega cuando la máquina víctima ha reservado uno de los limitados números de estructuras de datos requeridos para completar la conexión. El resultado es que la legítima conexión se deniega mientras que la máquina víctima espera a que se complete la conexión, esto no llega a suceder.

Utilización de los propios recursos contra la víctima: un intruso puede usar los recursos de la víctima contra ella misma de inesperadas maneras. El intruso usa paquetes UDP perdidos para conectar el servicio en la máquina que usa el servicio de otra máquina. El resultado es que los dos servicios consumen todo el ancho de banda disponible en la red.

Consumo de ancho de banda: un intruso puede ser capas de consumir todo el ancho de banda en una red generando una gran cantidad de paquetes dirigidos a la red de la víctima. El intruso no necesita actuar desde una de las máquinas de la subred, coordina varias máquinas de diferentes redes y obtener así el mismo resultado.

Consumo de otros recursos: un intruso consume las estructuras de datos escribiendo un script que aunque que no hace nada, pero que crea repetidamente copias de si mismo. Si la tabla de procesos no esta llena, la CPU puede estar ocupada con muchos procesos y el correspondiente tiempo para conmutar entre procesos. Un intruso puede consumir espacio de disco duro así:

Generando un excesivo número de mensajes de correo.
Generando intencionadamente errores que se almacenen en archivos Log.
Colocando archvos en áreas de ftps anónimos.

Destrucción o alteración de los datos de configuración:

Un computador mal configurado no funciona correctamente o puede dejar de hacerlo. Un intruso puede alterar la información de la configuración haciendo que el equipo evite el uso de la red.

Destrucción física o alteración de componentes de red:

Salvaguardar la seguridad física del equipo contra accesos sin autorización a computadores, routers, redes, segmentos de red, generadores de potencia, estaciones refrigeradas.

4.6.3. SISTEMAS DISTRIBUIDOS DE DENEGACIÓN DE SERVICIO

Ataques básicos A principios de la década de los 80, se suponía que controlar lo que ocurría en un sistema Unix no era difícil. El sistema proporcionaba comandos como el last, who, ps, etc, que supuestamente suministraba la información de los últimos accesos, quienes estaban conectados en un determinado momento, e incluso qué procesos se estaban ejecutando. [3]

Con el transcurrir del tiempo, los hackers fueron encontrando métodos que les permitían ocultar sus actividades, e incluso desarrollaron herramientas que facilitaban el borrado de las huellas que podían dejar al pasar por un sistema. De aquella época provienen grupos de news y publicaciones electrónicas como alt.2600 o Phrack.

Con el tiempo, entró en liza el mecanismo de modificar programas básicos del sistema operativo, de manera que sustituyendo al original, proporcionaban a los hackers mecanismos de acceso a información sensible del sistema y de los usuarios. Se denominaron Troyanos, en honor a los griegos y su famoso Caballo de Troya.

Los Root Kits son programas troyanos. Estos paquetes son auténticas colecciones de herramientas e instrucciones detalladas para asaltar sistemas operativos concretos. Existen Root Kits para SunOS/Solaris, Linux.

Identificar qué programas o archivos han sido modificados puede resultar una tarea compleja, los administradores han desarrollado mecanismos de verificación que permiten averiguar la autenticidad de los programas. Como ejemplo, Red Hat Linux emplea un mecanismo de distribución denominado Red Hat Package Manager (RPM), que mediante la utilización de checksums verifica y valida los paquetes instalados.

En cualquier caso, el restablecer la confianza en un sistema que ha sido asaltado es tarea compleja. Incluso aunque se reinstale todo el sistema operativo, que puede ser la solución más drástica, nadie puede garantizar el haber eliminado todos los posibles troyanos: no es posible reinstalar el área de usuarios, donde puede residir alguno.

Ataques de Denegación de Servicio Se han explotado otra serie de métodos de ataque, como pueden ser el spoofing, hijacking o smurfing. Todos orientados a conseguir el asalto o congestión de un sistema remoto. [3]

Con el paso del tiempo, y considerando la evolución que ha sufrido Internet, el enfoque sobre posibles ataques ya no es tanto el intentar acceder a un sistema, sino el imposibilitar su acceso. De cara a una empresa, quizás sea más costoso el que su sistema permanezca inaccesible a que accedan al mismo. Sin considerar que cada día resulta más complejo el asaltar sistemas considerados de interés. Es por ello que los hackers adoptan una nueva estrategia de ataque: provocar la denegación de servicio o imposibilidad de prestar el servicio del sistema atacado.

En las circunstancias actuales de globalización, el daño económico y de imagen que sufre una empresa por un ataque de este tipo probablemente sea mucho mayor que el derivado de una simple intrusión.

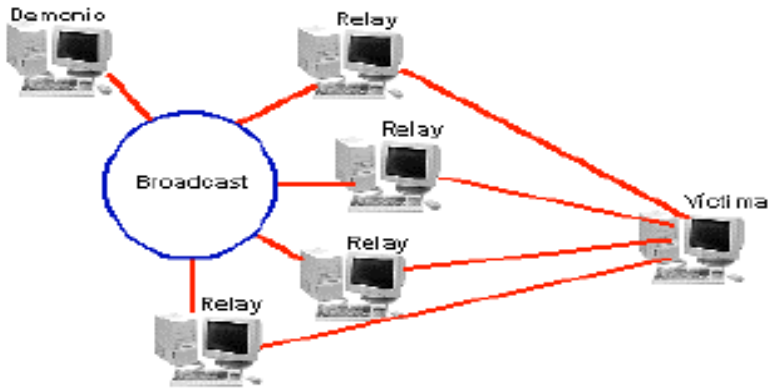
El primer sistema de denegación de servicio fue el denominado mail bombing, consistente en el envío masivo de mensajes a una máquina hasta saturar el servicio. Resulta curioso recordar que esta práctica se empleaba para castigar a quienes se consideraba hacían un uso incorrecto de Internet.

Hoy en día, los mecanismos de ataque por denegación de servicio resultan bastante más sofisticados, empleando debilidades de los protocolos TCP/IP para generar auténticas avalanchas de paquetes sobre un sistema concreto, o simples estados de inconsistencia que provocan que el proceso que atiende el servicio quede inoperante. En algunos casos se han llegado a detectar ataques que generaban más de 1Gbps hacia el sistema atacado. Es cierto que TCP/IP v.4 carece de mecanismos de seguridad que permitan atajar estas prácticas, pero cuando se diseñó la conectividad era lo importante, pues debía ser capaz de afrontar con éxito ataques externos en la infraestructura de comunicación, y en cualquier caso nadie podía imaginar en qué desembocaría aquella red.

El caso del smurfing, o amplificación de peticiones broadcast, ha sido ampliamente utilizado en ataques por denegación de servicio, y es relativamente fácil prevenir el no ser usados en un ataque de este tipo. Este sistema de ataque se basa en transmitir a la red una trama ICMP correspondiente a una petición de ping.

Esta trama lleva como dirección de origen la dirección IP de la víctima, y como dirección de destino la dirección broadcast de la red atacada. De esta forma se consigue que por cada trama que se transmite a la red, contesten a la víctima todos aquellos sistemas (relays) que tienen habilitado el poder contestar a paquetes destinados a la dirección broadcast de la red.

Figura 9 Red haciendo un ataque



Se define como factor de amplificación a la relación entre tramas recibidas por la víctima por cada trama transmitida por el demonio. Puede averiguar el factor de amplificación de su red mediante el siguiente comando: [9]

\/usr/sbin/ping –s <dirección de broadcast de la red> 0 <n>

donde <dirección de broadcast de la red> debe ser la dirección de broadcast que se utiliza en su red, y que depende del rango de direcciones y la máscara de red, y <n> es el número máximo de tramas que esperamos escuchar para finalizar el comando. Es asi como se muestra en la figura 10 un ejemplo de comando ping.

Figura 10 Ejemplo del Comando ping

/usr/sbin/ping –s 138.100.15.255 0 10
proporcionaría un resultado:
PING 138.100.15.255: 0 data bytes

Del resultado anterior puede deducirse que esta red tiene, como mínimo, un factor de amplificación de 10. Un análisis más amplio (n > 100) nos llevaría a afirmar que esta

red tiene un factor de amplificación superior a 100. Puede asegurarse que un ataque empleando esta técnica en una red como ésta sería fatídico. Las contramedidas a este problema son relativamente simples: hay que configurar los sistemas para que no contesten a tramas ICMP cuyo destinatario sea una dirección de broadcast. El problema se convierte en irresoluble cuando los usuarios no quieren o no saben cómo hacerlo.

Cuando el sistema a atacar era lo suficientemente potente como para poder absorber la carga extra de trabajo que pudiera generar el atacante, o se buscase crear algo de confusión sobre el origen del ataque, se organizaban ataques coordinados, realizándose ésta de forma telefónica o por cualquier otra vía de comunicación, como pueden ser los IRC (Internet Relay Chat). Métodos que en cualquier caso sólo eran útiles para un número limitado de atacantes.

Causas que hacen factible se produzcan este tipo de ataques Posibilidad: Es probable que existan en estos momentos cientos de miles o millones de sistemas informáticos conectados a la red y configurados con un bajo nivel de seguridad. Sistemas que prácticamente funcionan de forma desatendida las veinticuatro horas al día. [10]

Calidad del software: Cada día el software es más complejo, los tiempos de desarrollo son menores, los programadores poseen menos experiencia (más baratos) y no se dedica el suficiente esfuerzo en controles de calidad.

Prestaciones vs Seguridad: Hasta la fecha los usuarios optan por las prestaciones del producto, sacrificando o no reclamando niveles de seguridad. Se entiende que la seguridad es una complicación añadida, y que no necesariamente debe formar parte de la solución adoptada. De igual manera se diseñan redes pensando en la velocidad y funcionalidad, pero no en la seguridad.

Personal no cualificado: la capacidad de formación de administradores de sistemas se ha visto desbordada por la demanda, paralela al crecimiento observado en Internet, contratando como administradores de sistemas a personas no cualificadas y sin experiencia.

Defensa legal: la propia Internet facilita que se internacionalice el problema de los ataques, resultando en ocasiones imposible compatibilizar leyes y disposiciones de distintos países, lo que en definitiva juega a favor de los atacantes al existir de hecho una indefensión legal.

5. DESARROLLO DE LA INVESTIGACION

5.1. Listado de Software recopilado

A continuación Se encuentran los listados de software utilizado para generar controles de acceso y denegacion de servicio. En cada tabla se encuentra el nombre del programa y la direccion para descargar dicho programa. Tales direcciones fueron consultadas entre enero del 2004 y majo del 2004.

5.1.1 Hacking y desencripcion de archivos Este software se utiliza para averiguar las cadenas de caracteres correspondientes a claves capturadas por la red.

Tabla 1 Software de Hacking Y desencripcion de Archivos

Nombre	Tamaño	Url
John the Ripper (Win32 v1.6)	0,8 MB	http://www.openwall.com/john/.
John the Ripper (Dos v1.6)	0,7 MB	
John the Ripper (Unix tar.gz v1.6)	0,4 MB	
WebCracker v4.0	1,2 MB	http://packetstormsecurity.org/groups/rhino9/legionv21.zip
Brutus AE v.20	0,3 MB	http://217.125.24.22/h/brutus.zip
Scanner Automatizado vulnerabilidades v1.1	1,13 MB	http://packetstormsecurity.org/groups/rhino9/grinder11.zip
Legión v.2.1 Scanner Recursos	1,91 MB	http://packetstormsecurity.org/

Compartidos		groups/rhino9/legionv21.zip
NetCat para NT v1.1	0,09 MB	http://safariexamples.informit.com/0201719568/Misc/Netcat/NT/nc11nt.zip
Cain v.2.5 Beta 50 (Win 2000,NT,XP)	2,6 MB	http://www.oxid.it/downloads/cain25b50.exe
Librerías para el Cain (WinPcap 3.0)	0,4 MB	http://winpcap.polito.it/install/bin/WinPcap_3_0.exe
Cain 2.0 Crackea pwl, sniffer, etc. (Win 9X)	0,6 MB	http://www.oxid.it/downloads/cain20.exe
RainbowCrack v1.2 Win32	0,5 MB	http://www.antsight.com/zsl/rainbowcrack/rainbowcrack-1.2-win.zip
RainbowCrack v1.2 src Win/Linux	0,04 MB	http://www.antsight.com/zsl/rainbowcrack/rainbowcrack-1.2-src.zip
Arp-Work Network Utility ARP	N.D	http://www.oxid.it/downloads/arpworks10.exe
Services Scanner	N.D	http://www.oxid.it/downloads/irs18.exe
ftp-cracker	0,03 MB	http://217.125.24.22/h/Crackftp.zip
UDP Flooder (D.o.S)	0,06 MB	http://217.125.24.22/h/udpflood.zip
UDPFlood v2.0	N.D	http://www.foundstone.com/knowledge/zips/udpflood.zip
D.o.S Icmp_Echo	0,1 MB	http://217.125.24.22/h/panther.zip
WebSleuth (seguridad web-servers)	2,6 MB	http://www.sandsprite.com/Sle

		uth/SleuthSetup.exe
WebScan v0.92b Scanner cgi's,asp, etc	0,05 MB	http://217.125.24.22/h/webscan.tar.gz
Xnsscan v0.22 Crackeador ftp,pop3,etc	0,037 MB	http://217.125.24.22/h/xnsscan-0.22.tar.gz
Showpass v1.0	N.D	http://www.ipwar.it/ipwartool/showpassv10.zip
IP-Tools v2.08	1,1 MB	http://www.ks-soft.com/download/ip-tools.exe
IP-Tools v2.08 (Mirror)	1,1 MB	http://ks-soft.mastak.com/users/kssoft/download/ip-tools.exe
Crackeador de archivos .zip	0,80 MB	http://www.astalavista.com/tools/password/archives/uzpc.zip
Essential NetTools 3.1	1,4 MB	http://www.all-nettools.com/ent3.zip
Manual (Help File) del Essential NetTools 3.1	N.D	ftp://ftp.tamos.com/docs/en31_help_es.zip
Overflow de netbios	0,2 MB	http://217.125.24.22/h/SMBdie.zip
Libreria Visual Basic (MS Winsock)	0,55 MB	http://217.125.24.22/h/mswinsck.zip
Bug del ISAPI	0,01 MB	http://217.125.24.22/h/lanzadorisapi.zip
scanner netbios	0,01 MB	http://217.125.24.22/h/pqwak2.zip
ArpInject	0,1 MB	http://www.security.nnov.ru/files/PTwebdav.zip

IIS WebDav vulnerability testing tool	0,1 MB	http://packetstormsecurity.org/Win/arpinject.zip
Munga Bunga's HTTP Brute Forcer	N.D	http://ns13.eb1.biz/~clickont/mbhttpbf.exe
Http Flooder - Packet Storm 1.3 - By Subby	0,1 MB	http://217.125.24.22/h/PacketStorm1.3.zip
RpcScan	0,4 MB	http://217.125.24.22/h/RpcScan101.zip
MDcrack 1.2 linux (Crackear MD5/MD4/NTLM hashes)	0,04 MB	http://mdcrack.df.ru/download/mdcrack-1.2.tar.gz
MDcrack 1.2 win32	0,2 MB	http://mdcrack.df.ru/download/mdcrack.exe
MD5 Brute Force Cracker	0,2 MB	http://dev.code-mx.net/flux/md5_bf/md5_bf.tar.gz
GenXE: Generador de Cross Site Scripting	0,1 MB	http://genxe.sourceforge.net/genxe-beta-0.9.0.zip

5.1.2. Keyloggers Este tipo de software se utiliza para mantener una vitacora de lo que sucede en la maquina. Se captura todos los eventos que suceden entre la maquina y el usuario generando un archivo de registro.

Tabla 2 Key Loggers

Windows Keylogger 5.04	0,5 MB	http://www.littlesister.de/keylog5.exe
Perfect keylogger v1.472	0,4 MB	http://217.125.24.22/h/i_bpk2003.zip
Perfect Keylogger v1.3.0.0	N.D	

Nuclear Keys v1.0.	N.D	http://www.nuclearwinter.us/commandox2/Nuclear Keys.zip
Snort 2.1.1 (sniffer/logger)	1,5 MB	http://www.snort.org/dl/snort-2.1.1.tar.gz
RPKeylogger v0.1.	0,04 MB	http://217.125.24.22/h/rpkeylogger-0.1.zip
keylogger Xlog v2.21	0,3 MB	http://217.125.24.22/h/xlog2.21.zip
Key-Logger	0,9 MB	http://217.125.24.22/h/teclas.zip
Ill Logger	0,02 MB	http://217.125.24.22/h/ill-logger2k.zip
Tiny Keylogger	0,09 MB	http://217.125.24.22/h/TinyKL.zip
sc Keylog v2.0	N.D	http://www.astalavista.com/tools/utilities/keylogger/SC-KeyLog2.exe
Invisible Key Logger para Windows 9X	0,7 MB	http://www.amecisco.com/iksv12d.exe
Invisible Key Logger para Windows 2000	0,06 MB	http://www.amecisco.com/iks2k20d.exe
Invisible Key Logger para Windows NT	0,6 MB	http://www.amecisco.com/iksnt10d.exe
Hunt 1.5	0,1 MB	http://lin.fsid.cvut.cz/~kra/hunt/hunt-1.5.tgz

5.1.3 Sniffers Un Sniffer Huele todo el trafico que pasa por una red. De manera tal que la información que no le pertenece la captura, sin embargo muchos de estos Sniffers no logran descifrar la información capturada.

Tabla 3 Sniffers

Snort 2.1.1 (sniffer/logger)	1,5 MB	http://www.snort.org/dl/snort-2.1.1.tar.gz
Invisible Activity Spy Version 2.3	0,3 MB	http://217.125.24.22/h/ias_23.zip
SpyNet v3.12 Sniffer (Win 95/98/NT/2000/XP)	2,2 MB	http://packetstormsecurity.nl/sniffers/spynet/spynet312.exe
Sniffa	0,5 MB	http://217.125.24.22/h/Sniffer.zip
WinSniffer v1.22	0,9 MB	http://www.securityfocus.com/data/tools/ws122.exe
Sniffit	N.D	http://newdata.box.sk/neworder/a/sniffit.0.3.2.tar.gz
Ettercap 0.6.b network sniffer/interceptor/logger	0,6 MB	http://aleron.dl.sourceforge.net/sourceforge/ettercap/ettercap-0.6.b.tar.gz
Sniffer Multiplataforma v0.6.b Win32	2,6 MB	http://aleron.dl.sourceforge.net/sourceforge/ettercap/ettercap-0.6.b-installer-NT2KXP.exe
Ethereal 0.10.2 based network protocol analyzer	5,6 MB	http://www.mirrors.wiretapped.net/security/packet-capture/ethereal/ethereal-0.10.2.tar.gz
Ethereal 0.10.2 Win32	14 MB	http://www.ethereal.com/distribution/win32/ethereal-setup-

		0.10.2.exe
Hunt 1.5	0,1 MB	http://lin.fsid.cvut.cz/~kra/hunt/hunt-1.5.tgz
Ngrep Sniffer 1.4.1	0,5 MB	http://packetstorm.security-guide.de/sniffers/ngrep/ngrep-1.41.tar.bz2

5.1.4. Crackeadores Sirven para Eliminar codigo de algun programa de manera tal que eliminan la seguridad que viene con el. Muchos de estos crackeadores se usan en modo hexadecimal.

Tabla 4 Crackeadores

Advanced ACT Password Recovery 1.20	0,4 MB	http://www.elcomsoft.com/ACTPR/actpr.zip
Advanced Outlook Express Password Recovery 1.13	0,8 MB	http://www.elcomsoft.com/AOEPR/aoepr.zip
Advanced PDF Password Recovery v1.46	0,8 MB	http://www.crackpassword.com/dl/aoxppr_s.zip
Advanced Office XP Password Recovery 2.0 std	N.D	http://www.crackpassword.com/dl/aoxppr_s.zip
Advanced RAR Password Recovery	1,3 MB	http://www.elcomsoft.com/ARPR/arpr.zip
Advanced Instant Messengers Password Recovery 2.20	0,4 MB	http://www.elcomsoft.com/AIMPR/aimpr.zip
Password Cache	0,09 MB	http://217.125.24.22/h/E-pwdcache.zip
Excel-Cracking	0,03 MB	http://217.125.24.22/h/Excelcrack.zip

Word-Cracking	0,20 MB	http://217.125.24.22/h/Wordms.zip
Crackeador de archivos comprimidos con ZIP.	0,3 MB	http://217.125.24.22/h/azpr21k.zip
Crackeador de archivos comprimidos con ARJ.	0,2 MB	http://217.125.24.22/h/aapr107k.zip
Crack para el Winzip (Key-Generator)	0,22 MB	http://217.125.24.22/h/Winzip-k.zip
Decodificador Bases de Datos .MDB	0,2 MB	http://217.125.24.22/h/FL-PasswordRevealer1.0.zip
MS-Office Cracking	0,06 MB	http://217.125.24.22/h/Msofpas.zip
IM Password Recovery v2.10 (Crackear ZIP,ARJ,RAR)	0,5 MB	http://www.elcomsoft.com/AIMPR/aimpr.zip
Excel Password Recovery v1.0b	0,6 MB	http://www.intelore.com/excel/excel-password-recovery.exe
Advanced Zip Password Recovery v3.54	0,7 MB	http://www.elcomsoft.com/AZPR/azpr.zip
Office Password Recovery Key Light v6.1	1 MB	http://www.lostpassword.com/demos/offkeyld.exe

5.1.5. Crackeadores de BIOS Al igual de los crackeadores de software lo que buscan estos crackeadores de BIOS es eliminar el codigo de password que se encuentra en la BIOS de CMOS de una maquina.

