PECCE 2019 - Modulo V – Pentesting

Introducción

Los tests de penetración son la mejor manera en que una organización pueda comprobar hasta qué punto su red y/o sistemas son seguros ante un ciberataque. En un test de penetración la persona que lo realiza (pentester) no solo descubre posibles vulnerabilidades que podrían ser usadas por atacantes, sino que las explota hasta donde sea posible para identificar qué información y/o acceso se podría llegar a alcanzar en un hipotético ataque. Para ello es necesario conocer y seguir una serie de metodologías y usar técnicas y herramientas de manera ordenada, sistematizada y orientada a objetivos, tal como lo haría un atacante

Objetivo General:

Ser capaz de planificar y llevar a cabo un pentesting a una organización y a sus sistemas, aplicando la metodología, las técnicas y las herramientas adecuadas para ello

Objetivos específicos:

- Conocer los diferentes tipos de pentesting
- Ser capaz de planificar una prueba de penetración (definición de alcance, selección de metodología, etc.)
- Comprender las diferentes fases de un pentesting
- Conocer las técnicas y herramientas necesarias para cada fase del pentesting
- Conocer conceptos y buenas prácticas básicas para la elaboración de informes de pentesting

Contenido Curricular:

1. Introducción. Tipos de pentesting. Conceptos básicos
2. Fases de un pentesting
3. Recopilación de Información
4. Análisis de vulnerabilidades
5. Modelado de la Explotación
6. Post-explotación

CONTENIDO

• Que es un Ethical Hacking?

• En que consiste un Test de Intrusión?

• Alcance

• Metología de Ethical Hacking

• Etapas y Herramientas

• Descubrimiento y Exploración

• Ingeniería Social

DEFINICIÓN

Conjunto de metodologías y técnicas pasivas e intrusivas que recrean un ataque informático en un ambiente controlado.

CONSISTE en descubrir vulnerabilidades y vectores de ataques, para su posterior mitigación.

Quienes realizan un Test de Intrusión

• Personas con amplios conocimientos sobre plataformas utilizadas en el mercado y las vulnerabilidades asociadas a las mismas.

• Personas formadas con conocimiento sobre Seguridad Informática y de la Información.

• Personas con formación y experiencia en técnicas y el uso de las herramientas de ethical hacking

GARANTIZAR

SEGURIDAD: Confidencialidad, integridad, disponibilidad

Tipo de Hackers

- Sombrero blanco
- Sombrero gris
- Sombrero negro

ETAPAS

1. Definición del alcance
2. Descubrimiento y Exploración
3. Análisis de vulnerabilidades
4. Intrusión
5. Presentación de Informes

Tipo de amenazas

- Atacante interno
- Atacante externo

Definición del alcance

Se definen objetivos tales como Pool de direcciones IP Públicas, nombre de dominio, URL, Organización, escenarios, metodologías, herramientas, etc.

METODOLOGIAS

OSSTMM

Open Source Security Testing Metodology Manual

OWASP

Open Web Application Security Project

TIPO DE PRUEBAS

- Caja Negra
- Caja Gris
- Caja Blanca

Descubrimiento y Exploración

Se realizan tareas a fin de recabar datos asociados al objetivo mediante el uso de herramientas y técnicas de recolección de información (Information Gathering).

¿Por dónde empezar?

Descubrimiento

Obtener la mayor cantidad de información del objetivo. Herramientas de acceso público

• Motores de búsqueda

• Sitio Institucional del Objetivo

HACKING CON GOOGLE

Los “dorks” o “google dorks” son técnicas utilizadas para realizar filtros a través del motor de búsqueda de Google, el principal objetivo consiste en obtener resultados más acotados y obtener en algunos casos información que podría no encontrarse resguardada de manera apropiada.

SITIOS WEB CON INFORMACION PUBLICA

• SHODAN

• ARCHIVE.ORG

• NETCRAFT

• REDES SOCIALES

• PILP

• WHOIS

METADATOS

- ExifTool

NAVEGACION DEL SITIO WEB

Descubrimiento y Exploración

Técnicas

- Ingeniería social
    - Trashing
    - Spam
    - Llamadas telefónicas
- Footprinting
    - Netcraft
    - Archive
    - Pilp
    - Shodan
    - Google Dorks
- Fingerprinting
    - nmap
    - dnsenum

INGENIERÍA SOCIAL CON Ettercap / BeEF

ENVENENAMIENTO ARP | DNS SPOOF | INGENIERIA SOCIAL

DNS CICLO LEGÍTIMO / DNS CICLO MALICIOSO

ARP CICLO LEGÍTIMO / ARP CICLO MALICIOSO

GOOGLE HACKING

Google Hacking es una técnica en informática que utiliza operadores para filtrar información en el buscador de Google. Además, podemos encontrar otras aplicaciones de agujeros de seguridad en la configuración y el código informático que se utilizan en las páginas web.

