Tipos de ataques informáticos

Ángel García Illescas y Carmen Domínguez González

Índice

- **¿Qué es un ataque informático?**
- **Consecuencias**
- **Tipos de ataques informáticos**
- **Prevención de ataques**
- **Contrarrestar un ataque**
- **Biografía**

¿Qué es un ataque informático?

Un ataque informático es un intento organizado e intencionado causado por una o más personas para infringir daños o problemas a un sistema informático o red. Los ataques en grupo suelen ser hechos por bandas llamados "piratas informáticos" que suelen atacar para causar daño, por buenas intenciones, por espionaje, para ganar dinero, entre otras. Los ataques suelen pasar en corporaciones aunque también se puede llevar a cabo a particulares.

Un ataque informático consiste en aprovechar alguna debilidad o falla en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; para obtener un beneficio, por lo general de condición económica, causando un efecto negativo en la seguridad del sistema, que luego pasa directamente en los activos de la organización.

Consecuencias

Los ataques informáticos tienen varias series de consecuencias o daños que puede causar en un sistema operativo:

Daños triviales
En este tipo de daños causados por los virus son muy fáciles de remover y eliminar, por lo que se pueden quitar solo en segundos o minutos.

Daños menores
En este tipo de daños son causados por virus que como el virus Jerusalén, los viernes 13, borra todos los programas que uno trate de usar una vez haya infectado la memoria. Lo peor que puede suceder es que tocaría volver a instalar los programas borrados por dicho virus.

Daños moderados
Este daño sucede cuando un virus formatea el DISCO DURO, y mezcla los componentes del FAT (File Allocation Table), o también puede que sobreescriba el disco duro. Sabiendo esto se puede reinstalar el sistema operativo y usar el último backup. Esto llevará 1 hora aproximadamente.

Daños mayores
Algunos virus pueden pasar desapercibidos y pueden lograr que ni utilizando el backup se pueda llegar a los archivos. Un ejemplo es el virus Dark Avanger que infecta los archivos acumulando. Cuando llega a 16, el virus escoge un sector del disco duro al azar y en ella escribe: "Eddie lives... somewhere in time (Eddie vive... en algún lugar del tiempo) Cuando el usuario se percata de la existencia del virus ya será demasiado tarde pues los archivos más recientes estarán infectados con el virus.

Daños severos
Los daños severos son hechos cuando los virus hacen cambios mínimos y progresivos. El usuario no sabe cuando los datos son correctos o han cambiado, pues no se ve fácilmente, como en el caso del VIRUS Dark Avanger. También hay casos de virus que infectan aplicaciones que al ser

descontaminadas estas aplicaciones pueden presentar problemas o perder funcionalidad.

Daños ilimitados
Algunos programas como CHEEBA, VACSINA.44.LOGIN y GP1 entre otros, obtienen la clave del administrador del sistema, crean un nuevo usuario con el privilegio máximo poniendo el nombre del usuario y la clave. El daño lo causa la tercera persona, que ingresa al sistema y podría hacer lo que quisiera.

Tipos de ataques informáticos

Algunos ejemplos de los múltiples tipos de ataques que se pueden dar son:

Trashing (cartoneo):
Este ocurre generalmente cuando un usuario anota su login y password en un papel y luego, cuando lo recuerda, lo arroja a la basura. Esto por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar al sistema.

Monitorización:
Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro.

Ataques de autenticación:
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.(su forma más común es recibir un correo electrónico con un enlace de acceso directo falso de paginas que mas visitas)

Denial of Service(DoS):
Los protocolos existentes actualmente fueron diseñados para ser hechos 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 Denegación de Servicio(DoS) tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

Síntomas DoS:

-Rendimiento de la red inusualmente lento (abrir archivos o acceder a sitios web).
-Indisponibilidad de un sitio web en particular.
-Incapacidad para acceder a cualquier sitio web.
-Aumento dramático en la cantidad de spam que recibimos.

Algunos ataques DoS:

-Tear Drop Attack: Una serie de paquetes de datos se envían a la computadora destino con superposición de valores de campo y cargas útiles de gran tamaño. Como resultado, el

objetivo no puede volver a ensamblar estos paquetes y se fuerza a que se bloquee o incluso a reiniciar.