Tabla 5 Crackeadores de BIOS

Software para desencriptar BIOS	0,036 MB	http://217.125.24.22/h/BIOS320.zip

Passwords de diferentes tipos de máquinas.	0,001 MB	http://217.125.24.22/h/cmospwd.zip
Award Modular BiOS 4.50 crack tool para bios Award	0,005 MB	http://217.125.24.22/h/awardm.zip
American Megatrends WinBIOS password decrypter.	0,002 MB	http://217.125.24.22/h/winbios.zip
KiLLCMOS32 v.1.0 tool	0,20 MB	http://217.125.24.22/h/k-cmos32.zip

5.1.6. Scanners Un scanner revisa los posibles puertos que existan en la maquina victima. El objeto de este scaneo es averiguar cual de esos puertos es una ventana abirta para poder hacer la intrusión.

Tabla 6 Scanners

Apache Chunked Scanner	0,6 MB	http://datafull.com/datahack/prog/RetinaApacheChunked.exe
Range Scanner (Scanner de Troyanos, etc)	0,01 MB	http://217.125.24.22/h/RangeScanner.zip
HTTPCracker v.10	0,03 MB	http://217.125.24.22/h/HTTPCracker1_0.zip
FrontPage Scanner	0,01 MB	http://www.datafull.com/datahack/prog/FP.zip
Multi Scanner Exploit	0,01 MB	http://217.125.24.22/h/MultiExploit.zip
Scanner	0,3 MB	http://www.foundstone.com/resources/freetools/superscan.exe
Scanner Essencial Net Tools	N.D	http://www.tamofiles.com/ent3.zip

Scanner Net Scan Tools	N.D	ftp://ftp.netscantools.com/pub/nst420.zip
Saint Versión 4.1.4	N.D	http://www.saintcorporation.com/downloads/saint-install-4.1.4.gz
Scanner NMapWin v1.3.1	4,9 MB	http://download.insecure.org/nmap/dist/nmapwin_1.3.1.exe
Scanner nmapNT + Service Pack 1	N.D	http://www.eeye.com/html/Research/Tools/nmapnt/nmapNTsp1.zip
Scanner Nmap Win32 v3.50	0,3 MB	http://download.insecure.org/nmap/dist/nmap-3.50-win32.zip
Scanner Nmap para el NT	1,2 MB	http://packetstormsecurity.org/UNIX/nmap/Nmapnt.zip
Drivers para el Nmap NT	N.D	http://packetstormsecurity.org/UNIX/nmap/DRIVERS.zip
Scanner Nessus 2.0.10a src	N.D	http://ftp.nessus.org/nessus/nessus-2.0.10a/src/
Nessus v2.0.10a (nessus-installer)	N.D	http://packetstorm.security-guide.de/UNIX/audit/nessus/nessus-installer.sh
Scanner NessusWX 1.4.4 Win32	0,9 MB	http://nessuswx.nessus.org/archive/nessuswx-1.4.4.zip
Scanner remote nmap 0.9	0,029 MB	http://telia.dl.sourceforge.net/sourceforge/rnmap/rnmap_0.9.tar.gz
Scanner Nmap Linux/X86 tgz v3.50	1,4 MB	http://download.insecure.org/nmap/dist/nmap-3.50.tgz
Scanner Nmap Linux/X86 RPM	0,4 MB	http://download.insecure.org/n

v.3.50		map/dist/nmap-3.50-1.i386.rpm
Front End para el Nmap v3.50	32 KB	http://download.insecure.org/nmap/dist/nmap-frontend-3.50-1.i386.rpm
GFI LANguard Network Security Scanner 3.2	4,8 MB	http://software.gfi.com/lannetscan.exe
LANguard Port Scanner	0,2 MB	ftp://ftp.languard.com/lanportscan.exe
LANguard Network Scanner	1,5 MB	ftp://ftp.languard.com/lannetscan.exe
LANguard File Integity Checker (2000 y NT)	N.D	ftp://ftp.languard.com/lannetscan.exe
Shadow SecurityScanner Beta	8,1 MB	http://mirror1.safety-lab.com/SSS_Beta.exe
Shadow SecurityScanner v5.35	3,6 MB	http://www.safety-lab.com/SSS.exe
Shadow DoS Analyzer 1.03	N.D	http://mirror1.safety-lab.com/SDA.exe
Shadow Scanner v.2,11	1,5 MB	http://www.rsh.kiev.ua/ShadowScan.exe
Necrosoft NScan	0,3 MB	http://217.125.24.22/h/NScan0666b14f.zip
Scanner Bug Unico de/Decode	0,06 MB	http://www.terra.es/personal2/quickbasic/softwarez/uniscan2.0.zip
Monitorea Tráfico TCP/IP	0,1 MB	http://217.125.24.22/h/portmon301.zip
Port Scan v1.2	0,01 MB	http://217.125.24.22/h/portsca

		n12.zip
Exploit Scanner 2.0 Trojan Scanner	1,4 MB	http://www.megasecurity.org/Scanners/Exploitscan2.0.zip
Boping v2.0 Scanner BO	N.D	http://www.foundstone.com/knowledge/zips/boping.zip
Scaneador Dominios	0,2 MB	http://217.125.24.22/h/domainscan.zip
Vulnerabilidades cgi	0,3 MB	http://217.125.24.22/h/cgiscan.zip
Port Test	0,1 MB	http://217.125.24.22/h/porttest.zip
IP Search Toolbar	0,6 MB	http://www.panix.com/~saint/ipsearch/iptoolb2i.exe
IPsearch v1.9	1,2 MB	ftp://ftp.us.es/Mirror/www.winsite.com/win95/netutil/ipsrch19.zip
Amap Version 4.0	0,2 MB	http://packetstorm.security-guide.de/groups/thc/amap-4.0.tar.gz

5.1.7. Troyanos Equivalen a codigo maligno envuelto en software benefico o amistoso. Al ser ejecutado este amistoso, se ejecuta por debajo el codigo maligno, el cual puede desde abrir un puerto cualquiera a eliminar información.

Tabla 7 Troyanos

Insurrection	1,8 MB	http://www.evileyesoftware.com/files/insurrection.zip
Optix Pro v.1.32	1,1 MB	http://www.evileyesoftware.com/files/OptixPro.zip

Taladrator 2003 (Troyano Español)	1,2 MB	http://217.125.24.22/h/TDR2003.zip
troyano hacktool	0,30 MB	http://217.125.24.22/h/Skanner.zip
Turkoyan v1.0 (Troyano Turco)	1,6 MB	http://www.turkojan.com/turkojan.zip
Fx v1.1.	0,5 MB	http://www.boda-server.com/heibai/tools/trojan/client.rar
CS Trojan	0,6 MB	http://home.arcor.de/skripter/trojan.zip
Armageddon v2.0. (notificador de troyanos)	0,8 MB	http://www.evileyesoftware.com/files/Armageddon.zip
R.A.S. 2002 v1.0.	0,02 MB	http://217.125.24.22/h/ras2002.zip
Assasin v 2.0	6 MB	http://www.evileyesoftware.com/files/assasin2.zip
Assa*SIN* v1.1	0,7 MB	http://217.125.24.22/h/asassin.zip
Cyn v2.1	0,9 MB	http://217.125.24.22/h/CynV2.1.zip
Nexus Portal v3.5	0,6 MB	http://217.125.24.22/h/NexusPortalInstall.zip
Koko Trojan v2.0	0,3 MB	http://217.125.24.22/h/koko_trojan2.zip
Net-Devil 1.5	1,1 MB	http://217.125.24.22/h/netdevil_15.zip
Mosucker v3.0b	2,7 MB	http://217.125.24.22/h/mosucker_3.0b2.zip

Master's Paradise 98 Beta 9.7	N.D	http://packetstormsecurity.org/trojans/mastpara98v9.7b.zip
Busca y peta el netbus	0,2 MB	http://217.125.24.22/h/busconq.zip
NetBus Fucker	0,001 MB	http://217.125.24.22/h/netbusfucker.zip
Netbus Pro v2.01	1,7 MB	http://home.t-online.de/home/husky_college/nbpro201.exe
Netbus Pro v2.1	2 MB	http://fusionhack.iespana.es/fusionhack/Hacking/Programas/Troyanos/NetbusPRO.exe
Sub Seven v2.1.0	1,3 MB	http://www.hackemate.com.ar/sub7/files/Sub7 v2.1.0.zip
Sub Seven 2.1.5 Legends	1,3 MB	http://www.hackemate.com.ar/sub7/files/Sub7 v2.1.5 Legends.zip
Sub Seven v2.2.0	2,8 MB	http://www.hackemate.com.ar/sub7/files/Sub7 v2.2.zip
Bionet v4.0.5.	1,3 MB	http://217.125.24.22/h/BioNet_4-0-5.zip
LiTTLeWiTCH Cliente v6.3	0,9 MB	http://comunidad.ciudad.com.ar/argentina/capital_federal/yosoyelmencho/download/lwclient.zip
LiTTLeWiTCH Server (Actualizado 16-4-03)	0,36 MB	http://comunidad.ciudad.com.ar/argentina/capital_federal/yosoyelmencho/download/miniserver.exe

LiTTLeWiTCH Plug-in para Capturar Pantallas	0,85 MB	http://comunidad.ciudad.com.ar/argentina/capital_federal/yosoyelmencho/download/pluginccap.zip
Ptakks v2.1	0,4 MB	http://bcnhackers.iespana.es/bcnhackers/utilidades/ptakks21.exe
Back Oriffice v1.2	N.D	http://orifice.rotten.com/cDc/bo120.zip
Cliente del BO en Español	0,3 MB	http://217.125.24.22/h/Bofacil.zip
Faceless Stealth Tools v1.2	0,2 MB	http://217.125.24.22/h/Faceless Stealth Tools 1.2.zip
Remote Administrator v2.1	1,3 MB	ftp://files.mokry.cz/radmin/radmin21.zip

5.1.8. Mails Masivos Este tipo de software solo funciona con servidores de correo POP3 y que soporten el reenvio de mensajes. La capacidad de este software se extiende al envio de mensajes anonimos o con destinatarios falsos hasta el envio de mas de 1000 mensajes a un solo usuario.

Tabla 8 Mails Masivos

Minoza de Sunmatrix	0,7 MB	http://www.sunmatrix.net/do/minoza.zip
Direct Email Blaster XP 6.51	0,7 MB	http://www.zstools.com/download/edeb_set.zip
e-mail Bomber v8.1	0,8 MB	http://www.softheap.com/download/bomber.zip
Ubi Anonymous	0,8 MB	http://217.125.24.22/h/ubi_ano

		nymous.zip
Kaboom v3.0.	0,3 MB	http://217.125.24.22/h/kaboom v3.0.zip
Mcspammer	0,2 MB	http://217.125.24.22/h/mcspa mmer.zip
Fmbomb	0,02 MB	http://217.125.24.22/h/fmbomb .zip
Alanch v.3.4	0,1 MB	http://217.125.24.22/h/alanch3 4.zip
xmas 2000	0,4 MB	http://217.125.24.22/h/xmas20 00.zip
Bombita	0,1 MB	http://217.125.24.22/h/bombita .zip
Btopmail	0,2 MB	http://217.125.24.22/h/topmail. zip
Embozator	0,1 MB	http://217.125.24.22/h/emboza tor.zip
ebomber2002	0,1 MB	http://217.125.24.22/h/ebombe r2002.zip

5.1.9. Utilidades y otros En esta ultima seccion se encuentra un listado de las utilidades para proteccion de archivos. Algunas de ellas utilizan algoritmos como MD% o Shadow para cifrar la informacion

Tabla 9 Utilidades y Otros

freeware network query tool	1,7 MB	http://static.samspade.org/ssw /spade114.exe
Authorization bypass 99 (Auto	0,06 MB	http://217.125.24.22/h/authbyp

authorization)		ass99.zip
Genius 2.6 (telnet client, ftp, finger, html, smtp etc)	1,1 MB	http://217.125.24.22/h/genius26.zip
Fake NetStat	0,016 MB	http://217.125.24.22/h/Netstat.zip
Sockschain 3.6 Multi-proxy con Socks4 y Socks5.	0,3 MB	http://www.ufasoft.com/files/sockschain_setup.exe
Proxy Redirect	0,028 MB	http://217.125.24.22/h/ProxyRedirect.zip
Auto Downloader v1.0.0 (especie de troyano)	0,020 MB	http://217.125.24.22/h/autodlw100.zip
Stealth Tools v2.0.	0,2 MB	http://217.125.24.22/h/Stealthtools2.0.zip
ProcDump32	0,2 MB	http://217.125.24.22/h/procdp14.zip
YAB v2.0 (Binder)	0,4 MB	http://217.125.24.22/h/y4b_bln d.zip
Interactive Disassembler. DOS.	0,030 MB	http://217.125.24.22/h/disaster.zip
Editor hexadecimal. Windows	0,065 MB	http://217.125.24.22/h/exa.zip
Proxy-Bouncer sin logs + socks5 y 4	0,075 MB	http://217.125.24.22/h/evilsocks.zip
Anti-Binder Bound File Extractor 1.00	0,08 MB	http://217.125.24.22/h/bfe_10.zip
FSG Compressor 1.31 (Compresor troyanos y virus)	0,2 MB	http://217.125.24.22/h/fsg.zip
UPX-GUI 2001 (Compresor UPX con GUI)	0,2 MB	http://217.125.24.22/h/upxgui108w.zip
UPX 1.24 (Ultimate Packer for	0,1 MB	http://upx.sourceforge.net/dow

eXecutables)		nload/upx124w.zip
Haktek	0,2 MB	http://hjem.get2net.dk/T-Stick/programs/haktek.zip
E-mail Remover	0,2 MB	http://217.125.24.22/h/eremove20.zip
Desprotege los flash (*.swf)	0,09 MB	http://217.125.24.22/h/flashit11.zip

5.2 DOCUMENTACIÓN DE ALGUNOS DE LOS PROGRAMAS ENCONTRADOS

A continuación la documentación de algunos de los programas que se utilizaron para la investigación. En la figura 11 se encuentran las generalidades de todos los programas.

Figura 11 Generalidades de Instalacion de software Investigado

Descargar archivos (En sistemas Unix)
Wget [url]

Ejemplo
wget "http://www.openwall.com/john/john-1.6.tar.gz"

Descomprimir Código Fuente
Tar zxvf [ruta][Nombre archivo]
Ejemplo
tar -zxvf /home/install/sistema/john-1.6.tar.gz

Jonh The Ripper

John the Ripper es un crackeador de claves muy rápido, está disponible en muchos Unix, DOS, Hasefroch32, BeOS y OpenVMS. Su principal función es un detectar claves débiles de Unix, pero puede analizar claves hash de varios tipos Unix, Kerberos AFS y Hasefroch NT/2000/XP LM hashes, y otros muchos parches disponibles en la Red.

Se consigue en http://www.openwall.com/john/.

Instalación
Bajar el archivo desde la dirección especificada
Descomprimir el código fuente el código fuente
Compilar el programa
cd john-1.6/src
make
Seleccione linux-x86-any-elf como sistema en la mayoría de los casos
make linux-x86-any-elf

El ejecutable ha quedado en /usr/src/john-1.6/run/john
mv -f /usr/src/john-1.6/run/john /sbin
chown root.root /sbin/john
chmod 700 /sbin/john

Es posible que se requiera mas ayuda.
more /usr/src/john-1.6/doc/README
more /usr/src/john-1.6/doc/CONFIG

Utilización
cp /usr/src/john-1.6/run/john.ini /root/john.ini
cd /root

cp /etc/passwd /root/passwd
chmod 600 /root/passwd
chown root.root /root/passwd
john -single /root/passwd

Si se obtiene un resultado como:
Loaded 0 passwords, exiting...

Significa que el sistema a hachear tiene el paquete shadow passwords activado. En tal caso, es necesario exportar las claves encriptadas del archivo /etc/shadow al formato del /etc/passwd:
pwunconv
cp /etc/passwd /root/passwd
pwconv

Algunas distribuciones de Linux funcionan distinto
unshadow /etc/passwd /etc/shadow > /root/passwd
chmod 600 /root/passwd
chown root.root /root/passwd
john -single /root/passwd

Después de unos minutos se obtiene un resultado como el que sigue:
guesses: 128 time: 0:00:00:16 7%.

En este caso, por ejemplo, se ha logrado averiguar las claves de 128 cuentas, un 7% del total de las del sistema.

Otro test que resulta más largo que el anterior, pero que puede ofrecer más claves resueltas es el siguiente:
john -w:diccionario1.txt -rules passwd

En este caso se hace uso de un diccionario "diccionario1.txt", un archivo de texto plano con el aspecto miostrado en la figura 12

Figura 12 Aspecto de un diccionario de palabras

aaaaaa
aaaaaa1
aaaaaaa
aaadekoy
aaalmann
aaashfor
aadavis

de forma que John the Ripper intenta construir claves para probar a partir de las palabras del diccionario. Cuantas más palabras tenga el diccionario, más efectiva será la búsqueda. Un buen diccionario tiene palabras en los idiomas más conocidos: español, inglés, francés, Alemán, entre otros.

WebCracker v4.0

Web Craker es un crackeador de claves en fuerza bruta.

Se consigue en http://packetstormsecurity.org/groups/rhino9/legionv21.zip

Instalación
Bajar el archivo desde la dirección especificada
Descomprimir el código fuente
Compilar el programa
cd wbcrack/src
make

El ejecutable ha quedado en /usr/src/wbcrack

mv -f /usr/src/wbcrack /run/wbcrack /sbin

chown root.root /sbin/wbcrack

chmod 700 /sbin/wbcrack

Utilización

Las configuraciones se guardan en /usr/share/wbcrack/ y el programa debe ejecutarse como root

Los archivos *.chr y el wbcrack.conf son necesarios para que funcione el programa, cuando lo instale desde el código fuente estos archivos es posible que no se encuentren, los debe conseguir de la instalación del binario.

Existen tres formas de aplicar el Wbcrack:

Archivo de palabras:

Este es el modo más simple, todo lo que se necesita es especificar un archivo que contenga una palabra por línea.

wbcrack -wordfile:nombre_archivo archivo_password

o bien se pueden añadir -reglas para que use las palabras del diccionario

wbcrack -w>Archivo_diccionario -Reglas Archivo_password

SigleCrack:

Este es el modo con el que se debería comenzar a crackear. Este modo intentará usar la información de login/GECOS

wbcrack -single Archivo_password

Incremental (fuerza bruta):

El más efectivo, ya que probará todas las combinaciones de caracteres posibles. Necesita indicar la longitud de la clave y los juegos de caracteres.

wbcrack -i archivo password

puede especificar que caracteres usará con este método y la longitud, las configuraciones están en el archivo wbcrack.conf en la sección [incremental:MODO]

wbcrack -i:alpha archivo_password (a..z - 26 caracteres)
wbcrack -i:all archivo_password (todo - 95 caracteres)
wbcrack -i:digits archivo_password (0..9 - 10caracteres)

Externo:
Mediante funciones en un sublenguaje de C se pueden crear palabras que luego usará Wbcrack.
wbcrack -external:nombre_modo Archivo_password

Brutus AE v.20
Brutus es un crackeador de claves en fuerza bruta.

Se consigue en http://217.125.24.22/h/brutus.zip

Instalación
Bajar el archivo desde la dirección especificada
Descomprimir el código fuente
Compilar el programa
cd Brutus/src
make linux-x86

El ejecutable ha quedado en /usr/src/Brutus
cp -f /usr/src/Brutus /run/Brutus /sbin
chmod 777 /sbin/Brutus

Utilización

Standard

De esta manera brutus intentará usar un gran número de palabras que trae incorporadas

Brutus -s Archivo_password

Diccionario

El más efectivo, ya que probará todas las combinaciones de caracteres posibles. Necesita indicar la longitud de la clave y los juegos de caracteres.