Hay cientos de publicaciones en la red sobre este tema, pero al igual he visto, que no se aborda en ellos, aparte de los términos no muy bien claros es una poca complejidad sobre esta técnica muy utilizada, pero poco conocida. Quiero observar que "saber utilizar los parámetros avanzados de búsquedas de Google, no nos convierte en pentesters, analistas y mucho menos en hackers".

¿Que puedo encontrar a través de Google Hacking?

Las técnicas que búsqueda a través del buscador de Google, nos permiten conseguir información sensible suficiente sobre un objetivo, como archivos de configuración, paneles de servidores, puntos de acceso, claves y contraseñas de sistemas, ver videos privados, datos personales, números telefónicos, e- mails, hashes, errores de programación, y algo para lo que más ha sido utilizado es la búsqueda de puntos vulnerables para inyección de código arbitrario.

Pero como todo, tiene sus límites, esta vez el límite dependerá de la creatividad y el ingenio del usuario atacante, analista o un usuario común, ya que, dependiendo de nuestra creatividad, combinada con esta técnica podríamos conseguir cosas como:

- Datos de configuración de servidores Web y de redes.
- Datos de acceso a bases de datos.
- Mensajes y advertencias de errores de programación.
- Datos personales, o sensibles de alguna compañía.
- Búsquedas aleatorias de Victimas de Hacking.
- Números y claves de tarjetas de crédito.
- Claves y cuentas de correo.
- Acceso a archivos logs.
- Datos específicos de Sistemas Operativos.
- Bases de datos de usuarios y contraseñas.
- Puntos de acceso a paneles de administración de servidores Web.
- Consultas y mapeado de servidores.

PARAMETRO	MODO DE EJECUCIÓN	DETALLES
Inurl	inurl:login.asp	Busca el sitio que tengan “login.asp” que se encuentre como parte de la URL, por medio del cual podremos acceder a los recursos administrativos del sistema a nivel Web en este caso. Además podemos intercambiar las búsquedas y en vez de login.asp podemos poner algo como: admin.asp, password, etc.Esto dependerá enteramente de la creatividad y el ingenio del pentester.
Filetype	filetype:xls “tel”	Es un operador que nos permite hacer búsqueda de ficheros con extensiones específicos. Por ejemplo en el ejemplo le estamos diciendo que busque archivos de Excel (.xls) que hagan referencia a la palabra “tel”, o sea teléfonos, Cédulas de identidad, o también para buscar contraseñas. Esto depende que tipo de fichero queremos buscar, podemos usar de todo tipo de extensiones por ejemplo: pl, mp3, txt, mdb, sql, php, asp, php, sh, etc.
Link	link: lnxnetwork.com	Este operador muestra todos los sitios web que en sus paginas tengan links que apunten hacia el sitio web www.lnxnetwork.com, con esto al hacer un pentest podríamos saber la relación de la empresa que estemos testeando, ya sea con posibles provedores, ventas online, socios, publicidades, hasta blogs personales o fotografías.
Autor	autor: José Hernandez	Esto hará una búsqueda en google por todos sitios, foros, blogs, en la cual haya comentado e iniciado un tema la persona en cuestión: José Hernandez.
Site	site:lnxnetwork.com 'hacking'	Esto buscara dentro de lnxnetwork.com y mostrara todos los enlaces donde encuentre la palabra “hacking”. OBS.: Aquí en este ejemplo en vez de doble comilla puse una simple, eso hace mas especifica aun la búsqueda, será cuestión de cada uno seguir optimizando los métodos. Este parámetro puede usarse para encontrar palabras clave dentro del sitio al que estamos haciendo pentest.
Intitle	intitle:'index of/admin.php'	Esto busca en el titulo de una página web. Es útil para buscar directorios predefinidos en los servidores.
allinurl	inurl:passwords.txt site:com	Esto buscara el fichero passwords.txt dentro de todos los sitios .com que logre escanear.
allfiletype	filetype:xls cedula site:mec.gov.py filetype:xls cedula site:mec.gov.py	Esto buscara un fichero con datos de cedulas en sitios del gobierno.

