# CP-XV Exhibition Round Windows 10
# Image Answer Key

Welcome to the CyberPatriot Exhibition 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 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. However, not all vulnerabilities found on the image are scored vulnerabilities. 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.

## 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 called "Forensics Question 1”.

- How do I solve this problem?
  Calculators are available to convert to and from Base64. Find a reputable calculator such as the one on https://www.base64decode.org/ . Enter the Base64 code from the forensics question file and select decide to decode the message.

- Why is fixing this problem important?
  Base64 encoding is used to send text safely so that the message does not get corrupted before reaching its destination. If the sender uses Base64 to encode

the message, you will need to convert from Base64 to ASCII (code used for regular test) to view the message from the sender.

**2) Forensics Question 2 Correct: 8pts.**

- 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?
  The question asks for the full computer name of your image PC. In the search box, type “name”, and select “View your PC name”. A window will appear that displays the full computer name next to “PC Name”.

- Why is fixing this problem important?
  Computer names are used to identify individual computers on an organization’s network. This is important to know when you are making any changes on a network or asking for assistance with technical issues on your PC.

**3) Forensics Question 3 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 called "Forensics Question 3”.

- How do I solve this problem?
  This question asks you to research the Windows Elevation of Privilege vulnerability identified in CVE-2022-24530 and find the attack vector. Looking up CVE-2022-24530 at the Microsoft Security Response Center, we see that the attack vector is Local.

- Why is fixing this problem important?
  This vulnerability impacts multiple versions of Windows 10, Windows 11, and Server 2019. If a non-admin can gain admin or SYSTEM privileges through the Windows Installer service, they can delete files or directories on your computer. Doing research on the latest vulnerabilities on your operating system allows you to make decisions about what settings are most secure.

**4) Unauthorized user account has been removed: 4 pts. Each**

- 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?
  In the search box, type and select Control Panel. Select User Accounts → select Manage another account. In this window, you can click the users that are not listed on the authorized users 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 only those who need to use it to complete their tasks. By leaving these user accounts on the image, invaliv individuals may be able to log on to the computer and make changes that could affect the safety and security of legitimate users.

**5) Administrator account has been changed to Standard User: 4 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?
  In the search box, type and select Control Panel. Click on User Accounts → 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.

**6) Changed insecure passwords: 4pts each**

- <u>How do I find this problem?</u>
  In the search box, type and select Control Panel. Click on User Accounts → User Accounts → Manage another account.

- <u>How do I solve this problem?</u>
  Select an account. Select “change the password”. Enter and confirm a new password for the user. For information on strong passwords, see Unit Four on the Dashboard. IMPORTANT: Make sure you write down the new passwords, especially any Administrator passwords,so you do not potentially lock yourself out of the image. Close the User Accounts window when finished.
  Type a password hint in the field below.

- <u>Why is this problem important?</u>
  Having a weak password on a user account makes it extremely vulnerable to attacks by outside individuals. With a weak password, an attacker can more easily gain access to a user’s files. Strong passwords make it much more likely that only the authorized user of the account can access it.

**7) Set a secure maximum password age: 5 pts**

- <u>How do I find this problem?</u>
  Security settings in the Local Security Policy allow the administrator to set Account Policy, Audit Policy, User Rights Assignment and security settings. Password Policy appears in Account Policies.

- <u>How do I solve this problem?</u>
  Press the Windows key + R→type “secpol.msc” without the quotes→ Press OK → Under Security Settings, select Account Policies → select Password Policy→ select Maximum password age and enter a password age that is greater than 7 days and less than 91 days → select OK

- <u>Why is fixing this problem important?</u>
  The longer a password exists, the more likely it is that it will be compromised by an attacker. Setting a maximum password age prevents an attacker from having an unlimited amount of time to obtain the account password and access the account.

**8) Set a secure lockout threshold: 4pts**

- <u>How do I find this problem?</u>

Security settings in the Local Security Policy allow the administrator to set Account Policy, Audit Policy, User Rights Assignment and security settings. Account Lockout Policy appears in Account Policies.

- How do I solve this problem?
  Press the Windows key + R→type “secpol.msc” without the quotes→ Press OK → Under Security Settings, select Account Policies → select Account Lockout Policy → select Account lockout threshold → in the “invalid login attempts” field, enter a number greater than 4 and less than 51. Then, press OK.

- Why is this problem important?
  Setting a secure lockout threshold will ensure that a brute force password attack will result in the attacker being locked out of the account. The number of invalid login attempts should be low enough to prevent an attacker from accessing the account, but high enough so that users are not locked out of the account. Giving users at least 5 attempts prevents them from accidentally being locked out of their account.

**9) Set an Audit security policy: 5pts**

- How do I find this problem?
  Security settings in the Local Security Policy allow the administrator to set Account Policy, Audit Policy, User Rights Assignment and security settings.

- How do I solve this problem?
  Press the Windows key + R→type “secpol.msc” without the quotes→ expand Advanced Audit Policy Configuration → expand System Audit Policies → double-click Account Logon → double-click account credential validation→ check the Configure the following audit events box → select Success → select Apply → select OK.

- Why is fixing this problem important?
  This policy setting allows you to audit events generated by validation tests on user account logon credentials. Events in this subcategory occur only on the computer that is authoritative. For local accounts, the local computer is authoritative. Administrators can monitor successful authentication attempts to make sure authorized users are logging into the network.

**10) Set Security Policy: 5 pts.**

- How do I find this problem?

Security settings in the Local Security Policy allow the administrator to set Account Policy, Audit Policy, User Rights Assignment and other security settings.

