



CP-XI Practice Round Checklist and Instructions



Welcome to the CP-XI Practice Round! Teams are tasked with securing virtual machine images, which run in VMware software. Points are gained through the CyberPatriot Competition System (CCS) scoring client when a scored vulnerability is fixed. Additionally, answer keys are provided to teach teams how to find and fix vulnerabilities. Please read the checklist carefully and **completely** before your team opens the images.

Detailed instructions and troubleshooting tips follow the checklist.

Before the Round

- ☐ **ENABLE VIRTUAL TECHNOLOGY IN THE HOST COMPUTER BIOS IF IT IS DISABLED.** See Final Notes (last section).
- ☐ **ENSURE INTERNET CONNECTIVITY.** The images must connect to the Internet to report scores.
- ☐ **INSTALL THE NECESSARY SOFTWARE ON YOUR COMPUTER(S).**
 - [7-ZIP](#). Refer to the [7-Zip Installation instructions](#) for assistance.
 - [VMWARE WORKSTATION PLAYER 14.1.2 \(64-bit host\)](#). VMware Workstation Player 14.1.2 is free software that runs on 64-bit operating systems only. VMware Fusion or other versions of VMware Workstation Player may be used, but at the risk of the team with no special consideration or grounds for appeal during a scored round (during and after Round 1).
 - [WINMD5](#). Refer to the [WinMD5 Installation Instructions](#) for assistance.
- ☐ **DOWNLOAD THE IMAGES.** The images may be downloaded at the link in the [Download Virtual Machine Images](#) section.
- ☐ **VERIFY THE CHECKSUM.** The Checksums may be found in the [Download Virtual Machine Images](#) section.
- ☐ **VERIFY HOST SYSTEM TIME.** The time on your host system must be correct.

During the Round

- ☐ **UNZIP THE IMAGES.** The password to extract the images will be sent out in the accompanying email.
- ☐ **OPEN IMAGES IN VMWARE WORKSTATION PLAYER.**
- ☐ **AGREE TO THE COMPETITOR AGREEMENT AND ENTER UNIQUE IDENTIFIER.** **Your team's Unique Identifier(s) may be found on the Coach's Dashboard when you log in at www.uscyberpatriot.org. An improper or blank Unique Identifier entered in an image will result in audible and visual warnings and will flag the image to the CyberPatriot Program Office.**
- ☐ **READ THE README AND FORENSIC QUESTION FILES ON THE IMAGE DESKTOP FIRST.** This is the image scenario.
- ☐ **FIX VULNERABILITIES AND ANSWER QUESTIONS TO GAIN POINTS.**
- ☐ **CHECK YOUR PROGRESS BY SELECTING THE SCORING REPORT ICON. ALSO, CHECK THE SCORING REPORT FOR BROADCAST MESSAGES CONCERNING THE IMAGES.**
- ☐ **SHUT DOWN THE IMAGE.** Scoring and time will stop when the image is closed. You may click the CyberPatriot Stop Scoring icon or alternatively, shutdown using the procedure to close an operating system. If this does not work, please see the "Shutdown and Stop Scoring Button Issues" under the **Malfunctioning Image** section.
- ☐ **AVOID MODIFYING ORIGINAL VMWARE PLAYER IMAGE SETTINGS (e.g., MEMORY, NUMBER OF CORES, NETWORK ADAPTER SHOULD BE NAT, ETC.) BECAUSE IT MAY CAUSE IMAGE INSTABILITY.**

After the Round

- ☐ **DELETE IMAGES.** All images are the intellectual property of the Air Force Association and must be removed from computers after the Practice Round. Retaining images after the round is over is not authorized.

