CyberPatriot Windows 10 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 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: 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 called "Forensics Question 1”.

- How do I solve this problem?

  This question asks you to research the Windows Elevation of Privilege vulnerability identified in CVE-2021-36934, and what privileges an attacker would have in this CVE? Looking up CVE-2021-36934 at the Microsoft Security Response Center, we see the attacker assumes SYSTEM privileges. Remember to **Save** and close the file.

- Why is fixing this problem important?

  This vulnerability impacts multiple versions of Windows 10, Windows 11 and Server 2019. If a non-admin user can access the Security Account Manager (SAM) database file, the hashed user and admin passwords stored in this file would allow an attacker to be able to install programs, create new user accounts, and delete data. It is important to research and learn about the latest techniques used to attack systems and protect those systems by installing security updates and patches.

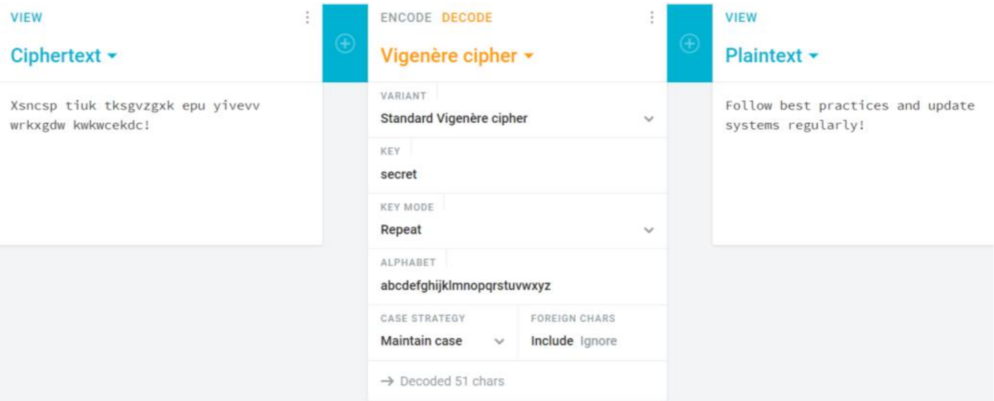
2) Forensics Question 2 Correct: 10 pts.

- 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 you to find the file cipher.txt under the user esbern. Open **File Explorer** by pressing the Windows key ⊞ on the keyboard + E → in the left-hand pane, select "This PC" → double-click on **Local Disk (C:)** → navigate to C:\Users\esbern\Documents → double-click "cipher.txt" → the hint tells it is a Vigenere cipher and the key is "secret" → use a website to decrypt the Vigenere cipher putting in "secret" as the key or passphrase the answer will show: **Follow best practices and update systems regularly!** → copy and paste this answer next to the "ANSWER:" in Forensics Question 2. Remember to **Save** and close the file.



```
Xsncsp tiuk tksgvzgxk epu yivevv
wrkxgdw kwkwcekdc!
```

VARIANT: Standard Vigenère cipher

KEY: secret

KEY MODE: Repeat

ALPHABET: abcdefghijklmnopqrstuvwxyz

CASE STRATEGY: Maintain case

FOREIGN CHARS: Include Ignore

→ Decoded 51 chars

```
Follow best practices and update
systems regularly!
```

- Why is fixing this problem important?

  During the competition, it is important to look for files on the image that can give you clues to the Forensic Questions or files that should be deleted following the scenario in the Readme. Always try to answer the Forensic Questions first before you delete files or make changes to the image.

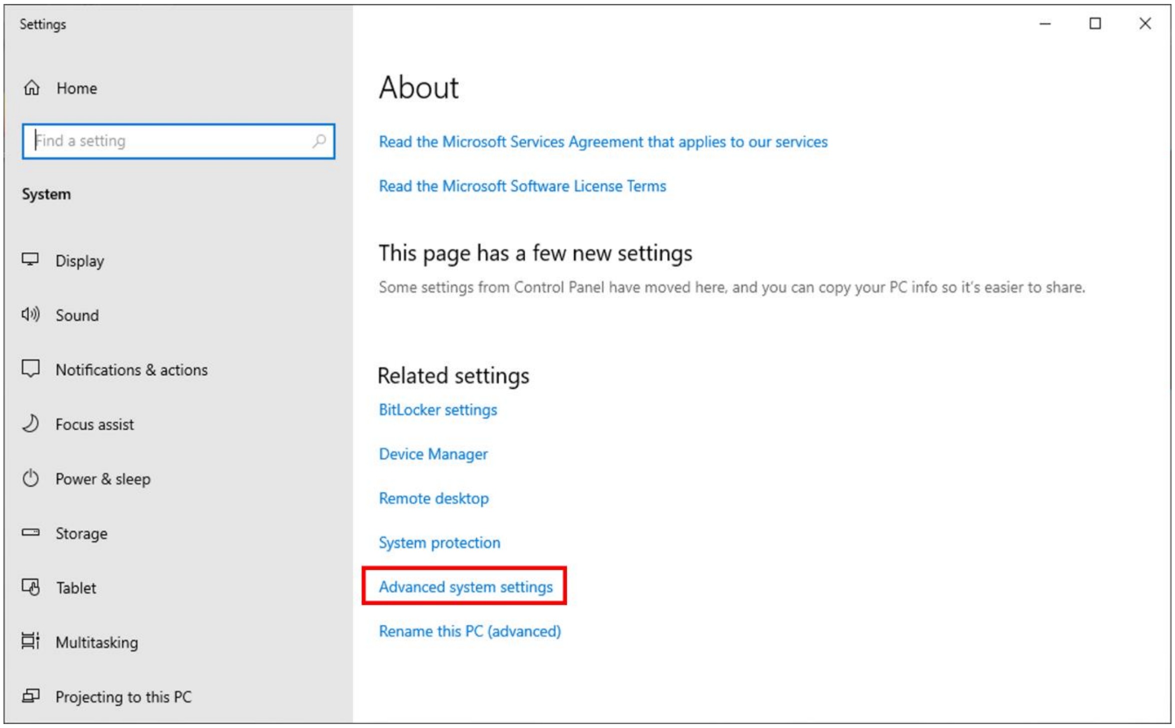
3) Forensics Question 3 Correct: 10 pts.