Brutus -d archivo password nombre diccionario

RainbowCrack v1.2 src Win/Linux

Rainbow es un crackeador de claves en fuerza bruta. Dispononible en sistemas Unix, y Windows

Se consigue en http://www.antsight.com/zsl/rainbowcrack/rainbowcrack-1.2-src.zip

Instalación

Bajar el archivo desde la dirección especificada

Descomprimir el código fuente

Compilar el programa

cd Rrbw/src

make linux-x86

El ejecutable ha quedado en /usr/src/Rrbw

cp -f /usr/src/Rrbw /run/Rrbw /sbin

chmod 777 /sbin/Rrbw

Utilización

Standard

De esta manera Rrbw intentará usar un gran número de palabras que trae incorporadas

Rrbw -s Archivo_password

Diccionario

El más efectivo, ya que probará todas las combinaciones de caracteres posibles. Necesita indicar la longitud de la clave y los juegos de caracteres.

Rrbw -d archivo password nombre diccionario

En Windows la instalación incluye un asistente y una interfaz GUI para la ejecución del programa

SMBDie

Utilidad para averiguar las claves de los directorios o carpetas compartidas en una red local mediante el protocolo NetBios. Puede generar una función como una denegación de servicio, ya que por fuerza bruta se dedica a saturar el número máximo de equipos entrando al directorio.

Se consigue en: http://217.125.24.22/h/SMBdie.zip

Instalación

Bajar el archivo desde la dirección especificada

Descomprimir el código fuente

El ejecutable ha quedado en /usr/src/smbdie

cd /run/smbdie /sbin

chown root.root /sbin/smbdie

chmod 700 /sbin/smbdie

Utilización

Las configuraciones se guardan en /usr/share/smbdie/ y el programa debe ejecutarse como root
Los archivos *.chr y *.conf son necesarios para que funcione el programa.

Es posible que requiera una librería propia del servicio samba, para ello instale los paquetes de samba, y actívelos al arrancar la maquina con el comando setup.

Existen varias formas de aplicar el SMBDie estas son las más comunes:

Archivo de palabras:
Este es el modo más simple, todo lo que se necesita es especificar un archivo que contenga una palabra por línea.
smbdie -f:nombre_archivo archivo_password

SigleCrack:
Este es el modo más sencillo para comenzar a crackear.
smbdie -single Archivo_password

MDcrack 1.2
Crackeador de claves hecha con un formato superior al de 8 caracteres o similar al de MD*

Se consigue en: http://mdcrack.df.ru/download/mdcrack-1.2.tar.gz

Instalación
Bajar el archivo desde la dirección especificada
Descomprimir el código fuente el código fuente
El ejecutable ha quedado en /usr/src/mdsrc/run/
cp /usr/src/mdsrc/run/john /sbin

chown root.root /sbin/john
chmod 700 /sbin/john

Es posible que se requiera mas ayuda.
more /usr/src/mdsrc/doc/README
more /usr/src/mdsrc/doc/CONFIG

Utilización
cp /usr/src/mdsrc/run/john.ini /root/john.ini
cd /root
cp /etc/passwd /root/passwd
chmod 600 /root/passwd
chown root.root /root/passwd
mdcrc -single /root/passwd

Después de unos minutos se obtiene un resultado como el que sigue:
guesses: 128 time: 0:00:00:16 7%.

En este caso, por ejemplo, se ha logrado averiguar las claves de 128 cuentas, un 7% del total de las del sistema.

Otro test que resulta más largo que el anterior, pero que puede ofrecer más claves resueltas es el siguiente:
mdcrc -w:diccionario1.txt -rules passwd

de forma que MdCrack intenta construir claves para probar a partir de las palabras del diccionario. Cuantas más palabras tenga el diccionario, más efectiva será la búsqueda.

MD5 Brute Force Cracker

Crackeador de claves hecha con un formato superior al de 8 caracteres o similar al de MD5.

Se consigue en: http://dev.code-mx.net/flux/md5_bf/md5_bf.tar.gz

Instalación

Bajar el archivo desde la dirección especificada

Descomprimir el código fuente el código fuente

El ejecutable ha quedado en /usr/src/mdsrc/run/

cp /usr/src/mdsrc/run/john /sbin

chown root.root /sbin/john

chmod 700 /sbin/john

Es posible que se requiera mas ayuda.

more /usr/src/mdsrc/doc/README

more /usr/src/mdsrc/doc/CONFIG

Utilización

cp /usr/src/mdsrc/run/john.ini /root/john.ini

cd /root

cp /etc/passwd /root/passwd

chmod 600 /root/passwd

chown root.root /root/passwd

mdcrc -single /root/passwd

Después de unos minutos se obtiene un resultado como el que sigue:

guesses: 128 time: 0:00:00:16 7%.

En este caso, por ejemplo, se ha logrado averiguar las claves de 128 cuentas, un 7% del total de las del sistema.

Otro test que resulta más largo que el anterior, pero que puede ofrecer más claves resueltas es el siguiente:
mdcrc -w:diccionario1.txt -rules passwd

de forma que MdCrack intenta construir claves para probar a partir de las palabras del diccionario. Cuantas más palabras tenga el diccionario, más efectiva será la búsqueda.

Snort 2.1.1

Snort es un IDS o Sistema de detección de intrusiones basado en red (NIDS). Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar alguna vulnerabilidad, análisis de protocolos, etc conocidos. Todo esto en tiempo real.

Una característica muy importante e implementada desde hace pocas versiones es FlexResp. Permite, dada una conexión que emita tráfico malicioso, darla de baja, hacerle un DROP mediante el envío de un paquete con el flag RST activa, con lo cual cumpliría funciones de firewall, cortando las conexiones que cumplan ciertas reglas predefinidas.

Se consigue en: http http://www.snort.org/dl/snort-2.1.1.tar.gz

Instalación
Bajar el archivo desde la dirección especificada
Descomprimir el código fuente el código fuente

Utilización

Digite el comando. /snort o snort simplemente y aparecerá una listado de opciones.

Snort [opción]

Es posible que desee un filtro de paquetes

Snort [opción] <Filtro>

Hunt 1.5

Hunt 1.5 es un IDS o Sistema de detección de intrusiones basado en red. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar alguna vulnerabilidad, análisis de protocolos, etc conocidos. Todo esto en tiempo real y con una interfaz GUI.

Se consigue en: http://lin.fsid.cvut.cz/~kra/hunt/hunt-1.5.tgz

Instalación

Bajar el archivo desde la dirección especificada

Descomprimir el código fuente el código fuente

El ejecutable ha quedado en /usr/src/hunt/run/

cp /usr/src/hunt/run/hunt /sbin

chown root.root /sbin/hunt

chmod 700 /sbin/hunt

Utilización

Digite el comando ./hunt 1.5 o hunt 1.5 simplemente y aparecerá una listado de opciones.

Hunt [opción]

Sniffit

Sniffit es un sniffer basado en red. Implementa un motor de detección de ataques y barrido de puertos que detecta ataques, barridos ajenos, intentos de aprovechar alguna vulnerabilidad, análisis de protocolos, etc.

Se consigue en: http://newdata.box.sk/neworder/a/sniffit.0.3.2.tar.gz

Instalación

Bajar el archivo desde la dirección especificada

Descomprimir el código fuente el código fuente

El ejecutable ha quedado en /usr/src/hunt/run/

cp /usr/src/hunt/run/hunt /sbin

chown root.root /sbin/hunt

chmod 777 /sbin/hunt

Utilización

Digite el comando ./sniffit o sniffit simplemente y aparecerá una listado de opciones.

./Sniffit [opción]

6. CONCLUSIONES

Existen muchas maneras de generar ataques por denegación de servicio, infortunadamente estas maneras se pueden ver como legales, debido a que son simples peticiones que realiza un usuario a un servidor.

Tal vez la mejor manera de contrarrestar un ataque por denegación de servicio sea la misma que se usa para evitar el continuo repique de un teléfono por alguien indeseado. Y es poner un identificador de llamadas de manera tal que cuando llame esa persona indeseada podamos identificarle con su número de teléfono. En el caso de los computadores podemos hacer que en el momento de identificar la dirección IP la cual está pidiendo el mismo servicio repetidas veces en un lapso de tiempo muy corto, automáticamente sea negada la petición.

Los accesos remotos son un mal necesario en muchos casos, las conexiones tipo Telnet, y Rlogin pueden permitir que la máquina sea administrada y reparada fácilmente, es decir sin desplazarse hasta el servidor. Sin embargo proporciona una amplia entrada para todo aquel intruso que tiene buenos conocimientos para descifrar claves e interceptar información.

Aunque aún no sabemos cómo, entendemos que se puede falsificar una dirección IP. De esta manera es posible que nunca se consiga un método totalmente seguro para evitar estos ataques, puesto que si un atacante remoto logra hacerse parecer alguien legal, no habrá manera de detectarlo. Por otra parte un atacante que desee bloquear una máquina al inundarla de paquetes, peticiones e información inútil, puede que enmascare su verdadera identidad con direcciones al azar cada vez que hace el envío de paquetes o información. De manera tal que la propuesta del identificador de llamadas seria inútil.

Un Scanner es una herramienta muy útil para verificar información, identificar intrusos y paquetes innecesarios, sin embargo usados por malas manos son perjudiciales para los administradores de sistemas. De igual manera todos aquellos programas que generan logs del movimiento en una maquina pueden ayudar a identificar personas ociosas en una entidad. Pero si este software es usado para el mal, puede ser muy perjudicial.

Aunque algunos de los programas que permiten la revelación del movimiento de una maquina, son detectables por el usuario o administrador, es muy incomodo y dispendioso estar revisando a cada momento si la maquina tiene un software de este tipo instalado. Es ahí en donde una política de seguridad y la expresión “todo lo que no esta expresamente permitido esta prohibido” hacen de una sistema mas ágil y robusto.

7. RECOMENDACIONES

Es importante mencionar que la seguridad no solo depende de las medidas que se tomen para evitar que los hackers ingresen al sistema, depende también de la política de uso que se tenga en la máquina. De nada sirven todas las medidas que se pongan si los usuarios intercambian claves unos con otros, ponen de clave su login, tienen privilegios de root, etc. No se puede olvidar, que la mayoría de los ataques, provienen de los usuarios de la propia máquina.

Unas normas básicas a seguir:

Conviene a cada uno de los usuarios explicarles unas ciertas normas sobre el uso de la máquina que podría empezar con la frase de "Todo lo que no esta explícitamente permitido, esta prohibido" y continuar explicando todo lo que está permitido.

Administrador no hay más que uno. A medida que el número de administradores tiende a infinito, la funcionalidad en la máquina tiende a cero. Si hay muchas personas modificando el sistema, unas tocaran sobre lo que ayer modifico otra persona y al final las cosas dejaran de funcionar y será imposible saber porque exactamente.

Los usuarios solo deben tener los privilegios necesarios para ser usuarios. En un exceso de celo, es posible cometer el error de limitar demasiado los privilegios de los usuarios. Esto hace que el usuario no pueda usar la máquina normalmente y se pierda de vista el objetivo por el que realiza todo esto. Por otro lado, si los usuarios tienen excesivos privilegios se puede encontrar que por desconocimiento, experimentación o maldad se cause daño al sistema.

Una buena política de claves es conveniente: obligar a cambiar el clave cada 3 meses, chequear la clave de los usuarios contra diccionarios para encontrar claves fáciles, no dejar repetir claves, etc.
Es conveniente que se verifique o audite constantemente el manejo de las claves de cada usuario. Podrá parecer paranoico, pero una revisión periódica ayuda a mantener alerta a los usuarios y evita que una clave pueda ser usada para efectos dañinos durante un largo tiempo.

La actualización de software es muy útil, muchas veces se dejan bugs o errores en los sistemas. Es por eso que una constante actualización permite al administrador defenderse de estos errores. Además, cada día nacen nuevas formas y maneras de ser atacados, la mente criminal de algunos personajes no cesa de generar ideas para bloquear servidores. Pero de igual manera esta un sin numero de programadores, diseñadores y usuarios de sistemas GNU/LINUX dispuestos a corregir y contrarrestar errores encontrados.

Actualmente es posible configurar la red de manera tal que una tarjeta de red no pueda recibir información de varias direcciones IP, esto se logra enlazando la direccion IP a la direccion MAC de la tarjeta de red. Al configurar la red de esta manera, se evita que puedan funcionar posibles sniffers en los demas equipos. Esta opción es posible si se manejan direcciones estáticas, de lo contrario lo que se lograra es bloquear el acceso de los equipos, ya que la direccion MAC no concordara con la direccion IP Asignada por el servidores de la red.

La última recomendación es... sentido común.

8. BIBLIOGRAFIA

Textos Guía

(1) STALLINGS, William. Sistemas Operativos. 4 Ed. España. 2002, 764 p.

(2) CARRETERO, Jesús; GARCIA, Felix. Sistemas Operativos Una Visión Aplicada. 1 Ed. España. 2001, 732 p.

(3) TANENBAUM, Andrew. Sistemas Operativos Modernos. 1 ed. México. 1992, 825 p.

(4) PETERSEN, Richard. Linux, Manual de Referencia. España. 2000. 1306 p.

(5) Revista Enter. Ed 57. Mayo 2003. Colombia.

(6) Revista Enter. Ed 61. Septiembre 2003. Colombia.

(7) B. Forouzan - Trasmisión de Datos y Redes de Comunicación - McGraw Hill - 2a Edición - 2002.

(8) John Y. Hsu - Computer Networks: architectures, protocols and software - Boston Artech House

(9) Fred Halsall - Comunicación de datos, redes de computadores y sistemas abiertos – Pearson Education Addison Wesley

(10) Douglas E. Comer. - Internet Working with TCP/IP - Volumen I; Principles, Protocols and Architectures - Second Edition. Prentice Hall International

(11) W. Richard Stevens - Unix Network Programming - Prentice Hall Software Series

(12) Uyless D. Black - Data Networks Concepts, Theory, and Practice - Prentice Hall.

(13)P. García - Trasmisión de Datos y Redes de Computadores - Prentice Hall - 2003.

Revistas:

(14) Linux Journal Ed 150. Ene 2003. España.

(15) Sys Admin Ed 22. Jun 2003. USA

(16) Perl Journal Ed 58. Mar 2004. España

Paginas WEB

(18) Firewalling and Proxy Server HOWTO
http://metalab.unc.edu/LDP/HOWTO/Firewall-HOWTO.html
(Ene 2004 – May 2004)

(19) Linux IPCHAINS HOWTO
http://metalab.unc.edu/LDP/HOWTO/IPCHAINS-HOWTO.html
(Ene 2004 – May 2004)

(20) Linux NETFILTER HOWTO
http://netfilter.kernelnotes.org/
(Ene 2004 – May 2004)

(21) Linux Security HOWTO
http://metalab.unc.edu/LDP/HOWTO/Security-HOWTO.html
(Ene 2004 – May 2004)

(22) Linux Shadow Password HOWTO
http://metalab.unc.edu/LDP/HOWTO/Shadow-Password-HOWTO.html
(Ene 2004 – May 2004)

(23) The Linux CIPE + Masquerading mini-HOWTO
http://metalab.unc.edu/LDP/HOWTO/mini/Cipe+Masq.html
(Ene 2004 – May 2004)

(24) Firewall Piercing mini-HOWTO
http://metalab.unc.edu/LDP/HOWTO/mini/Firewall-Piercing.html
(Ene 2004 – May 2004)

(25) Quota mini-HOWTO
http://metalab.unc.edu/LDP/HOWTO/mini/Quota.html
(Ene 2004 – May 2004)

(26) Secure POP via SSH mini-HOWTO
http://metalab.unc.edu/LDP/HOWTO/mini/Secure-POP+SSH.html
(Ene 2004 – May 2004)

(27) The VPN HOWTO (using SSH)
http://metalab.unc.edu/LDP/HOWTO/mini/VPN.html

(Ene 2004 – May 2004)

(28) Red Hat Knowledge Base
http://www.redhat.com/cgi-bin/support?faq
(Ene 2004 – May 2004)

(29) Bugtraq Archives
http://www.geek-girl.com/bugtraq/
(Ene 2004 – May 2004)

(30) CERT Incident Reporting Guidelines
http://www.cert.org/tech_tips/incident_reporting.html
(Ene 2004 – May 2004)

(31) SECURITY RISK ANALYSIS AND MANAGEMENT
http://www.norman.com/local/whitepaper.htm
(Ene 2004 – May 2004)

(32) An Introduction to Information Security
http://www.certicom.com/ecc/wecc1.htm
(Ene 2004 – May 2004)

(33) Site Security Handbook
http://sunsite.cnlab-switch.ch/ftp/doc/standard/rfc/21xx/2196
(Ene 2004 – May 2004)

(34) How to Handle and Identify Network Probes
http://www.network-defense.com/papers/probes.html
(Ene 2004 – May 2004)

(35) IANA Port Numbers
http://rlz.ne.mediaone.net/linux/papers/port_numbers
(Ene 2004 – May 2004)

(36) Free Firewall and related tools (large)
http://sites.inka.de/sites/lina/freefire-l/index_en.html
(Ene 2004 – May 2004)

(37)Internet FAQ Consortium (You want FAQ's? We got FAQ's!)
http://www.faqs.org/
(Ene 2004 – May 2004)

(38) The human side of computer security (an article on social engineering)
http://www.sunworld.com/sunworlden línea/swol-07-1999/swol-07-security.html
(Ene 2004 – May 2004)

(39) IBM Redbooks
http://www.redbooks.ibm.com/
(Ene 2004 – May 2004)

(40) SecurityPortal, tiene una sección de Linux y mi columna semanal (así que por supuesto es un gran sitio)
(Ene 2004 – May 2004)

(41)Open Security Solutions
http://www.opensec.net/
(Ene 2004 – May 2004)

ANEXOS

Anexo A Guia de control de acceso

En esta sección se podrá encontrar ayuda y técnicas para contrarrestar la intrusión de distintos atacantes. Iniciando con la definición de este fenómeno informático, siguiendo con la demostración de algunas de las técnicas y herramientas mas usadas por los intrusos, para terminar con una guía a manera de tutorial de manera que se puedan configurar los servidores y estaciones de trabajo garantizando la seguridad de la red y la información que viaja por ella.

Cómo determinar qué asegurar y cómo asegurarlo

Se protegen datos (propietarios, confidenciales o de cualquier otro tipo), también se intenta mantener ciertos servicios en marcha (servidor de correo, servidor www, etc.), algunas veces lo que se protege es el hardware y otras lo que se protege es solo el acceso a esos recursos.

Es necesario listar todos aquellos recursos (servidores, servicios, datos y otros componentes) que contengan datos, den servicios, formen parte de la infraestructura de la compañía, etc. A continuación se detalla una pequeña lista de ejemplo:

Servidores físicos
Servidores de correo.
Servidores de DNS.
Servidores de WWW.
Servidores de archivos
Datos internos de la compañía, como registros contables
Infraestructura de la red (cables, hubs, switches, routers, etc.)

Sistema telefónico (PBX, buzones de voz, etc.)

Después necesita definir contra qué se quiere proteger:

Intrusiones físicas (locales o desde la misma maquina)

Borrado / modificación de datos (registros contables, deterioro de su sitio Web, etc.)

Exposición de datos (registros contables, etc.)

Continuidad de servicios (mantenimiento activo de los servidores de correo/www/archivos)

Evitar que otros hagan uso ilegal/impropio de sus servicios (envíos masivos de correos, etc.)

Escaneos de red.

Ingeniería social.

Intrusión física.

Empleados que venden datos a la competencia.

La competencia, que alquile a gente especializada para penetrar activamente en su red.

Finalmente, ¿cuál es la probabilidad de que se dé un suceso determinado?

Una vez que se tiene una lista de sus recursos y de aquello que es necesario hacer, es hora de empezar a implementar los controles. Algunas técnicas (seguridad física para servidores, etc.), son pueden ser bastante útiles, en estos temas existen unas pautas de comportamiento de seguridad que por lo general están implementadas (poner claves a las cuentas, etc.). La gran mayoría de los problemas de seguridad suelen ser de origen humano, y la mayoría de los problemas que se han visto están debidos a la falta de educación/comunicación entre gente, no existe un sistema totalmente automático que no requiera administrador técnicamente hablando, incluso el mejor software necesita alguien para instalarse, configurarse y estar mantenido.

