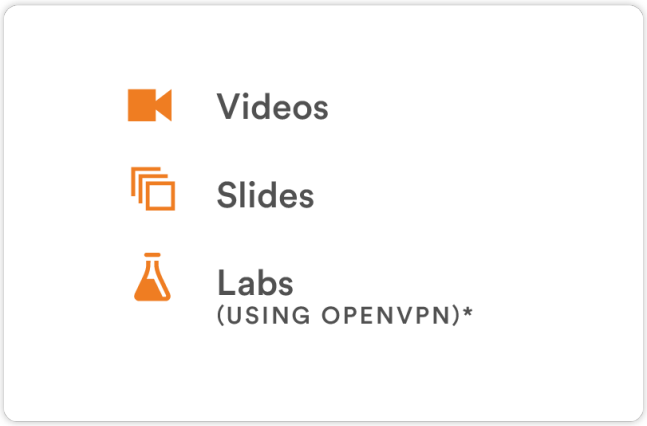
Cyber Security User Guide

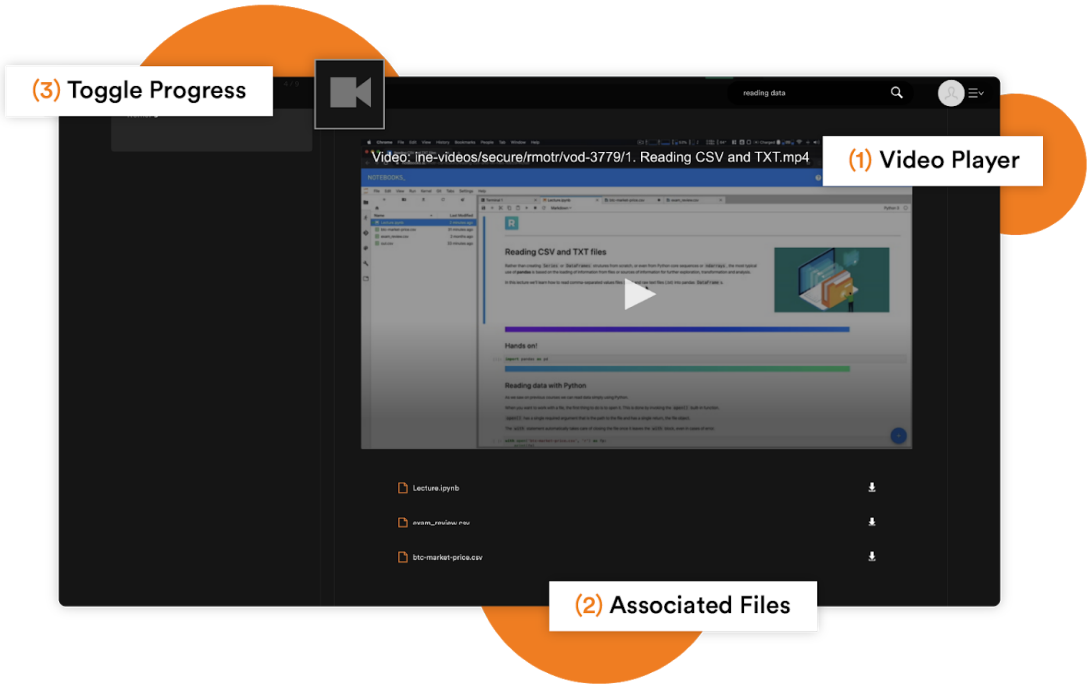
INE's Cyber Security courses provide an in-depth, hands on experience. This guide will walk you through the types of content you will encounter.



*** See the VPN Setup Section Below**

Videos

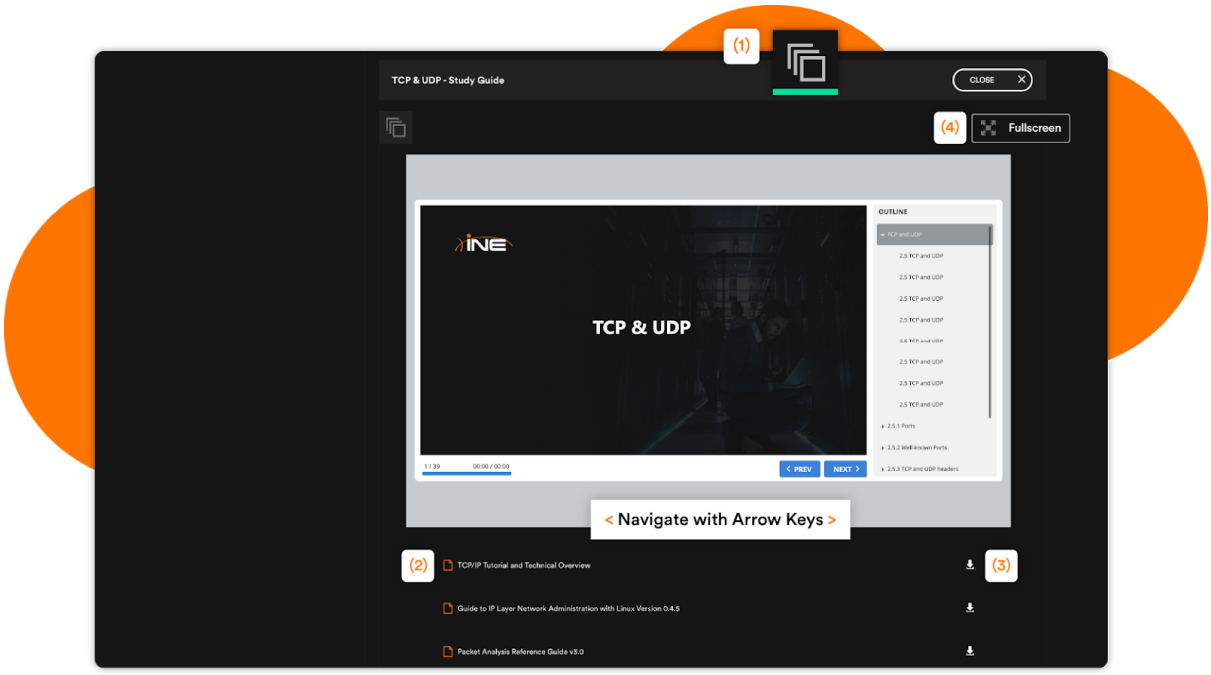
It all begins with our expert-led video courses. We use a multiplatform video player **(1)** optimized for different devices and connections, so you have a first-rate experience regardless of where you're watching.



Many videos include associated files **(2)**. Your instructor will make these resources available for you to download and see what materials they were referencing during the video.

Your progress is recorded once you've completed a video. You can manually toggle/untoggle your progress with the "Toggle Progress" button shown in the screenshot above **(3)**.

Slides



In the above slide, you will see the initial landing page for our Penetration Testing Student (PTS) course. You can navigate through the content using the arrow keys, by pressing the enter key on your keyboard, or clicking anywhere on the slide. Please use the reference guide below to help navigate through the course.