- 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 called "Forensics Question 3".

- How do I solve this problem?

  This question asks for the Workgroup name of the image. In the search box, type **workgroup**. Select "Show which **workgroup** this computer is on." Scroll until you see **Related Settings** and select **Advanced system settings**. Select **Computer Name**. You will see **DRAGONBORN** next to Workgroup.



About

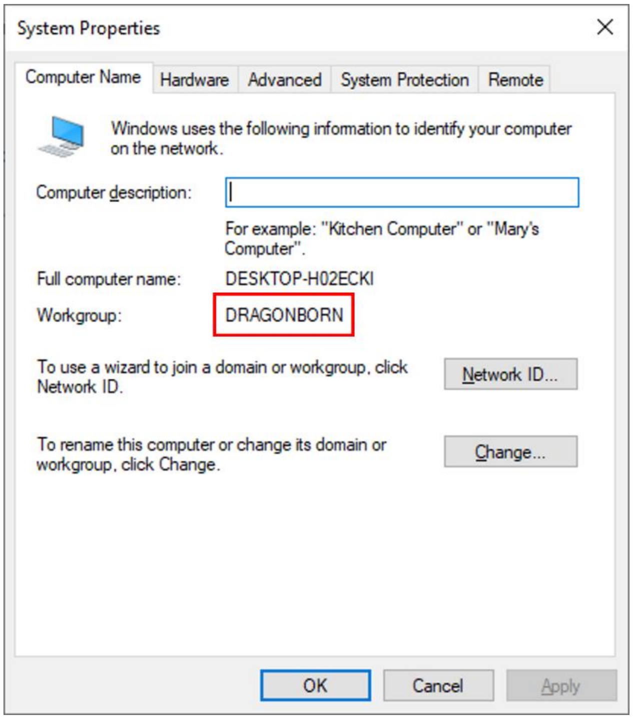
Read the Microsoft Services Agreement that applies to our services

Read the Microsoft Software License Terms

This page has a few new settings

Some settings from Control Panel have moved here, and you can copy your PC info so it's easier to share.

Related settings



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: DESKTOP-H02ECKI

Workgroup: DRAGONBORN

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

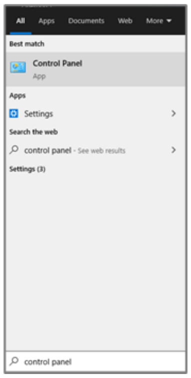
Type **DRAGONBORN** next to “Answer” in Forensics Question 3. Remember to **<u>Save</u>** and close the file.

- <u>Why is fixing this problem important?</u>
  Workgroups are used in peer-to-peer local area networks or for small businesses to share resources within the Workgroup. Each computer name should be unique in the workgroup. As the Administrator, you need to ensure your small network is secure. Know all the computers connecting within the workgroup and make sure they have the latest updates.

4) Unauthorized user account has been removed: 4 pts. each

- How do I find this problem?

  One of the first things you should do when starting an image during a competition is check the README file on the desktop. There, you will see the authorized users for the image. These are the only users that should have an account. All others should be removed.



- How do I solve this problem?

