# Seguridad de la Información

## TIPOS DE ATAQUE

### Scanning (Búsqueda)

El Scaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (scanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. Muchas utilidades de auditoría también se basan en este paradigma.

El Scaneo de puertos pertenece a la Seguridad Informática desde que era utilizado en los sistemas de telefonía. Dado que actualmente existen millones de números de teléfono a los que se pueden acceder con una simple llamada, la solución lógica (para encontrar números que puedan interesar) es intentar conectarlos a todos.

La idea básica es simple: llamar a un número y si el módem devuelve un mensaje de conectado, grabar el número. En otro caso, la computadora cuelga el teléfono y llama al siguiente número. Scanear puertos implica las mismas técnicas de fuerza bruta. Se envía una serie de paquetes para varios protocolos y se deduce que servicios están "escuchando" por las respuestas recibidas o no recibidas.

Existen diversos tipos de Scanning según las técnicas, puertos y protocolos explotados:

### TCP Connect() Scanning

Esta es la forma básica del scaneo de puertos TCP. Si el puerto está escuchando, devolverá una respuesta de éxito; cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con a él.

Las ventajas que caracterizan esta técnica es que no necesita de privilegios especiales y su gran velocidad.

Su principal desventaja es que este método es fácilmente detectable por el Administrador del sistema. Se verá un gran número de conexiones y mensajes de error para los servicios en los que se ha conseguido conectar la máquina que lanza el scanner e inmediatamente se ha desconectado.

### TCP SYN Scanning

Cuando dos procesos establecen una comunicación usan el modelo Cliente/Servidor para establecer la conexión. La aplicación del Servidor "escucha" todo lo que ingresa por los puertos. La identificación del Servidor se efectúa a través de la dirección IP del sistema en el que se ejecuta y del número de puerto del que depende para la conexión. El Cliente establece la conexión con el Servidor a través del puerto disponible para luego intercambiar datos.

La información de control llamada HandShake (saludo) se intercambia entre el Cliente y el Servidor para establecer un dialogo antes de transmitir datos.

Los "paquetes" o segmentos TCP tienen banderas que indican el estado del mismo.

El protocolo TCP de Internet, sobre el que se basa la mayoría de los servicios (incluyendo el correo electrónico, el web y el IRC) implica esta conexión entre dos máquinas. El establecimiento de dicha conexión se realiza mediante lo que se llama Three-Way Handshake ("conexión en tres pasos") ya intercambian tres segmentos. En forma esquemática se tiene:

1. El programa Cliente (C) pide conexión al Servidor (S) enviandole un segmento SYN (Synchronize Sequence Number). Este segmento le dice a S que C desea establecer una conexión.
2. S (si está abierto y escuchando) al recibir este segmento SYN (activa su indicador SYN) y envía una autentificación ACK de manera de acuse de recibo a C. Si S está cerrado envía un indicador RST.
3. C entonces ACKea (autentifica) a S. Ahora ya puede tener lugar la transferencia de datos.

Cuando las aplicaciones conectadas terminan la transferencia, realizaran otra negociación a tres bandas con segmentos FIN en vez SYN.

La técnica TCP SYN Scanning, se implementa un scaneo de "media-apertura", dado que nunca se abre una sesión TCP completa. Se envía un paquete SYN (como si se fuera a usar una conexión real) y se espera

por la respuesta. Al recibir un SYN/ACK se envía, inmediatamente, un RST para terminar la conexión y se registra este puerto como abierto.

La principal ventaja de esta técnica de escaneo es que pocos sitios están preparados para registrarlos. La desventaja es que en algunos sistemas Unix, se necesitan privilegios de Administrador para construir estos paquetes SYN.

## TCP FIN Scanning- Stealth Port Scanning

Hay veces en que incluso el scaneo SYN no es lo suficientemente "clandestino" o limpio. Algunos sistemas (Firewalls y filtros de paquetes) monitorizan la red en busca de paquetes SYN a puertos restringidos. Para subsanar este inconveniente los paquetes FIN, en cambio, podrían ser capaces de pasar sin ser advertidos. Este tipo de Scaneo está basado en la idea de que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente. Los puertos abiertos, en cambio, suelen ignorar el paquete en cuestión.

Este es un comportamiento correcto del protocolo TCP, aunque algunos sistemas (entre los que se hallan los de Microsoft(r)) no cumplen con este requerimiento, enviando paquetes RST siempre, independientemente de si el puerto está abierto o cerrado. Como resultado, no son vulnerables a este tipo de scaneo. Sin embargo, es posible realizarlo en otros sistemas Unix.

Este último es un ejemplo en el que se puede apreciar que algunas vulnerabilidades se presentan en las aplicación de tecnologías (en este caso el protocolo TCP nacido en los años ´70) y no sobre sus implementaciones. Es más, se observa que una implementación incorrecta (la de Microsoft(r)) soluciona el problema. "Muchos de los problemas globales de vulnerabilidades son inherentes al disño original de algunos protocolos".

