ETHICAL HACKING

Por: Juan Pablo Conde Mendoza

AGENDA

- TERMINOLOGIA
- PROCESO DE HACKING
- EL PENTEST
- METODOLOGIA

TERMINOLOGÍA

HACKER CONCEPTO EQUIVOCADO

Para poder hablar de Ethical Hacking primero debemos aclarar el significado de la palabra Hacker. Según la Real Academia Española la definición de hacker es la siguiente:

PIRATA INFORMATICO

Claramente esta no es la definición correcta. Dista mucho de ser la definición para un hacker. La gente tiende a pensar en el hacker como alguien que realiza actividades ilegales en los sistemas informáticos. La verdad es que hay hackers buenos ("the good guys") y hackers malos, así como existen médicos buenos y médicos que realizan actividades ilegales. Debemos acostumbrarnos a no pensar en un delincuente cuando escuchamos la palabra hacker así como no lo hacemos cuando escuchamos la palabra médico.

DEFINIENDO A UN HACKER

Un hacker es una persona curiosa, que disfruta de aprender y realizar desafíos. Le interesa mucho el funcionamiento de las cosas. Aunque la definición siempre se aplica a alguien que posee muchos conocimientos de informática (programación, redes, protocolos, etc), no necesariamente tiene que estar relacionado con ella. Un biólogo que se dedica a investigar como curar X virus puede ser un ejemplo de hacker. Un hacker es un entusiasta de cualquier tipo, alguien que desea aprender, crear y poner la información al alcance de todos.

LOS TRES SOMBREROS

Dentro del mundo de la seguridad informática los hackers son clasificados de la siguiente forma:

WHITE HATS: Son los hackers que se encargan de proteger los activos de las organizaciones. Aquellos que velan por la disponibilidad, la integridad y la confidencialidad de la información.

BLACK HATS: Son los que se dedican al cibercrimen. Ingresan a los sistemas ilegalmente por placer, reconocimiento, hacktivismo (activismo que emplea herramientas digitales) o resarcimiento económico. Los hackers dedicados al cibercrimen son también llamados crackers.

GREY HATS: Simplemente hackers que en épocas se dedican a trabajar protegiendo sistemas, como consultores de seguridad y en otras épocas se dedican al cibercrimen.

A QUE SE DEDICA UN ETHICAL HACKER?

Un ethical hacker (o hacker ético) brinda un servicio de seguridad. Utiliza las mismas metodologías, técnicas y herramientas de un black hat hacker para atacar un sistema con el fin de descubrir sus vulnerabilidades, explotarlas (o no, depende de lo acordado) y realizar un informe detallado de los resultados obtenidos.

Estos resultados permiten a la alta gerencia y a los encargados de sistemas conocer el estado de la seguridad de sus sistemas informáticos (lo recomendable es generar dos tipos de informes, uno más técnico para el personal de sistemas y uno más general para la gerencia). Para realizar las pruebas, el hacker ético debe firmar un contrato junto con su cliente en el cual se compromete a no divulgar a terceros ninguna pieza de información encontrada durante las pruebas, así como también a realizar las pruebas en determinados días y horarios, alcance de las pruebas, etc (aquí es donde interviene la parte ética). La prueba realizada por un Ethical Hacker se denomina Penetration Test.

PROCESO DE HACKING

EL PENETRATION TEST

Pentesting (un acrónimo de Penetration Testing) es la actividad mediante la cual se busca comprometer un sistema informático realizando un ataque hacia el mismo. Es decir, en un penetration test, las técnicas y procedimientos que se utilizan son las mismas que utilizan los hackers maliciosos. Lo que diferencia al pentester de un "atacante" o intruso, es la finalidad que persiguen al entrar al sistema. Mientras que el atacante busca demostrar sus conocimientos u obtener algún beneficio económico por robar información, espiar o "romper" , el pentester por su parte busca demostrar las vulnerabilidades del sistema para tratar de mitigarlas y así prevenir futuros ataques. El pentester tiene la responsabilidad de reportar todas las fallas o agujeros que posea el sistema que puedan representar un peligro para la organización, empresa o para quien trabaje. Los pentesters son denominados "Ethical Hackers" dado el compromiso moral que tienen con la entidad que los contrata.