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

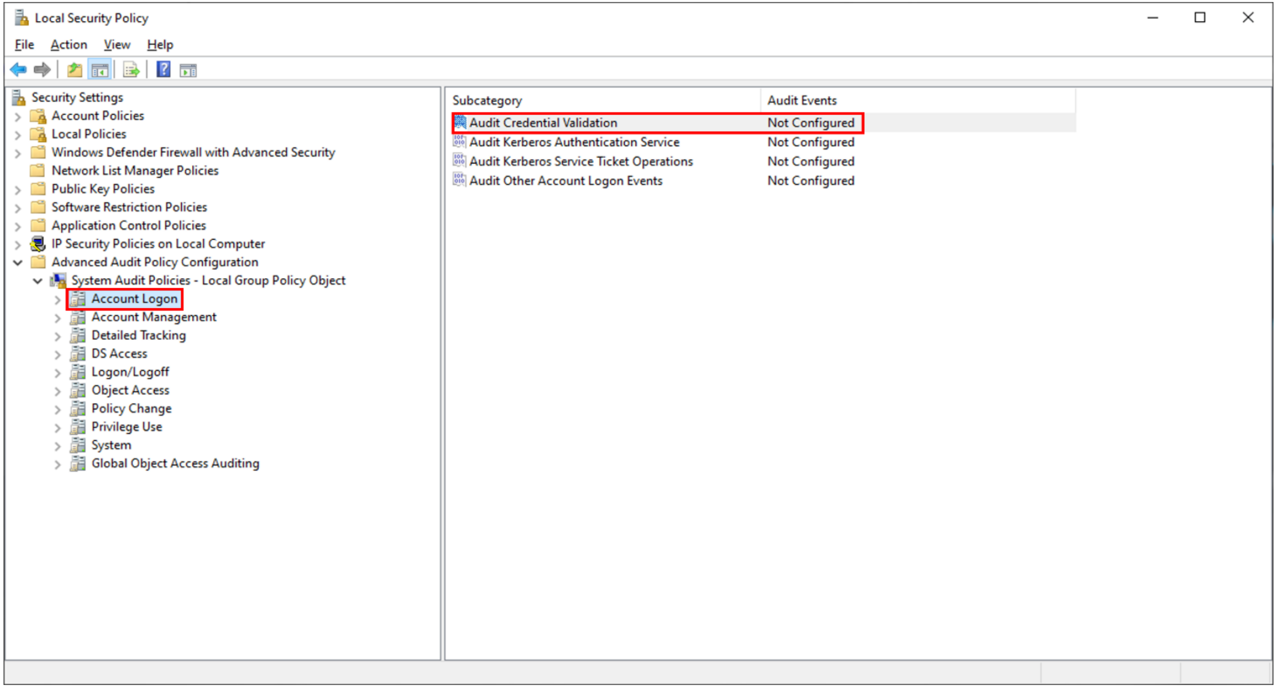
5) Set an Audit security policy: 5 pts.

- How do I find this problem?

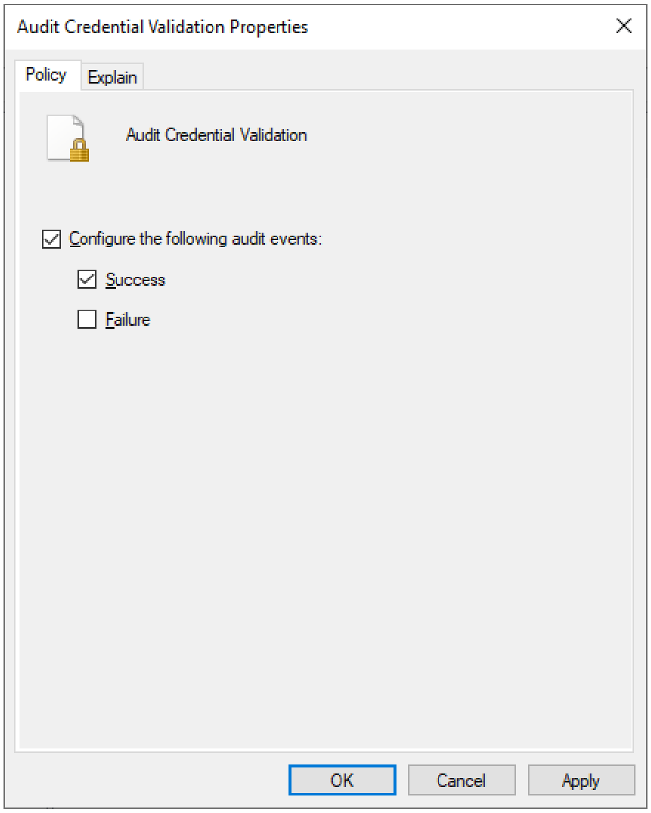
  Security settings in the Local Security Policy allow the administrator to set Account Policy, Audit Policy, User Rights Assignment and other security settings.

- How do I solve this problem?

  Press the Windows key ⊞ + R → type "**secpol.msc**" without the quotes → expand **Advanced Audit Policy Configuration** → expand **System Audit Policies** → double-click **Account Logon** → double-click **Account Credential Validation** → check the **Configure the following audit events** box → select **Success** → select **Apply** → select **OK**.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
System Audit Policies - Local Group Policy Object
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing

Subcategory	Audit Events
Audit Credential Validation	Not Configured
Audit Kerberos Authentication Service	Not Configured
Audit Kerberos Service Ticket Operations	Not Configured
Audit Other Account Logon Events	Not Configured



Audit Credential Validation Properties

Audit Credential Validation

☑ Configure the following audit events:

☑ Success

☐ Failure

- 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 those credentials. For domain accounts, the domain controller 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.

