🏴‍☠️ Write-Up: Máquina "BorazuwarahCTF"

📌 **Plataforma: Dockerlabs**
📌 **Dificultad: Muy fácil**
📌 **Autor: Joaquín Picazo**

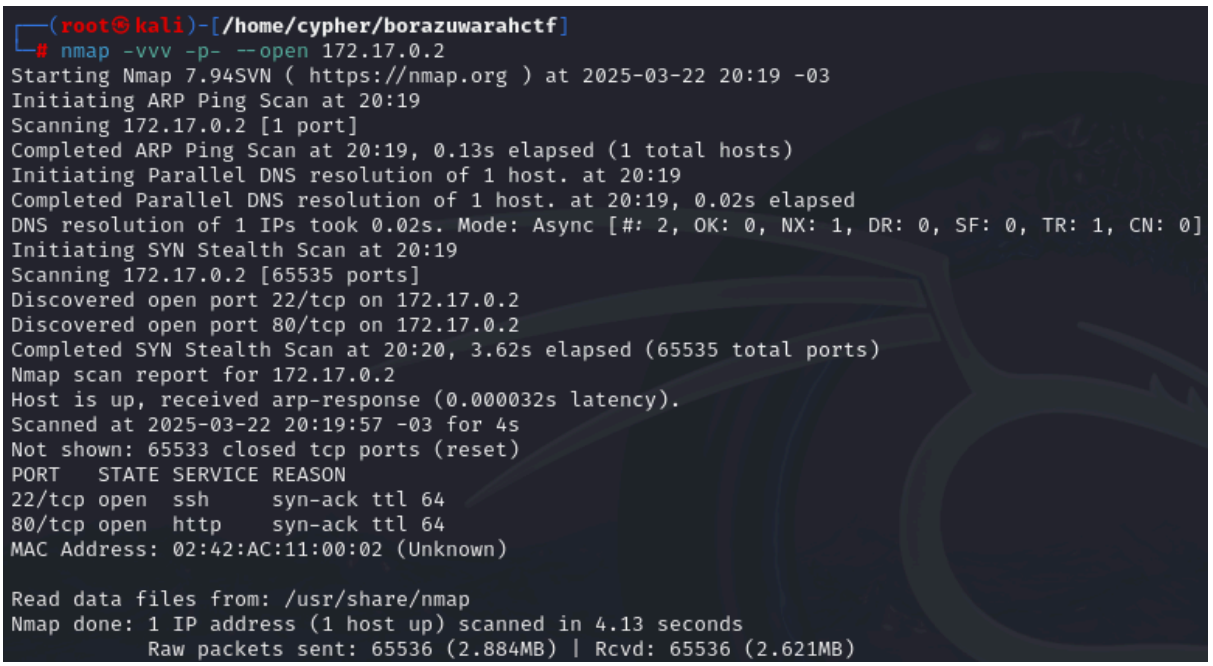
🔎 Metodología de Pentesting

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

Hacer un escaneo general solo para saber que puertos están abiertos.



