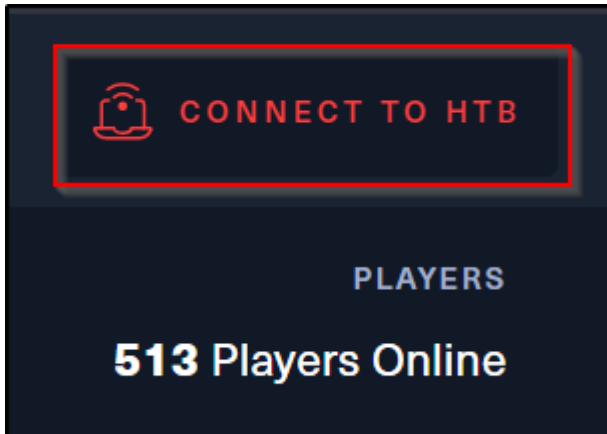


Connecting to HTB Starting Point VPN.

In order to access any server on HackTheBox, first, we need to connect to HackTheBox VPN. Since, in this module, we're going to be converging Starting Point Machines, hence, we've to connect to Starting Point VPN.

Procedure:

- Click on the icon that says **CONNECT TO HTB** in the top right hand corner of your screen.



- Now, since we'll be dealing with Starting Point Machines, we'll connect to the **Starting Point VPN**.

Connect To Hack The Box



Machines

Play Machines

● OFFLINE

EU FREE 3

Starting Point

Play Starting Point Machines

● OFFLINE

EU STARTINGPOINT 1



Release Arena - Paper

Compete on the latest released Machine

Sat 05 Feb, 19:00 UTC

● OFFLINE

INTRODUCTION TO LAB ACCESS

TROUBLE CONNECTING?

- Click on **OpenVPN** or **Pwnbox**, (based on personal preference). I'll be connecting to OpenVPN. Click on OpenVPN. Then set it up, choose the access points, after that, click on **Download VPN**.



Connect to Starting Point with OpenVPN



● OFFLINE



Connect to a VPN server

If you switch your Access or your Server,
you will have to re-connect.

VPN ACCESS

EU - Starting Point



VPN SERVER

EU StartingPoint 1



PROTOCOL



UDP 1337



TCP 443

DOWNLOAD VPN

INTRODUCTION TO LAB ACCESS

TROUBLE CONNECTING?

