



# Write-Up: Máquina "Extraviado"

📌 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

Realizo un escaneo simple para encontrar los puertos abiertos. Con **-sS** hago un escaneo sigiloso de puertos TCP y **-Pn** porque ya se que el host está activo.

```
(root@kali)-[~]
# nmap -p- --open -vvv -Pn -sS 172.17.0.2
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-02 15:08 -04
Initiating ARP Ping Scan at 15:08
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 15:08, 0.18s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:08
Completed Parallel DNS resolution of 1 host. at 15:08, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 15:08
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 15:09, 5.77s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000042s latency).
Scanned at 2025-06-02 15:08:58 -04 for 5s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.30 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 76346 (5.160MB)
```

## 2. Escaneo y Enumeración

Ahora, hago un escaneo más agresivo a los puertos abiertos encontrados anteriormente con intención de obtener las versiones de sus servicios.

```
(root@kali)-[~]
# nmap -p22,80 -sC -sV 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-02 15:09 -04
Nmap scan report for 172.17.0.2
Host is up (0.00010s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 256 cc:d2:9b:60:14:16:27:b3:b9:f8:79:10:df:a1:f3:24 (ECDSA)
|_ 256 37:a2:b2:b2:26:f2:07:d1:83:7a:ff:98:8d:91:77:37 (ED25519)
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
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 10.51 seconds
```

Uso Gobuster para buscar directorios de la web, pero no encontré nada interesante.

```
(root@kali)-[~]
# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

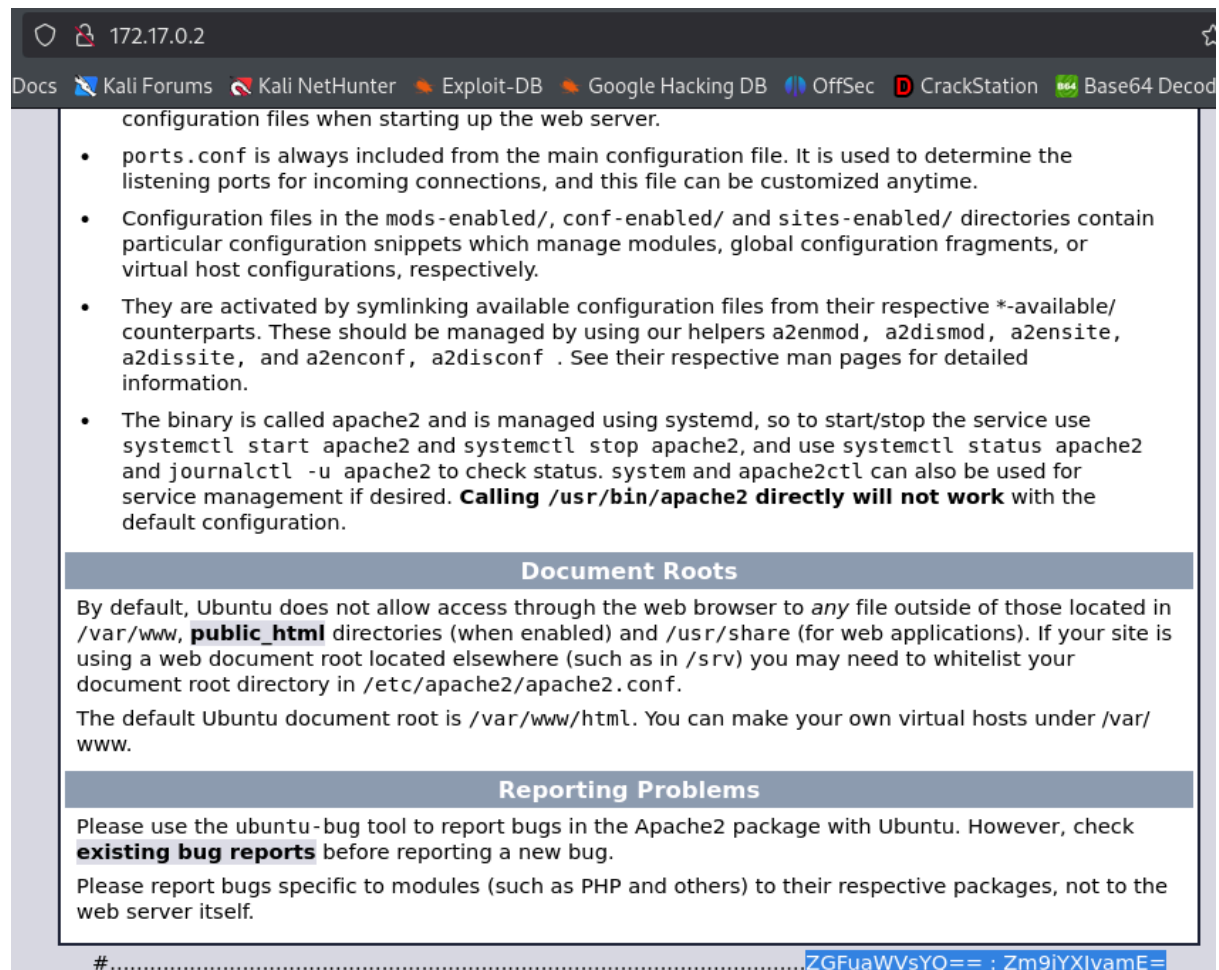
[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.html (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 10844]
/.html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)

Finished
```

