



CyberPatriot VI Practice Round Instructions

Thank you for your interest in the CyberPatriot VI Practice Round. We hope you enjoy this opportunity to get a feel for what the online competition rounds are like and to see the capabilities of the new CyberPatriot Competition System (CCS).

The information in this document will help you prepare and participate in the Practice Round. Please read it carefully and completely before your team attempts to begin the round. As always, we value your feedback. If you have comments or questions about CCS, please email them to: info@uscyberpatriot.org, subject: CCS RECOMMENDATION.

Team ID (hash). One Team ID (hash) will be issued to all registered Coaches for the Practice Round. In the Practice Round, teams may run as many instances of the images as they wish. During actual Qualification Rounds, teams shall run only one instance of a given image. Please note that the Team IDs (hashes) issued for the Practice Round WILL NOT BE USED FOR QUALIFICATION ROUNDS – new Team IDs (hashes) will be issued after the Practice Round.

Note: Team IDs (Hashes) are 10 characters and are not team numbers (e.g., 06-9564).

Scores. Practice Round scores do not count toward or affect any competition ranking or award. However, scores will be published on a near real-time scoreboard, the URL of which can be found at the end of this document. The scores are for reference only.

WARNINGS

- If you are unclear on how to prepare your host system, please refer to the checklist at the end of this document.
- Your image **MUST** connect to the CyberPatriot scoring server (over port 80) 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).
- In order for local scoring feedback to be provided, all users must enter a valid Team ID (hash). To enter a Team ID, double-click the CyberPatriot Set Team ID icon on the desktop of the image. An administrator password may be required to run CyberPatriot Set TeamID (see README.txt on desktop).

- Each virtual machine image contains a folder called “CyberPatriot” – [DO NOT OPEN, MODIFY, DELETE, or ALTER ANYTHING IN THIS FOLDER](#). Everything in this folder is *must* be there for the scoring system to function properly.
- Do not copy or move any part of the scoring client off of the virtual machine. Doing so may result in irreparable harm to your host system.
- 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.
- Virtual machine images will be running a “CyberPatriot Scoring” service. DO NOT MODIFY, STOP, REMOVE OR ALTER this service. It is legitimate and must be there for the scoring system to function properly.
- When you open an image in VMware Player, you may receive a message asking whether you moved or copied the images. Always select “I Copied It.”
- Coaches will receive the decryption password by email just before the start of the Practice Round.
- Please see the README.txt file on the desktop of the images for details on the scenario for each image, as well as the administrator password (if applicable).
- If the desktop of your Ubuntu image does not display properly, shut the image down, go to the VMware Player main menu, and select “Edit virtual machine settings.” Under the “Hardware” column, go to “Display,” and un-check the box by “Accelerate 3D graphics.” Restart the image.

Preparing Your Host System

As with previous CyberPatriot online rounds, you will secure and configure two virtual machines images (also called “images”). The images must be run using VMWare Player software which must be installed on your “host” system (the PC or laptop where you will download and run the images) before you can participate in the Practice Round. To help prepare, please make sure your host system has:

1. Enough Free Space. You will need at least 15 GB of disk space if you plan to download and run both images in this round.
2. Enough Memory. You should have at least 4 GB of memory in your host system.
3. Anx86 Compatible Processor. (2 Ghz with virtualization extensions recommended). A dual-core or better is recommended – the faster, the better.
4. Consistent and Reliable Internet Connection. Must be able to reach www.google.com and other web sites on TCP port 80.

Also, download and install:

1. 7-zip, which is free at <http://www.7-zip.org/>. This will allow you to unpack/extract the images you will download. WinZip (<http://www.winzip.com>) will also work. Also, computers running Windows 7 have built-in file compression/decompression.

2. [VMWare Player 6.0 here](#) (VMware Player 5.0 will also work). Make sure to reboot your host system after the VMWare Player software is installed.
3. **OPTIONAL:** WinMD5 from <http://www.winmd5.com>. WinMD5 allows you to verify the checksums of the image files you download to ensure that they were not corrupted during the download process. If the checksum of your downloaded image does not match the checksum provided in this document, you need to re-download that image.

Downloading Your Virtual Machine Images

Two images will be available for the Practice Round: Windows 7 and Ubuntu 12.04. Use the links below to download the images. The images will be in password-protected archives. The password to extract the images will be provided to you by email immediately before the start of the Practice Round. The image files are large, so please make every effort to have it downloaded and ready for extraction before your team is ready to participate in the Practice Round.

Windows 7 Image: http://d3e6hthsqofvwk.cloudfront.net/CyberPatriotVI_Win7.zip

Checksum: c5e4d7da4c082df1ee8e38e1a04e02cc

Ubuntu 12.04 Image: http://d3e6hthsqofvwk.cloudfront.net/CyberPatriotVI_Ubuntu_12.04.zip

Checksum: 30bc4997f54d47651888864b8675f91c

When you receive the extraction passwords (by email immediately prior to the start of the Practice Round), use a zip client to extract the images. You will be prompted to enter the password for each image when you extract them. As you extract the images, the process will create folders named according to the respective operating system. Please do not modify, delete, copy, or move any of the files in this folder. Once the images have been extracted, launch them using VMWare Player by selecting “Open a Virtual Machine” from the main menu. When you launch the images you may see a pop-up asking if you moved or copied the images – always click on “I copied it”.