Detailed Round Instructions

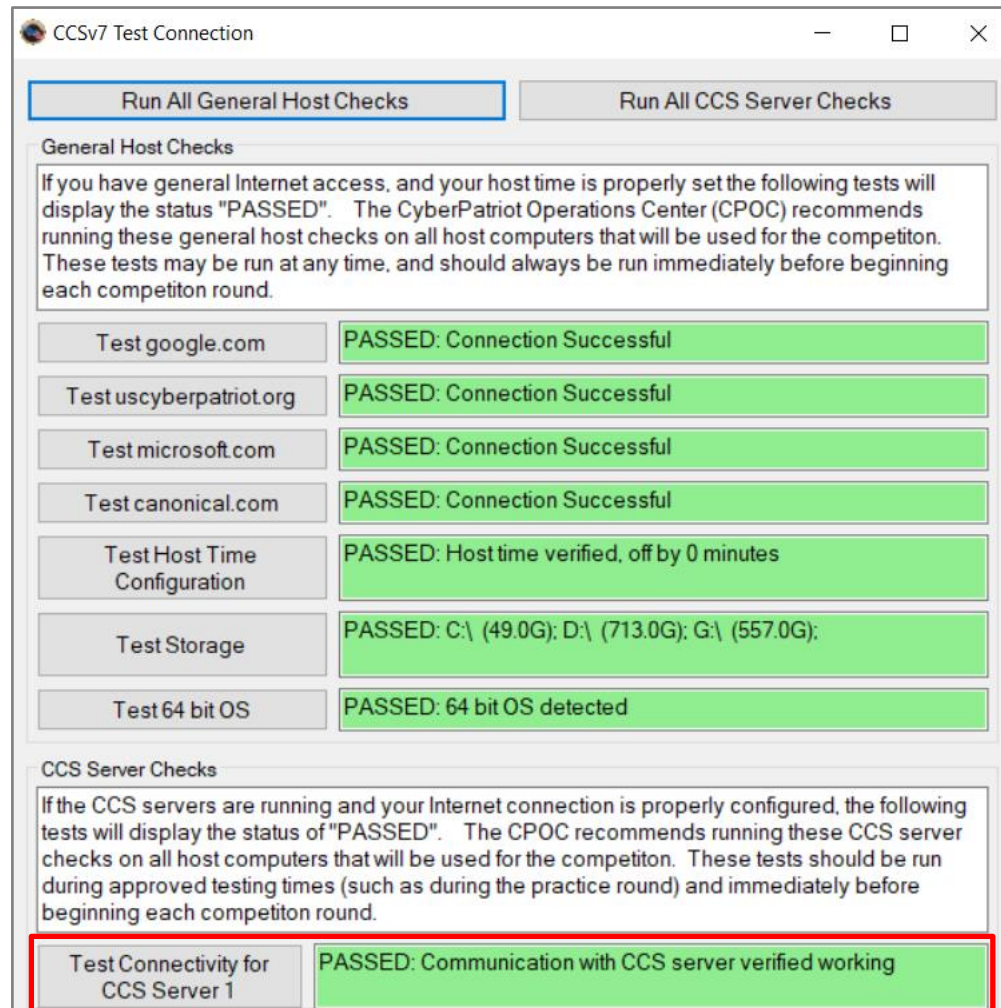
Before the Round

Ensure Internet Connectivity

Your image **MUST** connect to the CyberPatriot scoring server over port 80 during the competition. Internet connectivity is the responsibility of each team. Verify that there are no firewalls, proxy servers, or other security measures that might interfere with the connection from the CCS scoring client to the server. To ensure you can connect to the scoring server, please use the following software and guide. If you cannot remediate issues with your IT administrator, please contact the CyberPatriot Program Office.

IMPORTANT NOTE: The Practice Round is using a different Connection Test than the Training Round. **Please make sure you are downloading version 7.0.** The Connection Test Software file must be unzipped before you can run the test. **The Practice Round uses CCS Server 1.** If the connection test is green for Server 1, you should be able to participate in the round.