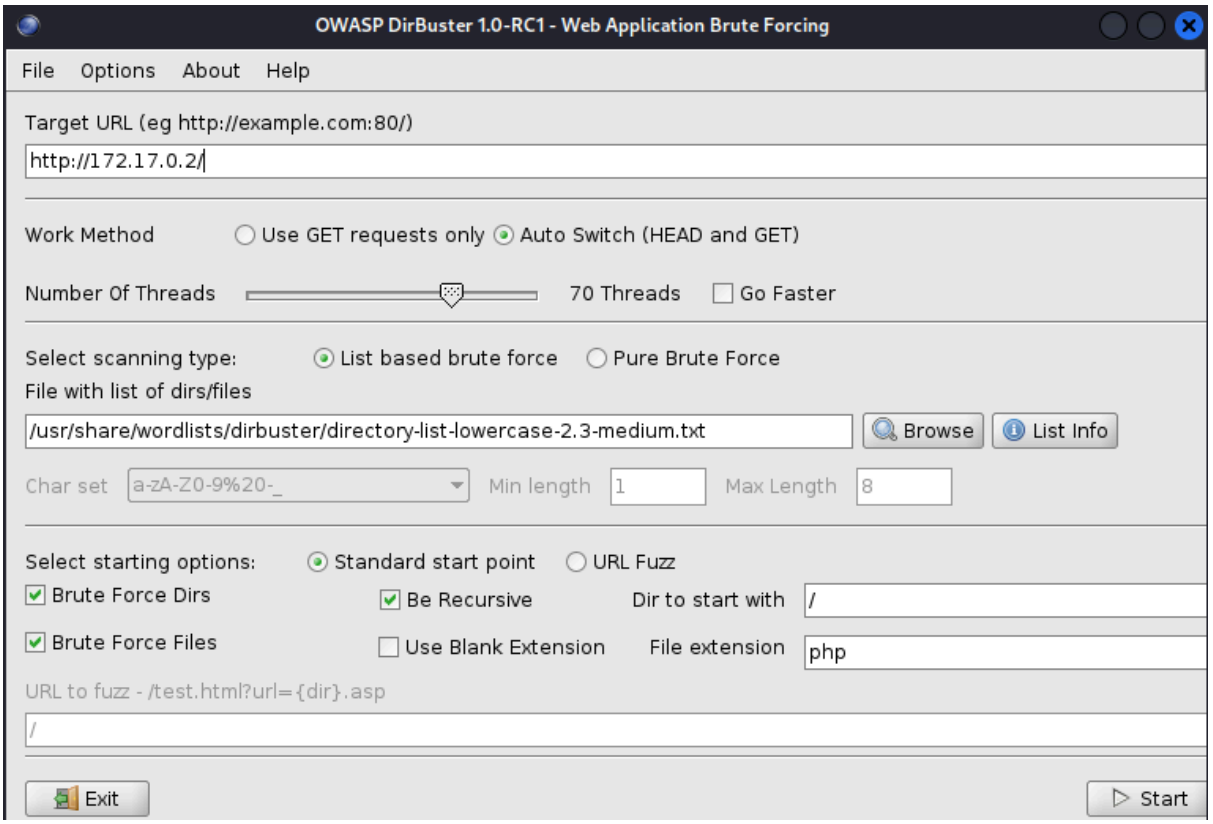
🎯 2. Escaneo y Enumeración

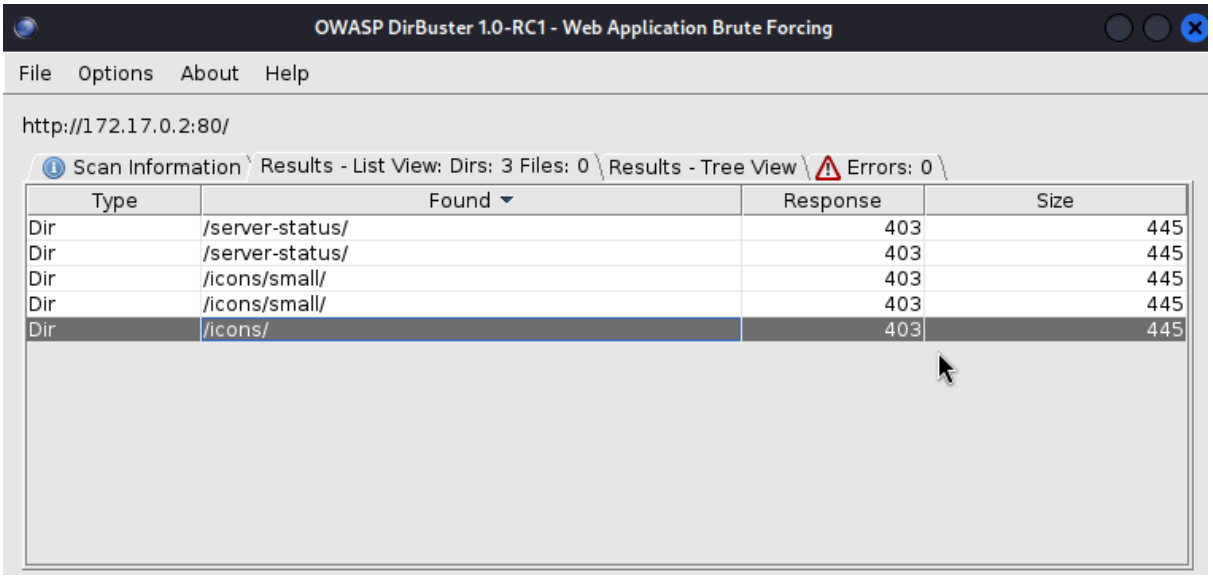
Ya sabiendo los puertos abiertos, se hace un escaneo más profundo específicamente en esos puertos para obtener versiones y servicios.

```
┌──(root㉿kali)-[/home/cypher/borazuwarahctf]
└─# nmap -vvv -p 22,80 -sV -sC 172.17.0.2
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 3d:fd:d7:c8:17:97:f5:12:b1:f5:11:7d:af:88:06:fe (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDuOdJLZN+CNU+7dcTJQbPr6zY2+Ou1YFR0w9Pan1DfaPUZljRHJcNmvSncrihzQ3HOAHfMWWvSzN+ZMC0YmWoA=
|   256 43:b3:ba:a9:32:c9:01:43:ee:62:d0:11:12:1d:5d:17 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGDv2JqKvBCR+Badmkr7YKPypEYshuCXxzM5+YdozyBD
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.59 ((Debian))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.59 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Busco directorios con Dirbuster. Sin embargo, no encontré nada interesante.





Al abrir la web que se encuentra en su puerto 80, hay una imagen. Se puede descargar para verificar si tiene archivos ocultos en ella o información importante en sus metadatos.

💥 3. Explotación de Vulnerabilidades

Uso steghide para encontrar archivos ocultos dentro de la imagen. Sin embargo, no hay nada interesante.

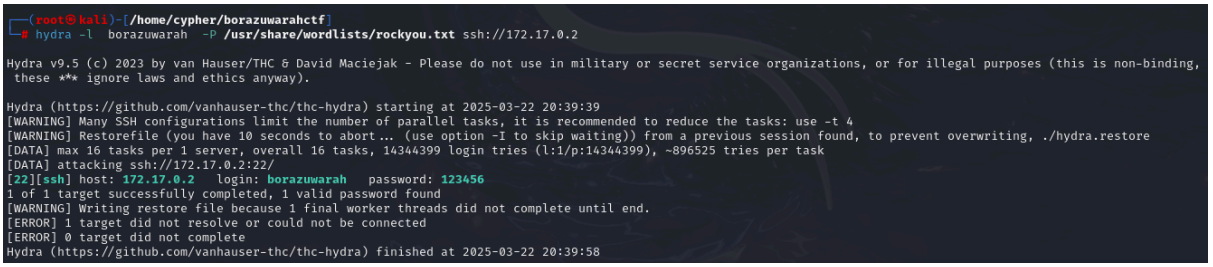
```
┌──(root㉿kali)-[/home/cypher/borazuwarahctf]
└─# steghide extract -sf imagen.jpeg
Anotar salvoconducto:
anot◆ los datos extra◆dos e/"secreto.txt".