The first time you start the images, the CyberPatriot Set Team ID utility should appear automatically. It should look similar to this (the first time you start the image, the desktop itself may be obscured leaving only the CyberPatriot Set Team ID utility):

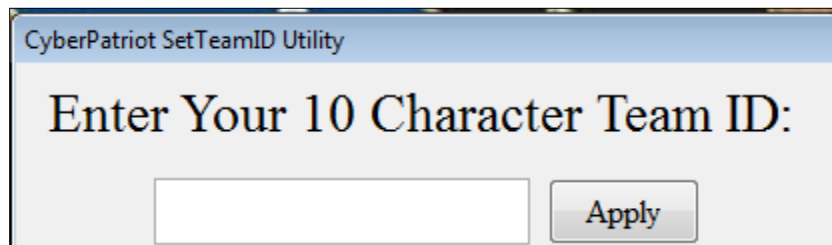


Desktop of Windows 7 virtual machine image

If the CyberPatriot Set Team ID utility does not start on its own, double-click the icon on the desktop; it looks like this:



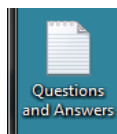
Double-clicking the Set Team ID icon will bring up a window that looks like this:



Setting your Team ID

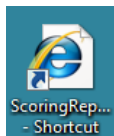
Enter your CyberPatriot VI Practice Round Team ID (hash, a ten-digit alphanumeric string) in the field and click OK. If you receive a message that you have entered an invalid Team ID, there is an error in your Team ID; verify and re-enter it. When you have entered your correct Team ID, you will receive a message indicating that your Team ID has been saved. If you fail to enter a valid Team ID, you will not receive local scoring feedback. After your Team ID is set, you should review the README.txt file on the desktop which contains a brief description of the scenario for that image, and provides a few hints to help you get started.

New for the CyberPatriot VI Practice Round, teams will be asked to provide information on their actions undertaken in the course of securing the image. On the desktop of the image, you will see a text file called “Questions and Answers.”



Open the file and follow the instructions. Providing the correct answers will earn points just as with fixing vulnerabilities. Please keep in mind that misspelling your answers may result in you not receiving points for your work. During actual Qualification Rounds, this portion of the competition will be geared more towards digital forensics.

To check your progress in fixing vulnerabilities, you can double-click on the “Scoring Report” shortcut (please note that the Scoring Report page will not be available for up to two minutes after the first time the image is started – this is normal). It will look similar to this:



This will launch your web browser and display a web page that looks something like this:



CyberPatriot Round 0 Image

Report Generated At: 2013-Sep-09 18:32:31 UTC

Approximate Running Time: 00:33:26

Current Team ID: 046A926BB3

20 out of 60 points received

Connection Status: No Errors Detected

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

0 penalties assessed, for a loss of 0 points:

2 out of 6 scored security issues fixed, for a gain of 20 points:

The CyberPatriot Competition System is the property of the Air Force Association and the University of Texas at San Antonio.
All rights reserved.

Scoring Report Example

This is your local scoring report which provides you with information about the status of your system and your progress in addressing the issues contained on that image. This page should auto-refresh roughly every two minutes, but if you notice that it has not refreshed be sure to hold down the Shift key and click on the refresh button in your web browser.

Let's examine the web page in more detail – at the top of the page you see the words “Report Generated At” followed by a date/time stamp. This indicates the time this scoring report was generated, and is expressed in Coordinated Universal Time (UTC). If you notice this time has not changed for at least 10 minutes then make sure you refresh the page. If the time still does not change, reboot your image (please note that any tampering with the CCS scoring client will likely result in termination of local scoring feedback; this can usually be resolved by rebooting the image).

Next, the Approximate Running Time displays the amount of time since the image was first started. During the Practice Round, teams can compete for as long as they like, as many times as they like. During a Qualification Round, however, teams have six hours to complete all activities for that round. As the name implies, the Approximate Running Time is just that – approximate. Teams should not base decision making on this time; rather, it is the responsibility of each team to keep track of time. The next field on the Scoring Report page displays the Team ID entered for that team.

Finally, the Scoring Report displays X out of Y points received. Vulnerabilities may be weighted, so some will earn more points than others. Keep in mind that scores are fluid in both directions – so reintroducing a vulnerability that was previously fixed can result in the loss of points.

CyberPatriot Round 0 Image
Report Generated At: 2013-Sep-09 18:32:31 UTC
Approximate Running Time: 00:33:26
Current Team ID: 046A926BB3

Top Section of Scoring Report Page

The next section of the Scoring Report deals with your image's network connection status.

