

Desplegamos la máquina.

```
> sudo bash auto_deploy.sh extraviado.tar  
[sudo] contraseña para kali:
```

##  
## ## ## ==  
## ## ## ## ==  
NNN {NN NNNN NNN NNNN NN N} ==- NNN  
0

DOCKEERLABS

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Le hacemos un ping para comprobar la conectividad y con el ttl de 64 vemos que estamos ante una máquina Linux.

```
> ping -c 1 172.17.0.2
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=0.058 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.058/0.058/0.058/0.000 ms
```

Con nmap comprobamos los puertos abiertos y sus servicios.

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 cc:d2:9b:60:14:16:27:b3:b9:f8:79:10:df:a1:f3:24 (ECDSA)
|_  256 37:a2:b2:b2:26:f2:07:d1:83:7a:ff:98:8d:91:77:37 (ED25519)
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

En la web encontramos en base64 una especie de usuario:contraseña.

**Reporting Problems**

Please use the `ubuntu-bug` tool to report bugs in the Apache2 package with Ubuntu. However, check **existing bug reports** before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to their respective packages, not to the web server itself.

#.....ZGFuaWVsYO== : Zm9iYXJvamE=

Lo desencriptamos para obtener el usuario y la contraseña en texto claro y accedemos mediante ssh a la máquina.

```
> echo 'ZGFuaWVsYQ==' | base64 -d; echo
daniela

> ssh daniela@172.17.0.2
daniela@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GN
```

Encontramos un directorio llamado .secreto y vemos a parte de Daniela que más usuarios hay.

```
daniela@dockerlabs:~/secreto$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
diego:x:1001:1001:diego,,,:/home/diego:/bin/bash
daniela:x:1002:1002:daniela,,,:/home/daniela:/bin/bash
```

Dentro del directorio vemos el archivo passwdiego y lo desencriptamos con base64.

```
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 -la
total 12
drwxrwxr-x 2 daniela daniela 4096 Jan 9 2025 .
drwxr-x--- 1 daniela daniela 4096 Jul 19 22:59 ..
-rw-rw-r-- 1 daniela daniela 17 Jan 9 2025 passwdiego
daniela@dockerlabs:~/secreto$ cat passwdiego
YmFsbGVuYW5lZ3Jh
> echo 'YmFsbGVuYW5lZ3Jh' | base64 -d; echo
ballenanegra
```

Accedemos como Diego con la contraseña en texto claro y leemos el archivo pass.

```
daniela@dockerlabs:~/secreto$ su diego
Password:
diego@dockerlabs:/home/daniela/secreto$ cd
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:~$ cat pass
donde estara?
```

Nos metemos en el directorio .passroot, pero es un trolleito.

```
diego@dockerlabs:~$ cd .passroot/
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=
> echo 'YWNhdGFtcG9jb2VzdGE=' | base64 -d; echo
acatampocoesta
```

Descubrimos un archivo en la carpeta share que se llama .-

```
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 .-
```

Le hacemos un cat para comprobar el contenido y es como una especie de acertijo.

```
diego@dockerlabs:~/.local/share$ cat .-
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?
```

El cual le pasamos a chatgpt y nos da una serie de contraseñas.

```
Resumen de posibles contraseñas:
• ositoazul
• osoazul
• osoazuldepeluche
• cariñositoazul
• pelucheazul
• azulito
```

Aplicamos una de las contraseñas proporcionadas con el usuario root y listo.

```
diego@dockerlabs:~/.local/share$ su root
Password:
root@dockerlabs:/home/diego/.local/share# id
uid=0(root) gid=0(root) groups=0(root)
```