🏴‍☠️ Write-Up: Máquina "Extraviado"

📌 **Plataforma: DockerLabs**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **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

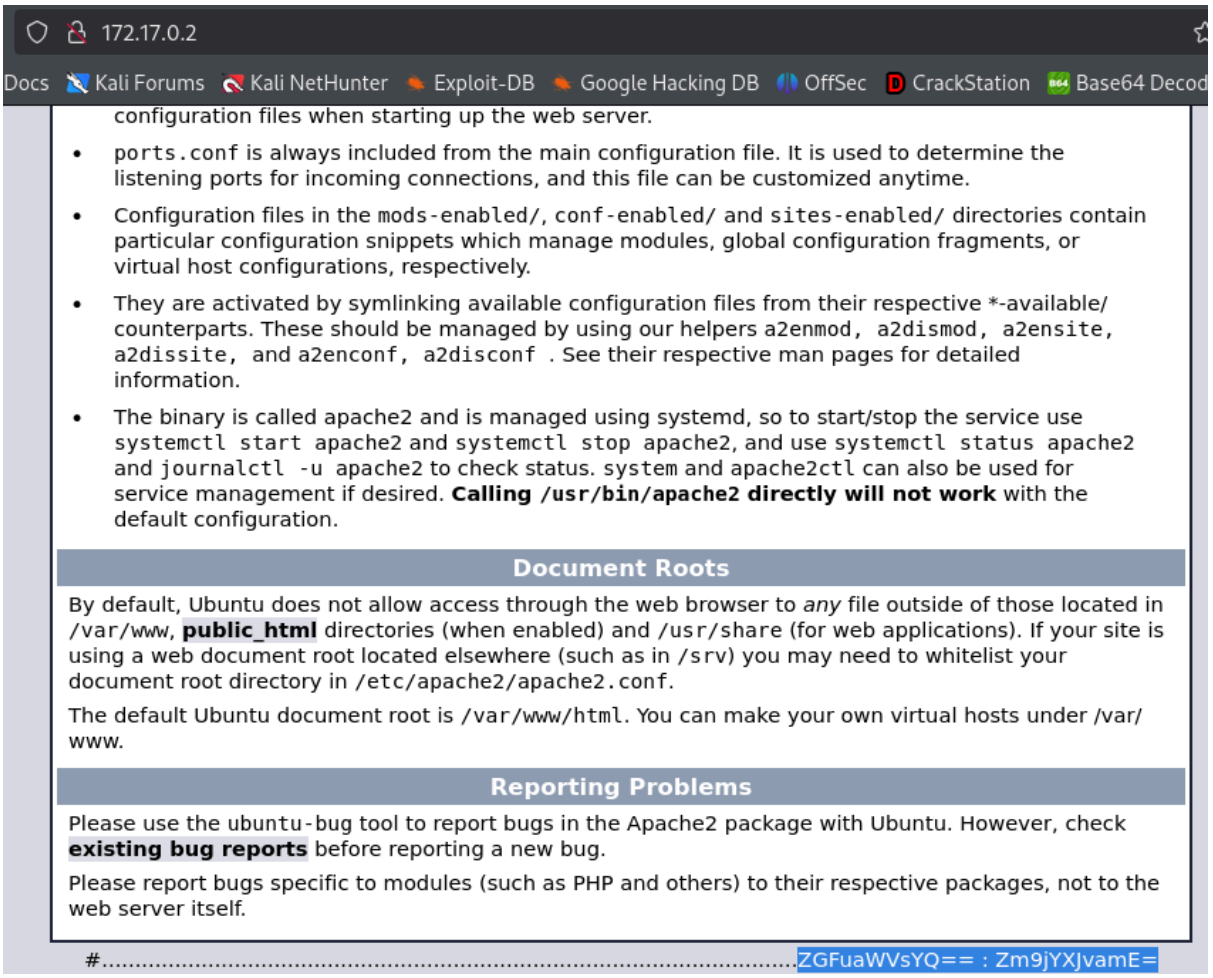
Ahora, hago un escaneo más agresivo a los puertos abiertos encontrados anteriormente con intención de obtener las versiones de sus servicios.

```
┌──(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
```

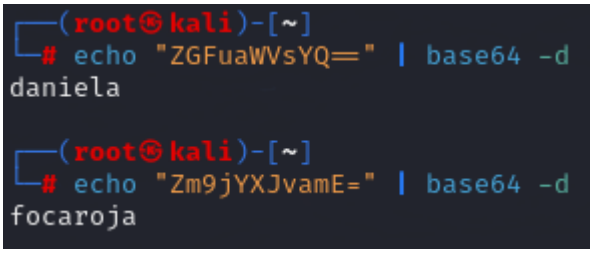
Uso Gobuster para buscar directorios de la web, pero no encontré nada interesante.

```
┌──(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:contaseña**. Lo copio.

