CyberPatriot Windows Server 2022

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 Server 2022 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: 10 pts.**

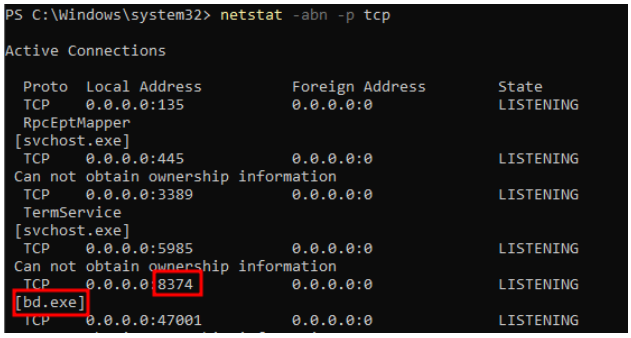
- How do I find this problem?

  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 find the port that “bd.exe” is using to listen for incoming connections.

  Right click on the Start Menu icon and select **Windows** PowerShell **(Admin)**. In Powershell run the command **netstat -abn -p tcp**



  The answer we are looking for is the local port, which appears above **[bd.exe]**, under Local Address, on the right side of the colon **:** .

  Remember to **Save** and close the file.

- Why is fixing this problem important?

  Backdoor processes are designed to give adversaries remote access to computers and networks.

  It's also important to know what processes are listening on the network, as anything listening on the network could be vulnerable to attack.

2) Forensics Question 2 Correct: 10 pts.

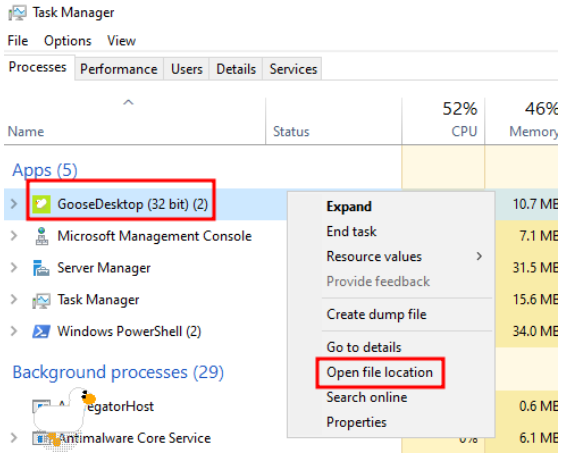
- How do I find this problem?

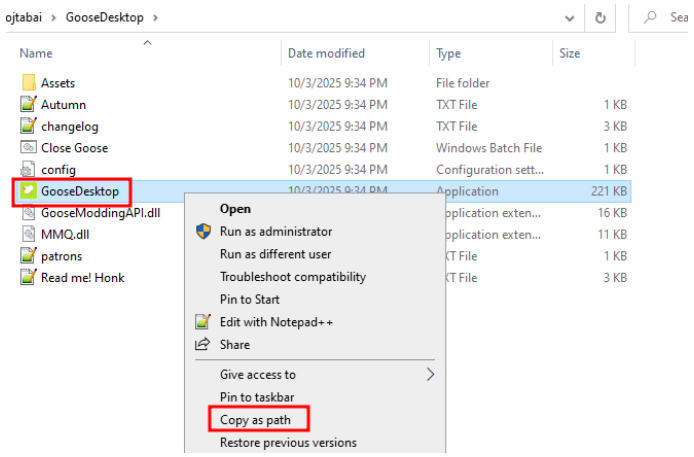
  When you open an image, please read all the "Forensics Questions" thoroughly before modifying the image as you may change something that prevents you from answering the question correctly. There is a file on the Desktop here named "Forensics Question 2".

- How do I solve this problem?

  This question asks you to list the absolute file path of the "GooseDesktop" application executable.

  Right click on the taskbar and select "Task Manager". In task manager, Right click on GooseDesktop (32 bit) and select "Open file location". In File Explorer, you can press the shift key and right click the application to then copy as path to get the absolute file path.





When pasting in the answer to the file, ensure that you remove the quotes. Remember to **Save** and close the file.

- Why is fixing this problem important?

