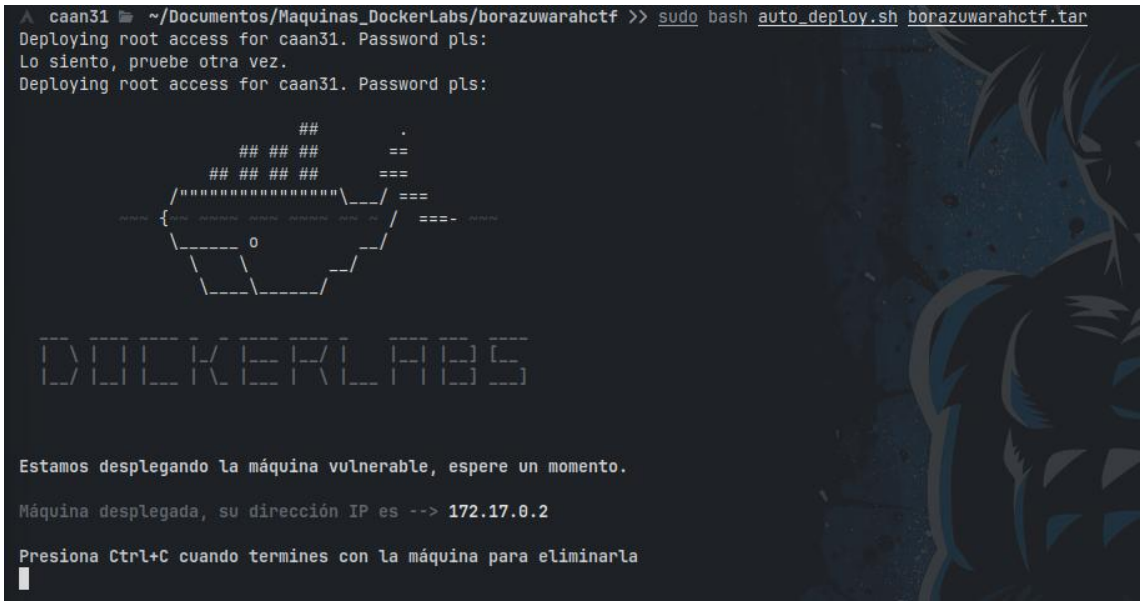
Desplegaremos la maquina



Haremos un ping para comprobar que tenemos conexión a la maquina víctima.

```
caan31 ~ >> ping -c 2 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.085 ms

64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.033 ms

--- 172.17.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 10
35ms
rtt min/avg/max/mdev = 0.033/0.059/0.085/0.026 ms
```

Haremos un escaneo con nmap, **-Pn** desactiva la detección de hosts activos (ping), tratando todos los objetivos como si estuvieran en línea, útil cuando los pings están bloqueados por firewalls.

```
caan31 ~ >> nmap -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 18:54 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00011s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Ahora que ya sabemos que puertos están abiertos, haremos un escaneo más profundo con la versión de cada servicio con -p y -sCV

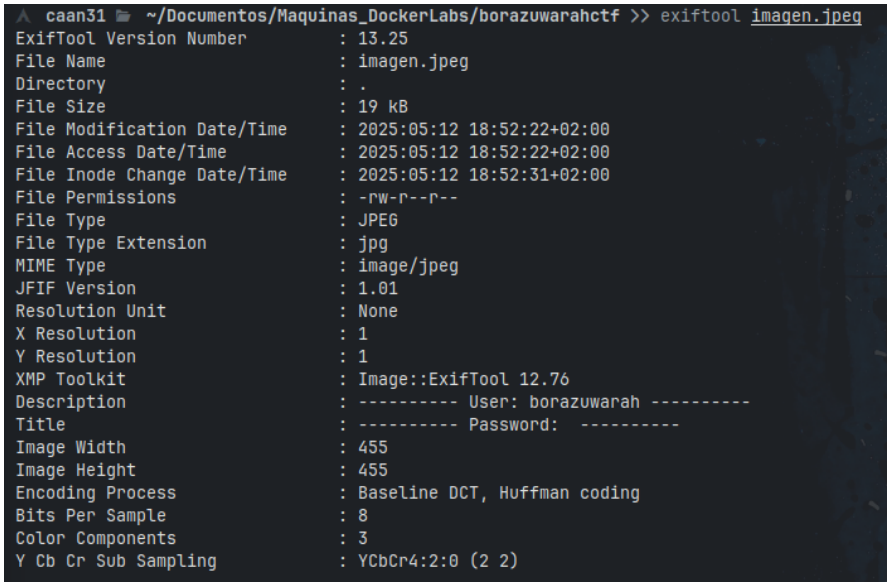
```
caan31 ~ >> nmap -p22,80 -sCV -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 18:54 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00038s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     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)
|_  256 43:b3:ba:a9:32:c9:01:43:ee:62:d0:11:12:1d:5d:17 (ED25519)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.59 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vemos que tenemos el puerto 80 abierto, así que miraremos que contiene la pagina del servidor.

