



CyberPatriot Windows 10 Training 2 Image Answer Key



Welcome to the CyberPatriot Training Round 2! 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: 7 pts.

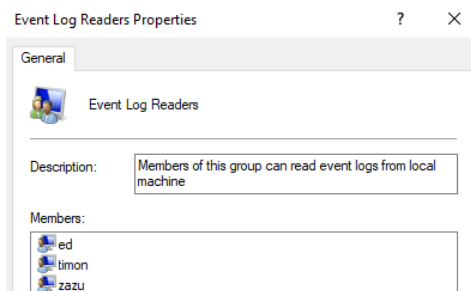
- How do I find this problem?

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 you to list the users that are in the Event Log Readers group.

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, then double click on **Event Log Readers**. The answer to the question is in the Properties window under Members.



- Why is fixing this important

It is a good practice to check the members of user groups on your computer. Members in user groups must be correct, because access to files is granted to groups on your computer. This ensures that access to files is only granted to the correct users on your computer.


2) Forensics Question 2 Correct: 7 pts.

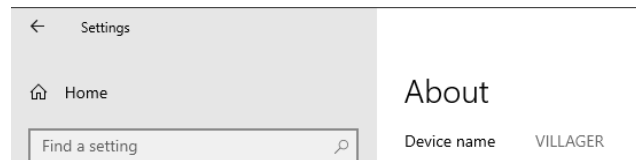
- How do I find this problem?

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 1".

- How do I solve this problem?

The question asks your system's full computer name.

Right click on the Start Menu icon  and select **Settings**, then click on **System**. On the left of the settings window, scroll down and click on About. The answer to the question is next to Device 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) Removed unauthorized user irwin: 2 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 **irwin** 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) User vasca is not an administrator: 2 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 to 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 **vasca** 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.

5) Changed insecure password for ygagarin: 2 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 another 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 **ygagarin**, 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 this problem important?


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.

6) Updated users in voyagers group: 5 pts.

- How do I find this problem?

The README requests that you set the membership of the "voyagers" group to gcooper, scar, zazu, and sarafina.

- 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 **voyagers** for the Group name. Select **banzai** and click **Remove**. Select **timon** and click **Remove**. Click **Add...** and enter all usernames separated by semicolons: **gcooper;scar;zazu;sarafina** then click **OK**, and **OK**.

- Why is 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.

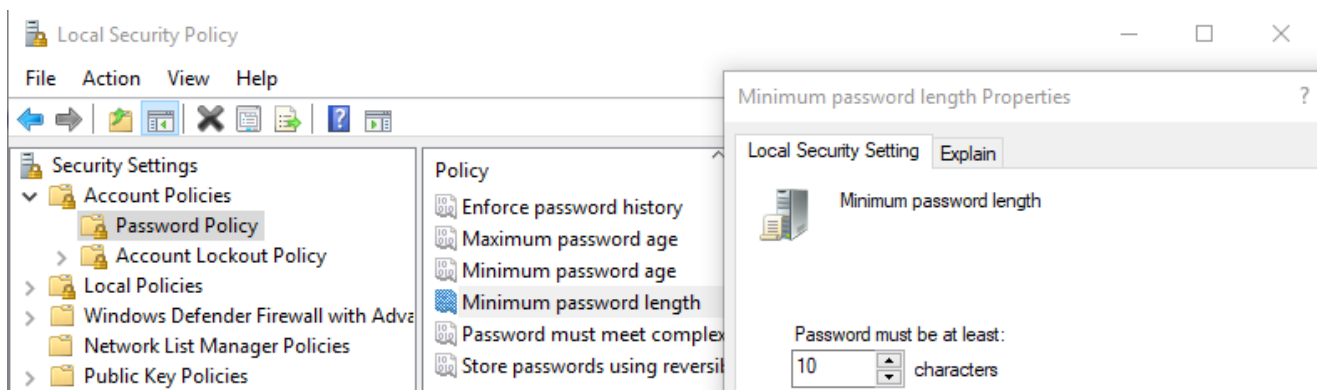
7) A secure minimum password length is required: 3 pts.

- How do I find this problem?

Enforcing industry recommended auditing 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**. Change the minimum password length to **10 characters** and click **OK**.



- Why is this problem important?


Having a password on a user account that is too short 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.

8) A secure lockout threshold exists: 3 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.