  Understanding how to identify the location of a process is essential in case you identify a malicious process (like the back door in the last question) in order to quarantine or remove the file.

3) Removed unauthorized users pkotsiopulos and mkirchoff: 5 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. 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 **pkotsiopulos** and select **Delete**. In the resulting dialog box click **Yes** to confirm that you want to delete the user. Repeat this for **mkirchoff.**

- 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 rreddington is not an administrator: 5 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 **rreddington** 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 hcooper: 5 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 **hcooper,** 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.

6) **A sufficient password history is being kept: 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 **Enforce password history**. Under keep password history for, select **5 passwords remembered** and click **OK**.

- Why is fixing this problem important?

  Setting a password history prevents users from changing their password back to a recently used password. Reusing a previously used password may be insecure because the password could have been cracked or compromised by an adversary.

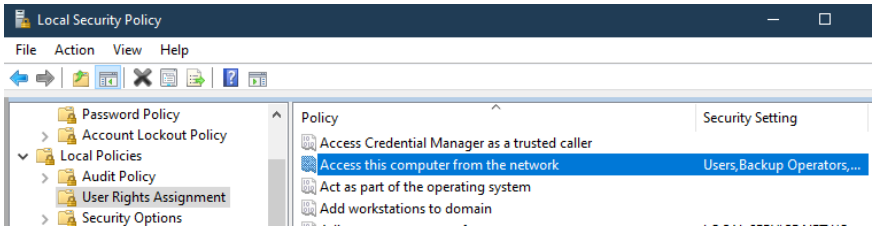
7) **Everyone may not access this computer from the network: 4 pts.**

- 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 **Access this computer from the network** to bring up a Properties window. Select **Everyone**, click **Remove,** click **OK**, and then click **Yes** to apply the setting and close the Properties window.



- Why is fixing this problem important?

  The Everyone group is included to ensure backwards compatibility, but Microsoft recommends removing Everyone from this user right. The recommended value for this setting is Administrators and Authenticated Users.

  https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/access-this-computer-from-the-network

  https://www.stigviewer.com/stig/microsoft_windows_server_2022/2022-08-25/finding/V-254434

8) **Let Everyone permissions apply to anonymous users [disabled]: 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: Let Everyone permissions apply to anonymous users** to bring up a Properties window. Select **Disabled** and click **OK** to apply the setting and close the Properties window.

- Why is fixing this problem important?

  In the Properties window, click Explain for a detailed explanation. This security setting determines what additional permissions are granted for anonymous connections to the computer. If this policy is enabled, anonymous users are able to access any resource for which the Everyone group has been given permissions.

  It is good practice to limit permissions that have been granted to users and groups to only what is necessary, especially permissions granted to anonymous users. The Explain tab also states that the default value for this setting is Disabled.

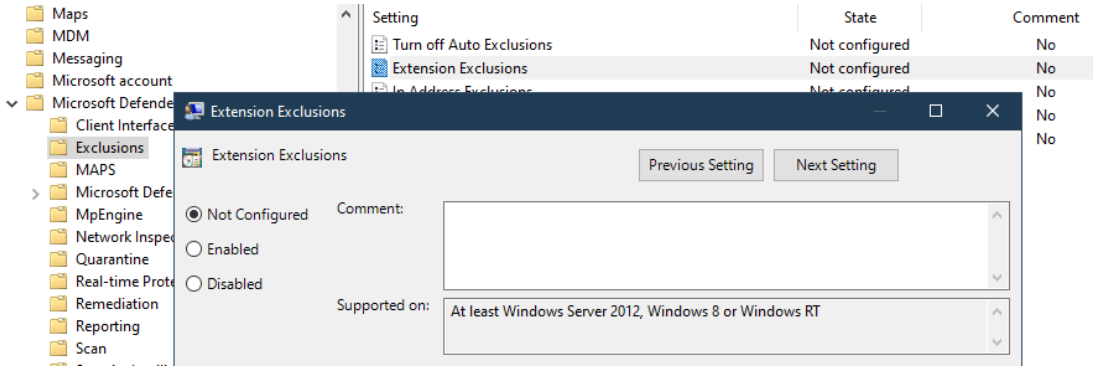
9) Windows Defender does not exclude .exe file extensions: 5 pts.