allinurl	all inurl:login.asp intitle:intranet site:com --- all inurl:login.php intitle:intranet site:com	Esto buscara ficheros login.asp de acceso a intranets que estén expuestas en Internet.
Site	site:presidencia.gov.py fraude	Buscara todo lo que tenga que ver con fraudes alojado en el sitio presidencia.gov.py
Site	site:presidencia.gov.py nomina	Buscara todo lo que tenga que ver con la nómina de funcionarios alojado en el sitio presidencia.gov.py
Site	site:gov.py filetype:pdf	Buscara en todos los sitios ".gov.py" todos los ficheros .pdf alojados en los servidores.
Site	site:com inurl:passwd filetype:log	Esto buscara dentro de los sitios .com en el directorio passwd el log de contraseñas.
Inurl	filetype	También se puede usar así: inurl:passwd filetype:txt site:com
Inurl	inurl:pass filetype:sql site:com	Esta búsqueda le permitirá accede a archives SQL que contengan password
Inurl	inurl:users filetype:sql site:com	Esta búsqueda le permitirá accede a archives SQL que contengan usuarios
Filetype	filetype:xls password site:.mil	Buscaría archivos con extensión excel en los sitios militares, que contengan la palabra password
Site	site:static.ow.ly/docs/ intext:@gmail.com | Password	Busca en el sitio static.ow.ly archivos con contraseñas de usuarios para realiza el login en static.ow.ly
Inurl	inurl:DiGIR.php	Búsqueda de archivos interesantes (juicy)
Filetype	filetype:sql intext:wp_users phpmyadmin	Búsqueda del usuario administrador del wordpress en tablas SQL.
Genérica	"Index of /wp-content/uploads/backupbuddy_backups" zip	Realiza una búqueda generica de backup de bases de datos de wordpress
Inurl	inurl:top.htm inurl:currenttime	Realiza una búsqueda de sitios que tengas dispositivos conectados a Internet (cámaras, impresoras, etc).
Intext	intext:"Hello visitor from" ext:asp	Busca respaldos sobre
Algunas que otras contraseñas: allinurl:auth_user_file.txt intitle:"Index of" config.php intitle:index.of.etc filetype:xls username password email		
intitle	intitle:"Index of" ".htpasswd" "htgroup" -intitle:"dist" -apache -htpasswd.c	Busca archives de configuración apache web server que pudieran contener contraseñas.
intitle	intitle:"Index of" .mysql_history	Busqueda de archivos relacionados a mysql

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 negocio**s, 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?

