🏴‍☠️ Write-Up: Máquina "Upload"

📌 **Plataforma: DockerLabs**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

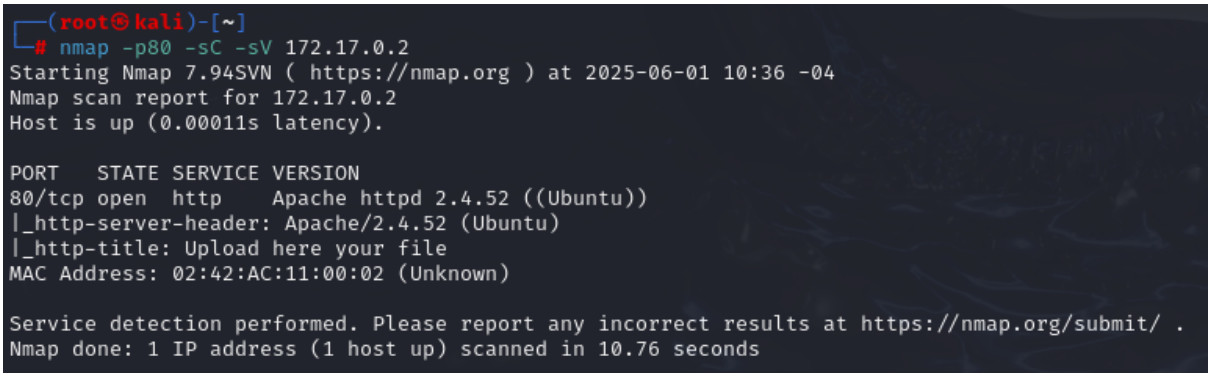
📡 1. Reconocimiento y Recolección de Información

Realizo un escaneo simple para encontrar los puertos abiertos. Con **-Ss** hago un escaneo sigiloso de puertos TCP y **-Pn** porque ya se que el host está activo.

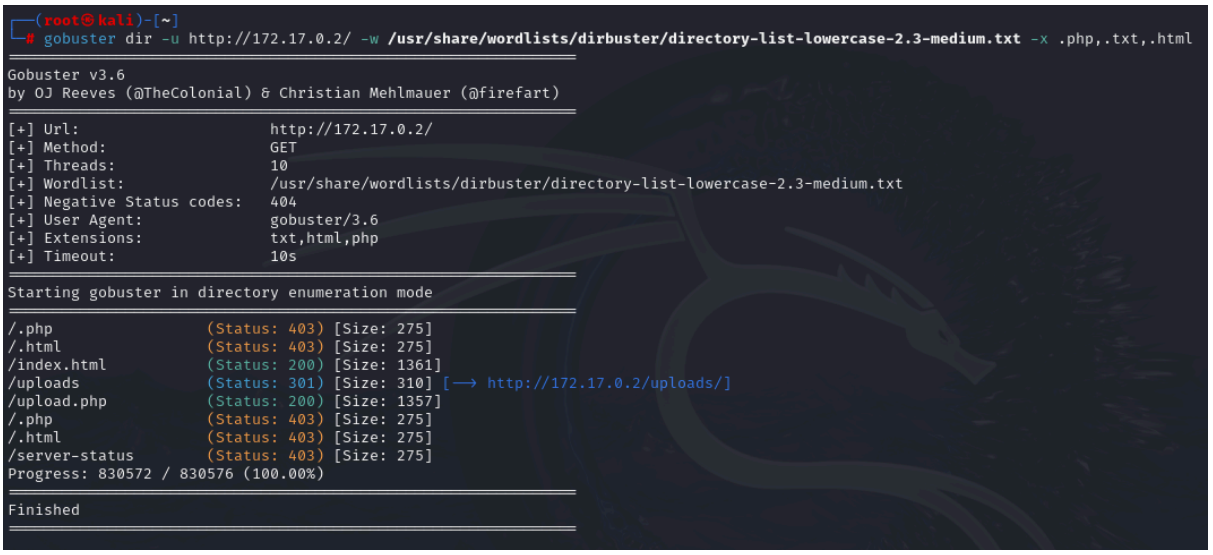
```
┌──(root㉿kali)-[~]
└─# nmap -p- --open -vvv -Pn -sS 172.17.0.2
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-01 10:35 -04
Initiating ARP Ping Scan at 10:35
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 10:35, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:35
Completed Parallel DNS resolution of 1 host. at 10:35, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 10:35
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 10:35, 3.96s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000041s latency).