## Fragmentation Scanning

Esta no es una nueva técnica de scaneo como tal, sino una modificación de las anteriores. En lugar de enviar paquetes completos de sondeo, los mismos se particionan en un par de pequeños fragmentos IP. Así, se logra partir una cabecera IP en distintos paquetes para hacerlo más difícil de monitorizar por los filtros que pudieran estar ejecutándose en la máquina objetivo.

Sin embargo, algunas implementaciones de estas técnicas tienen problemas con la gestión de este tipo de paquetes tan pequeños, causando una caída de rendimiento en el sistema del intruso o en el de la víctima. Problemas de esta índole convierte en detectables a este tipo de ataque.

## Eavesdropping-Packet Sniffing

Muchas redes son vulnerables al Eavesdropping, o a la pasiva intercepción (sin modificación) del tráfico de red. Esto se realiza con Packet Sniffers, los cuales son programas que monitorean los paquetes que circulan por la red. Los Sniffers pueden ser colocado tanto en una estación de trabajo conectada a la red, como a un equipo Router o a un Gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

En la cabecera de los paquetes enviados a través de una red, entre otros datos, se tiene, la dirección del emisor y la del destinatario. De esta forma, independientemente de protocolo usado, las tramas llegan a su destino. Cada maquina conectada a la red (mediante una placa con una dirección única) verifica la dirección destino del paquete. Si estas direcciones son iguales asume que el paquete enviado es para ella, caso contrario libera el paquete para que otras placas lo analicen.

Un Sniffers consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el Sniffer).Inicialmente este tipo de software, era únicamente utilizado por los Administradores de redes locales, aunque con el tiempo llegó a convertirse en una herramienta muy usada por los intrusos.

Actualmente existen Sniffers para capturar cualquier tipo de información específica. Por ejemplo passwords de un recurso compartido o de acceso a una cuenta, que generalmente viajan sin encriptar al ingresar a sistemas de acceso remoto. También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mails entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos. Para realizar estas funciones se analizan las tramas de un segmento de red, y presentan al usuario sólo las que interesan.

Normalmente, los buenos Sniffers, no se pueden detectar, aunque la inmensa mayoría, y debido a que están demasiado relacionados con el protocolo TCP/IP, si pueden ser detectados con algunos trucos.

## Snooping-Downloading

Los ataques de esta categoría tienen el mismo objetivo que el Sniffing: obtener la información sin modificarla.

Sin embargo los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos mas resonantes de este tipo de ataques fueron: el robo de un archivo con mas de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

# ATAQUES DE AUTENTIFICACIÓN

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

## Spoofing-Looping

Spoofing puede traducirse como "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping o Tampering (ver a continuación Ataques de Modificación y Daño). Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping, y tiene la finalidad de "evaporar" la identificación y la ubicación del atacante.

El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del Looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un Insider, o por un estudiante a miles de Km de distancia, pero que ha tomado la identidad de otros.

La investigación de procedencia de un Looping es casi imposible, ya que el investigador debe contar con la colaboración de cada Administrador de cada red utilizada en la ruta. El envío de falsos e-mails es otra forma de Spoofing que las redes permiten. Aquí el atacante envía E-Mails a nombre de otra persona con cualquier motivo y objetivo. Tal fue el caso de una universidad en EE.UU. que en 1998, que debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina de estudiantes.

Muchos ataques de este tipo comienzan con Ingeniería Social y los usuarios, por falta de cultura, facilitan a extraños sus identificaciones dentro del sistema usualmente través de una simple llamada telefónica.

## Spoofing

Este tipo de ataques (sobre protolocos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing IP Spoofing

### IP Spoofing

Con el IP Spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete. Su utilización más común es enviar los paquetes con la dirección de un tercero, de forma que la víctima "ve" un ataque proveniente de esa tercera red, y no la dirección real del intruso. El esquema con dos puentes es el siguiente:

Nótese que si la víctima descubre el ataque verá a la PC 3 como su atacante y no el verdadero origen. Este ataque se hizo famoso al usarlo Kevin Mitnick

### DNS Spoofing

Este ataque se consigue mediante la manipulación de paquetes UDP pudiéndose comprometer el servidor

de nombres de dominios (Domain Name Server-DNS) de Windows NT(c). Si se permite el método de recursión en la resolución de "Nombre"Dirección IP" en el DNS, es posible controlar algunos aspectos del DNS remoto. La recursión consiste en la capacidad de un servidor de nombres para resolver una petición de dirección IP a partir de un nombre que no figura en su base de datos. Este es el método típico (y por defecto) de funcionamiento.

### Web Spoofing

En el caso Web Spoofing el atacante crea un sitio web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorizar todas las acciones de la víctima, desde sus datos hasta las passwords, números de tarjeta de créditos, etc. El atacante también es libre de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

## IP Splicing-Hijacking

Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la víctima se identifique ante el sistema y tras ello le suplanta como usuario autorizado.

## Utilización de BackDoors

"Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo".

Esta situación se convierte en una falla de seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

## Utilización de Exploits

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrado un error en los programas utilizados.

Los programas para explotar estos "agujeros" reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo. Nuevos Exploits (explotando nuevos errores en los sistemas) se publican cada día por lo que mantenerse informado de los mismos y de las herramientas para combatirlos es de vital importancia.

