CyberPatriot Windows 11

Practice Image Answer Key

Welcome to the CyberPatriot Practice Round! This image will provide you with information on how to solve common vulnerabilities on a Windows 11 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: 7 pts.

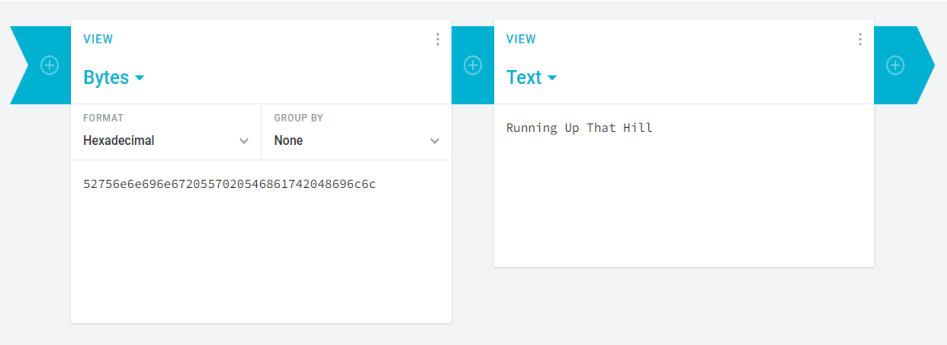
- How do I find this problem?

  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 meant for mmayfield. The message "52756e6e696e6720557020546861742048696c6c" is encoded from ASCII to hexadecimal (base 16).

  To decode the message, an online hexadecimal to ASCII converter such as https://cryptii.com/pipes/hex-decoder may be used.



  The answer to this question (and the decoded value) is "Running Up That Hill"

- Why is fixing this problem important?

  Having a grasp of simple encoding techniques, such as using hexadecimal, is a key skill. It allows us to uncover hidden messages that have been transformed using these techniques. Also, hexadecimal is a widely used format for data representation in cryptography and binary files.

2) Forensics Question 2 Correct: 7 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?

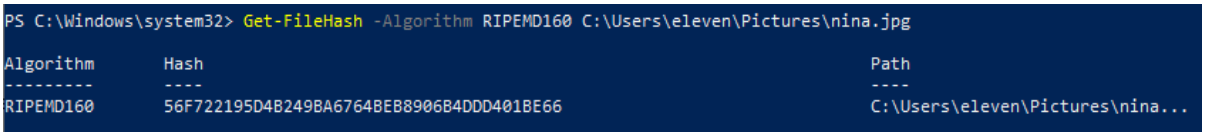
  This question asks you to find the RIPEMD-160 sum of the file in the Pictures directory of eleven named “nina.jpg”.

  While holding down the **Shift** key right click on the **Desktop** in an empty space and select **Open PowerShell window here**. In the PowerShell window type the following commands:

  cd C:\Windows\System32

  Get-FileHash -Algorithm RIPEMD160 C:\Users\eleven\Pictures\nina.jpg

  Press **Enter** and the answer to this question is located under Hash. Remember to Save and close the forensics question file.



- Why is fixing this problem important?

  It’s important to know what hash functions are and how they can be used. Hash functions, when used correctly, can be used to verify the integrity of files, ensuring they have not been modified by an adversary. Hash functions are one-way functions that rely on 4 main properties for security: pre-image resistance, second pre-image resistance, collision resistance, and pseudo-randomness. Hash functions have many uses in cryptography including playing an important role in digital signatures and encryption algorithms.

3) Removed unauthorized user pmckinney: 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 **pmckinney**

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 only 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 yismaylov: 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 **yismaylov** 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 only 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 jbyers 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 **jbyers** 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 mbauman 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 **mbauman** 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) Changed insecure password for sharrington: 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 README may list some known administrator passwords. Short, or simple word-based passwords are examples of passwords that adversaries can easily guess or brute force. In a real-world scenario, you wouldn't know other user's password and would need to employ password auditing techniques.

- 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 **sharrington,** select **Set Password…**, and click **Proceed**. Choose a secure password and type it into the **New password** and **Confirm password** text boxes. Click **OK** to change the password, and the **OK** again.

- 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.

8) User argyle has a password: 3 pts.

