



CyberPatriot V

Open Division Round 1 Instructions

The first online competition round of CyberPatriot V is almost here! The information in this document will help you prepare and participate – please read it carefully and completely before your team attempts to compete.

Teams are to run **only one** instance of the Round 1 image, a Windows 7 Enterprise workstation. The goal in Round 1 is to find and remediate as many vulnerabilities (anything that could weaken the security posture of the system) as possible in six hours. The image will have many vulnerabilities, but not all are scored. So, while you are likely to find many areas that need attention in the image, only ten of the vulnerabilities are scored.

Keep in mind that:

1. Each target 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.
2. Target 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.
3. 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.”**
4. Once you log into the image, immediately double-click the **“CyberPatriot Set Team”** icon on the desktop and enter your team hash (e.g. A1B2C3D4E).
5. Also on the desktop of the image, you will see a **README.txt** file. This file contains **valuable** information on the scenario for Round 1. Read this file carefully.
6. You may be prompted to restart the image immediately after logging in – this is normal. You can do so before or after you set your team hash, but you **MUST** do it before you start working on the image itself.
7. Coaches will receive the decryption password by email just before the start of the Competition Window they selected.
8. Coaches are responsible for ensuring that competition images are not distributed inappropriately, and are deleted once scores from the round have been published. Exceptions are teams that are the subject of appeals or inquiries. Once the Commissioner rules on their cases, the images must be deleted.

Preparing Your Host System

As with previous CyberPatriot online rounds, you will secure and configure a virtual machine called a “target”. That target must be run using VMWare’s Player software which must be installed on your “host” system (the PC or laptop where you will download and run the target) before you can participate in Round 1. 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 2 GB of memory in your host system to run a single target image. DO NOT attempt to run multiple target images at the same time if you have only 2 GB of memory.
3. An x86 compatible processor (2 Ghz with virtualization extensions recommended). A dual-core or better is recommended.
4. A consistent and reliable Internet connection that can reach www.google.com and other web sites on TCP port 80.

Also, download and install:

1. A free copy of 7-zip from <http://www.7-zip.org/>. This will allow you to unpack/extract the target images you will download. WinZip (<http://www.winzip.com>) will also work.
2. VMWare Player 5.0 from <http://www.vmware.com/products/player/>. Make sure to reboot your system after the VMWare Player software is installed.
3. **OPTIONAL:** Download and install 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 will need to re-download that image.

If you are unclear on any of the steps above, please refer to the Competition Checklist.

Downloading your target image

Use the links below to download the Round 1 image, which will be in a password-protected archive. The password to extract the image will be provided to you by email immediately before the start of Round 1. The image is a large file (3.1 GB), so please make every effort to have it downloaded and ready for extraction before you plan to compete.

Please note that there are two duplicate versions of the Round 1 image available – one for teams competing on Friday, one for teams competing on Saturday. Make sure you’ve downloaded the appropriate image for your Competition Window.

FRIDAY Windows 7 Image: <http://d3e6hthsqofvwk.cloudfront.net/FridayRound1Open.zip>

Checksum: 0c04ff0c6947969b865e7cfc18299f60

SATURDAY Windows 7 Image: <http://d3e6hthsqofvwk.cloudfront.net/SaturdayRound1Open.zip>

Checksum: 8d6cab5edbf508cf2f6680f1c9230132

Round 1 Instructions

When you are provided with the extraction password (you will receive it by email immediately prior to the start of the round), use WinZip or 7zip to extract the target image (you will be prompted to enter the password). As you extract the target images, the process will create a folder called "Round_1" followed by the target image name. Inside that folder are the files for the target image, as well as a file called "README.txt". The README file contains a brief description of the target image and provides a few hints to help you get started securing the image (this file is also provided on the desktop of the image). Please do not modify, delete, copy, or move any of the other files in this folder. Once the target image has been extracted, launch it using VMWare Player. When you launch the image you may see a pop-up asking if you moved or copied the images – always click on "I copied it". Once you have logged into the image, your target screen should look similar to this:



Desktop of Round 1 Target image

There are three items on the desktop you need to be aware of: the CyberPatriot Set Team utility, the README.txt file, and the “ScoringReport”. **Before you do anything else** – double-click on the CyberPatriot Set Team shortcut. That should produce a pop-up similar to what you see below.