## Obtención de Passwords

Este método comprende la obtención por "Fuerza Bruta" de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc. atacados. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia. En esta caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta. La política de administración de password será discutida en capítulos posteriores.

## Uso de Diccionarios

Los Diccionarios son archivos con millones de palabras, las cuales pueden ser passwords utilizadas por los usuarios. Este archivo es utilizado para descubrir dicha password en pruebas de fuerza bruta. El programa encargado de probar cada una de las palabras encripta cada una de ellas (mediante el algoritmo utilizado por el sistema atacado) y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema mediante el usuario correspondiente a la clave hallada. Actualmente es posible encontrar diccionarios de gran tamaño orientados, incluso, a un área específico de acuerdo al tipo de organización que se este atacando.

En la siguiente tabla podemos observar el tiempo de búsqueda de una clave de acuerdo a su longitud y tipo de caracteres utilizados. La velocidad de búsqueda se supone en 100.000 passwords por segundo (este número suele ser mucho mayor dependiendo del programa utilizado). Aquí puede observarse la importancia e la utilización de passwords con 8 caracteres de longitud (al menos) y con todos los caracteres disponibles.

# DENIAL OF SERVICE (DOS)

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

## Jamming o Flooding

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

Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (usando Spoofing y Looping). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas. Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Muchos Hosts de Internet han sido dados de baja por el "ping de la muerte" (una versión-trampa del comando ping). Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el bloqueo instantáneo del equipo. Esta vulnerabilidad ha sido ampliamente utilizada en el pasado pero, aún hoy pueden encontrarse sistemas vulnerables. Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los sistemas destinos.

## Syn Flood

Como ya se explicó en el TCP SYN Scanning el protocolo TCP se basa en una conexión en tres pasos. Si el paso final no llega a establecerse, la conexión permanece en un estado denominado "semiabierto". El Syn Flood es el más famoso de los ataques del tipo Denial of Service, publicado por primera vez en la revista Phrack. Se basa en un "saludo" incompleto entre los dos hosts. El Cliente envía un paquete SYN pero no responde al paquete ACK ocasionando que la pila TCP/IP espere cierta cantidad de tiempo a que el host hostil responda antes de cerrar la conexión. Si se crean muchas peticiones incompletas de conexión (no se responde a ninguna), el Servidor estará inactivo mucho tiempo esperando respuesta. Esto ocasiona la lentitud en los demás servicios.

El problema es que muchos sistemas operativos tienen un límite muy bajo en el número de conexiones "semiabiertas" que pueden manejar en un momento determinado. Si se supera ese límite, el servidor sencillamente dejará de responder a las nuevas peticiones de conexión que le vayan llegando. Las conexiones "semiabiertas" van caducando tras un tiempo, liberando "huecos" para nuevas conexiones, pero mientras el atacante mantenga el Syn Flood, la probabilidad de que una conexión recién liberada sea capturada por un nuevo SYN malicioso es muy alta.

La potencia de este ataque reside en que muchos sistemas operativos fijan un límite del orden de 5 a 30 conexiones "semiabiertas", y que éstas caducan alcabo de un par de minutos. Para mantener el servidor fuera de servicio, un atacante sólo necesita enviar un paquete SYN cada 4 segundos (algo al alcance de, incluso, un módem de 300 baudios). Este ataque suele combinarse también con el IP Spoofing, de forma de ocultar el origen del ataque.

## Connection Flood

La mayoría de las empresas que brindan servicios de Internet (ISP) tienen un límite máximo en el número de conexiones simultaneas. Una vez que se alcanza ese límite, no se admitirán conexiones nuevas. Así, por ejemplo, un servidor Web puede tener, por ejemplo, capacidad para atender a mil usuarios simultáneos. Si un atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, (como ocurre con el caso del Syn Flood) para mantener fuera de servicio el servidor.

## 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, de forma continua. Si se descuelga el teléfono (para que deje de molestar), tampoco se puede recibir llamadas de otras personas. Este problema

es habitual, por ejemplo, cuando alguien intenta mandar un fax empleando el número de voz: el fax insiste durante horas y sin que el usuario llamado pueda hacer nada al respecto.

En el caso de Net Flooding ocurre algo similar. El atacante envía tantos paquetes de solicitud de conexión que las conexiones auténticas simplemente no pueden competir. En casos así el primer paso a realizar es el ponerse en contacto con el Proveedor del servicio para que intente determinar la fuente del ataque y, como medida provisional, filtre el ataque en su extremo de la línea. El siguiente paso consiste en localizar las fuentes del ataque e informar a sus 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, ya que en muchos casos la fuente del ataque es, a su vez, víctima y el origen último puede ser prácticamente imposible de determinar.

### Land Attack

Este ataque consiste en un Bug (error) en la implementación de la pila TCP/IP de las plataformas Windows(c). El ataque consiste en mandar a algún puerto abierto de un servidor (generalmente al 113 o al 139) un paquete, maliciosamente construido, con la dirección y puerto origen igual que la dirección y puerto destino. Por ejemplo se envían un mensaje desde la dirección 10.0.0.1:139 hacia ella misma. El resultado obtenido es que luego de cierta cantidad de mensajes enviados-recibidos la máquina termina colgándose.