- [Connection Test Software](#)



Prepare Your Host System

We recommend your “host” system (your physical computer) has these specifications:

- 64-bit i3 processor of the generation “Sandy Bridge” or better OR AMD 64-bit processor of the generation “Bulldozer” or better (built in 2011 or later)
- **Virtualization Technology / Extensions (e.g., VT-x, Vx) must be ENABLED in the BIOS**
- 8 GB of RAM / 4 GB may cause performance issues that will not receive special consideration
- 40 GB of free disk space
- XGA (1024x768) or higher display / 1280x1024 recommended

Download and install this software:

1. [7-Zip](#) – This software will extract the virtual machine images after they are downloaded. The images are compressed in .zip format.
2. [VMware Workstation Player 14.1.2](#) – The images run in this software. Other virtualization software may work, but technical support is only provided for the VMware program listed above. VMware Fusion or newer versions of VMware Workstation Player or Workstation Player may be used, but at the risk of the team with no special consideration or grounds for appeal during a scored round.
3. [WinMD5](#) – This software verifies that your images were not corrupted during the download process by using a checksum. If the checksum of your downloaded image does not match the checksum provided in this document, you need to re-download that image.

Download Virtual Machine Images

Use the links below to download the images in password-protected folders. The images are large, so please download them as soon as possible.

Images

Windows 10: https://drzft7iigg5ul.cloudfront.net/cpxi_pr_se_win10.zip
Server 2016: https://drzft7iigg5ul.cloudfront.net/cpxi_pr_se_server2016.zip
Ubuntu 16: https://drzft7iigg5ul.cloudfront.net/cpxi_pr_se_ubu16.zip
Debian 8: https://drzft7iigg5ul.cloudfront.net/cpxi_pr_se_deb8.zip

Verify Image Checksum

After downloading, use WinMD5 to calculate the image checksum (Instructions [here](#)). If the checksum matches the one below, you have successfully downloaded the image. If it does not, re-download the image. If the checksum does not match after several attempts, try using a different browser, computer, or network.

Windows 10: **bd4036e5904567c2bba358b73678917**
Server 2016: **fd4c01ed7480fb593f1d76a72c4d21ee**
Ubuntu 16: **7c374b57c8ddb64cfb08c4793ca0dde**
Debian 8: **1452c73b771af3d1bd61518264ca2489**

During the Round

Unzip the Image

Use the 7-Zip software to extract each image. Please do not modify, delete, copy, or move any of the files in the folders created during extraction.

Open the Image in VMware Workstation Player

Do not open the image in VMware Workstation Player until your team(s) are ready to compete. Once an image has been extracted, launch it using VMWare Workstation Player by selecting “Open a Virtual Machine” from the main menu.

When you launch an image, you may see a pop-up asking if you moved or copied the image – always click on “**I Copied It.**” You do not need to download VMware Tools. If an image needs to be restarted, the current version must be closed and deleted and a new version may be extracted from the .zip file. **Note that the score for any newly extracted image will begin at 0.**

Competitor Agreement

Cyber ethics is a major component of the CyberPatriot program. The teams must agree to act ethically before starting work on the image. If Competitors do not check this box, which pops up when the image starts, they will be unable to compete.



CyberPatriot Competitor Agreement

While competing in CyberPatriot:

I will consider the ethical and legal implications of all of my actions. I will not conduct, nor will I condone, any actions that attack, hack, penetrate, or interfere with another team's or individual's computer system.

I will not keep or download any instances of competition images outside their specified dates of use.

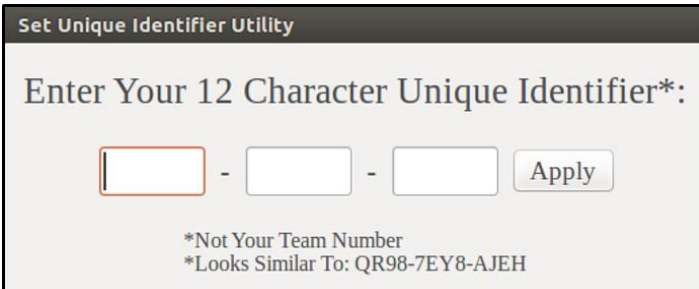
I will comply with the rules in the CyberPatriot Rules Book.

I will enter my team's Unique Identifier immediately.

☐ I Agree

Enter Your Unique Identifier

Your team(s) Unique Identifier is on the Coach's dashboard. Your Unique Identifier is 12 characters long and is NOT your team number (i.e. 11-XXXX). It must be **entered immediately** to receive scoring feedback and ensure your scores are recorded correctly. When you first start an image, a box will prompt you for your Unique Identifier. It should look like the box below. When you start the image, the desktop may be obscured, leaving only the CyberPatriot Set Unique Identifier utility.