Ya entrando en materia, he aquí una pequeña lista de los posibles resultados derivados de un incidente ocasionado por la falte de control de acceso:
Pérdidas de datos
Perdida directa de beneficios (ventas vía Web, el servidor de archivos inactivo, etc)
Costes en tiempo de personal
Pérdida de productividad del departamento de informática, así como de los trabajadores dependientes de su infraestructura
Implicaciones legales (registros médicos, registros contables de clientes, etc.)
Pérdida de la confianza por parte del cliente
Publicidad por parte de los medios de comunicación
Introducción al control de acceso
El control de acceso constituye en una herramienta para proteger la entrada a un sistema operativo, un Web, una Base de datos o a cualquier archivo se tenga compartido con otros usuarios. Este control consta generalmente de dos pasos:

• En primer lugar, la autenticación, que identifica al usuario o a la máquina que trata de acceder a los recursos, protegidos o no.
• En segundo lugar, procede la sesión de derechos, es decir, la autorización, que dota al usuario de privilegios para poder efectuar ciertas operaciones con los datos protegidos, tales como leerlos, modificarlos, crearlos, etc.

La forma más fácil de denegar el acceso a un servicio es desactivándolo. Es decir si se desea tener totalmente seguro una sitio, lo mejor será cerrar puertas y ventanas de manera tal que nadie salga, y nadie entre. Para ello se niegan los servicios administrados con xinetd y los servicios en la jerarquía /etc/rc.d.

Otra forma de administrar el acceso a los servicios del sistema es mediante el uso de iptables para configurar un firewall IP. Si se es un administrador nuevo de LINUX, hay que tener en cuenta que iptables puede que no sea la mejor solución.

La configuración de iptables puede ser complicada y es mejor que la realicen administradores de sistemas LINUX experimentados.

Por otro lado, la ventaja de utilizar iptables es flexibilidad. Por ejemplo, si necesita una solución personalizada que proporcione a determinados hosts el acceso a servicios concretos, iptables puede ser una herramienta muy útil.

Para poder construir un cortafuego IP con Linux, es necesario disponer de un núcleo compilado con soporte de cortafuegos de IP y de la utilidad de configuración adecuada. En todos los núcleos anteriores a la serie 2.2 se usaba la utilidad ipfwadm. Los núcleos 2.2.x supusieron el lanzamiento de la tercera generación de cortafuegos de IP para Linux que se denominó 'IP Chains'. 'IP chains' utiliza un programa similar a ipfwadm que se llama ipchains. Los núcleos de Linux 2.3.15 y siguientes soportan la cuarta generación de cortafuegos de IP de Linux que se denomina netfilter. El código de netfilter es el resultado de un gran rediseño del flujo en el manejo de paquetes en Linux. Netfilter es una criatura con múltiples caras, pues proporciona un soporte compatible hacia atrás tanto con ipfwadm como con ipchains además de una nueva orden alternativa que se llama iptables.

Alternativamente, si se está buscando una utilidad que establezca reglas de acceso generales para su máquina, y/o es un nuevo usuario de LINUX, pruebe con GNOME Lokkit. GNOME Lokkit es una aplicación tipo GUI que hace preguntas sobre cómo desea usar el equipo. Basado en las respuestas proporcionadas, configurará un cortafuego sencillo para la máquina. También se puede usar la Herramienta de configuración de nivel de seguridad (redhat-config-securitylevel), la cual permite seleccionar el nivel de seguridad para el sistema, similar a la pantalla de Nivel de seguridad en el programa de instalación de Linux.

Acceso ilícito.

Se considera imposible el ingresar a un sitio sin tener previo conocimiento de algo que pueda ayudarnos a entrar a ese lugar. Es el caso de una dirección, un nombre de maquina, puede ser un cable o una contraseña. Es similar al acceso ilegal a una residencia, Por lo menos se debe saber donde esta en la casa, o que tipo de cerraduras usan los residentes. Suponiendo que un ataque se efectuase sin tener ningún conocimiento previo de la victima, este no seria más que una casualidad, la cual no podría llegar más lejos a actos de vandalismo común. Es decir se afectaría a alguien sin saber a quien se esta afectando.

El acceso ilícito se inicia desde el momento en que una persona ingresa al sitio el cual no le es permitido, si el posible intruso, lo único que hace es revisar posibles puertas y ventanas por las cuales se pueda introducir, no es considerado ningún ataque. La ley no dice que el hecho de tener capacidad de atacar a alguien deba ser restringido, simplemente en el momento de cometer el delito, se le considera acceso ilícito. Sin embargo, de igual manera sucede con un ladrón que esta rondando una casa en busca de puertas, ventanas y huecos por donde introducirse. Esto no lo hace ladrón, pero si sospechoso, por lo cual hay que tomar medidas antes de que el intruso desee atacar.

Entonces bien, lo primero que debe hacer un intruso, es buscar esas puertas y ventanas que estén disponibles para ingresar al sistema. Algunas son demasiado sofisticadas como accesos remotos con decifración de claves, otros son mas sencillos basados en lo que se conoce como ingeniería social para averiguar las claves de los usuarios.

Contraseñas

Administración de contraseñas

En todo sistema operativo tipo UNIX se dan varias constantes, y una de ellas es el archivo /etc/passwd y la forma en que funciona. Para que la autentificación de

usuario funcione correctamente se necesitan (como mínimo) algún tipo de archivo(s) con UID (Numero que identifica al usuario) a mapas de nombres de usuarios, GID (Numero que identifica al grupo que identifica el grupo al que pertenece el usuario) a mapas de nombres de grupos, contraseñas para todos los usuarios y demás información variada. El problema es que todo el mundo necesita acceso al archivo de contraseñas, cada vez que se hace un ls, se verifica el archivo de contraseñas, de modo que ¿cómo se consigue almacenar todas las contraseñas con seguridad y a la vez mantenerlas legibles por el mundo? Durante muchos años, la solución ha sido bastante simple y efectiva, simplemente, haga un hash de las contraseñas y guarde el hash, cuando un usuario necesite autentificar, tome la contraseña que introduce, pásela por el hash y si coincide, evidentemente se trataba de la misma contraseña. El problema que tiene esto es que la potencia computacional ha crecido enormemente, y ahora se puede coger una copia del archivo de contraseñas e intentar abrirlo mediante fuerza bruta en una cantidad de tiempo razonable. Para resolver esto hay varias soluciones:

Utilice un algoritmo de hashing "mejor", como MD5. El problema que puede encontrar, es que se pueden dañar algunas cosas en las aplicaciones de los usuarios.

Almacene las contraseñas en alguna otra parte. Problema: el sistema/usuarios siguen necesitando tener acceso a ellas, y podría hacer que fallasen algunos programas si no están configurados de esta forma.

Varios Sistemas Operativos han escogido la primera opción, Linux ha implementado la segunda opción desde hace tiempo, se llama contraseñas con shadow. En el archivo de contraseñas, se reemplaza la contraseña por una ‘x’, lo cual le indica al sistema que verifique su contraseña contra el archivo shadow (se hace lo mismo con el archivo de grupos y sus contraseñas). Parece lo suficientemente simple, pero hasta hace bien poco, implementar el shadow era

una ardua tarea. Había que recompilar todos los programas que verificasen la contraseña (login, ftpd, etc, etc) y esto, por supuesto, implica una considerable cantidad de esfuerzo. Es aquí donde brilla Red Hat, con su confianza en PAM.

Para implementar contraseñas con shadow hay que hacer dos cosas. La primera es relativamente simple, cambiar el archivo de contraseñas, pero la segunda puede ser un calvario. Hay que asegurarse que todos sus programas tienen soporte para contraseñas con shadow, lo cual puede ser bastante penoso en algunos casos (esta es una más que importante razón por la cual un mayor número de distribuciones deberían venir con PAM).

Debido a la confianza de Red Hat en PAM para la autentificación, para implementar un esquema nuevo de autentificación todo lo que se necesita es añadir un módulo PAM que lo entienda y editar el archivo de configuración para cualquier programa (digamos el login) permitiéndole que use ese módulo para hacer la autentificación. No hace falta recompilar, Desde el Red Hat 6.0, durante la instalación se le da la opción al usuario de elegir contraseñas con shadow, o puede implementarlas más tarde vía las utilidades pwconv y grpconv que vienen con el paquete de utilidades shadow. La mayoría del resto de distribuciones también tienen soporte para contraseñas con shadow, y la dificultad de implementación varía de un modo u otro. Ahora, para que un atacante mire las contraseñas con hash, tiene que esforzarse un poco más que simplemente copiar el archivo /etc/passwd. También asegúrese de ejecutar cada cierto tiempo pwconv, para tener la certeza de que todas las contraseñas efectivamente tienen shadow. Hay veces que las contraseñas se quedan en /etc/passwd en lugar de enviarse a /etc/shadow como deberían, lo cual hacen algunas utilidades que editan el archivo de contraseñas.

Archivos de contraseñas
/etc/passwd

El archivo de contraseñas es sin discusión el archivo más crítico en Linux (y en la mayoría de otros Unix). Contiene el mapa de nombres de usuarios, identificaciones de usuarios y la ID del grupo primario al que pertenece esa persona. También puede contener el archivo real, aunque es más probable (y mucho más seguro) que utilice contraseñas con shadow para mantener las contraseñas en /etc/shadow. Este archivo debe ser legible por todo el mundo, o si no comandos tan simples como ls dejarían de funcionar correctamente. El campo directorio personal puede contener datos tales como el nombre real, el número de teléfono y otro tipo de cosas parecidas en cuanto al usuario, su directorio personal, que es el directorio en que se coloca al usuario por defecto si hace un login interactivo, y el shell de login tiene que ser un shell interactivo (como bash, o un programa de menús), y estar listado en /etc/shells para que el usuario pueda hacer login. El formato es:
nombreusuario: contraseña_cifrada:UID:GID:directorio personal:login_shell

Las contraseñas se guardan utilizando un hash de un sólo sentido (el hash utilizado por defecto es crypt, las distribuciones más nuevas soportan MD5, que es significativamente más robusto). Las contraseñas no pueden obtenerse a partir de la forma cifrada, sin embargo, se puede tratar de encontrar una contraseña utilizando fuerza bruta para pasar por el hash cadenas de texto y compararlas, una vez que el software encuentre una que coincide, se sabe que se ha conseguido la contraseña. Esto no suele ser un problema por sí mismo, el problema surge cuando los usuarios escogen claves que son fácilmente adivinables. Las encuestas más recientes han demostrado que el 25% de las contraseñas se pueden romper en menos de una hora, y lo que es peor es que el 4% de los usuarios utilizan su propio nombre como contraseña. Los campos en blanco en el campo de la contraseña se quedan vacíos, así que se vería "::", lo cual es algo crítico para los cuatro primeros campos (nombre, contraseña, uid y gid). Al tener los campos en blanco simplemente basta con logearse con el nombre de usuario que aparece en el archivo y presionar enter cuando el sistema pida la clave.

/etc/shadow

El archivo de shadow alberga pares de nombres de usuario y contraseñas, la fecha de expiración, y otros campos especiales. Este archivo debería protegerse a toda costa, y sólo el root debería tener acceso de lectura a él. Dado el caso que este archivo llegue a las manos de un hacker solo será cuestión de tiempo para que por fuerza bruta, este individuo tenga acceso a todo el sistema.

/etc/groups

El archivo de grupos contiene toda la información de pertenencia a grupos, y opcionalmente elementos como la contraseña del grupo (generalmente almacenado en gshadow en los sistemas actuales), este archivo debe ser legible por el mundo para que el sistema funcione correctamente. El formato es:

nombregrupo: contraseña_cifrada:GID:miembro1,miembro2,miembro3

Un grupo puede no contener miembros (p. ej., no está usado), sólo un miembro o múltiples miembros, y la contraseña es opcional (y no se suele usar).

/etc/gshadow

Similar al archivo shadow de contraseñas, este archivo contiene los grupos, contraseñas y miembros. De nuevo, este archivo debería ser protegido a toda costa, y sólo el usuario root debería tener permiso de lectura al mismo.

/etc/login.defs

Este archivo (/etc/login.defs) le permite definir algunos valores por defecto para diferentes programas como useradd y expiración de contraseñas. Tiende a variar ligeramente entre distribuciones e incluso entre versiones, pero suele estar bien comentado y tiende a contener los valores por defecto.

/etc/shells

El archivo de shells contiene una lista de shells válidos, si el shell por defecto de un usuario no aparece listado aquí, quizás no pueda hacer login interactivamente.

/etc/securetty

Este archivo contiene una lista de tty’s desde los que el root puede hacer un login. Los tty’s de la consola comúnmente van de /dev/tty1 a /dev/tty6. Los puertos serie

(pongamos que quiere hacer login como root desde módem) son /dev/ttyS0 y superiores por lo general. Si quiere permitirle al root hacer login vía red utilice conexiones ssh. Entonces añada /dev/ttyp1 y superiores (si hay 30 usuarios conectados y el root intenta conectar, el root aparecerá como procedente de /dev/ttyp31). Generalmente, sólo se debería permitir conectar al root desde /dev/tty1, y es aconsejable deshabilitar la cuenta de root, sin embargo antes de hacer esto, por favor, instale sudo o un programa que permita al root acceder a comandos.

PAM "Pluggable Authentication Modules" para Linux, es una suite de librerías compartidas que permiten al administrador local del sistema escoger cómo autentifican a los usuarios las aplicaciones. ¿Pero qué significa en realidad? Por ejemplo, tomando el programa "login", cuando un usuario se conecta a un tty (vía puerto serie o sobre la red), un programa responde la llamada (getty para líneas en serie, normalmente telnet o ssh para conexiones de red) e inicia el programa "login", y luego pide el típico nombre de usuario, seguido de la contraseña, lo cual se compara con el archivo /etc/passwd. Todo esto está bien y es muy bueno, hasta que se tiene una fenomenal tarjeta de autentificación nueva y se quiere utilizar. Bueno, pues tendrá que recompilar login (y cualquier otra aplicación que vaya a hacer la autentificación según el nuevo método) de modo que soporten el sistema nuevo. Como se puede imaginar, esto lleva bastante trabajo y está sujeto a errores.

PAM introduce una capa de middleware entre la aplicación y el mecanismo real de autentificación. Una vez que el programa está PAMificado, podrá ser utilizado por el programa cualquier método de autentificación que soporte PAM. Además de esto, PAM puede manejar cuentas y datos de sesiones, lo cual no suelen hacer

bien los mecanismos habituales de autentificación. Por ejemplo, usando PAM se puede deshabilitar con facilidad el acceso de login a los usuarios normales entre las 6pm y las 6am, y cuando hagan login, se les puede autentificar vía scanner retinal. Por defecto, los sistemas Red Hat son conscientes de PAM, y las versiones más recientes de Debian también. De esta forma, en un sistema con soporte PAM, todo lo que se debe hacer para implementar el shadow en contraseñas es convertir los archivos de contraseñas y de grupos, y posiblemente añadir una o dos líneas a algunos archivos de configuración de PAM (si no las tienen ya añadidas). En resumen, PAM proporciona una gran cantidad de flexibilidad al manejar la autentificación de usuarios, y soportará otras características en el futuro, como firmas digitales, con el único requerimiento de uno o dos módulos PAM para manejarlo. Es necesario este tipo de flexibilidad si se pretende que Linux sea un sistema operativo de tipo empresarial. Las distribuciones que no vengan como "PAMificadas" se pueden convertir, pero requiere mucho esfuerzo (tiene que recompilar todos los programas con soporte PAM, instalar PAM, etc), probablemente sea más fácil cambiarse a una distribución PAMificada si va a suponer un requisito.

Otros beneficios de un sistema orientado a PAM es que ahora se puede hacer uso de un dominio NT para autentificar usuarios, lo cual quiere decir que se pueden plantar estaciones Linux en una red Microsoft ya existente sin tener que comprar NIS / NIS+ para NT y pasar por el calvario de instalarlo.

Distribución	Versión	Soporte PAM
Red Hat	5.0, 5.1, 5.2, 6.0	Completamente
Debian	2.1	Sí
Caldera	1.3, 2.2	Completamente
TurboLinux	3.6	Completamente

Acceso Físico Alguien apaga el servidor principal de contabilidad, lo vuelve a encender, arranca desde un disquete especial y transfiere el archivo pagas.db a un ftp en el extranjero. A menos que el servidor de contabilidad esté bloqueado, ¿qué le impide a un usuario malintencionado (o al personal de limpieza del edificio, el chico de los recados, etc.) hacer tal cosa? Algunos relatos recibidos durante el transcurso de esta investigación pueden causar terror acerca de personal de limpieza desenchufando los servidores para poder enchufar sus aparatos de limpieza. Algunas veces la gente pulsa por accidente el pequeño botón de reset y reiniciaban los servidores. Tiene sentido bloquear los servidores en una habitación segura (o incluso en un armario). También es una buena idea situar a los servidores en una superficie elevada, para evitar daños en el caso de inundaciones (ya sea por un agujero en el techo o lo que sea).

La BIOS del computador La BIOS del computador es uno de sus componentes de más bajo nivel, controla la forma en que el computador arranca y otro tipo de cosas. Las BIOS viejas tienen fama de tener claves universales, asegúrese de que su bios es reciente y que no contiene semejante puerta trasera. La bios se puede utilizar para bloquear la secuencia de arranque de un equipo, limitándola a C: únicamente, por ejemplo, al primer disco duro, lo cual es una buena idea. Debería utilizar la bios para eliminar la unidad de diskette (el servidor típico no va a necesitar utilizarla), y puede evitar que los usuarios copien datos de la máquina a disquetes. También puede eliminar los puertos serie en las máquinas de los usuarios, de tal forma que puedan instalar módems, la mayoría de los computadores modernos utilizan teclados y ratones PS/2, así que quedan pocas razones por las que podría necesitarse un puerto serie (además de

que se comen IRQ's). Lo mismo sirve para el puerto paralelo, permitiendo a los usuarios imprimir obviando la red, o dándoles la oportunidad de instalar una grabadora de CDROM o un disco duro externo, lo cual puede disminuir la seguridad en buena medida. Como se puede ver, esto es un añadido a la política del menor privilegio, y puede disminuir considerablemente los riesgos, al igual que facilitar la administración de la red (menos conflictos de IRQs, etc.) Por supuesto que existen programas para obtener las contraseñas de la BIOS de un computador, hay uno disponible en http://www.esiea.fr/public_html/Christophe.GRENIER/, y está disponible para DOS y Linux.

LILO

Una vez que el computador ha decidido arrancar de C:, LILO (o cualquier otro gestor de arranque que utilice) despega. La mayoría de los gestores de arranque permiten algún tipo de flexibilidad en el modo en que se arranca el sistema, especialmente LILO, pero también es una espada de dos filos. Puede pasarle argumentos a LILO a la hora de arrancar, siendo el argumento más dañino (desde el punto de vista de la seguridad) "imagename single", lo cual arranca Linux en modo de único usuario, y por defecto, la mayoría de las distribuciones le vuelcan a un prompt de root en un shell de comandos sin preguntar contraseñas u otro tipo de mecanismos de seguridad. Hay varias técnicas para minimizar este riesgo.

delay=x

Esto controla la cantidad de tiempo (en décimas de segundo) que LILO espera a que el usuario introduzca datos antes de arrancar la opción por defecto. Uno de los requerimientos de la seguridad de nivel C2 es que este intervalo sea puesto a 0 (obviamente, cualquier máquina con arranque dual acaba con cualquier tipo de

seguridad). Es una buena idea poner esto a 0, a menos que el sistema arranque dualmente es decir con dos sistemas operativos.

prompt

Fuerza al usuario a introducir algo, LILO no arrancará el sistema automáticamente. Esto podría ser útil en servidores, como una forma de eliminar los reinicios sin que esté presente una persona, pero lo típico es que si el hacker tiene capacidad para reiniciar la máquina, podría reescribir el MBR con nuevas opciones de arranque. Si le añade una opción de cuenta atrás, el sistema continuará arrancando después de que haya terminado la cuenta atrás.

restricted

Pide una contraseña si se pasan opciones de tiempo de arranque (tales como "linux single"). Asegúrese de que utiliza esto en cada imagen (si no, el servidor necesitará una contraseña para arrancar, lo cual está bien si no planea arrancarlos remotamente nunca).

Esto reinicia el sistema utilizando el kernel /boot/vmlinuz-2.2.5, almacenado en el MBR del primer disco IDE del sistema, el prompt impediría hacer reinicios desatendidos, sin embargo está implícito en la imagen, de modo que puede arrancar "linux" sin problemas, pero pediría una contraseña si introduce "linux single", de modo que si quiere ir al modo "linux single", tiene 10 segundos para escribirlo, en cuyo punto le preguntaría por la contraseña ("aqu1_va_la_c0ntRaSeña"). Combine esto con una BIOS configurada para arrancar sólo desde C: y protegida con contraseña y ha conseguido un sistema bastante seguro para controlar el acceso al sistema (A no ser que el intruso pueda destapar la maquina y mover los Jumpers de la misma). Una medida menor de seguridad que puede tomar para asegurar el archivo lilo.conf es dejarlo invariable, utilizando el comando "chattr". Para hacer el archivo invariable, simplemente teclee:

chattr +i /sbin/lilo.conf

y esto evitará cualquier cambio (accidental o de otro tipo) en el archivo lilo.conf. Si quiere modificar el archivo lilo.conf necesitará quitar el flag de invariable:
chattr -i /sbin/lilo.conf

sólo el root tiene acceso al flag de invariable.

