🏴‍☠️ Write-Up: Máquina "WalkingCMS"

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

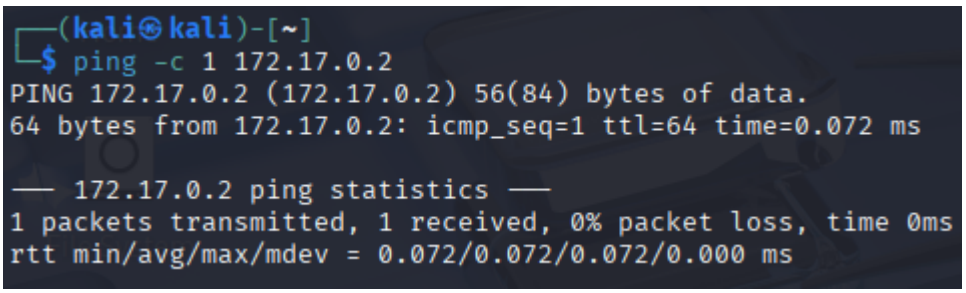
🔎 Metodología de Pentesting

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.

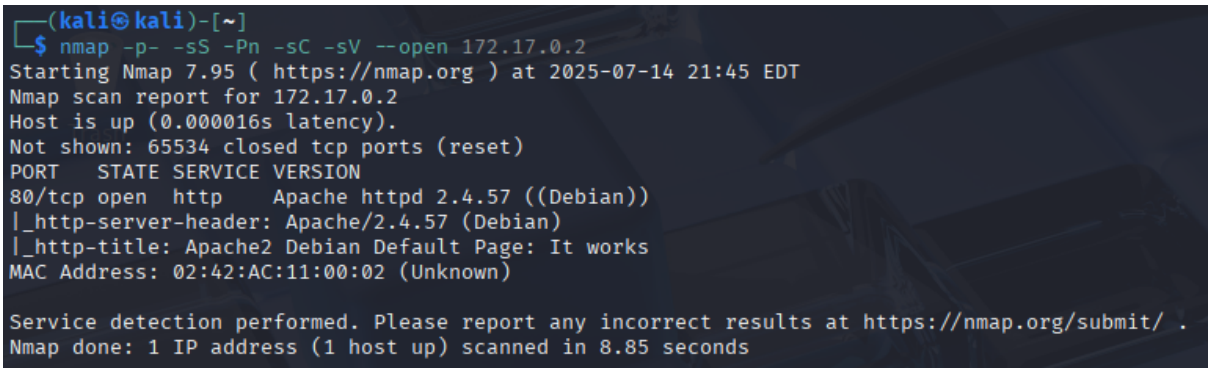
📡 1. Reconocimiento y Recolección de Información

Confirmo conectividad con la máquina objetivo.