-Land Attack

El atacante envía un paquete TCP SYN falsificado en el que la dirección IP de el objetivo se completa en los campos de origen y destino. Al recibir el paquete falsificado, el objetivo se confunde y se bloquea.Estos tipos de ataques son detectados por Anti-virus.

Modificación (daño) se puede dar como:

→ *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).

→ *Borrado de Huellas:* El borrado de huellas es una de las tareas más importantes que debe realizar el intruso después de ingresar en un sistema, ya que, si se detecta su ingreso, el administrador buscará cómo conseguir "tapar el hueco" de seguridad, evitar ataques futuros e incluso rastrear al atacante.

Ataque de fuerza bruta:

No es necesariamente un procedimiento que se deba realizar por procesos informáticos, aunque este sistema ahorraría tiempos, energías y esfuerzos. El sistema de ataque por fuerza bruta, trata de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que se busca, y que permite el acceso al sistema, programa o archivo en estudio.

Cómo prevenir un Ataque de fuerza bruta por ejemplo en Wordpress:

-Deja de usar el nombre de usuario que viene por defecto “admin”.

- Utiliza una contraseña segura.

-Haz regularmente copias de seguridad de archivos y base de datos.

-Usa autenticación de dos factores.

-Protege con una contraseña el WP-Admin y limita los intentos de conexión.

-Usar el plugin Wordpress Security.

Ping Flood:

Se basa en enviar a la víctima una cantidad abrumadora de paquetes ping, usualmente usando el comando "ping" de UNIX como hosts (el indicador -t en los sistemas Windows tiene una función mucho menos maligna). Es muy simple de lanzar, el requisito principal es tener acceso a un ancho de banda mayor que la víctima.

Ping de la muerte:

El atacante envía un paquete ICMP de más de 65.536 bytes. Como el sistema operativo no sabe cómo manejar un paquete tan grande, se congela o se cuelga en el momento de volver a montarlo. Hoy en día, el sistema operativo descarta dichos paquetes por sí mismo.

Algunos ataques del tipo Ping de la muerte:

-Distributed Denial of Service (DDos): En un ataque distribuido de denegación de servicio (DDoS), un atacante puede usar su computadora para atacar a otra computadora. Al aprovechar las vulnerabilidades o debilidades de seguridad, un atacante podría tomar el control del PC / Servidor. Él o ella podría obligar al PC a enviar grandes cantidades de datos a un sitio web o enviar correo no deseado a direcciones de correo electrónico particulares. El ataque se "distribuye" porque el atacante está utilizando varios PCs, incluida la suya, para lanzar el ataque de denegación de servicio. Actualmente dichos ataques son lanzados desde las Botnet

Escaneo de puertos:

El escaneo de puertos es una de las técnicas de reconocimiento más populares que utilizan los atacantes para descubrir los servicios expuestos a posibles ataques. Todas las máquinas conectadas a una red de área local (LAN) o Internet ejecutan muchos servicios que escuchan en puertos conocidos y no tan conocidos. Un escaneo de puertos ayuda al atacante a encontrar qué puertos están disponibles (es decir, qué servicio podría estar enumerando un puerto).

Cómo prevenir el escaneo de puertos:

-Si tenemos un servidor de acceso público, el sistema será vulnerable a los escaneos de puertos. No hay una forma segura de vencer los escaneos de puertos. Los sistemas judiciales han determinado que realizar exploraciones de puertos no es ilegal. Los escaneos de puertos son ilegales solo si el atacante usa información de un escaneo de puertos para explotar una vulnerabilidad o abrir un puerto en el sistema.

-Una forma de limitar la información obtenida de escaneos de puertos es cerrar los servicios innecesarios en los sistemas de destino, es decir, si está ejecutando un servidor web, http debe ser el único servicio ofrecido. En los sistemas UNIX, la manera más fácil de limitar la información proporcionada a los escáneres de puertos es editar el /etc/inetd.conf y comentar cualquier servicio innecesario.

-También editar el /etc/init.d y el archivo de nivel de ejecución que el sistema está devolviendo. Eliminar los servicios innecesarios. Además, asegurarnos de que el sistema no se esté ejecutando en el modo X11. Si se está ejecutando en el modo X11, el sistema transmitirá el servicio 6000 ya sea que haya iniciado sesión o no.

-Otra forma de limitar la información proporcionada a los escáneres de puertos es emplear encapsuladores TCP, cuando corresponda. Los Contenedores TCP dan al administrador la flexibilidad de permitir o denegar el acceso a los servicios en base a las direcciones IP o nombres de dominio. Las cápsulas de TCP funcionan junto con el archivo /etc/inetd.conf. TCP Wrappers funciona invocando el tcpd daemon antes de proporcionar el servicio especificado. Cuando se detecta una solicitud entrante procedente de un puerto autorizado, los contenedores TCP verifican primero el archivo /etc/hosts.allow para ver si la dirección IP o el nombre de dominio tiene permisos para acceder al servicio. Si no se encuentra ninguna entrada, TCP Wrappers verificará el archivo /etc/hosts.deny. Si no se encuentra ninguna entrada allí, o si se encuentra la instrucción ALL: ALL, los Contenedores TCP ignorarán la solicitud y no permitirán que se utilice el servicio solicitado. Cuando se escanea el sistema ,

los contenedores TCP aún permitirán que se anuncie el servicio; sin embargo, el escáner no recibirá ninguna información adicional del puerto a menos que el escaneo provenga de un host o dominio especificado en /etc/hosts.allow. Cuando se escanea, el sistema mostrará el servicio como abierto. Cuando el atacante intenta explotar el puerto abierto, TCP Wrappers rechazará la conexión entrante si no proviene de un host o dominio aprobado. El inconveniente de TCP Wrappers es que no todos los servicios están cubiertos. Los servicios como http y smtp no están cubiertos, y si no están configurados correctamente, serán susceptibles de explotación. TCP Wrappers no es susceptible a la suplantación de IP. Cuando se detecta una solicitud entrante, TCP Wrappers realizará una búsqueda DNS inversa en la dirección IP solicitante. Si la búsqueda inversa coincide con la IP solicitante, los contenedores TCP permitirán la conexión. Si la búsqueda inversa falla, TCP Wrappers supondrá que se trata de un host no autorizado y no permitirá la conexión.

-Finalmente, otra forma de limitar la cantidad de información dada a los escaneos de puertos es utilizar productos como PortSentry ofrecido por Psionic. PortSentry detecta las solicitudes de conexión en una serie de puertos seleccionados. PortSentry es personalizable y se puede configurar para ignorar una cierta cantidad de intentos. El administrador puede seleccionar qué puertos escuchará PortSentry para las solicitudes de conexión y la cantidad de solicitudes no válidas. El administrador enumerará los puertos que su sistema no admite. Tras la detección, PortSentry empleará los contenedores TCP y realizará una entrada en el archivo /etc/hosts.deny para el sospechoso de intrusión. PortSentry también configurará una declaración de ruta predeterminada para el sistema infractor. La instrucción de ruta predeterminada encaminará todos los paquetes desde el sistema infractor a otro sistema o a un sistema inactivo. El resultado es que el sistema objetivo aparecerá como inexistente. En los sistemas Linux, PortSentry puede detectar todos los escaneos TCP y UDP, mientras que en los sistemas Solaris sólo pueden detectar los escaneos TCP Vanilla y UDP.

Root kit:

Es un tipo de software que está diseñado para obtener el control de nivel de administrador sobre un sistema informático sin ser detectado. En prácticamente todos los casos, el propósito y el motivo es realizar operaciones maliciosas en un sistema informático host objetivo en una fecha posterior sin el conocimiento de los administradores o usuarios de ese sistema. Los *Root kit* se pueden instalar en hardware o software dirigidos en la BIOS, hipervisores, cargadores de arranque, kernel, o con menor frecuencia, bibliotecas y/o aplicaciones.

Cómo prevenir el Root kit:

- Instalar un sistema de seguridad (antivirus y antimalware) que permite detectar amenazas incluso desconocidas y mantenerla siempre actualizada.

-Evitar abrir correos electrónicos de procedencia dudosa.

-No activar enlaces sospechosos en nuestro cliente de mensajería instantánea.

-Evitar descargar archivos de sitios web extraños o descargar archivos sospechosos.

-Actualizar regularmente todas las aplicaciones que se ejecutan en nuestro ordenador para evitar vulnerabilidades de seguridad.

-Realizar análisis y escaneos de seguridad con herramientas potentes y reconocidas de manera periódica para garantizar que nuestro equipo esté libre de rootkits.

Prevención de ataques

-Utilizar un antivirus que analice todas las descargas. Que esté actualizado al día para que reconozca el mayor número de virus, y realiza análisis regularmente de todo el sistema.

-Mantener el sistema operativo y el navegador actualizados. Los virus aprovechan los agujeros del SO y navegador para infectar los dispositivos. La mejor forma para estar protegido es activar las actualizaciones automáticas de tu SO, navegador, plugins del navegador y resto de aplicaciones.

-Cuidar las contraseñas. Al introducirlas se debe estar seguro de que es la página correcta, ya que puede parecer idéntica a la legítima y tratarse de una suplantación (phishing). No se debe utilizar la misma contraseña en diferentes servicios porque si acceden a una cuenta fácilmente podrán acceder al resto. Tampoco se ha de compartir las contraseñas con nadie, aunque digan que son del servicio técnico, los servicios respetables nunca solicitarán las contraseñas por propia iniciativa.
-Confiar en la web, pero no ser ingenuo. Permanecer alerta, no todo lo que se dice en Internet tiene por qué ser cierto. Ante la duda, contrastar la información en otras fuentes de confianza.

-No hacer clic en enlaces sospechosos. Los mensajes falsos pueden ser muy convincentes con el fin de captar la atención del usuario y redirigirte a páginas maliciosas.

-Tener cuidado con lo que se descarga. No hay que precipitarse y se debe descargar los ficheros solo de fuentes confiables y los programas desde sus páginas oficiales.

-Desconfiar de los correos de remitentes desconocidos. Ante la duda, es recomendable no responder a los mismos y eliminarlos directamente.

-No abrir ficheros adjuntos sospechosos. Si es de un conocido hay que asegurarse de que realmente lo quiso enviar. Los virus utilizan esta técnica para propagarse entre los contactos del correo, así como los contactos de la mensajería instantánea y de las redes sociales.

-Conoce los riesgos asociados al uso de Internet.

Contrarrestar un ataque

Seguir estos cinco pasos puede prevenir el robo de datos o al menos acotar el impacto negativo del ataque:

1º Desconectar el equipo de Internet. Con la desconexión se podrá impedir que el virus que infectó el equipo continúe propagándose por la red y que se produzca una nueva infección después de la limpieza.

2º Instalar un programa antivirus. Es muy recomendable utilizar herramientas proactivas mejor que reactivas, por lo que es deseable instalar un software que incluya capacidades de detección proactiva de amenazas. Otra acción fundamental es la de descargar y actualizar la base de firmas del antivirus para conseguir un análisis más eficiente del equipo.

3º Realizar un análisis completo del sistema. Es muy importante analizar por completo todos los discos del equipo en busca de amenazas o daños.

4º Modificar todas las contraseñas de cualquier servicio que requiera autenticación. Con este procedimiento eliminaremos toda posibilidad de robo de credenciales.

5º Realizar una limpieza manual. Para poder llevar a cabo de una forma eficaz esta tarea, es recomendable identificar el tipo de malware responsable del ataque para buscar el método más adecuado de desinfección.

Biografía

https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

https://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico#Consecuencias

https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

https://openwebinars.net/blog/hacking-tutorial-como-hacer-ataque-ddos/

https://www.fundaciontelefonica.com/2016/10/14/actuar-ataque-informatico-malware/

https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

https://www.vexsoluciones.com/seguridad/tipos-de-ataques-ciberneticos-ciberseguridad-ciberdefensa/