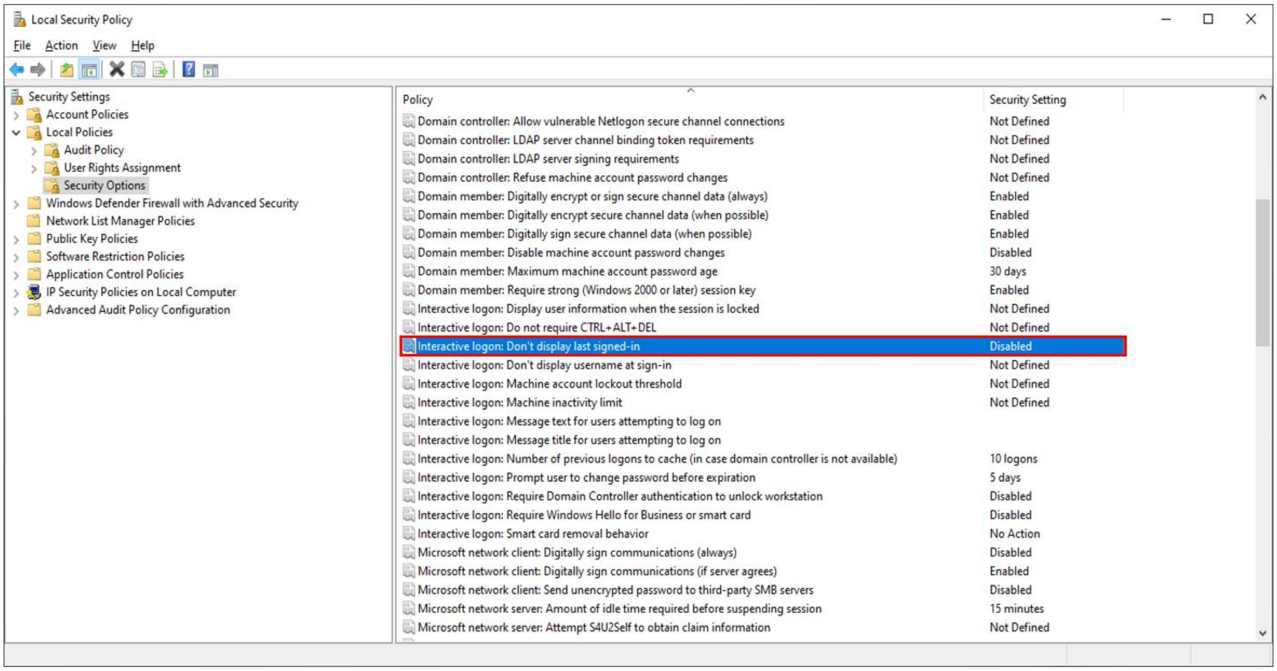
6) Set a security policy: 5pts.

- How do I find this problem?

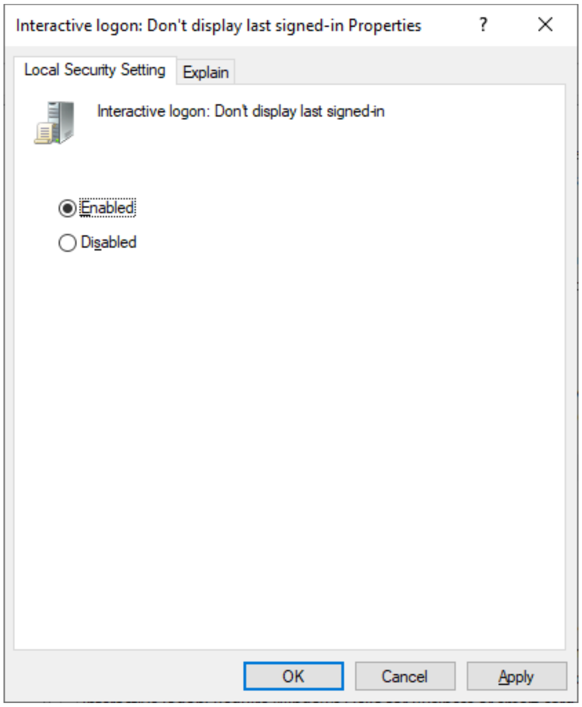
  Security settings in the Local Security Policy allow the administrator to set Account Policy, Audit Policy, User Rights Assignment and other security settings.

- How do I solve this problem?

  Press the Windows key ⊞ **+ R** → type "**secpol.msc**" without the quotes → expand **Local Policies** → double-click **Security Options** → scroll down until you find **Interactive logon: Don't display last signed-in** and double-click → select **Enabled** → select **Apply** → select **OK.**


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Domain controller: Allow vulnerable Netlogon secure channel connections	Not Defined
Domain controller: LDAP server channel binding token requirements	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Display user information when the session is locked	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Don't display last signed-in	Disabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require Windows Hello for Business or smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined



Interactive logon: Dont display last signed-in

● Enabled

○ Disabled

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

  This security setting determines whether the name of the last user to log on to the computer is displayed in the Windows logon screen. If this policy is enabled, the name of the last user to successfully log on is not displayed in the Logon Screen. If this policy is disabled, the name of the last user to log on is displayed.