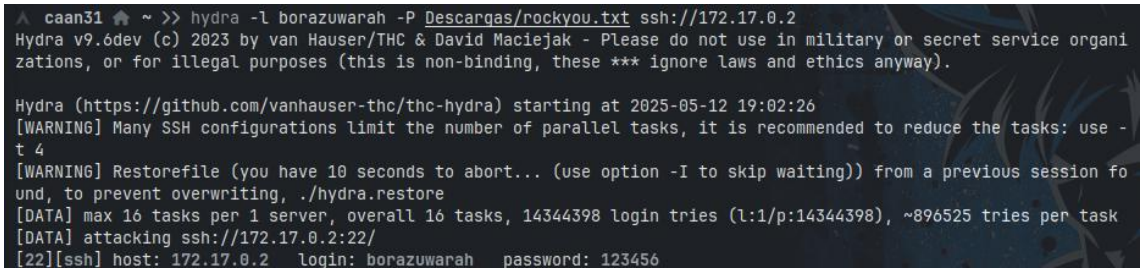
Vemos que tiene una imagen, inspeccionando el código no nos encontramos nada así que descargaremos la imagen para ver que podemos encontrar.

Utilizando **exiftool** que es una herramienta de línea de comandos que permite leer, editar y eliminar metadatos de archivos como fotos, videos, audios y documentos, examinaremos la imagen descargada.

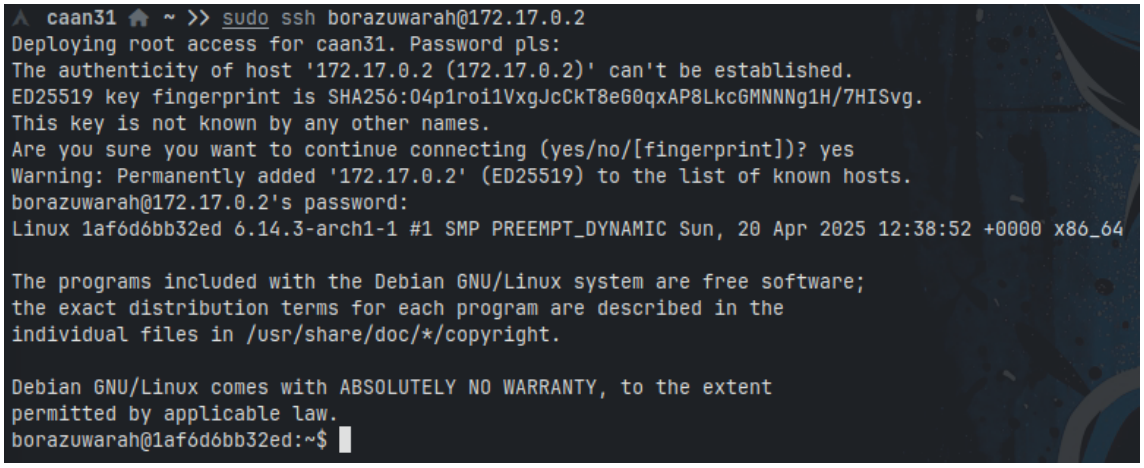
Podemos encontrar varios metadatos, dentro de ellos encontramos el usuario.



Ahora con el nombre del usuario podremos hacer un ataque con hydra para encontrar la contraseña.



Al encontrarla podremos conectarnos con el usuario y contraseña encontradas.



Al momento de escalar privilegios utilizamos el comando sudo -l y vemos que simplemente utilizando el comando sudo su, nos pedirá la contraseña del usuario y ya seremos root.