┌──(root㉿kali)-[/home/cypher/borazuwarahctf]
└─# cat secreto.txt
Sigue buscando, aquí no está to solución
aunque te dejo una pista....
sigue buscando en la imagen!!!
```

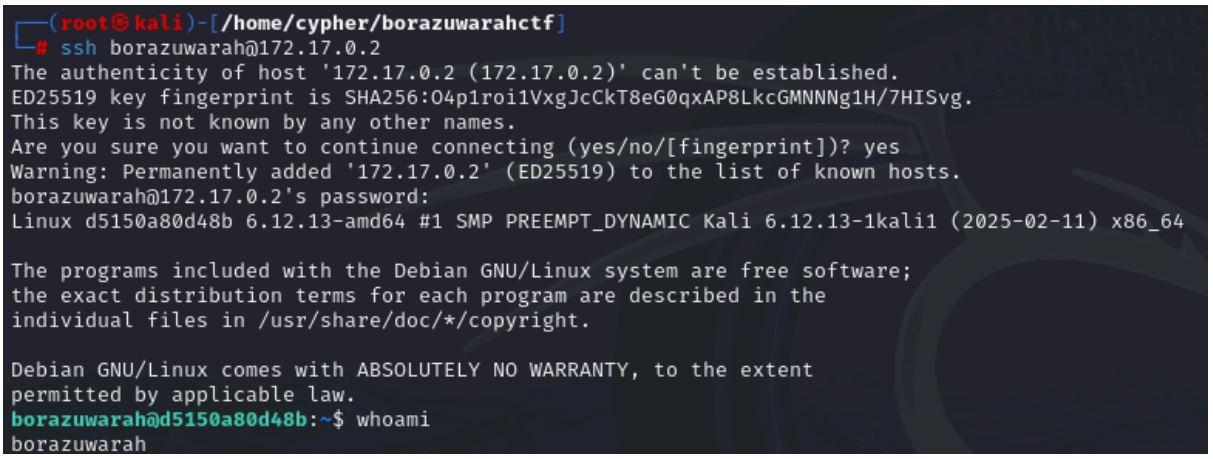
Ahora, utilizo la herramienta exiftool para ver información en sus metadatos. Se logra obtener un nombre de usuario, pero no se otorga ninguna contraseña. Esto podría ser un usuario para ingresar por vía SSH.