Connection Status: No Errors Detected
Internet Connectivity Check: OK
CyberPatriot Connection Status: OK
CyberPatriot Score Upload Status: OK

Connection Status Information

The top field in this section gives you an overall indicator of your connection status. If you see the word “No Errors Detected” then your image is able to connect to the Internet, connect to the scoring server, and upload your score. If there is an error in any of these areas, the Scoring Page will display any available additional information (e.g. proxy interception).

- Internet Connectivity Check: This checks your image’s ability to connect Google. If your image cannot connect to Google, then something is wrong with your image’s Internet connection, or there is likely a proxy server blocking access.
- CyberPatriot Scoring Server Connection Status: This checks your image’s ability to connect to the scoring server. If your image cannot connect to the scoring server, you will need to troubleshoot your network connection.
- CyberPatriot Score Upload Status: This checks your image’s ability to upload your scoring information to the scoring server. A failure here is most commonly the result of a proxy server or other security measure.

If your image has a functional network connection you should see the word “OK” at the status for each of the above checks. Again, please note that all teams must maintain an active connection to the CyberPatriot scoring server – failure to do so will result in local scoring feedback being disabled.

The last section of the Scoring Report contains information about the issues you have addressed on the image:

<p>0 penalties assessed, for a loss of 0 points:</p> <p>2 out of 6 scored security issues fixed, for a gain of 20 points:</p>

Scored Security Issues Fixed and Penalties Assessed

Each of the images has a number of issues, misconfigurations, and problems on it. Your job is to find and fix each of those issues. Not all of the issues on the images are being scored. This section of the scoring report will tell you how many issues are being scored for this image and when you have addressed an issue that is being scored. As you address issues, the counter will increment up and the scoring report will list which issue you fixed in this section.

New for CCS 2.0 is the assessment of penalties, which can result from actions that run contrary to the scenario outlined in the README.txt file. For example, if a server image is intended to act as a web server, closing port 80 or disabling HTTP will result in the assessment of a penalty. Points lost due to penalties can be regained by correcting whatever action caused them to be assessed (in the example above, reopening port 80 or re-enabling HTTP).

Also new for CCS 2.0, is the inclusion of sounds when scores change in either direction – teams will hear one sound when scores go up and a different sound when scores go down. Sounds will only be played when a scoring report is generated, which takes place roughly every two minutes.

Technical Support

Technical support will be offered throughout the Practice Round Monday-Friday during the round from 9 a.m. to 5.p.m. EDT through an Adobe Connect session. Technical support will not be offered on Monday, October 14, as the CyberPatriot Program Office will be closed for Columbus Day. Answers to common issues can frequently be found in the chat section. If you are unable to resolve your issue even after reviewing the chat log, please post your question (make sure that “Everybody” is selected as the recipient of the chat so that other teams can benefit as well).

To visit the Practice Round Adobe Connect session, please go to afa.adobeconnect.com/cpoc

Telephone support will be offered only for teams that did not receive their Team ID at 877-885-5716. Please do not call this number for technical support during the Practice Round; instead, please visit the Adobe Connect session described above.

Online Scoreboard

We are pleased to announce that during CyberPatriot VI, scores will be published online in (near) real time by team number. Scores are first sorted by score, then by time required to reach that score. Please keep in mind that only the top 100 teams are displayed, and since teams can run multiple instances of the images during the Practice Round, team numbers may appear more than once on the list. To view the Scoreboard, please go to: <http://107.21.183.129>.

Competition Checklist

Before the start of the Round

- ARRANGE INTERNET BACK-UP PLAN.** Image must connect with Internet to report scores. Possible back-up means: Public Library, Private Residence. You may request ATT Air Cards from the CyberPatriot Program Office.
- INSTALL [WINMD5](#).** Refer to the [WinMD5 Installation instructions](#) for assistance.
- INSTALL [VMWARE PLAYER 6.0](#).** Refer to the [VMware Installation instructions](#) for assistance.
- INSTALL [7-ZIP](#) OR [WINZIP](#).** Refer to the [7-Zip Installation instructions](#) for assistance.
- DOWNLOAD THE IMAGE(S).** Refer to the Pre-Competition Email for download URLs.
- VERIFY THE CHECKSUM** of the image(s).
- VERIFY HOST SYSTEM TIME.** The time and time zone must be correct within 10 minutes on your host system. Failure to do so may result in a team's score being flagged for review.

During the Round

- READ THE INSTRUCTIONS.** (Most trouble calls are caused by competitors not reading instructions.)
- DECOMPRESS THE IMAGE(S).** Use the password(s) provided in the Start-Ex E-mail.
- READ THE README.TXT FILE.** This file contains a description of the image, and tells teams where to start. It can be found on the desktop of the image.
- OPEN THE IMAGE(S).** Refer to the [Image Opening instructions](#) for assistance. Time starts when image background is displayed in VMWare Player
- CLOSE IMAGE(S) and Secure.** Scoring and time will stop when the image is closed.

Post Competition

- DO NOT OPEN IMAGE** unless requested by the CyberPatriot Program Office. Images opened or modified after the competition period will be considered tampered images.

DELETE IMAGE(S) per instructions in the Competition E-Mails. Teams pending appeals or inquiries shall not delete the images until requested by the CyberPatriot Program Office.