TIPOS DE PENTESTING

WHITE BOX: La entidad contratante le entrega información al pentester, usuarios, e-mails, software utilizado, etc. Con esto el pentester ya tiene una gran cantidad de información para comenzar a trabajar.

BLACK BOX: El pentester debe trabajar "a ciegas", como si fuera un atacante, sin información obtenida de antemano. El pentester debe comenzar a investigar y recopilar toda la información posible para realizar el ataque. Obviamente este tipo de penetration test tiene un costo más elevado, dado el tiempo que insume.

GREY BOX: Es una combinación de White y Black box ya que el pentester obtiene información de forma parcial de la organización. Por ejemplo esto puede puede ser, planos de arquitectura de red e información sobre aplicaciones utilizadas. Un Penetration Test de tipo Grey Box simula lo que podría ser un ataque desde el interior de la organización dado el conocimiento parcial del sistema.

EL PENTEST

TIPOS DE PENTESTING

Para realizar un pentest (y no morir en el intento), debemos seguir una metodología de trabajo, algo que nos marque los pasos a seguir con el fin de no omitir nada. Al seguir una metodología, también sabremos que límites podemos cruzar y cuales no. Recordemos que al realizar un test de penetración podemos llegar a dañar el sistema que estamos auditando. Esta metodología nos ayudará a lo largo de toda la auditoría, y al llegar al final, a realizar un reporte completo y comprensible (recordemos que el reporte será visto por gente que tiene conocimientos de informática y gente que no).

Metodologías de trabajo hay muchas. Cual elegir queda a gusto de cada pentester. Algunos especialistas de seguridad combinan distintas partes de cada una armando su propia metodología. A continuación se citan enlaces con metodologías a tener en cuenta:

ENLACES

OSSTMM (Open Source Security Testing Methodology Manual)

http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf

Penetration Testing Execution Standard:

http://www.pentest-standard.org/index.php/Main_Page

Curso gratuito de Introducción al Pentesting de la comunidad DragonJar donde exponen su metodología:

http://www.dragonjar.org/como-realizar-un-pentest.xhtml

CERTIFICACIONES DE SEGURIDAD

Las certificaciones en Seguridad Informática agregan valor a la hora de buscar empleos o postularse como consultores. Además, al estudiar para rendir una certificación, también aprendemos una metodología de trabajo. Aquí se mencionan algunas de las certificaciones más populares junto a sus enlaces:

- CISSP (Certified Information Systems Security Professional): www.isc2.org
- CEH (Certified Ethical Hacker): www.eccouncil.org
- Security+: www.comptia.org

HABILIDADES

EL (ETHICAL) HACKER, UN GRAN AUTODIDACTA

Podemos utilizar la mejor metodología y realizar cursos pero nada de esto va a servir si no nos esforzamos cada día por aprender por nuestra cuenta. La seguridad informática requiere de mucha teoría y de práctica. Debemos hacer todo lo posible por estar actualizados ante un campo en constante dinamismo. Si decidimos adentrarnos en el mundo del ethical hacking debemos hacerlo sabiendo que el camino no será fácil, para nada. Requiere de muchas horas de lectura, pruebas, montar máquinas virtuales, testear herramientas, escribir código, analizar tráfico y un montón de etcéteras. Debemos tener en cuenta que en este libro veremos muchas herramientas, pero no se trata solo de lanzar un par de ellas y armar un reporte con eso. Nuestro reporte tiene que brindar una información verdadera y completa y la única forma de lograr eso es aportando nuestros conocimientos. Las herramientas son un punto de partida y nos sirven para agilizar pruebas pero debemos conocer en profundidad como funcionan las cosas (ese es el espíritu hacker). Gracias a Internet podemos encontrar miles de recursos e información para aprender sin gastar un centavo. A continuación se muestran enlaces para que el lector investigue:

ENLACES

Aprendizaje

https://foro.hackxcrack.net/

www.cybrary.it

Practicar

www.hackthissite.org

http://www.dvwa.co.uk/

http://www.amanhardikar.com/mindmaps/Practice.html

Mantenerse informado

http://www.securitybydefault.com/

http://www.elladodelmal.com/

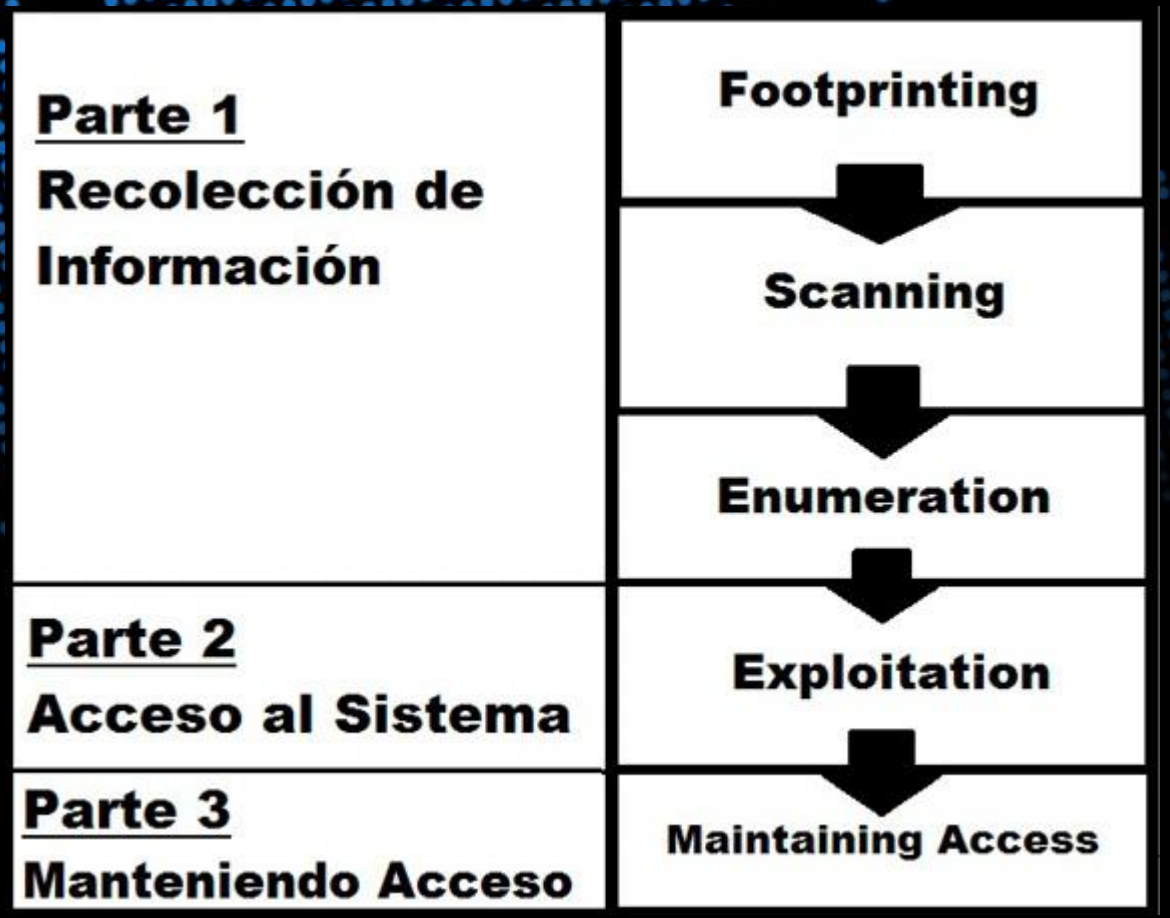
http://www.segu-info.com.ar/

http://unaaldia.hispasec.com/

METODOLOGIA

CONOCIENDO LA METODOLOGÍA

La metodología que utilizaremos está dividida en 5 fases, las cuales serán detalladas en cada capítulo del libro. Estas fases pueden agruparse en 3 grandes partes:



CONOCIENDO LA METODOLOGÍA

PARTE 1: RECOLECCIÓN DE INFORMACIÓN

- Footprinting
- Scanning
- Enumeration

PARTE 2: EXPLOTACIÓN

- System Hacking

PARTE 3: MANTENER EL ACCESO

- Privilege escalation
- Maitaining Access
- Covering tracks

PARTE 1 – RECOLECTANDO INFORMACIÓN

Por lo expuesto mas arriba, seguir un conjunto de pasos se vuelve fundamental, y sobre todo para esta primera fase que vamos a presentar, la fase de obtención de información (information gathering) del objetivo. Mientras mas información obtengamos del sistema, mayores probabilidades tenemos de comprometerlo, dado que vamos a conocer la mayoría de los vectores de ataque (uso de exploits, ingeniería social, inyecciones sql, xss, etc). En esta fase podemos tener una recolección de datos en forma pasiva y otra activa. Cuando hablamos de Information Gathering pasivo nos referimos a aquellos datos que podemos conseguir de la organización a auditar sin tener que interactuar con ella directamente. En el caso de la recolección de datos activa, interactuamos directamente con la organización, por ej. al realizar un escaneo. Dentro de esta primera parte tenemos:

FOOTPRINTING:

En esta fase armamos el perfil de la organización a auditar, buscamos información en la web, ya sea mediante buscadores (Google y el famoso "Google hacking"), sitios que brindan información sobre dominios (Serversniff.net, Netcraft.com, etc.) o herramientas especialmente desarrolladas para esta etapa (Maltego, Foca, etc.).

SCANNING:

En esta fase realizamos un escaneo de los equipos de la organización, aquí identificamos puertos abiertos, servicios que corren en esos puertos, firewalls, puntos de acceso, Sistemas Operativos y vulnerabilidades. Algunas herramientas para el escaneo de puertos y vulnerabilidades son Nmap, Nessus, Hping3 y Firewalk.

ENUMERATION:

En la enumeración tratamos de obtener información sobre nombres de usuario, claves, elementos compartidos que no se encuentren bien protegidos, recursos de red y aplicaciones. Generamos un mapa completo de la red que se encuentra detrás de la organización.

SOCIAL ENGINEERING:

La ingeniería social puede servirnos en cualquiera de las fases para conseguir información. La ingeniería social es el arte de engañar al factor humano (lo que algunos llaman, "hackear a las personas"). Apelando a la bondad, al deseo de ayudar, a la lástima y otros aspectos de las personas, se puede obtener ciertos datos muy útiles de la organización.

PARTE 2 – EXPLOTACIÓN: ACCEDIENDO AL SISTEMA

La siguiente fase es la que nos va a helar la sangre, la que nos hará latir a mil el corazón mientras miramos el monitor a la espera de los resultados. En esta fase nos dedicaremos a explotar las vulnerabilidades que encontramos en la etapa de INFORMATION GATHERING o de RECOLECCIÓN DE INFORMACIÓN. Por eso es que se hace tanto hincapié en la importancia de la primera fase, ya que gracias a ella conoceremos la mayoría de los vectores de ataque que tiene el sistema a auditar.

Entre los vectores de ataque que podemos identificar tenemos:

SOFTWARE, SERVIDORES Y SISTEMAS OPERATIVOS:

Como vimos anteriormente, en la fase de SCANNING, al escanear equipos de la organización obtendremos información sobre los servicios que están corriendo, así como también de los sistemas operativos utilizados. Estos servicios pueden ser aplicaciones conocidas (Servidores Web, bases de datos, Servidores FTP, Correo, etc.) o aplicaciones web propias de la organización. Estos servicios que se encuentran corriendo pueden tener bugs que nos permitan comprometerlos mediante el uso de exploits. Los exploits son programas que aprovechan cierta vulnerabilidad de un servicio/programa para conseguir un comportamiento no deseado del mismo. Hay diferentes tipos de exploits: Remoto, Local y ClientSide.

