**INJECTION.**

1. **Inicializar.**

Para iniciar desplegamos la máquina usando el comando de Kali Linux **sudo bash** para inicializar los archivos **.sh** y **.tar**

Texto

El contenido generado por IA puede ser incorrecto.

1. **Reconocimiento.**

Una vez inicializada, tomamos la ip y utilizamos la herramienta **nmap** para revisar los puertos abiertos. (**sudo nmap -p- --open -sS -min-rate 5000 -vvv -n -Pn “IP a escanear”)**En este caso estamos usando un reconocimiento activo (escaneo de puertos).

Donde:

**-p-** sirve para escanear los 65536 puertos TCP

**--open** se usa para mostrar solo los puertos abiertos

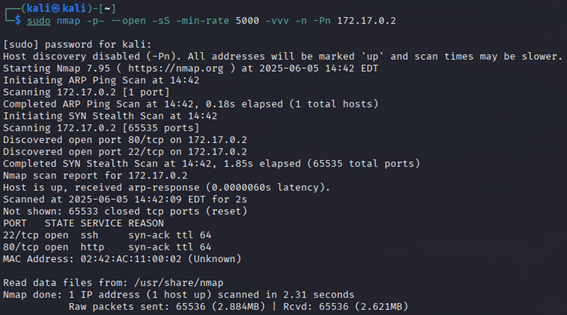
**-sS** hace un escaneo TCP SYN (semiabierto) más rápido e indetectable que un escaneo completo (-sT)