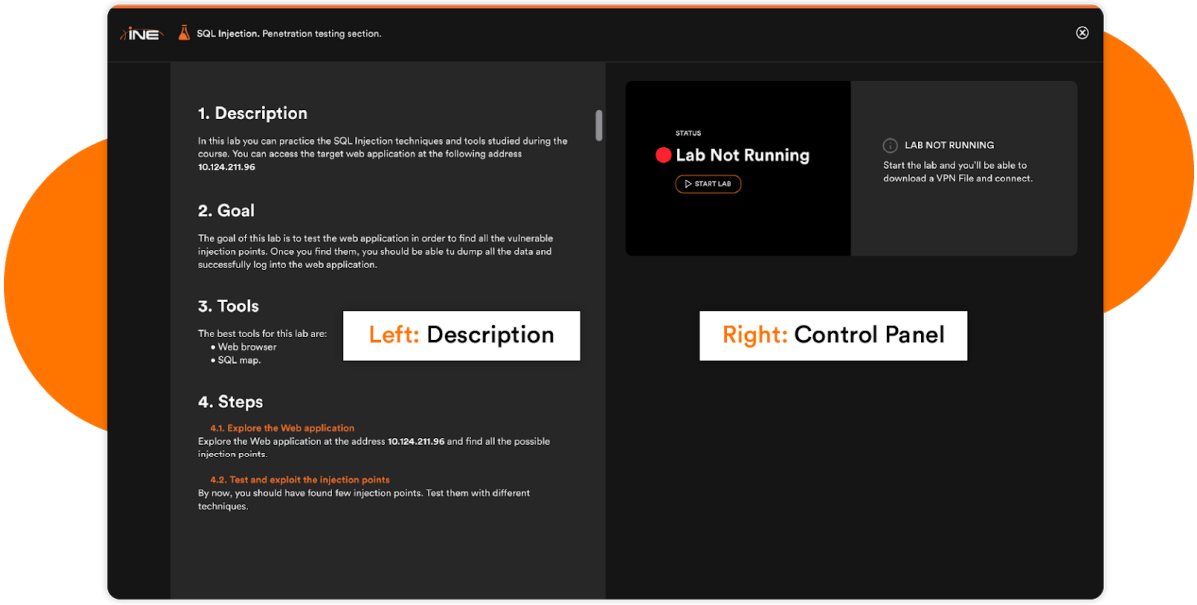
References

1. This Icon indicates that this is a slide view
2. There might be associated files with the slide
3. Download files with this icon
4. View slides in Full Screen, exit using the escape key

Labs

Important: Please check the OpenVPN section at the end of this manual to understand how to connect to your labs. What's described here assumes knowledge of OpenVPN.

At INE we're proud of our hands-on platform. Our Cyber Security courses include interactive labs in which you can practice your skills, and they are dedicated to you and only you. No one else will be in your environment, and they are isolated from every other student. Labs run on top of interconnected virtual machines simulating real-life scenarios. This means that Labs might look like a complicated piece of machinery. But don't worry! We've made it intuitive, so you can start working on them right away. First, this is what a lab screen looks like:



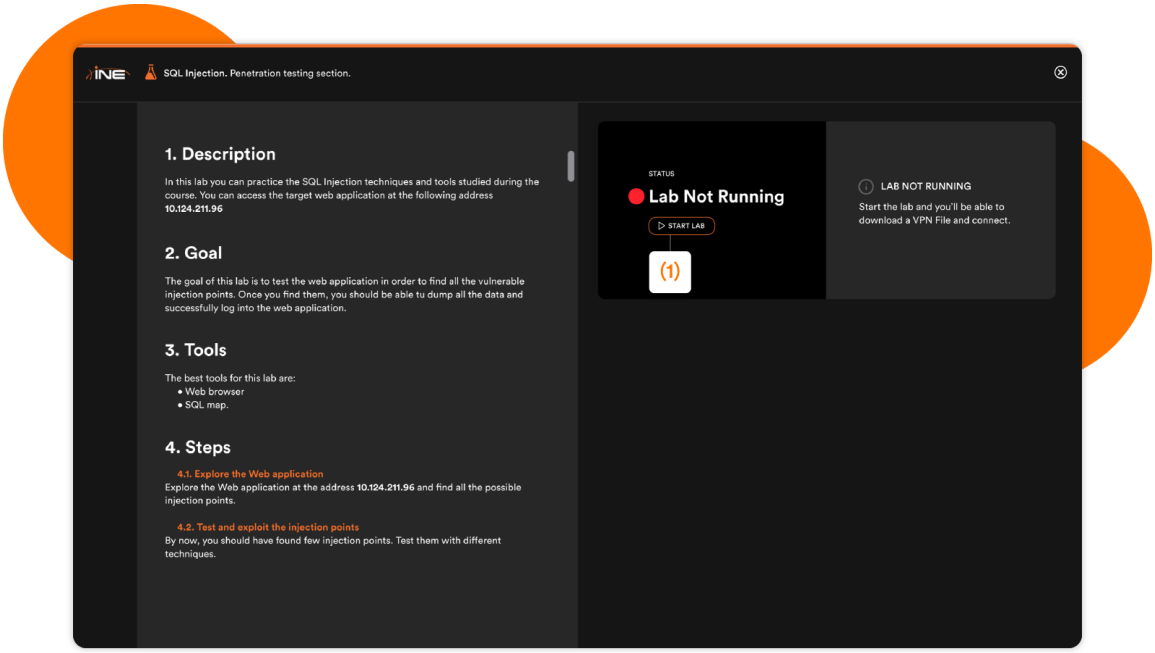
On the **Left Side** you'll find the instructors for that Lab. It'll be a step-by-step guide of what you need to do to complete it. It might also include solutions or references to additional readings.
On the **Right Side** you'll find the Control Panel allowing you to have full control of the Lab status. We'll go into more detail about the different Lab Statuses. Briefly, a Lab can be in either of these states:

- Not running (unstarted)
- Started (running, available to work)
- Stopped or paused (the lab is stopped but your progress was saved)
- Terminating / resetting (brief period while the lab is resetting back to its original state)

Basically, you'll have to Start the lab before you can connect and start doing any work on them. But **WARNING**, **you can only have 1 running lab at a single time**. If there's already a lab running, and you want to start another, you'll have to pause it first.