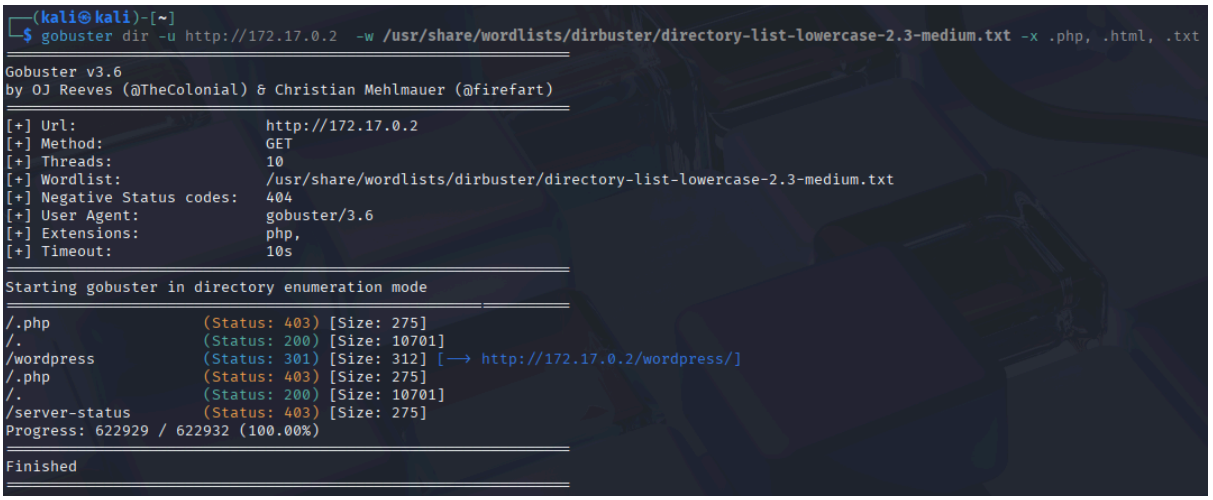


🎯 2. Escaneo y Enumeración

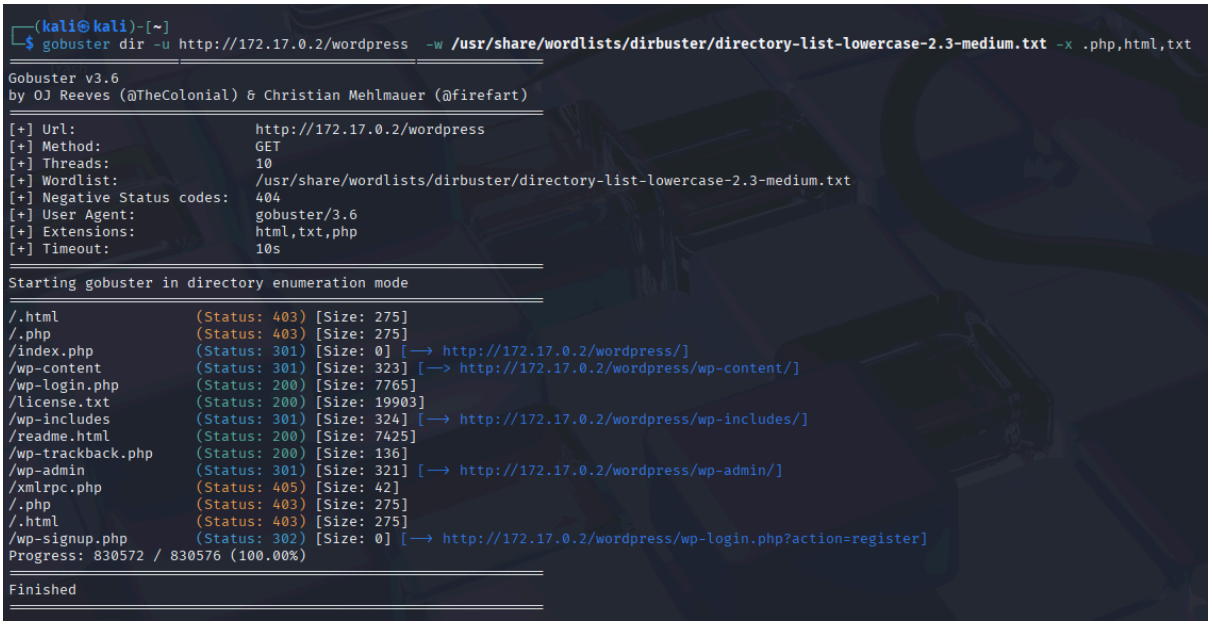
Escaneo y enumero puertos abiertos junto a sus versiones.



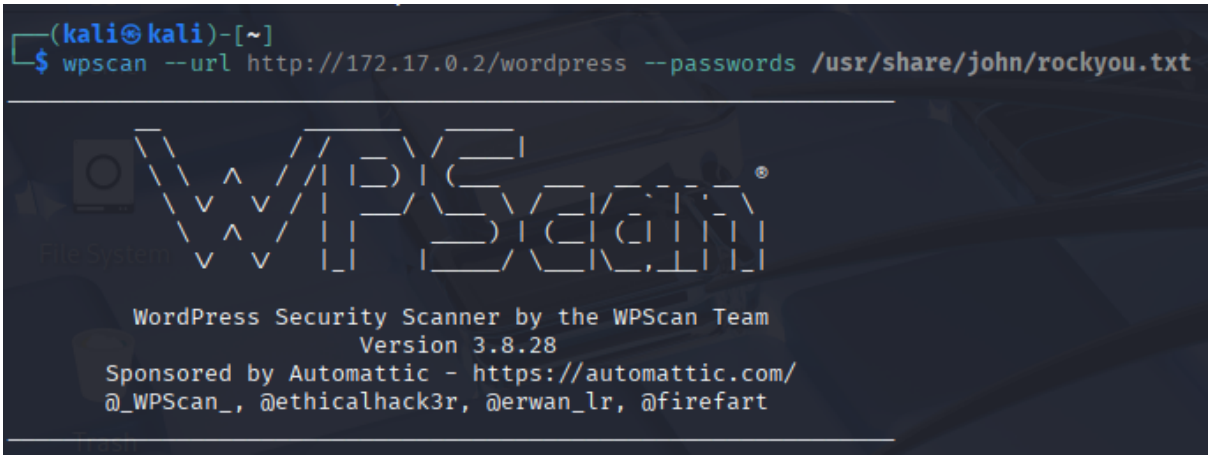
Busco directorios. Encuentro /wordpress, por ende, estoy ante una web de wordpress.