Set Unique Identifier Utility

Enter Your 12 Character Unique Identifier*:

- -

*Not Your Team Number
*Looks Similar To: QR98-7EY8-AJEH

If the Set Unique Identifier box does not appear after the Competitors Agreement, double-click the Set Unique Identifier icon on the desktop. Click “Yes” to start the Set Unique Identifier utility, and enter your Unique Identifier. Now click Apply and OK.

If you receive a message that your Unique Identifier is invalid, verify and re-enter it. When you have entered it correctly, you will receive a message indicating that it has been saved. All participants on a team will use the team's single Unique Identifier. **An improper or blank Unique Identifier entered in an image will result in audible and visual warnings and will flag the image to the CyberPatriot Program Office.**

Read the README File on the image Desktop

The README file contains a brief description of the scenario for that image and provides a few hints to help you get started. It will also contain any account passwords necessary for the image.



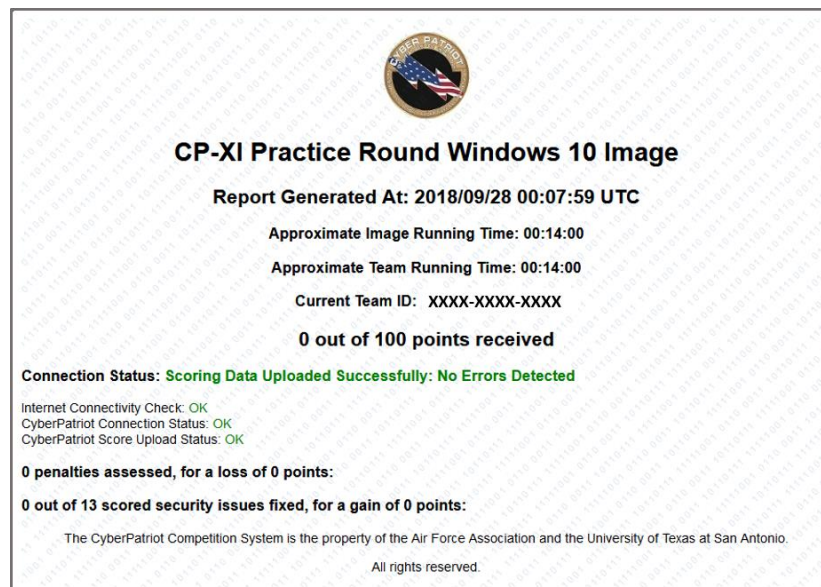
Fix Vulnerabilities and Answer Questions to Gain Points

Your team can increase its score during the round in two ways. First, you can find and fix the problems and misconfigurations on an image. While not all of the issues are scored, the README may point you in the right direction. For help with some basic vulnerabilities, visit the Training Materials on our website. These materials are designed only to be a starting point in your training.

Second, you can score points by answering questions about image problems. Questions can be answered in the “Scored Questions” or “Forensics Questions” file(s) on the desktop. Spelling your answers correctly counts!

Scoring Report

To check your score, use the “Scoring Report” shortcut on the desktop. The Scoring Report page may take up to **two minutes** to update after the first time the image is started. It will look like this:



Your Scoring Report provides information about the status of your system and your progress in fixing vulnerabilities. It will update roughly every minute. If it does not appear to refresh for a few minutes, hold down the Ctrl + R key.

At the top of the page you see the words “Report Generated At” followed by a date/time stamp. This time is expressed in Coordinated Universal Time (UTC). If this time has not changed for at least 10 minutes, refresh the page. If it still does not change, reboot your image. Tampering with the CCS Client service will stop local scoring feedback. If the local scoring client has been disrupted, stopped, or tampered with, you may see the following message:

Report Generated At: 2015/09/11 14:58:30 UTC

WARNING: CyberPatriot Scoring service may not be running

Approximate Image Running Time: 00:41:43

Rebooting your image should fix this issue. In the event the client has been removed from the image or stopped, please see the “Frozen Image” instructions under the **Malfunctioning Image** section below. If your team opens a new copy of the image, the score for the image will be reverted to **zero**.