```
┌──(root㉿kali)-[/home/cypher/borazuwarahctf]
└─# exiftool imagen.jpeg
ExifTool Version Number         : 13.00
File Name                       : imagen.jpeg
Directory                       : .
File Size                       : 19 kB
File Modification Date/Time     : 2025:03:22 20:38:12-03:00
File Access Date/Time           : 2025:03:22 20:38:23-03:00
File Inode Change Date/Time     : 2025:03:22 20:38:12-03:00
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
XMP Toolkit                     : Image::ExifTool 12.76
Description                     : ---------- User: borazuwarah ----------
Title                           : ---------- Password:  ----------
Image Width                     : 455
Image Height                    : 455
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 455×455
Megapixels                      : 0.207
```

Como sólo se tiene un usuario, pero ninguna contraseña. Se debe aplicar fuerza bruta a su servicio SSH. Se utilizará hydra.



Como se puede ver, se encontró una contraseña. Ahora se prueba acceso.

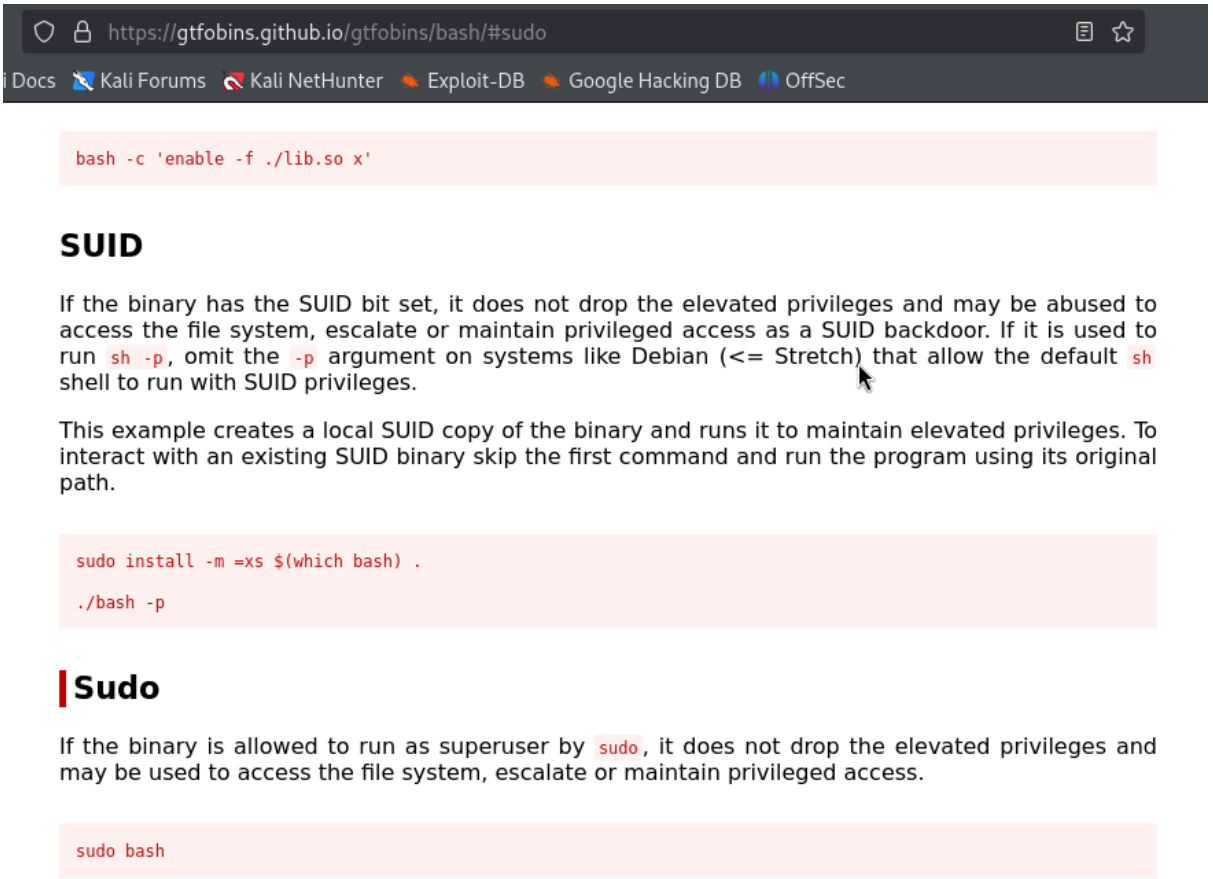


Acceso exitoso.

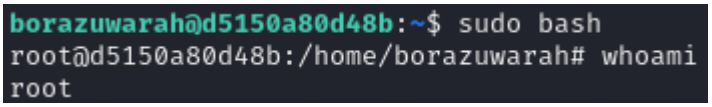
🔐 4. Escalada de Privilegios y Post-explotación

Primero, verificar si hay alguna forma de escalar privilegios con “sudo -l”. Y efectivamente hay un archivo que me podría ayudar a escalar pivilegios.

En GTFOBins busco el archivo encontrado para verificar si hay alguna forma de explotarlo para escalar privilegios. Y efectivamente, si la hay.



Ingresé el comando de GTFOBins, y se logró acceso a root.



🏆 Banderas y Resultados

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