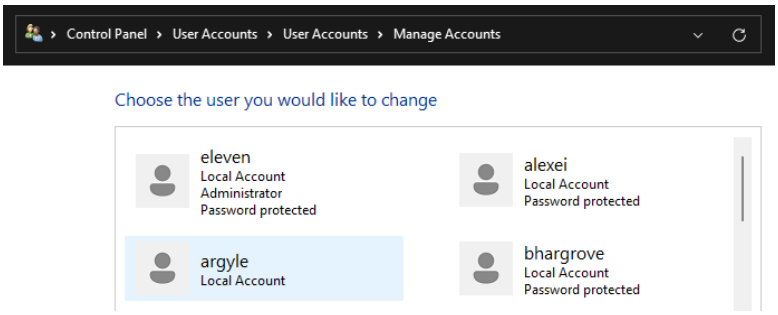
- How do I find this problem?

  9) It is good practice to ensure that all user accounts are password protected. Users with no passwords can be found by navigating to **Control Panel\User Accounts\User Accounts\Manage Accounts** in the **Control Panel**.

- How do I solve this problem?

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

the Control Panel. In the Control Panel, click **User Accounts**, then **User Accounts**, then click **Manage another account.** Note that the description under **argyle** does not say Password protected.



Click **argyle**, then click Create a password. Choose a secure password and type it into the **New password** and **Confirm new password** text boxes, and 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 without a password.

10) Created user account esinclair: 4 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 **esinclair** 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.

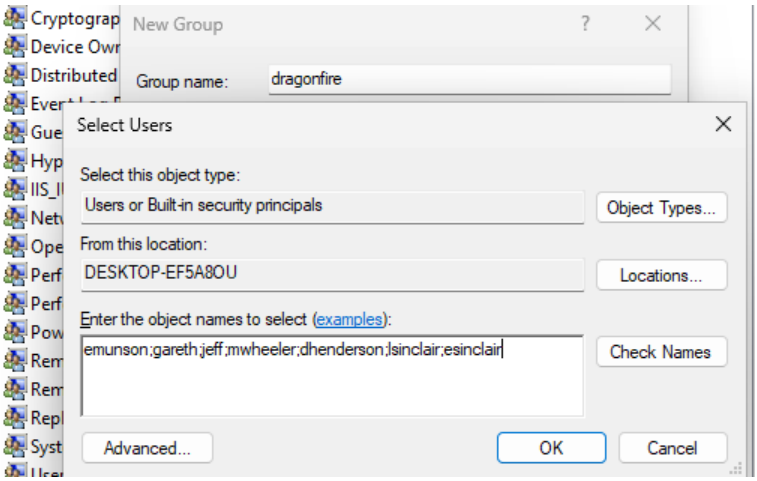
11) Created group dragonfire and **Added users to group dragonfire: 4 pts each.**

- 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 **dragonfire** for the Group name. Click add and enter all usernames separated by semicolons: **emunson;gareth;jeff;mwheeler;dhenderson;lsinclair;esinclair**. 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.

12) A secure maximum password age exists: 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 **Maximum password age**. Set the password to expire in **90 days** and click **OK**.

- Why is fixing this problem important?

  Setting a maximum password age 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.

13) 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.

14) Limit local use of blank passwords to console only [enabled]: 4 pts.

- How do I find this problem?

  Enforcing industry recommended security options 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 **Accounts: Limit local use of blank passwords to console only**. Set the setting to **Enabled** and click **OK**.

- Why is fixing this problem important?

  When this setting is enabled, local accounts may only log on at the computer's physical keyboard if they do not have a password set. While all user accounts should be password protected, the extra security measure is still important to prevent remote access without a password.

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

- How do I find this problem?

  Enforcing industry recommended security options 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.

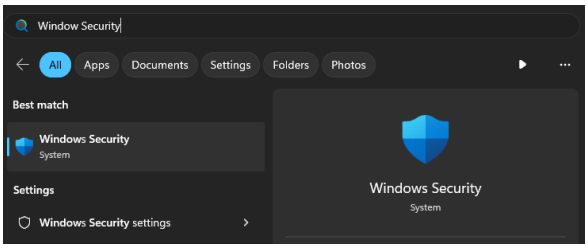
16) Firewall protection has been enabled: 5 pts.

- 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?

  Open the **Windows Security** application found in the **Start Menu**.



Under Firewall & network protection, click **Turn** on. In the User Account Control dialog box, click **Yes**.

- 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.