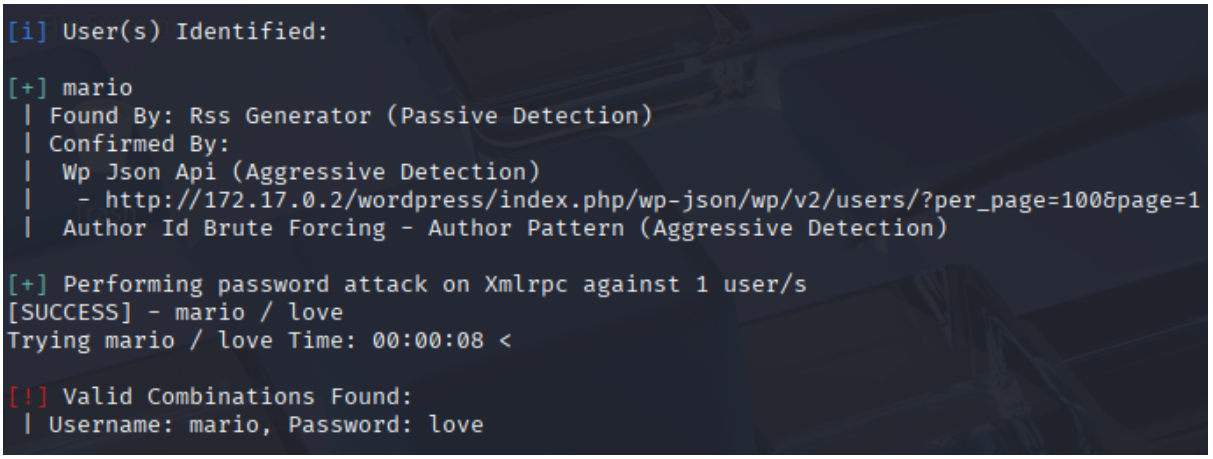


Busco directorios a partir de /wordpress y encuentro el panel de login.



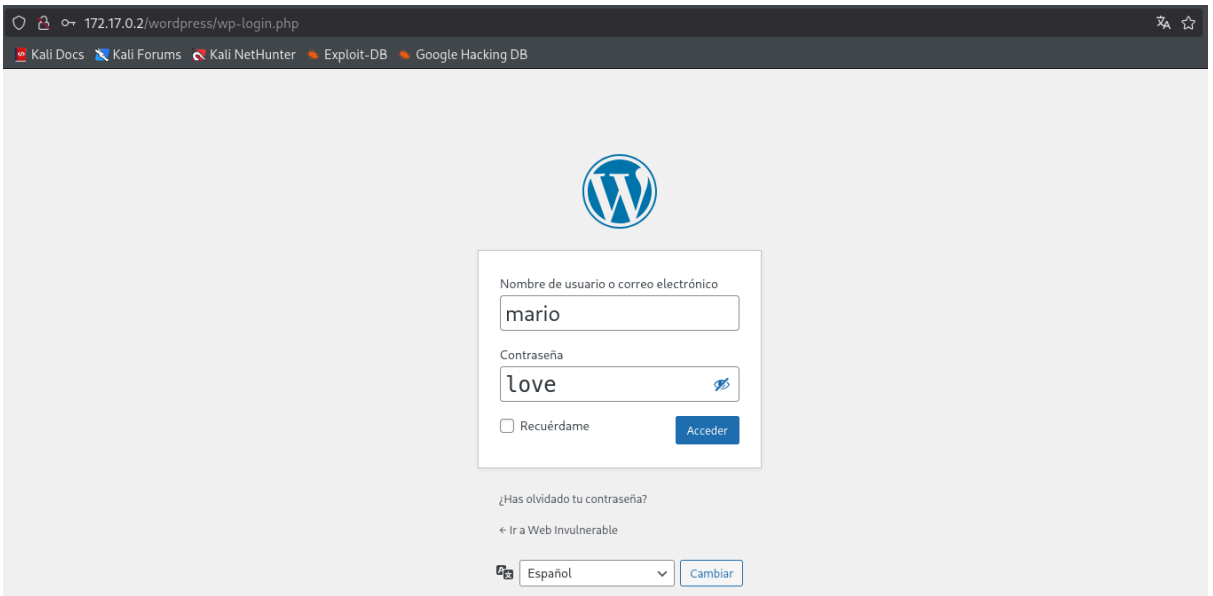
Uso wpscan para encontrar usuarios y contraseñas usando el diccionario de rockyou.txt



