Cybersecurity

Cybersecurity Boot Camp Virtual Machine Set-Up

IMPORTANT NOTE: IF YOU HAVE AN M1 MAC, YOU WILL NOT BE ABLE TO GO THROUGH THIS SETUP. PLEASE REFERENCE HARDWARE REQUIREMENTS FOR THIS COURSE.

Throughout this course, you will use a local virtual machine to simulate various operating systems, use specialized tools and target vulnerable machines. This guide provides instructions on installing and maintaining the virtual machine environment that you will use throughout this course.

In order to get our VMs up and running, we will need to:

1. Install VirtualBox. You should have already downloaded and installed **VirtualBox** as part of prework. If you haven't installed it yet, you should install it now using the instructions that follow.

2. Install Vagrant. Once VirtualBox is installed, you will install another tool called **Vagrant**. Vagrant will be used alongside a script and a vagrantfile to blueprint and build the environment.

These three main components work in conjunction with your local machine to run and manage your cybersecurity boot camp lab environment:

- **VirtualBox** is a virtualization platform that allows you to run isolated, virtual operating systems within your current operating system.
- **vagrant-linux.sh** is the script that you will run to ensure that your virtual machines are installed properly on your local machine.
- **Vagrantfile** configures and defines your virtual machine set-up. In our case, this Vagrant file, when executed via the vagrant-linux.sh script, will configure a custom Linux Ubuntu machine.

Following the instructions to download VirtualBox and Vagrant, this guide will provide a more detailed description of Vagrant, an overview of Vagrant commands, and best practices for keeping Vagrant machines updated.

Another term to know is **local machine**. Local machines are the physical computers we are using to run the virtual machines.

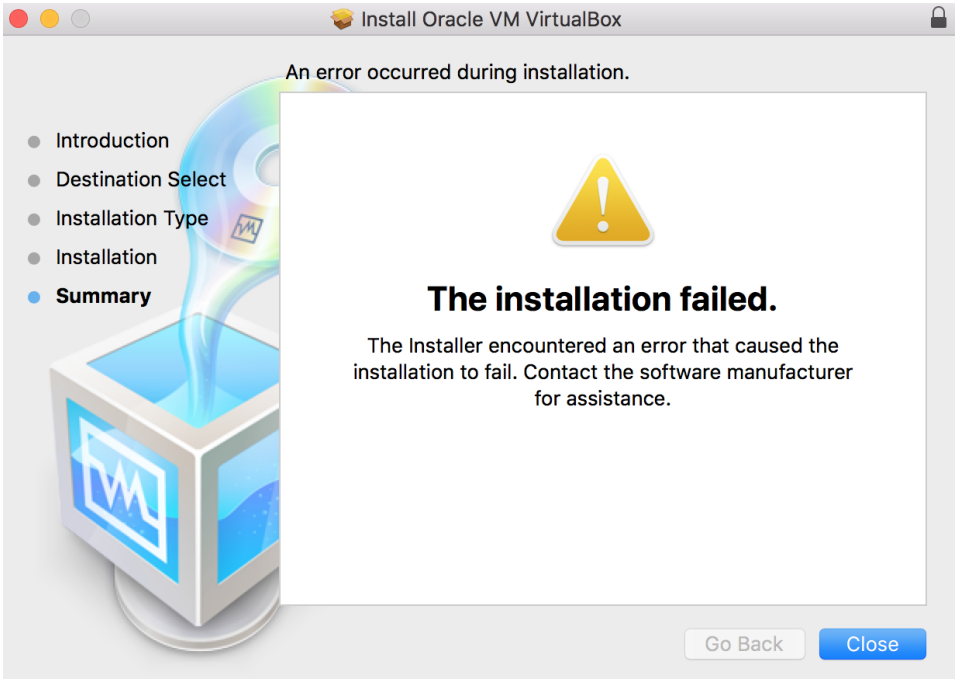
Part 1: Downloading and Running Virtual Box and Vagrant

IMPORTANT: Please read through **this document** for thorough step-by-step instructions on downloading and installing your virtual machine. This document also contains more detailed instructions on the Vagrant commands you'll need to update your virtual machine as well as common troubleshooting issues.

