CyberPatriot Windows 10 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 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. 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.

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: 8 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 named "Forensics Question 1".

- How do I solve this problem?

  This question asks for you to decode a message sent by miroh to gazula.

  The message is found in **C:\Users\Public\Public Downloads\thisisaffinecode.txt** and is encrypted using the Affine cipher with a=1 and b=3. To find the file, double click on the **This PC** icon on the Desktop and navigate to the file.

  You may use an online decryption tool such as CyberChef to decrypt the message. The answer is “Next Generation Cyber Warrior” (without quotes). Remember to **Save** and close the file.

- Why is fixing this problem important?

  Computer forensics investigations often require the examiners to locate information within files and folders that may provide relevant evidence in a case. This encoded message is an introduction to a simple technique an adversary might use to evade being discovered.

2) Forensics Question 2 Correct: 8 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 named "Forensics Question 2".

- How do I solve this problem?

  Adding multiple layers of security such as Multi-Factor Authentication (MFA) is critical in reducing risk to your business. This question asks you to find one of the three MFA requirements not listed:
  - something you know (PIN or password)
  - something you have (smart card or security key)

  ANSWER: something you are

- Why is fixing this problem important?

  Modern cyber threats require greater security beyond complex passwords. Multi-Factor Authentication should be enforced for all sensitive accounts and infrastructure. Remember to stay up to date on CISA.gov alerts, NIST.gov guidance, and perform data backups frequently.

3) Removed unauthorized user rsozin: 3 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 authorized administrators and users listed in the README are the only users that should exist on the system (aside from legitimate built-in system accounts and those used for services). All unauthorized user accounts should be removed.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **lusrmgr.msc** and press **Enter** to open the Local Users and Groups manager. Click **Users** on the left side of the window. Right click on **rsozin** and select **Delete**. In the resulting dialog box click Yes to confirm that you want to delete the user.

- 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 unauthorized user accounts on the image, unauthorized individuals may be able to log on to the computer and make changes that could affect the safety and security of legitimate users. Unauthorized user accounts also give adversaries a greater attack surface. For example, unauthorized user accounts increase the risk of having a user account compromised via password cracking.

4) Removed unauthorized user mozai: 3 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 authorized administrators and users listed in the README are the only users that should exist on the system (aside from legitimate built-in system accounts and those used for services). All unauthorized user accounts should be removed.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **lusrmgr.msc** and press **Enter** to open the Local Users and Groups manager. Click **Users** on the left side of the window. Right click on **mozai** and select **Delete**. In the resulting dialog box click Yes to confirm that you want to delete the user.

- 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 unauthorized user accounts on the image, unauthorized individuals may be able to log on to the computer and make changes that could affect the safety and security of legitimate users. Unauthorized user accounts also give adversaries a greater attack surface. For example, unauthorized user accounts increase the risk of having a user account compromised via password cracking.

5) User jsokka is not an administrator: 3 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 authorized administrators listed in the README are the only users that are authorized have administrator level access. All users not in the list of authorized administrators should have their administrator level access removed.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **lusrmgr.msc** and press **Enter** to open the Local Users and Groups manager. Click **Groups** on the left side of the window. Double-click on **Administrators** to open a Properties window. Select **jsokka** and click **Remove**, then click OK to apply the changes and close the Properties window.

- Why is fixing this problem important?

  Administrator level access gives individuals the ability to modify critical system files and functions and should be limited to authorized individuals only. The more users with administrator level access, the higher your risk, since compromising an account with administrator level access gives an adversary complete control of the system.

6) User jzhao is not an administrator: 3 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 authorized administrators listed in the README are the only users that are authorized have administrator level access. All users not in the list of authorized administrators should have their administrator level access removed.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **lusrmgr.msc** and press **Enter** to open the Local Users and Groups manager. Click **Groups** on the left side of the window. Double-click on **Administrators** to open a Properties window. Select **jzhao** and click **Remove**, then click OK to apply the changes and close the Properties window.

- Why is fixing this problem important?

  Administrator level access gives individuals the ability to modify critical system files and functions and should be limited to authorized individuals only. The more users with administrator level access, the higher your risk, since compromising an account with administrator level access gives an adversary complete control of the system.

