



CP-XI Windows 10 Practice Image Answer Key



Welcome to the CyberPatriot Training Round! This image will provide you with information on how to solve common vulnerabilities on a Windows 10 operating system. In doing so, it will help you on your way as you build your cybersecurity skills.

The vulnerabilities in this image are some of the most basic ones found during a CyberPatriot competition. Even if you do very well with these vulnerabilities, you will experience greater difficulty as the season progresses. To do well in each round, it is important to not only use this image and the training materials on the CyberPatriot website and the Coach, Mentor, and Team Assistant Dashboard; but to also use additional outside information on cybersecurity practices, including the expertise of your Technical Mentor(s). Also, the README file on the Desktop in this image may be more detailed than those you see during the competition. You will have to use your own knowledge, not just the hints in this file, to achieve a high score during the actual competition.

Below are the answers to the problems that exist in this image. Each one includes information on how the problem was found (if applicable), how it was solved, and why it is important from a cybersecurity standpoint. More information on these specific vulnerabilities can be found in Unit Seven and Unit Eight of the CyberPatriot XI Training Materials on the Dashboard when your Coach, Mentor, or Team Assistant signs into www.uscyberpatriot.org (not the archived Training Materials on the public side of our site). However, researching these vulnerabilities (and more advanced ones) on your own is also highly encouraged!

It is also possible to lose points during the competition. Simple penalties that may arise are noted below the answers. There are many ways to solve some of the problems below. This answer key just shows one method in each case.

Coaches will be sent categories of vulnerabilities following each online round.

Answers

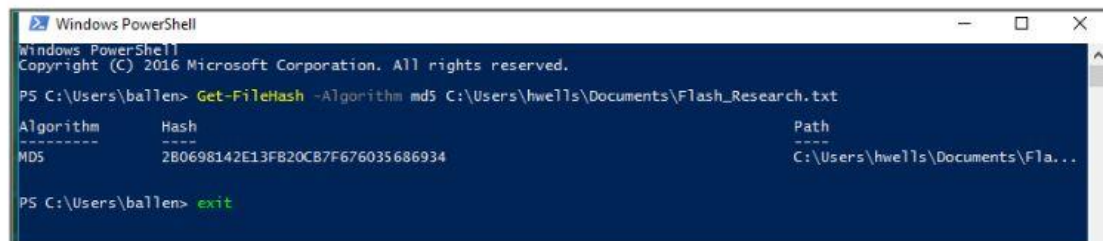
1) Forensic Question 1 Correct: 10 pts.

- How do I find this problem?

When you open an image, please read all the "Forensics Questions" thoroughly before modifying the image as you may change something that prevents you from answering the question correctly. There is a file on the Desktop here called "Forensic Question 1".

- How do I solve this problem?

This question asks you to identify the md5 hash of Dr. Wells research notes. Press the start button -> Type powershell -> Press **Enter**. In PowerShell, Type "Get-FileHash -Algorithm md5 C:\Users\hwell\Documents\FIash_Research.txt" (without quotes) -> Press **Enter**. This will generate the md5 hash for the Flash_Research.txt file. Copy and paste the hash into the "Forensic Question 1" document on the desktop. Remember to **Save** the document. To get out of PowerShell, type "exit" at the ballen prompt and press **Enter**.



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\ballen> Get-FileHash -Algorithm md5 C:\Users\hwell\Documents\FIash_Research.txt