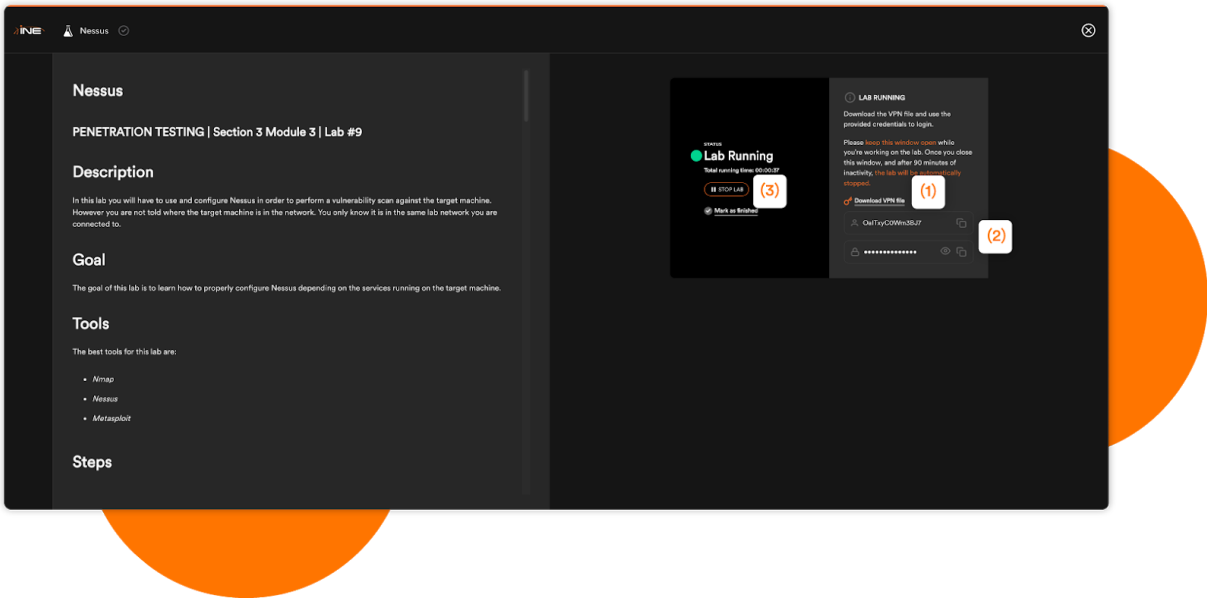
Let’s go deeper into each state:

Lab Not Running



This is the initial state. You have to press the Start Lab button **(1)** to start it. This might take a few minutes while the virtual lab is provisioned.

Lab Running



You'll be able to interact with the lab environment using your platform of choice including Linux, Mac, Windows (preferably with WSL2), or pre-configured Linux distros (Kali, Parrot, etc.) by using the Community Edition of OpenVPN (refer to the VPN Setup & Troubleshooting section below for step-by-step instructions). Since most security tools are created for use on Linux, it is imperative to learn Linux.

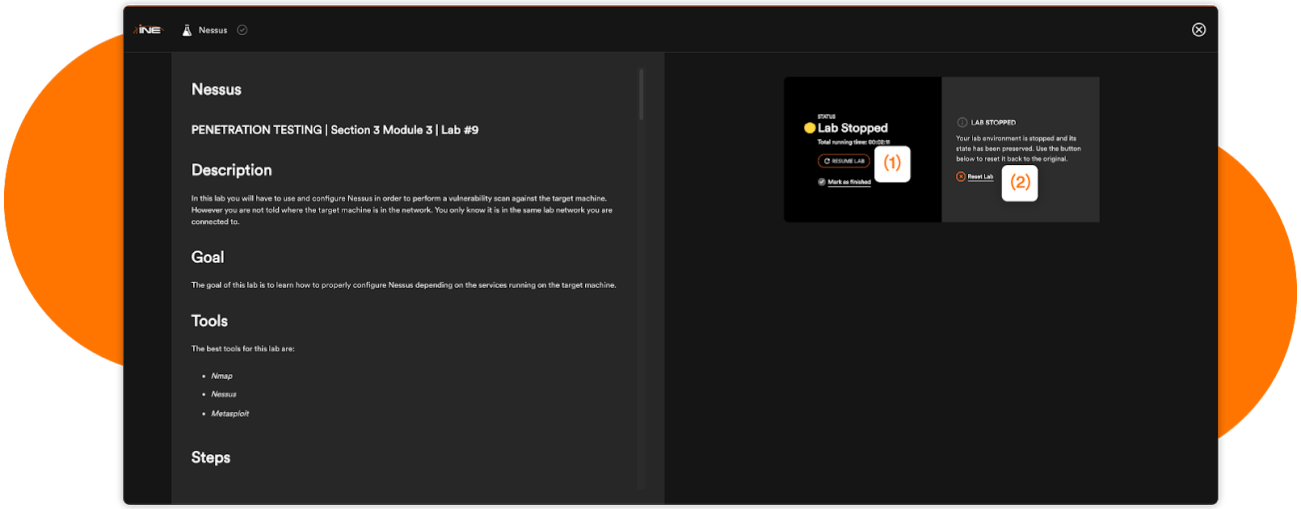
Here are some handy links to get you started quickly in using a Linux virtual machine for the labs. To run virtual machines on any platform, we recommend installing the latest version of VirtualBox as well as the Extension Pack (make sure the versions of the installation package and the extension pack are identical). Then download the VirtualBox specific image for Kali, a pre-configured Linux distro for cyber security, and import it into VirtualBox. Once complete, continue all coursework from inside Kali including logging into the INE platform, navigating to your chosen course and interacting with the virtual lab environment.

Once the lab has started, you can Download the OpenVPN configuration file using the Download VPN File Link **(1)**. When you try to connect, you'll be asked for a username/password set of credentials. Use the ones displayed in the platform **(2)**.

At any moment, you can Stop your lab with the Stop Lab button **(3)**. This will just "pause" it and free up resources. It'll save your current state and is a safe operation.

It's important to keep this window OPEN while you work. If the window is closed, your lab will automatically stop after 90 minutes.

Lab Stopped

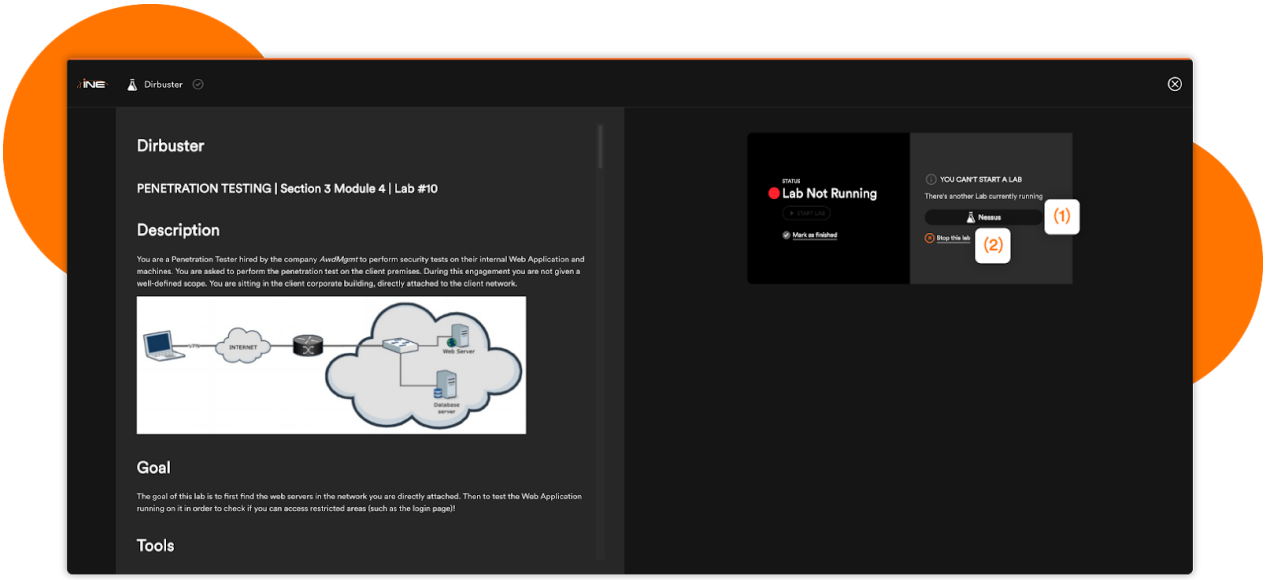


Labs might be in a Stopped state, because you explicitly stopped it or done automatically due to 90 minutes of inactivity. In any case, restarting it is simple. Just use the Restart Lab button **(2)**. If

you made changes to the lab and wish to go back to its original state, use the Reset Lab link **(2)**.