A Windows-style dialog box titled "CyberPatriotSetTeam". It has a blue title bar. The main area is white and contains the text "Please enter your unique Team ID:". Below this is a text input field with the placeholder text "Put team ID here". At the bottom are two buttons: "OK" and "Cancel".

CyberPatriotSetTeam

Please enter your unique Team ID:

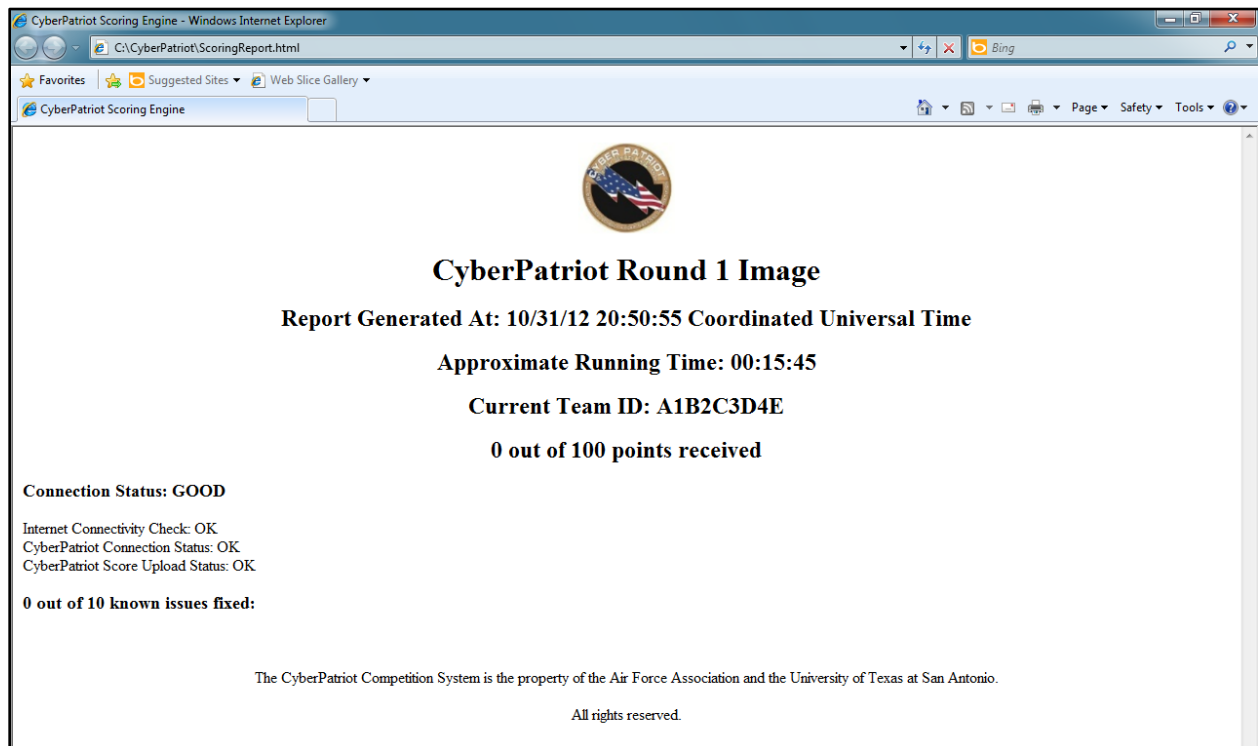
Put team ID here

OK Cancel

Setting your Team ID

Enter your CyberPatriot V team hash (e.g. A1B2C3D4E) in the field and click OK. It is **very** important that you enter your team hash correctly. Failure to do so could result in your team not receiving credit for your efforts. The pop-up will disappear when you click OK.