- How do I solve this problem?
  Press the Windows key + R → type "secpol.msc" without the quotes → expand Local Policies → double-click Security Options → scroll down until you find Interactive Logon: Do not display last user name and double-click → select Enabled → select Apply → select OK.

- Why is fixing this problem important?
  This security setting determines whether the name of the last user to log on to the computer is displayed in the Windows logon screen. If this policy is enabled, the name of the last user to successfully log on is not displayed in the Logon Screen. If this policy is disabled, the name of the last user to log on is displayed. If this setting is not enabled, a malicious user who has access to the console can leverage the username as part of a password guessing attack.

**11) Firewall has been enabled: 5 pts.**

- How do I find this problem?
  Turning on the firewall is a good cybersecurity practice to prevent unauthorized access to a system.

- How do I solve this problem?
  In the Search box, type Control Panel. Click on System and Security → Windows Defender Firewall → select Turn Windows Defender Firewall on or off → under Private and Public network settings, select Turn on Windows Defender Firewall → select OK.

- Why is fixing this problem important?
  Firewalls are your first line of defense against attacks. You can customize your firewall settings to allow traffic for specific programs. The two most common exceptions you can create are for ports or programs.

**12) File sharing has been disabled for C drive: 5pts**

- How do I find this problem?
  Checking file shares is a good cybersecurity practice to determine which files can be accessed on your organization's network.

- How do I solve this problem?

Press the Windows key + R → type “fsmgmt.msc” without the quotes → select Shares. Share names will appear in the first column. Under share names, right click C. Select stop sharing, then select Yes.

- Why is fixing this problem important?
  File sharing should be disabled when it is not necessary because it allows wireless access to your files over your network. Disabling/stopping shares makes your computer more secure because it prevents attackers on your network from accessing your computer’s files.

**13) Disable Simple TCP/IP service: 5 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?
  In the Search box, type Control Panel. Select Programs → select Programs and Features → in the left-hand pane, select Turn Windows features on or off → scroll down and uncheck Simple TCPIP services → select OK → at the Windows Features prompt, select Restart now.

- Why is fixing this problem important?
  Disabling unnecessary services decreases the attack surface of a system. The vulnerabilities in this service could allow for Denial of Service (DoS) attacks.

**14) Firefox has been updated: 4pts**

- How do I find this problem?
  The ReadMe states that the latest stable version of Firefox is required by the organization’s management.

- How do I solve this problem?
  Click on the Firefox shortcut on your desktop. Click on the menu on the top right corner of the screen, shown as 3 horizontal lines. Select the question mark icon at the bottom of the menu, then select the option About Firefox. A window will appear that allows you to click on Check for updates. Then selection Update to 47.02. Wait for the update to download, then select “Restart Firefox to Update” → Yes. Open Firefox again and repeat this process to Update to 56.0.

- Why is fixing this problem important?

Browser updates often contain security features to keep up to date with new methods of attacks and repair vulnerabilities found in previous versions. Updates are also generally better at detecting malware, trojan viruses, and other types of malware, which makes your computer less susceptible to these types of attacks.

**15) Geany has been updated: 5pts**

- <u>How do I find this problem?</u>
  Click on the Geany shortcut on the Desktop → select Help → select About. The version listed is 1.27. Use a web browser to research the latest version of Geany. Notice that the latest version is later than 1.27, and that your current version will need to be updated.
- <u>How do I solve this problem?</u>
  In a web browser, go to https://www.geany.org/download/releases/ or search Geany downloads and find their "Releases" page. Select geany-1.38_setup.exe for Windows 64-bit operating system → select Save file. Locate the file in your file explorer, and click on the file. You will be prompted to allow the app to make changes to your device. Select yes. Next you will be prompted to uninstall Geany 1.27. Select Yes → Ok. Follow the Geany setup wizard steps (Next > I Agree > Next > Next > Install > Finish)

- <u>Why is fixing this problem important?</u>
  Security vulnerabilities that have been discovered in software are often corrected by the developers in newer versions of the software. Keeping the latest version of software on your computer ensures that software vulnerabilities are kept at a minimum.

**16) Prohibited files have been removed: 5 pts.**

- <u>How do I find this problem?</u>
  The README file notes that non-work related files and hacking tools are prohibited on this image. You may find unauthorized files on an image, but they may also help you solve a Forensics Question. Always try to answer Forensics Questions first before you modify or delete files.

- <u>How do I solve this problem?</u>
  Music MP3 files are considered unauthorized and should be removed from the image. Open File Explorer or press the Windows Key + E. Select Local Disk (C:) → Users → moana → Music → right-click each MP3 file, and Select Delete.

- <u>Why is fixing this problem important?</u>

Keeping non-work related files or hacking tools on the computer is a violation of the company's policies as mentioned in the README file.

**17) Unauthorized software has been removed: 4 pts. Each**

- How do I find this problem?
  The README file states that unauthorized software is prohibited on this image.

- How do I solve this problem?
  Wireshark is considered unauthorized software and should be removed from the image. In the Search box, type Control Panel. Click on Programs → Programs and Features → right-click Wireshark and select Uninstall. MyCleanPC is also considered unauthorized software. Repeat this process to uninstall MyCleanPC.
- Why is fixing this problem important?
  Removing unauthorized software is a best security practice.

## Penalties

**1) Account lockout threshold is less than 5: -2 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 authorized users accidentally locking themselves out of the system.

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

- Why is this a penalty?
  The ReadMe states that Firefox is the required browser for all users on this computer, as determined by the organization’s management. Removing Firefox from this computer is a violation of the organization’s policy.