7) User abumi has a password: 3 pts.

- How do I find this problem?

  Every user account on the system should have a password for the system to be secure. It is important to review each account and check that the accounts have passwords. In the Control Panel, the option Manage Accounts shows information and the settings for each account. Accounts that have passwords show the option to “Change the password” while accounts with no passwords show the option to “Create a password”.

  How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **Control Panel** and press **Enter** to open the Control Panel. In the Control Panel, click **User Accounts**, then click **Manage another account.** Find the user account named dzuko, double click it, and click **Create a password.** Then choose a secure password and type it into the **New password** and **Confirm new password** text boxes. Then click **Create password**.

- Why is fixing this problem important?

  Not having a password on an account will allow an adversary with physical access to the machine to log in without a password. In some cases, this can also allow an adversary to log in over the network.

8) Created user account pakku: 3 pts.

- How do I find this problem?

  The README requests that you create a new user account for a new employee.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **lusrmgr.msc** and press **Enter** to open the Local Users and Groups manager. Click **Users** on the left side of the window. Under **Action** in the top left corner, select **New User…** Enter **pakku** for the User name and Full name, and give the user a secure password of your choice. Click **Create** then **Close**.

- Why is fixing this problem important?

  One important aspect of working as a security or IT professional is supporting business operations and knowing how to do administrative tasks when requested. Additionally, knowing how system administration tasks are performed and the consequences of those actions is important as a security professional, because you must know in detail how an operating system works before you can defend it.

9) TWO CHECKS: Created group hypersonic and Added users to group hypersonic: 4 pts each.

- How do I find this problem?

  The README requests that you create a new group with several members.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **lusrmgr.msc** and press **Enter** to open the Local Users and Groups manager. Click **Groups** on the left side of the window. Under **Action** in the top left corner, select **New Group…** Enter **hypersonic** for the Group name. Click add and enter all usernames separated by semicolons. Click **OK**, **Create**, and then **Close**.

- Why is fixing this problem important?

  One important aspect of working as a security or IT professional is supporting business operations and knowing how to do administrative tasks when requested. Additionally, knowing how system administration tasks are performed and the consequences of those actions is important as a security professional, because you must know in detail how an operating system works before you can defend it.

10) User jsuki password expires: 3 pts.

- How do I find this problem?

  You may find the properties of each user account in **lusrmgr.msc**.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **lusrmgr.msc** and press **Enter** to open the Local Users and Groups manager. Click **Users** on the left side of the window. Rightclick on **jsuki** and select **Properties**. Uncheck the box for **Password never expires** and check the box for **User must change password at next logon**. Select **Apply** and **OK**.

- Why is fixing this problem important?

  One important aspect of working as a security or IT professional is supporting business operations and

  knowing how to do administrative tasks when requested. Additionally, knowing how system administration tasks are performed, and the consequences of those actions is important as a security professional, because you must know in detail how an operating system works before you can defend it.

11) A secure minimum password length is required: 4 pts.

- How do I find this problem?

  Enforcing industry recommended password policies is good cybersecurity practice.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **secpol.msc** and press **Enter** to open the Local Security Policy. Navigate to **Security Settings ➔ Account Policies ➔ Password Policy**. Double click on **minimum password length**. Set the password to **10 characters or more** and click **OK**.

- Why is fixing this problem important?

  Setting a minimum password length limits your risk of having a password compromised and can help mitigate the damage if a password is compromised. When an adversary obtains password hashes or performs a brute force attack, they can obtain your password given enough time. Changing your passwords regularly can limit the risk of an adversary obtaining your password.

12) A secure lockout threshold exists: 4 pts.

- How do I find this problem?

  Enforcing industry recommended account lockout policies is good cybersecurity practice.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **secpol.msc** and press **Enter** to open the Local Security Policy. Navigate to **Security Settings ➔ Account Policies ➔ Account Lockout Policy**. Double click on **Account lockout threshold**. Set the account lockout threshold to **10 invalid logon attempts** and click **OK**.

- Why is fixing this problem important?

  Setting secure account lockout policies limits your risk of having a password compromised. When an adversary performs a brute force attack this will stop or slow down their attack, greatly increasing the time required to compromise a user account.

13) Audit Credential Validation [Failure]: 4 pts.