CONTRASEÑAS

Administración de contraseñas

En todo sistema operativo tipo UNIX se dan varias constantes, y una de ellas es el archivo /etc/passwd y la forma en que funciona. Para que la autentificación de usuario funcione correctamente se necesitan (como mínimo) algún tipo de archivo(s) con UID a mapas de nombres de usuarios, GID a mapas de nombres de grupos, contraseñas para todos los usuarios y demás información variada. El problema es que todo el mundo necesita acceso al archivo de contraseñas, cada vez que se hace un ls, se verifica el archivo de contraseñas, de modo que ¿cómo se consigue almacenar todas las contraseñas con seguridad y a la vez mantenerlas legibles por el mundo? Durante muchos años, la solución ha sido bastante simple y efectiva, simplemente, haga un hash de las contraseñas y guarde el hash, cuando un usuario necesite autentificar, tome la contraseña que introduce, pásela por el hash y si coincide, evidentemente se trataba de la misma contraseña. El problema que tiene esto es que la potencia computacional ha crecido enormemente, y ahora se puede coger una copia del archivo de contraseñas e intentar abrirlo mediante fuerza bruta en una cantidad de tiempo razonable. Para resolver esto hay varias soluciones:

Utilice un algoritmo de hashing "mejor", como MD5. Problema: se pueden romper muchas cosas si está esperando algo más.

Almacene las contraseñas en alguna otra parte. Problema: el sistema/usuarios siguen necesitando tener acceso a ellas, y podría hacer que fallasen algunos programas si no están configurados de esta forma.

Varios SO's han escogido la primera opción, Linux ha implementado la segunda desde hace tiempo, se llama contraseñas con shadow. En el archivo de contraseñas, se reemplaza la contraseña por una 'x', lo cual le indica al sistema que verifique su contraseña contra el archivo shadow (se hace lo mismo con el archivo de grupos y sus contraseñas). Parece lo suficientemente simple, pero hasta hace bien poco, implementar el shadow era una ardua tarea. Había que recompilar todos los programas que verificasen la contraseña (login, ftpd, etc, etc) y esto, por supuesto, implica una considerable cantidad de esfuerzo. Es aquí donde brilla Red Hat, con su confianza en PAM.
Para implementar contraseñas con shadow hay que hacer dos cosas. La primera es relativamente simple, cambiar el archivo de contraseñas, pero la segunda puede ser un calvario. Hay que asegurarse que todos sus programas tienen soporte para contraseñas con shadow, lo cual puede ser bastante penoso en algunos casos (esta es una más que importante razón por la cual un mayor número de distribuciones deberían venir con PAM).

Debido a la confianza de Red Hat en PAM para la autentificación, para implementar un esquema nuevo de autentificación todo lo que se necesita es añadir un módulo PAM que lo entienda y editar el archivo de configuración para cualquier programa (digamos el login) permitiéndole que use ese módulo para hacer la autentificación. No hace falta recompilar, y hay poco tejemaneje, ¿a que sí? En Red Hat 6.0, durante la instalación se le da la opción de elegir contraseñas con shadow, o puede implementarlas más tarde vía las utilidades pwconv y

grpconv que vienen con el paquete de utilidades shadow. La mayoría del resto de distribuciones también tienen soporte para contraseñas con shadow, y la dificultad de implementación varía de un modo u otro. Ahora, para que un atacante mire las contraseñas con hash, tiene que esforzarse un poco más que simplemente copiar el archivo /etc/passwd. También asegúrese de ejecutar cada cierto tiempo pwconv, para tener la certeza de que todas las contraseñas efectivamente tienen shadow. Hay veces que las contraseñas se quedan en /etc/passwd en lugar de enviarse a /etc/shadow como deberían, lo cual hacen algunas utilidades que editan el archivo de contraseñas.

Violando contraseñas

En Linux las contraseñas se guardan en formato hash, sin embargo ello no las hace irrecuperables, no es posible hacer ingeniería inversa de la contraseña a partir del hash resultante, sin embargo sí que puede hacer un hash de un lista de palabras y compararlas. Si el resultado coincide, entonces ha encontrado la contraseña, es por esto que es crítica la elección de buenas contraseñas, y las palabras sacadas de un diccionario son una idea horrible. Incluso con un archivo de contraseñas con shadow, el root puede acceder a las contraseñas, y si se han escrito scripts o programas que se ejecuten como root (pongamos un script CGI para www) los atacantes pueden recuperar el archivo de contraseñas. La mayoría del software para violar contraseñas también le puede permitir la ejecución en múltiples hosts en paralelo para acelerar las cosas.

John the ripper ("Juan el destripador")

Un eficiente viola-contraseñas disponible en: http://www.false.com/security/john/

Crack

El viola-contraseñas original y ampliamente extendido, lo puede conseguir en: http://www.users.dircon.uk/~crypto/

Saltine cracker

Otro viola-contraseñas con capacidades de red, lo puede descargar de: http://www.thegrid.net/gravitino/products.html

VCU

VCU (Velocity Cracking Utilities) es un programa basado en Windows para ayudar a reventar contraseñas "VCU intenta facilitar la tarea de reventar contraseñas a usuarios de computadores de cualquier nivel". Lo puede descargar desde: http://wilter.com/wf/vcu/

Almacenamiento de Contraseñas

Esto es algo que la mayoría de la gente no suele tener en cuenta. ¿Cómo se pueden almacenar las contraseñas de forma segura? El método más obvio es memorizarlas, pero suele tener sus inconvenientes, si se administran 30 sitios diferentes, por lo general se tendrán 30 contraseñas diferentes, y una buena contraseña tiene más de 8 caracteres de longitud, y por lo general no es la cosa más fácil de recordar. Esto conduce a que mucha gente utilice la misma contraseña en diferentes sistemas. Una de las formas más sencillas es escribir las contraseñas. Por lo general, esto suele ser un grandísimo NO-NO; le sorprendería saber lo que encuentra la gente echando un vistazo, y lo que encuentran si lo están buscando. Una mejor opción es almacenar las contraseñas en un formato cifrado, generalmente de forma electrónica en su computador o en el palm pilot, de forma sólo hay que recordar una contraseña para desbloquear el resto. Para esto se puede utilizar algo tan simple como PGP o GnuPG.

Gpasman

Gpasman es una aplicación que requiere el gtk (es relativamente fácil de instalar en un sistema que no sea Gnome, sólo hay que cargar las librerías gtk). Cifrar sus contraseñas utilizando el algoritmo rc2. Al inicio del programa se introduce la

contraseña maestra, y (suponiendo que es correcta) se presenta una lista de sus cuentas de usuario, sitios, contraseñas y un campo de comentario. Gpasman está disponible en: http://www.student.wau.nl/~olivier/gpasman/

Strip

Strip es un programa de almacenamiento seguro de contraseñas para palm pilot, y también se puede utilizar para generar contraseñas. Tiene licencia GNU y se encuentra disponible en: http://www.zetetic.net/products.html

CONTROL DE ACCESO BASICO A LA RED

Servicios de red

¿Qué se está ejecutando y con quién se está hablando?

No se pueden empezar a asegurar servicios hasta que no se sepa qué se está ejecutando. Para este tipo de tareas, ps y netstat no tienen precio; ps dice qué se está ejecutando (httpd, inetd, etc) y netstat le dirá cuál es el estado de los puertos (llegados a este punto, estamos interesados en los puertos que están abiertos y escuchando, es decir, esperando conexiones). Se les puede echar un vistazo a los diferentes archivos de configuración que controlan los servicios de red.

Salida de PS

El programa ps nos muestra el estado de procesos (información disponible en el sistema de archivos virtual /proc). Las opciones más comúnmente utilizadas son "ps -xau", que muestra algo así como toda la información que siempre quisiste saber. Por favor, tenga en cuenta: estas opciones cambian entre sistemas UNIX, Solaris, SCO, todos se comportan de manera diferente (lo cual es increíblemente molesto). Lo que viene a continuación es una salida típica de una máquina (utilizando "ps -xau").

Los interesantes son: portmap, named, Squid (y su servidor dns, los procesos hijos unlinkd y ftpget), httpd, syslogd, sshd, rpc.mountd, rpc.nfsd, dhcpd, inetd, y sendmail (este servidor parece estar proveyendo servicios de puerta de enlace, correo y compartición de archivos FNS). La forma más fácil de aprender a leer la salida de ps es irse a la página del manual de ps y aprender a qué se refiere cada campo (la mayoría se explican por sí mismos, tales como el %CPU, mientras que algunos como SIZE son un poco más oscuros: SIZE es el número de páginas de memoria de 4k que está utilizando un programa). Para averiguar qué programas se están ejecutando, una apuesta segura es hacer 'man <nombre_de_comando>'; lo cual casi siempre suele sacar la página del manual que pertenece a ese servicio (como httpd). Se dará cuenta de que servicios como telnet, ftpd, identd y otros no aparecen aunque estén ahí. Esto es debido a que se ejecutan desde inetd, el "superservidor". Para encontrar estos servicios, mire en /etc/inetd.conf o en la salida de "netstat -vat".

Salida de Netstat

netstat informa acerca de casi cualquier cosa que se pueda imaginar relacionada con la red. Es especialmente buena para sacar listados de conexiones y sockets activos. Al usar netstat se puede encontrar qué interfaces están activas en qué puertos. Lo que viene a continuación es la salida típica de un servidor, con netstat -an.

Algunas veces la salida numérica es más fácil de leer (una vez que se memoriza /etc/services). Los campos de interés son el primero, el tipo de servicio, el cuarto campo, que es la dirección IP de la interfaz y el puerto, la dirección externa (si no es 0.0.0.0.* significa que alguien le está hablando activamente), y el estado del puerto. La primera línea es un cliente remoto hablando con el servidor de Web de esta máquina (puerto 80). Cuando se ve el servidor www escuchando en 0.0.0.0:80 que significa, todos los interfaces, puerto 80, seguidos del servidor DNS ejecutándose en las 3 interfaces, un servidor samba (139), un servidor de correo

(25), un servidor NFS (2049), etc. Observará listado el servidor de ftp (21), que aunque se ejecuta desde inetd, y aunque actualmente no está en uso (p. ej., no hay nadie activo haciendo un ftp), sale en el listado de la salida de netstat. Lo cual convierte a netstat en una herramienta especialmente útil para averiguar qué es lo que está activo en una máquina, haciendo más sencillo el inventariado en el servidor del software activo e inactivo.

lsof

lsof es un práctico programa cuya idea es similar a la de ps, excepto en que muestra qué archivos /etc están abiertos, lo cual puede incluir sockets de red. Desafortunadamente, el lsof medio saca bastante información, de modo que será necesario utilizar grep o redireccionarlo mediante less ("lsof | less") para hacerlo más cómodo de leer.

squid 9726 root 4u inet 78774 TCP localhost:2074->localhost:2073 (ESTABLISHED)
squid 9726 root 5u inet 78777 TCP localhost:2076->localhost:2075 (ESTABLISHED)
squid 9726 root 6u inet 78780 TCP localhost:2078->localhost:2077 (ESTABLISHED)
squid 9726 root 7w CHR 1,3 6205 /dev/null
squid 9726 root 14u inet 78789 TCP host1:3128 (LISTEN)
squid 9726 root 15u inet 78790 UDP host1:3130
squid 9726 root 16u inet 78791 UDP host1:3130
squid 9726 root 12u inet 167524 TCP host1:3128->host2:3630 (ESTABLISHED)
squid 9726 root 17u inet 167528 TCP host1:3424->www.ejemplo.org:http (SYN_SENT)

Este ejemplo muestra que se tiene ejecutándose a Squid, escuchando en los puertos 3128 y 3130, las últimas dos líneas muestran una conexión abierta desde

un host interno al servidor de Squid y la acción resultante que ha emprendido Squid para cumplir con la solicitud (ir a www.playboy.com) host1 es el servidor de Squid y host2 es la máquina cliente haciendo la petición. Es una herramienta que no tiene precio para hacerse una idea exacta de qué es lo que está ocurriendo con el servidor en la red. Se puede conseguir lsof con algunas distribuciones. Tenga en cuenta que las versiones de losf compiladas para las versiones del kernel 2.0.x no funcionarán con el kernel 2.2.x y vice versa, pues hay bastantes cambios. El sitio primario de lsof es:
ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/

Archivos básicos de configuración de red

Hay varios archivos de configuración importantes, que controlan qué servicios ejecuta Linux y cómo lo hacen. Por desgracia, muchos de ellos se encuentran en diferentes localizaciones dependiendo de qué/cómo instalara Linux y los servicios.

Los lugares habituales son:
Archivo de configuración del servidor Inetd:
/etc/inetd.conf
Archivos de inicio de varios tipos:
/etc/rc.d/*
/etc/*

Lo mejor que se puede hacer es imaginarse qué servicios se quiere ejecutar, y deshabilitar/borrar el resto. Échele un vistazo a la sección apropiada de gestión de paquetes de su sistema (RPM, dpkg, tarballs)
inetd.conf
inetd.conf es el responsable de iniciar los servicios, generalmente aquellos que no necesitan ejecutarse de continuo, o que están basados en sesiones (como telnet o ftpd). Ello es debido a que la sobrecarga que supondría ejecutar un servicio

constantemente (como telnet) sería mayor que el costo de inicio ocasional (o que arrancar in.telnetd) cuando el usuario quisiera utilizarlo. Para algunos servicios (como DNS) que sirven a muchas conexiones rápidas, la sobrecarga de arrancar servicios cada pocos segundos sería mayor que tenerlo constantemente ejecutándose. De igual forma ocurre con servicios como DNS y el correo, donde el tiempo es crítico, sin embargo unos pocos segundos de retraso en empezar una sesión de ftp no le hacen daño a nadie. La página del manual de inetd.conf cubre los básicos ("man inetd.conf"). El servicio en sí se llama inetd y se ejecuta al arrancar, de modo que se le puede parar/arrancar/recargar manipulando el proceso inetd. Cada vez que se hagan cambios a inetd.con, hay que reiniciar inetd para hacer efectivos los cambios, killall –1 inetd lo reiniciará correctamente. Como de costumbre, las líneas del inetd.conf se pueden comentar con un # (lo cual es una forma muy simple y efectiva de deshabilitar servicios como rexec). Se aconseja deshabilitar tantos servicios de inetd.conf como sea posible, por lo general los que se suelen usar son ftp, pop e imap. Se debería reemplazar telnet y los servicios r por el SSH y servicios como systat/netstat y finger proporcionan demasiada información. El acceso a programas arrancados por inetd se puede controlar con facilidad mediante el uso de TCP_WRAPPERS.

Seguridad PPP

PPP permite conexiones TCP-IP, IPX/SPX y NetBEUI sobre líneas serie (las cuales pueden estar conectadas a módems, por supuesto). Este es el método principal que utiliza la gente para conectarse a Internet (prácticamente todas las cuentas de dial-up son PPP). La esencia de una conexión PPP consiste en dos dispositivos informáticos (un computador, un Palm Pilot, un servidor de terminales, etc.) conectados sobre enlaces de serie (generalmente vía módems). Ambos extremos llaman al PPP, se negocia la autentificación (mediante uno de entre varios métodos), y se establece el enlace. PPP no tiene soporte real para cifrado,

de modo que si se necesita un enlace seguro hay que invertir en algún tipo de software VPN.

La mayoría de los sistemas llaman a PPP de una forma bastante cutre, se hace un login al equipo (servidor de terminales, etc.) y luego se invoca al login shell del PPP. Por supuesto que esto significa que el nombre de usuario y contraseña se envían en texto claro sobre la línea, y que hay que tener una cuenta en ese tipo de equipo. En este caso el PPP no negocia la autentificación en absoluto. Un método algo más seguro de gestionarlo es utilizar PAP (Password Authentification Protocol, Protocolo de Autentificación de Contraseñas). Mediante PAP, la autentificación se hace internamente mediante PPP, de modo que no se requiere una cuenta "real" en el servidor. Sin embargo el nombre de usuario y la contraseña se siguen enviando en texto claro, pero al menos el sistema es algo más seguro dada la inexistencia de cuentas de usuario "reales".

El tercer (y mejor) método para la autentificación es utilizar CHAP (Challenge Handshake Authentication Protocol, Protocolo de Autentificación Desafío-Respuesta). Ambas partes se intercambian llaves públicas y las utilizan para cifrar los datos que se envían durante la secuencia de autentificación. De modo que el nombre de usuario y la contraseña están relativamente a salvo de fisgones, y sin embargo las transmisiones de datos se hacen con normalidad. Una advertencia con CHAP: La implementación de Microsoft utiliza DES en lugar de MD5, lo cual lo hace fallar si se conecta con un cliente Linux. Sin embargo existen parches para arreglarlo. PPP viene con cada distribución de Linux como parte del núcleo del SO.

Seguridad IP (IPSec)

Seguridad IP (IPSec) es el cifrado del tráfico de red. No se puede cifrar la información de la cabecera ni el trailer (p. ej. la dirección IP y puerto de donde

viene el paquete y su destino, los checksums de CRC, etc.), pero se puede cifrar la carga útil. Esto permite asegurar protocolos como POP/WWW sin tener que cambiarlos de ninguna forma, puesto que el cifrado se hace en el nivel IP. También permite conectar de forma segura LANs y clientes entre sí, sobre redes inseguras (como Internet). En la actualidad, IPSec para Linux está en fase de pruebas, sin embargo ya se han lanzado varias versiones estables. IPSec es un standard, y parte el protocolo IPv6, de modo que ya se puede comprar software IPSec para Windows 95/98/NT, Solaris y otros Unix, que interoperarán con Linux IPSec.

Soporte IPSec del kernel

Para utilizar IPSec es necesario tener soporte IPSec en el kernel. Desafortunadamente, ninguna distribución Americana de Linux puede exportar criptografía robusta fuera de Norte América, de modo que en general, suelen escoger no incluirla en absoluto, de las distribuciones extranjeras de Linux, en la actualidad ninguna viene con soporte IPSec dentro del kernel.

Es necesario conseguir el código fuente del kernel, disponible en:

http://www.xs4all.nl/~freeswan/

Instale el fuente del kernel (generalmente en /usr/src/linux) y compile el nuevo kernel, instálalo, arránquelo y pruébelo. Asegúrese de que sus redes funcionan correctamente, si no funcionan, hacer que lo haga IPSec será imposible. Ahora hay que descargar la última instantánea de IPSec (la versión 1.0 NO funcionará con los kernels 2.2.x). Después ir a /usr/local/src (o dondequiera que haya puesto el código fuente de sus programas), desempaquetar el fuente y ejecutar el programa de instalación (make menugo suele ser lo habitual para la configuración basada en ncurses). Lo cual parcheará los archivos del kernel, luego ejecute la configuración del kernel y después construya las herramientas IPSec y el kernel.

cd /usr/local/src/

tar –zvvxf /path/del/tarball/snapshot.tar.gz

chown –R root:root freeswan-snap1999Jun14b

cd freeswan-snap1999Jun14b
make menugo
asegúrese de guardar la configuración del kernel, incluso aunque se hayan elegido las opciones, no han sido guardadas. También tendrá que reconstruir el kernel, puesto que el comando "make menugo" ejecuta un "make zImage", lo cual suele fallar, debido a los grandes tamaños del kernel de la 2.2.x. Una vez que se ha hecho la compilación, debería dar uno o dos mensajes de error, simplemente haga:
cd /usr/src/linux
make bzImage
cp /usr/src/linux/arch/i386/boot/bzImage /boot/vmlinuz-2.2.10-ipsec

Ahora hay que editar lilo.conf, ejecutar lilo de nuevo y reiniciar para hacer uso del nuevo kernel.

Después reinicie y debería estar ejecutando el kernel 2.2.10 con soporte IPSec. A medida que la máquina se reinicia y empieza el IPSec se verán varios errores, por defecto IPSec está configurado para utilizar el interfaz eth999, el cual por supuesto no existe. Deberá añadir /usr/local/lib/ipsec en la frase del path o si no tendría que escribir el path completo un montón.

Configuración de redes IPSec

Tendrá que habilitar el TCP-IP forwarding en el servidor de enlace, en Red Hat Linux se hace cambiando la línea de /etc/sysconfig/network:
FORWARD_IPV4="false"
por:
FORWARD_IPV4="yes"
se puede habilitar vía sistema de archivos en /proc:
cat 1 > /proc/sys/net/ipv4/ip_forward

Puesto que la mayoría de la gente tiene por defecto políticas de denegación de paquetes de forwarding, tendrá que permitir que los paquetes atraviesen la rede remota / máquina de su red / máquina y vice versa. Además de esto, cualquier regla de enmascaramiento para redes internas que también estén usando IPSec debe venir después de las reglas que permiten el tráfico IPSec, o la máquina intentará enmascarar los paquetes, en lugar de pasarlos al IPSec.