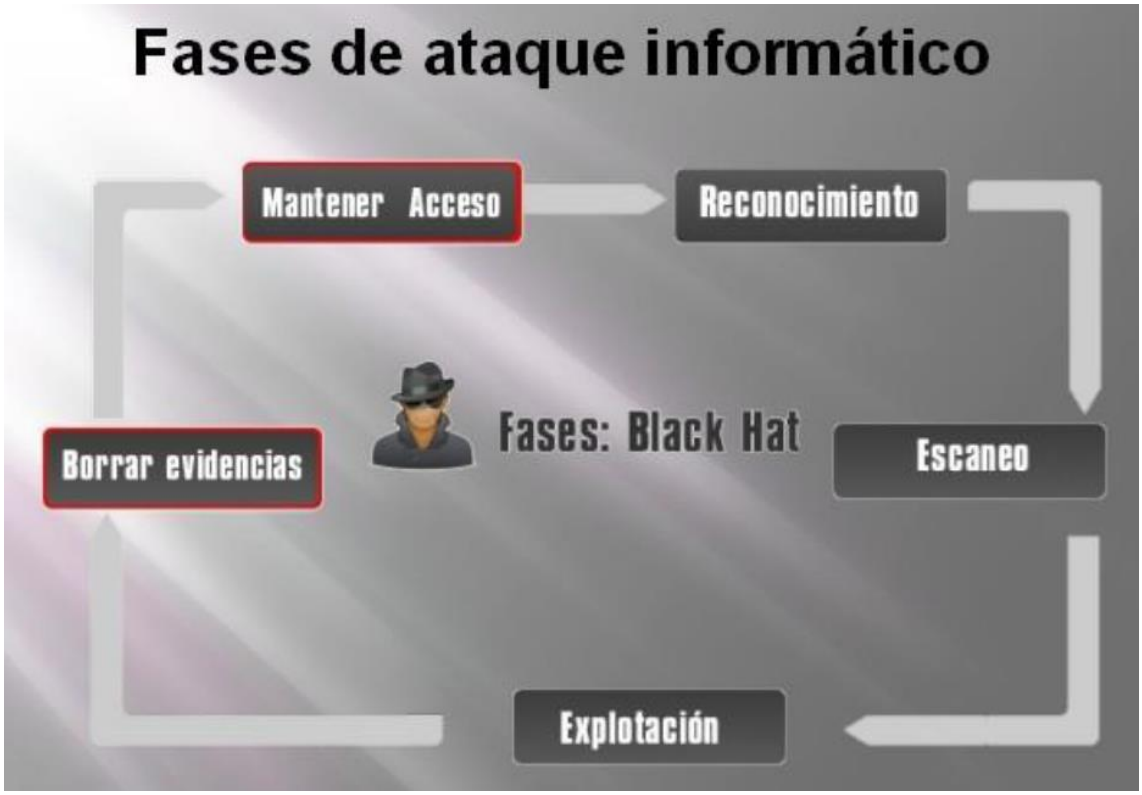
"Es Método por el cual, valiéndose de un vector de ataque se encuentra una vulnerabilidad y sin tener el permiso correspondiente, o sin validarse o identificarse, se puede realizar una negación de servicio, ejecutar código arbitrario, obtener información confidencial, escalar privilegios, administrar 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 específica 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 fases más 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.

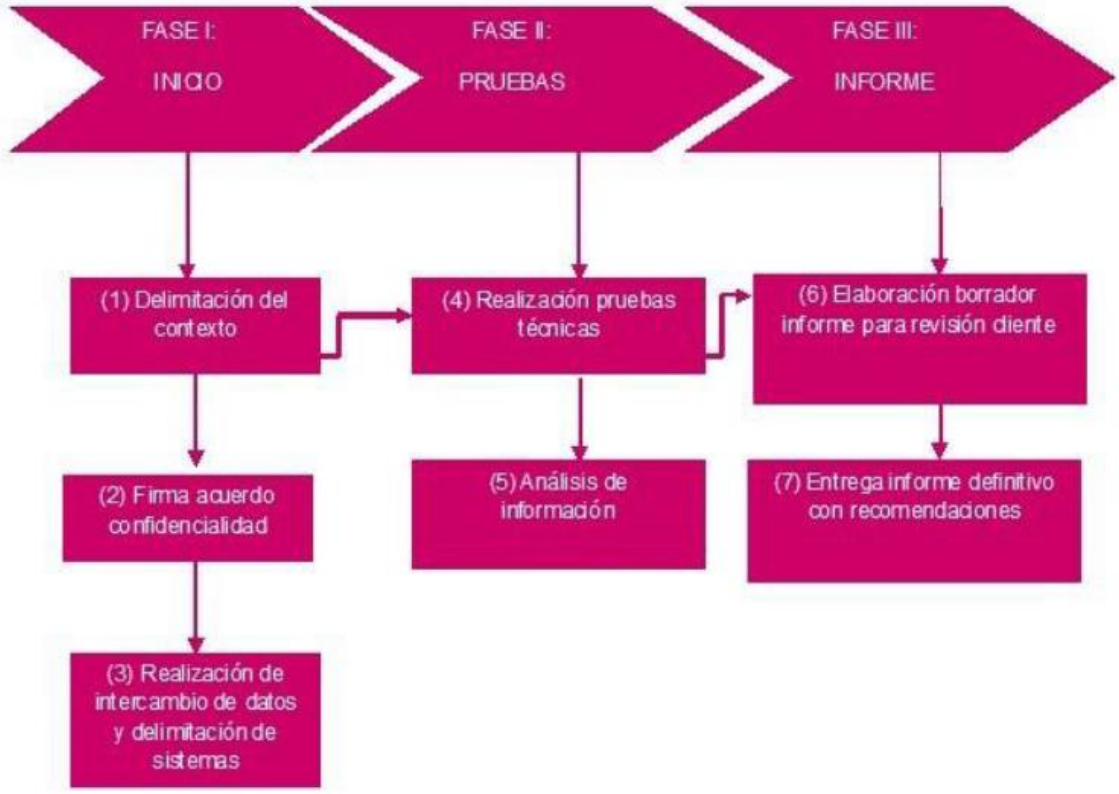
En esta fase el hacker quiere permanecer indetectable y para eso remueve evidencia de su penetración al sistema y hace uso de Backdoor (puertas traseras) y Troyanos para ganar acceso en otra ocasión y tratar de tener acceso a cuentas de altos privilegios como cuentas de Administrador. También usan los 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).