  If this setting is not enabled, a malicious user who has access to the console can leverage the username as part of a password guessing attack.

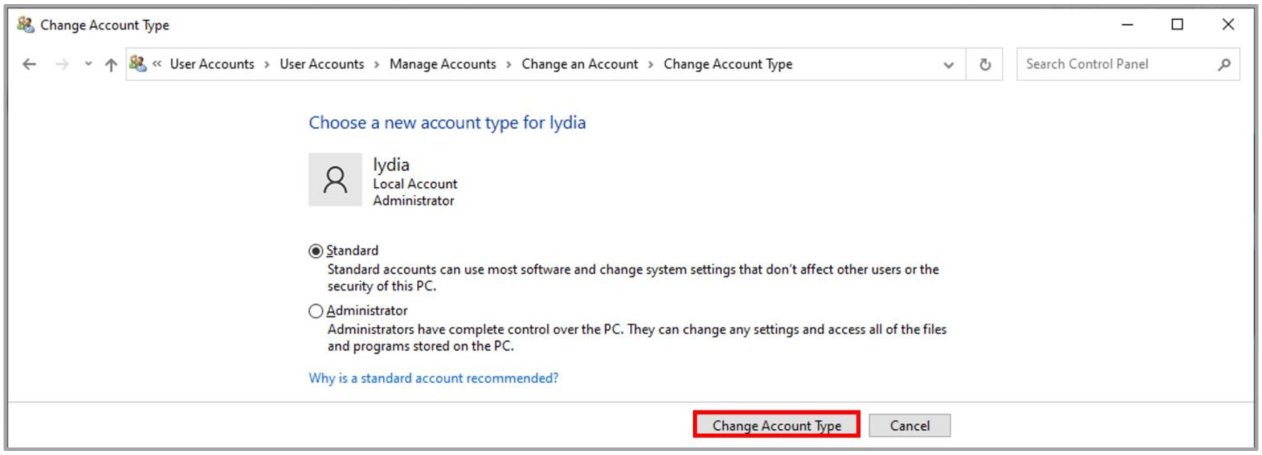
7) Administrator account has been changed to Standard User: 4 pts.

- How do I find this problem?

  One of the first things you should do when starting an image during a competition is check the README file on the Desktop. The README contains authorized users for the image and the account type for each user.

- How do I solve this problem?

  In the search box, type and select **Control Panel.** Click on **User Accounts** → **User Accounts** → **Manage another account**. Find the users that have an Administrator account who is listed only as a Standard user in the README file. Select **Change the account type** → select **Standard User** → select **Change Account Type.**


Change Account Type
« User Accounts › User Accounts › Manage Accounts › Change an Account › Change Account Type
Search Control Panel
Change Account Type
Cancel

Choose a new account type for lydia

lydia
Local Account
Administrator

● Standard
Standard accounts can use most software and change system settings that don't affect other users or the security of this PC.

○ Administrator
Administrators have complete control over the PC. They can change any settings and access all of the files and programs stored on the PC.

Why is a standard account recommended?

  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.

8) Disable Simple TCP/IP service: 5 pts.

- How do I find this problem?
  Disabling insecure or unnecessary services is a good cybersecurity practice in general.

- How do I solve this problem?

  In the Search box, type **Control Panel**. Select **Programs** → select **Programs and Features** → in the left-hand pane, select **Turn Windows features on or off** → scroll down and uncheck **Simple TCPIP services** → select **OK** → at the Windows Features prompt, select **Restart now**.

- Why is fixing this problem important?

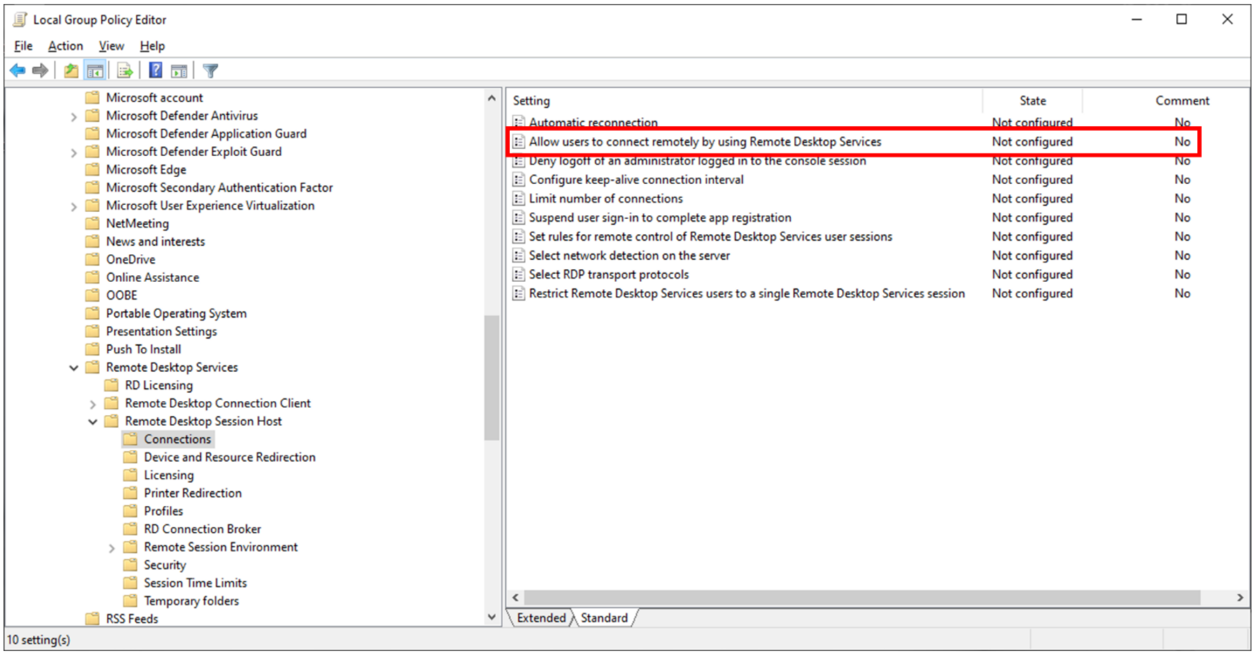
  Disabling unnecessary services decreases the attack surface of a system. The vulnerabilities in this service could allow for Denial of Service (DoS) attacks.