Existen ciertas variantes a este método consistente, por ejemplo, en enviar el mensaje a una dirección específica sin especificar el puerto Smurf o Broadcast Storm. Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones para a continuación mandar una petición ICMP (simulando un Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen. Este paquete maliciosamente manipulado, será repetido en Broadcast, y cientos ó miles de hosts (según la lista de direcciones de Broadcast disponible) mandarán una respuesta a la víctimacuya dirección IP figura en el paquete ICMP.

### Supernuke o Winnuke

Un ataque característico (y quizás el más común) de los equipos con Windows(c) es el Nuke, que hace que los equipos que escuchan por el puerto UDP 137 a 139 (utilizados por los protocolos Netbios de Wins), queden fuera de servicio (o disminuyan su rendimientos) al enviarle paquetes UDP manipulados. Generalmente se envían fragmentos de paquetes, que la máquina víctima detecta como inválidos pasando a un estado inestable.

### Teardrop I y II-Newtear-Bonk-Boink

Al igual que el Supernuke, los ataques Teardrop I y Teardrop II afectan a fragmentos de paquetes. Algunas implementaciones de colas IP no vuelven a armar correctamente los fragmentos que se superponen, haciendo que el sistema se cuelgue. Windows NT(c) 4.0 de Microsoft(r) es especialmente vulnerable a este ataque. Aunque existen Patchs (parches) que pueden aplicarse para solucionar el problema, muchas organizaciones no lo hacen, y las consecuencias pueden devastadoras.

Los ataque tipo Teardrop son especialmente peligrosos ya que existen multitud de implementaciones (algunas de ellas forman paquetes), que explotan esta debilidad. Las más conocidas son aquellas con el nombre Newtear, Bonk y Boink.

### E-Mail Bombing-Spamming

El E-Mail Bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando así mailbox del destinatario.El Spamming, en cambio se refiere a enviar el e-mail miles de usuarios, hayan estos solicitados el mensaje o no. Es muy utilizado por las empresas para publicitar sus productos. El Spamming esta siendo actualmente tratado por las leyes europeas como una violación de los derechos de privacidad del usuario.

# ATAQUES DE MODIFICACIÓN-DAÑO

### Tampering o Data Diddling

Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos). Son particularmente serios cuando el que lo realiza ha obtenido derechos de Administrador o Supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema. Aún así, si no hubo intenciones de "bajar" el sistema por parte del atacante; el Administrador posiblemente necesite darlo de

baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada. Como siempre, esto puede ser realizado por Insiders o Outsiders, generalmente con el propósito de fraude o de dejar fuera de servicio a un competidor.

Son innumerables los casos de este tipo: empleados (o externos) bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule una deuda impositiva. Múltiples Web Sites han sido víctimas del cambio en sus páginas por imágenes (o manifiestos) terroristas o humorísticos, como el ataque de The Mentor, ya visto, a la NASA. Otras veces se reemplazan versiones de software por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos, etc.). La utilización de programas troyanos y difusión de virus esta dentro de esta categoría, y se profundizará sobre el tema en otra sección el presente capítulo.

## Borrado de Huellas

El borrado de huellas es una de las tareas mas importantes que debe realizar el intruso después de ingresar en un sistema, ya que si se detecta su ingreso el Administrador buscará como conseguir "tapar el hueco" de seguridad, evitar ataques futuros e incluso rastrear al atacante. Las Huellas son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en Logs (archivo que guarda la información de lo que se realiza en el sistema) por el sistema operativo. Los archivos Logs son una de la principales herramientas (y el principal enemigo del atacante) con las que cuenta un Administrador para conocer los detalles de las tareas realizadas en el sistema y la detección de intrusos

## Ataques Mediante Java Applets

Java es un lenguaje de programación interpretado desarrollado inicialmente por SUN. Su mayor popularidad la merece en su alto grado de seguridad. Los más usados navegadores actuales, implementan Máquinas Virtuales Java (MVJ) para ser capaces de ejecutar programas (Applets) de Java. Estos Applets, al fin y al cabo no son más que código ejecutable y como tal, susceptible de ser manipulado por intrusos. Sin embargo, partiendo del diseño, Java siempre ha pensado en la seguridad del sistema. Las restricciones a las que somete a los Applets son de tal envergadura (imposibilidad de trabajar con ficheros a no ser que el usuario especifique lo contrario, imposibilidad de acceso a zonas de memoria y disco directamente, firma digital, etc.) que es muy difícil lanzar ataques. Sin embargo, existe un grupo de expertos especializados en descubrir fallas de seguridad en las implementaciones de las MVJ.