Note:

Only 1 lab can be running at a time, which means that if you browse another lab, you won't be able to start it. The platform will indicate what other lab is running (1) and give the possibility to stop it right there (2) to start the current lab.



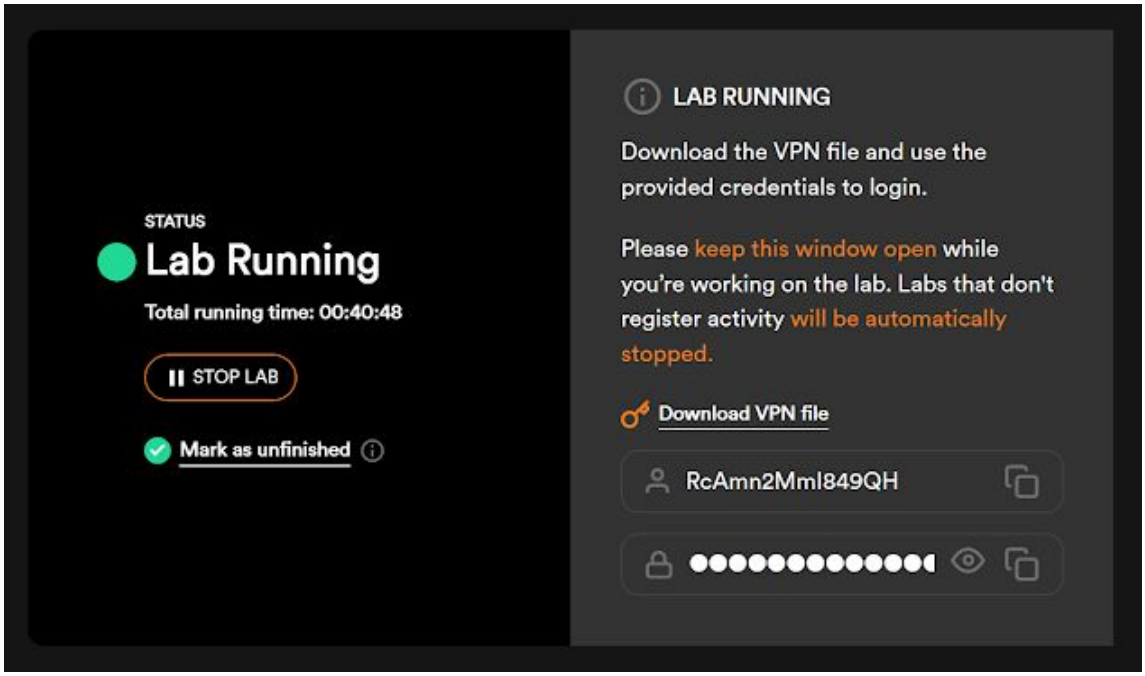
VPN Setup & Troubleshooting

Important: *Make sure you're using OpenVPN version 2.4 or newer.*

Setup

To test connectivity to the lab environment, we'll be using the very first lab in the Penetration Testing Student Path, "HTTP(S) Traffic Sniffing".

Once the lab is STARTED, you'll have access to 3 crucial pieces of information to connect to the virtual private network (VPN) created for each specific lab: a downloadable OpenVPN File (a config file with a .ovpn extension) and automatically generated, random username and password.



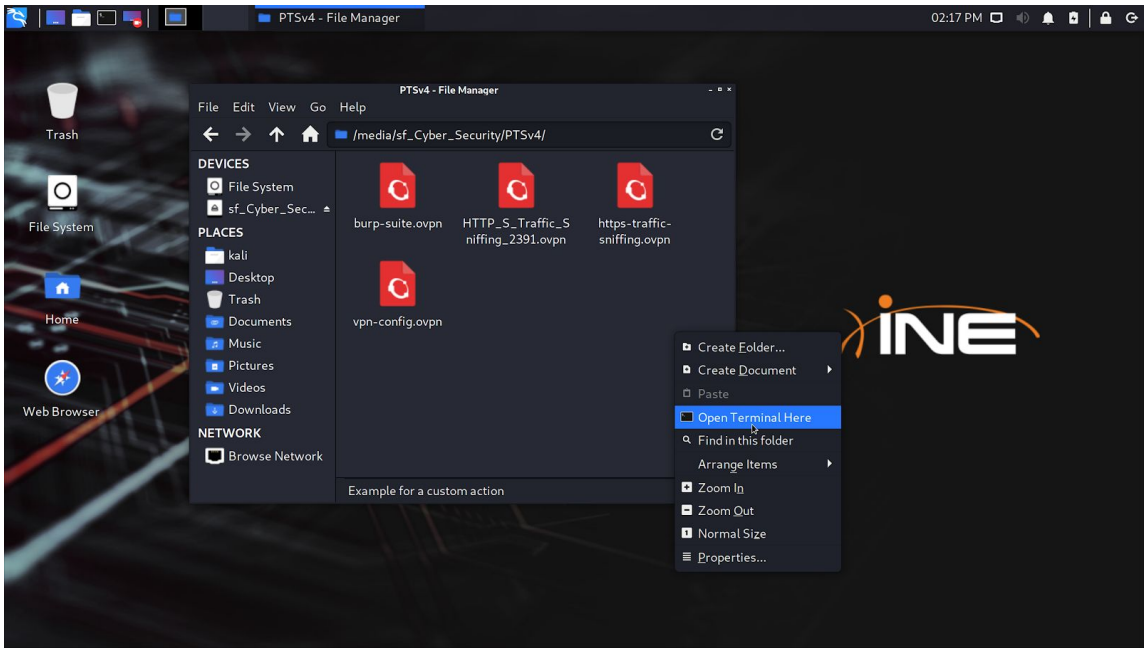
To connect to the lab, you'll need an OpenVPN client. Regardless of OS, you will use the same file, UN and PW. These are the OpenVPN clients we recommend for each operating system.