El siguiente ejemplo es para dos redes protegidas (usando direcciones IP no rutables, escondidas tras máquinas Linux haciendo enmascaramiento de IPs) conectadas vía Internet:

Conexión manual de llaves

Primero es necesario configurar un enlace utilizando la conexión manual de llaves (por simplicidad), hay que editar ipsec.conf, y las reglas del cortafuegos. La mayoría de las opciones por defecto del archivo ipsec.conf son correctas, pero hay que cambiar lo siguiente:

SSL y HTTP – SSL

El servidor www más habitual, Apache, tiene bastante buen soporte SSL, el cual se puede descargar gratuitamente fuera de los EE.UU. (las patentes de los EE.UU. sobre RSA/etc significan tener que pagar derechos dentro de los EE.UU, de modo que el software gratuito es ilegal) desde http://www.Apache-ssl.org/. Hay muchos servidores comerciales de www que soportan SSL, la mayoría de los cuales están basados en Apache, como el Servidor Seguro de Red Hat, Stronghold, etc.

Telnet – SSL

Para reemplazar al telnet, SSLtelnet y MZtelnet proporcionan un nivel de seguridad mucho más alto que el telnet original, aunque el SSLtelnet y el MZtelnet

no son tan flexibles como el SSH, son perfectamente libres (es decir, con licencia GNU) lo cual el SSL no lo es. Los paquetes cliente y servidor se encuentran disponibles como tarballs en: ftp://ftp.uni-mainz.de/pub/internet/security/ssl/, y como paquetes RPM en:
ftp://ftp.replay.com/pub/replay/linux/Red Hat/.

FTP – SSL

También existe un reemplazo para el ftpd (probablemente el WU-FTPD), también disponible como un conjunto de parches al WU-FTPD. Es altamente apropiado, pues la mayoría de los servidores tienen muchos usuarios que necesitan acceso ftp. El tarball se encuentra en: ftp://ftp.uni-mainz.de/pub/internet/security/ssl/, y los paquetes RPM están en: ftp://ftp.replay.com/pub/replay/linux/Red Hat/.

ADMINISTRACIÓN DEL SISTEMA
Herramientas administrativas
Acceso Remoto

Telnet

Telnet es con mucho la herramienta remota más vieja y conocida, prácticamente cualquier Unix viene con ella, incluso lo soportan sistemas como NT. Telnet sólo tiene uso cuando pueda administrar el sistema desde modo comandos (algo para lo que NT no es tan bueno), lo cual lo convierte en perfecto para sistemas Unix. Telnet es increíblemente inseguro, las contraseñas y los nombres de usuarios, al igual que los datos de las sesiones vuelan en texto simple, siendo el objetivo preferido de los sniffers. Telnet viene con todas las distribuciones de Linux. No debería utilizar nunca el telnet de fábrica para administrar remotamente un sistema.

SSL Telnet

SSL Telnet es telnet con el añadido de cifrado SSL, lo cual lo hace bastante más seguro. Usando certificados X.509 (también conocidos como certificados personales) se pueden administrar sistemas con facilidad. Al contrario de sistemas como el SSH, SSL Telnet es completamente GNU y gratis para cualquier uso. Puede encontrar el servidor Telnet SSL en ftp://ftp.replay.com

SSH

SSH era gratis al principio, pero ahora está bajo licencia comercial, sin embargo tiene numerosas características que lo hacen merecer la pena. Soporta diferentes tipos de autentificación (contraseña, basada en rhosts, llaves RSA), permite redireccionar puertos, y se puede configurar fácilmente a qué usuarios se les permite usarlo. SSH está disponible en ftp://ftp.replay.com. Si va a utilizarlo para uso comercial, o si quiere la última versión, diríjase a http://www.ssh.fi/

LSH

LSH es una implementación gratuita del protocolo SSH, LSH tiene licencia GNU y está empezando a perfilarse como la alternativa (comercialmente hablando) a SSH (que ya no es gratis). Lo puede descargar de http://www.net.lut.ac.uk/psst/, pero tenga en cuenta que está bajo desarrollo.

REXEC

REXEC es una de las utilidades UNIX más antiguas, le permite ejecutar comandos en un sistema remoto, aunque tiene el serio fallo de no tener un modelo de control de acceso real. El control de acceso se consigue mediante el uso de archivos ‘rhosts’, que especifican qué hosts/etc. pueden ejecutar comandos, lo cual está sujeto a spoofing y otro tipo de exploits. Jamás debería utilizar el REXEC standard para administrar un sistema.

Slush

Slush está basado en OpenSSL, y actualmente soporta certificados X.509, lo cual, para grandes organizaciones, es una apuesta mucho mejor (y más sana) que intentar recordar varias docenas de contraseñas en diferentes servidores. Slush es GPL, pero todavía no está terminado (implementa la mayoría de la funcionalidad que se requiere para ser utilizable, pero tiene límites). Por otra parte, está completamente basado en software de código abierto, dejando pocas posibilidades a que pueda tener puertas traseras/etc. En último caso, podría reemplazar al SSH por algo mejor. Lo puede conseguir en http://violet.ibs.com.au/slush/.

NSH

NSH es un producto comercial con todos sus detalles. Tiene soporte para cifrado, de modo que es relativamente seguro de usar (esto no se puede verificar completamente, ya que no es código abierto). Es de una gran facilidad de uso, hace un cd //nombredecomputador y con eso ya hace el log en ese computador, puedes copiar/modificar/etc archivos con facilidad, ejecutar ps y ver la lista de procesos de ese computador, etc. NSH también dispone de un módulo Perl, lo cual hace sencilla la redacción de scripts de comandos, y es ideal para administrar muchos sistemas similares (como estaciones de trabajo). Además de eso, NSH está disponible en múltiples plataformas (Linux, BSD, Irix, etc.) con RPM's disponibles para sistemas Red Hat. NSH está disponible en: http://www.networkshell.com/, y se pueden descargar versiones de evaluación de 30 días.

Fsh

Fsh significa "Ejecución rápida de comandos remotos", y el concepto es similar al de rsh/rcp. Evita el costo de estar creando continuamente sesiones cifradas,

habilitando un túnel cifrado utilizando ssh o lsh, y ejecutando todos los comandos sobre él. Lo puede conseguir en: http://www.lysator.liu.se/fsh/.

secsh

secsh (Shell Seguro) aporta otra capa más de seguridad de login, una vez que ha hecho log vía ssh o telnet SSL le pide otra contraseña, si introduce una errónea, secsh mata el intento de login. Se puede conseguir en:
http://www.leenux.com/scripts.

Acceso Local

YaST

YaST (Yet Another Setup Tool, "otra herramienta más de seguridad") es un comando gráfico de líneas bastante interesante, (muy similar a scoadmin) que aporta una sencilla interfaz para la mayoría de las tareas administrativas. Sin embargo, no está pensado para limitar accesos a usuarios, así que sólo es útil para depurar errores y para permitir administrar su sistema a nuevos usuarios. Otro problema es que al contrario que Linuxconf, no está orientado a redes, lo cual quiere decir que hay que hacer un log en cada sistema que quiera manipular.

sudo

Sudo le da a un usuario acceso setuid a un programa(s), se le puede especificar desde qué host(s) se les permite (o no) hacer login y tener acceso sudo (de modo que si alguien vulnera una cuenta pero está bloqueado, se minimizan los daños). Se puede especificar bajo qué usuario se ejecutará un comando, lo cual le da un grado de control relativamente preciso. Si tiene que dar acceso a los usuarios, asegúrese de especificar los hosts desde los que les está permitido hacer un login

cuando estén utilizando sudo, de igual forma, de la ruta completa a los binarios, lo cual le evitará problemas a la larga (p. ej. si le da acceso a "adduser" a un usuario, no hay nada que le impida editar su path y copiar bash a /tmp/adduser obteniendo el control de la máquina). Esta herramienta es muy similar a super pero con un control ligeramente inferior. Sudo está disponible para la mayoría de las distribuciones, como paquete interno, o paquete contribuido. Sudo está disponible en: http://www.courtesan.com/sudo/ , por si su distribución no viene con él.

Sudo le permite definir grupos de hosts, grupos de comandos, y grupos de usuarios, haciendo la administración más sencilla, a largo plazo. Aquí van varios ejemplos de /etc/sudoers :
Dar acceso total al usuario ‘seifried’
seifried ALL=(ALL) ALL

Crear un grupo de usuarios, un grupo de hosts, y permitirles apagar el servidor como root
host_alias WORKSTATIONS=localhost, estacion1, estacion2
User_alias SHUTDOWNUSERS=rober, maria, juana
Cmnd_Alias REBOOT=halt, reboot, sync
Runas_Alias REBOOTUSER=admin
SHUTDOWNUSERS WORKSTATIONS=(REBOOTUSER) REBOOT

Super

Super es una de las pocas herramientas que se pueden utilizar hoy en día para dar a ciertos usuarios (y grupos) diferentes niveles de acceso a la administración del sistema. Además, se pueden especificar horas y permitir el acceso a scripts, puesto que dar acceso setuid, incluso a comandos comunes, puede tener resultados inesperados (cualquier editor, cualquier herramienta de manipulación de archivos como chown, chmod, incluso herramientas como lp podrían comprometer partes del sistema). Debian viene con super, y existen rpm’s

disponibles en el directorio contrib. Es una herramienta potente, pero necesita una sustancial cantidad de esfuerzo para implementarse correctamente (como cualquier herramienta potente). Suele haber ejemplos de archivos de configuración en el directorio /usr/doc/super-xxxx/. El sitio principal de distribución de super es: ftp://ftp.ucolick.org/pub/users/will/ .

runas

runas es muy parecido a sudo y Super, con algunas variaciones. Se crea un archivo de configuración listando el comando, como quien se ejecuta, y a qué usuarios/grupos/etc. se les permite ejecutarlo como tal. Además de esto, se pueden restringir el uso de opciones (argumentos), y se le puede solicitar al usuario el motivo (lo cual queda registrado con syslog). Esta es una muy buena característica, ya que con un poco de entrenamiento, se puede conseguir que el staff de administración documente lo que está haciendo de forma liviana (p. ej. "quería reiniciar el sistema debido a fugas de memoria"). Runas se puede descargar de:
http://www.mindspring.com/~carpinello/runas/index.html.

Accesos Remotos basados en WWW

Webmin

Webmin es (actualmente), una herramienta de administración no comercial. Es un conjunto de scripts de perl con un servidor www autocontenido al cual se accede utilizando un visor de www. Tiene módulos para la mayoría de las funciones de administración del sistema, aunque algunas son un poco temperamentales. Una de sus características de mis preferidas es el hecho de que mantiene su propio usuario y contraseña para acceder a webmin, y se puede personalizar a qué tiene acceso cada usuario (p. ej. usuario1 sólo puede administrar usuarios, usuario2

sólo puede reiniciar la máquina y usuario3 puede modificar la configuración del Apache). Webmin está disponible en: http://www.webmin.com/.

Linuxconf

Linuxconf es una herramienta de administración Linux de propósito general, que se puede utilizar desde la línea de comandos, desde X, o vía su propio servidor www. Es una herramienta muy recomendada para la administración automatizada del sistema, ya que es relativamente ligera desde la línea de comandos (en realidad está dividida en varios módulos). Desde X proporciona un vistazo general de todo aquello que puede configurarse (PPP, usuarios, discos, etc.). Para utilizarlo vía visor www, primero hay que ejecutar Linuxconf en la máquina y añadir el o los hosts o red(es) a las que quiere permitir conectarse (Conf> Misc> Linuxconf network access), salvar los cambios y salir. Luego, cuando se conecte a la máquina (por defecto Linuxconf sólo acepta root como la cuenta, y Linuxconf no soporta ningún tipo de cifrado (se ejecuta independientemente en el puerto 901), de modo que desaconsejaría con vehemencia la utilización de esta característica entre redes, a menos que se tenga IPSec o algún otro tipo de nivel de seguridad IP. Linuxconf viene con Red Hat Linux y está disponible en: http://www.solucorp.qc.ca/linuxconf/. Linuxconf no parece que venga con páginas de manual/etc., la ayuda está contenida internamente.

COAS

El proyecto COAS (Caldera Open Administration System) es un proyecto muy ambicioso para proporcionar un marco abierto de administración de sistemas, desde línea de comandos (con interfaz semi-gráfico), desde X (utilizando el componente qt) hasta el web. Hace una abstracción de los datos reales de configuración aportando una capa intermedia, permitiendo de esta forma su uso en variadas plataformas Linux. Acaba de salir la versión 1.0, parece que

finalmente Caldera va adelante con ello. El sitio de COAS está en: http://www.coas.org.

Otras herramientas basadas en red

VNC

El Virtual Network Computer (VNC) es parecido a X o a PCAnywhere. Se puede mostrar un escritorio gráfico, y controlarlo remotamente, con NT o Linux como servidor y/o cliente. El VNC es bastante bueno a través de una Ethernet de 10 megabit, sin embargo tiende a utilizar un montón de potencia computacional relativamente comparado con otros métodos de administración remota. Se puede conseguir en:
http://www.uk.research.att.com/vnc/. La seguridad del VNC no es tan buena, pero hay varios sitios con información acerca de asegurar VNC, utilizando SSL, SSH y otros métodos. MindVNC es un cliente java que utiliza SSH, disponible en:

http://www.mindbright.com/english/technology/products/mindvnc.html.
Existe un parche disponible para añadir cifrado al VNC en:
http://web.mit.edu/thouis/vnc/.

Gestión de Software

RPM

RPM es una herramienta de gestión de software creada originalmente por Red Hat, y más tarde hecha GNU y puesta a disposición del público (http://www.rpm.org/). Forma parte del corazón de la administración en la mayoría de sistemas, ya que una de las tareas más importantes de cualquier administrador es la instalación y mantenimiento de software actualizado. Varias estimaciones

otorgan la mayor parte de la culpa de los incidentes de seguridad a las malas contraseñas, y al software viejo con vulnerabilidades conocidas. Lo cual no es tan sorprendente como uno podría pensar, pero mientras que el servidor medio contenga entre 200 y 400 paquetes de software de media, uno empieza e ver por qué mantener el software actualizado puede ser una tarea importante.

Las bases de RPM son autoexplicativas, los paquetes vienen en formato rpm, con una simple convención de nombre de archivo:
nombre_paquete-versión_paquete-rpm_versión_construcción-arquitectura.rpm

servidor-nfs-2.2beta29-5.i386.rpm sería "servidor-nfs", versión "2.2beta29" del "servidor-nfs", la quinta construcción de ese rpm (p. ej. se ha empaquetado y construido 5 veces, modificaciones menores, cambios en la localización de archivos, etc.), para la arquitectura Intel, y es un archivo rpm.

Comando	Función
-q	Consulta información de los paquetes / bases de datos
-i	Instala el software
-U	Actualiza o instala el software
-e	Extrae el software del sistema (borra)
-v	dar más información
-h	Marcas hash
Ejemplo de comando	Función
rpm –ivh paquete.rpm	Instala ‘paquete.rpm’, da más información, muestra marcas hash
rpm –Uvh	Actualiza ‘paquete.rpm’, da más información, muestra marcas

paquete.rpm	hash
rpm –qf /algún/archivo	Comprueba a qué paquete pertenece un archivo
rpm –qpi paquete.rpm	Consulta ‘paquete.rpm’, saca un listado con información
rpm –qpl paquete.rpm	Consulta ‘paquete.rpm’, saca un listado de todos los archivos
rpm –qa	Consulta la base de datos RPM, lista todos los paquetes instalados
rpm –e nombre-paquete	Elimina ‘nombre-paquete’ del sistema (según listado por rpm –qa)

Red Hat linux 5.1 venía con 528 paquetes, y Red Hat Linux 5.2 venía con 573, cuando se para a pensar se da cuenta que es un montón de software. Por lo general acabará con unos 200-300 paquetes instalados (más aplicaciones en estaciones de trabajo, los servidores tienden a ser más livianos, pero no siempre es el caso). Así que cuáles se deberían instalar y cuáles se debería evitar instalar si fuese posible (como los paquetes de servicios remotos).

dpkg

El sistema de paquetes de Debian es un paquete similar a RPM, sin embargo carece de cierta funcionalidad, aunque en conjunto hace un trabajo excelente gestionando los paquetes de software de un sistema. Combinado con la utilidad dselect (ya un poco desfasada), se puede conectar con sitios remotos, recorrer los paquetes disponibles, instalarlos, ejecutar scripts de configuración necesarios (como para gpm), todo desde la comodidad de su consola. La página del manual de dpkg "man dpkg" es bastante grande.

El formato general de un archivo con un paquete de Debian (.deb) es:

nombrepaquete_versiónpaquete-debversion.deb
ncftp2_2.4.3-2.deb

Al contrario que los archivos rpm, los archivos .deb no traen indicativo de la arquitectura (no es que tenga demasiada importancia, pero es algo que hay que tener en cuenta).

Comando	Función
-l	Consulta un paquete
-i	Instala el software
-l	Saca un listado del software instalado (equivalente a rpm –qa)
-r	Elimina el software del sistema
Ejemplo de comando	Función
dpkg –i paquete.deb	Instala paquete.deb
dpkg –l paquete.deb	Saca un listado de la información de paquete.deb (rpm –qpi)
dpkg –c paquete.deb	Saca un listado de todos los archivos de un paquete (rpm –qpl)
dpkg -l	Muestra todos los paquetes instalados
dpkg -r	Elimina ‘nombre-paquete’ del sistema (según listado por dpkg –l)

Anexo B Guia de Denegación de Servicio

Detección de DoS

A nivel de gestión de red, es aconsejable el disponer de filtros de entrada, consiguiendo de esta manera evitar que entren a la red paquetes cuya dirección IP haya sido falsificada. Y aunque esta medida no garantiza ser víctimas de un ataque, facilitará el análisis y seguimiento de éste en caso de producirse.

Cada día, y en más casos, los dispositivos de comunicaciones permiten especificar el ancho de banda máximo que puede ocupar cierto tipo de tráfico. Esta posibilidad permite detectar cuándo se está produciendo una anomalía, y poder tomar las contramedidas oportunas.

Zombie Zapper [http://razor.bindview.com/tools/index.shtml]. Este programa, funciona para todas las herramientas y versiones de DDoS conocidas, permite indicar a un sistema que este generando un ataque (Demonio/Agente) que cese. En este caso, no se evita el ataque, pero permite pararlo.

Como detectar si se ha realizado un ataque contra nosotros. Revisar los logs: es una de las partes más importantes para la detección de una intrusión, consiste en revisar los logs periódicamente en busca de indicios de ataques. En logs podemos encontrar los logs del S.O., los logs del firewall, los logs del IDS, etc...

Comprueban que todos los archivos del sistema hubieran sido modificados, (o algún s.o. de su familia) una opción seria al telnet, su, etc...que pueden haber sido cambiados por otros binarios troyanizados.

Buscar todos los archivos sospechosos que puedan ser backdoors e igualmente todos los procesos que puedan ser keyloggers del sistema, sniffers, etc...

Buscar indicios de sniffing, si se cree que en esos momentos alguien esta ejecutando un sniffer, haciendo un netstat, buscando alguna ip que este en modo promiscuo.

Inspeccione los puertos en busca de puertos abiertos de los que no se tenga conocimiento ninguno, en caso de que haya algún atacante es posible que haya dejado algún programa en escucha en algún puerto. Tener en cuanta los puertos UDP, no solo en los TCP.

Examinar los archivos de contraseñas para asegurarse de que no hay usuarios no autorizados con permisos de root, etc...

Buscar archivos ocultos que puedan contener puertas traseras, no dejarse engañar por el archivo "..." usado muchas veces por hackers/crackers para confundir con el ".." y el "."

9.2.1. Archivos de logeo

Hay una serie de archivos en linux que se encargan de realizar el loggeo de diferentes cosas. En linux hay diversos archivos que nos pueden mostrar información importante.

.bash_history : es un archivo oculto del sistema que se encarga de loggear todos los comandos que son realizados por un usuario (todos - todos no, pero si los ultimos) y se guardan en el archivo .bash_history en el home de cada usuario (con un ls...se hace ls -a).

console: Este archivo loggea todos los mensajes que lanza el kernel a la consola, como motivo de seguridad contra un atacante no es muy necesario. Se encuentra en /dev/console

secure: Este archivo loggea todas las conexiones que se realizan hacia la maquina del usuario... /var/log/secure

messages: Este archivo cumple la misma función que wtmp en algunos linux , informando cuando entra un usuario, cuando sale, la hora y fecha, etc... Se encuentra en /var/log/messages

httpd: teniendo servidor web, se loggean las conexiones, el archivo se llama httpd y algunas veces varia el nombre, esta en la carpeta /var/log/httpd

maillog: Loggea todos los mails en un archivo: /var/log/maillog

cron: loggea el cron /var/log/cron

boot.log : loggea los mensajes de arranque del sistema

batille-firewall. crea un script para una buena seguridad de la red, ayuda en otras tareas de seguridad como la de loggear, dar permisos de ejecución a algunos archivos SOLO para el root, etc... Realmente es muy recomendado para pequeñas redes o un solo equipo.