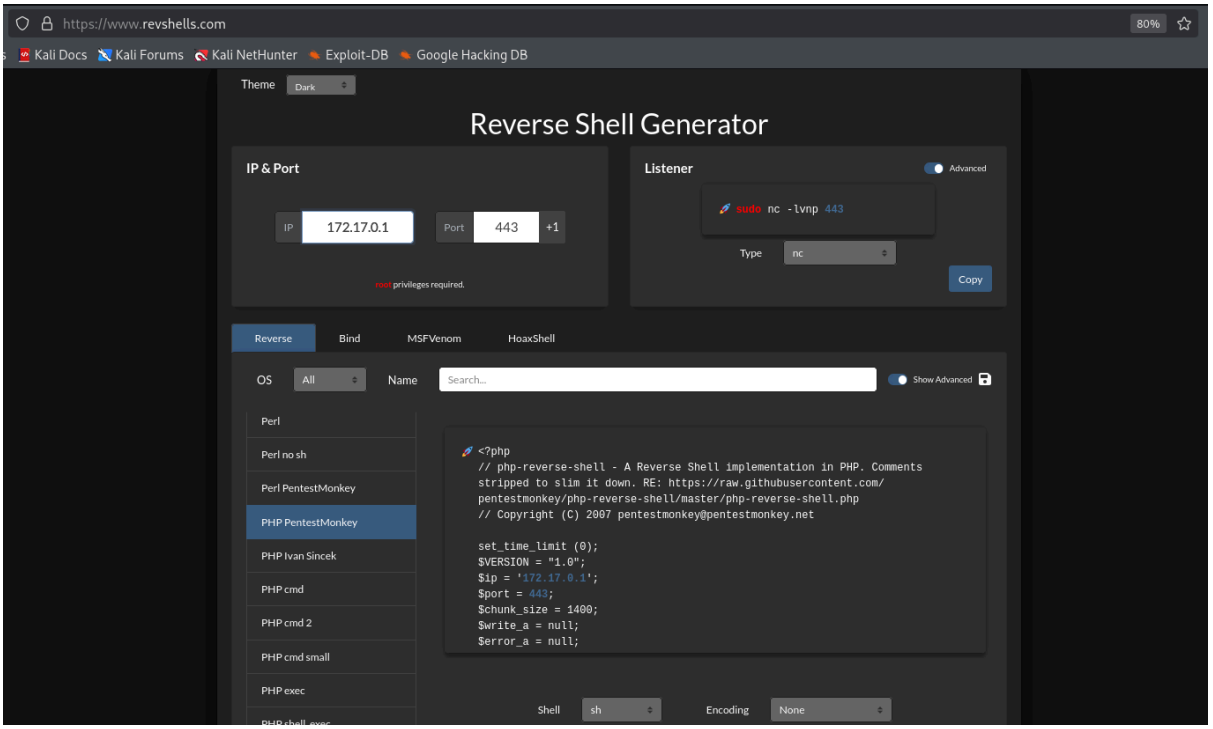


💥 3. Explotación de Vulnerabilidades

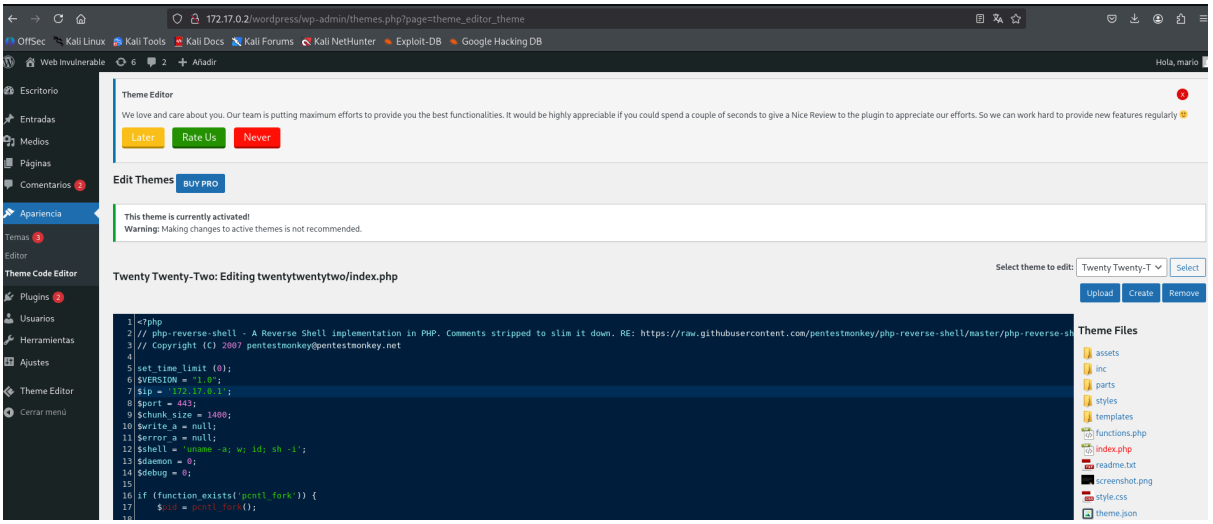
Ingreso al panel de wordpress usando la credencial encontrada anteriormente con wpscan.