9) Remote desktop sharing is turned off: 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?

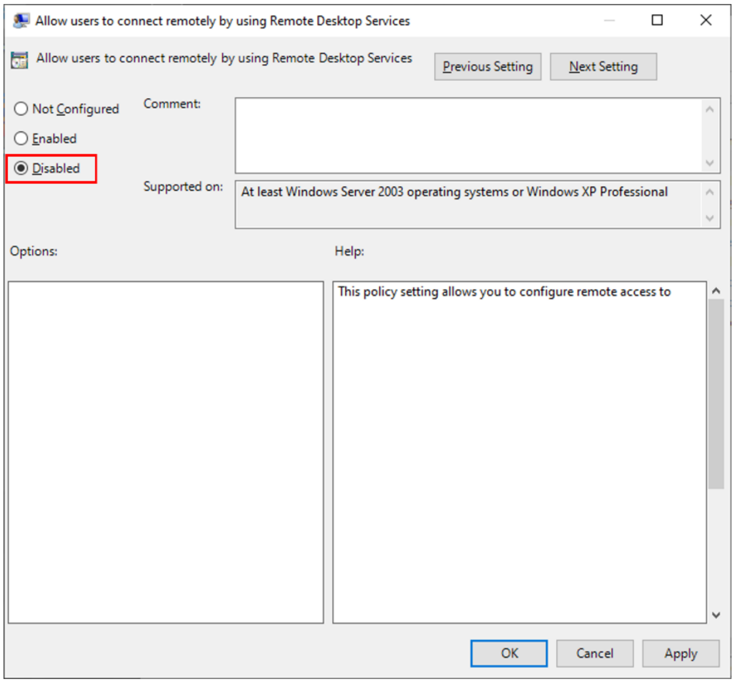
  In the Search box, type **gpedit.msc**. Expand **Computer Configuration** → expand **Administrative Templates** → expand **Windows Components** → expand **Remote Desktop Services** → expand **Remote Desktop Session Host** → double-click on **Connections** → double-click on **Allow Users to connect remotely by using Remote Desktop Services** → select **Disabled** → select **Apply** → select **OK**.



Microsoft account
Microsoft Defender Antivirus
Microsoft Defender Application Guard
Microsoft Defender Exploit Guard
Microsoft Edge
Microsoft Secondary Authentication Factor
Microsoft User Experience Virtualization
NetMeeting
News and interests
OneDrive
Online Assistance
OOBE
Portable Operating System
Presentation Settings
Push To Install
Remote Desktop Services
RD Licensing
Remote Desktop Connection Client
Remote Desktop Session Host
Connections
Device and Resource Redirection
Licensing
Printer Redirection
Profiles
RD Connection Broker
Remote Session Environment
Security
Session Time Limits
Temporary folders
RSS Feeds

Setting	State	Comment
Automatic reconnection	Not configured	No
Allow users to connect remotely by using Remote Desktop Services	Not configured	No
Deny logoff of an administrator logged in to the console session	Not configured	No
Configure keep-alive connection interval	Not configured	No
Limit number of connections	Not configured	No
Suspend user sign-in to complete app registration	Not configured	No
Set rules for remote control of Remote Desktop Services user sessions	Not configured	No
Select network detection on the server	Not configured	No
Select RDP transport protocols	Not configured	No
Restrict Remote Desktop Services users to a single Remote Desktop Services session	Not configured	No

10 setting(s)


Allow users to connect remotely by using Remote Desktop Services
Previous Setting
Next Setting

Allow users to connect remotely by using Remote Desktop Services

○ Not Configured
○ Enabled
● Disabled

Comment:

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options:

Help:

This policy setting allows you to configure remote access to

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

  Remote Desktop allows the user and potential attackers to connect to the computer remotely over a network connection. Disabling unnecessary services decreases the attack surface of a system.