Me puse a mirar la interfaz principal de la web existente en el puerto 80, y al final de la página hay un mensaje cifrado, yo diría que está en base64 porque suelen terminar en “==” o similar. Probablemente vengan en formato **usuario:contraseña**. Lo copio.



172.17.0.2

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec CrackStation Base64 Decoder

configuration files when starting up the web server.

- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective \*-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf. See their respective man pages for detailed information.
- The binary is called apache2 and is managed using systemd, so to start/stop the service use systemctl start apache2 and systemctl stop apache2, and use systemctl status apache2 and journalctl -u apache2 to check status. system and apache2ctl can also be used for service management if desired. **Calling /usr/bin/apache2 directly will not work** with the default configuration.

### Document Roots

By default, Ubuntu does not allow access through the web browser to any file outside of those located in /var/www, **public\_html** directories (when enabled) and /usr/share (for web applications). If your site is using a web document root located elsewhere (such as in /srv) you may need to whitelist your document root directory in /etc/apache2/apache2.conf.

The default Ubuntu document root is /var/www/html. You can make your own virtual hosts under /var/www.

### Reporting Problems

Please use the ubuntu-bug tool to report bugs in the Apache2 package with Ubuntu. However, check **existing bug reports** before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to their respective packages, not to the web server itself.

#.....ZGFuaWVsYQ== : Zm9jYXJvamE=

Los descifro por separado en mi terminal, obtengo el usuario y aparentemente su contraseña.

```
(root@kali)-[~]
# echo "ZGFuaWVsYQ==" | base64 -d
daniela

(root@kali)-[~]
# echo "Zm9jYXJvamE=" | base64 -d
focaroja
```

### 3. Explotación de Vulnerabilidades

Con las credenciales obtenidas anteriormente ingreso por el servicio SSH. Ingreso exitoso. No logré escalar privilegios de las formas comunes buscando archivos ejecutables con sudo ni archivos con bit SUID activo.

```
(root@kali)-[~]
# ssh daniela@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:+m+3lOrvpuNRPzkV7ZobI+TK6be0QFiuxBsmiIvgj+E.
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.
daniela@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.12.13-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.

daniela@dockerslabs:~$ whoami
daniela
daniela@dockerslabs:~$ id
uid=1002(daniela) gid=1002(daniela) groups=1002(daniela),100(users)
daniela@dockerslabs:~$ sudo -l
-bash: sudo: command not found
daniela@dockerslabs:~$ find / -perm -4000 <2/dev/null
-bash: 2/dev/null: No such file or directory
```