- How do I find this problem?

  Enforcing industry recommended security policy is good cybersecurity practice.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **secpol.msc** and press

  Enter to open the Local Security Policy. Navigate to **Security Settings ➔ Local Policies ➔ Advanced Audit Policy Configuration ➔ System Audit Policies – Local Group Policy Object**. Select **Account Logon** and double click on **Audit Credential Validation**. Check the **Configure the following audit events** box and select **Failure**. Click **OK**.

- Why is fixing this problem important?

  Audit credential validation verifies if the operating system produces an audit event based on credentials that are either successfully or unsuccessfully used in an account logon request. Auditing for failed authentication attempts can be very useful in tracking account compromise events and attacks on systems.

14) Do not allow anonymous enumeration of SAM accounts [enabled]: 4 pts.

- How do I find this problem?

  Enforcing industry recommended security policy is good cybersecurity practice.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **secpol.msc** and press **Enter** to open the Local Security Policy. Navigate to **Security Settings ➔ Local Policies ➔ Security Options**. Double click on **Network access: Do not allow anonymous enumeration of SAM accounts**. Set the setting to **Enabled** and click **OK**.

- Why is fixing this problem important?

  This security option restricts additional permissions granted for anonymous connections to this machine. When this setting is enabled, anonymous users may not list account names which could then be used for social engineering attacks or password guessing.

15) Users may not change the system time: 4 pts.

- How do I find this problem?

  Enforcing industry recommended security policy is good cybersecurity practice.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **secpol.msc** and press **Enter** to open the Local Security Policy. Navigate to **Security Settings ➔ Local Policies ➔ User Rights Assignment**. Double click on **Change the system time**. Select **the Users group** and click **Remove**. Click **OK**.

- Why is fixing this problem important?

  Preventing users from changing the system time is important because the system clock is tied to security, logging, and application functionality. Allowing users to change system time can disrupt authentication, bypass expiration controls, tamper with logs, and break time-sensitive software. Time should only be changeable by trusted admins.

16) Firewall protection has been enabled: 3 pts.

- How do I find this problem?

  Enabling a host-based firewall is very important to system security. Windows Defender Firewall is a standard utility that comes installed on all modern Windows operating systems.

- How do I solve this problem?

  Type Windows Security into the search bar and open the program. Click "Turn On" under **Firewall & network protection** to enable the Windows Defender Firewall.

- Why is fixing this problem important?

  Enabling and properly configuring a firewall is critical to ensuring that you are only allowing known, authorized traffic in and out of your computer.

17) Remote Assistance connections have been disabled: 5 pts.

- How do I find this problem?

  Disabling unnecessary features, especially those allowing remote connections to your computer is an import cyber security principle.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **Control Panel** and press **Enter** to open the Control Panel. Click on **System**. Click **Remote settings** on the left side of the System window. Uncheck **Allow Remote Assistance connections to this computer**. Click **OK**.

- Why is fixing this problem important?

  Remote Assistance is intended to let someone trusted control the computer. However, an adversary may find a way to abuse this feature through technical means or social engineering. Unnecessary services and features, especially those that communicate on the network should be disabled to reduce your risk.

18) The majority of Windows updates are installed: 6 pts.

- How do I find this problem?

  Updating your operating system is an important principle of good cybersecurity.

- How do I solve this problem?

  Open the Settings  application found on the left side of the Start Menu. Scroll down and click on **Update & Security**. Scroll down and click on **Download**. Windows updates can take a while to download and install. You do not need to leave the window open, updates will be downloaded and installed in the background. **Please note that you may be required to restart the system and install more updates to ensure that you have the majority installed.*

- Why is fixing this problem important?

  When security vulnerabilities are found in software, the software vendor publishes updates that patch the security vulnerabilities. Adversaries can more easily compromise your system if software is present that has known security vulnerabilities. Ensuring software is up-to-date removes known security vulnerabilities.

19) Firefox has been updated: 5 pts.

- How do I find this problem?

  Updating installed applications and services to fix security vulnerabilities is an important principle of good cybersecurity.

- How do I solve this problem?