10) All user accounts are password protected: 4 pts. each

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

  Password protecting all user accounts is good cybersecurity practice in general.

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

  In the Search box, type **Control Panel**. Click on **User Accounts** → **User Accounts** → **Manage another account**. Click on any of the user accounts that do not have passwords. On this page, select "Create a password." You can then create a password for that user. Make sure it's a strong, secure one! Do this for all users <u>**except dovahkiin**</u> (so you can log back in if you don't write down the new password). Make sure you **create or change insecure** passwords in all images and <u>**write down the username and new password.**</u>

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

  Not having a password on an account makes it extremely vulnerable to attacks by outside individuals. Without a password, an attacker can access the user account easily. Secure passwords are highly recommended as a deterrent to potential attackers.

11) Enforce a password history policy: 3 pts.

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

  Enforcing a password history policy is a good cyber security practice that administrators should implement.

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

  Press the Windows key ⊞ + R → type "secpol.msc" → **OK** → select **Account Policies** → select **Password Policy** → double-click on **Enforce password history** → type "10" in the password remembered text box and select **OK**.

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

  It is important to enforce a password history policy, so users won't reuse the same passwords again. Reusing a password gives the malicious user more time to obtain the users password via a brute force method.

12) Prohibited files have been removed: 3 pts. each

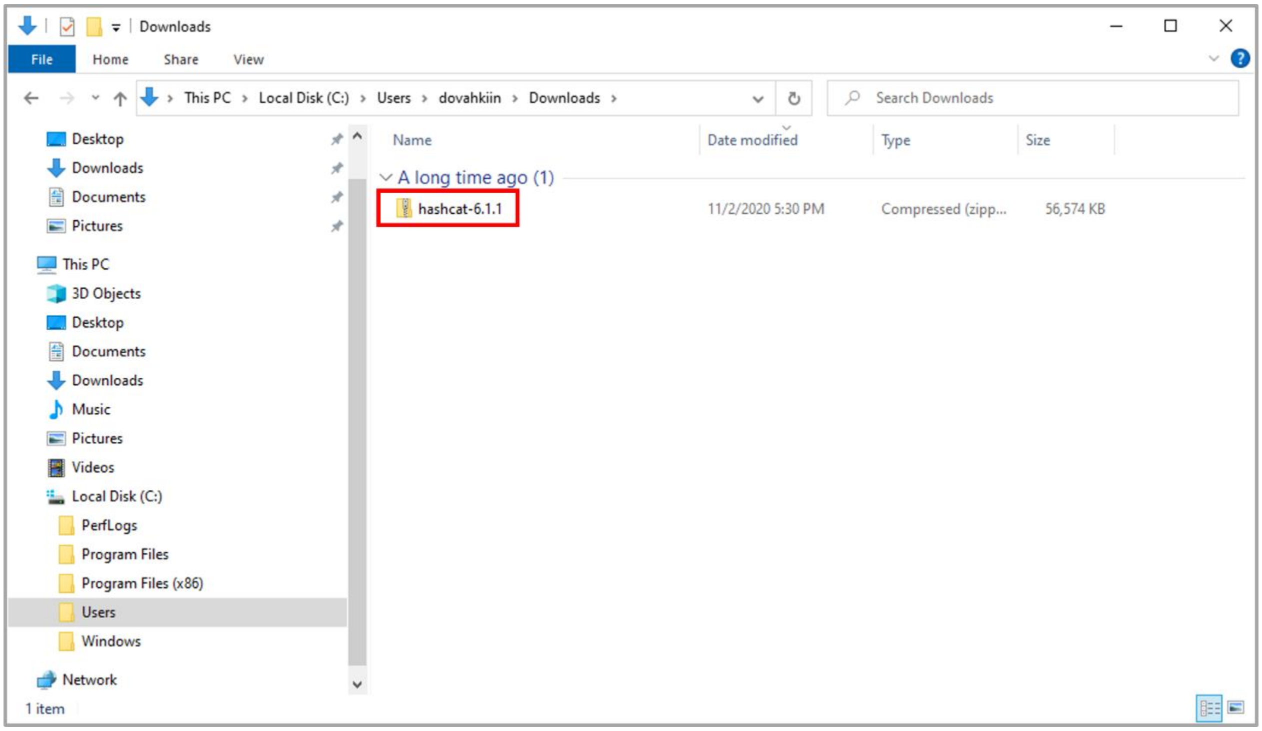
- <u>How do I find this problem?</u>

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

- How do I solve this problem?

  Open File Explorer or press the Windows Key ⊞ + E. Select **Local Disk (C:) → Users → esbern → Documents → cipher.txt**. Select **Delete**.

  Hashcat is considered unauthorized software and should be removed from the image. Open File Explorer or press the Windows Key ⊞ + E. Select **Local Disk (C:) → Users → dovahkiin → Downloads → hashcat-6.1.1**. Select **Delete**.



Name	Date modified	Type	Size
hashcat-6.1.1	11/2/2020 5:30 PM	Compressed (zipp...	56,574 KB

- 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.