Linux

In most Linux distributions, OpenVPN is already installed. If you don't have it, please follow this guide:
https://www.ovpn.com/en/guides/ubuntu-gui

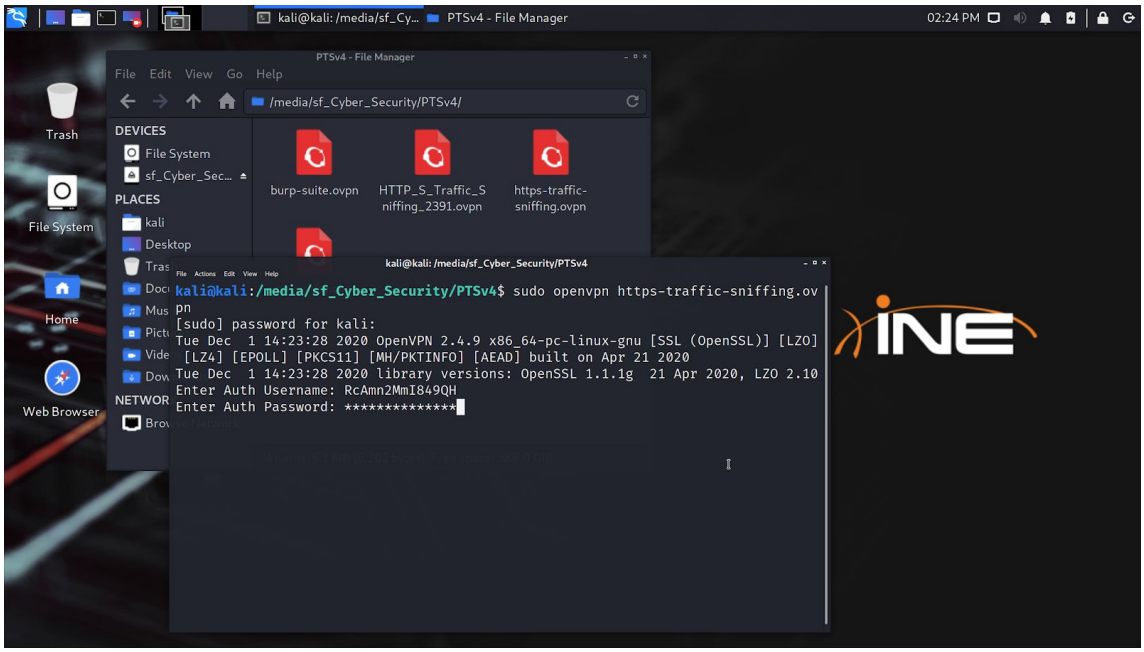
As mentioned above, we highly recommend not only using Linux (as most security tools are made for this OS) but more specifically to use a pre-configured VM of a Linux distribution such as Parrot or Kali. Kali is more widely used and what we'll show in this guide, however there are plenty of tutorials online for both.

After downloading the ovpn file, the easiest way to connect is to first open the Linux File Manager and navigate to the location where you saved the file. Then, go to a blank space, right-click and select “Open Terminal Here”.

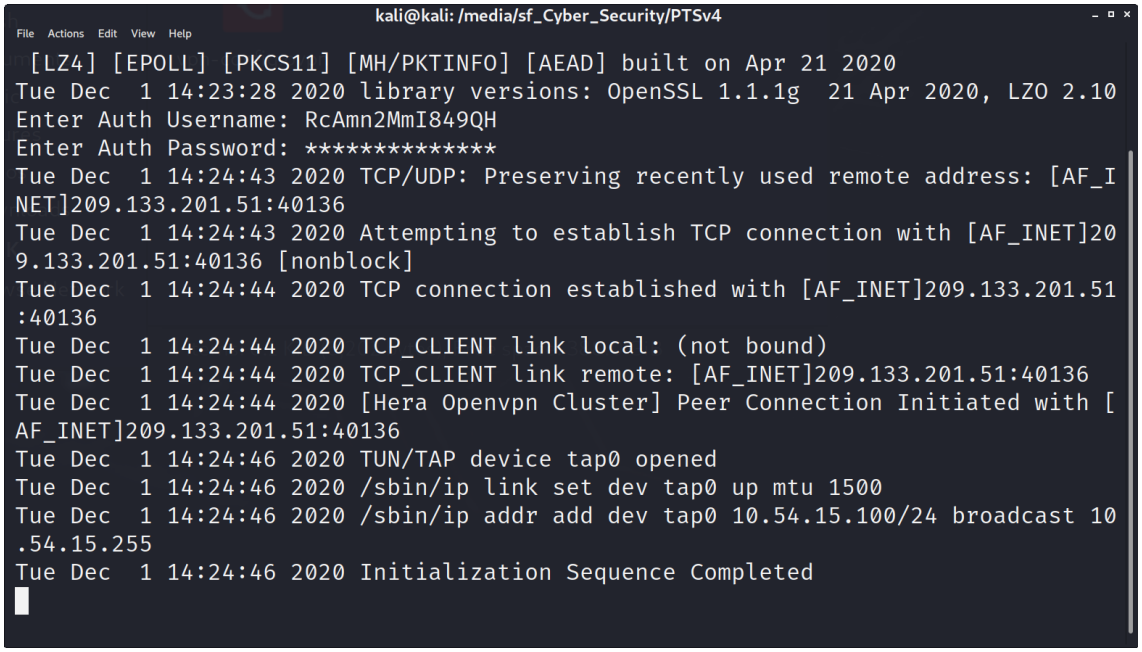


This will open a terminal window at this exact location preventing some typing. Hackers are lazy! At the command prompt, type “sudo openvpn https-traffic-sniffing.ovpn” and hit enter. Next, type your kali user password to verify usage of the sudo command and again hit enter. Then copy and paste

the un and pw provided for the lab.

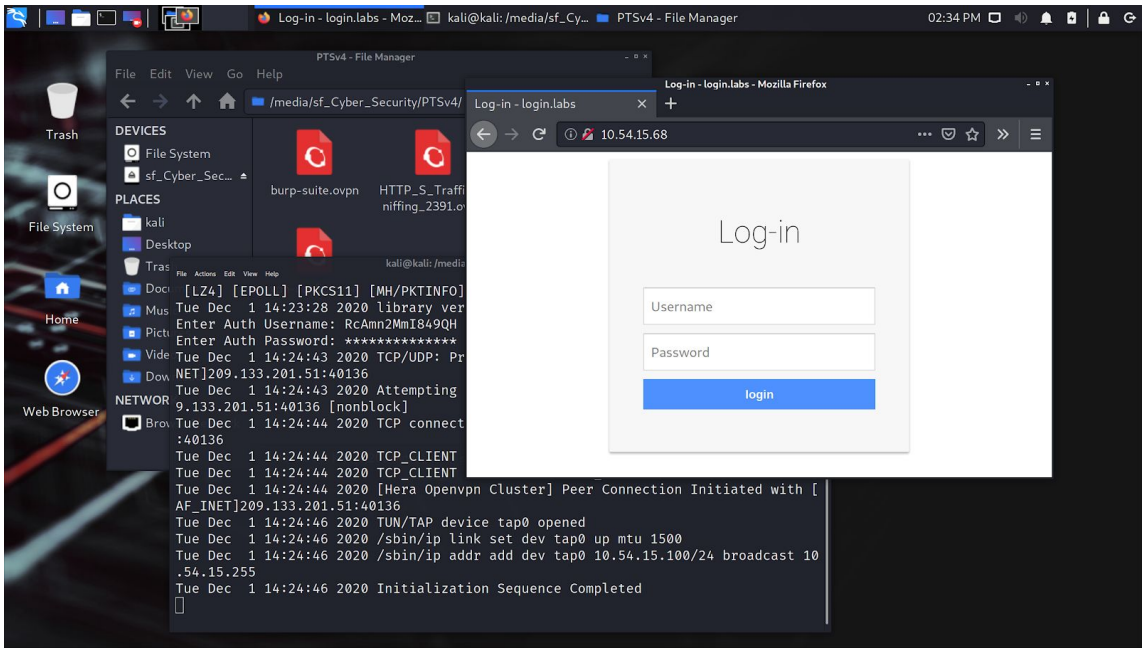


After hitting enter after the un and also after the pw, you will then be connected to the lab network.