Scanned at 2025-06-01 10:35:32 -04 for 4s
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.49 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

🎯 2. Escaneo y Enumeración

Realizo un escaneo más riguroso al puerto abierto encontrado anteriormente para encontrar sus servicios y versiones.

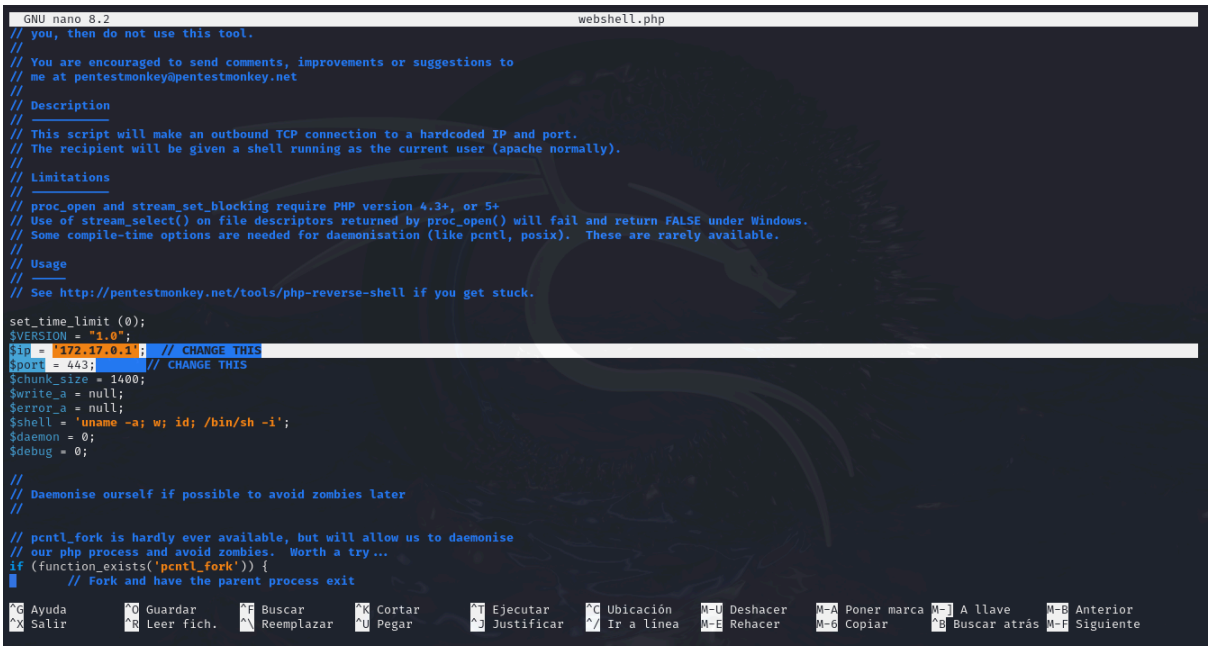


Uso gobuster para buscar directorios en la web del puerto 80. Los más interesantes parecen ser **/uploads** y **/uploads.php**

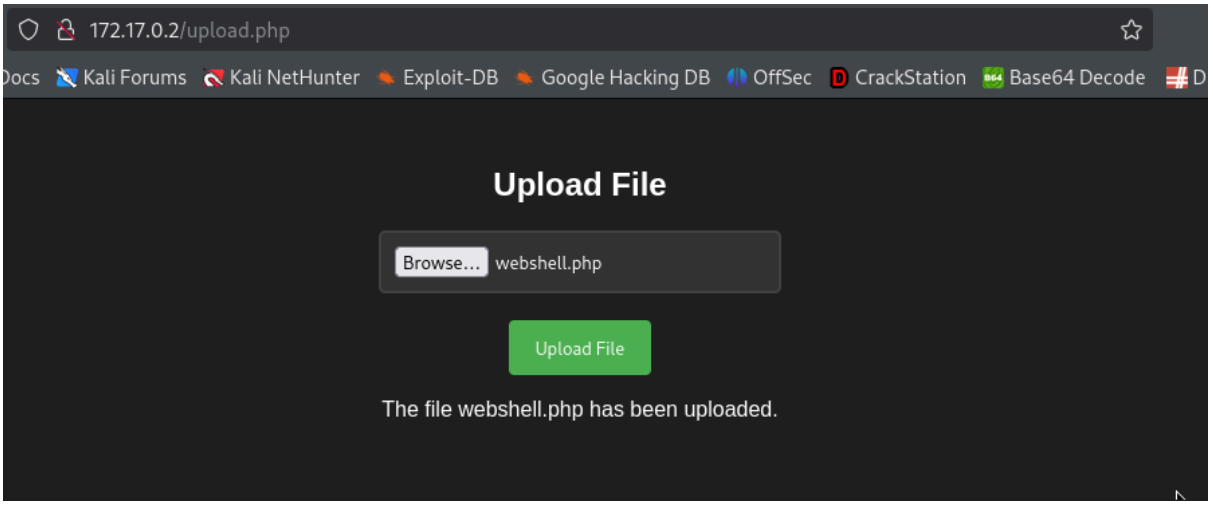


💥 3. Explotación de Vulnerabilidades

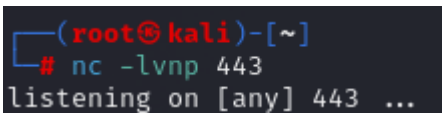
En /uploads.php permite subir archivos. Por ende, se podría intentar explotar con una reverse shell en php. Utilizo la reverse shell de pentestmonkey de github, modifico las variables para adaptarla a mi situación.