Comandos

Hay algunos comandos que sirven especialmente para mantener controlada la red.

ps -aux : permite saber los procesos en ejecución, puede ser útil para ver los procesos extraños.

who: muestra los usuarios conectados actualmente, es como el finger pero para ejecutar de forma local.

¿CÓMO DEFENDERSE DE ESTE TIPO DE ATAQUES?

Muchos de estos ataques de denegación de servicio se basan en fallos de diseño propios de Internet, por lo que no son "solucionables" en un plazo breve de tiempo.

Los ataques de "syn flood" ya no son un problema, si se instala un sistema operativo actualizado.

Los ataques de "connection flood" pueden ser detectados por un administrador de sistemas eficiente, y se pueden filtrar en el cortafuegos corporativo, siempre que los sitios atacantes sean pocos.

Por último, tenemos el caballo de batalla real: "net flood".

En estos casos, la red víctima no puede hacer nada. Aunque filtre el tráfico en sus sistemas, sus líneas estarán saturadas con tráfico malicioso, incapacitándolas para cursar tráfico útil. Un ejemplo habitual es el de un teléfono: si alguien quiere molestar, sólo tiene que llamar por teléfono, de forma continua. Y si descuelga el teléfono para que deje de molestar, tampoco se podrán recibir llamadas de otras personas. Este problema es habitual, por ejemplo, cuando alguien intenta mandar un fax empleando el número de voz, y el fax insiste durante horas y horas... sin que el usuario llamado pueda hacer nada al respecto.

En el caso de "net flooding" ocurre algo similar. Aunque se filtre el ataque en el cortafuegos, se encuentra que las líneas estarán tan saturadas de tráfico que las conexiones auténticas simplemente no pueden competir. En casos así el primer paso a realizar es el ponerse en contacto con el "carrier" (el operador de

"backbone") para que intente determinar la fuente del ataque y, como medida provisional, filtre el ataque en su extremo de la línea (normalmente de bastante mayor capacidad que el extremo).

El siguiente paso consiste en localizar las fuentes del ataque e informar a los administradores, ya que seguramente se estarán usando sus recursos sin su conocimiento y consentimiento. Si el atacante emplea "ip spoofing", esto puede ser casi imposible.

La fuente del ataque es muchas veces la víctima. El origen último puede ser prácticamente imposible de determinar.

Anexo C Entrevistas

Entrevista 1 TigerKick

Pregunta:

Hola amigo vi el artículo que publicaste en el foro de the_others.com acerca de los problemas que se tienen por usar de contraseñas comunes como nombres de usuario, cuidades natales o nombres de familiares. Estoy haciendo una recopilación de opiniones de varias personas acerca del tema de seguridad y mas exactamente en el campo del control de acceso a los recursos de una maquina.

Quisiera saber tus opiniones acerca de cómo controlar el acceso a las maquinas y creación de políticas de seguridad.

Tigerkick:

La situación es sencilla, como dije en el artículo, el control de acceso no es más que mantener bien salvaguardado un login y una contraseña. Si los usuarios son tan estupidos para soltar la clave a cualquiera que se la pida, o peor aun dejarla escrita en un post it pegado en el monitor, la seguridad informática no tiene ningun sentido. Puede ser que el administrador instale cuantos cortafuegos, sniffers y todo lo que respecte a seguridad, sin una política se salvaguardado de contraseñas no habra seguridad que valga.

Para la creación de una política de seguridad mira en

http://www.iec.csic.es/criptonomicon/linux/

Pregunta

Gracias por tu respuesta. Esto me ayudara a completar la investigación. Sin embargo también quisiera saber que opinas del uso de criptografía y sesiones telnet para accesos remotos a los servidores IINUX.

Tigerkick:

La criptografía es uno de los mas importantes temas en cuanto al envió de contraseñas, yo no soy el especialista en el campo de la criptografía, sin embargo ninguna información debe viajar en texo plano por la red, de ser así, cualquier sniffer la detectaría, y ahí si seria lo mismo que dejar las claves escritas sobre el monitor de tu pc.

Las sesiones remotas como rlogin, rsh y telnet son un mal con el cual se debe convivir. En la compañía donde trabajo se accesa al software aplicativo gracias a sesiones telnet, no tenemos problemas de intrusiones, porque los usuarios no salen a internet por medio de esta red, por lo tanto es como si estuviesen desconectados del mundo.

Pregunta

De nuevo gracias por la respuesta a mi correo, esta información es de gran ayuda. Quisiera saber, si es posible, como hacen en las empresas para contrarrestar el acceso ilícito.

Tigerkick:

Como te dije anteriormente, en mi red no hay problemas de seguridad en el campo de intrusos remotos. Sin embargo la solución mas común es el uso de sesiones ssh y ssl para enviar información encriptada con llaves publicas y privadas. Pero no soy un experto en el tema, para ello buscate la guía de configuración de ssh que viene con todas las distribuciones LINUX desde 1999.

Entrevista 2 Kevin Mitnick

El 13 de noviembre del 2003 fue liberado el hombre calificado por la prensa de EEUU como el hacker más buscado del planeta, Kevin Mitnick, salio a la calle. Según las autoridades estadounidenses, fue culpable de haber violado los sistemas informáticos de más de 35 multinacionales durante 13 años, ocasionándoles pérdidas de casi 50.000 millones de dólares.

En su primera entrevista tras salir de la cárcel, donde permaneció cinco años, dijo, que para ese ataque a la Red: «Pudieron ser chicos buscando emociones fuertes

los que provocaron el caos en Internet. O yuppies sin escrúpulos para ganar en Bolsa, anticipándose a la caída de valores. Lo cierto es que no es un trabajo de auténticos hackers. Falta sofisticación y elegancia. Cualquier estudiante podría haberlo hecho».

Pregunta.
¿Qué diferencia existe entre usted y esos hackers aficionados?
Kevin Mitnick.
Mi especialidad era copiar masters originales de teléfonos móviles. Estaba fascinado por las telecomunicaciones y quería saber cómo funcionan por dentro. Incluso cuando robé centrales telefónicas enteras era por divertirme y por un desafío intelectual, nunca para obtener un beneficio. He llegado a conseguir los números privados de grandes estrellas como Bruce Springsteen o Madonna. Pude haber llamado incluso a Clinton, pero no quería alertar al servicio secreto.

Pregunta.
Le consideran el hacker más peligroso de la historia.
Kevin Mitnick
Eso es un mito, que comenzó con varios artículos de John Markoff en The New York Times, llenos de acusaciones difamatorias, que más tarde fueron desmentidas por las autoridades. Markoff me la tenía jurada porque me negué a colaborar en su libro y creó el mito de Kevin Mitnick para hacer de Takedown [su libro] un best seller.

Pregunta.
¿Por qué le persiguen entonces las autoridades?
Kevin Mitnick
Aprovecharon la ocasión para transformarme en el chivo expiatorio de todos los hackers del mundo. Y para autojustificarse, exageraron hasta lo inverosímil el

daño que pude causar, que está muy lejos de los cientos de millones que me imputan.

Pregunta.
¿Por qué nunca sacó provecho de su talento informático?
Kevin Mitnick
Porque mis valores éticos me lo impiden. Unos valores que heredé de mis padres, judíos de origen ruso. Nunca fui capaz de robar dinero. Y eso que hoy podría ser multimillonario y vivir el resto de mis días al sol del Caribe. Pero mi conciencia me lo impidió. Y estoy orgulloso de ello. Aunque confieso que no sentía remordimiento alguno cuando atacaba a compañías monolíticas y riquísimas, que extraen el máximo beneficio de sus clientes. Me impulsaba más bien la euforia del descubrimiento científico, el placer mental que se siente cuando se resuelve un problema matemático.

Pregunta.
¿Qué va a hacer ahora?
Kevin Mitnick
Me gustaría encauzar mi talento para ayudar a la comunidad a defenderse de los hackers, pero el Gobierno me lo impide. Las restricciones impuestas por mi libertad vigilada durante los próximos años son increíbles. No puedo encontrar trabajo ni en un MacDonalds. Ni matricularme en la universidad o en sitio alguno donde haya un computador. También me están prohibidos los teléfonos celulares y las agendas electrónicas. Ya comienzo a tener crisis de abstinencia informática.

Pregunta
Revelaría el proceso para ingresar a los computadores de una gran compañía
Kevin Mitnick
Si hubiese sido hace cinco o seis años no me importaría decirlo a cualquiera. Pero hoy día hay un montón de adolescentes jugando en la red y queriendo sacar

dinero fácil, el ponerse a enseñar esto tan libremente puede generar un caos mundial. Además al igual que hace cinco años, después me harían responsable por lo que yo no he hecho. Por otro lado, no se me permite dar clases ni impartir conocimientos sobre el tema de la computación ni redes de información. En últimas lo que ellos quieren es callarme, pero no soy el único que sabe del tema, hay miles de hackers en el mundo que tienen conocimientos más avanzados que los míos.

Pregunta

Alguna vez trabajo para alguien?

Kevin Mitnick

Desde pequeño tuve la facilidad de manejar un computador, por eso tuve cantidad de empleos y ofertas referentes al tema, claro que nunca hice ningun daño, simplemente se me pedía que averiguara alguna información y yo solo la buscaba, y la entregaba sin mirar que era.

Pregunta

Trabajo para una entidad del estado como la CIA, el Ejército, FBI etc.

Kevin Mitnick

Eso es reserva del sumario, todo lo que yo diga puede ser usado en mi contra.

Entrevista 3 Richard Stallman

Una conversación con Richard Stallman, por David de Ugarte

Pregunta:

Lo que comenzó como movimiento del software libre parece ahora extenderse a través del copyleft a los libros. ¿Cree esta proyección natural? ¿La filosofía del software libre y el copyleft seguirá yendo cada vez más allá?

Richard Stallman

No exactamente. Los libros tienen distintos propósitos. Hay libros de uso funcional como manuales y diccionarios, libros de opinión, de Arte, de entretenimiento... no pienso que las cuestiones éticas sean independientes del propósito del libro. En los libros de propósito funcional las cuestiones son iguales. Esos libros deben ser libres. Pero no necesariamente los otros tipos. Hay ahora proyectos de libros de texto libres, hay una enciclopedia libre, la mayor del mundo y creo que hay un diccionario de castellano libre.

Pregunta
¿Y la música? ¿Cómo es aplicable el espíritu del software libre a la música?

Richard Stallman
Es una cuestión difícil. No tengo una respuesta que me satisfaga. Seguro que la gente debe tener por lo menos el derecho de compartir no comercialmente copias de la música grabada. La cuestión del hecho de compartir existe como consecuencia de un cambio de tecnología. En la época de la imprenta esto no existía como problema de importancia práctica porque sólo los impresores podían copiar libros eficientemente. Era un asunto de reglamentación industrial, no de derechos cívicos. A consecuencia de un cambio tecnológico se ha vuelto una cuestión de derechos cívicos. Otros cambios por venir pueden igualmente cambiar nuestra visión de los derechos. No los principios morales fundamentales que los sustentan. Esos no los cambia la tecnología aunque si sus resultados, las aplicaciones prácticas de esos principios.

Pregunta
Rechaza el término piratería para hablar de la copia no autorizada
Richard Stallman
La piratería es atacar barcos y eso es muy muy malo. Pero compartir copias de cualquier obra en la computadora con vecinos y conocidos es un acto bueno, es cooperación social. La idea de comparar los dos actos, uno muy inmoral otro muy

moral es completamente incorrecta. Es un término de propaganda y no quiero participar de la propaganda de los editores.

Pregunta
Volviendo sobre la copia no autorizada, esta vez la copia no autorizada de software, ¿no cree que a largo plazo favorece a los grandes monopolistas?
Richard Stallman
Puede que si, pero esto no quiere decir que sea legítimo imponer penas a los que hacen copias no autorizadas, porque compartir copias no es inmoral y no podemos tolerar el castigo sólo porque esperemos un resultado indirecto favorable a nuestra causa.

Pregunta
¿Qué ganarán nuestros hijos con el software libre?
Richard Stallman
La libertad derivada de guardar el control sobre todas las computadoras. Con el software no libre el dueño legal del programa tiene el control sobre lo que hace tu computadora. Ganarán una sociedad en la cual la cooperación entre los ciudadanos será promovida y no prohibida como hoy en día.

Pregunta
Hace poco releía un cuento suyo, El derecho a leer, una auténtica distopía en el que el sistema de pago por derechos ha avanzado tanto que es imposible leer sin tener que pagar. Y me acordaba de que en los años sesenta esto no era una pesadilla, sino una utopía llamada Xanadú que fue el comienzo del hipertexto.
Richard Stallman
Por eso no era yo tan partidario de Xanadu... He visto un día en los años ochenta que había una contradicción entre la licencia para publicar cualquier cosa en Xanadu y la GPL en GNU. Habría estado prohibido publicar cualquier programa bajo copyleft en Xanadu.

pregunta

¿Entiendes GPL como una negación de la propiedad intelectual?

Richard Stallman

En términos legales es un uso del derecho de autor, no una renuncia. En términos legales es muy claro. En términos morales es decidir no ser guardián del uso que los demás hacen de tu obra. Es por eso que violar la licencia de software libre es inmoral, no porque lo sea violar cualquier licencia, sino porque lo es violar los derechos del público. El copyleft implica el uso del derecho de autor que consiste precisamente en no usar el poder derivado de la propiedad excepto para impedir que otros diferentes al autor y al público impongan su poder.

Pregunta

El nuestro es un movimiento hacker que tiene mucho en común con el mundo científico, ¿se parecerán los científicos a los hackers? ¿Se extiende el hackerismo a otros sectores?

Richard Stallman

Hacker, usando la palabra inglesa, quiere decir divertirse con el ingenio [cleverness], usar la inteligencia para hacer algo difícil. No implica trabajar sólo ni con otros necesariamente. Es posible en cualquier proyecto. No implica tampoco hacerlo con computadoras. Es posible ser un hacker de las bicicletas. Por ejemplo, una fiesta sorpresa tiene el espíritu del hack, usa el ingenio para sorprender al homenajeado, no para molestarle. Hay algo también en común con el héroe medieval, la idea de mostrar la propia capacidad, a veces en competencia con otro

Pregunta

Pero no por dinero...

Richard Stallman

No, no por dinero, sino para mostrar fortaleza, identidad.

Pregunta

Pekka Himanen o Linux Thorvalds comentaban que el movimiento del software libre le debía mucho al espíritu de los años sesenta en California.

Richard Stallman

Es cierto, aunque yo no lo compartía en aquel momento

Pregunta

¿No? Porque no la compartía?

Richard Stallman

No, la contracultura estaba contra la ciencia y la racionalidad. Y en eso no estaba y no estoy de acuerdo. Pero había otra idea, que el dinero no es la medida de la vida, no es la última meta. Con eso sí estoy de acuerdo.

Pregunta

¿Cambia el software libre los ejes derecha-izquierda?

Richard Stallman

Siendo de izquierdas me gustaría que fuera de izquierdas, pero en el mundo entero la mayoría de los que se interesan en el software libre pertenecen a la derecha, son libertarios. No estoy de acuerdo con ellos, creo que tenemos un deber de cuidar a los enfermos, a los pobres, no dejar a nadie morirse de hambre.

Pregunta

Entonces el eje derecha izquierda es indiferente en la cuestión del software libre.

Richard Stallman

Es otro eje. El software libre no se ubica entre derecha e izquierda.

Pregunta

Pero la izquierda liberal también ha sido en buena medida tecnófoba. Es decir reacia a los avances de la tecnología

Richard Stallman

Hay buenas razones para la tecnofobia, las computadoras conllevan el peligro de un estado totalitario como nunca. Los políticos temen que se les demuestre todos los delitos de corrupción que cometen. Es ahí donde actúa el ciberpunk

Pregunta
Que es el ciberpunk
Richard Stallman
Ciberpunk.org es la asociación del movimiento ciberpunk español. Sin renunciar a sus orígenes como movimiento estético y literario está dedicada a la defensa de las libertades individuales y los derechos civiles en el ciberespacio, pero también a extender en el mundo real aquellas herramientas de la red útiles para el ejercicio de esos mismos derechos y libertades.

pregunta
En que consite Ciberpunk.org
Richard Stallman
Ciberpunk.org es toda una experiencia de ciberdemocracia: Los socios se comunican entre si a través de una serie de foros en esta misma web que mantienen abierta una suerte de asamblea permanente. También hacemos como mínimo un Congreso al año en el que se materializa el trabajo teórico, se presentan ensayos y obras literarias, se discuten las líneas de actuación y se eligen los responsables del mantenimiento de la página y los representantes de la asociación.

Pregunta
De donde nació Ciberpunk
Richard Stallman
Ciberpunk.org nace de la reflexión generada por el grupo de escritores y lectores que desde 1996 se fue generando alrededor del ezine Ciberpunk.com (continuado desde octubre de 2002 por la Bitácora de las Indias). Este ezine había nacido a su

vez de la evolución del primer grupo ciberpunk español (Berlín, 1989). En 2002 el grupo se constituyó como asociación y se registró con el número nacional 1702229

Pregunta
Cual es la pesadilla del ciberpunk
Richard Stallman
El peligro se acerca muy rápidamente. Hay planes para desarrollar tecnologías que reconozcan a las personas por la calle. Es muy peligroso para la libertad. Esta tecnología en manos un gobierno opresivo como el actual de algunas naciones que no respeta los derechos civiles ni la democracia, es muy peligrosa. Ciberpunk denuncia esos proyectos que lo único que intentan es mantener pueblos oprimidos.

Entrevista 5 Saintgohe

Pregunta
En concreto, ¿qué es un hacker?
Saintgohe
El término hacker es objeto de continuo debate entre el mismo movimiento, pero por lo que puedo deducir (y sentir) un hacker sería aquel amante de la informática, con grandes conocimientos de la materia (programación, sistemas, redes, criptografía, etc) que se siente parte de un movimiento contracultural positivo (es decir, constructivo) para que la información sea libre, al igual que el acceso a la misma, y que luchan contra la tentación de grandes compañías, instituciones públicas y demás, para controlar esta información, a pesar de que sea la lucha de David contra Goliat. Creo que son los últimos románticos con un gran arma en sus manos, la imaginación.

Pregunta
Son parecidos a los que se ven en televisión
Saintgohe
Las películas de Hollywood presentan a los hackers como jóvenes "gamberros" que entran en la Red para pasar el rato

Pregunta
Esta usted de acuerdo con esta visión?
Saintgohe
Existe bastante confusión en cuanto a este movimiento entre la población en general. Entre los Hackers hay muchos jóvenes (un gran colaborador mío para la tesis, un hacker de Barcelona llamado Azidbla, es un claro ejemplo) aunque no son todos. Y tan gamberros como cualquiera con esa edad. Disfrutan con los ordenadores y sus complicaciones son retos. Pero a su vez ayudan a mejorar el mundo de la informática, crean, innovan y se relacionan con otros/as aficionados.

Pregunta
Que opina de la imagen que dan los medios de comunicación sobre los hackers?
Saintgohe
El desconocimiento de este mundillo es un grave problema entre colegas periodistas, aunque a veces no es fácil determinar cuando la culpa es de un periodista por no informarse mejor, cuando de un jefe de redacción por juzgar que "vende" más la noticia sobre "crackers" que provocan daños a empresas o crean virus por afán de destruir, o cuando es un "cierto poder interesado" en desacreditar este movimiento que no hace lo anteriormente dicho.

Pregunta
Los hackers son un claro ejemplo de "Aprende por ti mismo". ¿Cree que este tipo de educación autodidacta se terminará imponiendo en el futuro?

pregunta

En el caso del hacker, existe un muy alto porcentaje de educación autodidacta, aunque suele complementar otros conocimientos "reglados", como Telecomunicaciones, Informática ...

Pregunta

Son los hackers el ídolo de la nueva generación digital?

Saintgohe

La publicidad ya está intentando aprovecharse de su aureola de luchadores románticos, quedándose tan solo con la pose y dejando lo importante, el contenido, fuera. Podrían ser los ídolos, si realmente su imagen supusiera la lucha por la libertad, la creatividad y la búsqueda de un futuro mejor.

Pregunta

Un hacker tiene más posibilidades de encontrar trabajo?

Saintgohe

Un auténtico hacker tiene grandes conocimientos informáticos, y como tal puede acceder a puestos de esta gama con facilidad, no por el hecho de ser hacker.