- How do I find this problem?

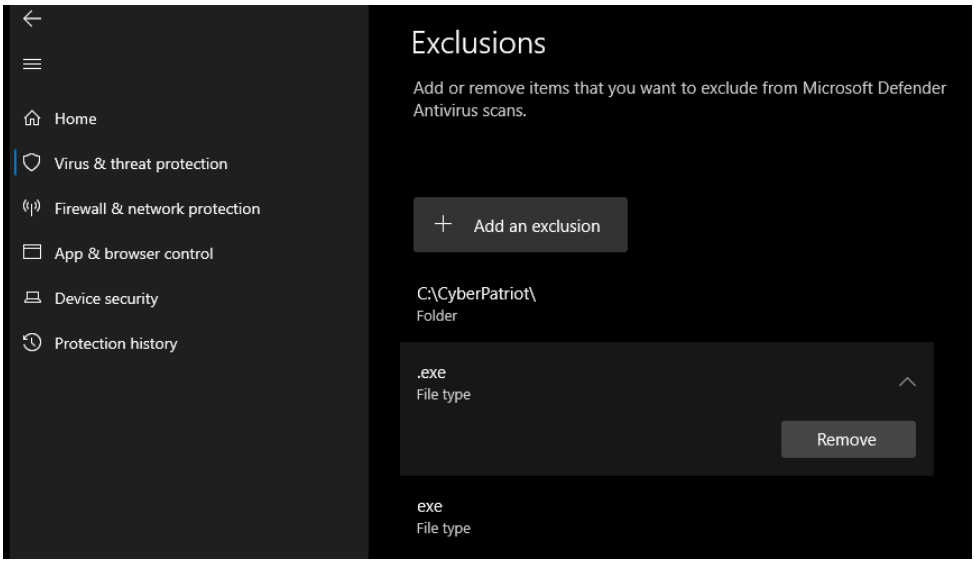
  It's important to review your antivirus settings to ensure that it is properly configured. Excluding exe files is an obviously bad configuration, as it is very common for malware to be an executable with an exe extension.

- 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 → Microsoft Defender Antivirus → Exclusions**. Double click on Extension Exclusions to bring up a separate window. Select **Not Configured** and click **OK**.



Press the Windows key + R to open the Run dialog. In the Run dialog type **windowsdefender:** (make sure and include a colon at the end) and press **Enter** to open Windows Security. Click **Virus & threat protection**, then click **Manage Settings** under Virus & threat protection settings. Scroll down and click on **Add or remove exclusions** under Exclusions. If prompted, click **Yes** in the UAC popup to continue. Click on **Remove** under .exe, then click **Remove** under exe.



- Why is fixing this problem important?

  Although there are many types of malware, one of the most common types are executable files. If Microsoft defender is not configured to check exe files for malware, then it will not be able to detect a large number of malware files and virus infections.

10) File sharing disabled for hidden share USERS$: 4 pts.

- How do I find this problem?

  It's important to know what files and directories are being shared over the network.

- How do I solve this problem?

  Press the Windows key + R to open the Run dialog. In the Run dialog type **fsmgmt.msc** and press **Enter** to open Shared Folders. Click **Shares** on the left side of Shared Folders. Right-click on **USERS$** and select **Stop Sharing.** Click **Yes** to confirm that you want to stop sharing USERS$.

- Why is fixing this problem important?

  Unauthorized file shares are a security vulnerability. Any shares that end with a $ are *hidden* shares and are slightly more difficult to detect. The C$, ADMIN$, and IPC$ shares are default administrative shares created automatically by Windows. **Microsoft does NOT recommend disabling the administrative shares.**

11) DNS Server service has been stopped and disabled: 4 pts.