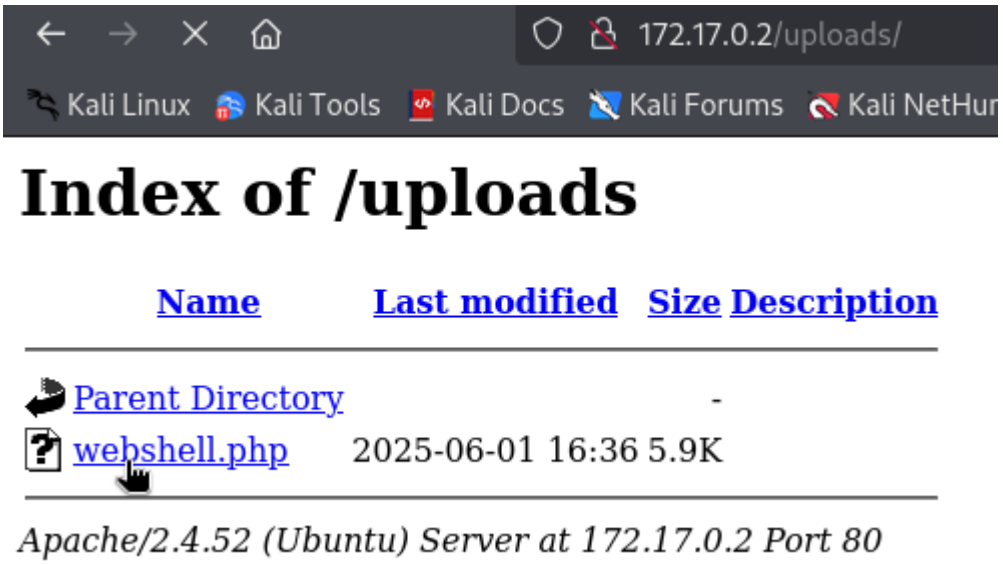
Subo el archivo malicioso para la reverse shell.



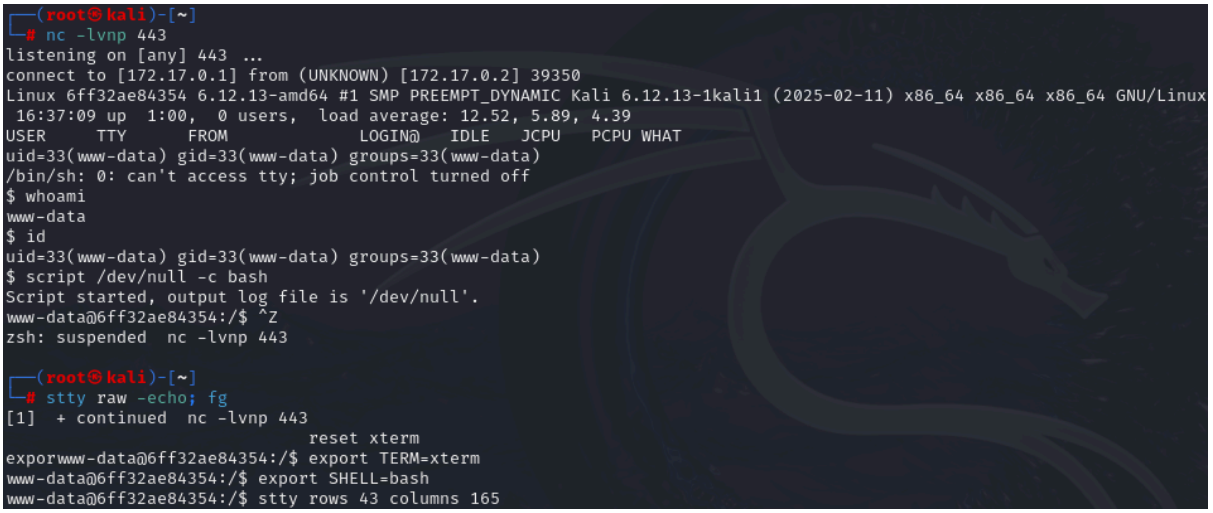
En mi máquina me pongo a la escucha con netcat en el puerto 443.



