- Seguridad Informática - Métodos de ataque -

En los comienzos, los ataques involucraban poca sofisticación técnica. Los insiders (empleados disconformes o personas externas con acceso al sistema dentro de la empresa) utilizaban sus permisos para alterar archivos o registros.
Los outsiders (personas que atacan desde fuera de la organización) ingresaban a la red simplemente averiguando una contraseña válida.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque utilizando los "agujeros" en el diseño, configuración y operación de los sistemas. Esto permitió a los intrusos tomar control de sistemas completos, produciendo verdaderos desastres.

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

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

Eavesdropping y Packet Sniffing

Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red.
En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados.
El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet y esto puede ser realizado por un usuario con acceso legítimo o por un intruso que ha ingresado por otras vías.
Existen kits disponibles para facilitar su instalación.
Este método es muy utilizado para capturar loginIDs y contraseñas de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mail entrantes y salientes.
El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

Snooping y Downloading

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

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software.
Los casos mas notorios 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 guerra.

Tampering o Data Diddling

Esta categoría se refiere a la modificación desautorizada a los datos o al software instalado en un sistema, incluyendo borrado de archivos.

Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de ejecutar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.
Esto puede ser realizado por insiders o por outsiders, generalmente con el propósito de fraude o dejar fuera de servicio un competidor.

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

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

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

Spoofing
Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering.
Una forma común de spoofing, es conseguir el nombre y contraseña de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en su nombre, como puede ser el envío de falsos e-mails.
El intruso usualmente utiliza un sistema para obtener información e ingresar en otro y luego utiliza este para entrar en otro y en otro.
Este proceso, llamado Looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante.

El camino tomado desde el origen hasta el destino puede tener muchas estaciones que exceden obviamente los límites de un país.
Otra consecuencia del looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad 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.

El looping hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta que pueden ser de distintas jurisdicciones.

Los protocolos de red también son vulnerables al spoofing.
Con el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete.

El envío de falsos e-mails es otra forma de spoofing.
Aquí el atacante envía a nombre de otra persona e-mails con otros objetivos. Tal fue el caso de una universidad en USA que en 1998 debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina (163 estudiantes).

Muchos ataques de este tipo comienzan con ingeniería social y la falta de cultura por

parte de los usuarios para facilitar a extraños sus identificaciones dentro del sistema. Esta primera información es usualmente conseguida a través de una simple llamada telefónica.

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

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

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

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

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

Bombas Lógicas
Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificara la información o provocara la interrupción del sistema.

Ingeniera Social
Consiste, básicamente, en convencer a alguien de que haga lo que en realidad no debería. Por ejemplo llamar a un usuario haciéndose pasar por el administrador del sistema y requerirle la contraseña con alguna excusa convincente.

Difusion de Virus
Si bien es un ataque de tipo tampering, difiere de este porque puede ser ingresado al sistema por un dispositivo externo (diskettes) o través de la red (e-mails u otros protocolos) sin intervención directa del atacante.

Dado que el virus tiene como característica la autorreplicación, no necesita de mucha ayuda para propagarse a través de una LAN o WAN rápidamente, si es que no esta instalada una protección antivirus en los servidores y estaciones de trabajo.

Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (".exe", ".com", ".bat", etc) y los sectores de boot-particion de discos y diskettes, pero aquellos que causan mas problemas son los macro-virus que están ocultos en simples documentos o planilla de cálculo, aplicaciones que utiliza cualquier usuario de PC y cuya difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet.
Además, estos son multiplataforma, es decir, no están atados a un sistema operativo en particular, ya que un documento de MS-Word puede ser procesado tanto por un sistema operativo MS-Windows, como en una Macintosh u otras.

Cientos de virus son descubiertos regularmente y técnicas más complejas se desarrollan a una velocidad creciente a medida que el avance tecnológico permite la creación de nuevas puertas de entrada a los sistemas.
Por eso es indispensable contar con una herramienta antivirus actualizada y que pueda responder rápidamente ante cada nueva amenaza.

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