

Cyber Fire OT Class

Remote Setup & FAQ



Remote Training Setup and FAQ

Overview

The labs for the Cyber Fire OT Class use real industrial equipment. For in-person trainings, the class units are placed at each desk. For the remote offering, changes were made to the equipment to accommodate remote access to class units. A remote-access VPN allows individual users to establish secure connections with a remote computer network, in this case the the Cyber Fire OT Class network. Each student will be provided an OpenVPN configuration that will allow them to connect to a network with an OT Class unit. Additionally, an IP camera has been added to the network and is pointed at the training unit. Students can login to the camera's web-interface and view live feeds of their designated class unit. The labs for The Cyber Fire OT Class use a Virtual Machine (VM) running Kali Linux. This virtual machine has been made available to students via a box.com link. **The virtual machine is approximately 10 GB in size and may require significant time to download.**

Prior to the start of class, students should have virtualization software installed, the VM downloaded, and the VM imported to their computer.

System Requirements

1. The ability to run virtualization software such as VMware or VirtualBox.
2. At least 6GB of memory, as the VM utilizes 4GB. This can be lowered to 2GB in special circumstances, but **we strongly recommend having a machine that has 8GB of memory** or greater and running the VM at its recommended 4GB memory allocation.
3. VMware has its own system requirements, detailed [here](#).
4. We recommend using VMware, but if you are using VirtualBox, its requirements are detailed [here](#).

Download the The Cyber Fire OT Class Virtual Machine

1. The virtual machine required for the workshop will be downloaded from an INL Box account. A link to download the VM will be provided to you via your registration email prior to class.
 - a. After you receive the email with the download link, proceed to step b. below.
 - b. Download the .zip file and then unzip/extract the file to your computer
 - c. Follow the instructions in the "Importing the Kali VM" section below to load the virtual machine into your virtualization software

Install Virtualization Software

1. [VMware Player](#) is free for Windows and Linux users.
2. [VMware Fusion](#) is available for Mac OSX users, but not for free.
3. [VirtualBox](#) is free for Windows, Linux, and Mac OSX users.

Importing the Kali VM Using VMware Products

1. Extract the zip file to a folder on your computer.
2. Open VM Workstation/Fusion/Player.
3. From the File Menu select 'Open'
4. Select the **Student-Kali-Remote.ovf** file from folder where the files were extracted.
5. Push Play on the VM. You should see the Kali VM start.
6. The logon credentials are '**root**' and '**icslab**'.
7. After successfully logging in, you may turn off the virtual machine until the start of the class.
8. **You are now ready** to participate in the Remote Cyber Strike Training.

Importing the Kali VM Using VirtualBox

1. Extract the zip file to a folder on your computer.
2. Open VirtualBox.
3. From the File Menu select '**Import Appliance**'.
4. Select the **Student-Kali-Remote.ovf** file from folder where the files were extracted.
5. Push Play on the VM. You should see the Kali VM start.
6. The logon credentials are '**root**' and '**icslab**'.
7. After successfully logging in, you may turn off the virtual machine until the start of the class.
8. **You are now ready** to participate in the Remote Cyber Strike Training.

OpenVPN

OpenVPN has been installed on the Kali Linux VM provided for you. At the start of class, you will be assigned a student number. You will need this number to configure the VPN. This process only needs to be done once.

You connect the VM to the The Cyber Fire OT Class network by:

1. Turn on your Kali Linux VM
2. Log in with "**root**" and "**icslab**" as the credentials.
3. Open a terminal prompt.
4. Type "**./vpn_config.sh**" and press "enter".
5. When prompted, type your student number and press enter. It will be two digits (ex: 01, 02, 11, etc.). The script configures the connection and verifies that it was successful. Contact an instructor if you receive an error message.

If you have previously done the VPN setup above, but at any time during class it becomes disconnected:

1. Open a terminal prompt.
2. Type "**./vpn_restart.sh**" and press "enter" to reconnect. Contact an instructor if you receive an error message.

Frequently Asked Questions

I get an error when extracting the zip archive file.

Verify that the provided MD5 or SHA1 hash matches. The hashes.txt file, from the download link, includes the hashes for the Kali-Remote.zip file. You can use a checksum application, such as [Hash Tool](#) or [Hash My Files](#) to verify that the file has not been corrupted. If the hashes match and you are still seeing errors, try using a different archive tool. If you are using windows, try using [7zip](#). If you are using Mac, try using, [WinZip](#) for Mac (free 45 day trial).

“This host supports Intel-VT-x, but Intel-VT-x is disabled” error message

Follow the [instructions](#) here.

Can I use my own VM of Kali?

You can use your own version of Kali to do many of the techniques we cover in the class. However, you will not be able to connect to the Cyber Strike Network from your own VM.