## Ataques Mediante JavaScript y VBScript

JavaScript (de empresa Netscape(r)) y VBScript (de Microsoft(r)) son dos lenguajes usados por los diseñadores de sitios Web evitando el uso de Java. Los programas realizados son interpretados por el navegador. Aunque los fallos son mucho más numerosos en versiones antiguas de JavaScript, se pueden encontrar algunos de los siguientes:

- Cuando apareció JavaScript, éste permitía el envío de mensajes de correo electrónico sin el reconocimiento del usuario, la lectura del historial de páginas visitadas, la lectura de directorios y de archivos. Estas fueron razón más que suficiente para que cientos de intrusos informáticos se aprovecharan de estas debilidades.
- El problema más importante apareció en Netscape 2.0 y fue bautizado como "Stuck On Load". Lo que sucedía es que se podía crear una ventana de 1*1 pixeles, por la cual los intrusos podían seguir extrayendo información sin que el usuario se enterase y aún cuando éste hubiese salido de la página, ya que esta ventana (un simple punto en la pantalla) era imperceptible para el usuario.

## Ataques Mediante ActiveX

ActiveX es una de las tecnologías más potentes que ha desarrollado Microsoft(r). Mediante ActiveX es posible reutilizar código, descargar código totalmente funcional de un sitio remoto, etc. Esta tecnología es considerada la respuesta de Microsoft(r) a Java. ActiveX soluciona los problemas de seguridad mediante certificados y firmas digitales. Una Autoridad Certificadora (AC) expende un certificado que acompaña a los controles activos y a una firma digital del programador. Cuando un usuario descarga una página con un control, se le preguntará si confía en la AC que expendió el certificado y/o en el control ActiveX. Si el usuario acepta el control, éste puede pasar a ejecutarse sin ningún tipo de restricciones (sólo las propias que tenga el usuario en el sistema operativo). Es decir, la responsabilidad de la seguridad del sistema se deja en manos del usuario, ya sea este un experto cibernauta consciente de los riesgos que puede acarrear la acción o un perfecto novato en la materia.

Esta última características es el mayor punto débil de los controles ActiveX ya que la mayoría de los usuarios aceptan el certificado sin siquiera leerlo, pudiendo ser esta la fuente de un ataque con un control

dañino.

La filosofía ActiveX es que las Autoridades de Certificación se fían de la palabra del programador del control. Es decir, el programador se compromete a firmar un documento que asegura que el control no es nocivo. Evidentemente siempre hay programadores con pocos escrúpulos o con ganas de experimentar. Así, un conocido grupo de hackers alemanes, desarrolló un control ActiveX maligno que modificaba el programa de Gestión Bancaria Personal Quicken95(c) de tal manera que si un usuario aceptaba el control, éste realizaba la tarea que supuestamente tenía que hacer y además modificaba el Quicken, para que la próxima vez que la víctima se conectara a su banco, se iniciara automáticamente una transferencia a una cuenta del grupo alemán.

Otro control ActiveX muy especialmente "malévolo" es aquel que manipula el código de ciertos exploradores, para que éste no solicite confirmación al usuario a la hora de descargar otro control activo de la Web. Es decir, deja totalmente descubierto a ataques con tecnología ActiveX el sistema de la víctima. La autentificación de usuarios mediante Certificados y las Autoridades Certificadoras será abordada con profundidad en capítulos posteriores.

### Ataques por Vulnerabilidades en los Navegadores

Generalmente los navegadores no fallan por fallos intrínsecos, sino que fallan las tecnologías que implementan, aunque en este punto analizaremos realmente fallos intrínsecos de los navegadores, como pueden ser los "Buffer Overflow". Los "Buffer Overflows" consisten en explotar una debilidad relacionada con los buffers que la aplicación usa para almacenar las entradas de usuario. Por ejemplo, cuando el usuario escribe una dirección en formato URL ésta se guarda en un buffer para luego procesarla. Si no se realizan las oportunas operaciones de comprobación, un usuario podría manipular estas direcciones.

Los protocolo usado pueden ser HTTP, pero también otros menos conocidos, internos de cada explorador, como el "res:" o el "mk:". Precisamente existen fallos de seguridad del tipo "Buffer Overflow" en la implementación de estos dos protocolos. Para poder lanzar este tipo de ataques hay que tener un buen conocimiento de lenguaje Assembler y de la estructura interna de la memoria del Sistema Operativo utilizado. También se puede citar el fallo de seguridad descubierto por Cybersnot Industries(r) relativo a los ficheros ".lnk" y ".url"de Windows 95(c) y NT(c) respectivamente. Algunas versiones de Microsoft Internet Explorer(c) podían ser utilizadas para ejecutar la aplicación que se deseara siempre que existiera en el ordenador de la víctima (por ejemplo el tan conocido y temido format.com).

Para más información relacionada con los ataques intrínsecos a los navegadores, se aconsejan las páginas no oficiales de seguridad tanto en Internet Explorer(c) como en Netscape Communicator(c).

### EXPLOTACIÓN DE ERRORES DE DISEÑO, IMPLEMENTACIÓN Y OPERACIÓN

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" son descubiertas (cada día) en sistemas operativos, aplicaciones de software, protocolos de red, browsers de Internet, correo electrónico y todas clase de servicios informático disponible.

Los Sistemas operativos abiertos (como Unix y Linux) tienen agujeros mas conocidos y controlados que aquellos que existen en sistemas operativos cerrados (como Windows(c)). La importancia (y ventaja) del código abierto radica en miles de usuarios analizan dicho código en busca de posibles bugs y ayudan a obtener soluciones en forma inmediata.