9) Passwords must meet complexity requirements: 3 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 **Password must meet complexity requirements**. Select **Enabled**, and click **OK**.

- Why is this problem important?


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.

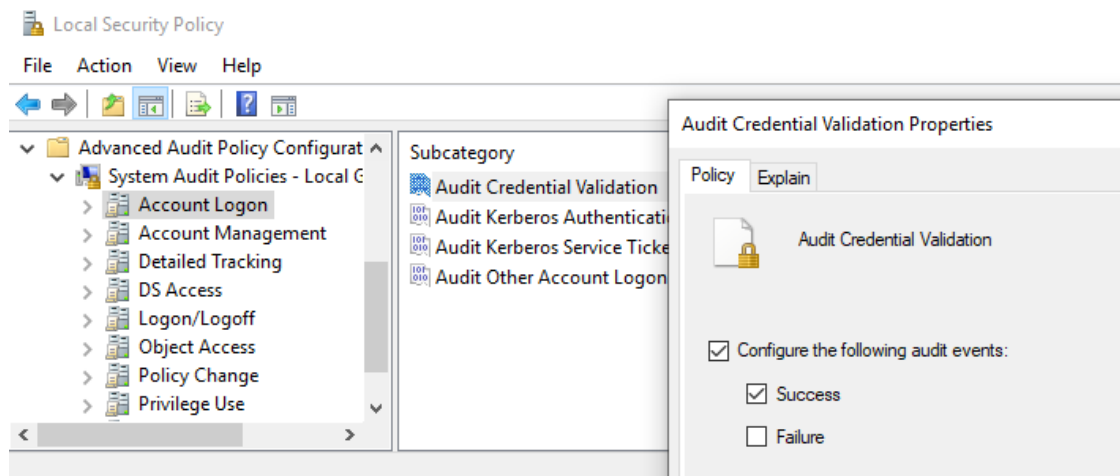
10) Audit Credential Validation [Success]: 4 pts.

- How do I find this problem?

Enforcing industry recommended auditing 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** → **Advanced Audit Policy Configuration** → **System Audit Policies** → **Account Logon**. Double click on **Audit Credential Validation**. Select the checkbox labeled **Success** and click **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. Be careful what you audit however, as auditing some things, or too many things, can use a lot of disk space and negatively impact the performance of the computer.

11) Behavior of the elevation prompt for administrators in Admin Approval Mode configured to prompt: 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 **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode** to bring up a Properties window. Select **Prompt for consent on the secure desktop**, click **OK**, then click **YES** to apply the setting and close the Properties window.

- Why is this problem important?


It is good practice to prompt administrators before executing programs that are given administrator privileges. This helps prevent administrators from unknowingly running malicious programs and giving them administrator privileges.

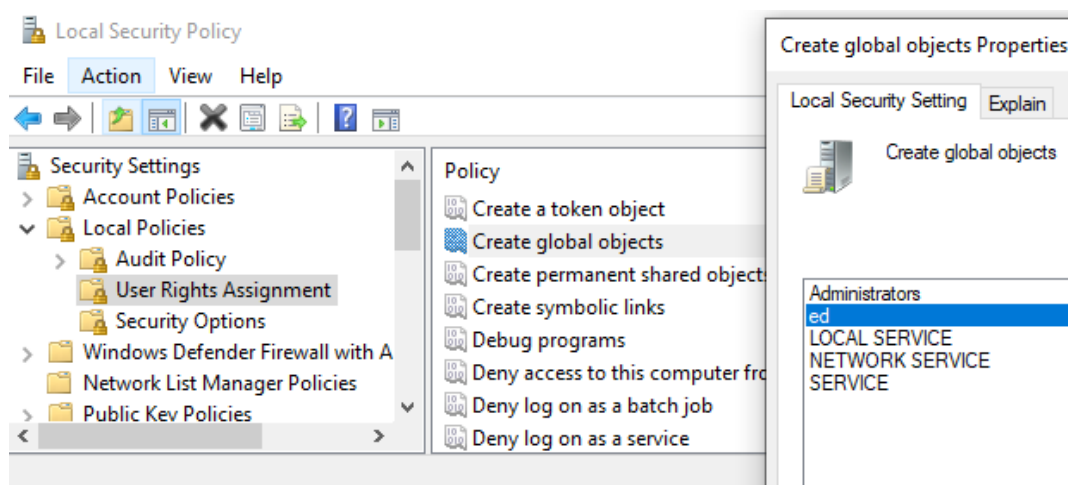
12) User ed may not create global objects: 4 pts.