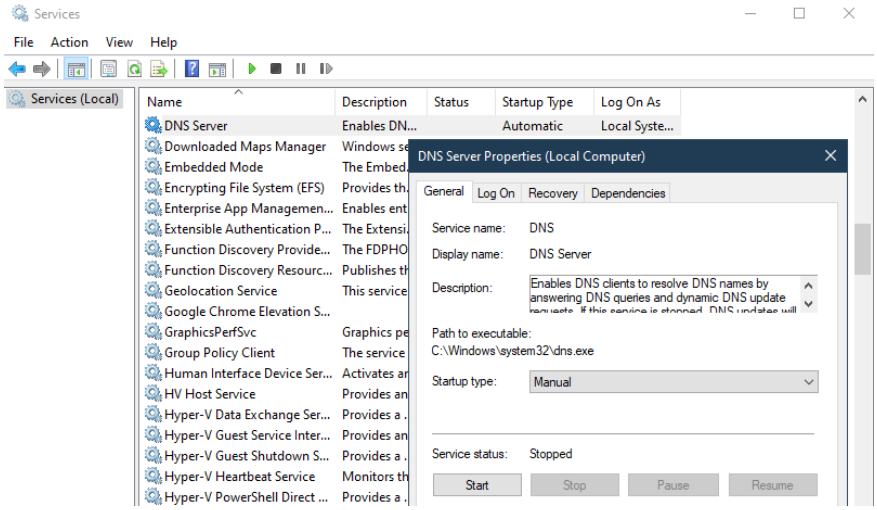
- How do I find this problem?

  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 **DNS Server** 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.

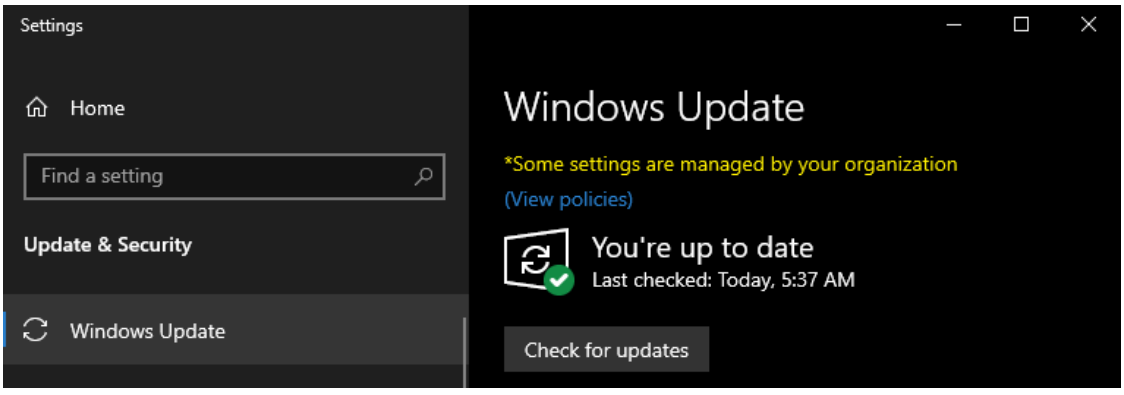
12) The majority of Windows updates are installed: 4 pts.

- 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**. Scroll down and click on **Update & Security**. Click on **Check for updates** and wait for Windows to finish checking for updates. After checking for updates, Windows should automatically begin downloading and installing updates. 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.*



- 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.

13) 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.

14) Notepad++ 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?

  Using a web browser, navigate to https://notepad-plus-plus.org/downloads/ **.** Click on the latest version of Notepad++ (currently v8.8.5). Download the 64-bit installer by clicking the link labeled **Installer**. Be sure to NOT click the ads on the page, which may be labeled Download or Get Now. Alternatively, the latest installer can also be downloaded from https://github.com/notepad-plus-plus/notepad-plus-plus/releases . After downloading, run the Notepad++ installer to update Notepad++ 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.

15) Removed GooseDesktop: 4 pts.

