Udacity Cybersecurity Course #1 Project

Contents

Learning Objectives:

- Explain security fundamentals including core security principles, critical security controls, and cybersecurity best practices.
- Evaluate specific security techniques used to administer a system that meets industry standards and core controls
- Assess high-level risks, vulnerabilities and attack vectors of a sample system
- Explain methods for establishing and maintaining the security of a network, computing environment, and application.

Student Information

Student Name: **Shaden Alsahali**

Date of completion: 14 Oct 2022

Scenario

Congratulations!

You have been hired to secure the PC used at your friend's business: Joe's Auto Body. Joe provides car repair services throughout the tri-state area. He's had previous employees use it for activities un-related to work (e.g., web browsing, personal email, social media, games, etc.) and he now uses it to store his critical business information. He suspects that others may have broken into it and may be using it to transfer files across the internet. He has asked that you secure it for him according to industry best practices, so it can be once again used as a standard PC.

You will be given access to a virtual image of Joe's Auto Body's PC. It's a copy of the actual computer operating system in use that will be transferred to Joe's computer once you are done.

This template provides you with the high-level steps you'll need to take as part of securing a typical computer system. For each step, use the virtual Windows 10 PC to answer the questions and challenges listed in this project. You'll also need to explain how you got the answers and provide screenshots showing your work.

It's important that you read through the entire document before securing the system and completing this report.

To start, you need to login to the virtual PC. You can use Joe's account using the user-id and password below. You may also use any other account on the PC.

Account Name: JoesAuto
Password: @UdacityLearning#1

1. Reconnaissance

The first step in securing any system is to know what it is, what's on it, what it's used for and who uses it. That's the concept of systems reconnaissance and asset inventory. In this step, you'll document the hardware, software, user access, system and security services on the PC.

Complete each section below.

Hardware

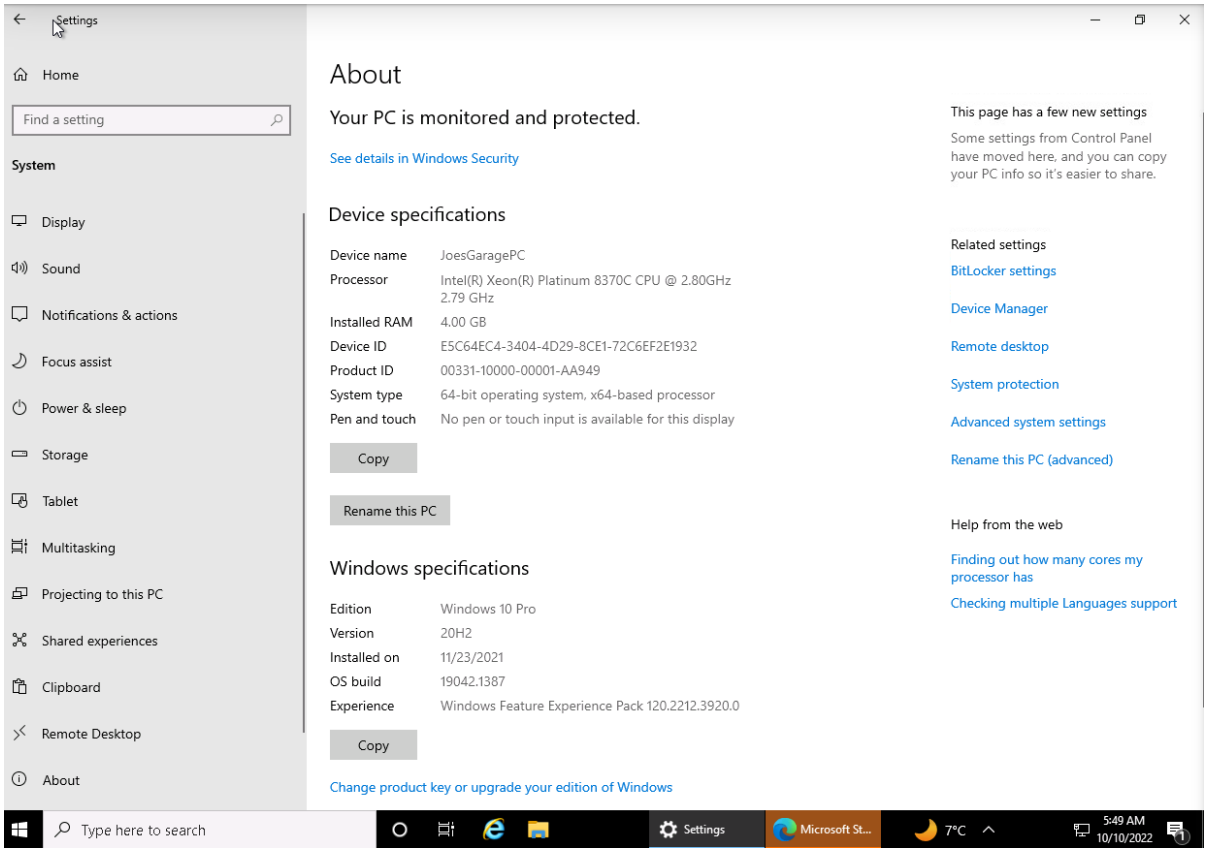
1. *Fill in the following table with system information for Joe's PC.*

Device Name	**JoesGaragePC**
Processor	**Intel(R) Xeon(R)Platinum 8370C CPU @2.80GHz 2.79 GHz**
Install RAM	**4.00 GB**
System Type	**64-bit operating system,64-based processor**
Windows Edition	**Windows 10 Pro**
Version	**20H2**
Installed on	**11/23/2021**
OS build	**19042.1387**

2. *Explain how you found this information:*

Go to setting About you can find all the related information for this PC.

3. *Provide a screenshot showing this information about Joe's PC:*



Software

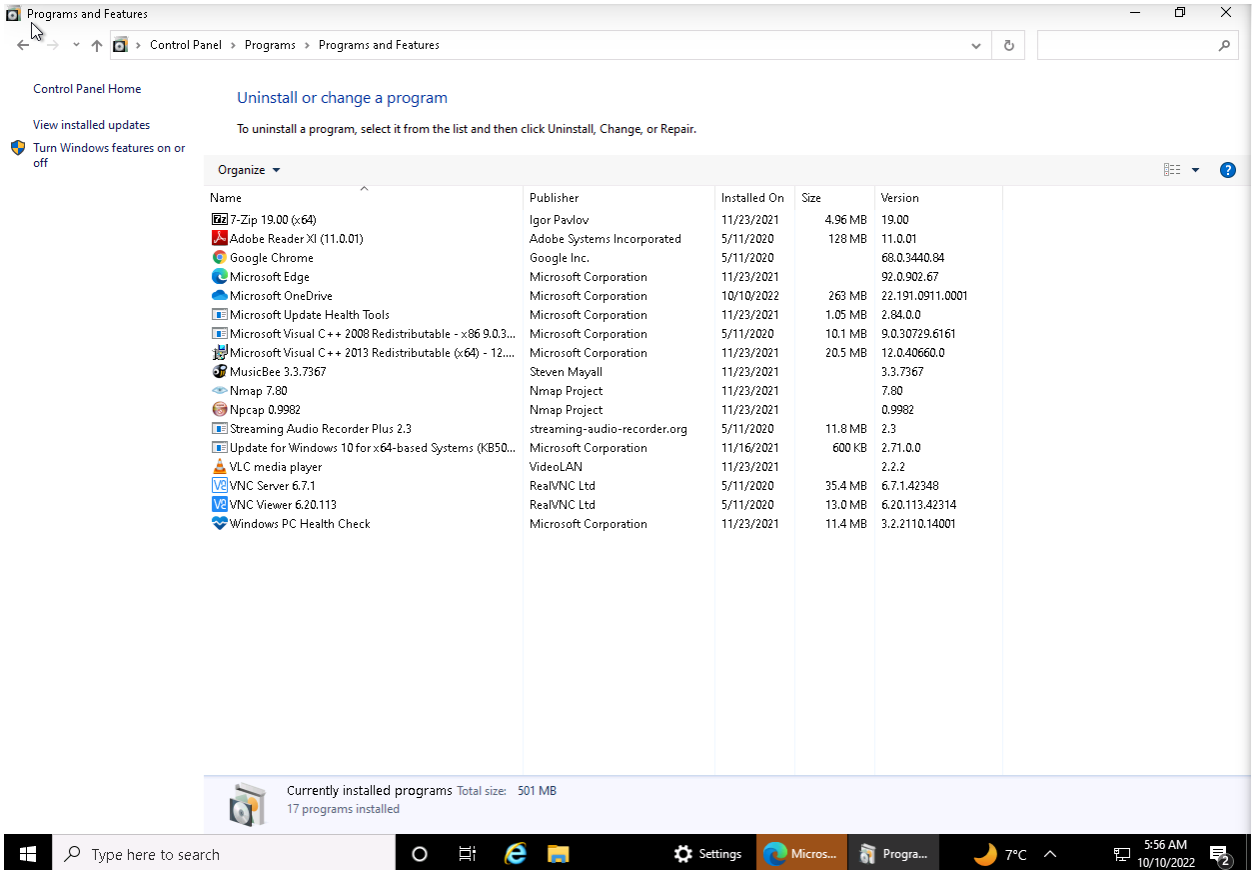
Another common early step in securing is taking an inventory of software or applications installed on a computer system. These are programs outside of the standard operating system.

1. *List at least 5 installed applications on Joe's computer:*

- **7-Zip 19.00 (x64)**
- **Nmap 7.80**
- **Npcap 0.9982**
- **Google Chrome**
- **Microsoft Edge**

2. *Explain how you found this information. Provide screenshots showing this information.*

Go to Control Panel Programs Programs and Features you will find a list of all the programs in the PC.



3. *The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?*

Inventory and control of the software assets.

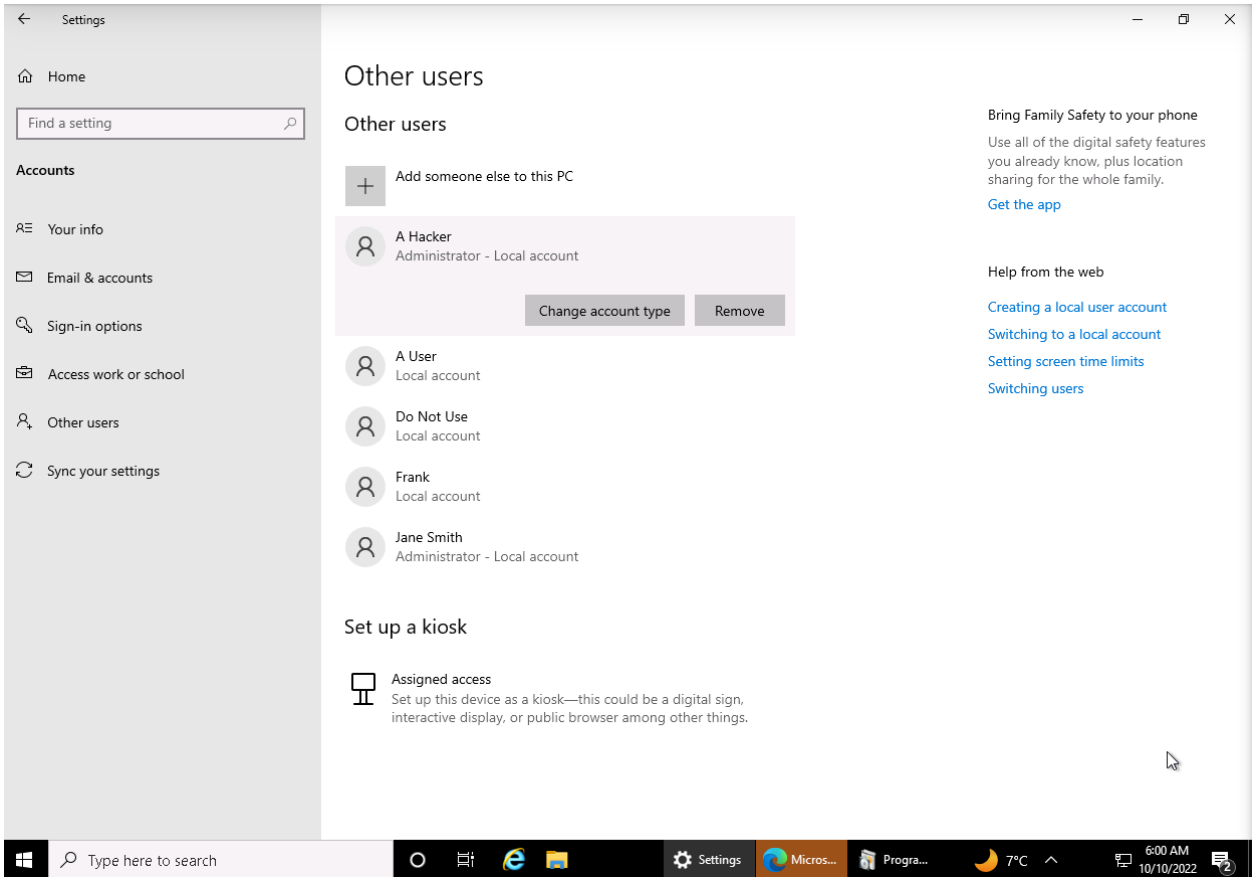
Accounts

As part of your security assessment, you should know the user accounts that may access the PC.

1. *List the names of the accounts found on Joe's PC and their access level.*

Account Name	**Full Name**	**Access Level**
Frank	Frank	Local account -Standard
Do Not Use	Do Not Use	Local account -Standard
A User	A User	Local account -Standard
A Hacker	A Hacker	Administrator -Local account
Jane Smith	Jane Smith	Administrator -Local account

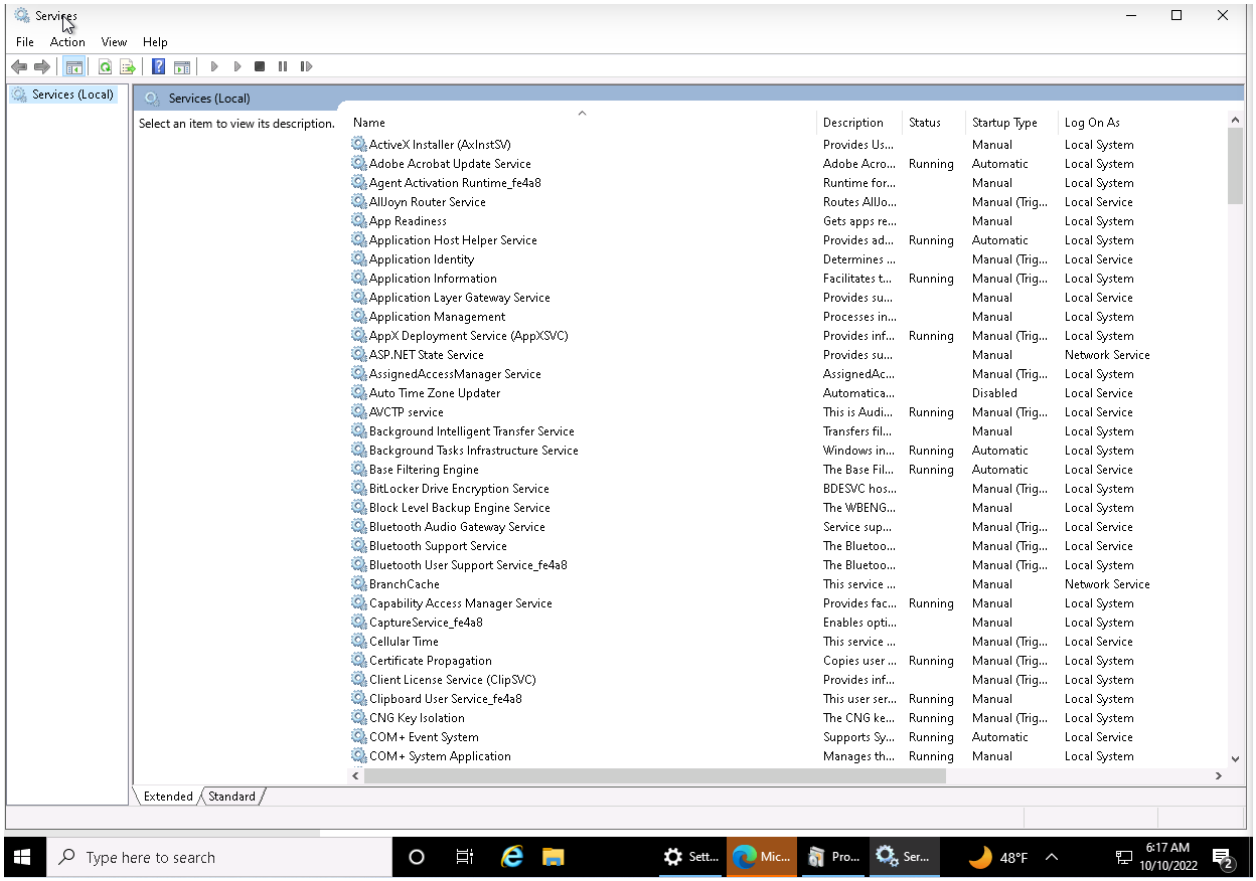
2. *Provide a screenshot of the Local Users.*



Services

Services are applications often running in the background. Most of them provide needed functionality for the PC. Some may also be used to violate security policies.