**-min-rate 5000** fuerza nmap para enviar 5000 paquetes por segundo (puede arrojar falsos negativos)

**-vvv** Modo verbose x3, o lo máximo detallado posible.

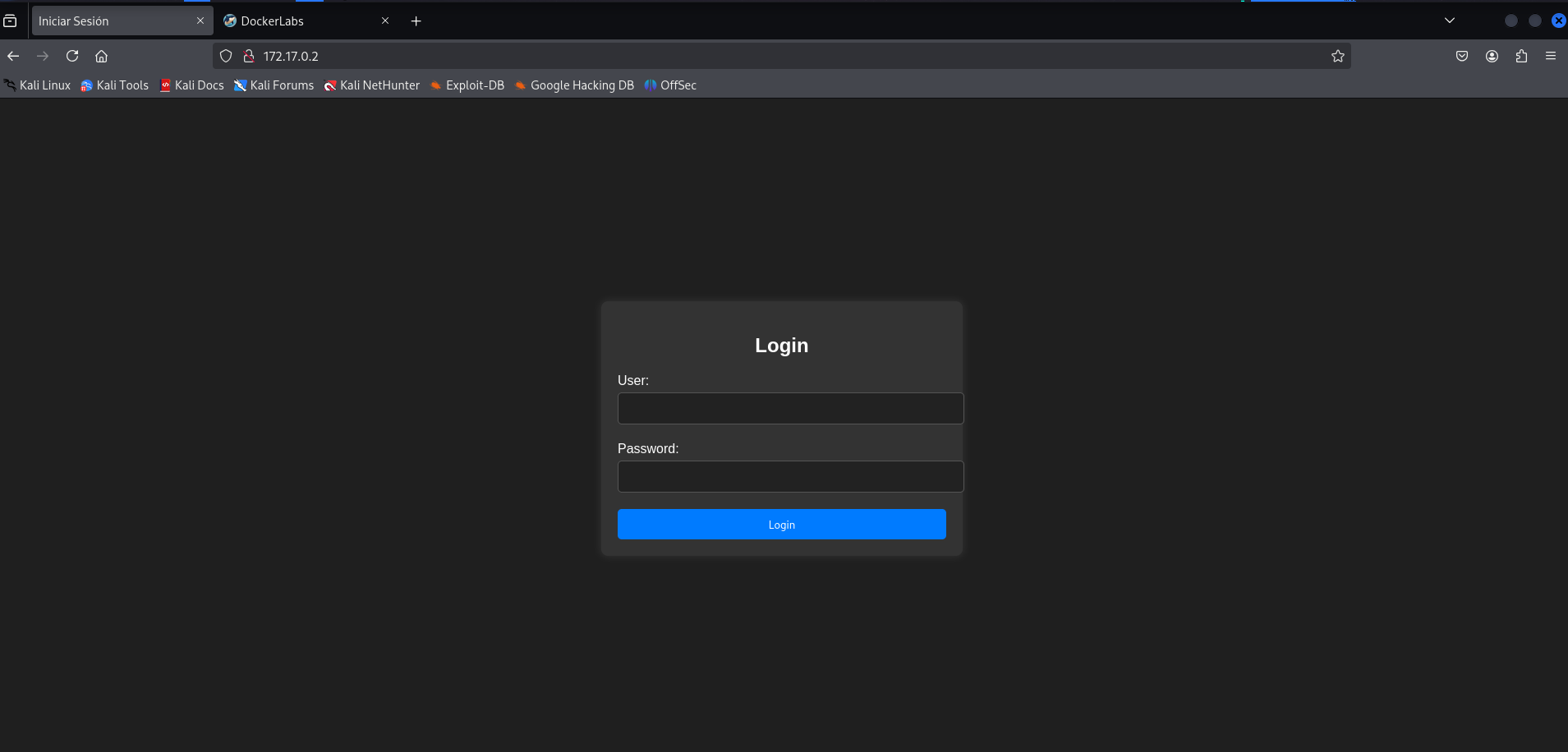
**-n** elimina la resolución DNS

**-Pn** Evita que nmap haga ping previo, asumiendo que el host está up (se usa para evitar filtros ICMP o Firewall).



Como podemos observas en la imagen, están abiertos los puertos 22 y 80, que corresponden a los protocolos SSH y HTTP, por lo que revisamos si hay alguna página asociada a la ip.

1. **Enumeración.**



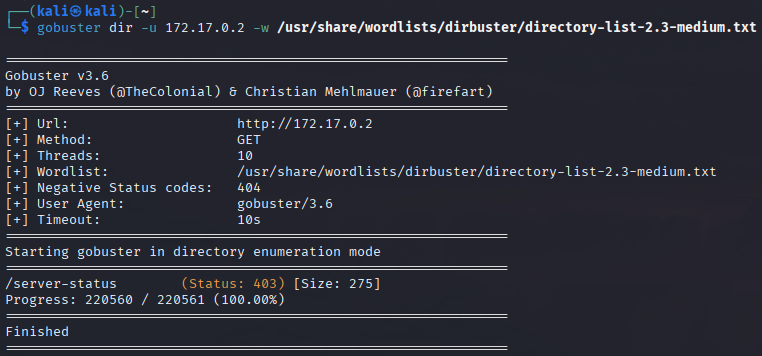
Como podemos ver existe un dominio asociado a la ip con un cuadro de inicio de sesión.

Usamos Gobuster para realizar fuerza bruta y encontrar Subdominios asociados con un diccionario de direcciones comunes.  
**(gobuster dir -u http://IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt)**

Donde:  
  
**dir** es el modo de busca por direcciones.

**-u** es una flag que en este caso se usa para denotar la url a donde vas.

-**w** es una flag que en este caso se usa para buscar en una wordlist.