1. First, you will need to access the command line.

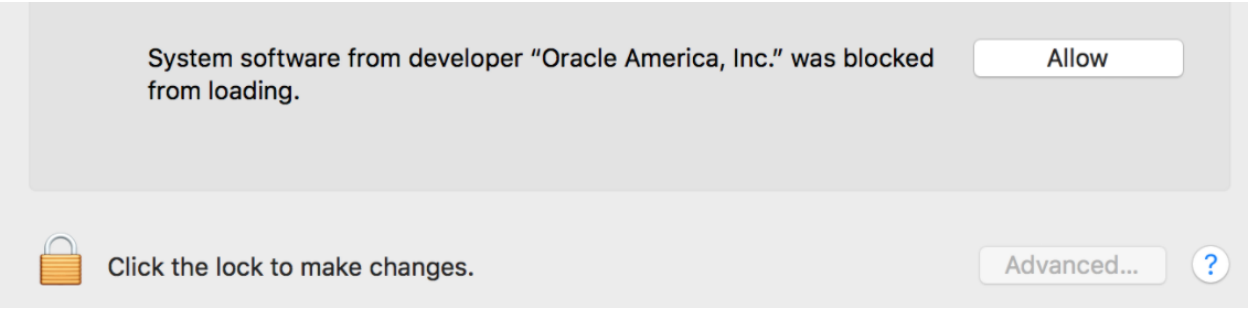
    - **Windows users** will need to install Git Bash.
    - **Mac users** will use Terminal.

2. Download and install **Virtual Box** at https://www.virtualbox.org/wiki/Downloads.
    - **macOS Mojave/Catalina users:** at the end of the VirtualBox installation, if it says **The installation failed**, you will need to go to your Security & Privacy settings, and allow software from Oracle, America:



    - If you see the above after running the VirtualBox installer, this means that you need to update your Security & Privacy settings to allow the installer to finish. Complete the following steps:

- Re-run the installer until it says ***The installation failed***. Click **Close** and choose to **Keep** the installer.
- Go to your **System Preferences** and select **Security & Privacy**.
- Within the **Security & Privacy** settings, click the **General** tab. You should see the following message in the bottom-half of the window:



- Click on the padlock icon and enter your password/touch ID.
- Click on the **Allow** button.
- Re-run the Virtualbox installer and it should finish properly this time.

3. Download and install the latest version of **Vagrant** at https://www.vagrantup.com/downloads.html.

    - Select the appropriate installer for your operating system:

        - The installer should save to your `~/Downloads` directory.
        - Open this directory and then double-click the installer.
        - This will install Vagrant on your system.

Part 2: Downloading the Virtual Machine

Now that we have the software needed to create and run our virtual machine, we will use **Vagrantfile** and **vagrant-linux.sh** to create and download the machine.

- Download the script **vagrant-linux.sh.**
- Download the **Vagrantfile**

Open Git Bash (Windows) or Terminal (Mac).

NOTE: Windows users must verify that they open Git Bash as an administrator. This usually happens by default, but to confirm, complete the following:

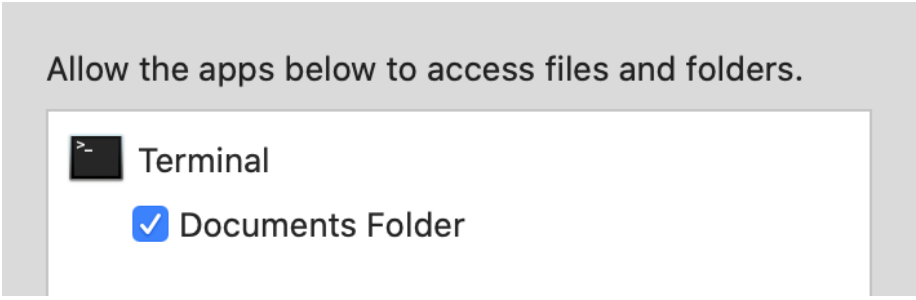
- Search for Git Bash in the Windows search bar in the bottom-left of the screen.
- Right-click Git Bash and then click **Run as Administrator**.

On the command line, navigate to the directory where you downloaded the script and Vagrantfile. This is usually the Downloads directory.

- Type `cd ~/Downloads` and press **Enter**.

