CyberOps Associates v1.0

Virtual Machine Lab Environment - Frequently Asked Questions

Last Updated 20 July 2020

What is Oracle VirtualBox? Where do I get it? and how much does it cost?

Oracle VirtualBox is a free, open source, cross-platform virtualization software used in this course. It can be installed on Windows, Linux, Mac OS X, and Solaris x86 computers. The VirtualBox base software is licensed under the GNU General Public License version 2 and the extension pack is available under the Personal Use and Evaluation license. If you qualify under the terms of this license, VirtualBox is available at no cost. VirtualBox can be downloaded from Oracle: http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html

Back to Top

I can’t get the virtual machines to work properly in Oracle VirtualBox. What can I do?

If you currently have a version of Oracle VirtualBox that is older than the 5.2.4 version, you need to update to the 5.2.4 version or higher for the virtual machines to work properly.

Back to Top

What are CyberOps Workstation and Security Onion virtual machines?

The CyberOps Workstation is a custom-built VM based on Arch Linux. This VM is used in most of the labs in this course. The Security Onion VM is used in later labs to review pre-populated alerts and log messages generated during the exploits. The Security Onion VM is used for network security monitoring, intrusion detection, and log management.

Click here to learn more about Security Onion.

Back to Top

What is Mininet?

Mininet is installed in the CyberOps Workstation VM to support the labs in this course. Mininet is a *network emulator* that creates a network of virtual hosts, switches, controllers, and links.

Back to Top

Why do I need all that RAM memory?

In this course, two virtual machines are used: CyberOps Workstation and Security Onion. The minimum RAM memory requirement to run CyberOps Workstation virtual machines is 1 GB. However, for the Security Onion virtual machine, 4 GB RAM is recommended. The RAM memory recommendation on Security Onion VM allows the services, such as network security monitoring (NSM), to function properly. While working with computers without the minimum RAM memory, the VM may appear to be functioning properly; however, some of necessary services will stop functioning without warning. This will result in the loss of captured data with alerts and log messages and the inability to perform the labs that use the Security Onion VM.

Back to Top

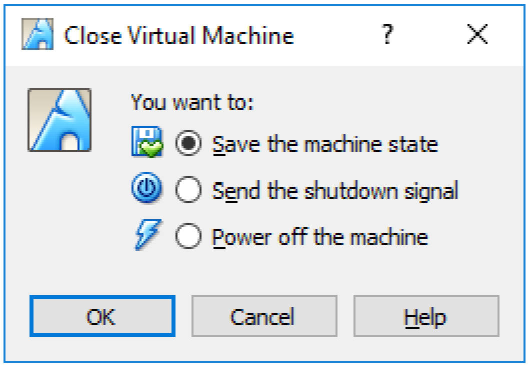
Why are my mouse and keyboard not working outside of the VM?

If your keyboard or mouse does not function outside of the VM, press the CTRL key that is on the right side of the keyboard. This is called the VirtualBox host key. The host key is shown on the lower right-hand corner of the VM window. Other host operating systems may use another key as the host key.

Back to Top

The labs are too long, and we can't finish it in one class period. What should I do?

Become familiar with the labs before class if possible. The state of the VM can be saved so that you can continue the labs at a later time. To save the VM state, click the **Save the machine state** radio button and click **OK** when closing the VM. The next time you start the virtual machine, you will be able to resume working in the operating system from the saved state.



Close Virtual Machine

You want to:

● Save the machine state

○ Send the shutdown signal

○ Power off the machine

When you are ready to resume the labs, select the desired VM and click **Start**. The VM will start in the same state as when it was saved.

Back to Top

How do I remove the virtual machines when I am done with the course?

1) Shut down the VM

2) Right-click the VM > **Remove**, select **Delete all files**

Back to Top

How do I replace a file that was accidentally deleted?

1) Shut down the VM
2) Right-click the VM > **Remove**, select **Delete all files**
3) Re-import the VM: **File** > **Import Appliance**

Back to Top

I made a change in a VM, and it is not working properly anymore.

1) Shut down the VM
2) Right-click the VM > **Remove**, select **Delete all files**
3) Re-import the VM: **File** > **Import Appliance**

Back to Top

The VM screen is black, what do I do now?

When the VM has been idle for some time, the screen may be black. Click anywhere within the VM to display the login screen.

Back to Top

I copied the command from the PDF and pasted it into the terminal. Why is it not working?

When copying and pasting commands from lab documents, there is a possibility that the formatting and characters from the document may not be compatible with the command line. The solution is to delete and retype the offending characters. The command should then run.

Back to Top

Network security monitoring (NSM) is not working in Security Onion? How do I restart it?

The NSM services take time to initialize. Depending on the host system resources, they may take a minute or more. If that period has passed and the NSM services are not running, open a terminal and enter the **sudo so-restart** command. The NSM services will then begin to reinitialize.

Back to Top

The command is really long. What can I do to make it easier?

Linux is designed for the command line interface. Several features are included to facilitate entering commands. One of those features is TAB key autocompletion. When typing a command or a directory path, use the TAB key to complete it. Linux will display the possible completions if the typed portion is not unique. Linux will autocomplete the command or path as soon as the typed portion is unique.

Some of the long complex commands are documented in a text file (**/home/analyst/lab.support.files/long_commands***)* stored in the CyberOps Workstation virtual machine.

Back to Top

I have mistyped a long command. Do I have to retype again to fix it?

You can use the up arrow to access the commands that were executed earlier in the same terminal window. The command can then be edited.

Back to Top