1. *Provide a screenshot of the services running on this PC.*

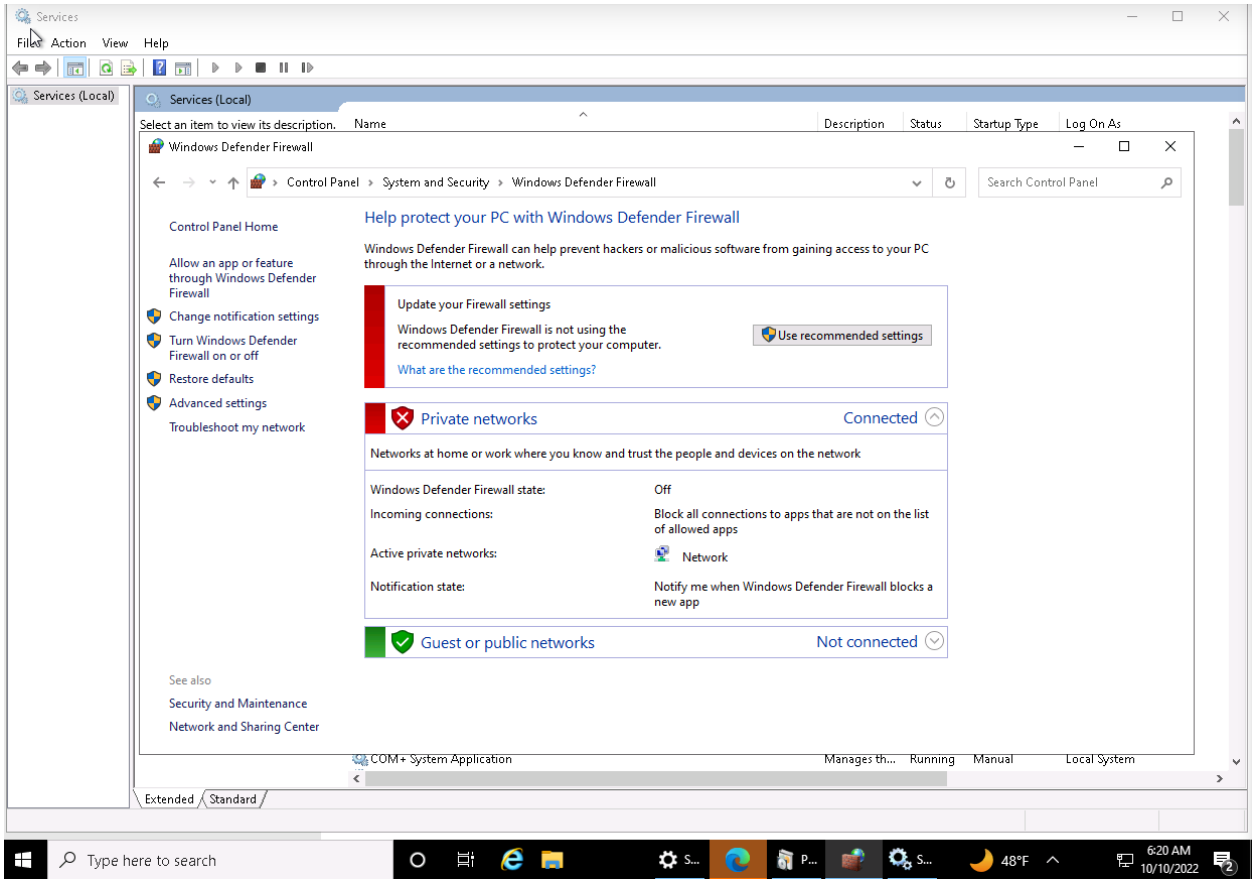


Security Services

Joe wants to ensure that standard security services are running on his PC. He's content with using default Windows security settings and applications except for the rules outlined later. **Reminder that at this point you are just reporting what you observe. Do not make any changes to security settings yet.**

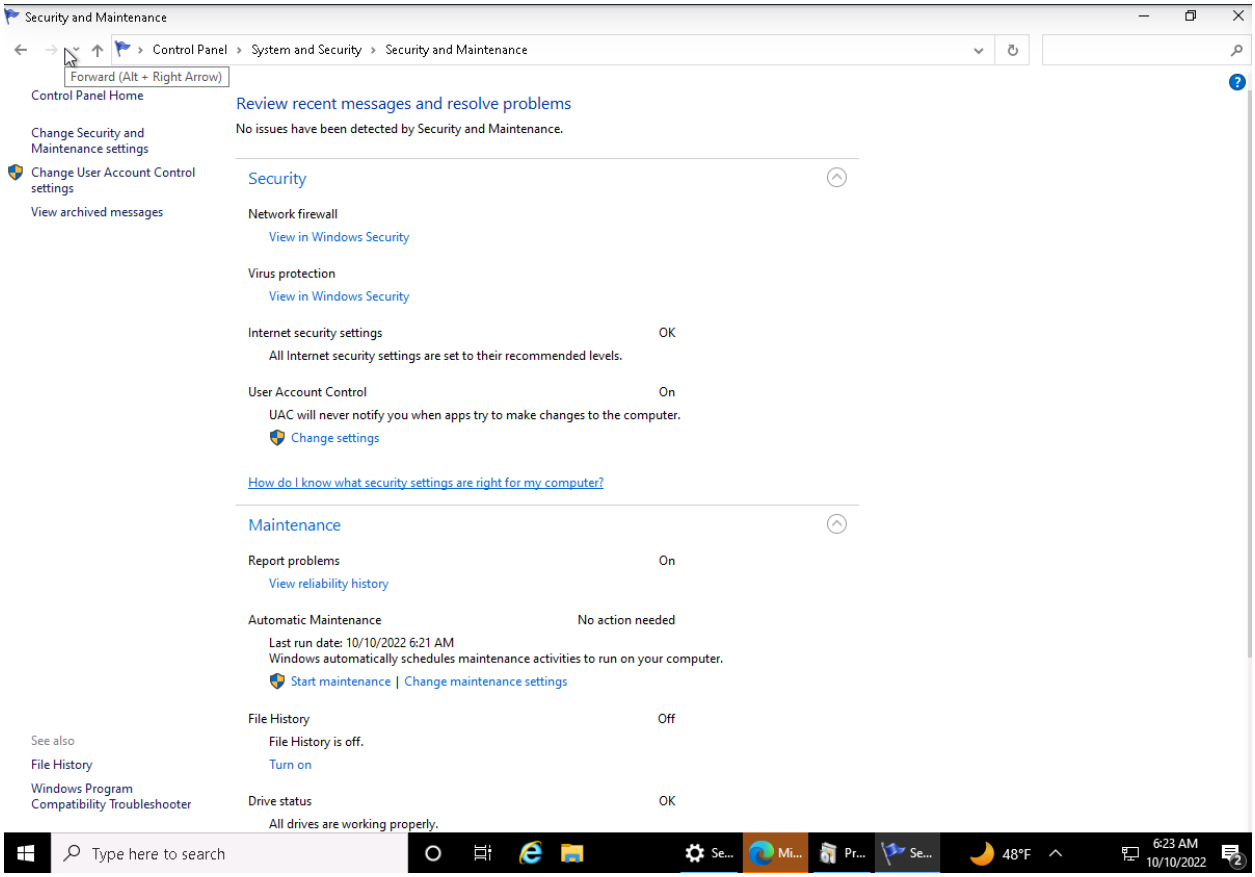
1. *To view a summary of security on Windows 10, start from the **Control Panel**. Use the "Find a setting" bar and search on Windows Defender. You can also search for Windows Defender using the Windows Run bar.*

Take a screenshot of what you see on the Windows Security screen and include it here:

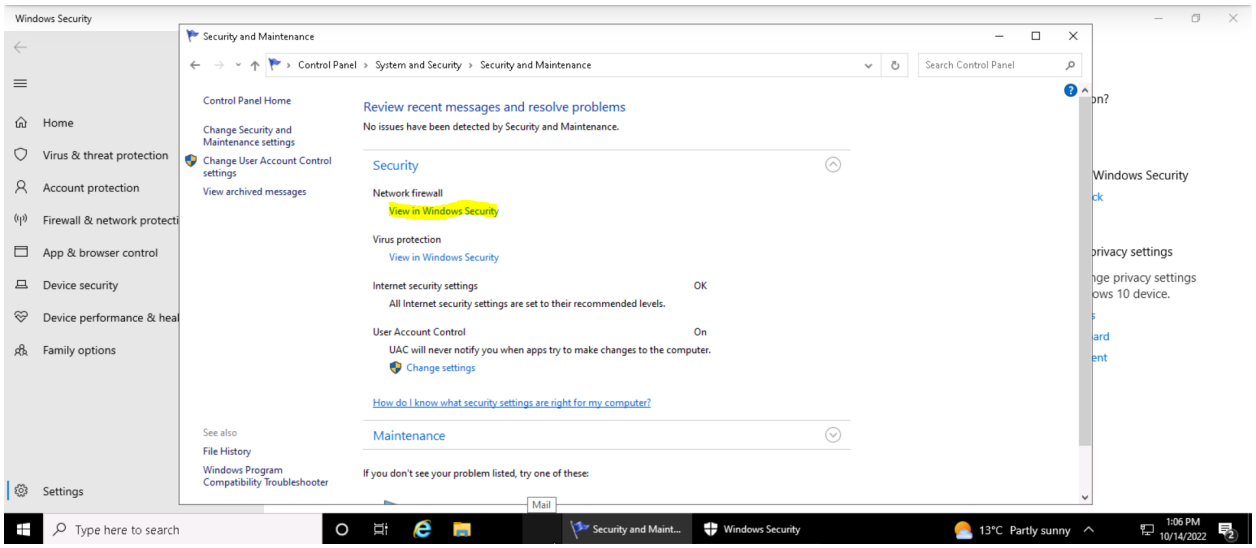


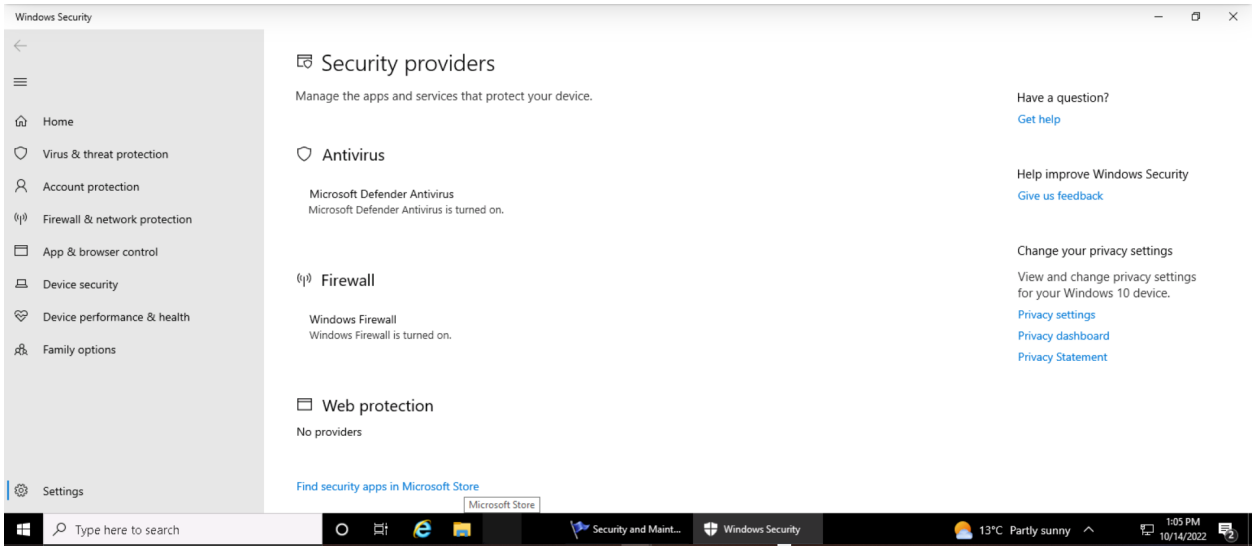
2. *The Windows 10 Security settings are also found from the* ***Control Panel > System and Security > Security and Maintenance****. Start by viewing* ***"Review your computer's status and resolve***

issues." *Provide a screenshot of this below:*

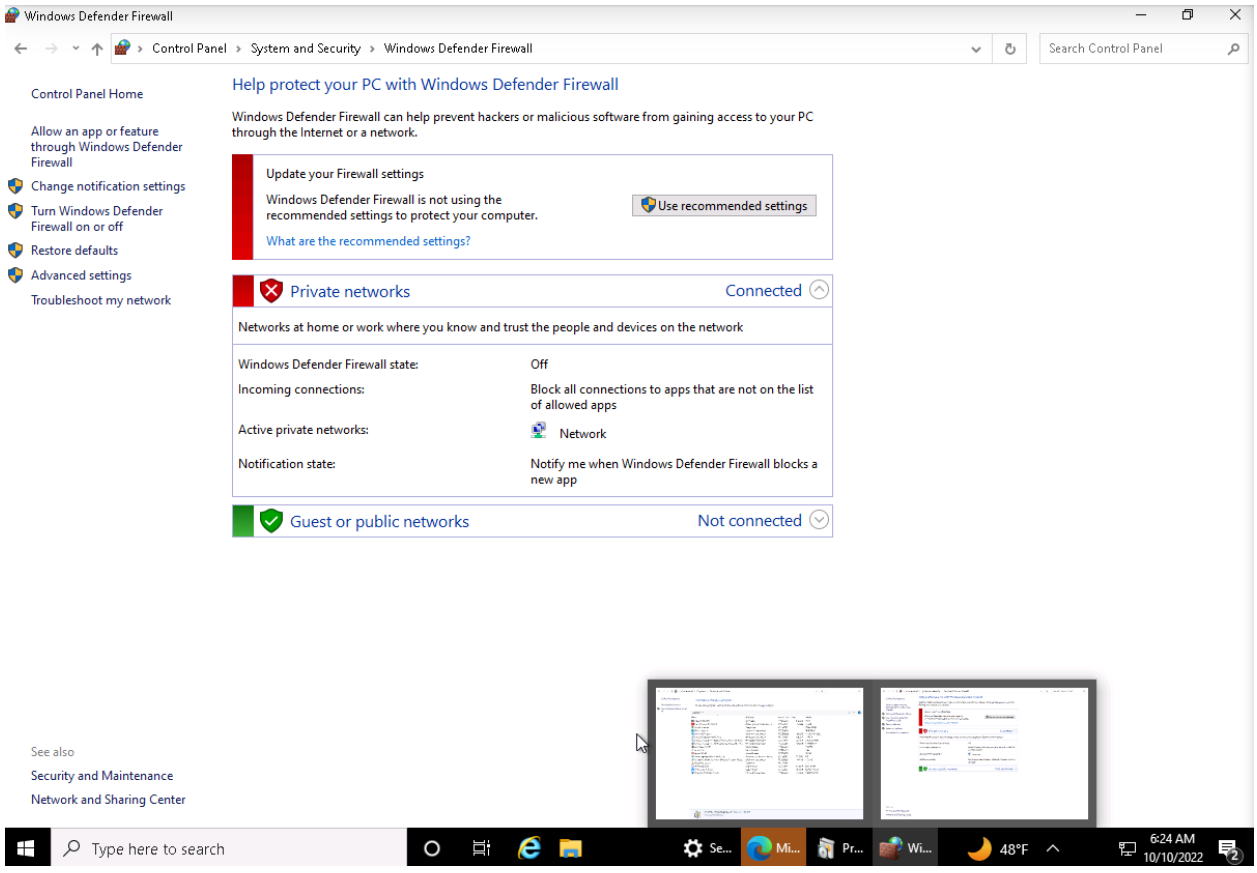


3. *Click on View in Windows Security to see the status there. Provide a screenshot of the* ***Firewall*** *settings.*

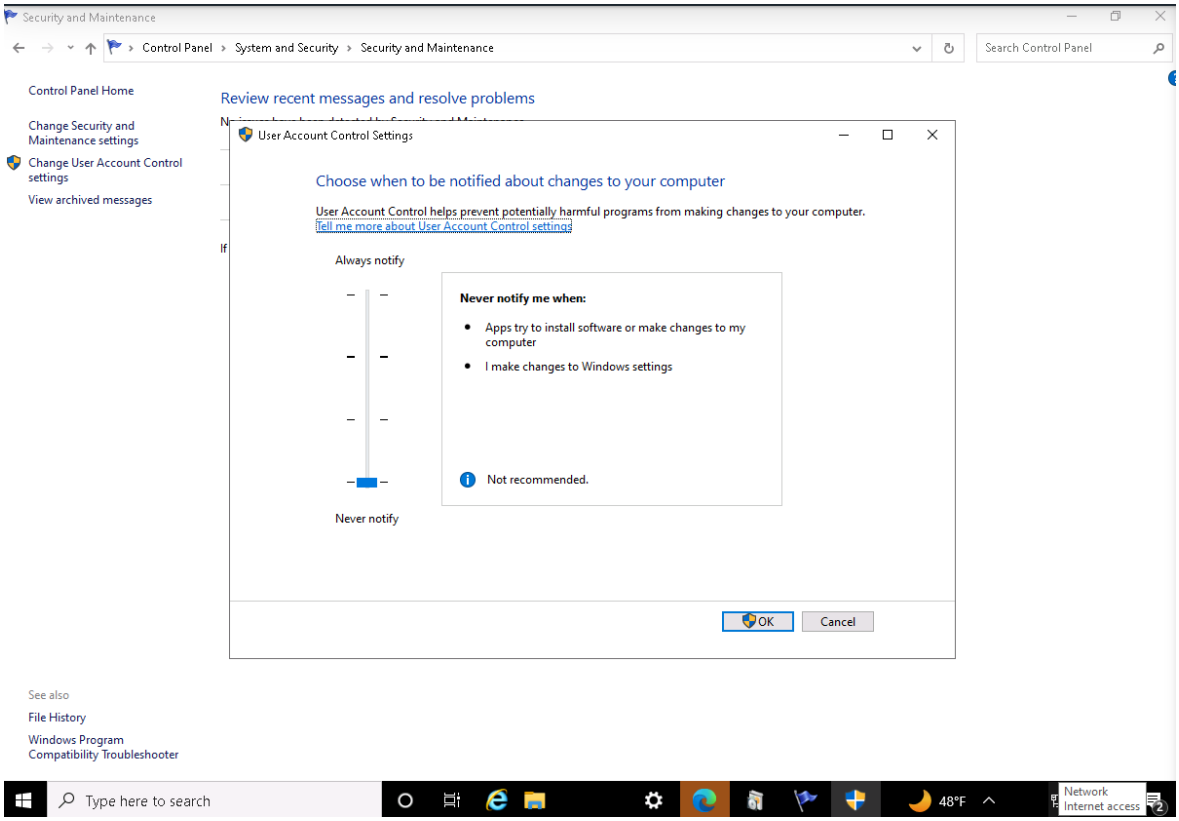




4. *From the **Control Panel**, go to **System and Security**. In that window, select **Windows Defender Firewall**. Provide a screenshot of it here:*



5. *PC users should be notified whenever there is a security or maintenance message. In the Security & Maintenance window, click on Change Security and Maintenance settings and take a screenshot. Paste it here:*



6. *Document the status of the PC's security settings listed below. Include the process you used to determine this information along with any screenshots. At this point, you are only documenting what you find. Do not make changes (yet).*

Security Feature	Status
Firewall product and status – Private network	**Connected**
Firewall product and status – Public network	**Not Connected**
Virus protection product and status	**No Current threats**
Internet Security messages	**Checked**
Network firewall messages	**Checked**
Virus protection messages	**Checked**
User Account Control Setting	**Never notify me**

7. *Now that you are familiar with the security settings on Joe's PC, explain at least three vulnerabilities and risks with these settings. In other words, what can happen to Joe's PC if these are not changed?*
   [Hint: Refer to the CIS Controls document for ideas.]

- **The network will be weak and there will be no defense against the threats.**
- **Insufficient privileges for users to assets and software.**
- **Network devices will be insecure from attackers exploiting the vulnerability.**

2. Securing the PC

Baselines

Joe has asked that you follow industry standards and baselines for security settings on this system.

1. *What industry standard should Joe use for setting security policies at his organization and justify your choice?*

I will recommend Joe's NIST standard and baseline for his system since NIST specified and consists of standards, guidelines, and practices to promote the protection of critical infrastructure to keep the business or devices safe from any vulnerability.

2. *What industry baseline do you recommend to Joe?*
   [Hint: Look in the documents folder]

Center for Internet Security (CIS)

The System and Security functions in the Windows Control Panel are where you can establish the security settings for the PC. This is found from the Control Panel > System and Security > Security and Maintenance. On the Security and Maintenance window, you see a synopsis of the Windows 10 security settings.

3. Assume Joe uses the CIS as his baseline, what controls or steps does this meet?

It will meet with the malware defenses and secure configuration of both the HW and SW on the devices as well as servers, laptop,s and mobile devices.