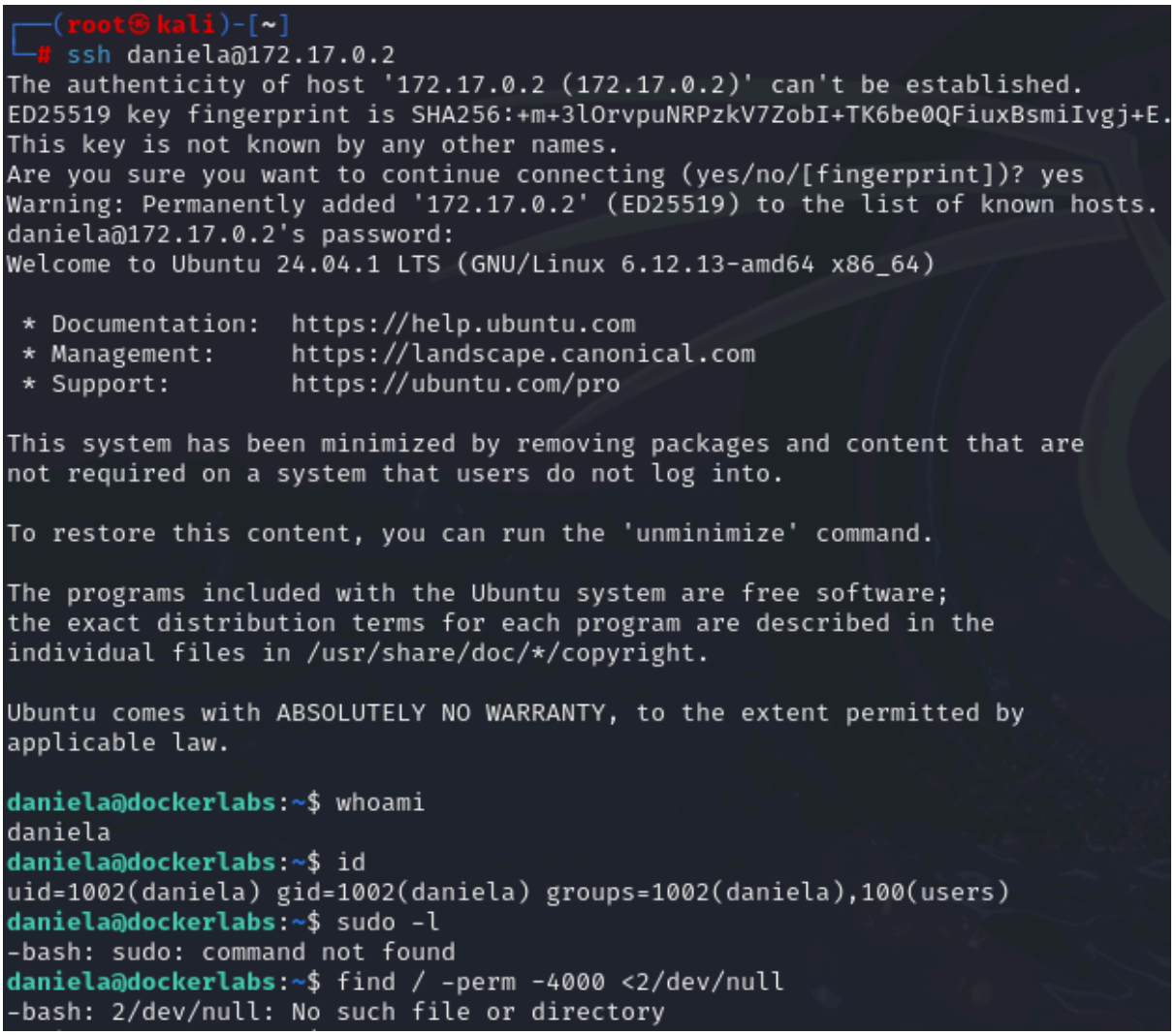


Los descifro por separado en mi terminal, obtengo el usuario y aparentemente su contraseña.



💥 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.



🔐 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
```

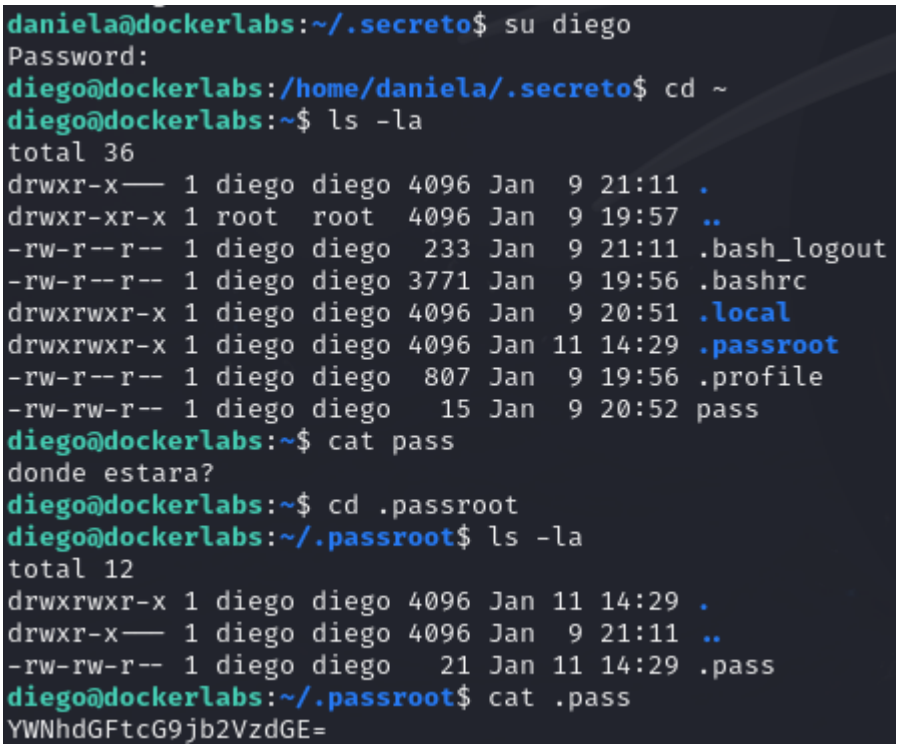
En un directorio oculto encuentro un archivo que contiene la contraseña del usuario “**diego**”. La verdad no adiviné a la primera que era en base64, suelo asimilar que los base64 por lo general terminan con un “=” pero en este caso no fué así.