- After downloading the **.ovpn** file, fire up a terminal, and Use the `apt install openvpn` to install the OpenVPN module.
- After installing OpenVPN, use the `cd Downloads` command to access the Downloads folder. Then, use the `openvpn starting_point_{Your_Username_on_HTB}.ovpn` to start connecting to HTB VPN.

```

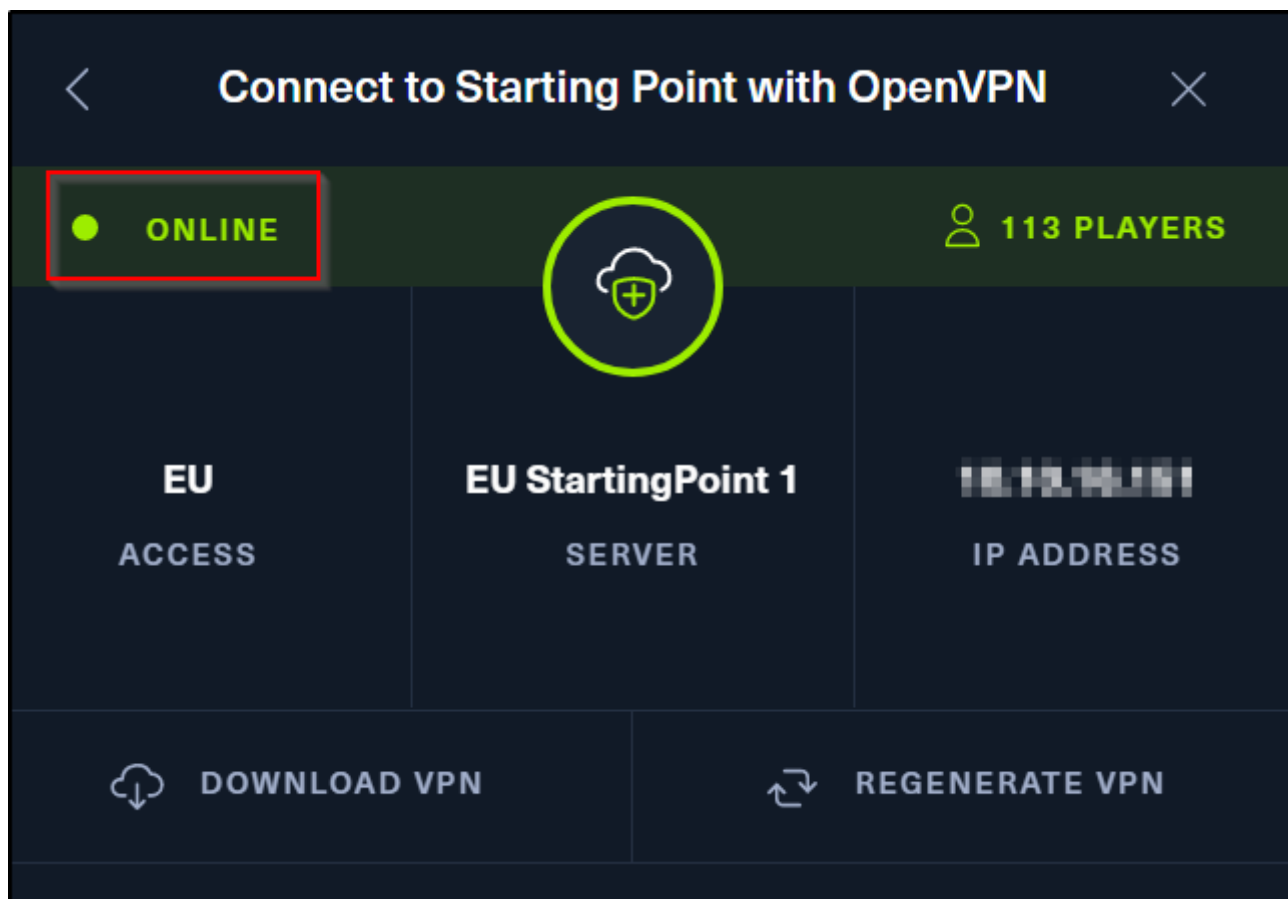
root@kali: ~/Downloads
File Actions Edit View Help

(root@kali)-[~]
# cd Downloads

(root@kali)-[~/Downloads]
# openvpn starting_point_...l.ovpn
2022-02-03 00:36:01 WARNING: Compression for receiving enabled. Compression h
in the past to break encryption. Sent packets are not compressed unless "allo
yes" is also set.
2022-02-03 00:36:01 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but miss
-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will ignore --ciph
negotiations. Add 'AES-128-CBC' to --data-ciphers or change --cipher 'AES-12
ata-ciphers-fallback 'AES-128-CBC' to silence this warning.
2022-02-03 00:36:01 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [
[PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2022-02-03 00:36:01 library versions: OpenSSL 1.1.1m 14 Dec 2021, LZO 2.10
2022-02-03 00:36:01 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR'
with 256 bit key
2022-02-03 00:36:01 Outgoing Control Channel Encryption: Using 256 bit messag
6' for HMAC authentication
2022-02-03 00:36:01 Incoming Control Channel Encryption: Cipher 'AES-256-CTR'
with 256 bit key
2022-02-03 00:36:01 Incoming Control Channel Encryption: Using 256 bit messag
6' for HMAC authentication
2022-02-03 00:36:01 TCP/UDP: Preserving recently used remote address: [AF_INE
1:443
2022-02-03 00:36:01 Socket Buffers: R=[131072→131072] S=[16384→16384]
2022-02-03 00:36:01 Attempting to establish TCP connection with [AF_INET]5.44
[nonblock]
2022-02-03 00:36:01 TCP connection established with [AF_INET]5.44.235.181:443
2022-02-03 00:36:01 TCP_CLIENT link local: (not bound)
2022-02-03 00:36:01 TCP_CLIENT link remote: [AF_INET]5.44.235.181:443
2022-02-03 00:36:02 TLS: Initial packet from [AF_INET]5.44.235.181:443, sid=6
c13
2022-02-03 00:36:02 VERIFY OK: depth=1, CN=HackTheBox
2022-02-03 00:36:02 VERIFY KU OK
2022-02-03 00:36:02 Validating certificate extended key usage
2022-02-03 00:36:02 ++ Certificate has EKU (str) TLS Web Server Authenticatio
S Web Server Authentication
2022-02-03 00:36:02 VERIFY EKU OK
2022-02-03 00:36:02 VERIFY OK: depth=0, CN=htb
2022-02-03 00:36:02 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_
bit RSA
2022-02-03 00:36:02 [htb] Peer Connection Initiated with [AF_INET]5.44.235.18
2022-02-03 00:36:03 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2022-02-03 00:36:03 PUSH: Received control message: 'PUSH_REPLY,route 10.10.1
54.0,route 10.129.0.0 255.255.0.0,route-ipv6 dead:beef::/64,tun-ipv6,route-ga
6.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:4::1095/
4::1,ifconfig 10.10.16.151 255.255.254.0,peer-id 0,cipher AES-256-GCM'

```

- After executing these commands successfully, you'll see something like this on HackTheBox.



- And with this, you've successfully made the connection with HackTheBox VPN.