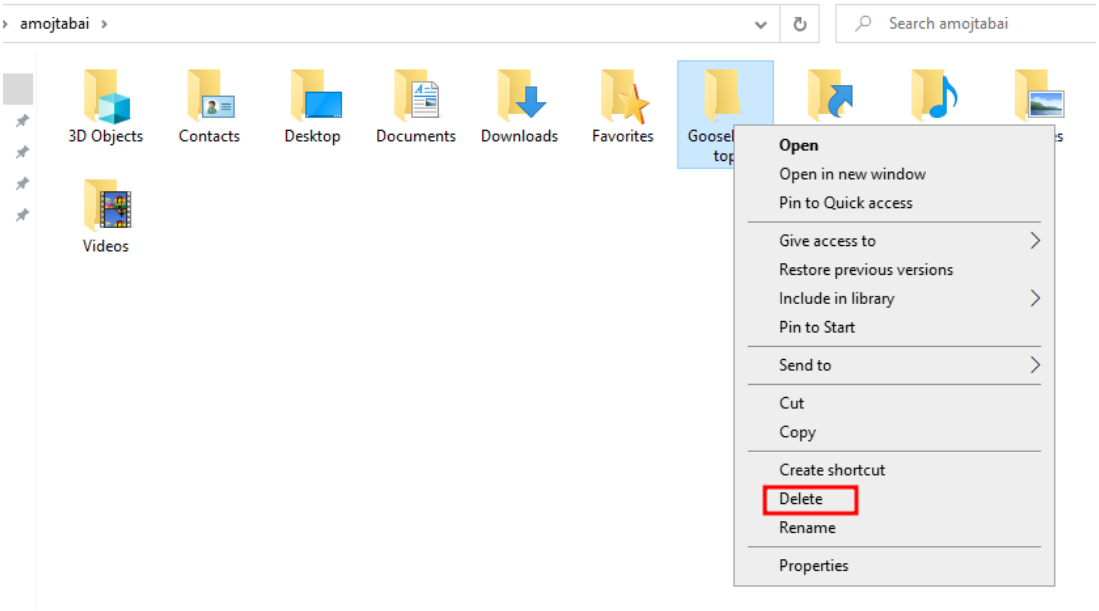
- How do I find this problem?

  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. As mentioned in the second

forensics question, there is a GooseDesktop application running on your desktop.

- How do I solve this problem?

  Follow the instructions for **2) Forensics Question 2 Correct** to locate the GooseDesktop application location. Navigate back a directory, right click on the GooseDesktop folder, and click delete. If you are given an error message stating that the folder is open in another program, then use task manager to kill the GooseDesktop process. After the process is closed, press the try again button to delete the application.



- 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 and security vulnerabilities, or could introduce unwanted legal and regulatory issues.

16) Removed CCleaner: 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?

  The CCleaner64 application is present on the current user's desktop. As this is a third party software that is not required, we can delete the executable. Right click on CCleaner, and select delete to remove it.

- 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 and security vulnerabilities, or could introduce unwanted legal and regulatory issues.

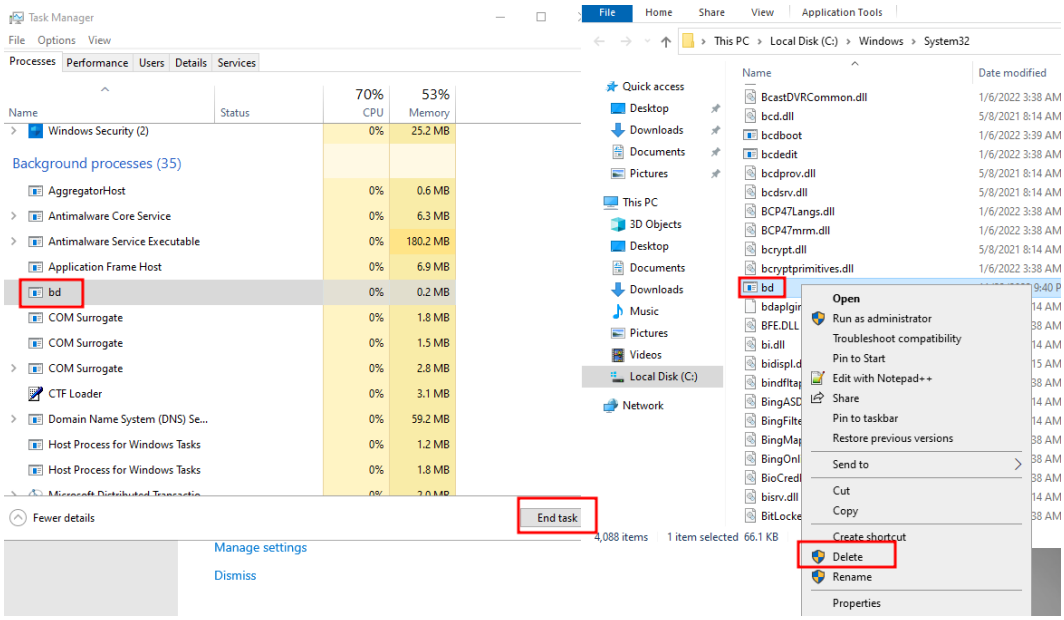
17) Removed netcat backdoor: 5 pts.