Constantemente encontramos en Internet avisos de nuevos descubrimientos de problemas de seguridad (y herramientas de Hacking que los explotan), por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades, puedan diagnosticarlas y actualizar el programa afectado con el parche adecuado.

# ENCRIPTACION, CLAVE PUBLICA Y CLAVE PRIVADA

## Como funciona la encriptación

El increíble crecimiento de Internet ha excitado a gente de negocios y consumidores con la promesa de cambiar el modo de trabajar e incluso de vida. Sin embargo, paralelo a esta forma nueva forma de hacer transacciones comerciales, existe una preocupación sobre lo seguro que es Internet, especialmente cuando se manda información privada o sensitiva en la red.

Tenemos que reconocerlo, existe muchos tipos de información que no queremos que otros vean, como pueden ser:

- Información de tarjetas de crédito.
- Números de la seguridad social.
- Correspondencia privada.
- Datos personales.
- Información sensitiva de una compañía o empresa.
- Información de datos bancarios.

La seguridad en la red es ofrecida entre ordenadores por Internet mediante una variedad de métodos. Uno de los modos más básicos y simples que se han utilizado siempre, es tener esta información privilegiada en dispositivos de almacenamiento, como pueden ser disquetes, CD o más actualmente DVD. Hoy en día, este método es insuficiente y por ello los métodos de seguridad más populares utilizan la encriptación, el cual es el proceso de codificar la información de tal manera, que solo la persona (u ordenador) con una clave determinada, puede decodificarla y hacer uso de dicha información.

# Sistemas de encriptación

La encriptación en ordenadores, está basada en la ciencia de la criptología, que ha sido usada a través de la historia con frecuencia. Antes de la era digital, los que más hacían uso de la criptología, eran los gobiernos, particularmente para propósitos militares. La existencia de mensajes codificados han sido verificados desde los tiempos del imperio romano. Hoy en día, la mayoría de los sistemas de criptografía son aplicables a ordenadores, simplemente porque la complejidad de los algoritmos es demasiada para ser calculada por seres humanos.

Muchos de los sistemas de encriptación pertenecen a dos categorías:

- Encriptación de clave simétrica.
- Encriptación de clave pública.

## Clave simétrica

En este tipo de encriptación, cada ordenador tiene una clave secrete (como si fuera una llave) que puede utilizar para encriptar un paquete de información antes de ser enviada sobre la red a otro ordenador. Las claves simétricas requieren que sepas los ordenadores que van a estar hablando entre si para poder instalar la clave en cada uno de ellos.

Podemos entender una clave simétrica, como un código secreto que deben saber los ordenadores que se están comunicando para poder decodificar la información a su llegada. Como ejemplo sencillo, imagina que envías un mensaje otra persona pero sustituyes ciertas letras por signos como asteriscos o interrogaciones. La persona que recibe el mensaje sabe de antemano que letras en particular han sido sustituidas con esos signos por lo que volviendo a ponerlas en su sitio, podrá leer el mensaje. Para los demás, la información no tendrá ningún sentido.

## Clave pública

Este método usa una combinación de una clave privada y una clave pública. La clave privada solo la sabe tu ordenador, mientras que la clave pública es entregada por tu ordenador a cualquier otros ordenador que quiere realizar una comunicación con el. Para decodificar un mensaje encriptado, un ordenador debe hacer uso de la clave pública, entregada por el ordenador original, y su propia clave privada.

Una clave pública de encriptación muy popular es PGP (Pretty good Privacy) que permite encriptar casi todo.

Para implementar la encriptación de clave pública a gran escala, como puede ser un servidor Web, se necesita realizar otra aproximación. Aquí es donde entran los certificados digitales. La autoridad certificada actúa como un intermediario en el que ambos ordenadores confían. Confirma que cada ordenador es en realidad quién dice que es, y entonces provee las claves públicas de un ordenador a otro.

## Clave pública: SSL

Una implementación de la encriptación de clave pública es SSL (Secure Sockets Layer). Originalmente desarrollada por Netscape, SSL es un protocolo de seguridad para Internet usado por navegadores y

servidores Web para transmitir información sensitiva. SSL se ha convertido en parte de un protocolo de seguridad general llamado TLS (Transport Layer Security).

En tu navegador, puedes saber si estás usando un protocolo de seguridad, como TLS por ejemplo, de varias formas. Podrás ver que en la barra de direcciones, las primeras letras “http”, serán reemplazadas con “https”, y podrás ver un pequeño cerrojo en la barra de estado en la parte inferior del navegador.

La encriptación de clave pública conlleva mucha computación, por lo que muchos sistemas usan una combinación de clave pública y simetría. Cuando dos ordenadores inician una sesión segura, un ordenador crea una clave simétrica y la envía al otro ordenador usando encriptación de clave pública. Los dos ordenadores pueden entonces comunicarse entre ellos usando una encriptación de clave simétrica. Una vez que la sesión ha finalizado, cada ordenador descarta la clave simétrica usada para esa sesión. Cualquier sesión adicional requiere que una nueva clave simétrica sea creada, y el proceso es repetido.