To confirm success, let's focus on the final 3 lines. From the bottom moving our eyes upward, you'll see a cursor and not the command prompt. This means that the openvpn process is running. If it was unsuccessful or stopped, you'd be taken back to

the prompt. HINT: If you see the prompt instead of the cursor, you're not connected. Try again. Moving up from there, you can see that the "Initialization Sequence Completed" which is also good. Finally one line above that, you can see that the IP address assigned to your Kali machine should match the address range of the next step in the lab guide, which is to navigate to http://10.54.15.68 in a browser. All of this should confirm that you are properly connected, but we can do one final test and navigate to that web server.



We see the login screen. Success!

You may continue your studies.

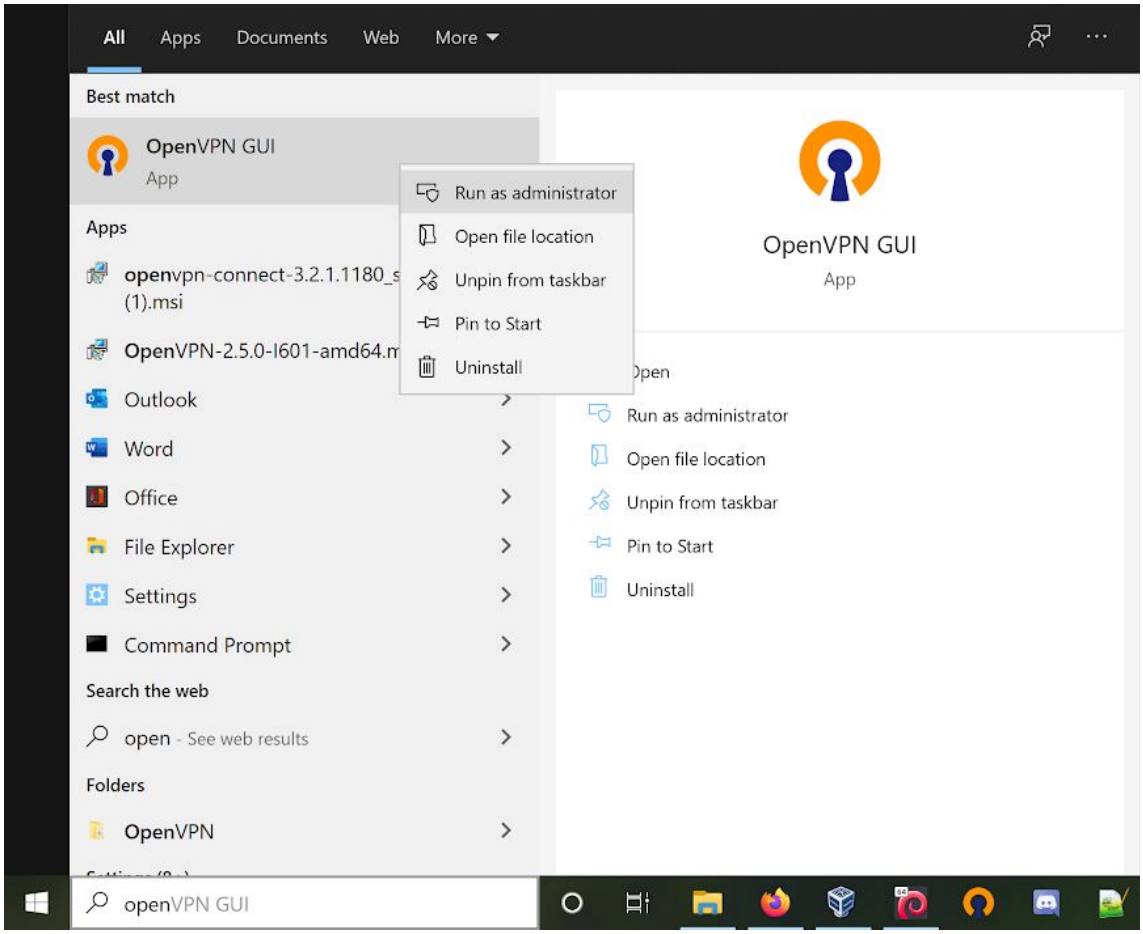
Windows

For Windows, we recommend the official OpenVPN Community GUI client. You can download it from this URL: https://openvpn.net/community-downloads/

Run the installer with the default options. Make sure the following components are selected:

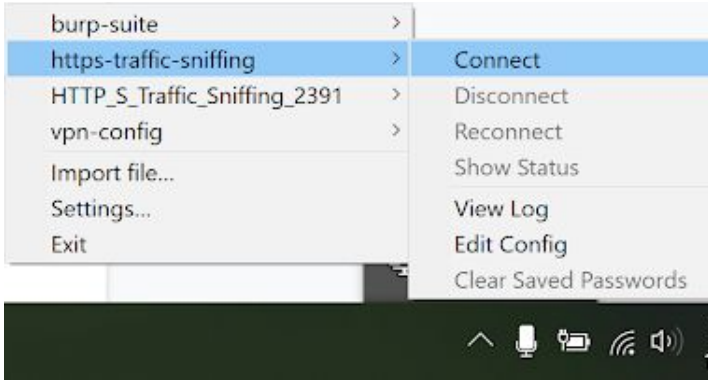
- TAP Virtual Ethernet Adapter
- Add OpenVPN to PATH

Some systems might require extra privileges. In these cases, run the OpenVPN GUI as Administrator. This can be done by right-clicking the executable and selecting “Run as administrator” as shown below.

