



## CP-XI Windows Server 2016 Training 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 Server 2016 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 score 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 are being scored 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](http://www.uscyberpatriot.org) (not the archived Training Materials on the public side of the CyberPatriot 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) Forensics Question 1 Correct: 6 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 "Forensics Question 1."

- How do I solve this problem?

This question asks you to identify the users in the "Remote Desktop Users" group. To do this, first click the **Search** icon (magnifying glass in the lower left corner), type "mmc," and then double-click on **mmc** (Microsoft Management Console), select **Yes**.



From the mmc window, select **File**, and in the drop-down menu select **Add/Remove Snap-in**. In the “Available snap-ins” column, select **Local Users and Groups** and then click the **Add** button. At the “Choose Target Machine” dialog box, select **Finish**, then click **OK**. From the mmc window, double-click on the new **Local Users and Groups** snap-in you just added. Then double-click on the **Groups** folder and double-click **Remote Desktop Users**. This will show you a list of users who are members of this group. The users are cramon and csnow. When you exit MMC, you might be asked if you want to save the console settings. Select “Yes,” and name the console file.

Now that you know the members of this group, enter the answers in the “Forensics Question 1” document on the desktop one user per line. Remember to save the document by selecting **File**, **Save**.

- Why is fixing this problem important?


It is important to understand how to view and edit user group settings. All users in a user group have the same security rights, so having them in the wrong groups could create potential security issues by allowing a user access to files or software he or she should not have.

## 2) Forensics Question 2 Correct: 6 pts.

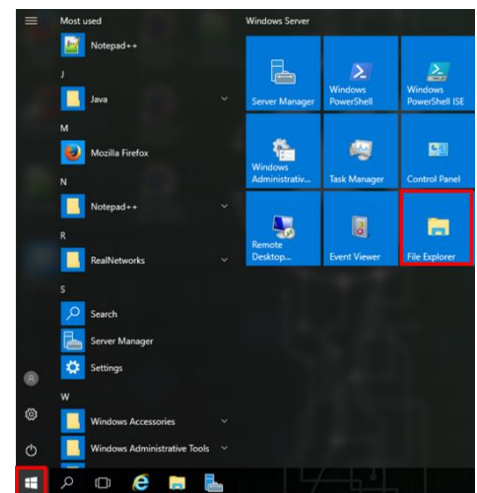
- How do I find this problem?

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 “Forensics Question 2.”

- How do I solve this problem?

This question asks you to locate password.txt file. First, press the Start icon  and double-click on **File Explorer**. Select **Local Disk (C:)** in the left-hand pane. In the search bar, type “password.txt” and press **Enter**. Right-click on password.txt file and select **Open file location**. This will open the file location of the password.txt file. Click inside the directory bar to see the full path to the password.txt file. Copy the path “C:\Users\hzolomon\Desktop\”.

Now that you located the password.txt file, enter the answer “C:\Users\hzoloman\Desktop\password.txt” (follow the Example) in the “Forensics Question 2” document on the desktop. Remember to **Save** the file.



- Why is fixing this problem important?

It is important to understand how to search for files in a Windows environment. Try using wildcards such as the \* in the search bar i.e. \*.mp3. \*.mp3 will search your entire filesystem for anything that has the extension mp3.

## 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 and select **Control Panel**. Select **User Accounts** --> and **Manage another account**. In this window, you can click the users that are not listed on the valid 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 their account. Select **Delete Files**.

- 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) New employee account has been created: 10 pts.

- How do I find this problem?

The README file contains important information that will allow you to be successful securing the image.

- How do I solve this problem?

You can create a user by going through the same steps in #1 to get into MMC. Under **Local Users and Groups**, select **Users**. Select **Action -> New User ...** -> type in the User name "rdibney" -> type in a secure password (with at least 10 characters), and confirm the password. Make sure the box is checked for the password to be changed on next logon -> select **Create** -> select **Close** -> look for the new user rdibney.

- Why is fixing this problem important?

As a System Administrator, you need to know how to add authorized users and make sure they follow the security policies of the company (strong passwords with at least 10 characters).

#### 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 select **Control Panel**. Click **Administrative Tools** --> **Local Security Policy** --> **Account Policies** --> **Password Policy** --> **Minimum password length**. In this window, you can set the number of characters required in a user password to at least 10 characters. Always remember to write down any changes you make to passwords.

- Why is fixing this problem important?

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

#### 6) 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 select **Control Panel**. 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 ballen (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.

## 7) RealPlayer program has been removed: 10 pts.

- How do I find this problem?

The README file notes that only software for basic office tasks should be on this image. RealPlayer is a media playing software that does not meet these requirements, and therefore should be removed.

- How do I solve this problem?

Press the Start icon and select **Control Panel** -> select **Programs and Features** -> right-Click **RealPlayer** -> select **Uninstall** -> Ensure both RealPlayer and Library are both selected -> select **OK** -> uninstallation of RealPlayer prompt, select **Yes** -> uninstaller Shell executable prompt, select **Close** program.

To finish removing RealPlayer from the user's computer, press the Start button -> select **File Explorer** -> in the left-hand pane, double-click the **Local Disk (C:)** -> open the **Program Files (x86)** folder -> delete the folder called **Real**.

- Why is fixing this problem important?

This software is a violation of the company's security policies. Unknown programs on a computer could contain malware or allow outside individuals access to the computer. It is important to keep only well-known software that is used for a necessary purpose on your computer.

## 8) Remove unnecessary file sharing: 10 pts.

- How do I find this problem?

To find active shares, the user has to open up the Computer Management screen and navigate to the "Shared Folders" directory.

- How do I solve this problem?

Select the Search icon (magnifying glass in lower left corner) -> Type "Computer Management" and press **Enter** -> select **Shared Folders** -> select **Shares** -> right-click the "C" share (**not C\$**) -> select **Stop Sharing** -> Shared Folders prompt, select **Yes**. This should remove the C drive from being shared with anyone on the network.

- Why is fixing this problem important?


Removing unnecessary shares can prevent unauthorized access to sensitive data. Unused shares are sometimes forgotten and could pose a security risk if a malicious user connects to this share.

#### 9) Require Ctrl + Alt + Del at login: 20 pts.

- How do I find this problem?

Enabling this feature is a good security practice in general.

- How do I solve this problem?

Press the Windows key  + R at the same time to open the run program and type in the text field "secpol.msc". Select **Local Policies** -> **Security Options** -> double-click on **Interactive logon: Do not require CTRL + ALT + DEL**. Change the setting from Enabled to **Disabled** -> select **OK**.

- Why is fixing this problem important?

When the user presses Ctrl + Alt + Del and a login screen is shown, this will indicate it is an authentic login screen and not a malicious program trying to obtain the user's credentials. You can get more information about a policy by selecting the **Explain** tab.

### Penalties

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

- Why is this a penalty?

The README file notes that Notepad++ and Firefox are required software.

#### 2) Valid users have been deleted: -5 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.

#### 3) Remote Desktop is disabled: -5 pts.

- Why is this a penalty?

The README specified that this was a critical service and that some users need to work remotely.

#### 4) 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.