- 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 → User Rights Assignment**. Double-click on **Create global objects** to bring up a Properties window. Select **ed**, click **Remove**, and then click **OK** to apply the setting and close the Properties window.



- Why is fixing this problem important?

The Explain tab states that assigning this user right can be a security risk, and that this right should only be assigned to trusted users. By default this right is only granted to Administrators, Local Service, Network Service, and Service.

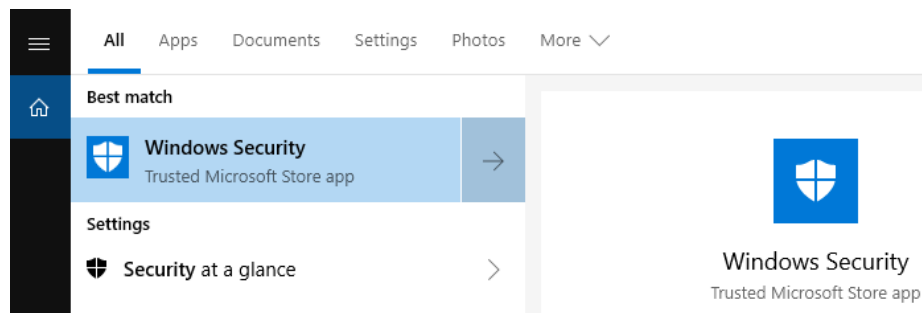
13) Firewall protection has been enabled: 5 pts.

- 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.

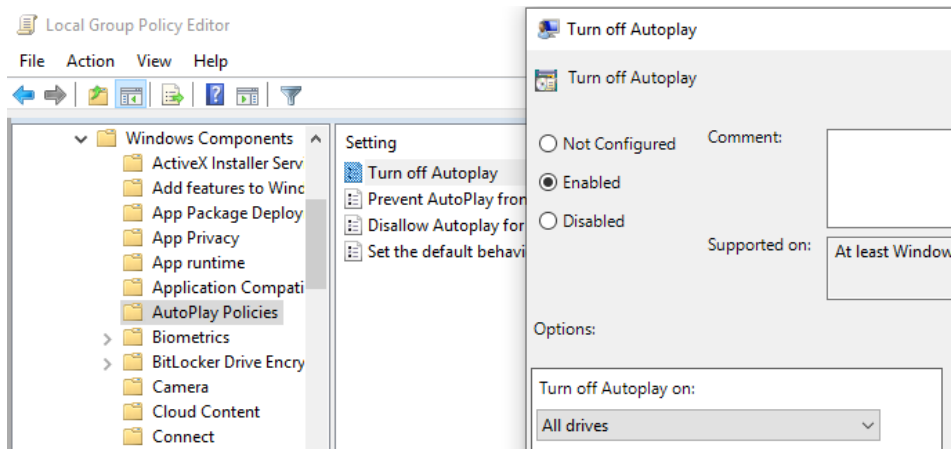
14) AutoPlay has been disabled [all users]: 5 pts.

- 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 **gpedit.msc** and press **Enter** to open the Local Group Policy Editor. In the Local Group Policy Editor, navigate to **Local Computer Policy** → **Computer Configuration** → **Administrative Templates** → **Windows Components** → **AutoPlay Policies**. Double click on **Turn off Autoplay** to bring up a dialog window. Select **Enabled**, and ensure Turn off Autoplay on is set to **All drives** and click **OK**.



- Why is fixing this problem important?


AutoPlay is a Windows feature that allows devices connected to your computer (disks, USB drives, etc.) to run programs automatically. It is best to turn this feature off because it prevents your computer from automatically installing malware that is on a USB drive or other device.