Pregunta

Que opina del lado oscuro de la piratería informática: violación de la intimidad, daños a empresas...?

Saintgohe

Como le pasaba a Luke Skywalker en la saga de Lucas, tener poder supone una constante lucha con el lado oscuro. La tentación de aprovechar los conocimientos para hacer dinero ilegalmente siempre está ahí, pero sólo caen los menos fuertes de voluntad. Otros que trabajan en el lado oscuro pueden ser expertos, pero no hackers, al igual que los que entran en un lugar y destrozan lo que encuentran son lamers. Grupos hackers atacan lugares que su conducta ética considera aborrecibles, como las páginas de pornografía infantil. Un método de ataque muy efectivo es crear programas útiles de distribución libre, gratis, lo que hace daño a

las grandes compañías, y el ejemplo claro es el del Linux, un gran sistema operativo mejor que los habituales "de pago", que es gratis.

Entrevista 5 Toom

Este hacker a quien llamaremos Toom. Es uno de los hackers nacionales más sonados. Aunque no se sabe su verdadera identidad, nisiquiera su seudónimo en la red, se cree que es Colombiano dado el conocimiento que tiene de las entidades gubernamentales del país. El Conversó vía Messenger acerca de su profesión o pasatiempo, de cómo pirateó servicios y de muchas cosas más.

Pregunta
Entraste con tu computador a los servicios del Departamento Administrativo de Seguridad (DAS). Y revisaste lo que hubiera.
Toom
Entré por joder. Nunca hubo mala intención. Si me hubiera querido cubrir las espaldas, podría haberlo hecho perfectamente. Pero tendría que haber sido malo.

Pregunta
Malo?

Toom
Y sí, porque si borro todo la información del DAS no hay manera de que me agarren después. Entré por entrar, no hice nada extraño, no rompí nada. Cuando vi que no había nada interesante me fui. Pero de todas maneras, algo me cubrí. En primer lugar: entré por Australia. Todo apareció un mes, un mes y medio después de que hubiera entrado. Pero desde que pasó todo esto, santito. Nunca más. Estoy al tanto de lo que pasa, de lo que se hace, pero no me pongo a jugar con nada.

Pregunta

Entraste para hacer algún trabajo especial?

Toom

No. Entré por ocio y por desocupe pero no a joder. Lo único que exploté fue un agujero que tenía el DAS. Se mataron en seguridad, porque pusieron códigos de acceso (passwords), y en realidad tenían un agujero por el que se podía entrar con cierto tipo de programas. Yo hubiera podido hacer lo que hubiera querido. El agujero estaba en la parte de html. Si de alguna forma yo logro que el html haga las cosas que quiero, me convierto en un usuario con acceso de administrador. Y como administrador puedo arreglar o agregar más cosas. Ellos no se dieron cuenta. En muchos lugares del mundo existen esos agujeros, pero casi nunca la página de html está ejecutando como supervisor.

Pregunta

En otros países, cuando se encuentra a alguien que detecta un agujero en un sistema, lo contratan enseguida.

Toom

Sí, pero ya viste cómo es acá. Fue todo un poco disparatado. En primer lugar, la prensa salió a decir a Búsqueda cómo había hecho yo para entrar, pero la mitad de las cosas era mentira y la otra mitad la inventaron ellos. Dijeron que me había robado las contraseñas, por ejemplo, y no me sirvieron para nada. Al tener los equipos, los usuarios que realmente tienen entrada externa por el DAS son tres. Son los que están en el well, en el well de root. Aunque vos tengas una cantidad de passwords, esa información en realidad no existe. Lo que vos tenés son claves, pero las claves están "encriptadas".

Pregunta

Hay manera de descifrar esas claves

Toom

Hay un método para romper claves llamado fuerza bruta. Se usa porque no existe una computadora que pueda romper una clave. Si se pone a todas las computadoras del mundo a hacerlo, demorarían un año en sacar un password, y la cantidad de cálculos necesarios convierte a todo el asunto en algo muy jodido.

Pregunta

Y como funciona eso de la desencripcion?

Toom

Es muy sencillo. Se basa en el funcionamiento de los passwords. Cuando se entra en forma legal se ingresa el login y el password. El método de encriptado funciona en una sola dirección, no existe la posibilidad de desencriptar. Cuando entrás, la computadora encripta el password que ponés y lo compara con el que ya tiene el sistema. Si ambos son iguales, yo soy el usuario correcto. Si son desiguales, no podés entrar.

Pregunta

Y el método de fuerza bruta?

Toom

El método fuerza bruta trabaja con diccionarios. Se parte de la base de que una gran cantidad de usuarios usa palabras comunes para su password. Nombres de personas, o palabras como manzana, por ejemplo, pero no una combinación extraña de caracteres. Entonces lo que se hace es encriptar diferentes palabras y compararlas. Comparo, y, si no son iguales, encripto otra, y otra. El problema es que sólo voy a tener una lista limitada.

Pregunta

Y cómo consigue la lista de passwords?

Toom

En este caso, la parte de html servía para robar la lista de passwords. El comando era sencillo. Y si el html puede cumplirlo, te devuelve la lista de passwords del sitio. Sólo tenía que teclear eso, nada más.

Pregunta

Suena como inseguro.

toom

Los servidores que siguen usando cierto tipo de programas todavía tienen ese agujero; los que dejaron de usarlos ya no lo tienen más. Pero buscando entre 300 o 400 alguno sale, alguno todavía está bien. Pero además tiene que darse que la página de html tenga privilegio suficiente como para leer el archivo de passwords. Yo obtuve el archivo, me puse a hackear la máquina y me hackeó diez cuentas, diez accounts.

Pregunta

Pero con 10 cuentas alguna debía servir para algo o no?

Toom

Pero no servían para nada, porque sólo tres personas tenían acceso externo. Si hubiera estado en el DAS, dentro de una computadora, hubiera entrado como menganito. Pero sólo tenía acceso a lo que tiene menganito, es decir a nada. Además, lo que yo estaba haciendo hasta ese momento era indetectable. Luego modifiqué el programa, un proceso un poco complicado de explicar, pero en concreto después de tener la lista de passwords puse el nombre de uno de los usuarios que tenía acceso.

Pregunta

Y lo de Australia fue hackeado también?

Toom

No. En Internet podés hacer trade de cualquier cosa, todo vale. Si yo quiero hacer trades de accounts, lo hago. Te dicen: "Mirá, tengo el último jueguito, pásame dos accounts de Australia". Puedo canjear naranjas por peras. Se pueden hacer mil accounts piratas. Hacés telnet a ese account y de ese hacés otro. Así que el registro quedó cuando hice el telnet al DAS, pero no antes.

Pregunta
Si entraste haciendo Telnet desde varios equipos uno tras otro como te agarraron?
Toom
Otro rastro que seguramente debo de haber dejado es cuando ejecuté un comando que te permite saltar de cualquier usuario a supervisor, a root; eso siempre queda registrado.

Pregunta
Y para que quería ser supervisor?
Toom
Mi idea era compilar un programa que me permitiera tener una entrada segura siempre, para no hacer todo ese lío y quedar registrado.

Pregunta
porque supo que no se podía?
Toom
Porque no tenían un compilador en línea, y que el sistema que tenían era SunOs y no Lynux y eso lo complica todo, porque es muy difícil conseguir un compilador para SunOs.

Pregunta
Como lo atraparon?
Toom

Hice algunas cosas m Un mes y medio más tarde se aparecieron por casa y se llevaron la computadora. Estuve ocho meses sin poder trabajar. Yo hice una cantidad de programas para mi trabajo que estaban en la máquina. Los del DAS proponían que se borrara mi disco duro, toda la información. Si lo hacían yo les hacía un juicio, porque no tienen derecho de destruir nada.

Pregunta
Supongo que las perdidas no solo fueron de información
Toom
Yo estaba quedando mal con la gente para la que trabajaba; entregaba fuera de fecha; debí contratar gente para que hiciera mi trabajo, lo que fue una pérdida de dinero. Cantidad de veces les pedí a los del DAS que me dieran los programas que estaban en la máquina, pero claro, cómo iban a darle una mano al tipo que estaba metido ahí.

Pregunta
No intentaron negociar o solucionar todo en buenos términos.
Toom
Yo no tenía problema en darles lo que exigieran. Pero claro, yo soy el delincuente y el malo de la película siempre es malo. Al final estuve ocho o nueve meses sin la máquina, y eso me rejodió.

Pregunta
Cómo se dieron cuenta de que habías entrado?
Toom
Tenían una entrada. Dicen que detectaron mi entrada desde Australia, pero yo me huelo algo totalmente diferente.

Pregunta
Diferente? Que quiere decir?

Toom

Lo que pasa es que el account que yo estaba usando en Australia no era sólo mío. Al ser un account pirata, lo usa un montón de personas. Y si un pueblo lo usa, los que están en Australia, más tarde o más temprano, se van a dar cuenta. O alguno hizo una manganeta muy grande que saltó. Mi log, el que uso desde aca, estaba registrado en ese account. Entonces ese account llamó a todo el mundo donde entré yo y todos los demás y avisó. Les dijo al DAS: "el día tal tuviste una entrada a las tantas horas gmt de un tipo que vino de mi ciudad. Y este account estaba siendo pirateado". Creo que así es como pasó.

Pregunta

Pero dices que no tenías nada que robar

Toom

Nunca tuve intención de robar algo. Y el juez también lo entendió. De todas maneras la ley es la ley, y por algo me tenían que agarrar.

Pregunta

¿Hay ley de esto?

Toom

No existe ley de hacking aca. Lo que se dio es que como yo tenía en mi poder un archivo con claves que estaban encriptadas y todo lo demás, supuestamente tengo un conocimiento de documentos secretos y según el artículo no sé cuánto...

Pregunta

Pero aparte de todo eso, hay una pasión, ¿o no?

Toom

¡Claro! Todo pasa por violar el sistema. Hay gente que lo hace por negocio, por plata. Pero el 99 por ciento no.

Pregunta

Te agarraron de casualidad o te andaban buscando?

Toom
Cada dos años limpian a uno. Yo tenía un amigo que conocía a algunos hackers -hablo de hace cinco o seis años- que los limpiaron durante la Guerra Fría.

Pregunta
Los asesinaron?
Toom
Claro, porque robaban a todo el mundo, a la kgb, a organismos del Estado. Y a esos los limpiaron.

Pregunta
Conocés personalmente a otros hackers?
Toom
Personalmente no. Es que Internet une mundialmente a todas las personas que tienen algo en común. Ya no hay más límites geográficos. Todos están ahí. Pero yo no estaba con un grupo de gente que fuera salada, todo era muy legal.

Pregunta
Cuál es tu situación legal actual? De qué se te acusa en concreto?
Toom
Estoy procesado sin prisión y tengo que esperar a que se termine el juicio. Me acusan de "conocimiento de un documento secreto".

Pregunta
Tu abogado, en que se basa para defenderte?
Toom
Mi abogado busca demostrar que lo que ellos consideran un documento secreto en realidad no lo es, y que sobre esa base no se me puede acusar.

Entrevista 6 Capitan ZAP

¿Quién es el Capitán Zap?

El año ..... 1981. La administración Reagan se encontraba en su infancia. "Elvira" se colocaba en las gráficas del Billboard. Y un joven hacker estaba a punto de convertirse en la primera persona arrestada por un crimen de cómputo.

Dieciocho meses antes, Ian Murphy (también conocido como "Capitán Zap"), junto con tres cómplices, hackearon las computadoras de AT&T y cambiaron sus relojes internos. Los clientes de repente empezaron a recibir descuentos nocturnos en plena tarde, mientras que otros que habían esperado hasta la media noche para usar el teléfono recibieron facturas elevadísimas. Por su participación en el crimen, Murphy recibió una condena de mil horas de servicios comunitarios y dos años y medio en libertad condicional (considerablemente menos de lo que reciben hoy en día los hackers). También fue tema de inspiración para la película "Sneakers".

Hoy Murphy, como otros hackers, maneja su propia empresa de seguridad "IAM Secure Data Systems, Inc." Por cinco mil dólares diarios mas gastos, Murphy se ha disfrazado de empleado de una compañía telefónica y ha crackeado un sistema de seguridad bancaria, ha ayudado en investigaciones de asesinatos, y a dirigir los estudios en cuanto a terrorismo aéreo. Pero para Murphy lo mejor es hackear sistemas de seguridad de empresas, con su permiso, y ayudándolos a protegerse de intrusiones.

Aquí LatinoSeguridad les presenta un fragmento de la entrevista que concedió:

Pregunta

¿Qué te impulso en primer lugar a hackear sistemas?

CapZap

Hackear sistemas es un término muy amplio para denominar los pensamientos que han sido parte de mi vida. Desde muy joven, fui una persona muy curiosa.

Este amor a los sistemas tecnológicos nació desde una niñez muy temprana ya que mis padres se aseguraron que mi educación fuera la mejor posible en el área donde me iba a desarrollar. A temprana edad, los juguetes que me regalaron los aparte e investigaba para que habían sido hechos. También tenía una increíble curiosidad a cualquier tipo de personal de servicio que viniera a casa para atender problemas con los televisores, a los dispositivos de basura, sistemas de intercomunicación, de telefonía, y cualquier otro tipo de sistema que estuviera en casa.

Supongo que puedo imaginar que mi primera exposición a un hackeo de sistemas pudo empezar con mi temprana fascinación a la red telefónica. En ese tiempo, a principios y mediados de los sesenta, había una solo una compañía telefónica en el país, y la compañía telefónica guardaba sus secretos tecnológicos del público en general. Puedo decir que mi primer pensamiento de hackeo fue con el sistema telefónico y de hecho estaba interceptando llamadas telefónicas de las chicas del vecindario para conocer de qué estaban hablando. Haciendo "conexiones en crudo" de cables para hacer que desde un polo tuviera la posibilidad de escuchar llamadas o para hacerlas a cualquier lugar del mundo.

Leer fue una gran fuente de satisfacción, hay una gran variedad de libros de ciencia que ayudan a entender las cosas que trabajan en el mundo. Lo cierto es que además de que tengamos problemas como la guerra bio-química así como los escenarios de ataques terroristas, yo estaba fascinado con estos sistemas y con la manufactura de dichos dispositivos y formulas. Recuerdo el primer libro que leí sobre el tema y era un libro que fue escrito a principio de los setenta llamado Armamentos Químicos y Biológicos por Seymour Hersch del New York Times. También estuve fascinado con las armas nucleares y explosivos. Esto abrió mis ojos para ver lo que acontecía a una temprana edad.

Pero siempre fui un hacker si lo quieres ver de esa manera. Yo prefiero llamar una investigación ortodoxa de protocolos que pone a prueba los límites de la sociedad, avances tecnológicos, impactos globales sobre la insaciable sed del hombre de ver que hay más allá sabiendo que el infierno esta ahí afuera. Realmente pienso que la necesidad de los ciudadanos en cuanto a tecnología, deja solo el entendimiento de cómo trabaja todo guardando la mayoría de la gente una visión provincial de la tecnología y reprime su mente en general.

Ahora tenemos una gran sociedad que no entiende el trabajo de una simple luz que enciende en sus casas, y tiene que llamar al eléctrico para cambiar el switch. Y luego se queja de que gasto $150 dólares por eso. Crezcan y aprendan a tomar las riendas de su entorno para entender que están viviendo en el. La cuestión sobre todo lo que viene antes de ti no lo tomes a condición que todo esta muy bien.

Pregunta
Cómo era la seguridad de la Tecnología de la Información en esos ayeres?
CapZap
La seguridad de la tecnología de la información era inexistente. Era una broma si es que algo existía. Control de acceso, contraseñas y control de la información no existía en el entorno del mundo real. Solo los militares tenían las computadoras más poderosas y eso lo hacía mucho más divertido. De hecho para todos ustedes que desean conocer de la historia, el internet no estaba planeado como ahora surgió. Era una red construida para la guerra, guerra nuclear y como una forma para que los militares conversaran y supieran que se requería o que tenían que hacer del otro lado. Ahora uno de los problemas de la seguridad de la tecnología de la información es que nadie lo pensó así antes ni que pudiera ocurrir lo que pasa ahora. Las computadoras eran maquinas enormes que la gente solo podía ver en cine de ciencia ficción que eran enormes muros de luces destellantes, nadie tenía acceso a ellas solo para fines de investigación o cosas similares.

Pregunta

En su opinión, que ha cambiado en la postura de seguridad en las empresas de hoy en día?

CapZap

La seguridad ha sido defendida por un gran número de nosotros desde la década de los ochenta hasta hoy en día. Nosotros nos mantenemos al margen ya que nada ha pasado en los sistemas centrales y no hay muchos sistemas conectados a tiempo completo. Solo los militares tienen sistemas conectados en una base de tiempo completo, y en esa red, "Arpanet" es el campo de juego. Ahora en las mayoría de las computadoras es usual un NIC, la distancia de frecuencias ancha es estándar y popular.

Pero nosotros seguimos viendo rechazo de seguridad de parte de las masas porque ellos no entienden que es necesario. Las compañías siguen sin ver el costo beneficio y solo responden cuando tienen un incidente. Las ideas de seguridad siguen en segundo plano tanto para los dueños pequeños y medianos. El costo de los programas es alto y si vienen con desperfecto en el área de seguridad son vulnerables a los ataques desde cualquier punto del planeta. Los virus son incontrolables y la mayoría de la gente aun no tiene idea de cómo actualizar su software antivirus.

Ahora en el tema de seguridad están completamente solos, es tu responsabilidad la postura que asumas en cuanto a la seguridad y tu propia elección estar expuesto al resto del mundo. Si dejas tu auto abierto es probable que lo roben, lo mismo en tu casa, puede ser robada, tú tienes la opción, diario hay la oportunidad y cada día puedes verificar la información de la situación que tiene la seguridad en el mundo.

Pregunta

¿Que tan sencillo es para ti, en los ambientes actuales, hackear el sistema de una empresa mediana?

CapZap

Se ha vuelto un poco más difícil entrar a los sistemas, pero siguen estando ahí y puedes encontrar varias herramientas en la red, además de muchos agujeros de seguridad, se convierte en un juego de niños. Los scripts están incontrolables en la red y los usuarios no toman las herramientas que existen "gratis" para protegerse. De hecho el sólo pensar el hackear viene acompañado del factor diversión, tanto que puedo salir a cenar y regresar y encontrar las brechas en los sistemas que están ahí esperando a que juegue con ellas.

Los usuarios aun no toman su posición dentro de las políticas de protección de la seguridad porque no han entendido el valor ni la necesidad de estas políticas. Hace falta el conocimiento por parte de los usuarios. No existen políticas reales para las generación de contraseñas en ningún sistema chico o mediano, se necesita de una combinación de herramientas de seguridad. La seguridad cuesta dinero y muchas empresas recortan el presupuesto porque no ven un beneficio directo. Todos deberían estar conscientes de que la seguridad cuesta y que se requiere.

Pregunta

¿Cómo te ganas el dinero?

CapZap

Realmente es una buena pregunta, retirado en algunos aspectos, activo, vigoroso y robusto en otros, sigo manteniendo mis dedos en muchos pies. Sigo haciendo investigaciones y dando servicio a un buen numero de clientes internacionales. Es ahora mucho más fácil hacer consultorías vía tele conferencia y el intercambio de información por la velocidad que se maneja en la red. Adicionalmente, acabo de terminar una serie de video británica para el Discovery Channel sobre seguridad de la información, respondiendo una serie de entrevistas, como esta, y estoy

escribiendo mi cuarto libro de temas de seguridad y los cambios en internet, completando una publicación que se llamará "A Madman's view of Terrorism!" sobre un sitio de terrorismo internacional e información de armamentos, operando parte del tiempo en Florida.

Pregunta

¿Que consejo le das a nuestros lectores para protegerse de los hackeos?

CapZap

Debido al punto de vista anticuado de las compañías sobre temas de seguridad, los programas estáticos y el presupuesto, es necesario para todas ellas examinar las necesidades de seguridad sobre una base dinámica por lo menos con una frecuencia de cuatro meses. Los usuarios y los sistemas se desarrollan dinámicamente y siempre cambian. Recomiendo que se establezcan los puntos de vista de un hacker para atacar sistemas, cada día checar las herramientas disponibles en la red, tener una persona dedicada exclusivamente a la investigación de seguridad, buscando formas de romper cualquier sistema de la empresa. Esto incluye sistemas, soporte, estructura o cualquier forma de conexión con el mundo real. Los sistemas hidráulicos, físicos, electrónicos, plantas eléctricas, sistemas de respaldo, telecomunicaciones, administración y destrucción de información confidencial, y cualquier otra cosa que pueda ser utilizada como información, arma o material de inteligencia. Si uno no sabe contra que tiene que luchar, que es el mundo entero, entonces necesitas sentarte en una caja cerrar la tapa y morir.