Run the following command to download and initiate the VM:

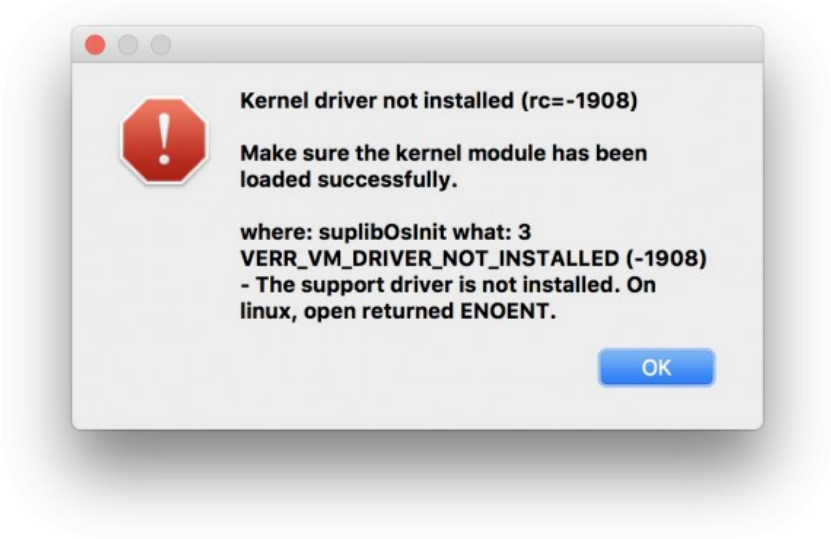
- **Windows users**: Type `bash vagrant-linux.sh --create` and press **Enter**.
- **Mac users**:
  - Type `chmod +x ./vagrant-linux.sh` to make the script executable and press **Enter**.
  - Type `sudo bash vagrant-linux.sh --create` and press **Enter**.
  - **macOS Mojave/Catalina users:** when running the script for the first time, you may see a popup that says ***"Terminal" would like to access files in your Documents folder***.
    - You will need to once again go to the **Security & Privacy** settings, but this time, go to the **Files and Folders** tab, where you should see the Terminal icon. Click the lock, and then click the checkbox next to the folder:



    - After running the script, your virtual machine will automatically start in a new window. You should see the following Ubuntu loading screen:

- You'll then be able to log into the machine with the credentials given to you in class.

- **macOS Mojave/Catalina users**: that if you see the following error when the machine is launching, then you will need to follow the earlier instructions on re-running the VirtualBox installer and changing your **Security & Privacy** settings. Afterward, you can re-run the script and the virtual machine should show up properly.



Once the VM is downloaded, it will appear as a graphical user interface (GUI).

Part 3: Accessing Your Virtual Machine

In the upcoming units, you will learn how to access your virtual machine via the command line.

For now, we will use the GUI to access the machine. GUI is simply the term for the windows and visuals we see on a typical computer screen, contrary to the minimalist lines of the command line. We'll learn much more about GUIs and command lines in Week 3.

- Open VirtualBox. In the left pane of the window, you should see the machine you downloaded.
- Click the Linux machine.
- Click the Start icon in the top menu.
- Allow three to five minutes for the machine to start up.

When prompted, enter the log-in credentials:

- Username: sysadmin
- Password: cybersecurity

When you are done using the machine, you can close the Virtual Box window.

- When exiting Virtual Box, you will be provided options as to how to shut down.
- Select the first option: "Save the Machine State".

At this point, you VM should be set up. The remainder of this document contains the below sections:

1. Steps on how to update your machine
2. Common troubleshooting issues you might encounter when updating your machine

Please note that you will not need to update your machine on the same day you download and install it for the first time. However, it is best practice to update your machine at the end of every unit, after you have completed that unit's homework.

Virtual Machine Set-Up and Maintenance

In the following sections, we'll explain Vagrant more in depth and what Vagrant commands you'll need to know to make sure your machines are updated and managed properly.

What Exactly Does Vagrant Do?

Vagrant is a tool that allows teams to easily create reproducible, configurable, and portable work virtual environments with VirtualBox or other programs, such as Hyper-V and Docker.

You'll use Vagrant in conjunction with VirtualBox extensively throughout the boot camp, so it is important to know how to use common Vagrant commands in order to keep your boot camp lab environments updated, stable, and secure (or in some cases, intentionally unsecure).

The virtual machines will be constantly optimized and refined. Vagrant allows you, the user, to quickly receive the latest changes without having to make any configurations on your own.

Instead, Vagrant will get the latest virtual machine updates for you and make sure your virtual machines are up-to-date. We'll cover what commands to run for this as well as other general Vagrant commands in the next section.

Vagrant Commands

If you are on a Mac computer, you'll use Terminal. Windows users will use Git Bash.

If you are unfamiliar with these terms or the command line, do not worry! You will get familiar with them in this course.

When using Vagrant commands, make sure that you are running these commands within the directory where you have your Vagrantfile.