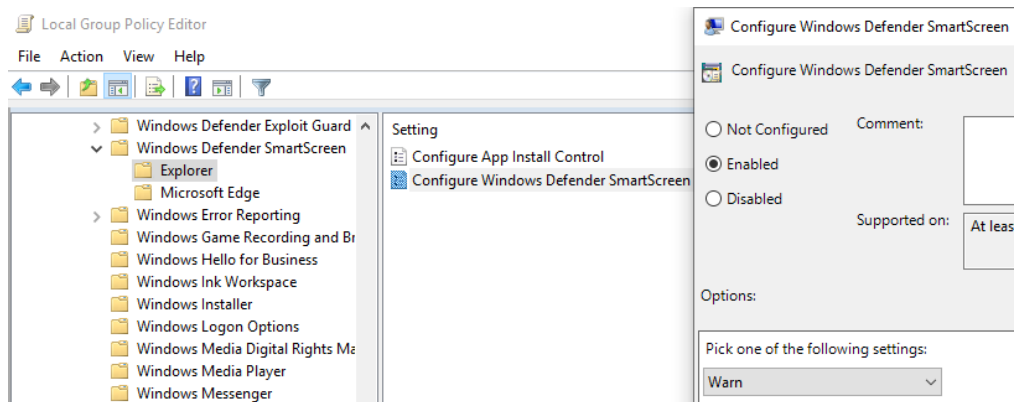
15) Windows SmartScreen configured to warn or block: 4 pts.

- 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 **gpedit.msc** and press **Enter** to open the Local Group Policy Editor. In the Local Group Policy Editor, navigate to **Local Computer Policy → Computer Configuration → Administrative Templates → Windows Components → Windows Defender SmartScreen → Explorer**. Double click on **Configure Windows Defender SmartScreen** to bring up a dialog window. Select **Enabled**, and ensure that it is configured to **Warn** and click **OK**.



- Why is fixing this problem important?


Windows SmartScreen protects the system warning users before running potentially malicious programs downloaded from the internet. If it is configured to warn, it will notify users that an app appears suspicious, but will permit the user to disregard the warning. Preventing bypass is more secure than warning, but warning is more secure than the current configuration. Be careful when preventing bypass, as this could prevent legitimate software from running.

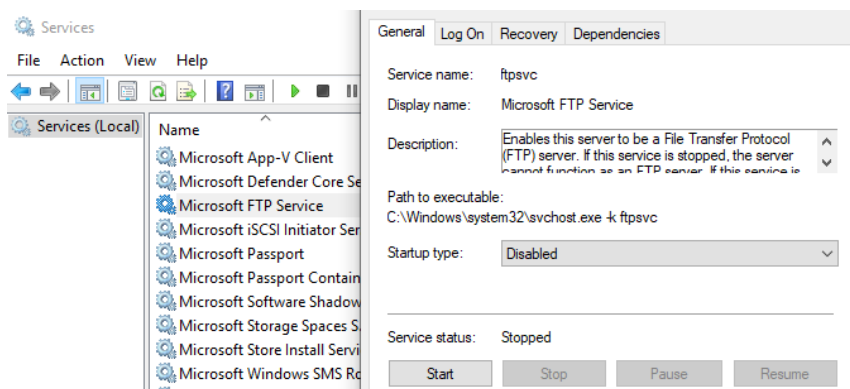
16) FTP service has stopped and disabled: 5 pts.

- 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, 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 may 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.

17) World Wide Web Publishing 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 **World Wide Web Publishing Service** to open a Properties window. Change the Startup type to **Disabled** to prevent the service from starting automatically, 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 may 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.

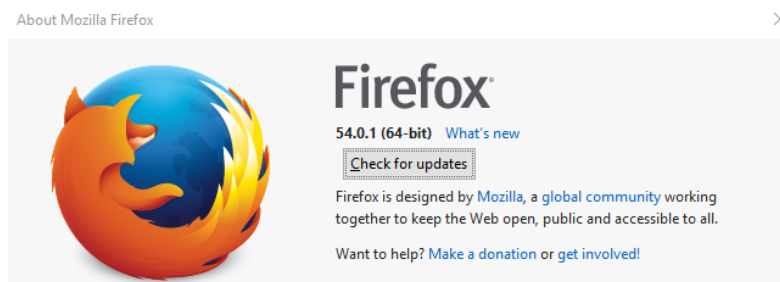
18) Firefox has been updated: 5 pts.

- 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?

Using a web browser, navigate to <https://www.mozilla.org/en-US/firefox/windows/>. Click on **Download Now** to download the Firefox Installer. After downloading, run the **Firefox Installer** to update Firefox 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.

19) Removed prohibited MP3 files: 4 pts.

- How do I find this problem?

The README file notes that non-work related media files are prohibited on this image. One way to find unauthorized media files is to use the search functionality in File Explorer.

- How do I solve this problem?

