Vamos a desplegar la maquina

Haremos un escaneo profundo de la máquina.

En el fichero que hemos generado podemos ver los puertos abiertos de la máquina.

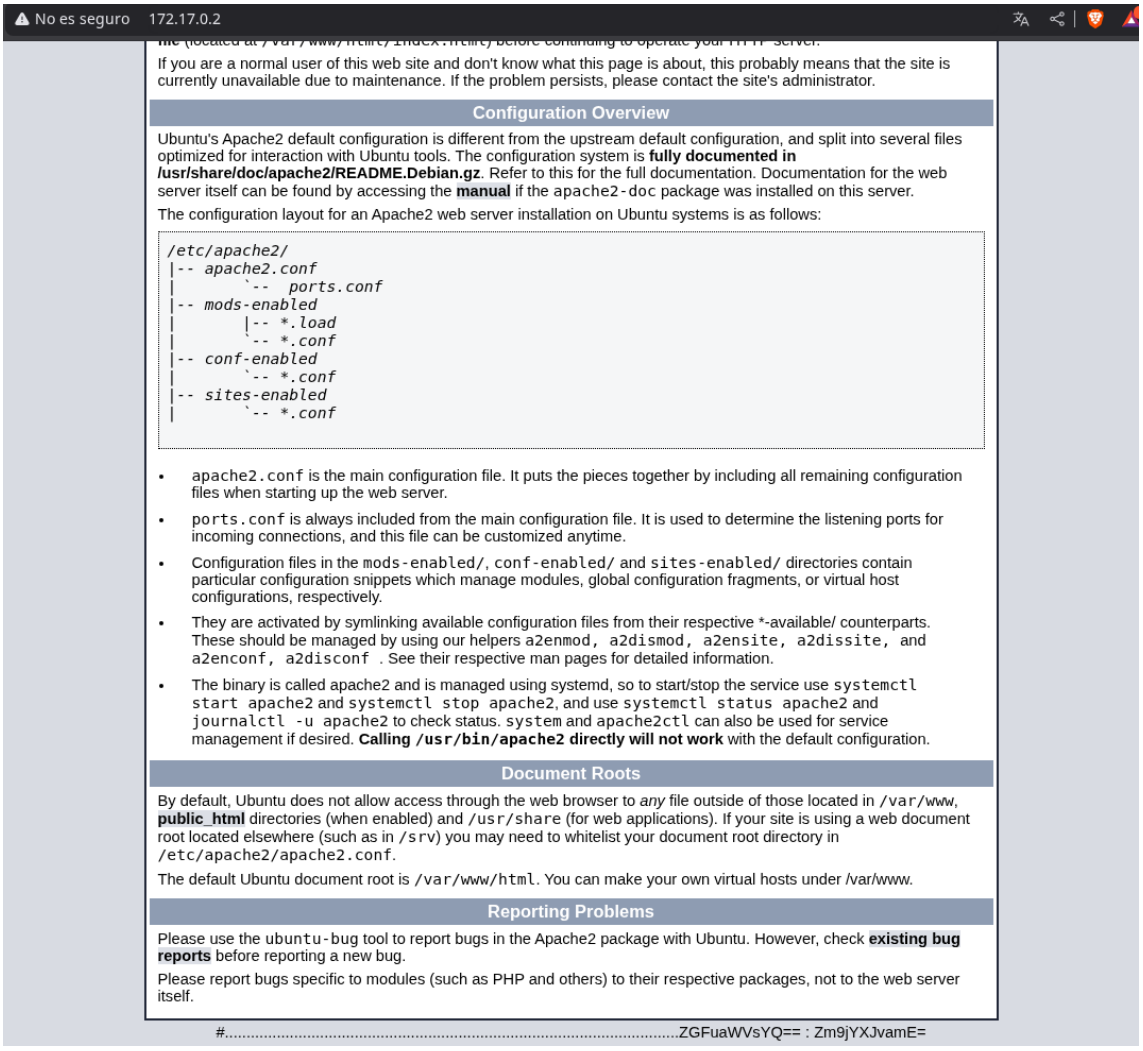
```
❯ cat PuertosExtraviado
```

File: **PuertosExtraviado**

```
# Nmap 7.95 scan initiated Wed Sep  3 21:19:20 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p
- -vvv --open -oN PuertosExtraviado 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000070s latency).
Scanned at 2025-09-03 21:19:20 CEST for 1s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
| ssh-hostkey:
|   256 cc:d2:9b:60:14:16:27:b3:b9:f8:79:10:df:a1:f3:24 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP+OTZeMj+iOYGoGNHCDrHUIQkt2SFwk
2xRrNbDmWaMzKU2VijE4vADaT1p2MEwe5CYAks/5ZWAc53IbmeEKD4k=
|   256 37:a2:b2:b2:26:f2:07:d1:83:7a:ff:98:8d:91:77:37 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJrTvCLEYLPYegFzNm0ZZPbG02YvabBcv7CH6nhpbBKH
80/tcp open  http    syn-ack ttl 64
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
# Nmap done at Wed Sep  3 21:19:21 2025 -- 1 IP address (1 host up) scanned in 1.20 seconds
```

Vamos a ver que contiene el servidor web y podemos ver que al final de la página encontramos una codificación en base64.



Utilizaremos nuestra propia maquina para poder ver que es lo que contiene ese código.

```
❯ echo "ZGFuaWVsYQ=" | base64 -d
daniela%
❯ echo "Zm9jYXJvamE" | base64 -d
focaroja%
```

Podemos ver un supuesto usuario y posiblemente la contraseña, así que intentaremos acceder por ssh.

```
❯ ssh daniela@172.17.0.2