```
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**”.

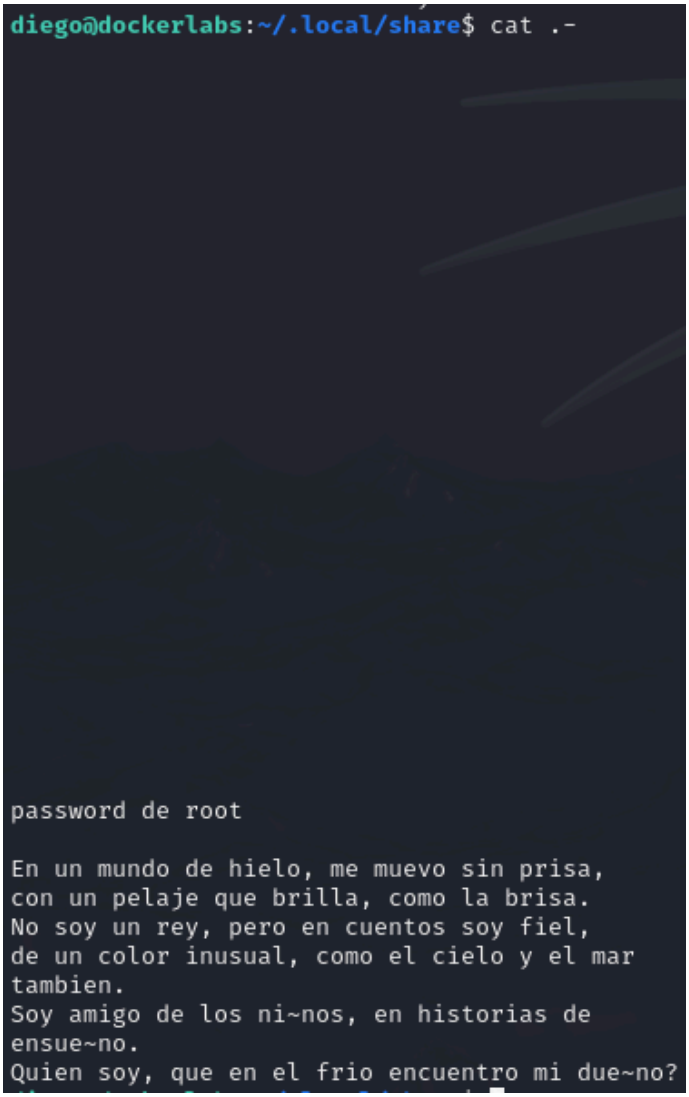
```
┌──(root㉿kali)-[~]
└─# echo "YmFsbGVuYW5lZ3Jh" | base64 -d
ballenanegra
```

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.

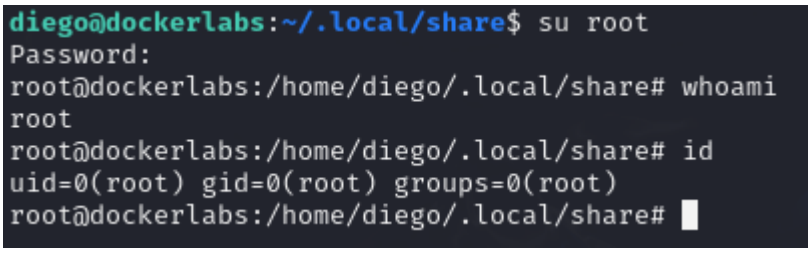


Lo descifro en mi terminal, pero fuí estafado, no era nada importante.

Seguí explorando la máquina, fué un poco tedioso, sobre todo la parte en que fui estafado. Finalmente encontré algo raro, un acertijo que la respuesta debe ser la contraseña de root.



Bueno, después de unos intentos adiviné como era la contraseña. Básicamente el acertijo hacía referencia a un oso azul (contraseña: **osoazul**) siguiendo el juego de contraseñas anteriores como “**ballenanegra**” o “**focaroja**”.



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.