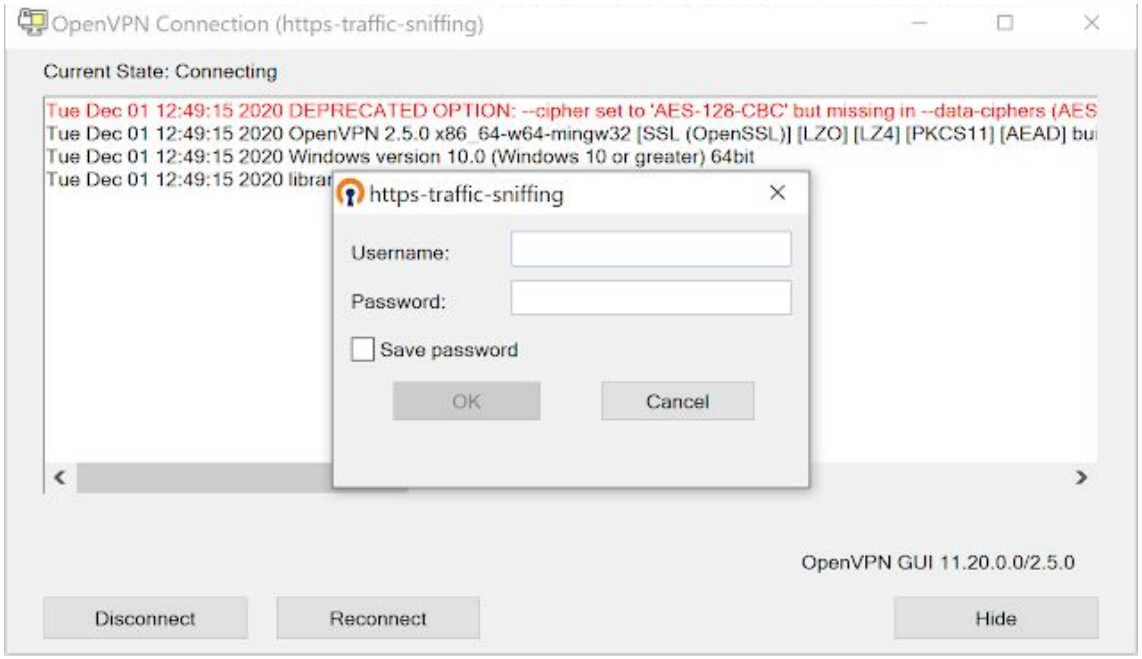


Once the client is running, you should see an OpenVPN icon in the System Tray (on the far right side of the Task Bar) that looks like a screen with a lock on it.

Connecting to a lab for the first time is a 2-step process, import the ovpn file, then connect to that lab network. Right-clicking the OpenVPN icon reveals a menu. If this is the first time you're running OpenVPN, you will see nothing above the gray line on the left. Choose "Import file..." to tell OpenVPN about the ovpn file that you just downloaded. After importing the file, the filename without extension will appear on the list (the image below shows 4 imported ovpn files). To connect to this lab, hover over the ovpn filename and choose "Connect".



You will be presented with a login dialog in which you type the automatically generated username and password when you started the lab. Copy and paste them here and click OK.



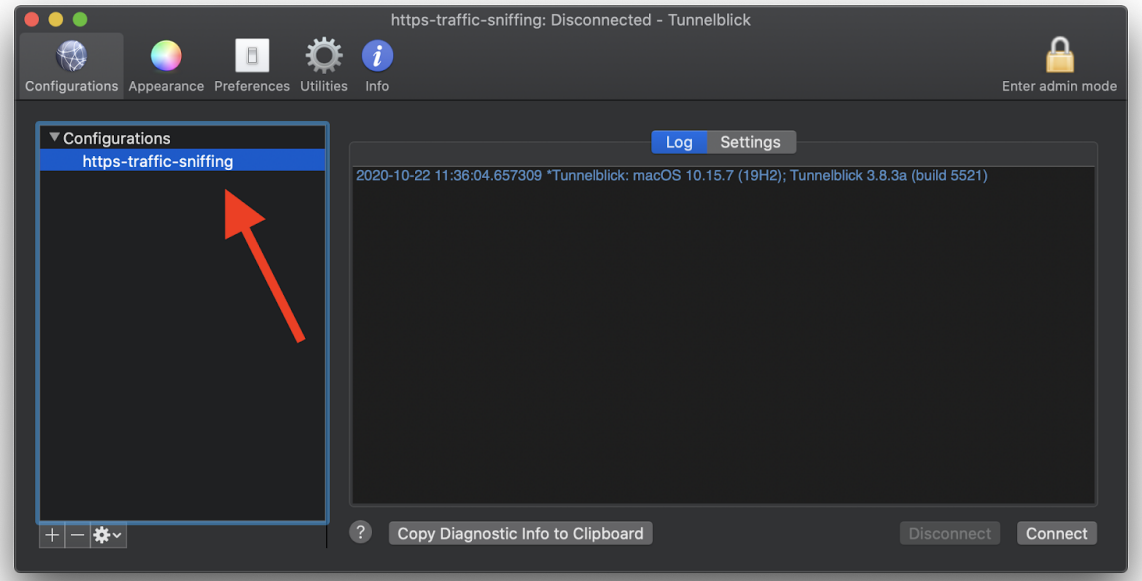
When successfully connected, you will see a notification and be assigned an IP address from the lab network. You can then try to navigate to http://10.54.15.68 in your browser of choice. If you can see the login screen, you're in!

MacOS

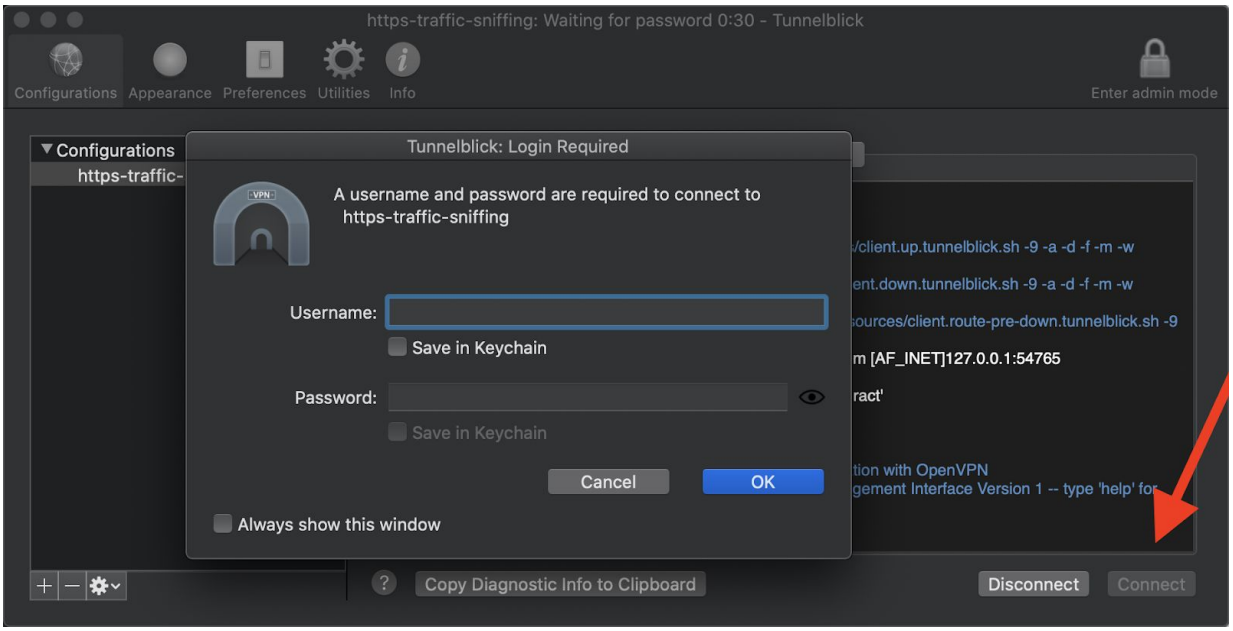
On MacOS, the recommended client is Tunnelblick. You can download it here: https://tunnelblick.net/downloads.html

Install the .dmg and make sure it can run with system privileges from the Security Preference configuration.