Algorithm      Hash                                           Path
-----
MD5            2B0698142E13FB20CB7F676035686934           C:\Users\hwell\Documents\FIa...
```

PS C:\Users\ballen> exit

- Why is fixing this problem important?


It is important to know if important files, programs or folders have not been tampered with by unauthorized users. If the hash is not the same as when the user last generated it, the user can be sure that an outside force has modified the objects contents.

2) Forensic Question 2 Correct: 10 pts.

- How do I find this problem?

You should always look on the Desktop of the image to see if there are questions for you to answer about the vulnerabilities that exist. There is a file on the Desktop here called "Forensic Question 2".

- How do I solve this problem?

The question asks you to identify the owner of the Cold Research document that Leonard Snart has obtained. Open **File Explorer**, press the Windows key  (on the keyboard)+ E -> in the left-hand pane, select "This PC" -> double-click on **Local Disk (C:)** -> navigate to C:\Users\lsnart\Desktop -> right-click "Cold Research" -> select **Properties**, then the **Security** tab -> at the bottom of screen, select **Advanced**. At the top of this screen, we can see that the owner of this document is cramon.

- Why is fixing this problem important?

Even though some users may be in possession of certain documents, they may not have been their original creators. In an investigation, it is important to know all parties involved in the creation of certain content to ask the right questions to the right user.

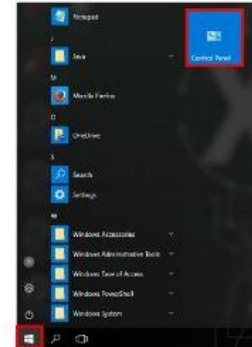
3) Former employee account has been removed: 10 pts.

- How do I find this problem?

One of the first things you should do when starting an image during a competition is check the README file on the desktop. There, you will see the authorized users for the image. These are the only users that should have an account. All others should be removed.

- How do I solve this problem?

Press the Start icon in the lower left corner of the image and double-click on **Control Panel**. Select **User Accounts** -> select **Manage another account**. In this window, you can click the users that are not listed on the authorized user list in the README file and select the option to "Delete the Account." Make sure to write down the names of any user you deleted. You may need this information later. You will then be prompted to delete or keep this user's files before you delete the account. Select **Delete Files** -> **Delete Account**.



- Why is fixing this problem important?

Computer access should be limited to just those who need to use it to complete their tasks. By leaving these user accounts on the image, invalid individuals may be able to log on to the computer and make changes that could affect the safety and security of legitimate users.

4) All user accounts are password protected: 10 pts.

- How do I find this problem?

Password protecting all user accounts is good cybersecurity practice in general.

- How do I solve this problem?

Press the Start icon and double-click on **Control Panel**. Click on "Category" next to "View by:" and change to "Small icons." Click on **User Accounts** -> **Manage another account**. Click on any of the user accounts that do not have passwords. On this page, select "Create a password." You can then create a password for that user. Make sure it's a strong, secure one! Do this for all users except CyberPatriot (so you can log back in if you don't write down the new password). This is only true for this Training image! Make sure you create or change insecure passwords in all images for CP-XI, and write down the user name and new password.

- Why is fixing this problem important?

Not having a password on an account makes it extremely vulnerable to attacks by outside individuals. Without a password, an attacker can access the user account easily. Secure passwords are highly recommended as a deterrent to potential attackers.

5) A password of at least 10 characters is required: 10 pts.

- How do I find this problem?

Enforcing use of longer passwords is a good cybersecurity practice in general.

- How do I solve this problem?

Press the Start icon and double-click on **Control Panel**. Select **System and Security** -> **Administrative Tools** -> **Local Security Policy** -> **Account Policies** -> **Password Policy** -> **Minimum password length**. In this window, you can set the number of characters for passwords to 10 or above.

- Why is fixing this problem important?

Setting a password policy ensures that all users on the system must set a secure password. By setting a password minimum length, IT administrators force users to create more secure passwords.

6) Administrator account has been changed to User: 10 pts.

- How do I find this problem?

One of the first things you should do when starting an image during a competition is check the README file on the Desktop. The README contains authorized users for the image and the account type for each user.

- How do I solve this problem?

Press the Start icon and select **Control Panel**. Click on **User Accounts -> Manage another account**. Find the users that have an Administrator account who is listed only as a Standard user in the README file. Select **Change the account type** -> select **Standard User** -> select **Change Account Type**.