### Algoritmos de encriptación “hashing”

La clave en una encriptación de clave pública está basada en un valor llamado hash. Este valor está computado a partir de un número usando un algoritmo llamado hashing. En esencia, este valor es una modificación del valor original. Lo más importante de un valor hash es que es casi imposible conocer el valor original sin saber los datos que se utilizaron para crear el valor hash.

## Autenticación

Este proceso, es otro método para mantener una comunicación seguro entre ordenadores. La autenticación es usada para verificar que la información viene de una fuente de confianza. Básicamente, si la información es autentica, sabes quién la ha creado y que no ha sido alterada. La encriptación y la autenticación, trabajan mano a mano para desarrollar un entorno seguro.

Hay varias maneras para autenticar a una persona o información en un ordenador:

- **Contraseñas** – El uso de un nombre de usuario y una contraseña provee el modo más común de autenticación. Esta información se introduce al arrancar el ordenador o acceder a una aplicación. Se hace una comprobación contra un fichero seguro para confirmar que coinciden, y si es así, se permite el acceso.
- **Tarjetas de acceso** – Estas tarjetas pueden ser sencillas como si de una tarjeta de crédito se tratara, poseyendo una banda magnética con la información de autenticación. Las hay más sofisticadas en las que se incluye un chip digital con esta información.
- **Firma digital** – Básicamente, es una manera de asegurar que un elemento electrónico (email, archivo de texto, etc.) es autentico. Una de las formas más conocidas es DSS (Digital Signature Standard) la cual está basada en un tipo de encriptación de clave pública la cual usa DSA (Digital Signature Algorithm). El algoritmo DSA consiste en una clave privada, solo conocida por el que envía el documento (el firmante), y una clave pública. Si algo es cambiado en el documento después de haber puesto la firma digital, cambia el valor contra lo que la firma digital hace la comparación, invalidando la firma.

Recientemente, otros métodos de autenticación se están haciendo populares en varios medios que deben mantenerse seguros, como son el escaneo por huellas, de retina, autenticación facial o identificación de voz.

# ¿Qué son los virus, gusanos y troyanos?

Los virus, gusanos y troyanos son programas malintencionados que pueden provocar daños en el equipo y en la información del mismo. También pueden hacer más lento Internet e, incluso, pueden utilizar su equipo para difundirse a amigos, familiares, colaboradores y el resto de la Web. La buena noticia es que con un poco de prevención y algo de sentido común, es menos probable ser víctima de estas amenazas.

## ¿Qué es un virus?

Un virus es código informático que se adjunta por sí mismo a un programa o archivo para propagarse de un equipo a otro. Infecta a medida que se transmite. Los virus pueden dañar el software, el hardware y los archivos.

El virus es un código escrito con la intención expresa de replicarse. Un virus se adjunta a sí mismo a un programa host y, a continuación, intenta propagarse de un equipo a otro. Puede dañar el hardware, el

software o la información.

Al igual que los virus humanos tienen una gravedad variable, desde el virus Ébola hasta la gripe de 24 horas, los virus informáticos van desde molestias moderadas hasta llegar a ser destructivos. La buena noticia es que un verdadero virus no se difunde sin la intervención humana. Alguien debe compartir un archivo o enviar un mensaje de correo electrónico para propagarlo.

## ¿Qué es un gusano?

Un gusano, al igual que un virus, está diseñado para copiarse de un equipo a otro, pero lo hace automáticamente. En primer lugar, toma el control de las características del equipo que permiten transferir archivos o información. Una vez que un gusano esté en su sistema, puede viajar solo. El gran peligro de los gusanos es su habilidad para replicarse en grandes números. Por ejemplo, un gusano podría enviar copias de sí mismo a todos los usuarios de su libreta de direcciones de correo electrónico, lo que provoca un efecto dominó de intenso tráfico de red que puede hacer más lentas las redes empresariales e Internet en su totalidad. Cuando se lanzan nuevos gusanos, se propagan muy rápidamente. Bloquean las redes y posiblemente provocan esperas largas (a todos los usuarios) para ver las páginas Web en Internet.

El gusano es una subclase de virus. Por lo general, los gusanos se propagan sin la intervención del usuario y distribuye copias completas (posiblemente modificadas) de sí mismo por las redes. Un gusano puede consumir memoria o ancho de banda de red, lo que puede provocar que un equipo se bloquee.

Debido a que los gusanos no tienen que viajar mediante un programa o archivo "host", también pueden crear un túnel en el sistema y permitir que otro usuario tome el control del equipo de forma remota. Entre los ejemplos recientes de gusanos se incluyen: Sasser y Blaster.

## ¿Qué es un troyano?

Del mismo modo que el caballo de Troya mitológico parecía ser un regalo pero contenía soldados griegos que dominaron la ciudad de Troya, los troyanos de hoy en día son programas informáticos que parecen ser software útil pero que ponen en peligro la seguridad y provocan muchos daños. Un troyano reciente apareció como un mensaje de correo electrónico que incluye archivos adjuntos que aparentaban ser actualizaciones de seguridad de Microsoft, pero que resultaron ser virus que intentaban deshabilitar el software antivirus y de servidor de seguridad.