Press the Windows key  + R to open the Run dialog. In the Run dialog type **C:\Users\ashepard\Music** and press **Enter** to open the Explorer. Right click on the folder **Pure Piano Improv**, then click **Delete**.

- Why is fixing this problem important?


Company policy prohibits non-work related media as mentioned in the README. Additionally, media files may contain exploits that could compromise systems.

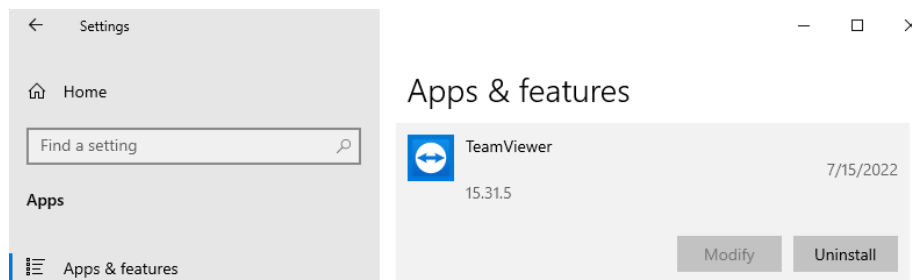
20) Removed TeamViewer: 5 pts.

- 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 **Settings**, then click on **Apps**. Click on **TeamViewer**, then click on **Uninstall**.



- 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.

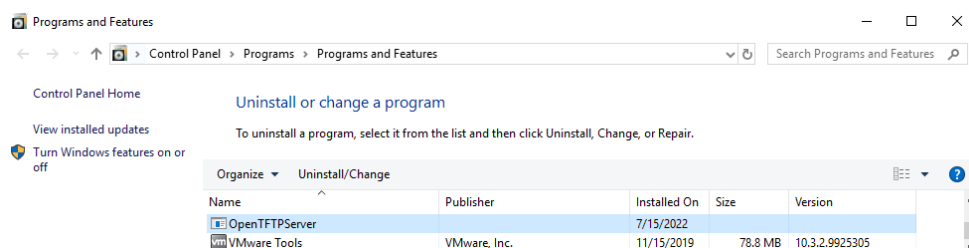
21) Removed Open TFTP server: 5 pts.

- 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 **appwiz.cpl** and press **Enter** to open Programs and Features. Click on **OpenTFTPServer**, click on **Uninstall/Change**, then click **Yes** and **Yes**.



- 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 netcat backdoor: 5 pts.


- How do I find this problem?

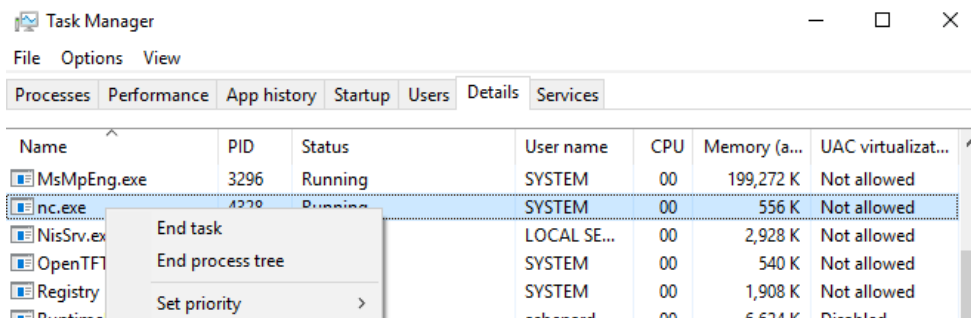
Removing malware such as backdoors, keyloggers, sniffers, viruses, trojans, worms, botnets, among others, is very important. Malware can often be found by using antivirus and antimalware scanners. Malware that is currently running can be found by analyzing the currently running processes, network traffic, and open ports. Autoruns, and other sysinternals tools can help identify malware as well.

- How do I solve this problem?

Make sure you have installed Windows Defender, see **15) Microsoft Defender Antivirus Service has been installed** before continuing.

Press the Windows key  + R to open the Run dialog. In the Run dialog type **taskmgr** and press **Enter** to open the Task Manager. Click on **More details**, in the bottom left corner of the Task Manager, then click on the **Details** tab. Scroll down, and right click on **nc.exe** and select **Open file location** to File Explorer in C:\Windows.

Still in the Task Manager window, right click on **nc.exe**, click **End task**. Back in **File Explorer**, in C:\Windows, right click on **nc** (the .exe file extension is hidden), and select **Delete**. You may need to click the  **UAC dialog icon** on the taskbar, then click **Yes**.



