Using the Practice Images

Introduction

Hello GSMST CyberDragons!
In the parent folder of this Google document titled "CyberPatriot Practice Images," there are four different practice images that we created. Practice images are virtual machines that are not created by the Air & Space Forces Association and come preconfigured with vulnerabilities. On the following pages, we will tell you how to download these images and run them using a virtual machine of your choice to help you prepare for the actual CyberPatriot competition. If you haven't signed up for the CyberPatriot team, that's okay too! We will be reviewing these images in detail over the course of our next few meetings, and it is highly recommended that you try them on your own so that you have a good idea of what's going on.

Getting Started

To actually open the images, you need to install [VMWare Workstation Player] (on Windows/Linux) or [VMWare Fusion] (on Mac) on a PERSONAL COMPUTER. Make sure you click on the option that says “Download Now” and not one that asks you to register for a personal license. Then, simply go through the installation process and install VMWare.

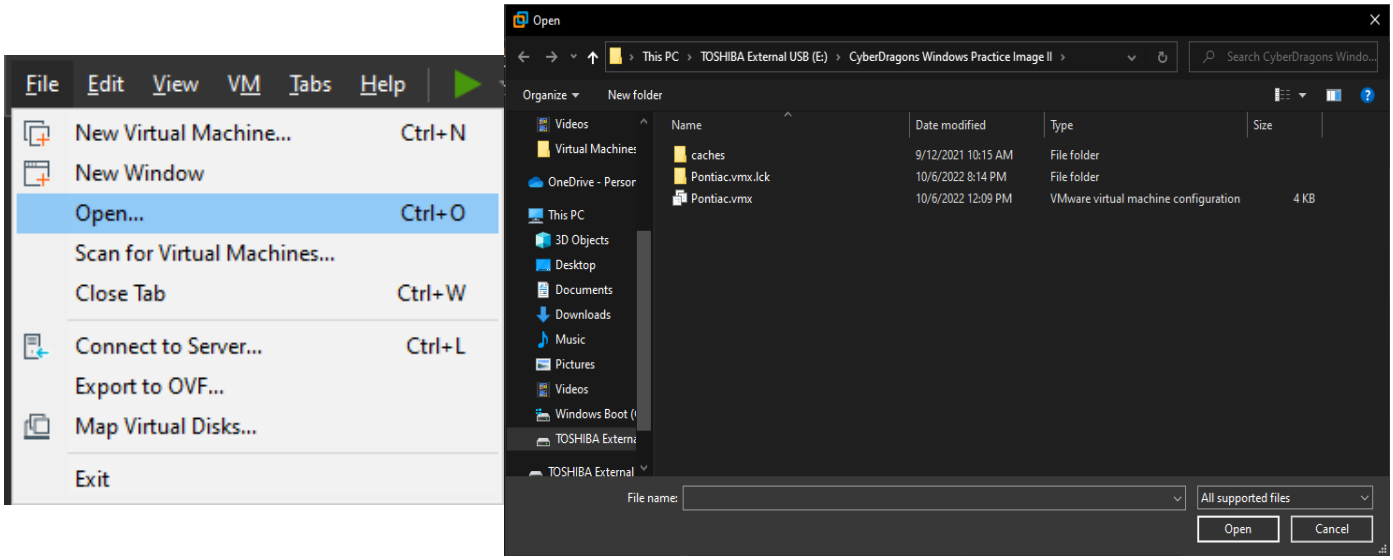
Downloading the Images

Once you have installed VMWare, install the image(s) that you would like to practice. Once the zip file for the image is done downloading, you can extract it. Below is a table of the minimum spatial requirements you need to install each image. If these file sizes are too heavy for your computer, you may want to consider downloading the images on an external hard drive or flash drive instead.