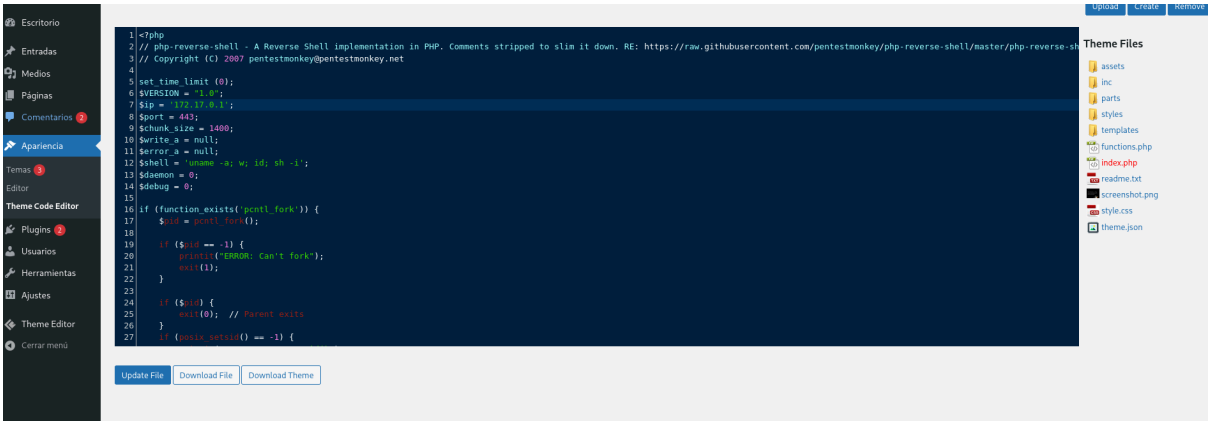
Vi que puedo editar código php de un tema de Wordpress. Busco la famosa reverse shell en php de PentestMonkey.



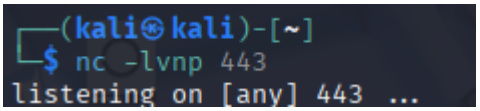
Pego la reverse shell en index.php.