Make sure to write down the names of the users you make changes to or delete. You may need this information later.

- Why is fixing this problem important?

Ensuring account types are set correctly is very important. A Standard user given administrative permissions can accidentally or purposefully cause significant damage to a system because they would have unrestricted full read and write access to all files on the system, not just their own.

7) Disable FTP service: 10 pts.

- How do I find this problem?

Disabling insecure or unnecessary services is a good cybersecurity practice in general.

- How do I solve this problem?

Press the Start icon and double-click on **Control Panel**. Select **Programs** -> select **Programs and Features** -> in the left-hand pane, select **Turn Windows features on or off** -> expand **Internet Information Services** -> uncheck **FTP Server** -> select **OK** -> at the Windows Features prompt, select **Restart now**.

- Why is fixing this problem important?


Disabling services that transport data insecurely, such as FTP, helps prevent files from being sent over the network in cleartext. Sending data over in cleartext means anyone who is listening on the network can steal unencrypted data without the user's knowledge.

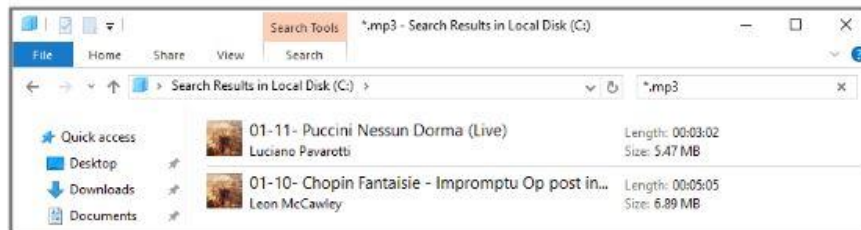
8) Prohibited MP3 files have been removed: 10 pts.

- How do I find this problem?

The README file notes that all media files are prohibited on this image.

- How do I solve this problem?

Open File Explorer or press the Windows Key  (on the keyboard) + E. Double-click **This PC** -> **Local Disk (C:)** and search for "*.mp3" (without quotes) in the top right box. All the files that have a ".mp3" file extension are music files. Select "Puccini Nessun Dorma" and "Chopin Fantaisie" -> right-click on one of the highlighted songs -> Select **Delete**.



- Why is fixing this problem important?

Keeping music on the computer is a violation of the company's policies as mentioned in the README file.

9) Enforce a password history policy: 10 pts.

- How do I find this problem?

Enforcing a password history policy is a good cyber security practice that administrators should implement.

- How do I solve this problem?

Press the Windows key  + R -> type "secpol.msc" -> **OK** -> select **Account Policies** -> select **Password Policy** -> double-click on **Enforce password history** -> type "10" in the password remembered text box, and select **OK**.

- Why is fixing this problem important?

It is important to enforce a password history policy, so users won't reuse the same passwords again. Reusing a password gives the malicious user more time to obtain the users password via a brute force method.

10) Set a maximum password age policy: 10 pts.

- How do I find this problem?

Enforcing a maximum password age policy is a good cyber security practice that administrators should implement.

- How do I solve this problem?

Press the Windows key + R -> type "secpol.msc" -> expand **Account Policies** -> select **Password Policy** -> double-click **Maximum password age** -> type "90" in the password remembered text box -> select **OK**.

Penalties

1) Required software has been removed: -5 pts. each

- Why is this a penalty?

The README file notes that Firefox is a required software.

2) Account lockout threshold is less than 5: -10 pts.

- Why is this a penalty?

Setting the account lockout threshold is an important security precaution to prevent brute force password cracking. The threshold should be set between 5 and 50 failed logon attempts. A threshold of under 5 is too few and may result in valid users accidentally locking themselves out of the system.

3) Valid users have been deleted: -10 pts.

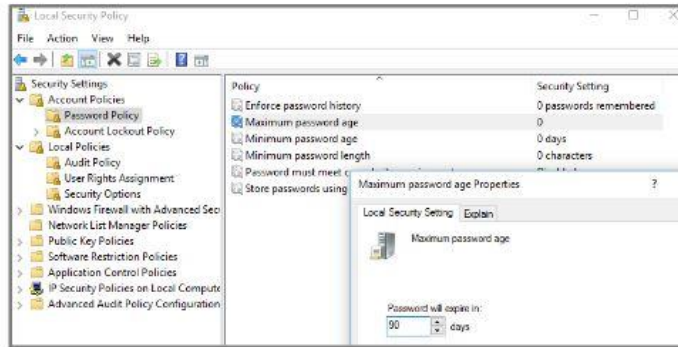
- Why is this a penalty?

The README file notes the list of valid users for this machine. By removing valid user accounts from the image, you are making it impossible for them to access this computer and do their jobs.

4) Valid user directories have been deleted: -10 pts.

- Why is this a penalty?

The README file notes the list of valid users for this machine. By removing valid user directories from the image, you are removing important files and folders that these individuals need to complete their duties.



- Why is fixing this problem important?

It is important to set a maximum password age policy because the system will require the user to change their passwords when the set time has been met. As there is much work to be done throughout the day, the user may forget to change their passwords periodically. It is good practice to have the user change their passwords in case a malicious agent is trying to brute force their way into the system.

Penalties

1) Required software has been removed: -5 pts. each

- Why is this a penalty?

The README file notes that Firefox is a required software.

2) Account lockout threshold is less than 5: -10 pts.

- Why is this a penalty?

Setting the account lockout threshold is an important security precaution to prevent brute force password cracking. The threshold should be set between 5 and 50 failed logon attempts. A threshold of under 5 is too few and may result in valid users accidentally locking themselves out of the system.