	Ubuntu 16 Practice Image II	Ubuntu 16 Practice Image III	Windows 10 Practice Image I	Windows 10 Practice Image II
Zip file size	2.71 GB	3.77 GB	9.17 GB	18.57 GB
Uncompressed file size	7.25 GB	10.86 GB	19.05 GB	40.81 GB
Total space required	9.96 GB	14.63 GB	28.22 GB	59.38 GB

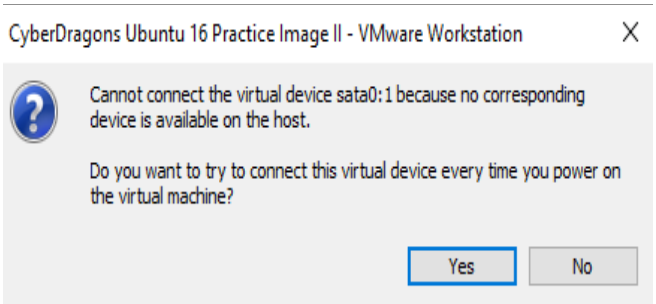
Opening the Images

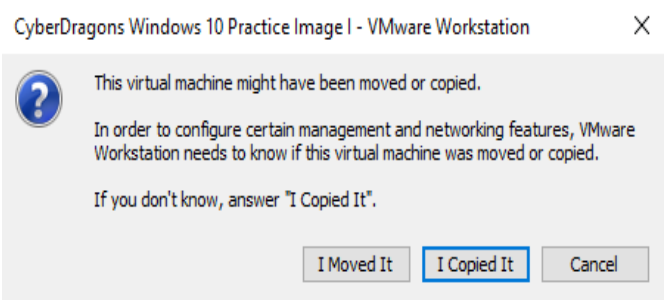
To open an image, launch VMWare, click on “File” in the top left and “Open.” Then, navigate to the folder that you extracted the image to, select the .vmx file, and click “Open” again. Finally, power on the virtual machine!

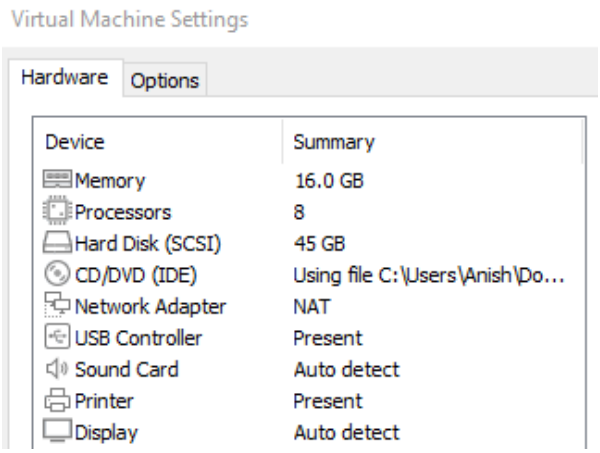


Virtual Machine Tips

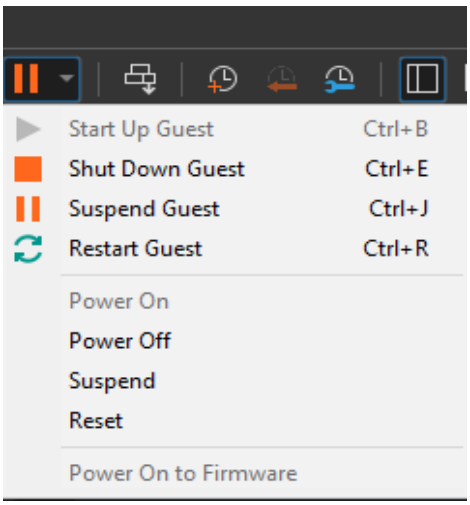
If you get a prompt that asks you to connect to sata0:1 every time you start the virtual machine, always click “Yes.” If you get a prompt that asks whether you moved or copied an image, always click “I Copied It.”





