

VMs on School of Cyber Studies Infrastructure

Overview

Each student in this course is allocated a Virtual Machine (VM) running Ubuntu Linux that will be used through multiple projects. These VMs are hosted on School of Cyber Studies (SoCS / CYB) infrastructure and can be accessed remotely throughout the semester.

In order to connect to your personal VM, you will first need to connect to the private network where the VMs are hosted. The outline for connecting to your VMs is as follows:

- **Enroll** in CYB Labs Single-Sign-On (SSO)
- **Obtain OpenVPN configuration** from SSO
- **Import** the OpenVPN config to **OpenVPN Connect** (available to download at: <https://openvpn.net/client/>)
- **Connect** to the VPN using SSO credentials
- **Log in** to personal Ubuntu VM via SSH

School of Cyber Studies SSO

We utilize a Single-Sign-On system for access to VPN configurations and resources used in other courses. This account is *separate* from your standard TU account.

- To access the infrastructure and VPN you need to have or create an account for <https://auth.tulsacyber.com>.
- **To create an account, utilize the following registration link:**
 - <https://auth.tulsacyber.com/if/flow/default-enrollment-flow/?itoken=32804ecc-b4ba-4a41-a046-540ee51...>
- *Please make sure to use your TUNetID exactly (no spaces, uppercase, etc.) to ensure that permissions are automatically set correctly on your SSO account.*
- If you have previously created an account for a different course, please login and check that you see "**Cyber Studies VPN**" and "**Lab Portal**" under the list of applications. If you do not see them, please reach out to your instructor to have your account added to the appropriate groups granting you access.

Note: This SSO account is used for later CYB courses, so please save your credentials. If you lose access to your account credentials and need your password or 2FA authenticator reset, please reach out to your instructor, not TU IT.

Download the OpenVPN Config and Connect

In order to protect the security of this course's VMs from external threats, they are not publicly accessible and can only be accessed via a VPN. We utilize OpenVPN for this.

- Click on the **Cyber Studies VPN** application within the CYB SSO page. This should automatically download the VPN profile (cyber-studies.ovpn) and redirect you to a page containing instructions for installing the **OpenVPN Connect** client (for if you do not already have this installed).
- **Import** the OpenVPN profile (.ovpn file) into your OpenVPN Connect application.
- Click on the File tab at the top of the Import screen.
- Login to this VPN with your SSO credentials
- Note: TU email address is not accepted in the VPN - only the *tunetid* portion of *tunetid@utulsa.edu* works correctly.)
- It is recommended to **save** your username and password so that you can quickly connect to the VPN when working on labs and disconnect when finished.

Once you have **connected** to the VPN, continue to the next section to learn how to SSH into your personal VM.

Use SSH to login to your private VM instance

Before continuing, ensure that you are connected to the VPN.

You will access your personal VM using a terminal tool called OpenSSH. The command for this is **ssh** and installed by default on most Windows, macOS, and Linux operating systems. For Windows users, feel free to use Windows Terminal, Powershell, or a GUI program called PuTTY. MacOS users can use the built-in Terminal program.

You need 3 things to SSH to your VM:

- First, get your assigned **private IP address** for your VM by viewing it in the Lab Portal Application from CYB SSO (<https://portal.tulsacyber.com>); click on "Details")
- The **username** for these each of these VMs is **student** (not your TUNetID)
- The default student password is **StudyOS26**
- *Please change it after first login*

Type the following into your computer's Terminal to initiate an SSH session to your VM as the "student" user:

```
# Replace XX below with your personal IP address
% ssh student@10.30.248.XX
```

You should be prompted for a password.

Tips:

- Linux does not show anything being typed into password fields, but it is being entered!
- If you are on Windows, pasting into a terminal is slightly weird. You paste with a single right-click on your mouse. Again, it will appear nothing is happening if pasting into a password

field, so you will need to trust that it was pasted and press enter. It takes time to be comfortable with this.

- Copying text on a Windows Terminal is done by selecting the text with your mouse. There is no need to use Ctrl+C, in fact, that shortcut has an entirely different meaning in a Terminal - killing whatever CLI program is currently running.
- macOS and Linux users should right click to open a menu and then select Paste.

Try it out for yourself. Once you are logged into the VM, you can issue some commands to explore a bit.

The first command you should run is the **passwd** command. This will allow you change your VM's password from the default to something that you will remember.