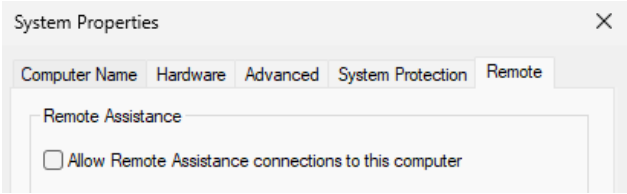
17) Remote Assistance connections have been disabled: 5 pts.

- 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 **sysdm.cpl** and press **Enter** to open System Properties. Click on **Remote**, then uncheck **Allow Remote Assistance connections to this computer**, the 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) FTP service has been stopped and disabled: 5 pts.

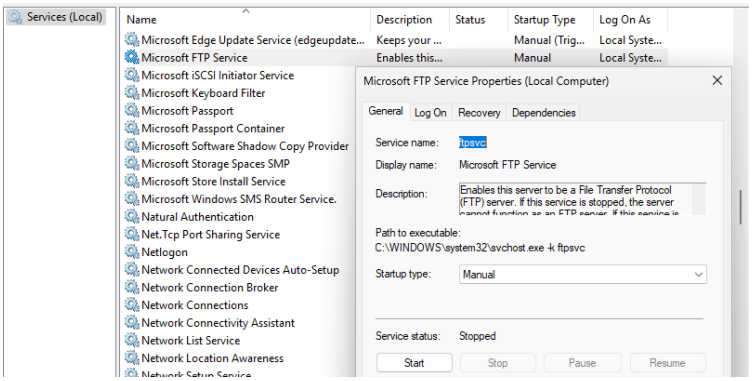
- How do I find this problem?

  Stopping and disabling insecure or unnecessary services is an important principle of good cybersecurity. Many services need to be running to ensure normal and secure operation of computer systems. Reading about the services on your system and doing research can help you determine the importance of a service and if it is necessary for normal operation. Additionally, business-critical services listed in the README should remain running at all times. The Services management console lists all services, their startup type, and their status.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **services.msc** and press **Enter** to open Services. Scroll down, and double click on **Microsoft FTP Service** to open a Properties window. Change the

Startup type to **Disabled** to prevent the service from starting automatically. If the service is currently running, then click **Stop** to stop the service. Click **OK** to apply the changes and close the Properties window.



- Why is fixing this problem important?

  Disabling unnecessary services can limit your attack surface. The fewer services an adversary has to attack and potentially exploit, the lower your risk. Adversaries may attack known or unknown vulnerabilities in services to obtain information, escalate privileges, or gain unauthorized access.

19) The majority of Windows updates are installed: 5 pts.

- How do I find this problem?

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

- How do I solve this problem?

  Right click on the start menu icon and select **Settings**. On the left side of Settings, click on **Windows Update**. To begin applying the updates, click **Download & install all**. 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 all the most recent updates installed.*

Time to install Windows updates can vary depending on your system, network speed, etc. If the updates are stuck for a long time while Windows is starting back up, you may try to restart the virtual machine using the VMWare Workstation Pro Restart Guest button.

- 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) Tiled has been updated: 4 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 Tiled and click on **Help** in the upper left corner. Select **About Tiled** and click on the **Update Available** button. Select **Download** to open a new browser tab on the download page for the latest Tiled version. Select on **No thanks, just take me to the** downloads and download the installer for **Windows 10+ (64-bit).** After downloading, run the Tiled installer to update Tiled to the latest version.

- 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.

21) Google Chrome has been updated: 4 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?

  In a web browser, navigate to https://www.google.com/chrome/, uncheck the checkbox **labeled Help make Google Chrome better**…, then click **Download Chrome**. Run the Chrome installer to update Google Chrome to the latest version.

- 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.

22) 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?

  Right click on the start menu icon  and select **Installed apps**. Click the menu **…** next to **Wireshark**, then click

Uninstall, and click **Uninstall** again. 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.

23) 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?

  Right click on the start menu icon and select **Installed apps**. Click the menu **…** next to **Network Stumbler**, then click **Uninstall**, and click **Uninstall** again. 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 business-critical software and services, contain various malware, contain security vulnerabilities, or could introduce unwanted legal and regulatory issues.

24) 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?

  Right click on the start menu icon and select **Installed apps**. Click the menu **…** next to **PC Cleaner**, then click **Uninstall**, and click **Uninstall** again. Follow the prompts to ensure that PC Cleaner 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.

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.

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

- Why is this a penalty?

  The README states that Tiled is required software.