NOTE: Javascript is required for this error message to appear correctly. To ensure that you only receive correct error messages, please do not disable Javascript.

Broadcast Message. Below Report Generated At, you see the words “**Broadcast Message Test**” in blue. (This text may be different from that in this example or nonexistent because it may be changed during rounds.) This is where the CyberPatriot Program Office can send text directly to teams’ scoring report pages concerning competition updates and changes. **READ ANY BROADCAST MESSAGES AT THE TOP OF THE SCORING REPORT PAGE.** The messages are part of the competition.

Broadcast Message Test

Approximate Image Running Time: 01:30:01

Approximate Team Running Time: 01:30:01

Current Team ID: XXXX-XXXX-XXXX

Under the **Broadcast Message Test**, you will see two times. The first of these is the “Approximate Image Running Time.” It shows how long the current instance of an image has been running since it was first started in VMware. The second time, “Approximate Team Running Time” displays how long your team has been using the image.

The next line shows the 12-character Unique Identifier for the team.

The next section of the Scoring Report deals with an image’s network connection status. If you see “No Errors Detected” after “Connection Status,” then you have no problems connecting to our server. If there is an error, then one or more of the following checks are failing. In most cases, these problems can only be fixed by talking to your IT administrator.

- **Internet Connectivity Check:** Checks an image’s ability to connect to Google. If it fails, there is a problem with the image’s connection or something on the network is blocking access.
- **CyberPatriot Scoring Server Connection Status:** Checks an image’s ability to connect to the scoring server. If it fails, you will need to troubleshoot your network connection.
- **CyberPatriot Score Upload Status:** This checks an image’s ability to upload scoring data to the scoring server. A failure is usually the result of a proxy server or other security measure.

Connection Status: **Scoring Data Uploaded Successfully: No Errors Detected**

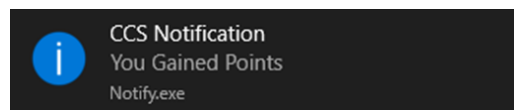
Internet Connectivity Check: **OK**
CyberPatriot Connection Status: **OK**
CyberPatriot Score Upload Status: **OK**

The next line shows how many points the team has scored. Some scored vulnerabilities are worth more points than others. Additionally, reintroducing a vulnerability that was previously fixed can result in the loss of points.

0 penalties assessed, for a loss of 0 points:

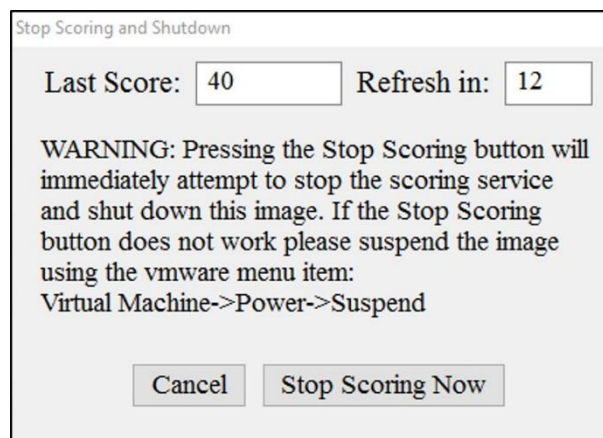
1 out of 11 scored security issues fixed, for a gain of 10 points:

The last section of the Scoring Report contains a list of scored vulnerabilities and possible penalties found in the image. This section of the scoring report will tell you how many issues are being scored for this image and notify you when an issue that is being scored has been addressed. The scoring system will also assess penalties, which can result from actions that run contrary to the scenario outlined in the README file. Points lost due to penalties can be regained by correcting whatever action caused them to be assessed. When scores change in either direction, teams will be notified with both a sound and a visual cue. These will only be played when a scoring report is generated, which is roughly every minute. The visual cue will look like this:



CyberPatriot Stop Scoring Icon

The Stop Scoring icon will attempt to stop the CCS scoring service and shutdown the image. Using this icon is **optional**, as you may also shut down the image using the procedure to close an operating system. If you use the Stop Scoring Icon, select "Yes" to allow Stop.exe to execute. You will receive a warning pop up showing your last score and a countdown to give you time to make that final determination. If you are not over the competition time, you may simply restart the image and continue to find vulnerabilities. Please be mindful of the Team Running Time to not receive a penalty for going overtime. If the icon does not work, please see the "Shutdown and Stop Scoring Button Issues" under the **Malfunctioning Image** section below. **DURING THE COMPETITION ROUNDS (ROUND 1 AND AFTER), DO NOT WAIT UNTIL THE LAST FEW MINUTES OF THE COMPETITION TO USE THE STOP SCORING ICON. FAILURE OF THE STOP SCORING ICON TO SHUT DOWN THE VIRTUAL MACHINE WILL NOT RECEIVE SPECIAL CONSIDERATION.**



NEW THIS SEASON!

New Alerts for Images

These are notifications teams may see and hear while working on an image:

You Gained Points

You Lost Points

Invalid Unique Identifier

Your Team is Approaching the Maximum Competition Time

Your Team is Over the Maximum Competition Time

Multiple Instances Detected

Malfunctioning Image

Image Will Not Open. If an image that has a correct MD5 checksum does not open, you may try the following:

1. Verify the file name at the top of the VMware Workstation Player is correct. Sometimes old images are mistaken for current images.
2. Verify that the file is not a zipped file by opening the unzipped image from the VMware Workstation Player. This is a common error.
3. **Ensure virtual extensions or Virtual Technology settings are enabled in the BIOS.** See **Final Notes**.
4. Remove and re-install the VMware Workstation Player.
5. Open the image on a different computer.

Frozen Image. If an image appears frozen, doesn't score, or otherwise does not function properly, a team has three choices:

1. Go back through your notes and reverse what may have caused the issue.
2. Stop working on the image and accept the current score.
3. Shutdown the image, remove it from the library in VMware Workstation Player as well as the unzipped copy from the folder it was in, and reboot the host computer. Then unzip a new image, open the image in VMware Workstation Player, and start with a score of zero.

Shutdown and Stop Scoring Button Issues. There are certain image security settings that will cause the **Stop Scoring Button** to malfunction. In the event your team receives an error using the **Stop Scoring Button**, please suspend the image using the following steps below:

- Click the **Player** drop-down
- Click **Power**
- Click **Suspend Guest**, then **Yes on the pop up**

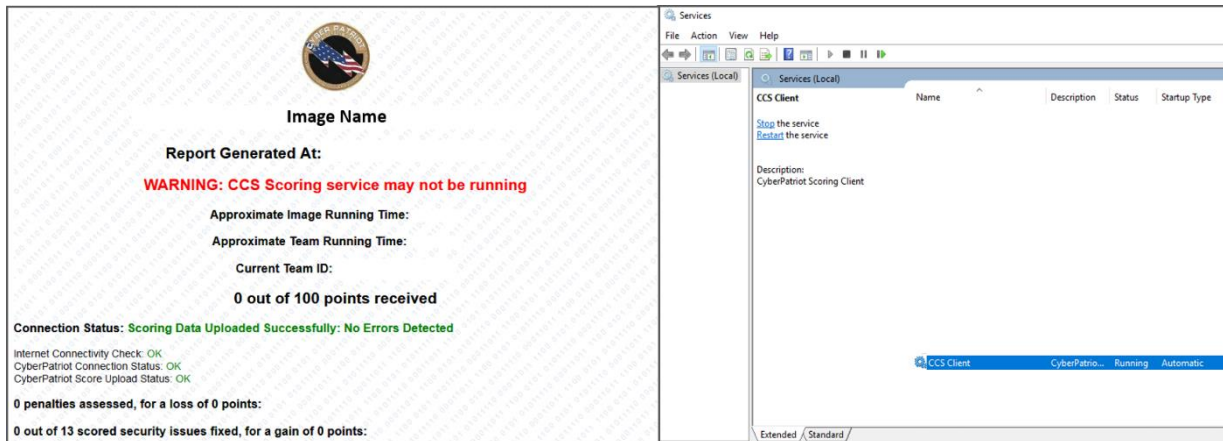
Shutdown or restart the host computer and **do not** re-open the image or you may incur an overtime penalty. Please ensure the images are deleted at the end of each round.