System and Security

At this point, you need to enable security services for this PC. Pick at least 3 of the following 5 areas to secure in order to satisfactorily meeting the project requirements:

- **Firewall**
- **Virus & Threat Protection**
- **App & Browser Control**
- **User Account Control settings**
- **Securing Removable Media**

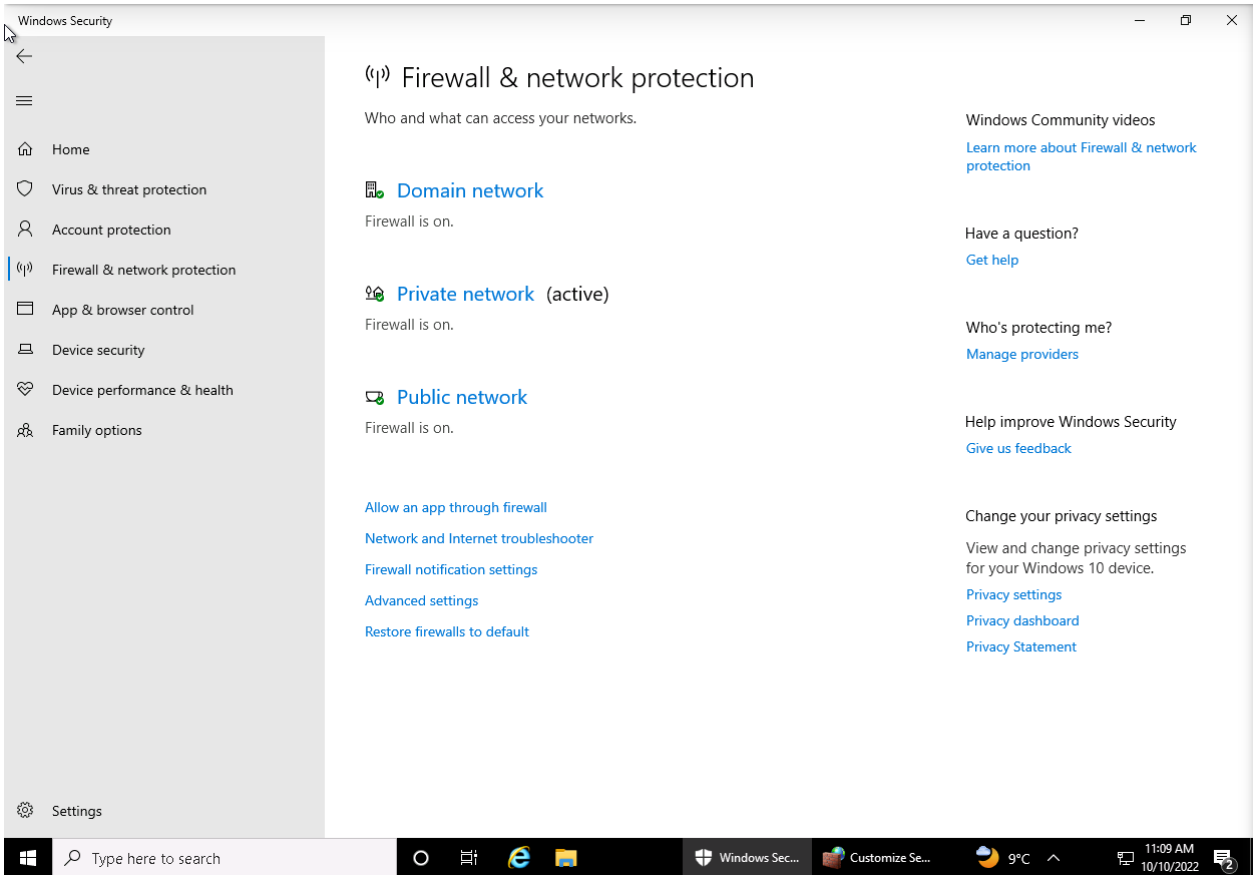
Firewall

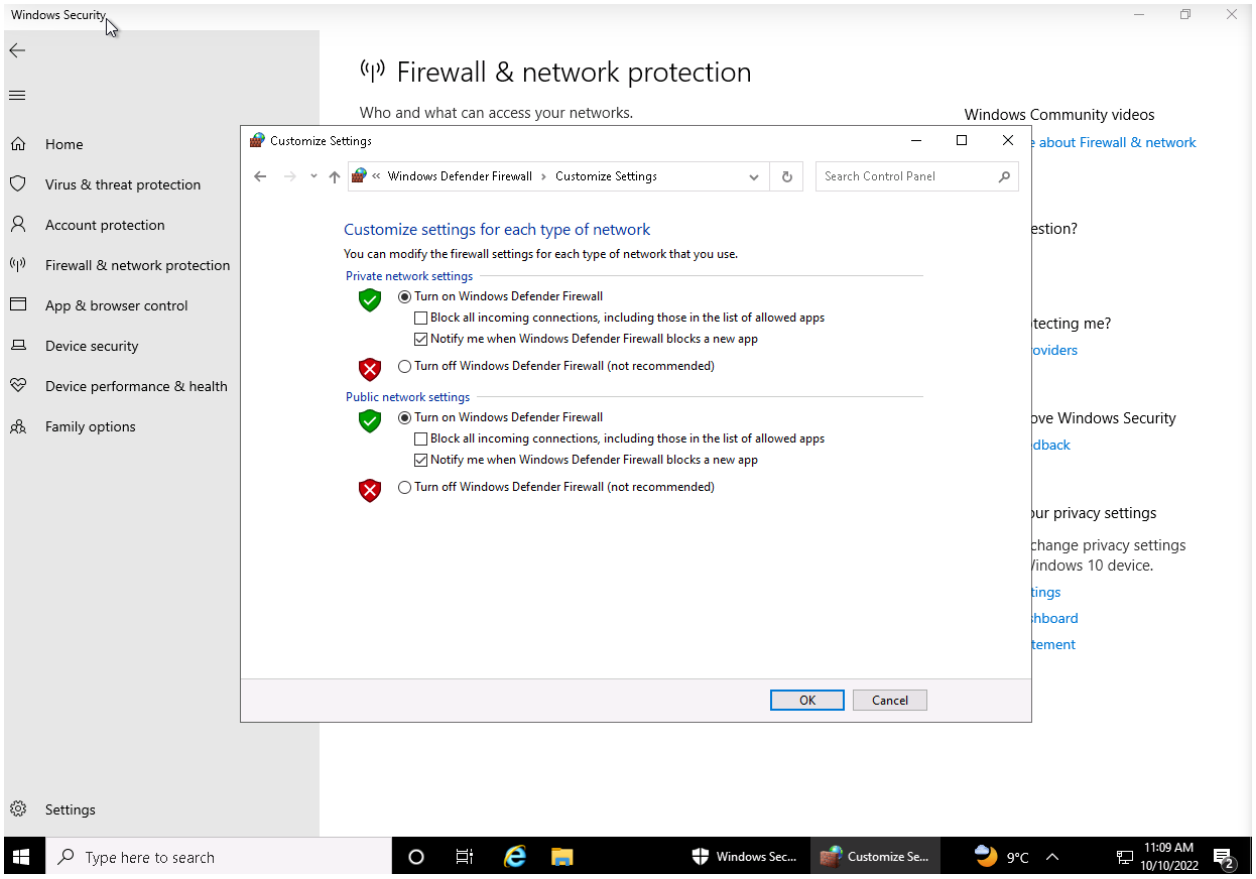
You need to ensure the Windows Firewall is enabled for all network access.

1. *Explain the process you take to do this.*

The firewall was turned off and this leads to risk,Go to setting → Firewall & network protection → Turn on the firewall for the networks.
Go to control panel → system and security → windows Defender Firewall →Customize Setings → make sure you trun on windows Defenders wall for both networks.

2. *Include screenshots showing the firewall is turned on.*





3. *What protection does this provide?*

The firewall provides protection to private and public networks by blocking any connection that may relate to threats to the network and PC.

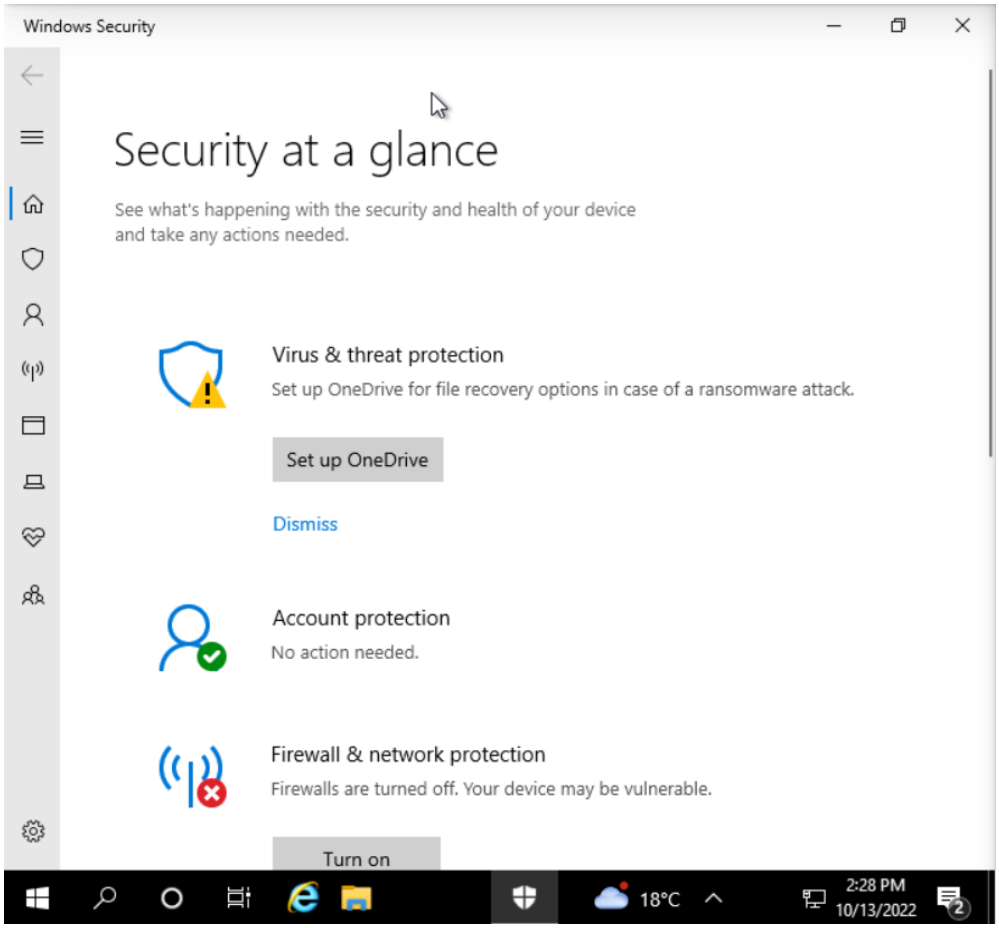
Virus & Threat Protection

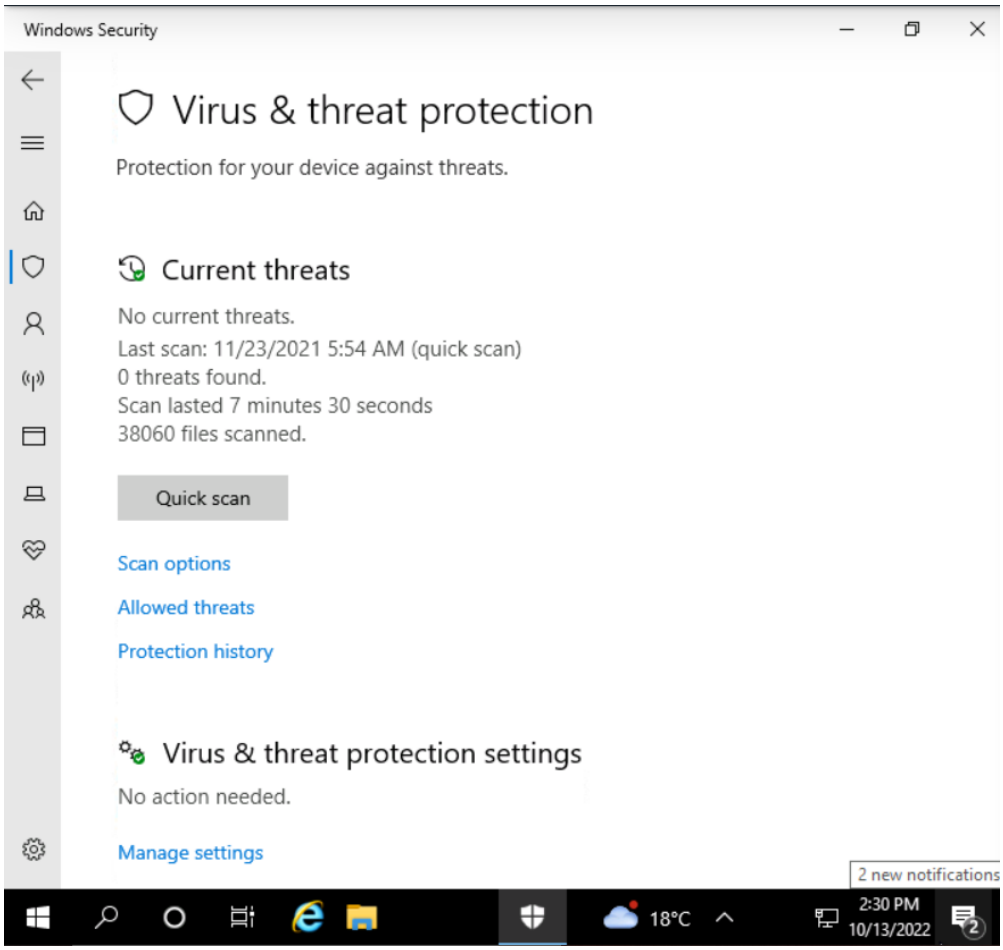
You need to ensure the Windows Defender anti-virus is enabled to always protect against current threats. It should be set to automatically update and continually scan the PC for malicious software. Note: Ignore any alerts about setting up OneDrive.

1. *Explain the process you take to do this.*

Go to Virus & Threat Protection → check if the there are no threats by click scan.

2. *Include screenshots to confirm that anti-virus is enabled.*


Windows Security
Security at a glance
See what's happening with the security and health of your device and take any actions needed.
Virus & threat protection
Set up OneDrive for file recovery options in case of a ransomware attack.
Set up OneDrive
Dismiss
Account protection
No action needed.
Firewall & network protection
Firewalls are turned off. Your device may be vulnerable.
Turn on
18°C
2:28 PM
10/13/2022

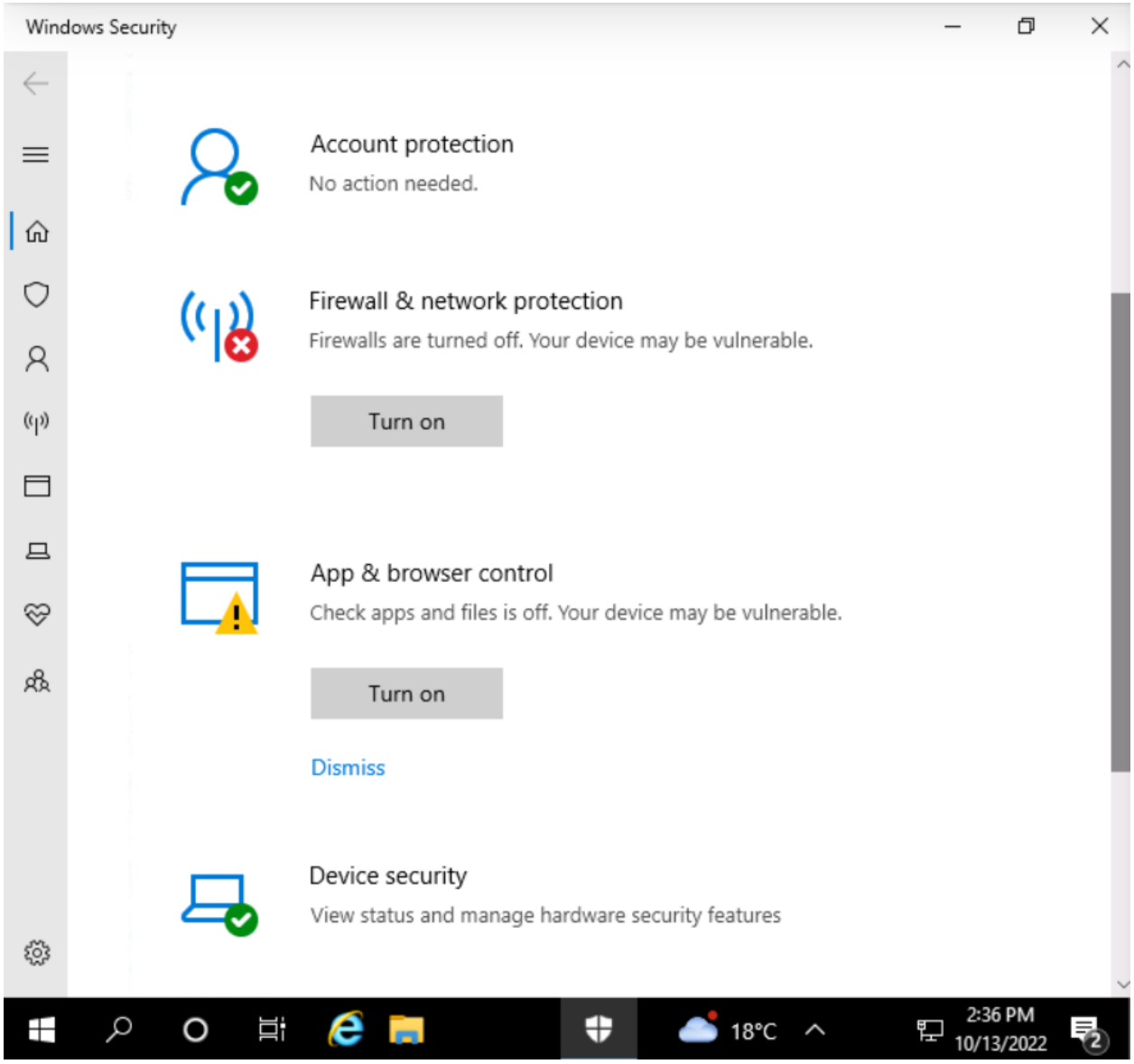


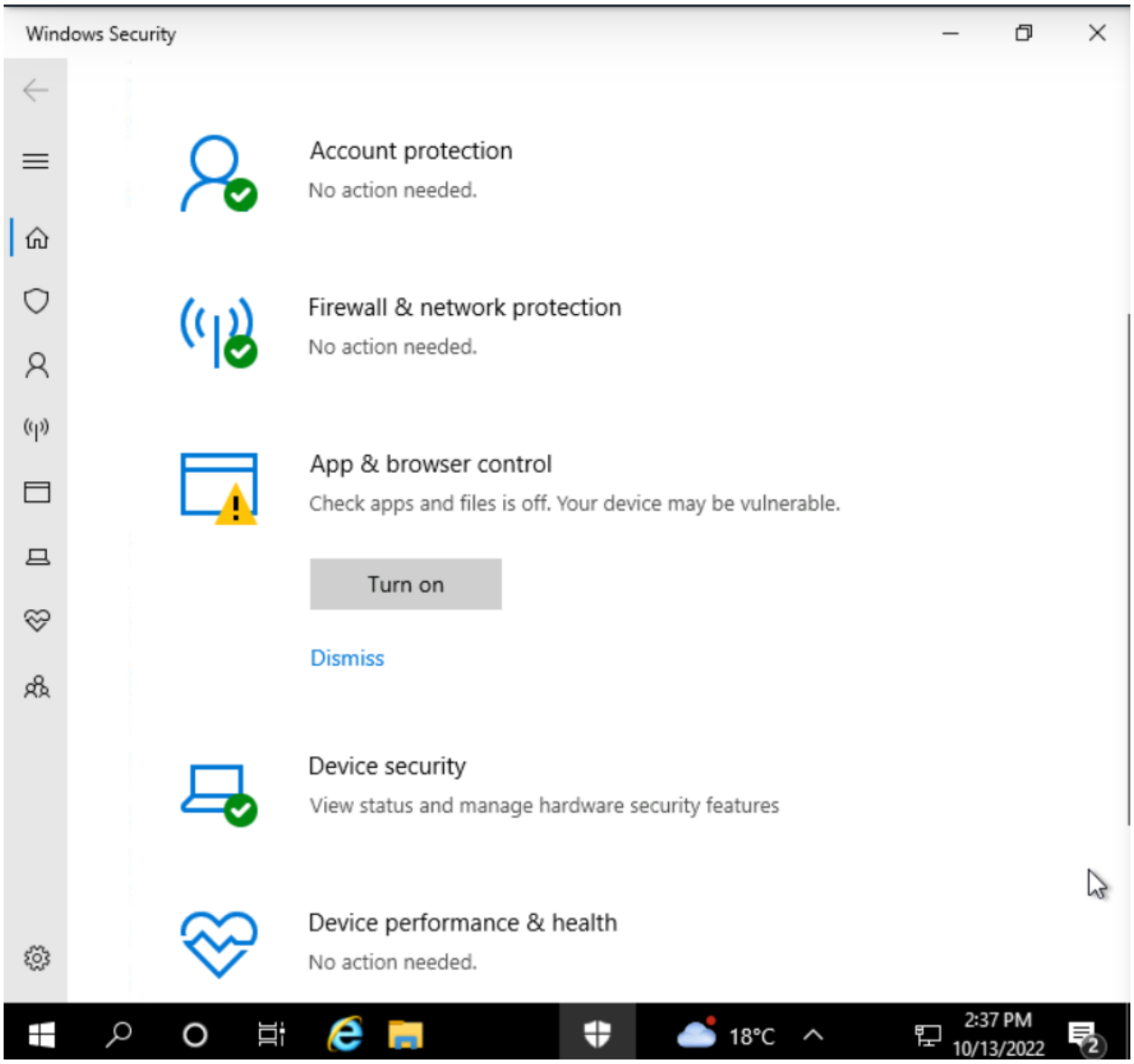
Once you determine that virus & threat protection is on and updated, you need to turn on messages about the Network firewall and Virus protection. Refer to the instructions above for viewing the settings within Security and Maintenance, Review recent messages and resolve problems.

1. *Turn on the Network firewall and Virus protection messages using Change Security and Maintenance Settings.*

Go to windows security → click on turn on button for the Network firewall and Virus protection.

2. *Show a screenshot here of them enabled.*





3. *Provide at least two risks mitigated by enabling these security settings:*

- **Administrator will received a message if the network was breach.**
- **The system will be scure against any virus and threat due to auto scan.**

4. *From the CIS baseline controls, provide the controls satisfied by completing this.*

Malware defenses and Network Monitoring and Defense and Infrastructure Management.

App & Browser Control

The App protection within Windows Defender helps to protect your device by checking for unrecognized apps and files and from malicious sites and downloads. Review the settings found within the *Account protection window, and App & browser control windows* found on the *Windows Defender Security page*.
Advanced students: You should also review the settings on the Exploit protection page.

1. *Change the settings to provide **maximum** protection for Joe's PC and provide a screenshot of your results.*

User Account Control Settings

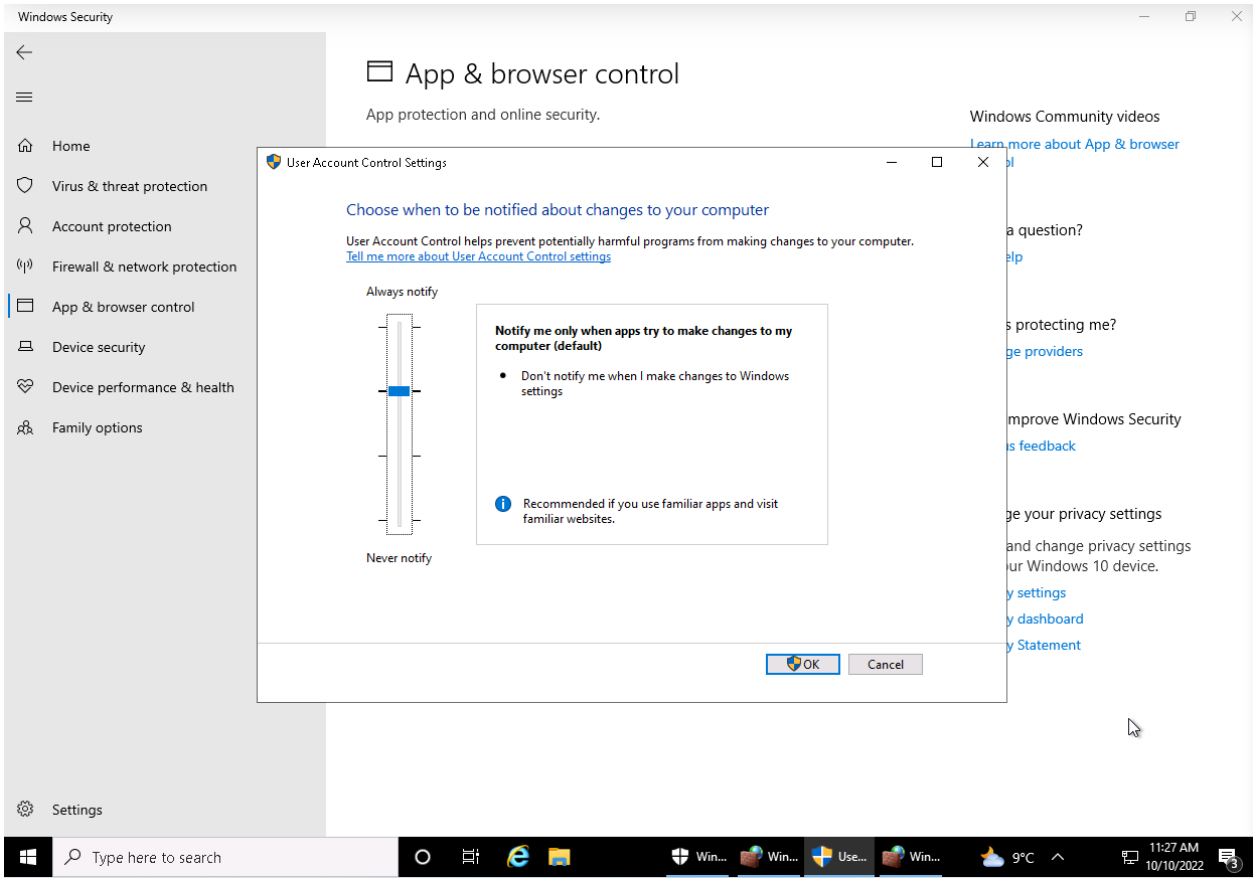
Joe wants to prevent potentially harmful programs from making changes and wants to be notified whenever apps try to make changes to his computer. This is done through the User Account Control Setting.

1. *What is the current UAC setting on Joe's computer?*

   This is available from the above security settings.
   Never notify me when apps install or make changes to the computer.

2. *What should it be set to? Include a screenshot of the new setting.*

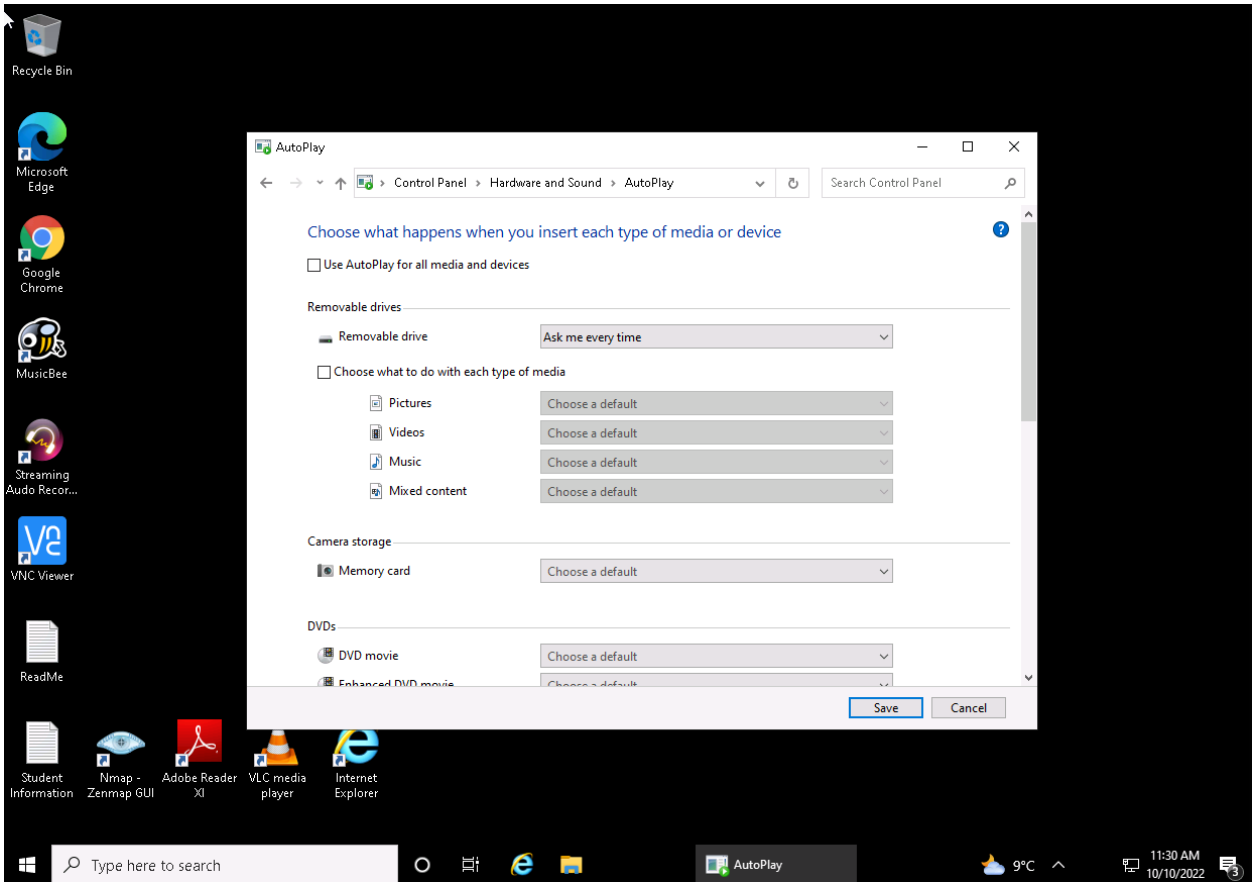
Notify me only when apps try to make changes to my computer (Default)because this is the recommended setting.



Securing Removable Media

A security best practice is to not allow the use of removable hard drives (USB sticks, Memory Cards, and DVDs). They are needed as part of Joe's backup policy. The next best thing is to make sure that any applications don't automatically start when the media is inserted and the user is asked what should happen. This is set from the Control Panel > Hardware and Sound > Autoplay menu.

1. *On Joe's computer, go to that function and deselect "Use AutoPlay for all media and devices."*
2. *For the Removable Drive, make the default, "Ask me every time." Include a screenshot of your results.*



3. Securing Access

Ensuring only specific people have access on a computer system is a common step in information security. It starts by understanding who should have access and the rules or policies that need to be followed.

On Joe's computer, only the following accounts should be in use:

- JoesAuto
- Jane Smith (Joe's assistant)
- A User - Used for exercises (Not used in this project)
- Notadmin - Built-in administrator account (Not used for this project)
- Windows built-in accounts: Guest, DefaultAccount, and WDAGUtility (Not used for this project)

Joe's Auto Access Rules:

- Only JoesAuto and A User should have administrative privileges on this PC.
- Joe wants to prevent potentially harmful programs from making changes and wants to be notified whenever apps try to make changes to his computer.
- All valid users should have a password following Joe's password policy below
    - At least 8 characters
    - Complexity enabled

    - Changed every 120 days
    - Cannot be the same as the previous 5 passwords
- Account should be automatically disabled after 5 unsuccessful login attempts. The account should be locked for 15 minutes and then should automatically unlock.
- Upon first logging into the PC, Joe wants a warning banner letting anyone using to know that this is to only be used for work at Joe's Auto Body shop by authorized people.
- There is to be no remote access to this computer.

User Accounts

1. *What user accounts should not be there?* ***Hacker***
2. *Bonus questions: What is Hacker's password?*
3. *Explain the steps you take to disable or remove unwanted accounts.*

Go to control panel → user accounts → make changes to my account in PC settings → other users → select the unwanted account then remove it.

4. *Why is it important to disable or remove unneeded accounts from a PC or application? Include potential vulnerabilities and risks.*

It's very important to remove unneeded accounts to avoid any unauthorized users having access to make any changes.

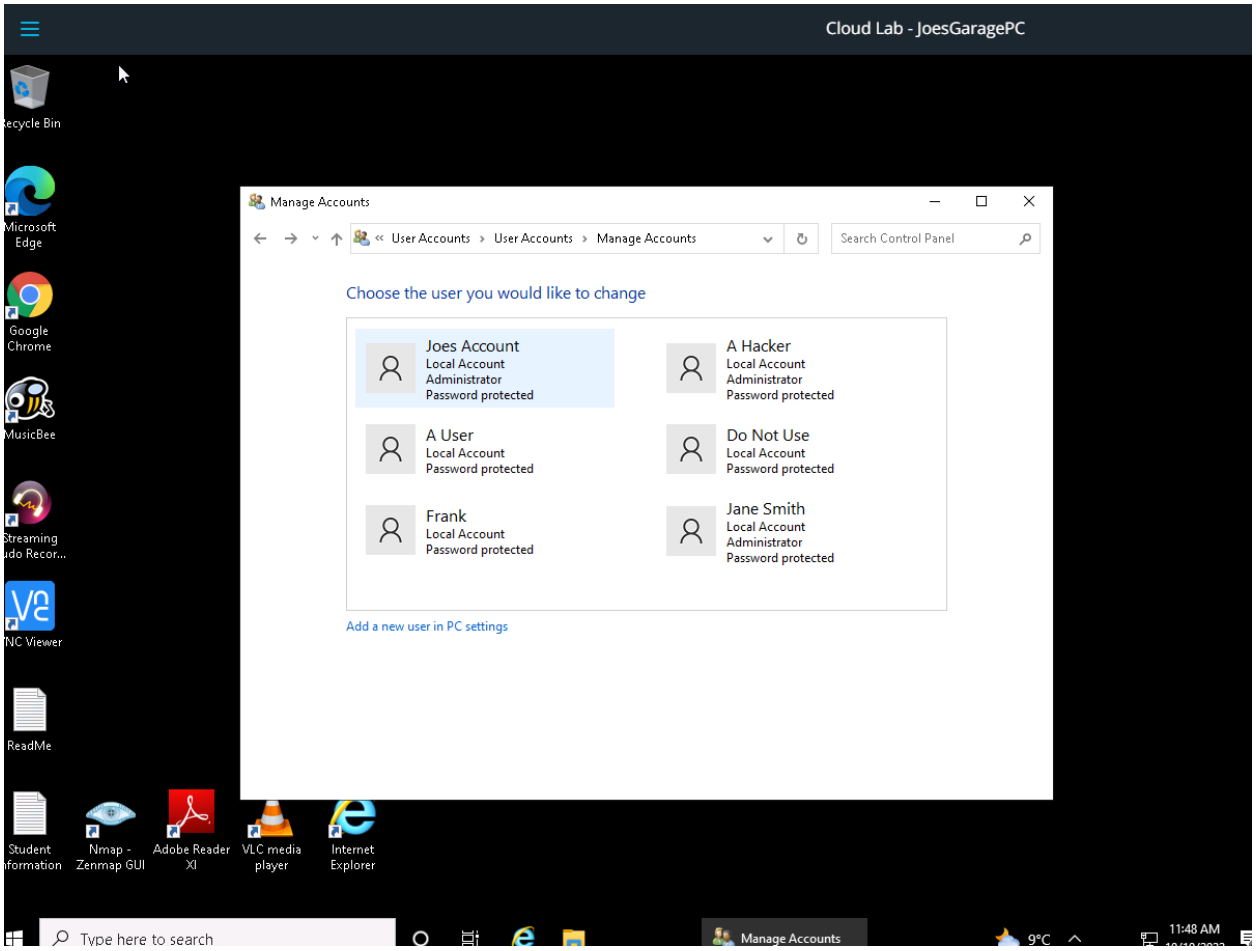
<u>Potential vulnerabilities and risks:</u>

Unauthorized users may have access to sensitive data and be misused.

Only specific accounts should have administrator privileges. This reduces the ability for unwanted applications to be installed including malware.

5. Which account(s) have administrator rights that shouldn't?
   A Hacker Local Account
6. Explain how you determined this. Provide screenshots as needed.

Only Joe should have administrator rights and privileges.



Administrator privileges for too many users are another security challenge.

7. Provide at least three risks associated with users having administrator rights on a PC.

- **Users can intentionally or unintentionally execute a malicious program, which may lead to an infection that could span many computers on the network.**
- **If multiple users have access or privileges to the administrator account, it will allow for data breaches, theft, and privacy concerns.**
- **administrator users' could modify the operating system settings causing potential consequences.**

Now you need to remove administrator privileges for any user(s) that should have it.

8. *Explain the process for doing this. Include screenshots to show your work.*

Go to Control Panel → Users Accounts → Make changes to my account in PC settings → select (Other Users) → select the account whose privlages must be changed→ change account type → select standard account which gives only local privilages to the account user.

9. *What is the security principle behind this?*

Integrity

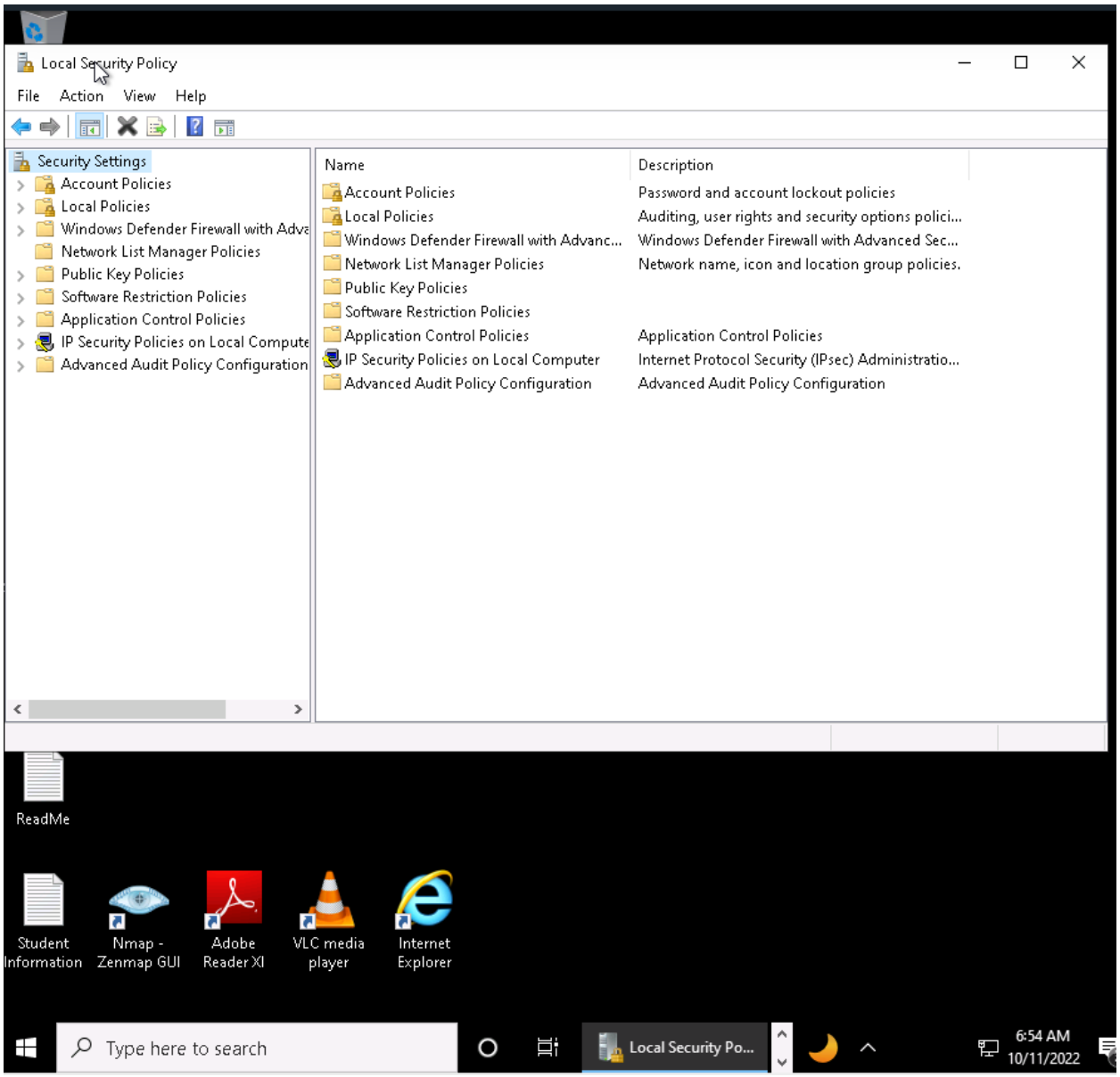
10. The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?

Controlled use of administrator privileges.

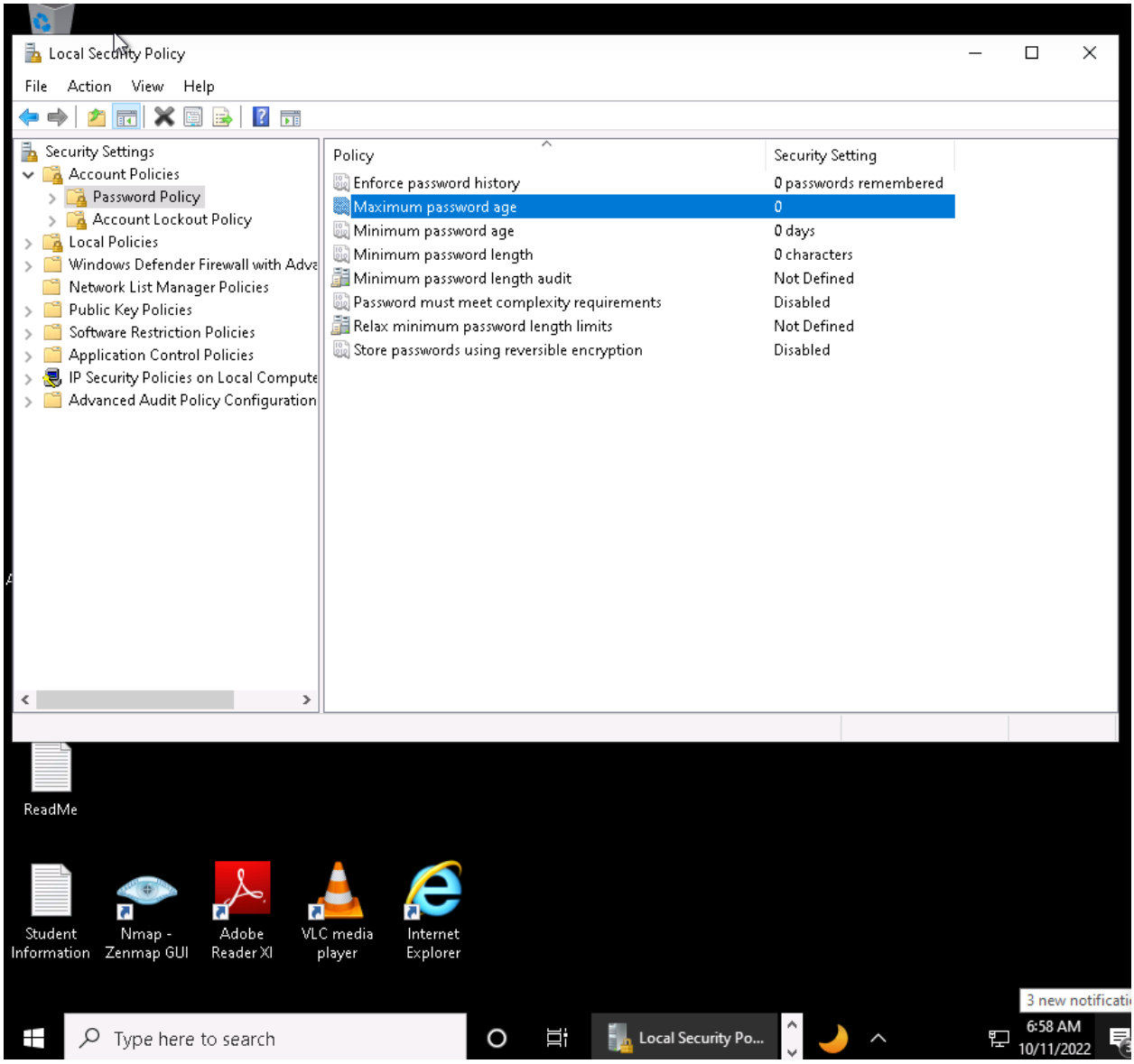
Setting Access and Authentication Policies

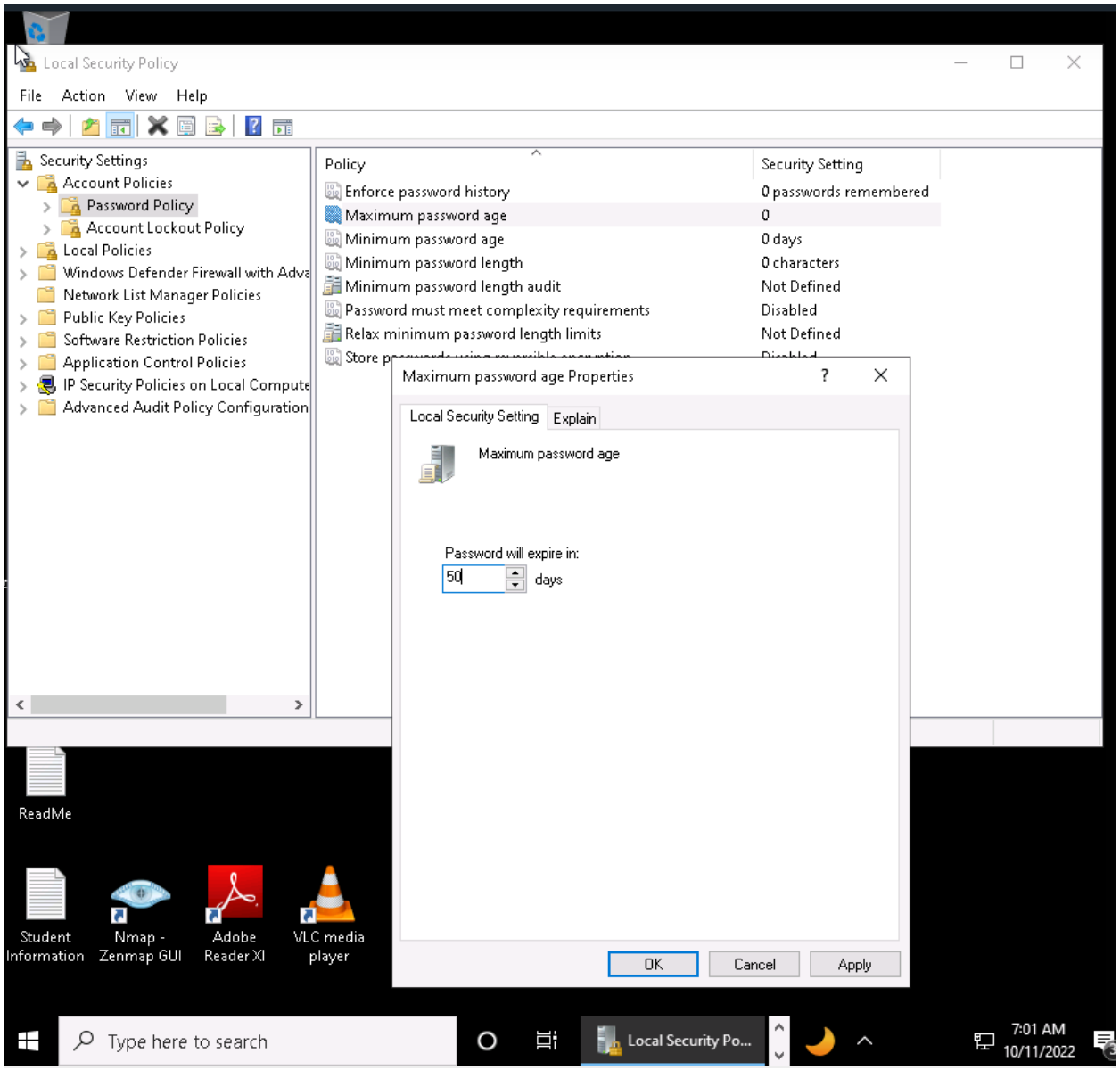
After you talked with Joe about security, he has asked that the access rules outlined above be in place on his PC. These are set using the Local Security Policy function in Windows 10. On the Windows search bar, type "*Local Security Policy*" to access it. Click the > arrow next to both "*Account Policies*" and "*Local Policies*" and review their contents.

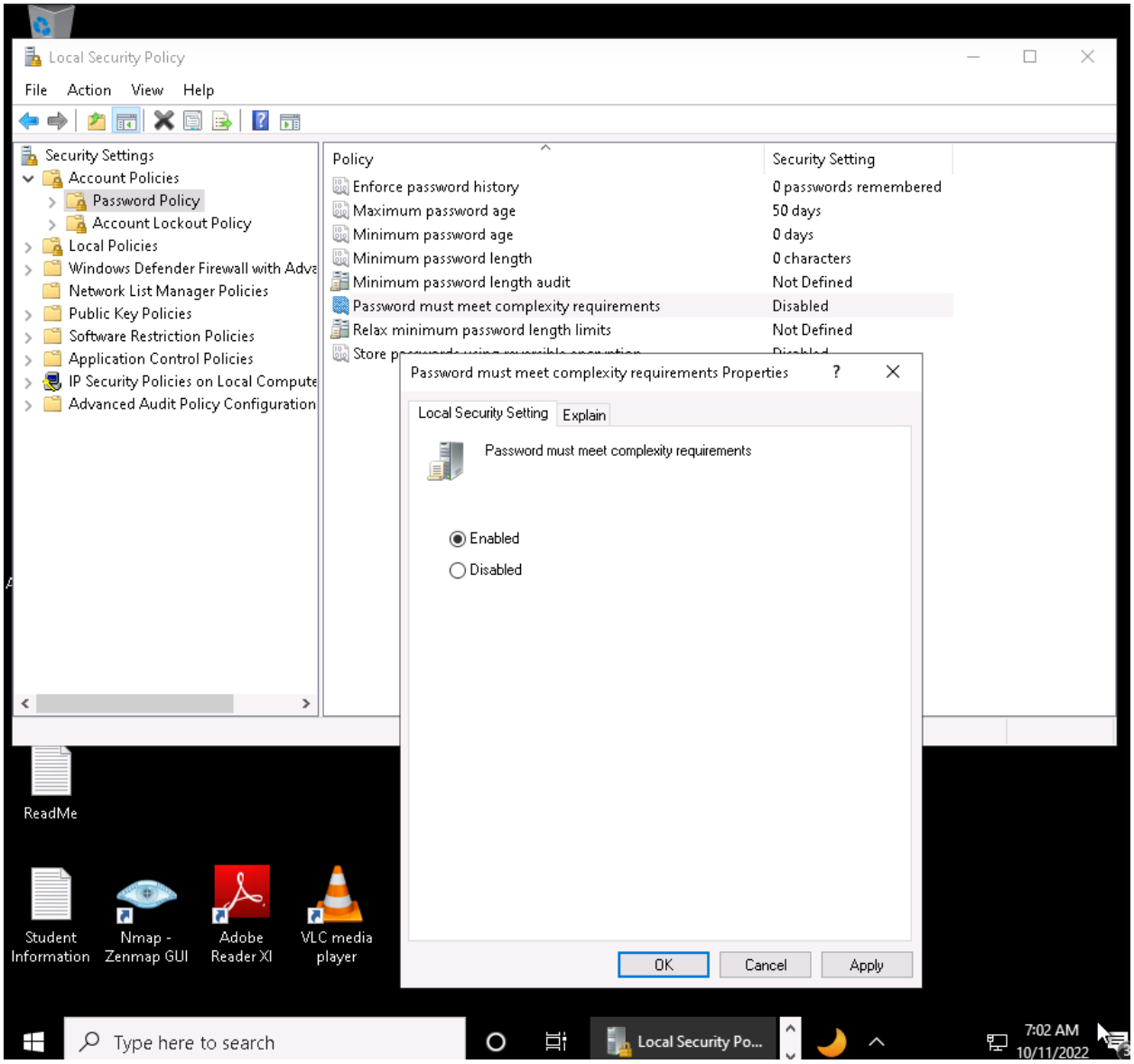
1. *Provide a screenshot of the Local Security Policy window here.*
   [Note: Local Security Policy is not available on Windows 10 Home edition.]

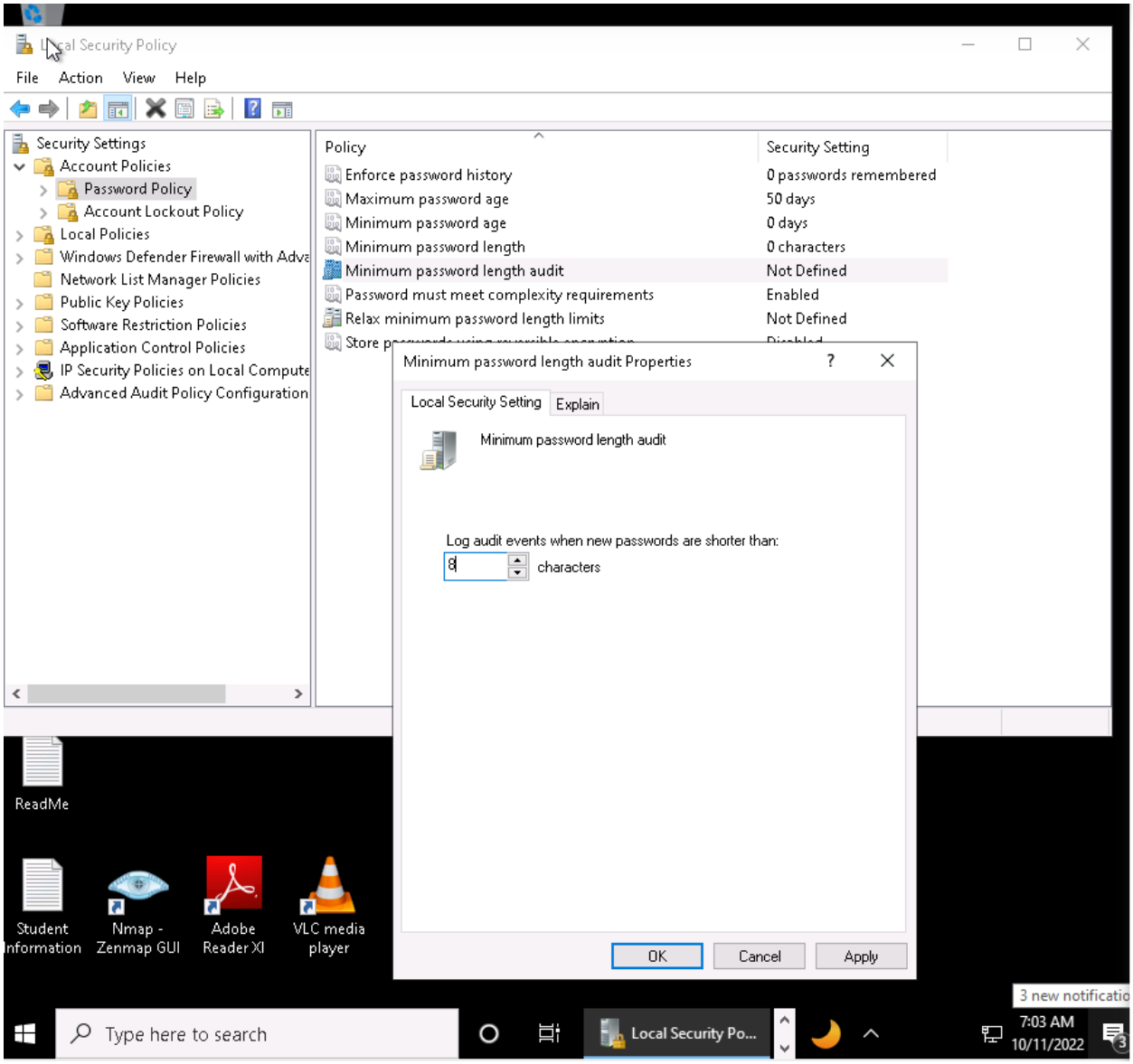


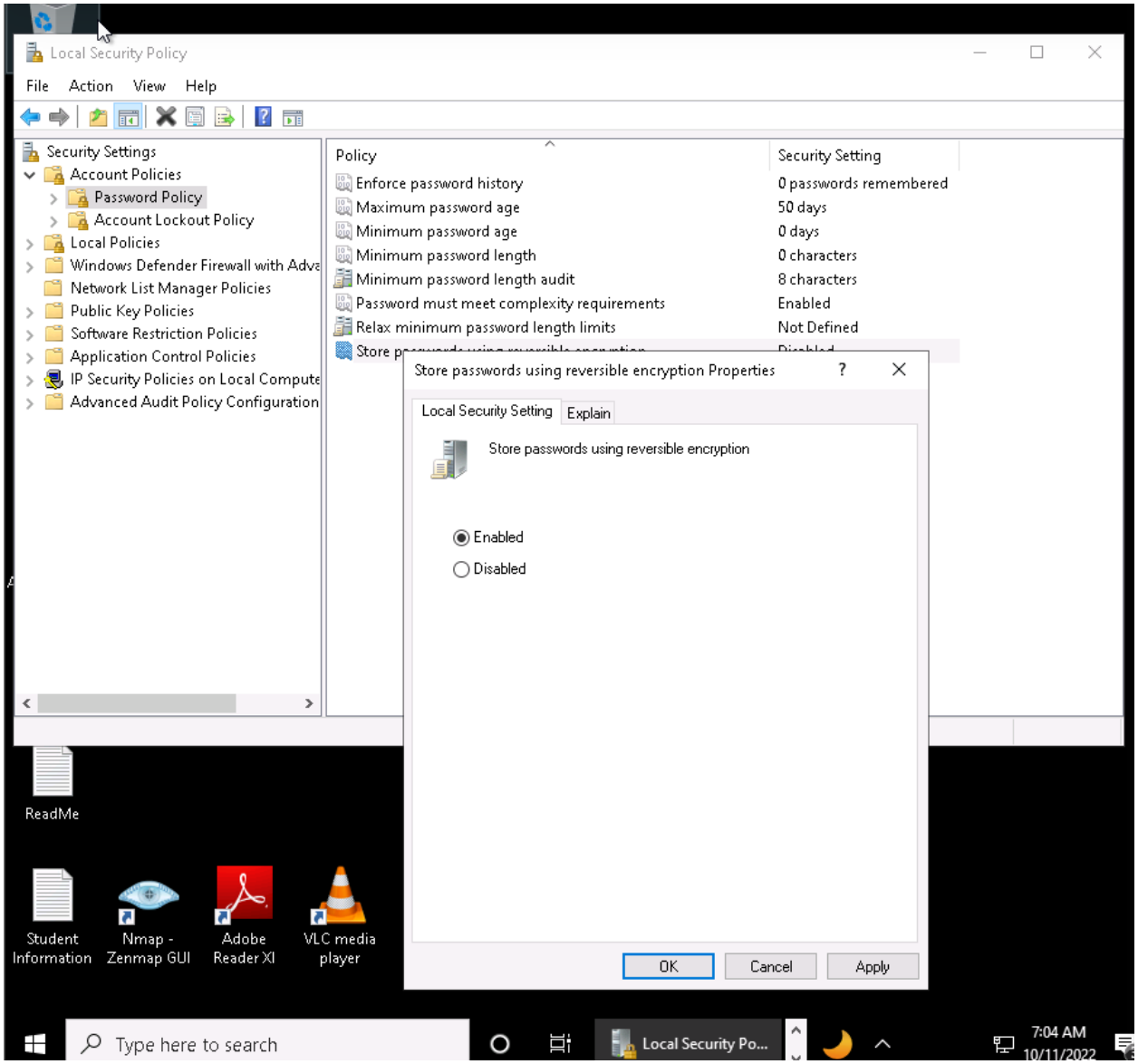
2. Explain the process for setting the password and access control policies locally on a Windows 10 PC. Provide screenshots showing how you set the rules on the PC.
   Go to →(type in the search bar) Local Security Policy → click on Account policies → password policy → policy settings → set the new rules.
   - Setting the Password Policy:

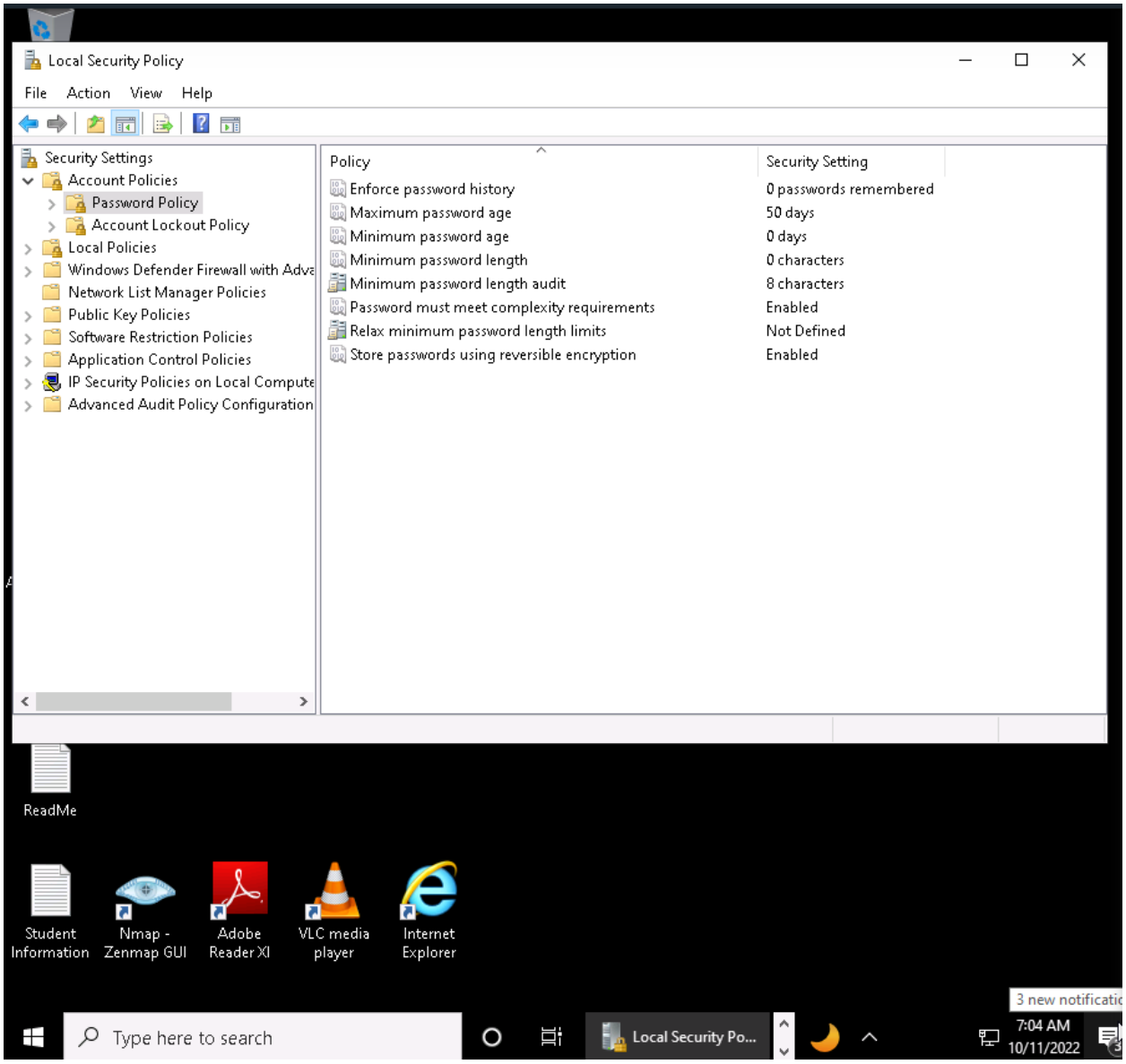

Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Enforce password history
0 passwords remembered
Maximum password age
0
Minimum password age
0 days
Minimum password length
0 characters
Minimum password length audit
Not Defined
Password must meet complexity requirements
Disabled
Relax minimum password length limits
Not Defined
Store passwords using reversible encryption
Disabled
ReadMe
Student Information
Nmap - Zenmap GUI
Adobe Reader XI
VLC media player
Internet Explorer
Type here to search
Local Security Po...
6:58 AM
10/11/2022


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Enforce password history
0 passwords remembered
Maximum password age
0
Minimum password age
0 days
Minimum password length
0 characters
Minimum password length audit
Not Defined
Password must meet complexity requirements
Disabled
Relax minimum password length limits
Not Defined
Maximum password age Properties
Local Security Setting
Explain
Maximum password age
Password will expire in:
50
days
OK
Cancel
Apply
ReadMe
Student Information
Nmap - Zenmap GUI
Adobe Reader XI
VLC media player
Type here to search
Local Security Po...
7:01 AM
10/11/2022

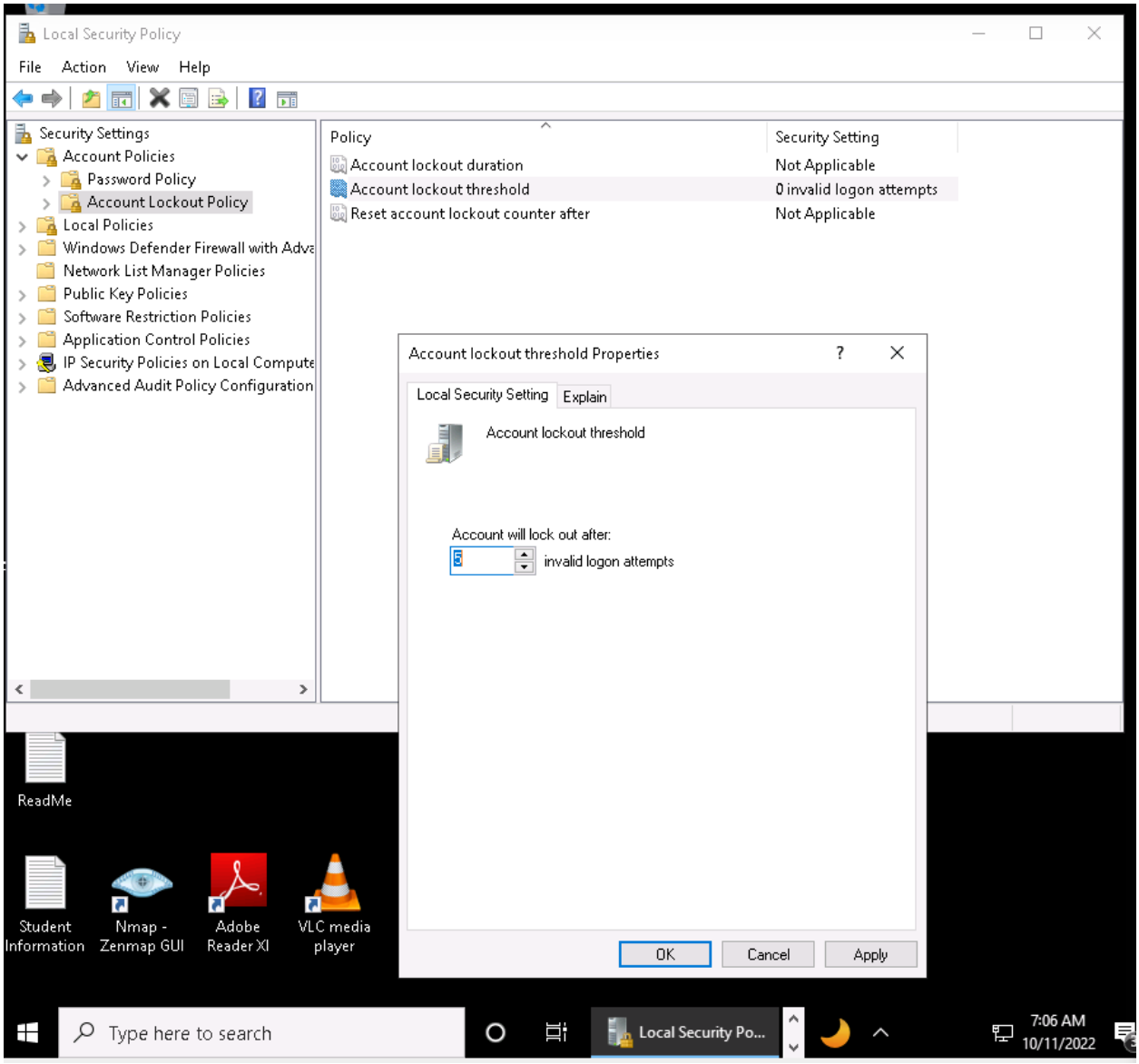

Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Enforce password history
0 passwords remembered
Maximum password age
50 days
Minimum password age
0 days
Minimum password length
0 characters
Minimum password length audit
Not Defined
Password must meet complexity requirements
Disabled
Relax minimum password length limits
Not Defined
Password must meet complexity requirements Properties
Local Security Setting
Explain
Password must meet complexity requirements
Enabled
Disabled
OK
Cancel
Apply
ReadMe
Student Information
Nmap - Zenmap GUI
Adobe Reader XI
VLC media player
Type here to search
Local Security Po...
7:02 AM
10/11/2022

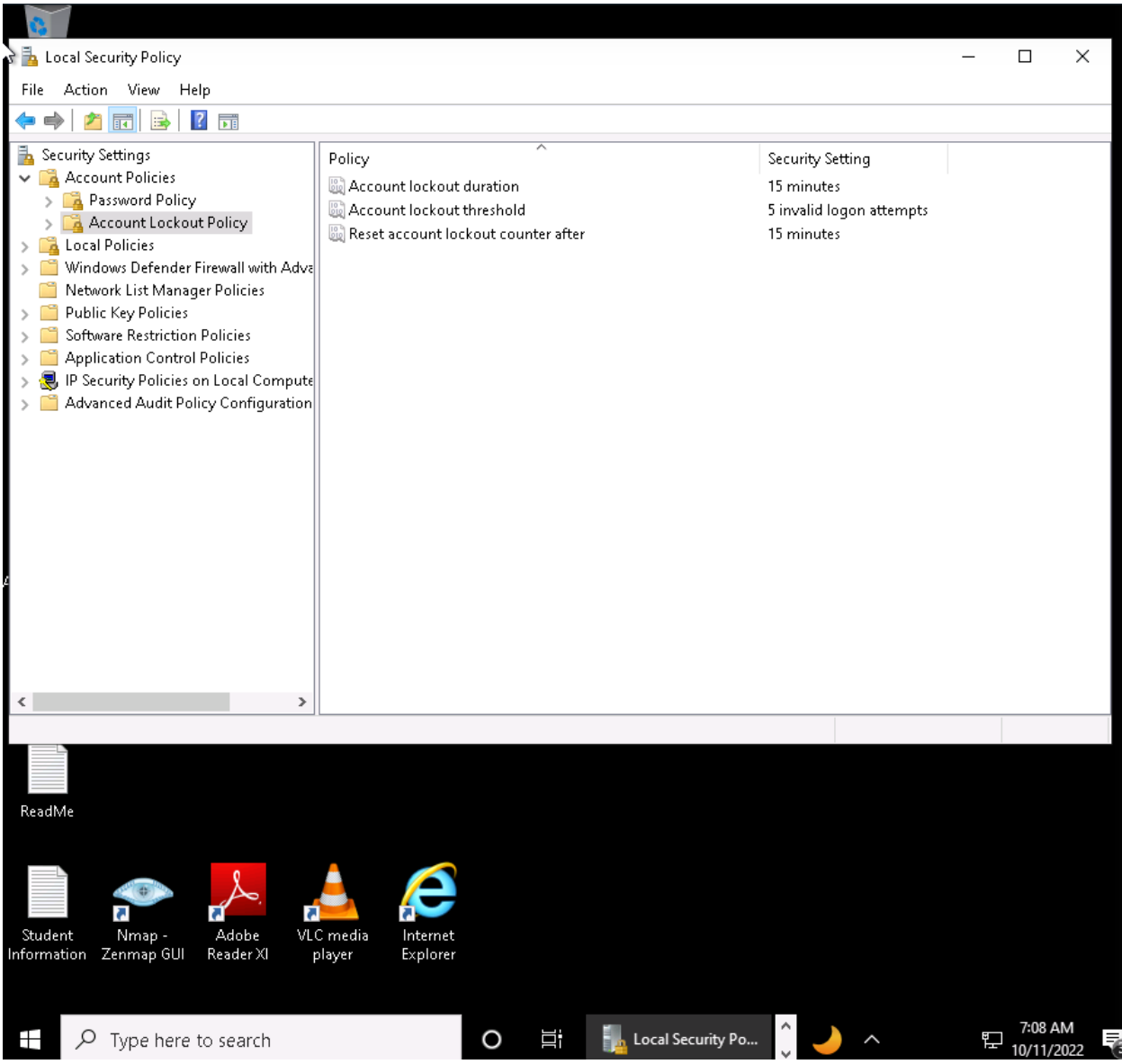

Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Enforce password history
0 passwords remembered
Maximum password age
50 days
Minimum password age
0 days
Minimum password length
0 characters
Minimum password length audit
Not Defined
Password must meet complexity requirements
Enabled
Relax minimum password length limits
Not Defined
Minimum password length audit Properties
Local Security Setting
Explain
Minimum password length audit
Log audit events when new passwords are shorter than:
8
characters
OK
Cancel
Apply
ReadMe
Student Information
Nmap - Zenmap GUI
Adobe Reader XI
VLC media player
Type here to search
Local Security Po...
3 new notificatio
7:03 AM
10/11/2022


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Enforce password history
0 passwords remembered
Maximum password age
50 days
Minimum password age
0 days
Minimum password length
0 characters
Minimum password length audit
8 characters
Password must meet complexity requirements
Enabled
Relax minimum password length limits
Not Defined
Store passwords using reversible encryption Properties
Local Security Setting
Explain
Store passwords using reversible encryption
Enabled
Disabled
OK
Cancel
Apply
ReadMe
Student Information
Nmap - Zenmap GUI
Adobe Reader XI
VLC media player
Type here to search
Local Security Po...
7:04 AM
10/11/2022


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Enforce password history
0 passwords remembered
Maximum password age
50 days
Minimum password age
0 days
Minimum password length
0 characters
Minimum password length audit
8 characters
Password must meet complexity requirements
Enabled
Relax minimum password length limits
Not Defined
Store passwords using reversible encryption
Enabled
ReadMe
Student Information
Nmap - Zenmap GUI
Adobe Reader XI
VLC media player
Internet Explorer
Type here to search
Local Security Po...
3 new notificatio
7:04 AM
10/11/2022

- Setting the Account Lockout Policy:



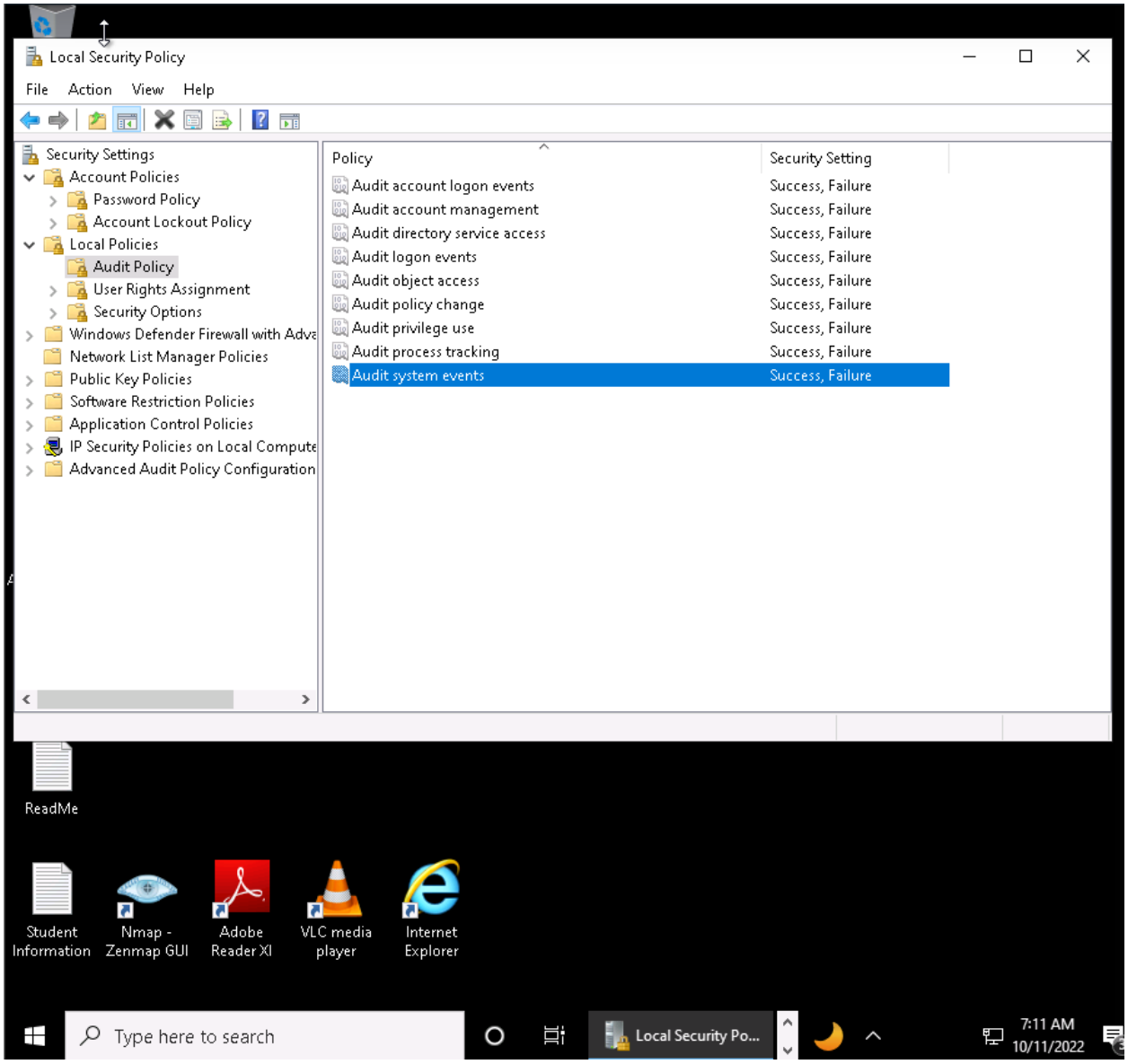


Auditing and Logging

Security best practices like those found in the CIS Controls or NIST Cybersecurity Framework require systems to log events. You need to enable the Audit Policy for Joe's PC to meet these standards.

1. From the Local Security Policy window, select Audit Policy and make applicable changes to Joe's PC to enable minimal logging of logon, account, privilege use, and policy changes.

2. Provide a screenshot of your changes here.



4. Securing Applications

As part of the inventory process, you determined computer programs or applications on the PC. The next step is to decide which ones are needed for business and which ones should be removed. Unneeded programs could be vulnerable to attacks and allow unauthorized access into the computer. They also consume system resources and could also violate licensing agreements.

Joe has established the following rules regarding PC applications:

- Joe wants everyone to use the latest version of the Chrome browser by default.
- There should be no games or non-work-related applications installed or downloaded.
- Joe is also concerned that there are “hacking” programs downloaded or installed on the PC that should be removed.

- This PC is used for standard office functions. The auto-body has a separate service they use for their website and to transfer files from their suppliers.

Remove unneeded or unwanted applications

1. *List at least three application(s) that violate this policy.*

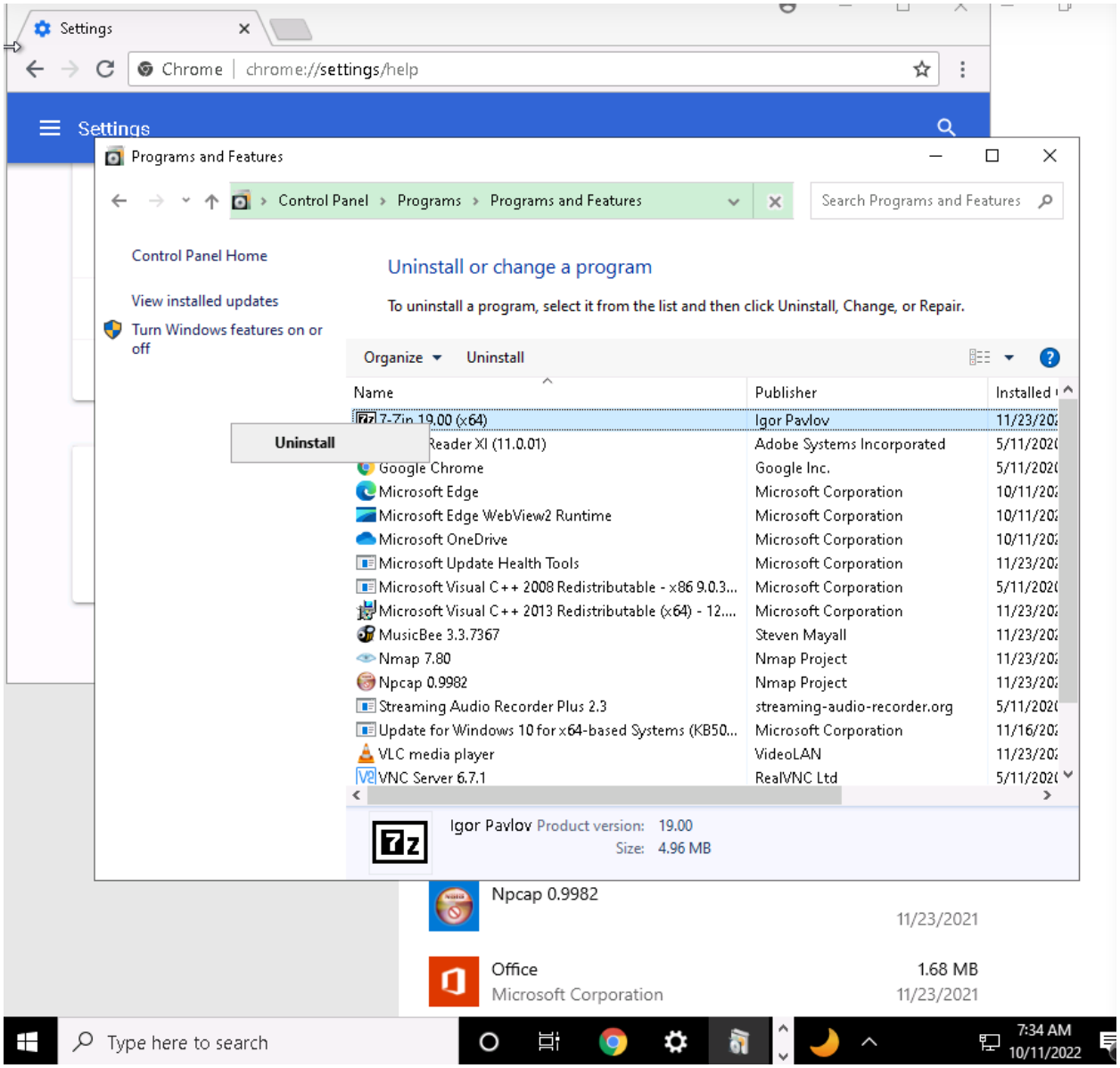
- ***Npcap 0.9982***
- ***Nmap 7.80***
- ***7 Zip 19.00 (x64)***

2. *Name at least three vulnerabilities, threats or risks with having unnecessary applications:*

- ***It may access to sensitive data and disclosure or misuse the data.***
- ***Ransomware threats will lead to locking shared files across the network.***
- ***Collect user data in the background.***

3. *Joe wants you to make sure unneeded applications or programs are no longer on the PC. Explain the steps you take to disable or remove them. Include screenshots to show your work.*

Joe can easily uninstall unneeded apps from the control panel --> programs -->programs and features.

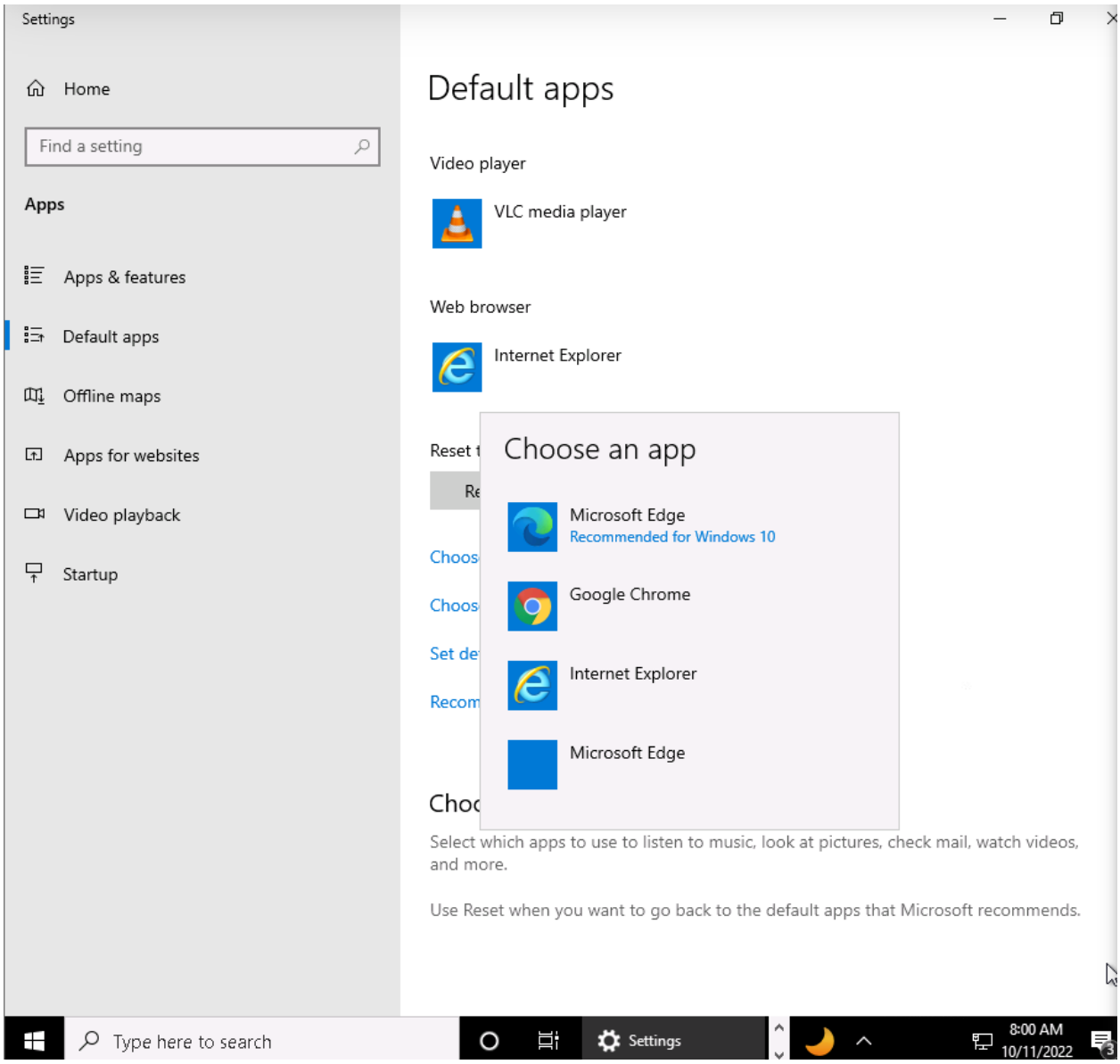


Default Browser

As mentioned in the policy, Joe wants all users to use Chrome as their browser by default.

1. *Explain how you set default applications within the Windows 10 operating system. Include screenshots as necessary.*

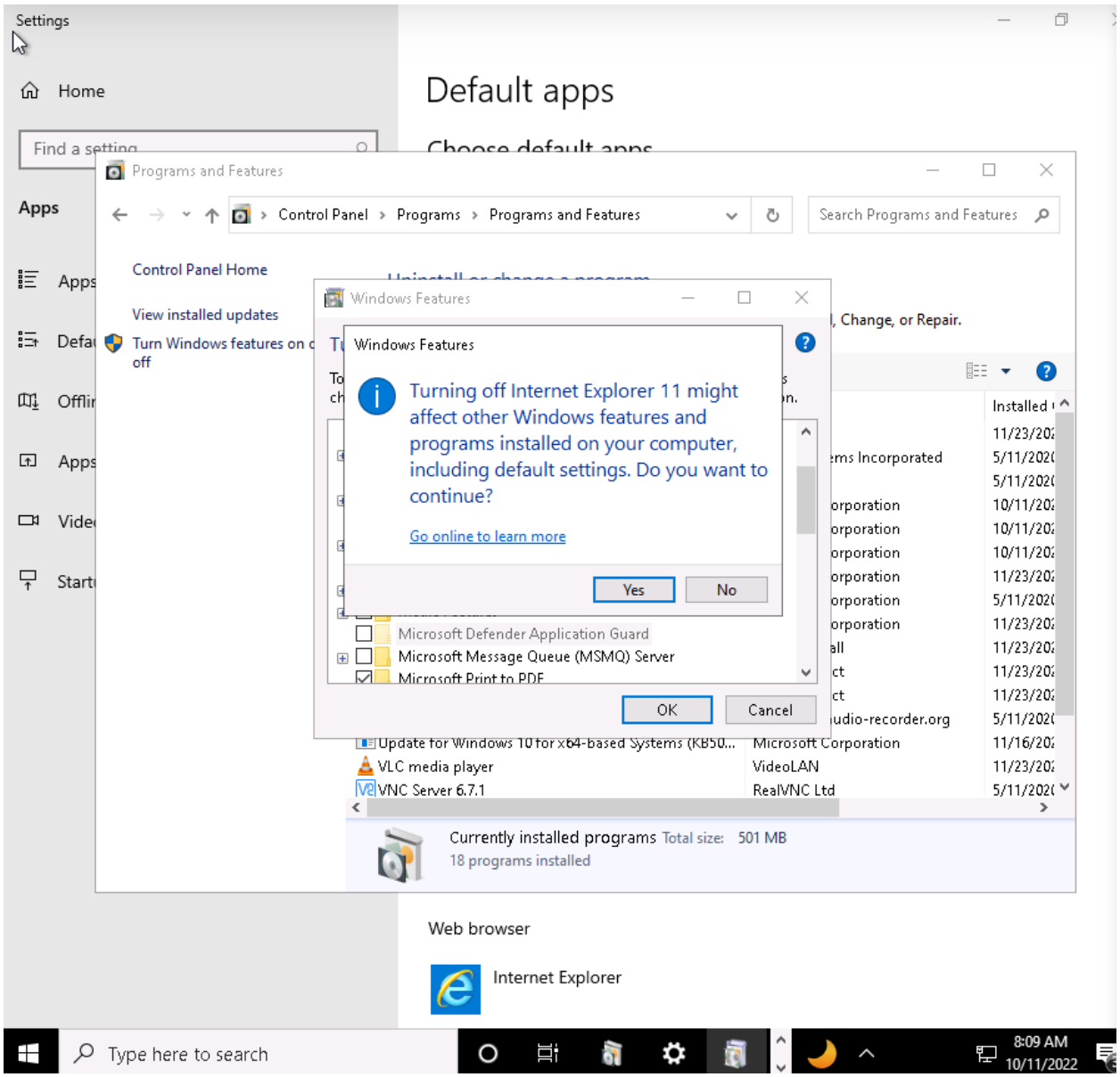
Go to Settings → Apps → Default Apps → change the default web browser (Internet explorer)to Google Chrome by clicking on the icon of the browser.

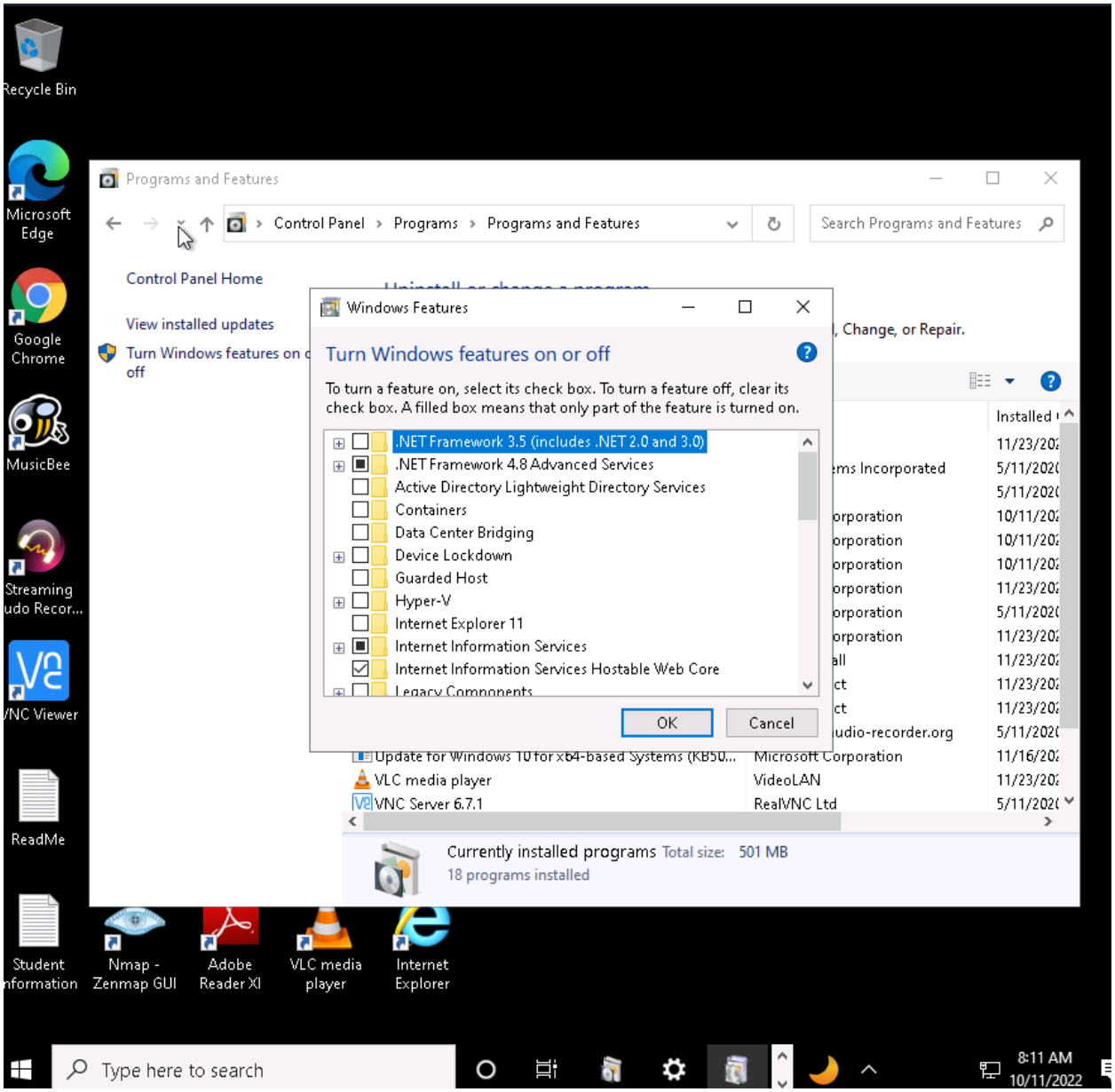


2. *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
    - **Internet Explorer has several zero-day vulnerabilities.**
    - **It doesn't have a lot of updates to fix the *vulnerabilities.***

Because of the reasons you give above, Internet Explorer should be removed. To do that, go to the **Control Panel**, select **Programs**. On the **Programs and Features** window, select "**Turn Windows features on or off**."