13) A password of at least <u>10</u> characters is required: 3 pts.

- How do I find this problem?

  Enforcing use of longer passwords is a good cybersecurity practice in general.

- How do I solve this problem?

  Press the Start icon and double-click on **Control Panel**. Select **Administrative Tools → Local Security Policy → Account Policies →Password Policy → Minimum password length**. In this window, you can set the number of characters for passwords to 10 or above.

- Why is fixing this problem important?

  Setting a password policy ensures that all users on the system must set a secure password. By setting a minimum password length, IT administrators force users to create more secure passwords.

14) **Required software has been updated: 5 pts. each**

- How do I find this problem?

  The Readme lists Firefox as required software.

- How do I solve this problem?

  Ensure you have selected automatic updates for programs or select Check for Updates frequently. You may also download and install the latest versions from the developer website.

- Why is fixing this problem important?

  Installing the latest versions of software is a best security practice to protect against cyberthreats.

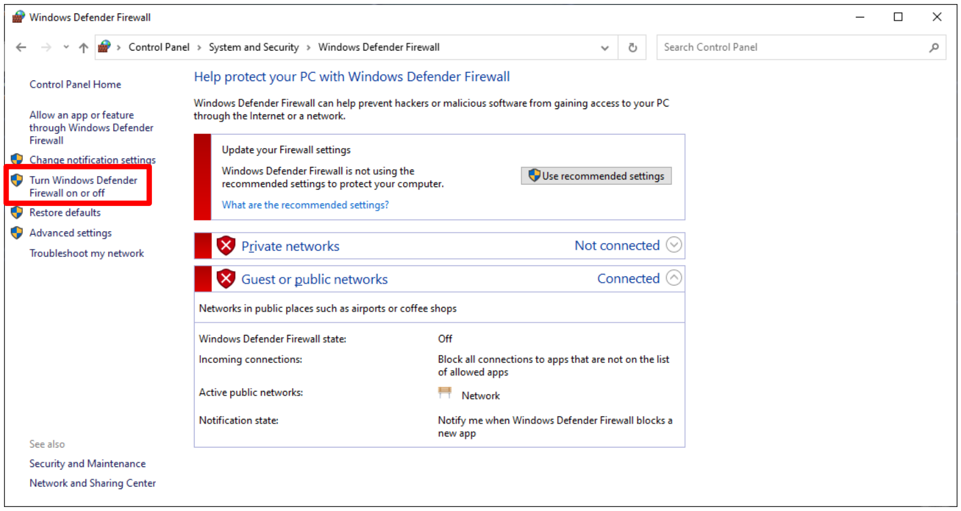
15) **Firewall has been enabled: 5 pts.**

- 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**.



Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center
Use recommended settings

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

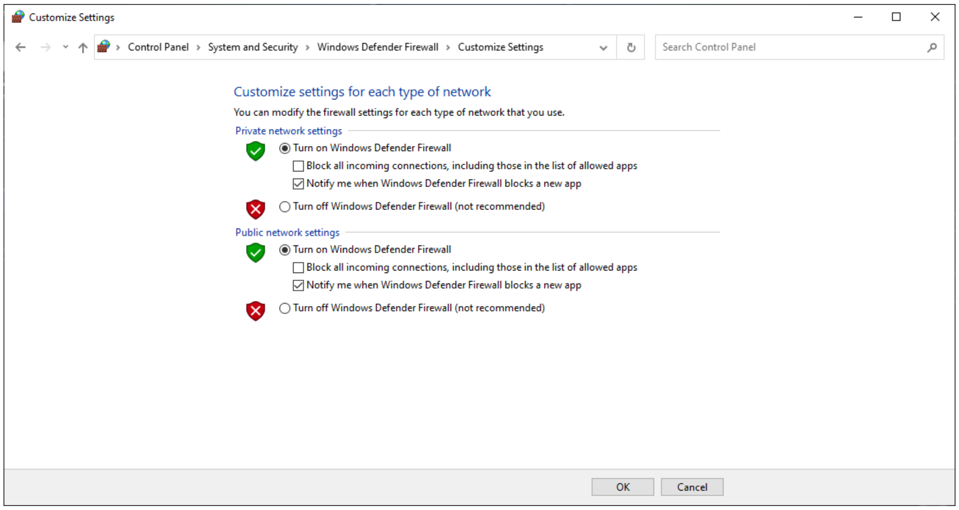
What are the recommended settings?

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	Off
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Network
Notification state:	Notify me when Windows Defender Firewall blocks a new app



Customize Settings
Control Panel › System and Security › Windows Defender Firewall › Customize Settings
Search Control Panel
OK
Cancel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Public network settings

● Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

- 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.

16) Unauthorized software has been removed: 4 pts.

- How do I find this problem?

  The README file states that unauthorized software is prohibited on this image.

- How do I solve this problem?

  Nmap 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 **Nmap 7.91** and select **Uninstall**.

- Why is fixing this problem important?

  Removing unauthorized software is a best security practice.

Penalties

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