Points may not be awarded if they are not recorded on the CyberPatriot server.

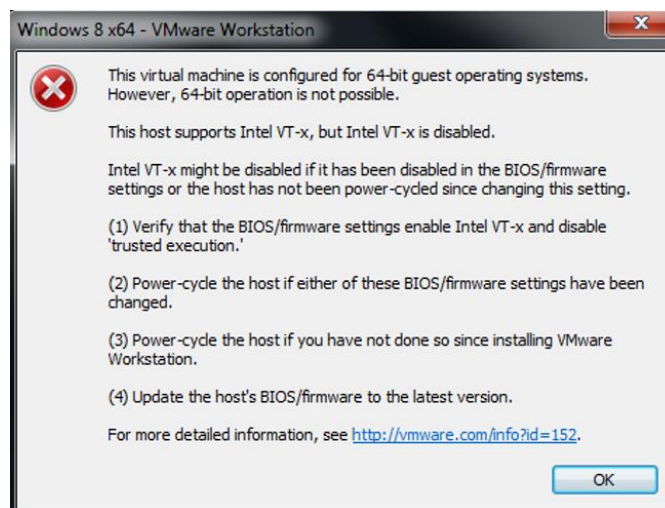
Final Notes

Warnings

- DO NOT MODIFY, DELETE, OR ALTER the "CCS Client" service or anything in the folder called "CyberPatriot." All of these files are required for the system to run properly and MUST NOT be changed. This is an example from the Scoring Report of a Windows image with the **Warning**:



- Do not copy or move any part of the scoring client off the image. Doing so may result in irreparable harm to your image.
- Teams should work only at the operating system level. Do not attempt to modify the master boot record, file system, etc. Doing so may result in your team's score being flagged or vacated.
- Your image MUST connect to the CyberPatriot scoring server to receive local scoring feedback. Internet connectivity is the responsibility of each team. If you plan to compete from a school or library, verify that there are no firewalls, proxy servers, or other security measures that might interfere with transmission of data from the CCS scoring client to the server (i.e. teams need an unrestricted internet connection on port 80).
- Enable Virtual Technology (VT, VT-x, etc.) in the Host Computer BIOS if it is disabled.** You will receive an error like the following in the VMware Workstation Player if your Virtual Technology is disabled.



To access the BIOS, you will have to check with your computer manufacturer or their website. Normally the BIOS can only be accessed in the few seconds a black or blue screen appears at the beginning of the booting or re-starting process. A note to press a key such as Esc or F1 is to enter **Setup** or the **BIOS** is normally shown at the bottom of the screen. It may take several attempts because it is a short period of time before the Windows screen appears. Please check with your computer manufacturer for the exact steps to change the BIOS. Below is a screen capture of a BIOS screen with Virtual Technology enabled.

Phoenix TrustedCore(tm) Setup Utility		
Advanced		
Advanced Processor Configuration		Item Specific Help
CPU Mismatch Detection:	[Enabled]	When enabled, a VM (Virtual Machine Monitor) can utilize the additional hardware capabilities provided by Vanderpool Technology.
Core Multi-Processing:	[Enabled]	
Processor Power Management:	[Disabled]	
Intel(R) Virtualization Technology	[Enabled]	
Execute Disable Bit:	[Enabled]	If this option is changed, a Power Off-On sequence will be applied on the next boot.
Adjacent Cache Line Prefetch:	[Disabled]	
Hardware Prefetch:	[Disabled]	
Direct Cache Access	[Disabled]	
Set Max Ext CPUID = 3	[Disabled]	
F1 Info	↑↓ Select Item	~/+ Change Values
Esc Exit	+ Select Menu	Enter Select ▶ Sub-Menu
		F9 Setup Defaults
		F10 Save and Exit