El troyano es un programa informático que parece ser útil pero que realmente provoca daños.

Los troyanos se difunden cuando a los usuarios se les engaña para abrir un programa porque creen que procede de un origen legítimo. Para proteger mejor a los usuarios, Microsoft suele enviar boletines de seguridad por correo electrónico, pero nunca contienen archivos adjuntos. También publicamos todas nuestras alertas de seguridad en nuestro sitio Web de seguridad antes de enviarlas por correo electrónico a nuestros clientes.

Los troyanos también se pueden incluir en software que se descarga gratuitamente. Nunca descargue software de un origen en el que no confíe. Descargue siempre las actualizaciones y revisiones de Microsoft de los sitios Microsoft Windows Update o Microsoft Office Update.

## ¿Cómo se transmiten los gusanos y otros virus?

Prácticamente todos los virus y muchos gusanos no se pueden transmitir a menos que se abra o se ejecute un programa infectado.

Muchos de los virus más peligrosos se difundían principalmente mediante archivos adjuntos de correo electrónico, los archivos que se envían junto con un mensaje de correo electrónico. Normalmente se puede saber que el correo electrónico incluye un archivo adjunto porque se muestra el icono de un clip que representa el archivo adjunto e incluye su nombre. Algunos tipos de archivos que se pueden recibir por correo electrónico habitualmente son fotos, cartas escritas en Microsoft Word e, incluso, hojas de cálculo de Excel. Un virus se inicia al abrir un archivo adjunto infectado (normalmente se hace clic en el icono de archivo adjunto para abrirlo).

**Sugerencia**: Nunca abra nada que esté adjunto a un mensaje de correo electrónico a menos que espere el archivo y conozca el contenido exacto de dicho archivo.

Si recibe un correo electrónico con un archivo adjunto de un desconocido, elimínelo inmediatamente. Por desgracia, en ocasiones tampoco resulta seguro abrir archivos adjuntos de personas que conoce. Los virus y los gusanos tienen la capacidad de robar la información de los programas de correo electrónico y enviarse a todos los incluidos en la libreta de direcciones. Por lo tanto, si recibe un correo electrónico de alguien con

un mensaje que no entiende o un archivo que no esperaba, póngase siempre en contacto con la persona y confirme el contenido del archivo adjunto antes de abrirlo.

Otros virus se pueden propagar mediante programas que se descargan de Internet o de discos repletos de virus que dejan los amigos o incluso que se compran en una tienda. Existen formas menos habituales de contraer un virus. La mayoría de las personas se contagian de virus si abren y ejecutan archivos adjuntos de correo electrónico desconocidos.

## ¿Cómo puedo saber si tengo un gusano u otro virus?

Al abrir y ejecutar un programa infectado, es posible que no sepa que ha contraído un virus. Su equipo puede hacerse más lento o bloquearse y reiniciarse cada pocos minutos. En ocasiones, un virus ataca los archivos que necesita para iniciar un equipo. En este caso, puede presionar el botón de encendido y estar mirando una pantalla vacía.

Todos estos síntomas son signos habituales de que el equipo tiene un virus, aunque se pueden deber a problemas de hardware o software que nada tengan que ver con un virus.

Preste atención a los mensajes que indiquen que ha enviado correo electrónico con virus. Puede significar que el virus ha incluido su dirección de correo como el remitente de un correo electrónico infectado. Esto no significa necesariamente que tenga un virus. Algunos virus tienen la capacidad de falsificar las direcciones de correo electrónico.

A menos que tenga instalado software antivirus actualizado en el equipo, no existe un modo seguro de saber si tiene un virus. Si no dispone de software antivirus actual o si desea instalar otra marca de software antivirus, visite nuestra página de descargas de software de seguridad.

## Pasos para reducir el riesgo de virus

Nada puede garantizar la seguridad del equipo de forma absoluta. No obstante, puede reforzar la seguridad de su equipo si mantiene el software actualizado y mantiene una suscripción actualizada a un programa antivirus.

Las amenazas de seguridad recientes, como MyDoom, se han difundido por los mensajes de correo electrónico disfrazadas de mensajes de error de correo que parecían familiares. El archivo adjunto parecía ser el texto de un mensaje que podía haber enviado a una dirección errónea, pero al abrirlo era víctima del virus. No importa lo auténtico que pueda parecer un mensaje de correo electrónico, asegúrese de que conoce el contenido del archivo adjunto antes de abrirlo.

### Protección contra virus, gusanos y troyanos

Aunque los virus, los gusanos y los troyanos tienen características muy distintas, existen cuatro pasos para protegerse de todos ellos.

Paso 1: Nunca abra un archivo adjunto de correo electrónico de un desconocido.

Paso 2: Nunca abra un archivo adjunto de correo electrónico de alguien que conozca a menos que sepa exactamente qué es el archivo adjunto.

Paso 3: Mantenga siempre el software antivirus actualizado.

Paso 4: Mantenga el software actualizado con estos recursos en línea: