CP-18 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

Forensics Question 1 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 1".

How do I solve this problem?

Go to the search bar on the desktop and type “computer management”. Click on the computer management application to open the application. Click on ‘Local Users and Groups” in the left panel. Select the “groups” option in the middle panel. Click on the group “Event Log Readers” to view all members of the group.

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.

Forensics Question 2 Correct: 8 pts.

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 “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.

Unauthorized user account has been removed: 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. 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.

Administrator account has been changed to Standard User: 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 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.

Changed insecure password: 5 pts.

How do I find this problem?

In the search box, type and select Control Panel.

Click on User Accounts → User Accounts → Manage another account.

How do I solve this problem?

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.

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.

Passwords Meet Complexity Requirements: 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.
Password Policy appears in Account Policies.

How do I solve this problem?

In the Password Policy menu, “Password must meet complexity requirements” is disabled. Double-click on “Password must meet complexity requirements”. In the window that appears, select “Enable”, then select “Apply”.

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.

Set Minimum Password Length: 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 security settings.
Password Policy appears in Account Policies.

How do I solve this problem?

In the Password Policy menu, minimum password length is set at 0 characters. Double-click on “minimum password length” policy to change the number of characters. A window will appear where you can use the arrows to change the number of characters. When the number is set to 8 characters or more, select “Apply”.

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.

Update Users in voyagers Group: 5 pts

How do I find this problem?

The ReadMe states that the membership of the group “voyagers” must contain users: gcooper, scar, zazu, sarafina. Other users should not be in this group. In the search bar, type “computer management” and open the Computer Management desktop app. In the left panel, select “Local users and groups”. Click on the “groups” folder. Then, double-click on the group “voyagers” to view the list of users that are currently in the group.

How do I solve this problem?

For each user that needs to be removed, click on the user name. Then, select “remove”. For each user that must be added, select “Add”. Enter the user name and click “OK”. Select “Apply” after all of the user changes have been made to the group.

Why is this problem important?

User groups are used to grant file permissions and access to other privileges on your system. Having incorrect users in groups will allow unauthorized users to access files and make changes on your computer.

Set a secure lockout threshold: 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 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.

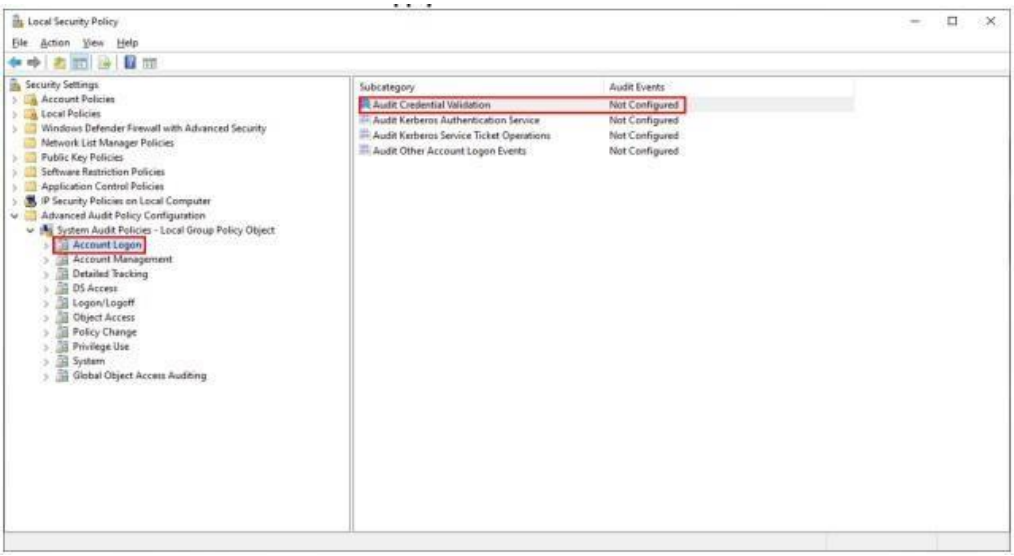
Set an Audit security policy: 5 pts.

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 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 → doubleclick 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.

Set User Account Control to prompt Admin Approval Mode: 5 pts.

How do I find this problem?

Open the “control panel” desktop app. In the menu select “System and Security”. Under “Security and Maintenance”, select “Change User Account Control Settings”. The slider is currently set to “Never Notify”.

How do I solve this problem?

Use the slider in “Change User Account Control Settings” from “Never Notify” to

“Always Notify”. Select “OK”, then “Yes”

Why is this problem important?

When User Account Control settings are set to “Always Notify”, administrators are prompted when performing tasks like changing windows settings and downloading new software.User accounts will be prompted and required to enter administrator account

credentials to change windows settings and download new software. This prevents local user accounts or unauthorized users from downloading malware or making changes to security settings that weaken your system.

Disable AutoPlay: 5 pts.

How do I find this problem?

Autoplay Policies can be found in the Local Group Policy editor. Select Administrative Templates > Windows Components > Autoplay Policies. The list of policies shows under “State” that the policies have not been configured.

How do I solve this problem?

In the list of settings in Autoplay Policies, select “Turn off Autoplay”. In the window that appears, select “Enabled”, then “Apply”.

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.

Firewall has been enabled: 5 pts.

How do I find this problem?

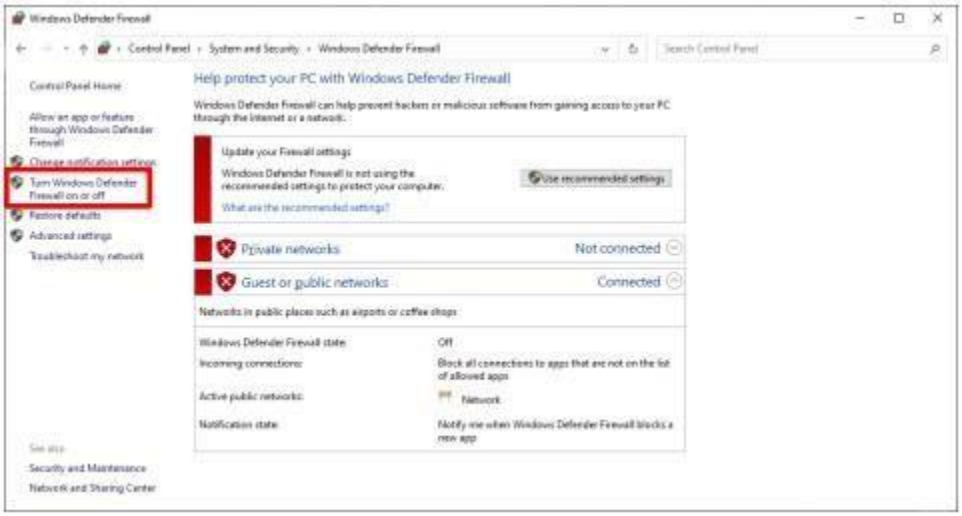
Turning on the firewall is a good cybersecurity practice to prevent unauthorized access to a system.

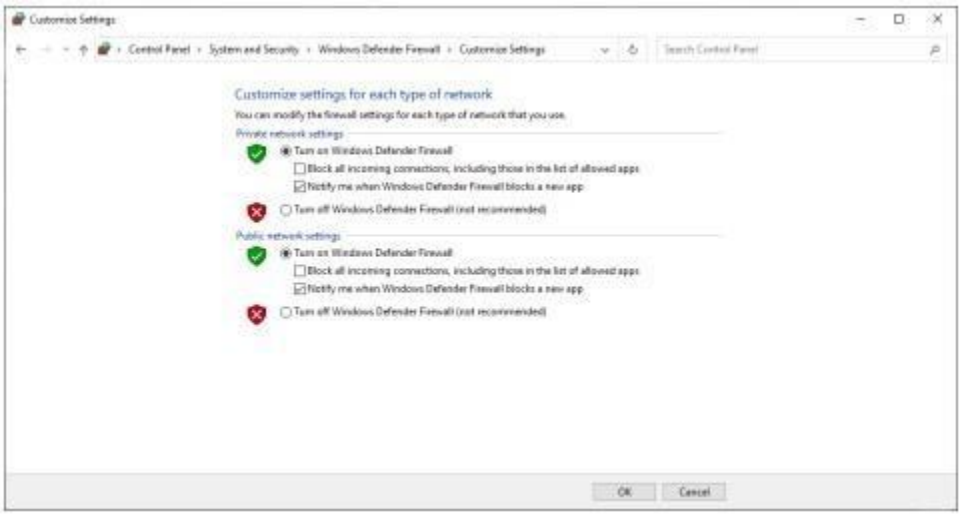
How do I solve this problem?

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.





Firefox has been updated: 5 pts

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 until it has updated to a version greater than 127.0.0

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.

Set Windows SmartScreen to warn or block: 5pts.

How do I find this problem?
In the Local Group Policy editor, select Administrative Templates → Windows Components → Windows Defender SmartScreen → Explorer. The option “Configure Windows Defender SmartScreen” is disabled.

How do I solve this problem?

Select “Configure Windows Defender SmartScreen”, “Enable”, and “Apply”. In “options:” select “Warn”. Go back and repeat this process with the settings for Microsoft Edge in Windows Defender Smartscreen settings. In the desktop search bar, enter “smartscreen” and select “App and Browser Control” (system settings).

Why is fixing this problem important?

Windows SmartScreen protects the system by preventing users from installing malicious software and visiting malicious websites while browsing. If it is configured to warn or block, it will notify users that a site/download is malicious or not allow them to download or visit the site.

Disable FTP 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 FTP 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.

Prohibited files have been removed: 5 pts.

How do I find this problem?

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.

How do I solve this problem?

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 → ashepard→ Music → right-click each MP3 file, and Select Delete.

Why is fixing this problem important?
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.

Unauthorized software has been removed: 5 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?
TeamViewer 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 TeamViewer and select Uninstall. TFTP server is also considered unauthorized software. Repeat this process to uninstall Open TFTP Server.

Why is fixing this problem important?

Removing unauthorized software is a best security practice.

Penalties

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.

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.

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

Why is this a penalty?

The ReadMe states that Thunderbird is required software for all users on this computer, as determined by the organization's management. Removing
Thunderbird from this computer is a violation of the organization's policy.