

Connecting Using VPN

A [virtual private network \(VPN\)](#) allows us to connect to a private (internal) network and access hosts and resources as if we were directly connected to the target private network. It is a secured communications channel over shared public networks to connect to a private network (i.e., an employee remotely connecting to their company's corporate network from their home). VPNs provide a degree of privacy and security by encrypting communications over the channel to prevent eavesdropping and access to data traversing the channel.



At a high-level, VPN works by routing our connecting device's internet connection through the target VPN's private server instead of our internet service provider (ISP). When connected to a VPN, data originates from the VPN server rather than our computer and will appear to originate from a public IP address other than our own.

There are two main types of remote access VPNs: client-based VPN and SSL VPN. SSL VPN uses the web browser as the VPN client. The connection is established between the browser and an SSL VPN gateway can be configured to only allow access to web-based applications such as email and intranet sites, or even the internal network but without the need for the end user to install or use any specialized software. Client-based VPN requires the use of client software to establish the VPN connection. Once connected, the user's host will work mostly as if it were connected directly to the company network and will be able to access any resources (applications, hosts, subnets, etc.) allowed by the server configuration. Some corporate VPNs will provide employees with full access to the internal corporate network, while others will place users on a specific segment reserved for remote workers.

Why Use A VPN?

We can use a VPN service such as [NordVPN](#) or [Private Internet Access](#) and connect to a VPN server in another part of our country or another region of the world to obscure our browsing traffic or disguise our public IP address. This can provide us with some level of security and privacy. Still, since we are connecting to a company's server, there is always the chance that data is being logged or the VPN service is not following security best practices or the security features that they advertise. Using a VPN service comes with the risk that the provider is not doing what they are saying and are logging all data. Usage of a VPN service **does not** guarantee anonymity or privacy but is useful for bypassing certain network/firewall restrictions or when connected to a possible hostile network (i.e., a public airport wireless network). A VPN service should never be used with the thought that it will protect us from the consequences of performing nefarious activities.

Connecting to HTB VPN

HTB and other services offering purposefully vulnerable VMs/networks require players to connect to the target network via a VPN to access the private lab network. Hosts within HTB networks cannot connect directly out to the internet. When connected to HTB VPN (or any penetration testing/hacking-focused lab), we should always consider the network to be "hostile." We should only connect from a virtual machine, disallow password authentication if SSH is enabled on our attacking VM, lockdown any web servers, and not leave sensitive information on our attack VM (i.e., do not play HTB or other vulnerable networks with the same VM that we use to perform client assessments). When connecting to a VPN (either within HTB Academy or the main HTB platform), we connect using the following command:

```
giancarix117@htb[/htb]$ sudo openvpn user.ovpn

Thu Dec 10 18:42:41 2020 OpenVPN 2.4.9 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11]
Thu Dec 10 18:42:41 2020 Library versions: OpenSSL 1.1.1g 21 Apr 2020, LZO 2.10
Thu Dec 10 18:42:41 2020 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for
Thu Dec 10 18:42:41 2020 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for
Thu Dec 10 18:42:41 2020 TCP/UDP: Preserving recently used remote address: [AF_INET]
Thu Dec 10 18:42:41 2020 Socket Buffers: R=[212992->212992] S=[212992->212992]
Thu Dec 10 18:42:41 2020 UDP link local: (not bound)
<SNIP>
Thu Dec 10 18:42:41 2020 Initialization Sequence Completed
```

The last line [Initialization Sequence Completed](#) tells us that we successfully connected to the VPN. Where [sudo](#) tells our host to run the command as the elevated root user, [openvpn](#) is the VPN client, and the [user.ovpn](#) file is the VPN key that we download from either the Academy module section or the main HTB platform [Access page](#). If we type [ifconfig](#) in another terminal window, we will see a [tun](#) adapter if we successfully connected to the VPN.

```
giancarix117@htb[/htb]$ ifconfig

<SNIP>

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.10.x.2 netmask 255.255.254.0 destination 10.10.x.2
    inet6 dead:beef:1::2000 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::d82f:301a:a94a:8723 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen
```

Typing [netstat -rn](#) will show us the networks accessible via the VPN.

```
giancarix117@htb[/htb]$ netstat -rn

Kernel IP routing table
Destination        Gateway            Genmask           Flags   MSS Window  irtt Iface
0.0.0.0            192.168.1.2       0.0.0.0           UG        0 0          0 eth0
10.10.14.0         0.0.0.0           255.255.254.0     U          0 0          0 tun0
10.129.0.0         10.10.14.1       255.255.0.0       U          0 0          0 tun0
192.168.1.0        0.0.0.0           255.255.255.0     U          0 0          0 eth0
```

Here can see that the 10.129.0.0/16 network used for HTB Academy machines is accessible via the [tun0](#) adapter via the 10.10.14.0/23 network.

Help with VPN

If this is your first time using a VPN, the following resources on the Hack The Box support portal will be helpful:

- [Introduction to Lab Access](#)
- [Connection Troubleshooting](#)

Cheat Sheet

Table of Contents

Introduction

Infosec Overview

Setup

Getting Started with a Pentest Distro

Staying Organized

Connecting Using VPN

Pentesting Basics

Common Terms

Basic Tools

Service Scanning

Web Enumeration

Public Exploits

Types of Shells

Privilege Escalation

Transferring Files

Getting Started with Hack The Box (HTB)

Starting Out

Navigating HTB

Attacking Your First Box

Nibbles - Enumeration

Nibbles - Web Footprinting

Nibbles - Initial Foothold

Nibbles - Privilege Escalation

Nibbles - Alternate User Method - Metasploit

Problem Solving

Common Pitfalls

Getting Help

What's Next?

Next Steps

Knowledge Check

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left

Previous Next

Mark Complete & Next