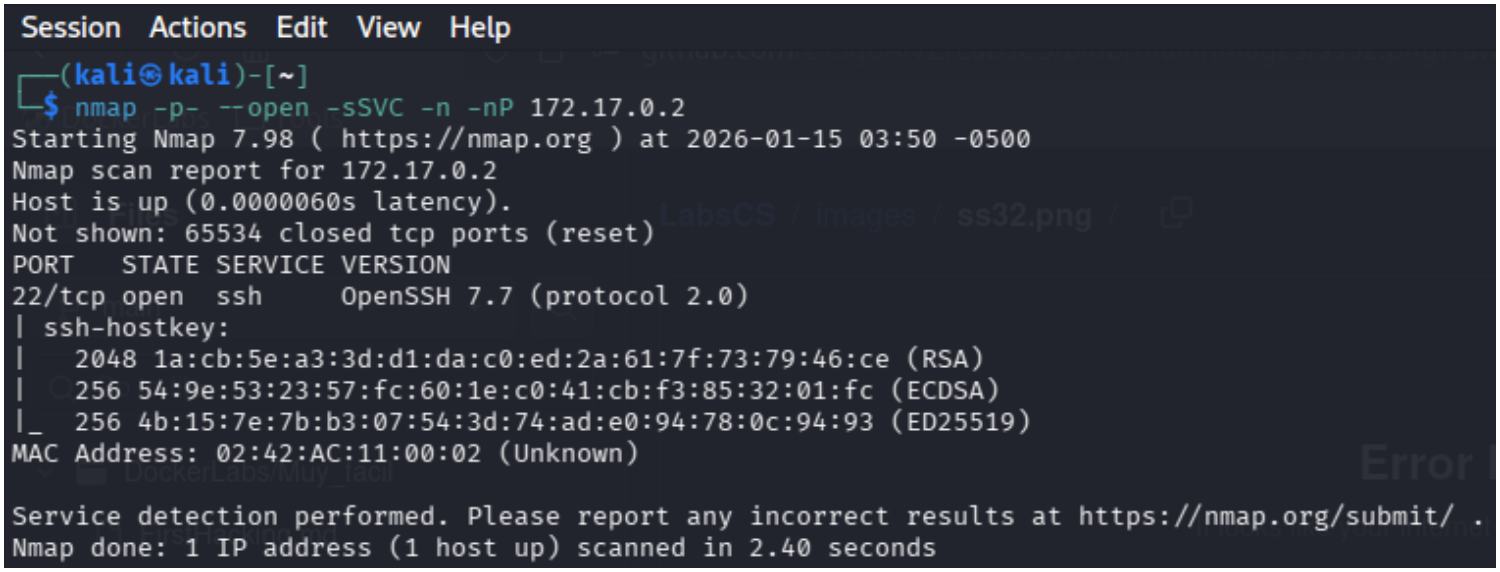
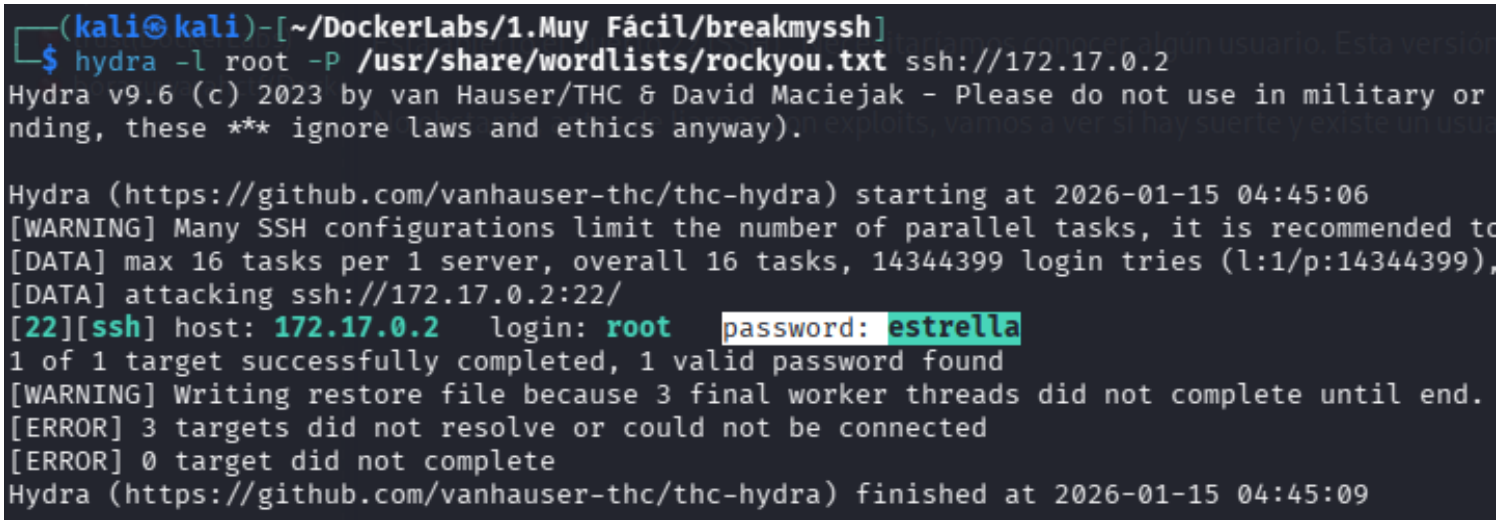
breakmyssh

Lo primero, como siempre, ***nmap*** para ver posibles vías de entrada:



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***:



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!!