- 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?

  Right click on the taskbar and select “Task Manager”. In task manager, Right click on “bd” and select “Open file location”. You may need to select the “More details” expand dialog to find it. Now, you can end the **bd** process and delete the file in the opened File Explorer window. You must end the process before deleting the file.



- 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 and security vulnerabilities, or could introduce unwanted legal and regulatory issues.

18) RDP network level authentication enabled: 5 pts.

- How do I find this problem?

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

  https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/remotepc/remote-desktop-allow-access

- 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 the System Properties. In System Properties, navigate to **Remote** tab. Check the **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)** to enable this setting.

- 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 large targets for adversaries. Network level authentication requires users to authenticate themselves before a remote session is established, preventing unauthorized access to the machine.

19) SMB 1.x removed or disabled: 5 pts.

- How do I find this problem?

  The README states that SMB is a critical service. As a security professional, it is your job to research how to secure critical services. Microsoft and other reputable sites provide significant guidance on this:

  https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-security-hardening

  https://learn.microsoft.com/en-us/windows-server/storage/file-server/manage-smb-dialects

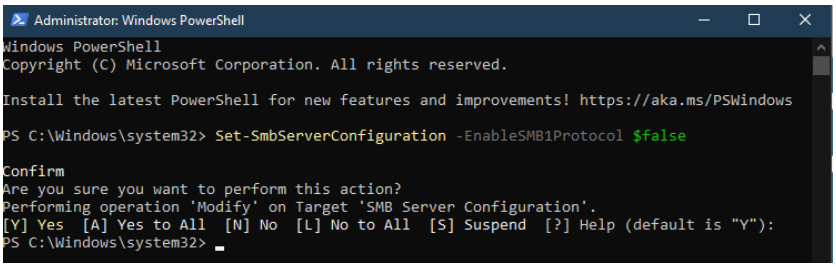
  https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

- How do I solve this problem?

  Right click on the Start Menu icon and select **Windows** PowerShell **(Admin)**. In Powershell run one of the following commands:

  Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

  Set-SmbServerConfiguration -EnableSMB1Protocol $false



- 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 large targets for adversaries.

Penalties

1) WARNING: VirtualBox is unsupported: -0 pts.

- Why is this a penalty?

  This is a warning to inform the user that VirtualBox is **NOT** supported to run the CyberPatriot 18 competition images. Failure to use the version of VMWare Workstation Pro specified on the CyberPatriot website may result in issues that will not be considered for appeals.

2) Account lockout policy less than 5 is deprecated: -4 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.

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

- Why is this a penalty?

  The README states that this system requires Remote Desktop access. Remote Desktop should remain enabled and be further secured for use.

4) **File sharing disabled for AFA: -5 pts.**

- Why is this a penalty?

  The README states that this system has been authorized to share the C:\AFA directory on the network with a share name of AFA and lists SMB as a critical service.

5) **Google Chrome is not installed at the default location: -5 pts.**

- Why is this a penalty?

  The README states that Google Chrome is required software.

6) **Notepad++ is not installed at the default location: -5 pts.**

- Why is this a penalty?

  The README states that Notepad++ is required software.

7) **Critical business file(s) deleted from SMB share: -5 pts.**

- Why is this a penalty?

  The README states that this system has been authorized to share the C:\AFA directory on the network with a share name of AFA and lists SMB as a critical service. The pizza.txt file is a critical file necessary for business operations.