Debilidades de seguridad comúnmente explotadas.

A lo largo del tiempo, el avance de los medios tecnológicos y de comunicación ha provocado el surgimiento de nuevos vectores de ataques y de nuevas modalidades delictivas que han transformado a Internet y las tecnologías informáticas en aspectos sumamente hostiles para cualquier tipo de organización, y persona, que tenga equipos conectados a la World Wide Web (WWW).

A diferencia de lo que sucedía años atrás, donde personas con amplias habilidades en el campo informático disfrutaban investigando estos aspectos con el ánimo de incorporar mayor conocimiento; en la actualidad se ha desvirtuado completamente dando origen a nuevos personajes que utilizan los medios informáticos y el conocimiento sobre su funcionamiento como herramientas para delinquir y obtener algún beneficio económico.

Cada día se descubren nuevos puntos débiles y, por lo general, son pocos los responsables de IT que comprenden en su justa medida la importancia que tiene la seguridad y cómo pueden abordar el grave problema que existe detrás de vulnerabilidades que permiten a un atacante, violar la seguridad de un entorno y cometer delitos en función de los datos robados.

Bajo esta escenografía donde los principales actores son las organizaciones de cualquier magnitud y rubro, los sistemas de información, el dinero y delincuentes informáticos; se torna realmente necesario y fundamental idear estrategias de seguridad que permitan establecer barreras defensivas orientadas a mitigar efectivamente ataques tanto externos como internos.

Pero para lograr mitigar de manera eficaz el impacto provocado por los ataques informáticos, es de capital importancia conocer de qué manera atacan y cuáles son los puntos débiles de un sistema comúnmente explotados en los que se deben enfocar los esfuerzos de seguridad tendientes a la prevención de los mismos.

¿De qué estamos hablando?

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

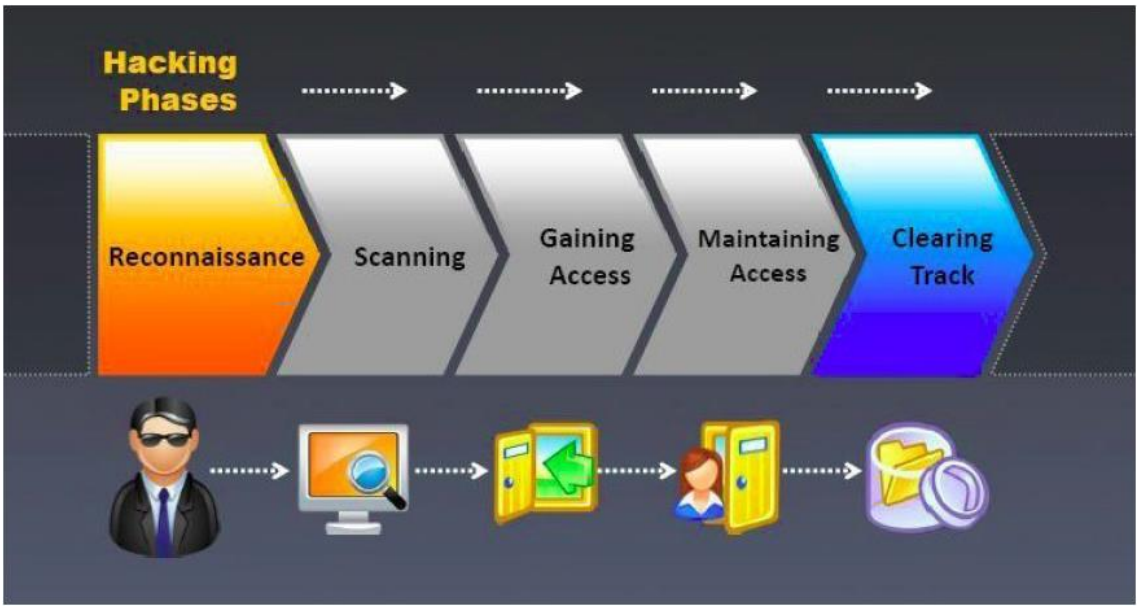
Para minimizar el impacto negativo provocado por ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques.