daniela@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.12.25-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.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

daniela@dockerlabs:~$
```

Ahora explorando un poco, podemos ver una nota que nos da indicios que la contraseña de root tiene que estar por aquí escondida.

```
daniela@dockerlabs:~$ ls
Desktop
daniela@dockerlabs:~$ cd Desktop/
daniela@dockerlabs:~/Desktop$ ls
nota
daniela@dockerlabs:~/Desktop$ cat nota
Daniela no recuerdo donde guarde la password de root, si la encuentras me dices.
```

Al buscar un poco mas en ficheros ocultos, podemos ver un fichero .secreto donde encontramos la contraseña del usuario diego en base64

```
daniela@dockerlabs:~$ ls -la
total 40
drwxr-x--- 1 daniela daniela 4096 Sep  3 13:22 .
drwxr-xr-x 1 root    root    4096 Jan  9  2025 ..
-rw-r--r-- 1 daniela daniela  220 Jan  9  2025 .bash_logout
-rw-r--r-- 1 daniela daniela 3771 Jan  9  2025 .bashrc
drwx------ 2 daniela daniela 4096 Sep  3 13:22 .cache
drwxrwxr-x 3 daniela daniela 4096 Jan  9  2025 .local
-rw-r--r-- 1 daniela daniela  807 Jan  9  2025 .profile
drwxrwxr-x 2 daniela daniela 4096 Jan  9  2025 .secreto
drwxrwxr-x 2 daniela daniela 4096 Jan  9  2025 Desktop
daniela@dockerlabs:~$ cd .secreto/
daniela@dockerlabs:~/.secreto$ ls
passdiego
daniela@dockerlabs:~/.secreto$ cat passdiego
YmFsbGVuYW5lZ3Jh
daniela@dockerlabs:~/.secreto$
```

```
❯ echo "YmFsbGVuYW5lZ3Jh" | base64 -d
ballenanegra%
```

Al ver cuantos usuarios podemos ver que un usuario es diego.

```
daniela@dockerlabs:/etc$ cd /home/
daniela@dockerlabs:/home$ ls
daniela  diego  ubuntu
```