En /uploads se encuentran los archivos subidos mediante /uploads.php. Por ende, después de ponerme a la escucha con netcat hago click en el archivo php malicioso para que se ejecute.



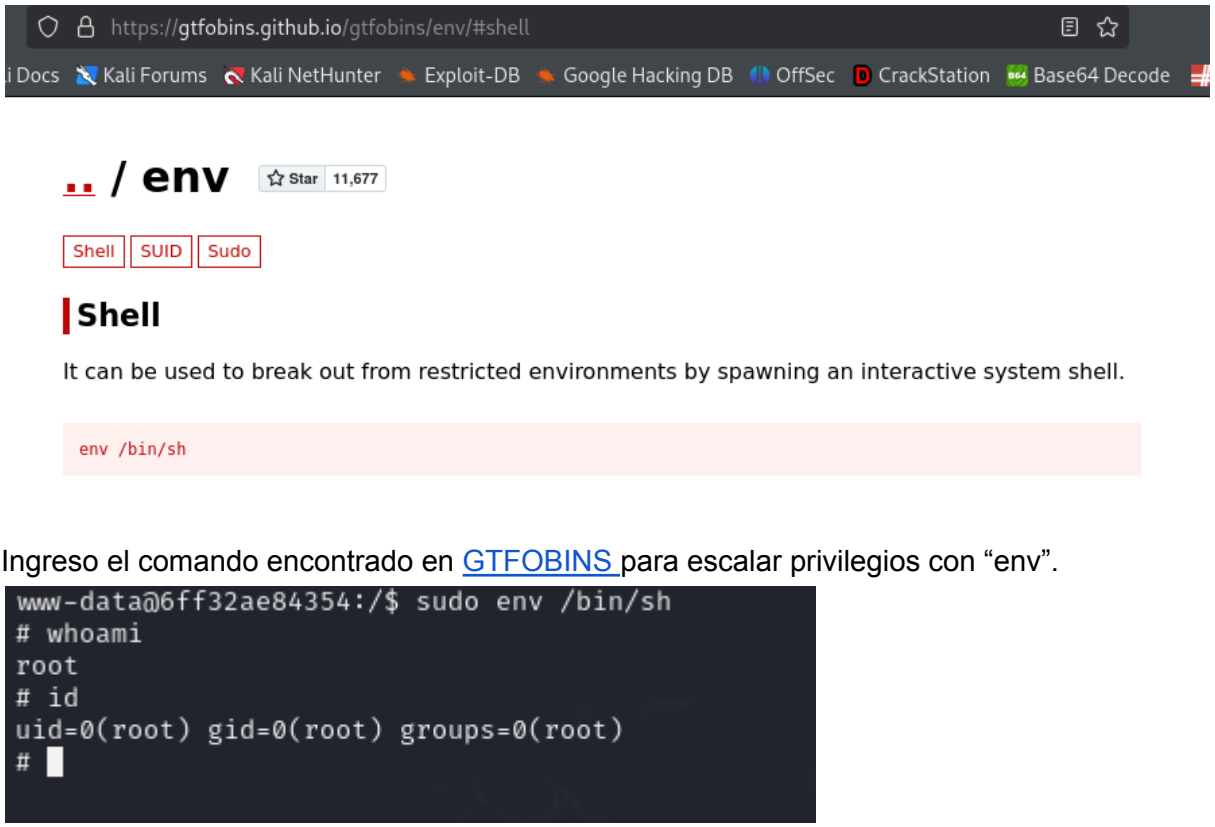
Obtengo la conexión de la reverse shell. Busco arreglar un poco la terminal.



🔐 4. Escalada de Privilegios y Post-explotación

Aplico “**sudo -l**” para ver que archivos tienen permisos sudo. El archivo “env” tiene permisos sudo.

En GTFOBINS busco algún comando para escalar privilegios con “env”.



Ingreso el comando encontrado en GTFOBINS para escalar privilegios con “env”.

Escalada de privilegios exitosa.

🏆 Banderas y Resultados

✔ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
✔ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.