Uno de los pasos más importantes en seguridad, es la educación. Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas.

Anatomía de un ataque informático

Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad.

Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque.



Fase 1: Reconnaissance (Reconocimiento).

Esta etapa involucra la obtención de información (Information Gathering) con respecto a una potencial víctima que puede ser una persona u organización.

Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el Dumpster Diving, el sniffing.

Fase 2: Scanning (Exploración).

En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el network mappers, port mappers, network scanners, port scanners, y vulnerability scanners.

Fase 3: Gaining Access (Obtener acceso).

En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema (Flaw exploitation) descubiertos durante las fases de reconocimiento y exploración.

Algunas de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow, de Denial of Service (DoS), Distributed Denial of Service (DDos), Password filtering y Session hijacking.

Fase 4: Maintaining Access (Mantener el acceso).

Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos.

Fase 5: Clearing Tracks (Borrar huellas).

Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS).

La seguridad consta de tres elementos fundamentales que forman parte de los objetivos que intentan comprometer los atacantes. Estos elementos son la confidencialidad, la integridad y la disponibilidad de los recursos.

Bajo esta perspectiva, el atacante intentará explotar las vulnerabilidades de un sistema o de una red para encontrar una o más debilidades en alguno de los tres elementos de seguridad.

Para que, conceptualmente hablando, quede más claro de qué manera se compromete cada uno de estos elementos en alguna fase del ataque, tomemos como ejemplo los siguientes casos hipotéticos según el elemento que afecte.

Confidencialidad.

Un atacante podría robar información sensible como contraseñas u otro tipo de datos que viajan en texto claro a través de redes confiables, atentando contra la confidencialidad al permitir que otra persona, que no es el destinatario, tenga acceso a los datos. Un ejemplo que compromete este elemento es el envenenamiento de la tabla ARP (ARP Poisoning).

Integridad.

Mientras la información se transmite a través del protocolo de comunicación, un atacante podría interceptar el mensaje y realizar cambios en determinados bits del texto cifrado con la intención de alterar los datos del criptograma. Este tipo de ataques se denomina Bit-Flipping y son considerados ataques contra la integridad de la información.

Disponibilidad.

En este caso, un atacante podría utilizar los recursos de la organización, como el ancho de banda de la conexión DSL para inundar de mensaje el sistema víctima y forzar la caída del mismo, negando así los recursos y servicios a los usuarios legítimos del sistema. Esto se conoce como Denial of Service (DoS) y atenta directamente contra la integridad de la información.

Debilidades de seguridad comúnmente explotadas

Afortunadamente, en la actualidad existe una gama muy amplia de herramientas de seguridad lo suficientemente eficaces que permiten obtener un adecuado nivel de seguridad ante intrusiones no autorizadas haciendo que la labor de los atacantes se transforme en un camino difícil de recorrer.

Ingeniería Social

Más allá de cualquiera de los esquemas de seguridad que una organización pudiera plantear, existen estrategias de ataque que se basan en el engaño y que están netamente orientadas a explotar las debilidades del factor humano.

Los atacantes saben cómo utilizar estas metodologías y lo han incorporado como elemento fundamental para llevar a cabo cualquier tipo de ataque. Si bien esta técnica es utilizada en cualquier ámbito, en lo que a informática se refiere, consiste en la obtención de información sensible y/o confidencial de un usuario cercano a una sistema u organización explotando ciertas características que son propias del ser humano.

Ya sea por ignorancia, negligencia o coacción, pueden permitir a un atacante obtener acceso no autorizado, quien, de esta manera, podrá eludir los complejos esquemas y tecnologías de seguridad que se hayan implementado en la organización.

Como contramedida, la única manera de hacer frente a los métodos de Ingeniería Social es la educación. Absolutamente todas las personas que forman parte de la organización, desde la secretaria, los administradores de la red y la cúpula mayor, deben estar capacitados en cuanto a las debilidades y los métodos de engaño más empleados por los atacantes para que logren

identificarlos y dar aviso de cualquier anomalía que se produzca en el equipo o en determinado ambiente.