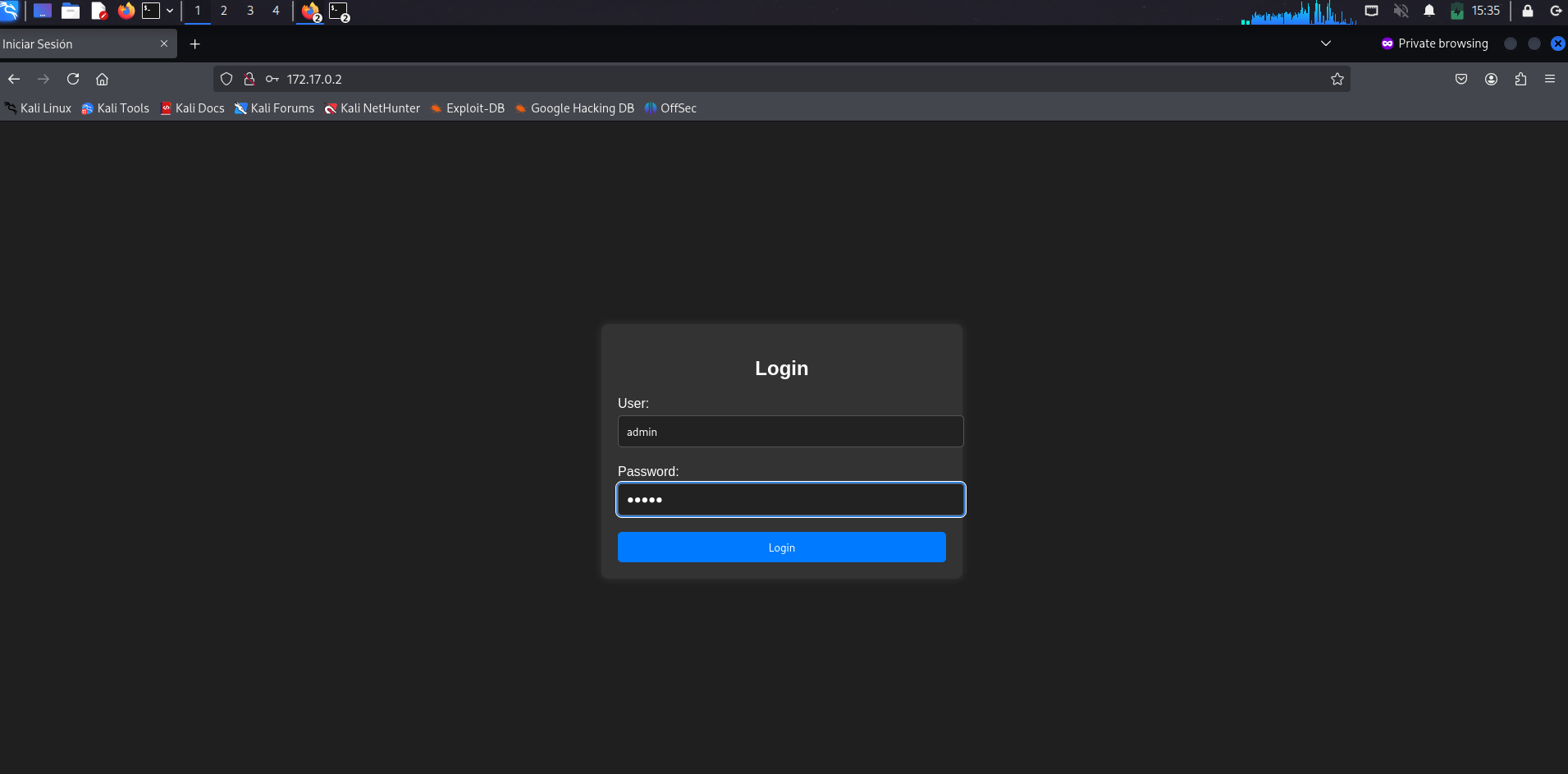


El resultado arroja un subdominio llamado /server-status con status 403, es decir acceso prohibido.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Probamos **login:admin / password:admin**.

 Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

Debido a que no podemos ingresar a ese directorio intentamos realizar una inyección SQL para ver si la página posee dicha vulnerabilidad y lograr bypassear el login.

1. **Explotación**

Usamos la línea de comando **‘or 1=1-- -** que básicamente le dice a SQL que si el usuario suministrado es válido, busque en su base de datos el usuario y realice el login, pero también debe hacer esto mismo si 1=1 lo cual se cumple siempre.

(En el apartado de password ponemos cualquier cosa).

Captura de pantalla de un celular

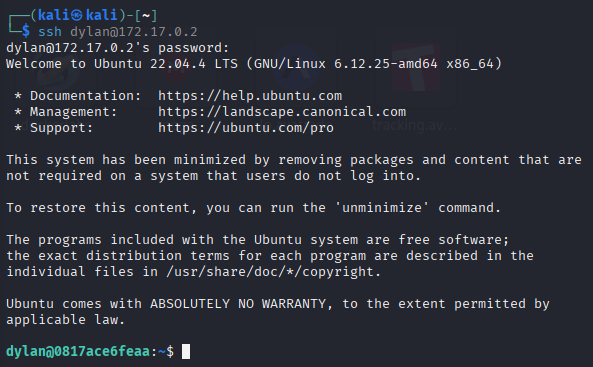
El contenido generado por IA puede ser incorrecto.

Notamos que efectivamente, es vulnerable a **SQLi**  y pudimos ingresar con las credenciales de un usuario llamado Dylan.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

Mediante el servicio **ssh** con el usuario de Dylan, intentamos ingresar al sistema usando el comando **ssh usuario@ip** e ingresando la contraseña encontrada.



Revisamos que permisos tiene Dylan con el comando whoami.

Texto

El contenido generado por IA puede ser incorrecto.

Vemos que no tiene permisos de root (superusuario).

1. **Post- explotación.**

Intentemos escalar privilegios. Iniciamos buscando binarios SUID para usuarios root (Set User ID).

**find / -perm -4000 -user root 2>/dev/null**

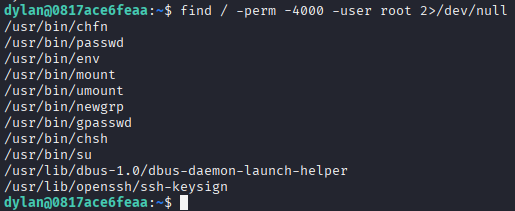
Donde:

**find/** Se usa para buscar en todos los directorios.

**-perm-4000** Busca archivos con el bit SUID activo (4000 en octal). El - antes del número significa "al menos estos permisos".

**-user root** Solo muestra archivos que pertenezcan al usuario root.

**2>/dev/null** Redirige los errores (stderr) al "basurero" (/dev/null). Esto evita que se llene la pantalla con mensajes de "permiso denegado".



|  |
| --- |
|  |

|  |
| --- |
|  |

Vemos que está el binario **/usr/bin/env** por lo que es sencillo usar

Texto

El contenido generado por IA puede ser incorrecto.

Donde **-p** preserva los privilegios efectivos del usuario (por ejemplo, root) al iniciar el shell.

Y listo, somos usuarios **ROOT.**