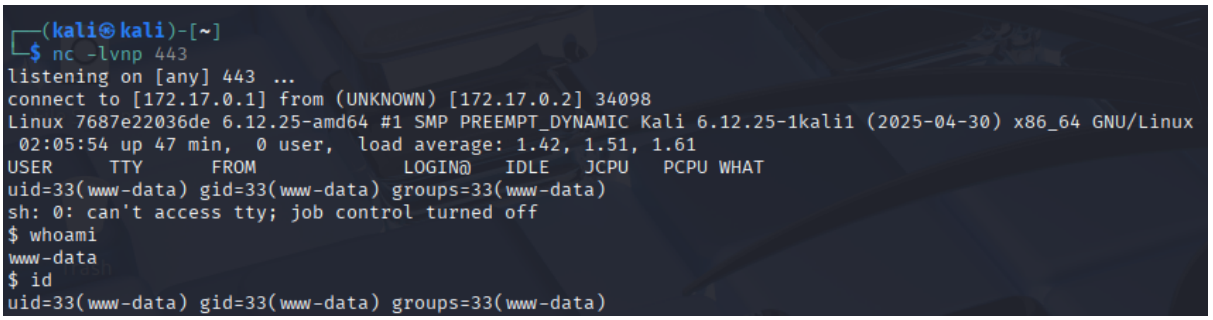
Guardo el contenido en “Upload File”.



Me pongo a la escucha con netcat.

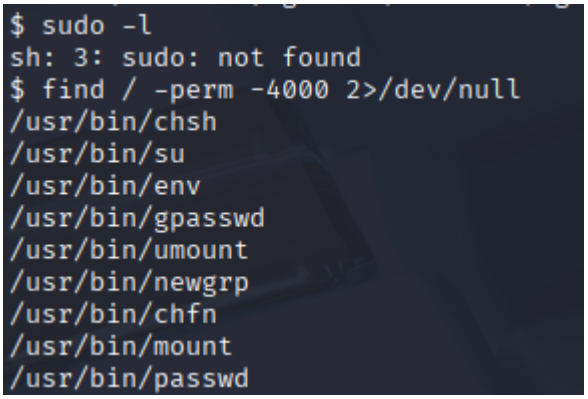


Ingreso a la ubicación de la reverse shell, en mi caso http://172.17.0.2/wordpress/wp-content/themes/twentytwentytwo/index.php lo que generará que el navegador ejecute el código malicioso en php enviando la solicitud de conexión a mi puerto 443 que estoy esperando con netcat. Conexión establecida.

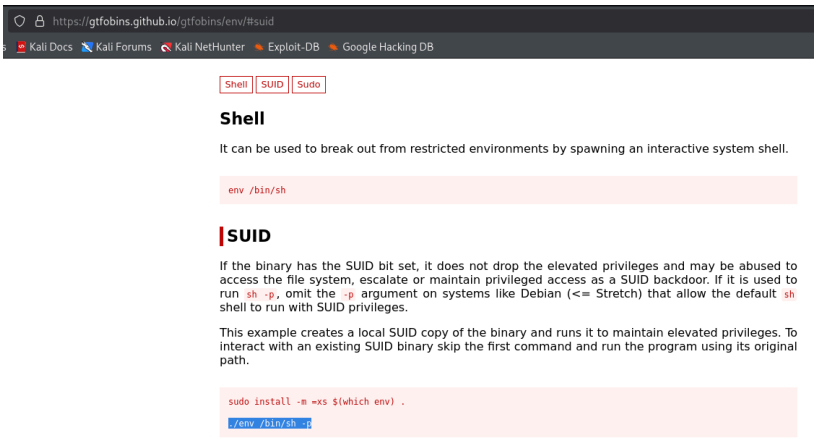


🔐 4. Escalada de Privilegios y Post-explotación

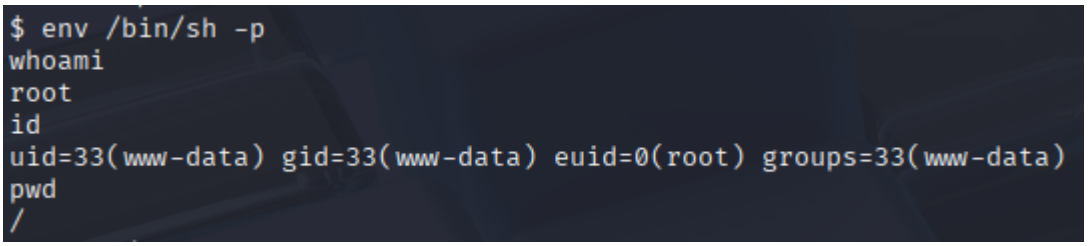
No tiene sudo para encontrar archivos con permisos SUDO. Pero, encontré un binario SUID.



En GTFOBINS busco un comando para escalar privilegios con “env” teniendo permisos SUID.



Ejecuto el comando y obtengo acceso a root.



🏆 Banderas y Resultados

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