Fases de Un Ataque

La seguridad informática se ha tomado un lugar muy privilegiado en el área informática, ya que las personas ya están tomando **conciencia de los posibles riesgos** a los cuales se está expuesto, la gran mayoría de las **empresas están cambiando** la forma de **realizar sus negocios**, todo gracias al **apoyo de la tecnología.**

Gracias al desarrollo del software y la interconexión hace imaginable el hasta donde se puede llegar gracias a los computadores, servidores, las telecomunicaciones, los servicios prestados, pero … no le estamos dando foco a la seguridad: como aseguro mis sistemas, mis redes, mi información confidencial?. ¿**Toda la tecnología adquirida y adoptada es segura?.**

Como evito irme a la quiebra por la información sustraída ya sea por cualquier técnica Hacker o medio humano como por ejemplo ingeniería social?, estas personas inescrupulosas o expertas contratadas por terceros para hacerme daño, o divulgar información confidencial robada, que viendo desde otro ángulo puede afectar un gobierno, una organización, una empresa, una familia, una persona, o que tal esta información sustraída ayude o sirva como una prueba fehaciente para incriminar a cualquier ente que este obrando fuera de la ley. La información es un activo muy valioso, y hay que protegerla, y que mejor manera entendiendo como se perpetúa un ataque, entender los pasos, las formas, aprender a estudiar a estas personas que con malas intenciones puede penetrar en nuestros sistemas abruptamente, sin nuestro consentimiento, sin nuestro permiso y afectarnos de una manera o otra.

Por este motivo es importante saber cuál es el **"modus operandi"** de estas personas que sin importar la ideología, razón, motivos o circunstancias logra penetrar a nuestros sistemas y así evitarles el éxito, ya que estaríamos un paso adelante de ellos, claro está que la tecnología cambia a diario, entonces debemos siempre pensar en la protección proactiva, es decir estar anunciando lo nuevo, así evitaremos ser atacados.

¿COMENCEMOS: QUE ES UN ATAQUE?

"Es Método por el cual, valiéndose de un vector de ataque se encuentra una vulnerabilidad y sin tener el permiso correspondiente, o sin validarse o identificarse, se puede realizar una negación de

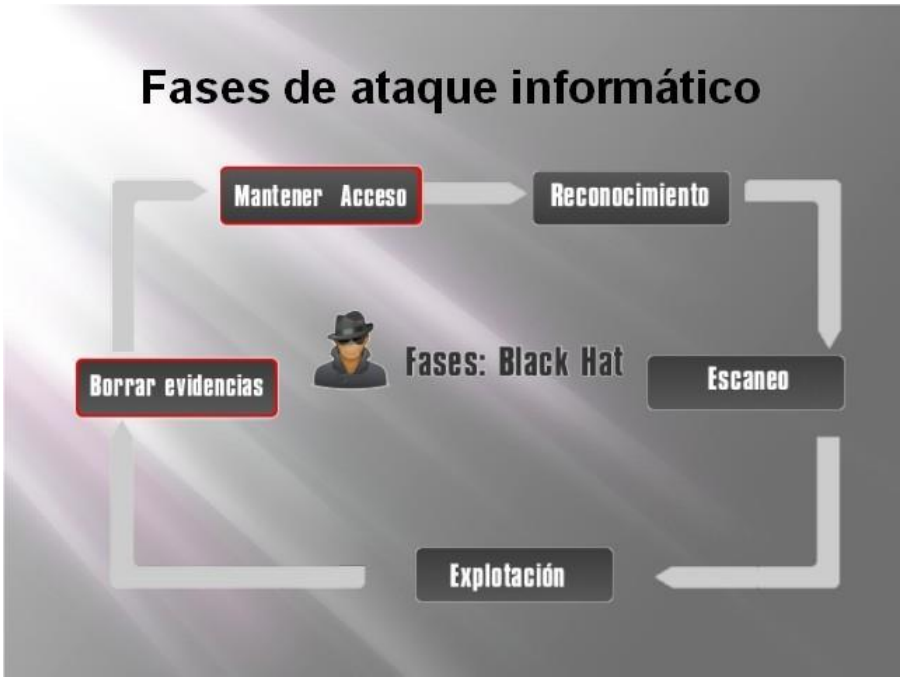
servicio, ejecutar código arbitrario, obtener información confidencial, escalar privilegios, administrar el sistema, tomar el control del mismo, o simplemente detener o dañar el sistema informático".

TIPOS DE ATAQUES

- Ataque Activo y Ataque Pasivo
- Ataque Interno y Ataque Externo

Los ataques se dividen en dos tipos: **Ataque Activo** que **altera el sistema o red atacado** y **ataque pasivo** que es simplemente **obtener información del sistema o red**; y puede provenir desde dos sitios: Interno es decir dentro la red, los empleados descontentos, terceros dentro de la organización y Externo o refiérase a ataques fuera del perímetro de la red o otras redes, Internet, proveedores y hackers maliciosos.

FASES DE UN ATAQUE



(Fases mas conocidas)

OCHO FASES QUE FORMAN PARTE DE UN ATAQUE:

FASE 1: DEFINICIÓN DEL OBJETIVO
Esta es la primera fase del ataque o Hacking en el cual se define el objetivo a atacar, sea una red, un servidor remoto, una página web, una aplicación cliente/servidor, hardware, un proceso o procedimiento, una compañía, una organización, etc.

En esta primera fase el hacker tiene el reto en su mente y visualiza su objetivo.

FASE 2: RECONOCIMIENTO
También conocido como **Footprinting**: que significa construir el mapa de red y sistemas del objetivo a atacar, por medio de los datos adquiridos del ambiente y arquitectura, también identifica vulnerabilidades, servicios, identifica medios por donde se podría ingresar para atacar el objetivo. Esta fase le permite al atacante crear una estrategia para su ataque. Esta fase puede incluir la Ingeniería Social, buscar en la basura (Dumpster diving), buscar que tipo de sistema operativo y aplicaciones usa el objetivo o víctima, cuales son los puertos que están abiertos, donde están localizados los routers (enrutadores), cuales son los host (terminales, computadoras) más accesibles, buscar en las bases de datos del Internet (Whois) información como direcciones de Internet (IP), nombres de dominios, información de contacto, servidores de email y toda la información que se pueda extraer de los DNS. Algunas técnicas para realizar footprinting es utilizar herramientas como el whois, traceroute, e-mail tracking, nslookup, sam spade, web spiders a la IP o Dominio del objetivo.

FASE 3: EXPLORACIÓN Y ENUMERACIÓN
También conocido como Scanning. Es la fase de pre-ataque donde el Hacker escanea la red para obtener información especifica generada en la fase de reconocimiento.

Esta es la fase que el atacante realiza antes de la lanzar un ataque a la red (network). En el escaneo el atacante utiliza toda la información que obtuvo en la Fase del Reconocimiento (Fase 2) para identificar vulnerabilidades específicas. También hace un escaneo de puertos para ver cuáles son los puertos abiertos para saber por cual puerto va entrar y usa herramientas automatizadas para escanear la red y los host en busca de mas vulnerabilidades que le permitan el acceso al sistema.

FASE 4: ANONIMATO:
El anonimato es una de las faces mas importantes de todo Hacker ya que en esta oculta todo sus movimientos.

FASE 5: ENUMERACIÓN:
Es el proceso de obtener las cuentas de usuarios y vulnerabilidades (recursos mal protegidos) La Enumeración incluye conexiones activas a sistemas y consultas directas.

FASE 6: GANAR ACCESO:
Se refiere a la fase de penetración, el Hacker explota vulnerabilidades en el sistema. El Hacker puede ganar acceso a nivel del sistema operativo, aplicación o red.
"Es la fase más importante en términos de daño potencial" porque es la fase de penetración al sistema, en esta fase el Hacker explota las vulnerabilidades que encontró en la fase 3. La explotación puede ocurrir localmente, offline (sin estar conectado), sobre el LAN (Local Area Network), o sobre el Internet y puede incluir técnicas como buffer overflows (desbordamiento del buffer), denial-of-service (negación de servicios), sesión hijacking (secuestro de sesión), y password cracking (romper o adivinar claves usando varios métodos como: diccionary atack y brute forcé atack).

Los factores que ayudan al Hacker en esta fase a tener una penetración exitosa al sistema dependen de cómo es la arquitectura del sistema y de cómo está configurado el sistema objetivo o víctima, una configuración de seguridad simple significa un acceso más fácil al sistema, otro factor a tener en cuenta es el nivel de destrezas, habilidades y conocimientos sobre seguridad informática y redes que tenga el Hacker y el nivel de acceso que obtuvo al principio de la penetración.

FASE 7: ESCALAR PRIVILEGIOS
En esta etapa ya se tiene un usuario valido en el sistema, el cual puede tener permisos mínimos por esta razón se debe realizar una escalación de privilegios que simplemente es añadir mas permisos o derechos a la cuenta de usuario que se tiene, la idea es volverlo administrador del sistema para instalar y ejecutar aplicaciones. En esta fase el Hacker usa sus recursos y recursos del sistema y usa el sistema objetivo como plataforma de lanzamiento de ataques para escanear y explotar a otros sistemas que quiere atacar, también usa programas llamados sniffers para capturar todo el trafico de la red, incluyendo sesiones de telnet y FTP (File Transfer Protocol).

En esta fase el Hacker puede tener la habilidad de subir, bajar y alterar programas y data.
En esta fase el hacker quiere permanecer indetectable y para eso remueve evidencia de su penetración al sistema y hace uso de Backdoor (puertas traseras) y Troyanos para ganar acceso en otra

ocasión y tratar de tener acceso a cuentas de altos privilegios como cuentas de Administrador. También usan los caballos de Troya (Trojans) para transferir nombres de usuarios, passwords e incluso información de tarjetas de crédito almacenada en el sistema.

FASE 8: BORRADO DE HUELLAS

Esta es la etapa final de todo ataque en que una vez obtenido nuestro objetivo procederemos al borrado total de nuestras actividades. En esta fase es donde el Hacker trata de destruir toda la evidencia de sus actividades ilícitas y lo hace por varias razones entre ellas seguir manteniendo el acceso al sistema comprometido ya que si borra sus huellas los administradores de redes no tendrán pistas claras del atacante y el Hacker podrá seguir penetrando el sistema cuando quiera, además borrando sus huellas evita ser detectado y ser atrapado por la policía o los Federales.

Las herramientas y técnicas que usa para esto son caballos de Troya, Steganography, Tunneling, Rootkits y la alteración de los "log files" (Archivos donde se almacenan todos los eventos ocurridos en un sistema informático y permite obtener información detallada sobre los hábitos de los usuarios), una vez que el Hacker logra plantar caballos de Troya en el sistema este asume que tiene control total del sistema.

Las fases de un PENTEST son muy diferentes a la fase de un ataque: (en el pentest, no se aplican todas las fases de un ataque, salvo que haya un acuerdo mutuo para exonerarnos de responsabilidades).