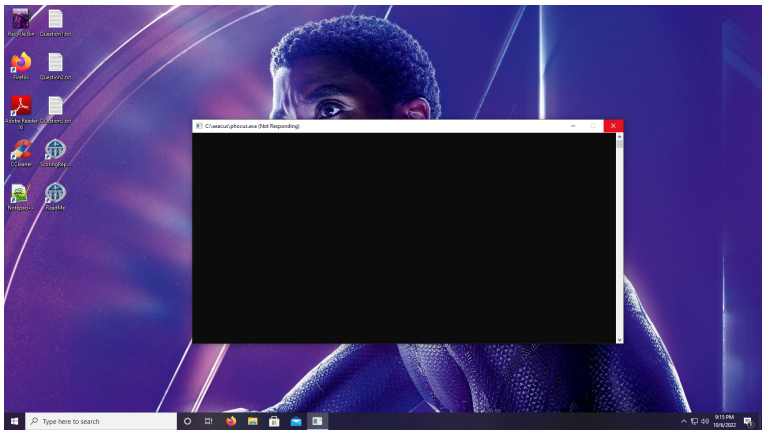


You can also configure the virtual machine to have more memory and processor cores if your personal computer supports that. Just right click on the virtual machine, go to its settings, and customize its hardware.



You can suspend a virtual machine by pressing the button that looks like a “pause” button. This will save the current state of the virtual machine until you decide to continue working on it, and the state persists through reboots of the host machine. Otherwise, you can just shut down the virtual machine completely.

While working on a Windows practice image, you may see a command prompt window named “phocus.exe” on startup. You can just close out of it, as its only use is starting the autoscoring engine.



Getting Started With Solving Images

When booting up a CyberPatriot image for the first time, ALWAYS read the README of the image! This will give you the scenario behind the image, which provides necessary context on what actions you should and should not take while working on the image. To check your point count, click on the “Scoring Report” shortcut on the desktop.

CyberDragons Windows 10 Practice Image I
README

Please read the entire README thoroughly before modifying anything on this computer.

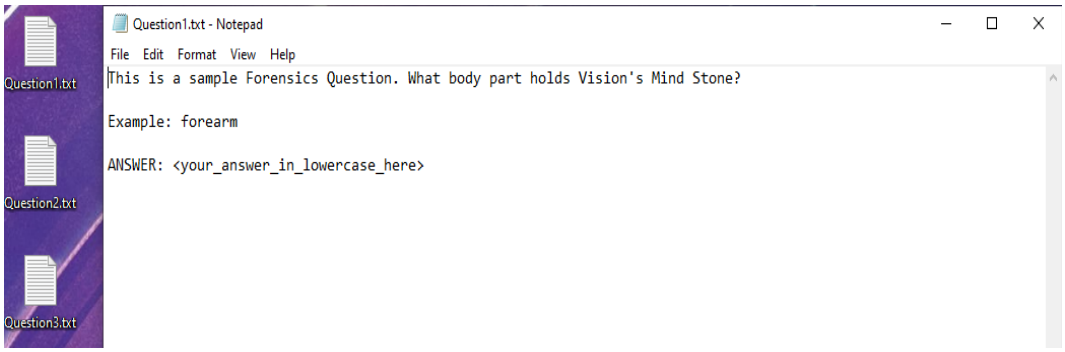
Forensics Questions

If there are "Forensics Questions" on your Desktop, you will receive points for answering these questions correctly. Valid (scored) "Forensics Questions" will only be located directly on your Desktop. Please read all "Forensics Questions" thoroughly before modifying this computer, as you may change something that prevents you from answering the question correctly.

Competition Scenario

This company's security policies require that all user accounts be password protected. Employees are required to choose secure passwords, however this policy may not be currently enforced on this computer. The presence of any non-work related media files and "hacking tools" on any computers is strictly prohibited. This company currently does not use any centralized maintenance or polling tools to manage their IT equipment. This computer is for official business use only by authorized users. This is a critical computer in a production environment. Please do **NOT** attempt to upgrade the operating system on this machine.

To earn points, we recommend doing the Forensics Questions first, which test your knowledge on what actions to take to locate certain vulnerabilities and are usually located in text files on the desktop. Combined, the Forensics Questions award the greatest amount of points and usually do not take that long to solve. If you are spending more than 10-15 minutes on a single Forensics Question, skip it and come back to it later. User management and permissions are also another category of vulnerabilities that allow for quick and easy points.