Now we just need to drag the .ovpn file to our client (Tunnelblick in this case). Your Operating System might require administrator access or your password.

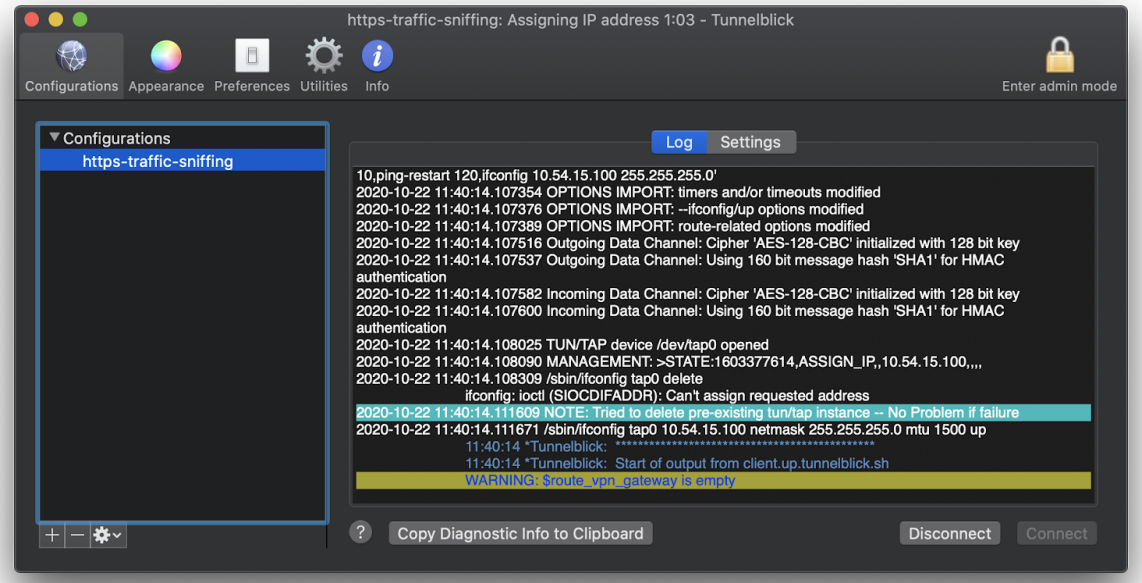


Once the .ovpn file is imported, click on Connect, and you'll be prompted to enter the lab credentials.



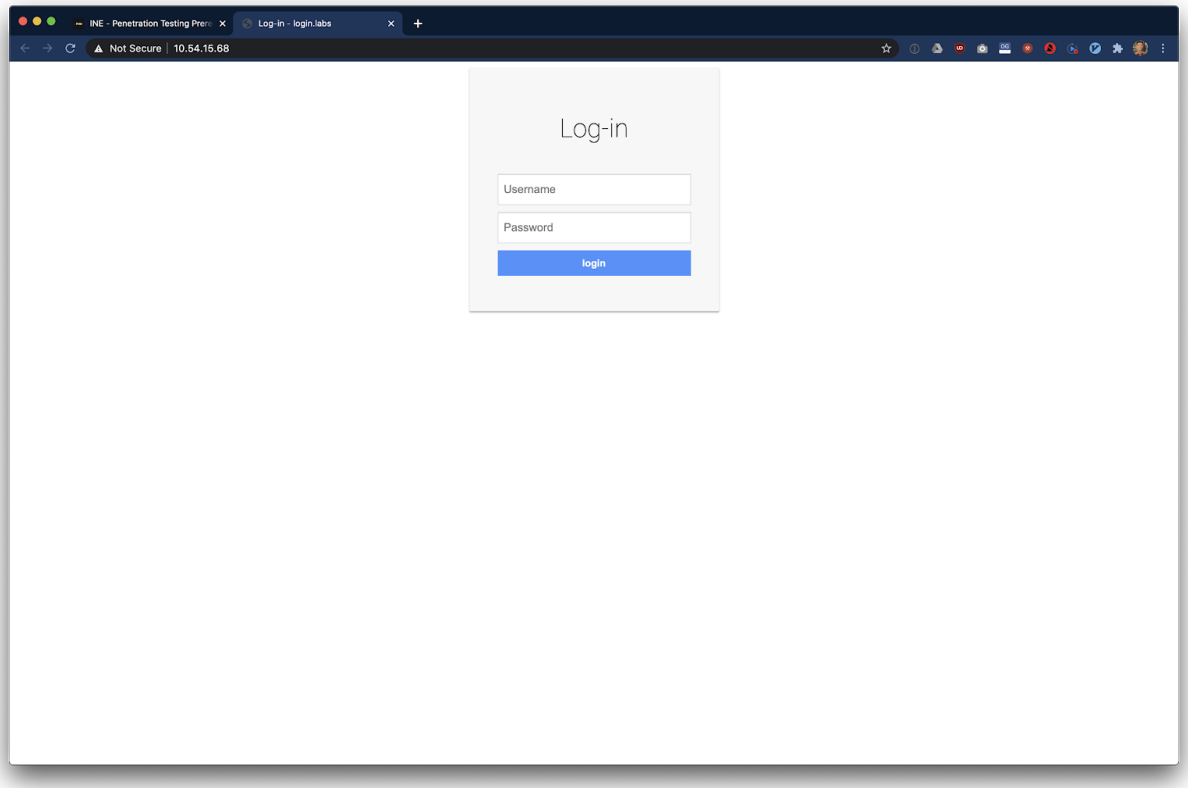
Enter the credentials provided in your lab and click OK. After a few moments, the connection will be established. Some WARNINGS

might appear, but don't worry, these might even be part of the lab you're working on. This is how the client looks once connected:



Congratulations!

Now it's time to move forward with the lab instructions. In this case, we open a special URL in a browser http://10.54.15.68. Seeing the login page appear is proof that we are indeed connected to the lab.



Troubleshooting

Below are some common issues to consider if you're running into trouble.

- Firewalls may be in place at your organization, your ISP or even your country. Some firewalls block all traffic, however many may block only certain sites or types of activity such as using security tools. If you're confident that you followed the instructions above and are still having issues, please inquire as to what equipment may be blocking you between your machine and our virtual network.
- Some OSs are case-sensitive, so be sure to double-check the exact spelling of OVPN files. Tab completion is your friend!
- Most OSs use standard user accounts that don't have root or administrator privileges. Running OpenVPN as an admin is then required. Each case for a given OS is addressed above.

NOTE: This is an evolving document and will be updated regularly. Last updated 12.01.2020.

EXPERTS AT MAKING YOU AN EXPERT