- Why is fixing this problem important?


Malware, including backdoors, keyloggers, sniffers, viruses, trojans, worms on your system means your system has been compromised. In the real world you may want to take actions such as contacting law enforcement, imaging the disk drive for later analysis, conducting a forensics investigation, isolating the system, and eventually wiping it. Since this is a competition environment, answer any related forensics questions and then remove all signs of the malware.

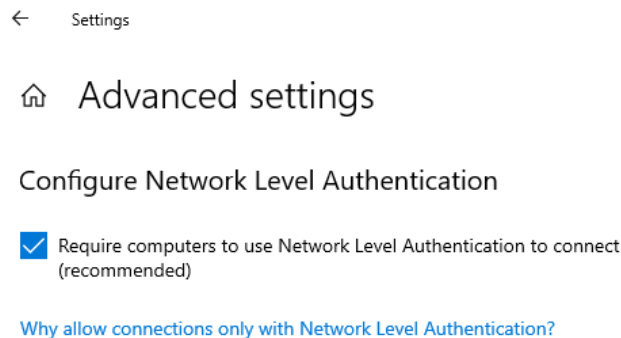
23) RDP network level authentication enabled: 4 pts.

- How do I find this problem?

The README lists RDP as a critical service. As a security professional, it is your job to research how to secure critical services.

- How do I solve this problem?

Right click on the Start Menu icon  and select **Settings**, then click on **System**. On the left side, scroll down and click on **Remote Desktop**, select **Enable Remote Desktop**, then click on **Advanced Settings**. Click on **Require computers to use Network Level Authentication to connect (recommended)**, then click **Yes**. On the confirmation prompt, click **Confirm**.



- Why is fixing this problem important?


Securing critical services, especially those listening on the network is critical. Critical services should not be disabled and often listen on the network making them alluring targets for adversaries.

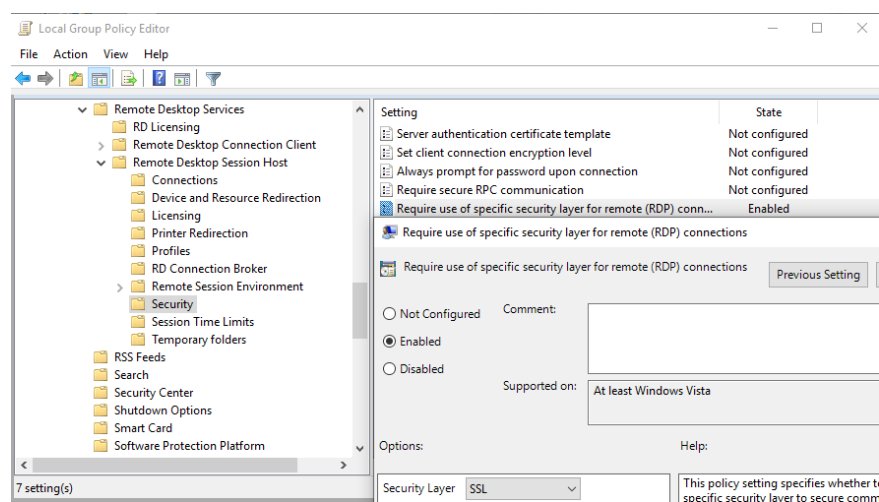
24) RDP Security Layer set to SSL: 5 pts.

- How do I find this problem?

The README lists RDP as a critical service. As a security professional, it is your job to research how to secure critical services.

- How do I solve this problem?

Press the Windows key  + R to open the Run dialog. In the Run dialog type **gpedit.msc** and press **Enter** to open the Local Group Policy Editor. In the Local Group Policy Editor, navigate to **Local Computer Policy** → **Computer Configuration** → **Administrative Templates** → **Windows Components** → **Remote Desktop Services** → **Remote Desktop Session Host** → **Security**. Double click on **Require use of specific security layer for remote (RDP) connections** to bring up a dialog window. Select **Enabled**, ensure that Security Layer is set to **SSL**, and click **OK**.



- Why is fixing this problem important?

Securing critical services, especially those listening on the network is critical. Critical services should not be disabled and often listen on the network making them alluring targets for adversaries.

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

- Why is this a penalty?

The README states that Thunderbird is required software.