SOFTWARE, SERVIDORES Y SISTEMAS OPERATIVOS:

El sitio web de la organización puede contener algunos fallos de seguridad que también pueden ser explotados a través de técnicas como SQLInjection o Cross Site Scripting. Estos fallos pueden ser detectados mediante herramientas que veremos mas adelante.

SOFTWARE, SERVIDORES Y SISTEMAS OPERATIVOS:

Es importante mantenerse actualizado para conocer los ultimos fallos de seguridad, dado que en muchos casos las organizaciones tardan en actualizar el software o en parchearlo para evitar ser atacados. Un sitio web muy interesante es el National Vulnerability Database: http://nvd.nist.gov/. Allí podemos encontrar una cantidad impresionante de vulnerabilidades, las cuales podemos buscar por nombre de fabricante, software, fecha, etc.

HUMANOS:

A través de la información recopilada sobre los usuarios de la organización (nombres, cuentas de email, perfiles en redes sociales, gustos. Ya veremos técnicas y herramientas para realizar esto) podemos hacer uso de la ingeniería social para, por ejemplo, llamar a un empleado y engañarlo para obtener cierta información que puede ser útil al momento de intentar atacar el sistema. Esto genera un ciclo dado que existe retroalimentación. Pensemos que:

1° Obtenemos información de un usuario (haciendo uso de ingeniería social o escarbando en la red)

2° Con los datos obtenidos podemos seguir buscando información en la red o hacer uso nuevamente de ingeniería social.

HUMANOS:

Por ej: Obtenemos datos sobre la dirección de correo electrónico de un usuario perteneciente a la organización. Luego enviamos un mail a ese usuario, falseando la dirección del remitente, haciéndonos pasar por un empleado del área de sistemas el cual le solicita que por un cambio en la gestión de seguridad de las claves de correo electrónico debe clickear en un enlace que lo llevará a un sitio de la empresa donde deberá ingresar su clave actual y la clave nueva. Obviamente ese enlace lo llevará a una página alojada en un servidor nuestro el cual guardará los datos (mas adelante veremos como realizar estas acciones). Con las credenciales de ese usuario, podemos ingresar a su correo y obtener mas información para continuar con nuestro ataque. Por eso los usuarios de las organizaciones deben ser capacitados sobre ciertos temas de seguridad, ya que son el eslabón mas débil en la cadena de la seguridad informática.

REDES WIFI:

Muchas veces, por como esta realizada la arquitectura de red, las redes wifi de las organizaciones permiten que los usuarios conectados a ella puedan visualizar los equipos pertenecientes a la organización, o incluso los dispositivos personales de los empleados, lo cual permitiría a un atacante con acceso a ella capturar información sensible o atacar los mencionados equipos.

PARTE 3 – MANTENIENDO EL ACCESO

Una vez que el atacante obtiene acceso a un sistema, va a querer obtener información en archivos alojados en el equipo victima, información de la red (sniffeando tráfico, mapeando otros equipos) así como también escalar privilegios. Como todo esto lleva tiempo, lo mas lógico es que el atacante deje, por ejemplo, un backdoor (puerta trasera) en el equipo victima con el fin de lograr un acceso mas sencillo cada vez que quiera conectarse nuevamente.

El Pentester debe realizar estas actividades con el fin de demostrar hasta donde se puede llegar una vez vulnerado el sistema, generando el reporte correspondiente. Obviamente, se podrá avanzar hasta donde lo permita el acuerdo firmado con la organización.

PARTE 3 – MANTENIENDO EL ACCESO

Otra cuestión a tener en cuenta en esta fase es la de borrado de huellas, dado que cada vez que nos conectamos a un equipo queda un registro de esa "visita" y de las cosas que modificamos, con lo cual se vuelve de suma importancia eliminar toda evidencia de nuestro paso por los equipos de la víctima.

Cuando comencemos con las técnicas y herramientas para cada fase veremos como montar un backdoor en un equipo, así como también que debemos tener en cuenta a la hora de borrar nuestras huellas.