Accederemos al perfil de diego y explorando un poco podremos encontrar un fichero pass, vamos a ver que contiene.

```
daniela@dockerlabs:/home$ su diego
Password:
diego@dockerlabs:/home$ ls
daniela  diego  ubuntu
diego@dockerlabs:/home$ cd
diego@dockerlabs:~$ ls
pass
diego@dockerlabs:~$ cat pass
donde estara?
diego@dockerlabs:~$ ls -la
total 36
drwxr-x--- 1 diego diego 4096 Jan  9  2025 .
drwxr-xr-x 1 root  root  4096 Jan  9  2025 ..
-rw-r--r-- 1 diego diego  233 Jan  9  2025 .bash_logout
-rw-r--r-- 1 diego diego 3771 Jan  9  2025 .bashrc
drwxrwxr-x 1 diego diego 4096 Jan  9  2025 .local
drwxrwxr-x 1 diego diego 4096 Jan 11  2025 .passroot
-rw-r--r-- 1 diego diego  807 Jan  9  2025 .profile
-rw-rw-r-- 1 diego diego   15 Jan  9  2025 pass
diego@dockerlabs:~$ cd .passroot/
diego@dockerlabs:~/.passroot$ ls
diego@dockerlabs:~/.passroot$ ls -la
total 12
drwxrwxr-x 1 diego diego 4096 Jan 11  2025 .
drwxr-x--- 1 diego diego 4096 Jan  9  2025 ..
-rw-rw-r-- 1 diego diego   21 Jan 11  2025 .pass
diego@dockerlabs:~/.passroot$ cat .pass
YWNhdGFtcG9jb2VzdGE=
diego@dockerlabs:~/.passroot$
```

Vemos que continuamos sin encontrar la contraseña de root.

```
❯ echo "YWNhdGFtcG9jb2VzdGE" | base64 -d
acatampocoesta%
```

Al explorar un poco mas podemos ver un archivo con un nombre raro .-, lo exploramos a ver con que nos encontramos.

```
drwxrwxr-x 1 diego diego 4096 Jan  9  2025 .local
drwxrwxr-x 1 diego diego 4096 Jan 11  2025 .passroot
-rw-r--r-- 1 diego diego  807 Jan  9  2025 .profile
-rw-rw-r-- 1 diego diego   15 Jan  9  2025 pass
diego@dockerlabs:~$ cd .local/
diego@dockerlabs:~/.local$ ls -la
total 12
drwxrwxr-x 1 diego diego 4096 Jan  9  2025 .
drwxr-x--- 1 diego diego 4096 Jan  9  2025 ..
drwx------ 1 diego diego 4096 Jan 11  2025 share
diego@dockerlabs:~/.local$ cd share/
diego@dockerlabs:~/.local/share$ ls -la
total 16
drwx------ 1 diego diego 4096 Jan 11  2025 .
-rw-r--r-- 1 root  root   319 Jan 11  2025 .-
drwxrwxr-x 1 diego diego 4096 Jan  9  2025 ..
drwx------ 2 diego diego 4096 Jan  9  2025 nano
diego@dockerlabs:~/.local/share$ cat .-
```

Podemos ver la contraseña de root en un acertijo.

```
password de root

En un mundo de hielo, me muevo sin prisa,
con un pelaje que brilla, como la brisa.
No soy un rey, pero en cuentos soy fiel,
de un color inusual, como el cielo y el mar
tambien.
Soy amigo de los ni~nos, en historias de
ensue~no.
Quien soy, que en el frio encuentro mi due~no?
```

Luego de buscar el acertijo que es osoazul, podremos ingresar como root.

```
diego@dockerlabs:~/.local/share$ su root
Password:
root@dockerlabs:/home/diego/.local/share# cd
root@dockerlabs:~# whoami
root
root@dockerlabs:~#
```