---

## 4. Escalada de Privilegios y Post-explotación

Me puse a explorar directorios típicos a ver si encontraba algo interesante, incluyendo la búsqueda de archivos ocultos. Encontré una nota pero no es nada tan importante.

```
daniela@dockerlabs:~$ ls
Desktop
daniela@dockerlabs:~$ cd Desktop
daniela@dockerlabs:~/Desktop$ ls
nota
daniela@dockerlabs:~/Desktop$ cat nota
Daniela no recuerdo donde guarde la password de root, si la encuentras me dices.
daniela@dockerlabs:~/Desktop$ ls -la
total 12
drwxrwxr-x 2 daniela daniela 4096 Jan  9 20:35 .
drwxr-x--- 1 daniela daniela 4096 Jun  2 13:12 ..
-rw-rw-r-- 1 daniela daniela   81 Jan  9 20:35 nota
```

En un directorio oculto encuentro un archivo que contiene la contraseña del usuario **“diego”**. La verdad no adiviné a la primera que era en base64, suelo asimilar que los base64 por lo general terminan con un “=” pero en este caso no fué así.

```
daniela@dockerlabs:~/secreto$ ls -la
total 12
drwxrwxr-x 2 daniela daniela 4096 Jan  9 20:47 .
drwxr-x--- 1 daniela daniela 4096 Jun  2 13:12 ..
-rw-rw-r-- 1 daniela daniela   17 Jan  9 20:47 passdiego
daniela@dockerlabs:~/secreto$ cat passdiego
YmFsbGVuYW5lZ3Jh
```

Descifro el mensaje que estaba en base64 y obtengo la contraseña de **“diego”**.

```
(root@kali)-[~]
# echo "YmFsbGVuYW5lZ3Jh" | base64 -d
ballenanegra
```

Me cambio al usuario diego usando la contraseña encontrada anteriormente. Me pongo a buscar nuevamente directorios o archivos ocultos, y encuentro uno, este si supe que estaba cifrado en base64 instantáneamente.

```
daniela@dockerlabs:~/secreto$ su diego
Password:
diego@dockerlabs:/home/daniela/secreto$ cd ~
diego@dockerlabs:~$ ls -la
total 36
drwxr-x— 1 diego diego 4096 Jan  9 21:11 .
drwxr-xr-x 1 root  root  4096 Jan  9 19:57 ..
-rw-r--r-- 1 diego diego  233 Jan  9 21:11 .bash_logout
-rw-r--r-- 1 diego diego 3771 Jan  9 19:56 .bashrc
drwxrwxr-x 1 diego diego 4096 Jan  9 20:51 .local
drwxrwxr-x 1 diego diego 4096 Jan 11 14:29 .passroot
-rw-r--r-- 1 diego diego  807 Jan  9 19:56 .profile
-rw-rw-r-- 1 diego diego   15 Jan  9 20:52 pass
diego@dockerlabs:~$ cat pass
donde estara?
diego@dockerlabs:~$ cd .passroot
diego@dockerlabs:~/passroot$ ls -la
total 12
drwxrwxr-x 1 diego diego 4096 Jan 11 14:29 .
drwxr-x— 1 diego diego 4096 Jan  9 21:11 ..
-rw-rw-r-- 1 diego diego   21 Jan 11 14:29 .pass
diego@dockerlabs:~/passroot$ cat .pass
YWNhdGFtcG9jb2VzdGE=
```

Lo descifro en mi terminal, pero fuí estafado, no era nada importante.

```
(root@kali)-[~]
# echo "YWNhdGFtcG9jb2VzdGE=" | base64 -d
acatampocoesta
```

```
diego@dockerlabs:~/local/share$ cat .-  
  
password de root  
  
En un mundo de hielo, me muevo sin prisa,  
con un pelaje que brilla, como la brisa.  
No soy un rey, pero en cuentos soy fiel,  
de un color inusual, como el cielo y el mar  
tambien.  
Soy amigo de los ni~nos, en historias de  
ensue~no.  
Quien soy, que en el frio encuentro mi due~no?
```

```
diego@dockerlabs:~/local/share$ su root
Password:
root@dockerlabs:/home/diego/.local/share# whoami
root
root@dockerlabs:/home/diego/.local/share# id
uid=0(root) gid=0(root) groups=0(root)
root@dockerlabs:/home/diego/.local/share#
```

La verdad no me gustó esta máquina, la escalada de privilegios consistía solo en entrar y salir de carpetas, perder tiempo en trampas y un acertijo que era fácil de adivinar, no creo que en un caso real haya algo así.

## Banderas y Resultados

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