Esto no significa que cada uno de los empleados deba realizar cursos de seguridad informática, sino que el proceso de capacitación debe formar parte de las Políticas de Seguridad de la Información y debe ser ejecutada a través de planes dinámicos de concientización.

Por otro lado, es muy común que el personal crea erróneamente que su posición dentro de la Institución u organización es de poca importancia y que por lo tanto no podrían ser objeto de ataque, pero contrariamente, son en realidad los objetivo preferidos por los atacantes; en consecuencia, la educación es una contramedida muy efectiva, pero es de suma importancia que las personas tomen real conciencia de que ellos son el blanco perfecto de la Ingeniería Social.

"Usted puede tener implementada la mejor tecnología, Firewalls, sistemas de detección de intrusos o complejos sistemas de autenticación biométricos... Pero lo único que se necesita es una llamada telefónica a un empleado desprevenido y acceden al sistema sin más. Tienen todo en sus manos"

Factor Insiders

Cuando se habla sobre las personas que se dedican a atacar sistemas informáticos, se asume que se trata de alguien desconocido que realiza el ataque y maneja todo desde un lugar remoto llevándolo a cabo a altas horas de la noche.

Aunque en algunos casos puede ser cierto, varios estudios han demostrado que la mayoría de las violaciones de seguridad son cometidos por el Factor Insiders, es decir, por los mismos empleados desde dentro de la Institución u Organización.

Una de las formas más eficaces que posee un atacante para romper los esquemas de seguridad, es desde el interior de la organización. Por ejemplo, el atacante podría conseguir un empleo en la organización que desea atacar y obtener el suficiente nivel de confianza en la organización para luego explotar los puntos de acceso. Del mismo modo, cualquier integrante puede convertirse en un empleado disgustado y decidir robar información y/o causar daños como una forma de venganza.

Cuando este tipo de actos es cometido con intenciones de obtener beneficios económicos a través de información corporativa, es denominado Insiders Trading (comercio de personal interno).

En cualquiera de los casos, muchas de las herramientas y medidas de seguridad que se implementen en el entorno informático no serán eficaces. Bajo esta perspectiva, es necesario acudir a estrategias de defensa internas y específicas para el control de posibles ataques ocasionados por el personal de la organización. Estas estrategias defensivas funcionarán como contramedidas.

Una de las mejores soluciones es realizar auditorías continuas que incluyan monitoreos a través de programas keyloggers que pueden ser por hardware o por software, mecanismos que impidan la instalación de programas por parte del personal, estricta configuración del principio de privilegios mínimos, deshabilitación de puertos USB y prohibición del uso de dispositivos de almacenamiento extraíbles para evitar la fuga de información y entrada de otras amenazas

como malware, si las computadoras forman parte de un dominio es necesario establecer políticas rigurosas en el Active Directory, entre otras.

Códigos maliciosos

Los códigos maliciosos, o malware, constituyen también una de las principales amenazas de seguridad para cualquier Institución u Organizaciones y aunque parezca un tema trivial, suele ser motivo de importantes pérdidas económicas.

Esta amenaza se refiere a programas que causan algún tipo de daño o anomalía en el sistema informático. Dentro de esta categoría se incluyen los programas troyanos, gusanos, virus informáticos, spyware, backdoors, rootkits, keyloggers, entre otros.

Actualmente, casi el 80% de los ataques informáticos llevados a cabo por códigos maliciosos, se realizan a través de programas troyanos.

La carga dañina que incorporan los troyanos puede ser cualquier cosa, desde instrucciones diseñadas para destruir algún sector del disco rígido, por lo general la MBR, eliminar archivos, registrar las pulsaciones que se escriben a través del teclado, monitorear el tráfico de la red, entre tantas otras actividades.

Los atacantes suelen utilizar troyanos de manera combinada junto a otros tipos de códigos maliciosos. Por ejemplo, cuando han ganado acceso a través del troyano, implantan en el sistema otros códigos maliciosos como rootkits que permite esconder las huellas que el atacante va dejando en el equipo (Covering Tracks), y backdoors para volver a ingresar al sistema cuantas veces considere necesario; todo, de manera remota y sin que, en la mayoría de los casos, los administradores de la red adviertan su actividad.