Additional Resources

If you need any additional help getting started, we recommend looking up CyberPatriot resources (e.g. “Vulnerability Checklists”) on Google. In official CyberPatriot competitions, the Internet is an allowed valuable resource that can be utilized by teams to guide them and further reinforce their concepts in securing systems. We trust you will use the Internet in this same manner. Additionally, feel free to use the PicoCTF & Dichotomize presentation as a reference for basic commands to use while in a shell.

Closing Remarks

“CyberDragons Ubuntu 16 Practice Image III” and “CyberDragons Windows 10 Practice Image II” are significantly harder than their paired Ubuntu and Windows practice image. All applicants of the CyberDragons team must **complete EITHER the Ubuntu 16 Practice Image III or the Windows 10 Practice Image II to the best of their ability.** Please do not attempt to reverse engineer the images as all of the answers are encrypted in the scoring engine files, and you could permanently damage the image as a result. Please do not share answers to the difficult practice images with anyone else either, as we will review them in a future meeting together once the CyberPatriot teams are fully formed. Answers to the “easier” practice images for each operating system are on the following pages. Even though it is not required for team applicants to complete the easier practice images, it is highly recommended that they do so in order to “ease into” the more difficult images. Good luck, everyone!

Answers to Ubuntu 16 Practice Image II (“Super Girl”)

100 out of 100 points received

Connection Status: OK

Internet Connectivity Check: N/A
Aeacus Server Connection Status: N/A

0 penalties assessed, for a loss of 0 points:

23 out of 23 scored security issues fixed, for a gain of 100 points:

Forensic Question 1 correct - 7 pts
Forensic Question 2 correct - 7 pts
Forensic Question 3 correct - 7 pts
Removed Unauthorized user lexluthor - 5 pts
Removed Unauthorized user sarias - 5 pts
User mel is not an administrator - 4 pts
User jjons is now an administrator - 4 pts
Guest Account has been Disabled - 4 pts
Changed insecure password for user adanvers - 4 pts
Default Password MAX Days set to 90 - 3 pts
Default Password MIN Days set to 10 - 3 pts
Firewall protection has been enabled - 4 pts
PureFTPd service has been disabled or removed - 4 pts
Auto Updates have been enabled - 3 pts
Linux Kernel has been updated - 4 pts
Bash has been updated - 4 pts
FireFox has been updated - 4 pts
Prohibited MP3 files are removed - 4 pts
Unauthorized app kismet has been (un)installed - 4 pts
Prohibited software aircrack-ng removed - 4 pts
Prohibited software Doomsday removed - 4 pts
Catco and deo groups added - 4 pts
Groups Catco and DEO now have members added - 4 pts

Answers to Windows 10 Practice Image I (“Infinity War”)

100 out of 100 points received

Connection Status: OK

Internet Connectivity Check: N/A
Aeacus Server Connection Status: N/A

0 penalties assessed, for a loss of 0 points:

21 out of 21 scored security issues fixed, for a gain of 100 points:

Forensic Question 1 is correct - 9 pts
Forensic Question 2 is correct - 9 pts
Forensic Question 3 is correct - 9 pts
Disabled Guest Account - 2 pts
User Thanos has been Deleted/Disabled - 8 pts
User Loki has been Deleted/Disabled - 2 pts
Created new user (T'Challa) - 7 pts
AutoUpdate is enabled - 6 pts
Proper users are in Administrators group - 1 pts
Internet Explorer 11 Feature Disabled/Removed - 8 pts
IIS FTP Server Feature Disabled/Removed - 8 pts
Maximum Password Age Set Properly - 8 pts
Minimum Password Length Set Properly - 8 pts
Set Lockout Threshold Set Properly - 8 pts
Service: FTP Server Svc is Stopped with the startup type set as Disabled - 1 pts
Firewall is Turned ON (Default settings) - 1 pts
Package Google Chrome has been removed - 1 pts
Package CCleaner has been removed - 1 pts
Firefox has been Updated - 1 pts
MP3 removed - avengers.mp3 - 1 pts
MP3 removed - 47_avengers_infinity_war_original_soundtrack_mp3_ringtone_ringtone_mp3.mp3 - 1 pts