  Open Firefox and click the hamburger menu button near upper right corner of the Firefox window. Click on the **Help Menu** ➔ **About Firefox**, then click **Check for updates**, then click on **Update to _**. Click on **Restart to Update Firefox**. *Be sure to check for and install updates again when finished*.

- Why is fixing this problem important?

  When security vulnerabilities are found in software, the software vendor publishes updates that patch the security vulnerabilities. Adversaries can more easily compromise your system if software is present that has known security vulnerabilities. Ensuring software is up-to-date removes known security vulnerabilities.

20) Removed Prohibited Affine Encrypted Text File: 4 pts.

- How do I find this problem?

  This file relates to Forensics Question 1 on the Desktop. During the competition, it is important to look for files on the image that can give you clues to the Forensics Questions or files that should be deleted following the scenario in the README file. Always try to answer the Forensics Questions first **before** you delete files or make changes to the image.

- How do I solve this problem?

  Double click on the **This PC** icon on the Desktop and navigate to the file in **C:\Users\Public\Public Downloads\thisisaffinecode.txt**. **Delete** the file.

- Why is fixing this problem important?

  Unauthorized files and programs may leak confidential information, interfere with business-critical software and services, contain various malware, contain security vulnerabilities, or could introduce unwanted legal and regulatory issues.

21) Removed Wireshark: 4 pts.

- How do I find this problem?

  Removing unauthorized and potentially unwanted programs from a computer is an important

  cybersecurity principle. Third party software installed on the system should be limited to the software listed in the README, and software required for normal operation of the operating system, and services and software listed in the README.

- How do I solve this problem?

  Press the Windows  key + R to open the Run dialog. In the Run dialog type **Control Panel** and press **Enter** to open the Control Panel. In the Control panel click **Programs and Features**. Click **Wireshark**, then click **Uninstall**. Follow the prompts to ensure that Wireshark is completely uninstalled.

- Why is fixing this problem important?

  Removing unauthorized software from your system is important for limiting your risk and reducing your attack surface. Unauthorized programs may leak confidential information, interfere with business critical software and services, contain various malware, contain security vulnerabilities, or could introduce unwanted legal and regulatory issues.

22) Removed NetStumbler: 4 pts.

- How do I find this problem?

  Removing unauthorized and potentially unwanted programs from a computer is an important cybersecurity principle. Third party software installed on the system should be limited to the software

listed in the README, and software required for normal operation of the operating system, and services and software listed in the README.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **Control Panel** and press **Enter** to open the Control Panel. In the Control panel click **Programs**, then click **Programs and Features**. Click **Network Stumbler 0.4.0 (remove only)**, then click **Uninstall/change**. Follow the prompts to ensure that NetStumbler is completely uninstalled.

- Why is fixing this problem important?

  Removing unauthorized software from your system is important for limiting your risk and reducing your attack surface. Unauthorized programs may leak confidential information, interfere with businesscritical software and services, contain various malware, contain security vulnerabilities, or could introduce unwanted legal and regulatory issues.

23) Removed PC Cleaner: 4 pts.

- How do I find this problem?

  Removing unauthorized and potentially unwanted programs from a computer is an important cybersecurity principle. Third party software installed on the system should be limited to the software and services listed in the README, and software required for normal operation of the operating system.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **Control Panel** and press **Enter** to open the Control Panel. In the Control panel click **Programs**, then click **Programs and Features.** Click **PC Cleaner v9.0.0.9**, then click **Uninstall.** Follow the prompts to ensure that PCCleaner is completely uninstalled.

- Why is fixing this problem important?

  Removing unauthorized software from your system is important for limiting your risk and reducing your attack surface. Unauthorized programs may leak confidential information, interfere with businesscritical software and services, contain various malware, contain security vulnerabilities, or could introduce unwanted legal and regulatory issues.

Penalties

1) Account lockout policy less than 5 is deprecated: -3 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 their accounts, or adversaries easily being able to perform a denial-of-service attack and locking users out of their accounts.

2) Firefox is not installed at the default location: -5 pts.

- Why is this a penalty?

  The README states that Firefox is required software.

3) Inkscape is not installed at the default location: -5 pts.

- Why is this a penalty?

  The README states that Inkscape is required software.

4) GIMP is not installed at the default location: -5 pts.

- Why is this a penalty?

  The README states that GIMP is required software.