Las contramedidas tendientes a prevenir ataques a través de este tipo de amenazas, radican principalmente en la implementación de programas antivirus que operen bajo mecanismos de detección avanzados como la heurística, que también permitan monitorear, controlar y administrar de manera centralizada cada uno de los nodos involucrados en la red, junto a planes de educación orientados a crear conciencia en el personal sobre los riesgos de seguridad que representa el malware.

Contraseñas

Otro de los factores comúnmente explotados por los atacantes son las contraseñas. Si bien en la actualidad existen sistemas de autenticación complejos, las contraseñas siguen, y seguirán, siendo una de las medidas de protección más utilizadas en cualquier tipo de sistema informático.

En consecuencia, constituyen uno de los blancos más buscados por atacantes informáticos porque conforman el componente principal utilizado en procesos de autenticación simple (usuario/contraseña) donde cada usuario posee un identificador (nombre de usuario) y una contraseña asociada a ese identificador que, en conjunto, permiten identificarse frente al sistema.

En este tipo de proceso, llamado de factor simple, la seguridad del esquema de autenticación radica inevitablemente en la fortaleza de la contraseña y en mantenerla en completo secreto,

siendo potencialmente vulnerable a técnicas de Ingeniería Social cuando los propietarios de la contraseña no poseen un adecuado nivel de capacitación que permita prevenir este tipo de ataques.

Si el entorno informático se basa únicamente en la protección mediante sistemas de autenticación simple, la posibilidad de ser víctimas de ataques de cracking o intrusiones no autorizadas se potencia.

Si bien es cierto que una contraseña que supere los diez caracteres y que las personas puedan recordar, es mucho más efectiva que una contraseña de cuatro caracteres, aun así, existen otros problemas que suelen ser aprovechados por los atacantes. A continuación, se expone algunos de ellos:

La utilización de la misma contraseña en varias cuentas y otros servicios.

Acceder a recursos que necesitan autenticación desde lugares públicos donde los atacantes pueden haber implantado programas o dispositivos físicos como keyloggers que capturen la información.

Utilización de protocolos de comunicación inseguros que transmiten la información en texto claro como el correo electrónico, navegación web, chat, etcétera.

Técnicas como surveillance (videoconferencia) o shoulder surfing (mirar por detrás del hombro), entre otras tantas, que permiten evadir los controles de seguridad.

Como contramedida destinada a fortalecer este aspecto de la seguridad, es posible implementar mecanismos de autenticación más robustos como “autenticación fuerte de doble factor”

De nada sirve utilizar contraseñas fuertes si luego son olvidadas o compartidas, ya que con ello se compromete la seguridad de todo el mecanismo de autenticación.”

Configuraciones predeterminadas

Las configuraciones por defecto, tanto en los sistemas operativos, las aplicaciones y los dispositivos implementados en el ambiente informático, conforman otra de las debilidades que comúnmente son poco atendidas por pensar erróneamente que se tratan de factores triviales que no se encuentran presentes en la lista de los atacantes.

Sin embargo, las configuraciones predeterminadas hacen del ataque una tarea sencilla para quien lo ejecuta ya que es muy común que las vulnerabilidades de un equipo sean explotadas a través de códigos exploit donde el escenario que asume dicho código se basa en que el objetivo se encuentra configurado con los parámetros por defecto.

Muchas aplicaciones automatizadas están diseñadas para aprovechar estas vulnerabilidades teniendo en cuenta las configuraciones predeterminadas, incluso, existen sitios web que almacenan bases de datos con información relacionada a los nombres de usuario y sus contraseñas asociadas, códigos de acceso, configuraciones, entre otras, de los valores por defecto de sistemas operativos, aplicaciones y dispositivos físicos.

Sólo basta con escribir en un buscador las palabras claves “default passwords” (contraseña por defecto) para ver la infinidad de recursos disponibles que ofrecen este tipo de información.

Por lo tanto, una de las contramedidas más eficaces para mitigar y prevenir problemas de seguridad en este aspecto, y que muchas veces se omite, es simplemente cambiar los valores

por defecto. En este sentido, es importante no sacrificar la disponibilidad de los recursos por ganar seguridad. Se debe encontrar un equilibrio justo entre usabilidad y seguridad.

La práctica de fortalecer el ambiente informático configurando de manera segura la tecnología para contrarrestar los vectores de ataque se denomina hardening. En este aspecto, la responsabilidad de realizar todo lo que se encuentre a su alcance para modificar los valores predeterminados recae en quienes se encargan de la administración de los equipos.