Unless your instructor directed you to set up Vagrant in another way, and depending on how far you are in the curriculum, your lab's Vagrantfiles can be found in the following directories:

- `$HOME/Documents/Cybersecurity-Bootcamp/Linux-Module` which contains your ongoing Linux Ubuntu virtual machine that you will use for several weeks in the program.
- `$HOME/Documents/LabEnvironments/linux-scavenger` which contains a specific smaller virtual machine that you will use only for the Unit 6.3 activity.

> **NOTE:** After you complete the Unit 6 HW, you will have an additional Vagrantfile. Download this file during the Unit 6 HW.

To find the locations of your Vagrant machine installations:

- Run `vagrant global-status --prune` to see a listing of all known installation directories. Vagrant will also check to see which machines are running.

You can always access your virtual machine by opening up VirtualBox but you can also open your virtual machine on the command line:

- Run `vagrant up` to open your virtual machine.

To get the most recent changes onto your machine, run these commands:

- Run `vagrant box update` to get the most recently updated virtual machine.

  This might take several minutes or longer, depending on your internet connection. Once this is complete, run the following command:

- Run `vagrant destroy` within the directories that your Vagrantfiles are installed to ensure that the virtual machines are stopped and all associated files are removed.
- Run `vagrant up` to launch the newer version.
- (Optional) Run `vagrant box prune` afterwards to delete all old, unused versions of the virtual machine.

Shutting down your machine (via Vagrant, but not necessary)

- When you are done with your session, run `vagrant halt` to shut down your virtual machine.

An all-in-one-command to ensure you get the latest build

- The following command can be run to update the Ubuntu machine:

```
cd $HOME/Documents/Cybersecurity-Bootcamp/Linux-Module && vagrant box update
&& vagrant destroy --force && vagrant up
```

How Often Should I Update My Vagrant Virtual Machine?

Remember to update your machine at the end of every unit. Ideally you should be updating your machine after you have completed the unit's homework, but in most cases, you can update your machine at the end of the Day 3 lesson in the unit.

Be aware that when you update your machine, your machine will reset the contents. You will lose any files and programs you have installed, as well as progress on work you have made.

If you have any questions or issues on how to do this, please attend office hours with your TA and instructor to get guidance.

Remember when updating your machine you MUST run the following commands. The last one is optional:

- `vagrant box update`

- `vagrant destroy`
- `vagrant up`
- `vagrant box prune` (Optional)

NOTE: When you update your machine, you will lose your progress as the box is getting replaced. However this should not be an issue as the units in this program are independent from each other and there are no dependencies from one week to the next that you must maintain in your virtual machines.

Troubleshooting

Unable to download the latest version of a Vagrant machine

The latest version of the boot camp's Ubuntu Vagrant machine can be found at https://app.vagrantup.com/cybersecurity/boxes/UbuntuVM.

If the above is not updating your machine properly, run the `vagrant box remove cybersecurity/UbuntuVM --all` command and attempt to `vagrant destroy && vagrant up` again.

- `vagrant box remove cybersecurity/UbuntuVM --all` removes all versions of the Ubuntu VM provided by the Cybersecurity Boot Camp.

If neither work, use the deep clean process:

1. Run `vagrant destroy` in all of the boot camp's vagrant directories.
2. Delete any `.vagrant.d` subdirectory in the boot camp's vagrant directories and in your `$HOME` directory.
3. Go back to the boot camp's vagrant directories and re-run `vagrant up` in each to grab the latest versions of the machines.

If you see the following: `playbook' does not exist on the host - error`

If you see the above error error when running `vagrant up`, run the command `vagrant box remove cybersecurity/UbuntuVM --all` and attempt to `vagrant destroy && vagrant up` again.

Permission issues after running *sudo vagrant up* (Mac)

If you're using a Mac and you used ***sudo*** to launch the vagrant machine, you can either continue using `sudo vagrant up / sudo virtualbox` for the rest of the boot camp or swap to the "best practice," which is to use regular `vagrant up`.

If you want to essentially deep clean permission issues caused by using **sudo vagrant up**:

1. First, use **vagrant global-status --prune** to check where vagrant directories exist on your machine. Then run **sudo vagrant destroy** in each of these directories to remove the virtual machines. If **vagrant global-status --prune** didn't work, just run **sudo vagrant destroy** in the default boot camp directories listed earlier in this document.
2. Next, you need to get rid of the **.vagrant** directories on your machine by running **sudo rm -rf .vagrant***.
3. Lastly, re-run **vagrant up**, *WITHOUT* ***sudo***, in each of the directories to grab the latest boxes.