After your team ID is set, you should double-click on the “ScoringReport” shortcut. This will launch your web browser and display a web page that looks something like this:

A screenshot of a web browser window showing the CyberPatriot Scoring Engine interface. The browser is Internet Explorer. The address bar shows "C:\CyberPatriot\ScoringReport.html". The page has a blue header with "CyberPatriot Scoring Engine" and a search bar. The main content area is white and features a circular logo with an American flag. Below the logo, the text reads: "CyberPatriot Round 1 Image", "Report Generated At: 10/31/12 20:50:55 Coordinated Universal Time", "Approximate Running Time: 00:15:45", "Current Team ID: A1B2C3D4E", and "0 out of 100 points received". At the bottom, it says "Connection Status: GOOD", "Internet Connectivity Check: OK", "CyberPatriot Connection Status: OK", "CyberPatriot Score Upload Status: OK", "0 out of 10 known issues fixed:", and "The CyberPatriot Competition System is the property of the Air Force Association and the University of Texas at San Antonio. All rights reserved.".

CyberPatriot Scoring Engine - Windows Internet Explorer

C:\CyberPatriot\ScoringReport.html

Search

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

0 out of 10 known issues fixed:

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 and provides you with information about the status of your system and your progress in addressing the issues contained on that target image. This page should auto-refresh 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” followed by a date/time stamp. This indicates the time this scoring report was generated.

This time is generated locally by the scoring agent on your system, and is displayed by default in Coordinated Universal Time. 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 target image.

The scoring report will also display an Approximate Running Time, which is roughly how long your team has had the image open. The time displayed is not exact, and teams are responsible for not exceeding the six consecutive-hour time limit. Reliance on the Approximate Running Time is not grounds for an appeal.

Report Generated and Points Received

The second item of interest at the top of the Scoring Report is X of Y points received. This tells you how many points you've received out of the maximum possible points for this target image (there are a total of **TEN** vulnerabilities in the Round 1 image). Please note you can lose points – if you fix an issue and do something later that re-introduces that issue, the points you earned for fixing the issue are taken away. The next section of the Scoring Report deals with your target image's network connection status.

Connection Status: GOOD

Internet Connectivity Check: OK

CyberPatriot Scoring Server Connection Status: OK

CyberPatriot Score Upload Status (tells you if your score has been uploaded): OK

Connection Status Information

The top part of this section gives you an overall indicator of your connection status. If you see the word “GOOD” then your target image is able to connect to the Internet, connect to the scoring server, and upload your score. If you see the words “ERRORS DETECTED” then your target image has an issue with one of the following:

- Internet Connectivity Check: This checks your target image's ability to connect Google. If your target image cannot connect to Google then something is wrong with your target's Internet connection.
- CyberPatriot Scoring Server Connection Status: This checks your target image's ability to connect to the scoring server. If your target cannot connect to the scoring server, you will need to troubleshoot your network connection.
- CyberPatriot Score Upload Status: This checks your target image's ability to upload your scoring information to the central scoring server.

If your target image has a functional network connection you should see the word “OK” at the status for each of the above checks. If you are having connection issues, refer to the Connection Status Troubleshooting document.

The last section of the Scoring Report contains information about the issues you have addressed on the target image. Each of the target 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 targets 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 and the scoring report will list which issue you fixed in this section.

Technical Support

Telephone technical support will be offered during Round 1. Additionally, we will use Adobe Connect chat rooms to answer any questions that may arise. We are limited to 100 connections per Adobe Connect session, so if you attempt to join the “CPOC” room (primary URL below), but get an error message that the room has exceeded its connection limit, use the secondary “CPOC2” room (URL below).

CyberPatriot Operations Center: 1-877-885-5716

Primary: <http://afa.adobeconnect.com/cpoc>

Secondary: <http://afa.adobeconnect.com/cpoc2>

We encourage you to check the Adobe Connect chat rooms prior to calling into the CPOC – these rooms quickly become a valuable technical knowledge base. If you are unable to locate your team hash, or have a technical question, please call the CPOC. Please note that the CPOC **will not** answer questions related to the substance of the competition (e.g. how to fix a given vulnerability, what the vulnerabilities are, etc.). The CPOC **will only** assist with issues stemming from a failure of CCS, or some other issue beyond the team’s control. Any time-sensitive information (e.g. regarding a systemic issue) will be emailed to registered coaches from info@uscyberpatriot.org, as well as posted to the CyberPatriot website and Facebook page.