3. *Provide a screenshot showing Internet Explorer 11 is off.*


Settings
Home
Find a setting
Apps
Default apps
Choose default apps
Programs and Features
Control Panel › Programs › Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Uninstall or change a program
Change, or Repair.
Windows Features
Turning off Internet Explorer 11 might affect other Windows features and programs installed on your computer, including default settings. Do you want to continue?
Go online to learn more
Yes
No
Microsoft Defender Application Guard
Microsoft Message Queue (MSMQ) Server
Microsoft Print to PDF
OK
Cancel
Update for Windows 10 for x64-based Systems (KB50...
Microsoft Corporation
VLC media player
VideoLAN
VNC Server 6.7.1
RealVNC Ltd
Currently installed programs Total size: 501 MB
18 programs installed
Web browser
Internet Explorer
Type here to search
8:09 AM
10/11/2022

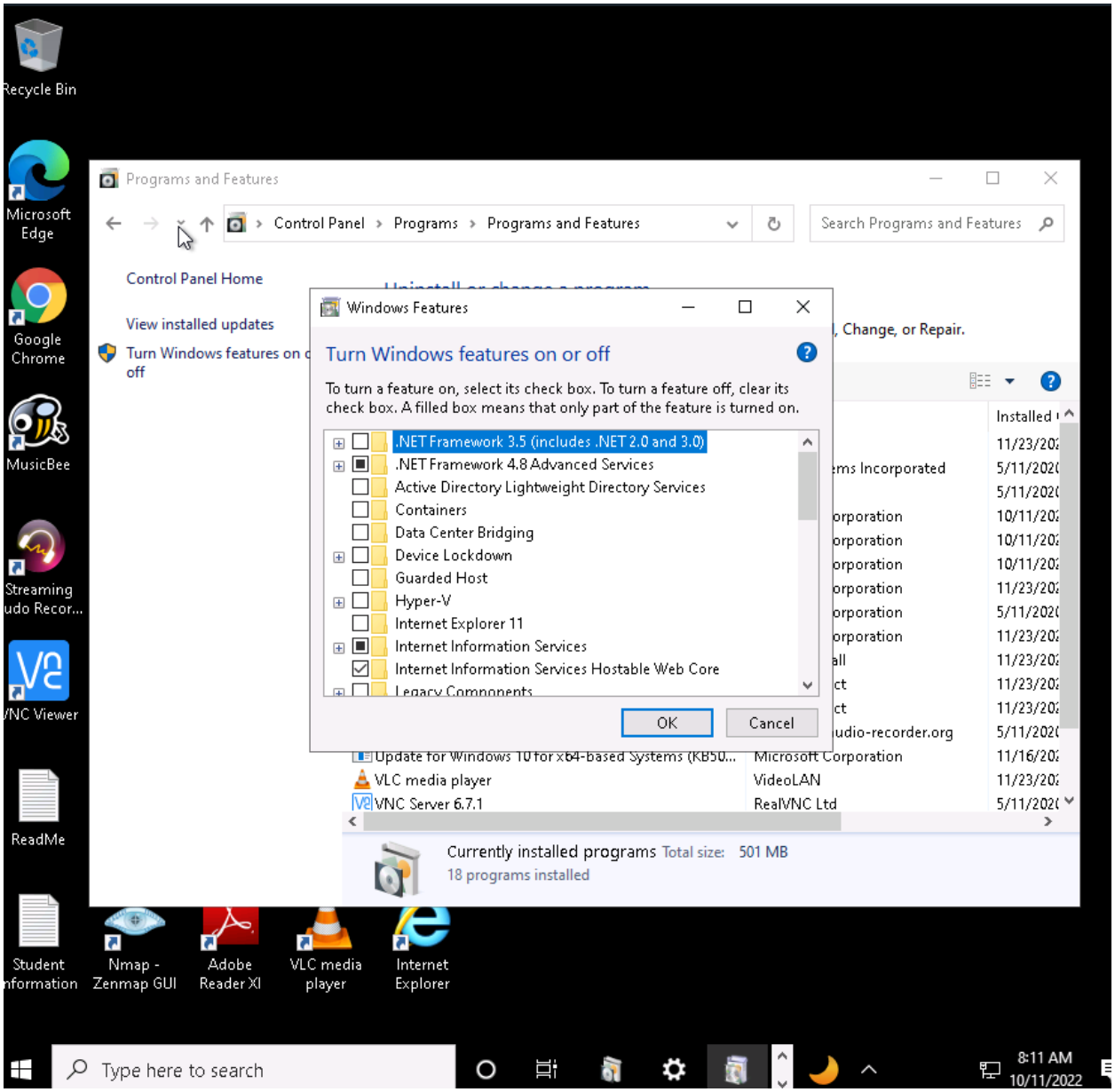


Windows Services

There are Windows features running on Joe's computer that could allow unwanted activity or files. He suspects that someone may have used the PC as a web server in the past. Joe wants you to confirm if web services are turned on, stop it if it is and make sure it is not running whenever the computer restarts.

1. How did you determine these services were running? Include screenshots to show how you found them.

From Turn Windows features on or off you can check all the services.



2. Advanced users should provide at least two methods for determining a web server is running on a host
3. How do you disable them and make sure they are not restarted?

From Control Panel → programs → programs and features → search Internet information services then Turn it off.

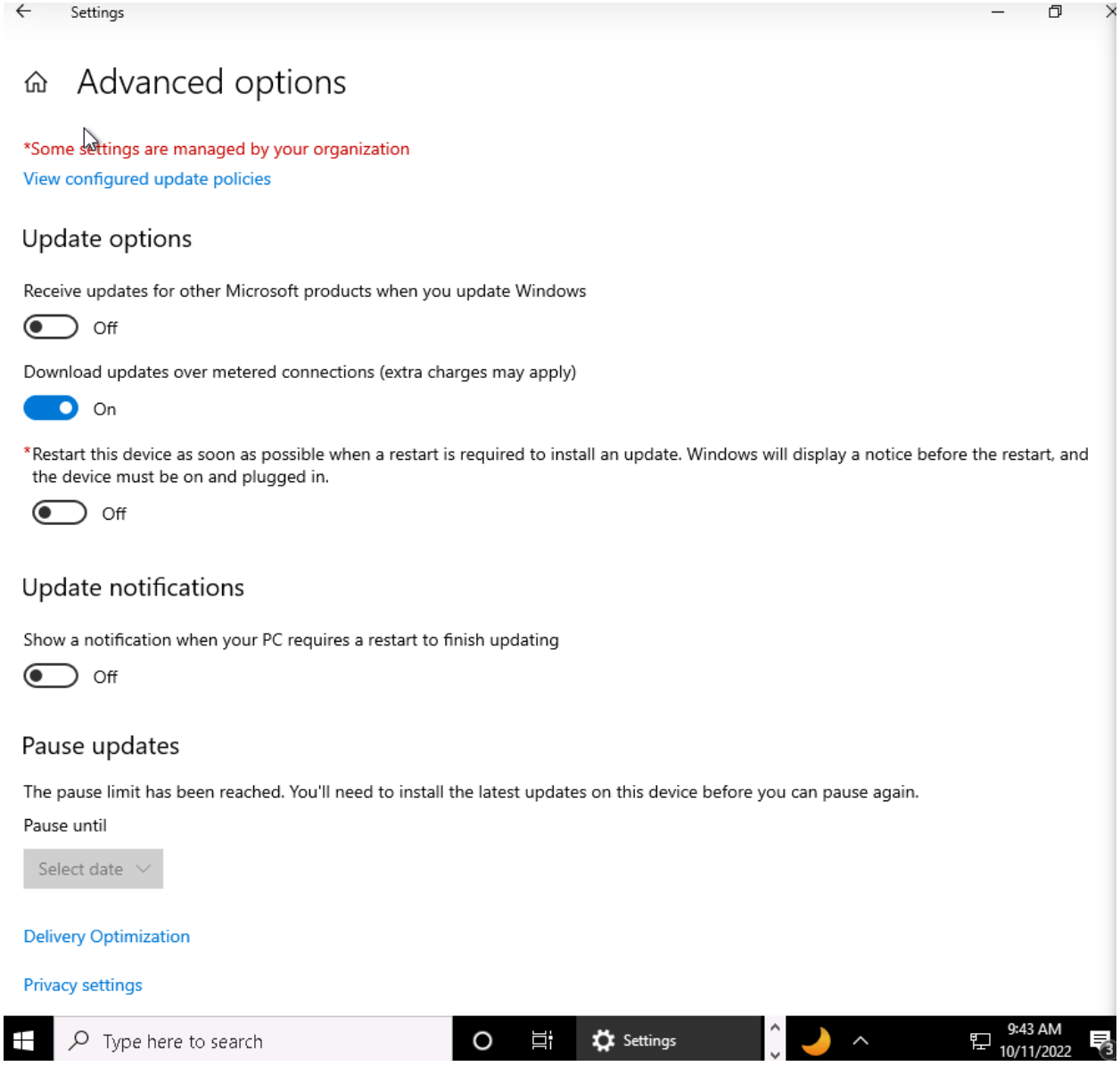
4. Advanced Users: The File Transfer Protocol FTP service is also running on this PC and shouldn't. Explain the process for disabling it and ensuring it is not automatically restarted.

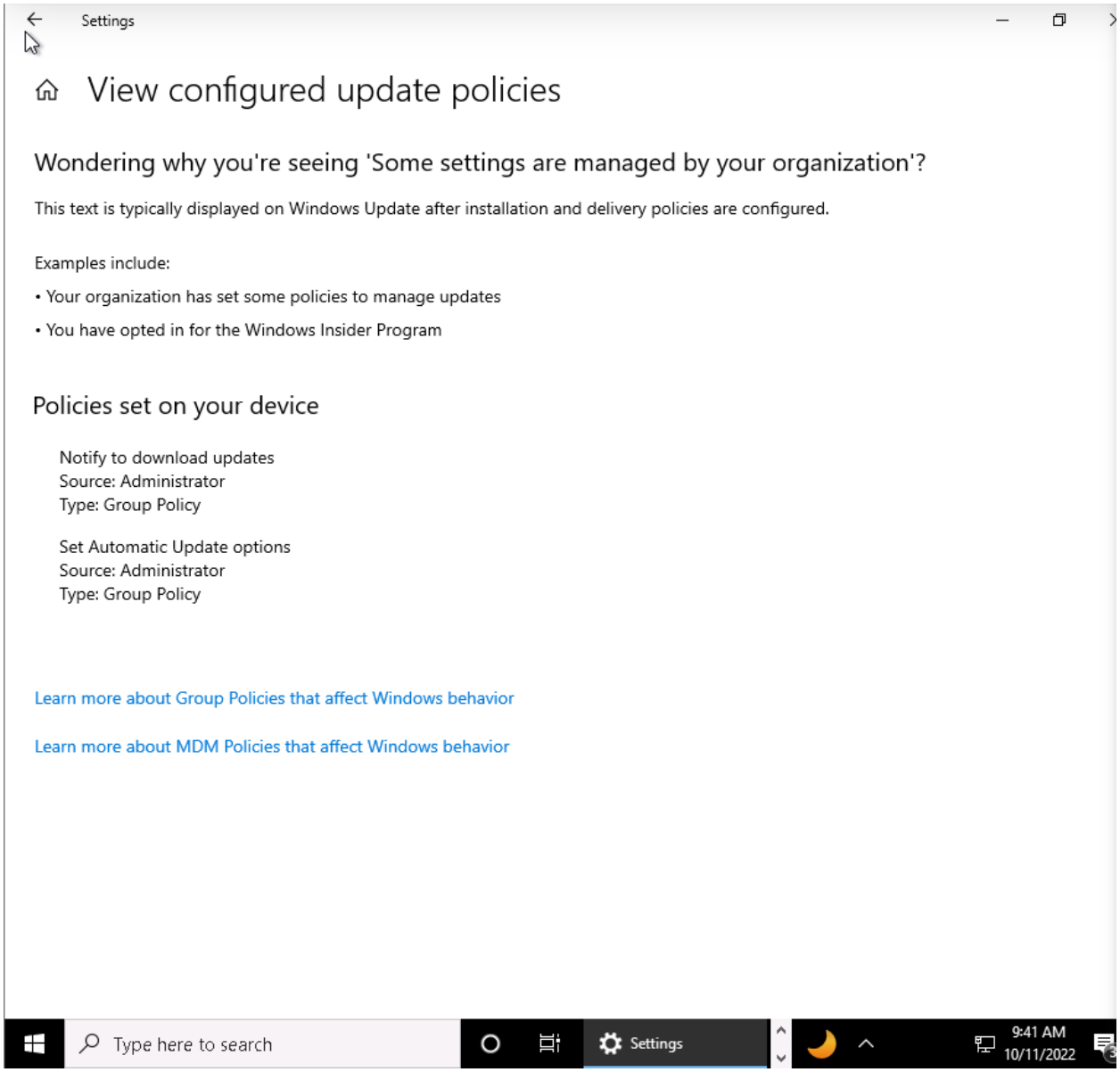
Patching and Updates

Keeping the operating system current on patches and fixes is a critical part of security. Joe wants his PC to be on the latest version of Windows 10. He also wants you to set it up for automated updates.

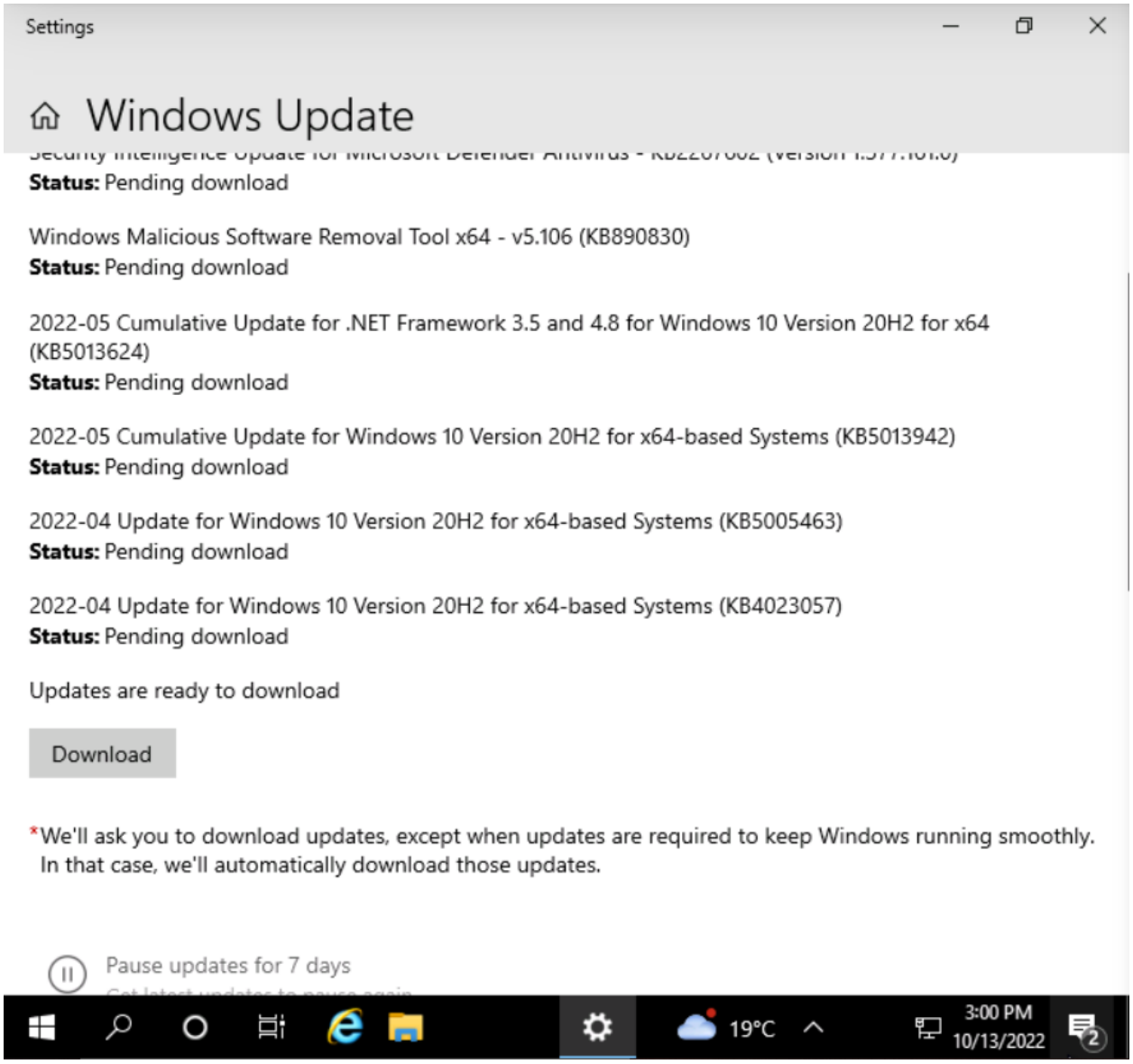
1. *Explain the process for doing this. Include screenshots as needed.*

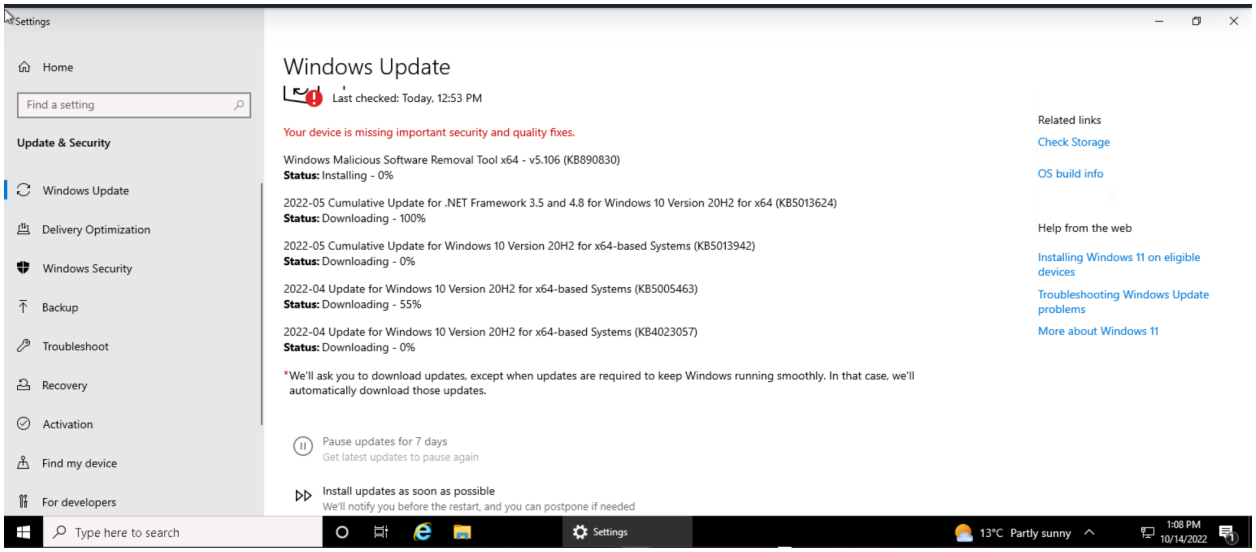
From Settings → Advanced options → turn on the download updates over metered connections.





2. *Go ahead and update this PC to the latest version. Warning this may take a while and require numerous restarts. When it is complete, provide a screenshot showing the PC is on the latest version.*


Settings
Windows Update
Status: Pending download
Windows Malicious Software Removal Tool x64 - v5.106 (KB890830)
Status: Pending download
2022-05 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 20H2 for x64 (KB5013624)
Status: Pending download
2022-05 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5013942)
Status: Pending download
2022-04 Update for Windows 10 Version 20H2 for x64-based Systems (KB5005463)
Status: Pending download
2022-04 Update for Windows 10 Version 20H2 for x64-based Systems (KB4023057)
Status: Pending download
Updates are ready to download
Download
*We'll ask you to download updates, except when updates are required to keep Windows running smoothly. In that case, we'll automatically download those updates.
Pause updates for 7 days
19°C
3:00 PM
10/13/2022



All applications should also be up to date on patches or fixes provided by the manufacturer. Any old versions of software should be uninstalled.

3. *List at least two applications on Joe's PC that are out of date. List them below:*

- I couldn't update the windows in the VM.

4. *Explain the steps you took to determine this information.*
5. *Explain the steps for updating each of these applications. Include screenshots as needed.*

5. Securing Files and Folders

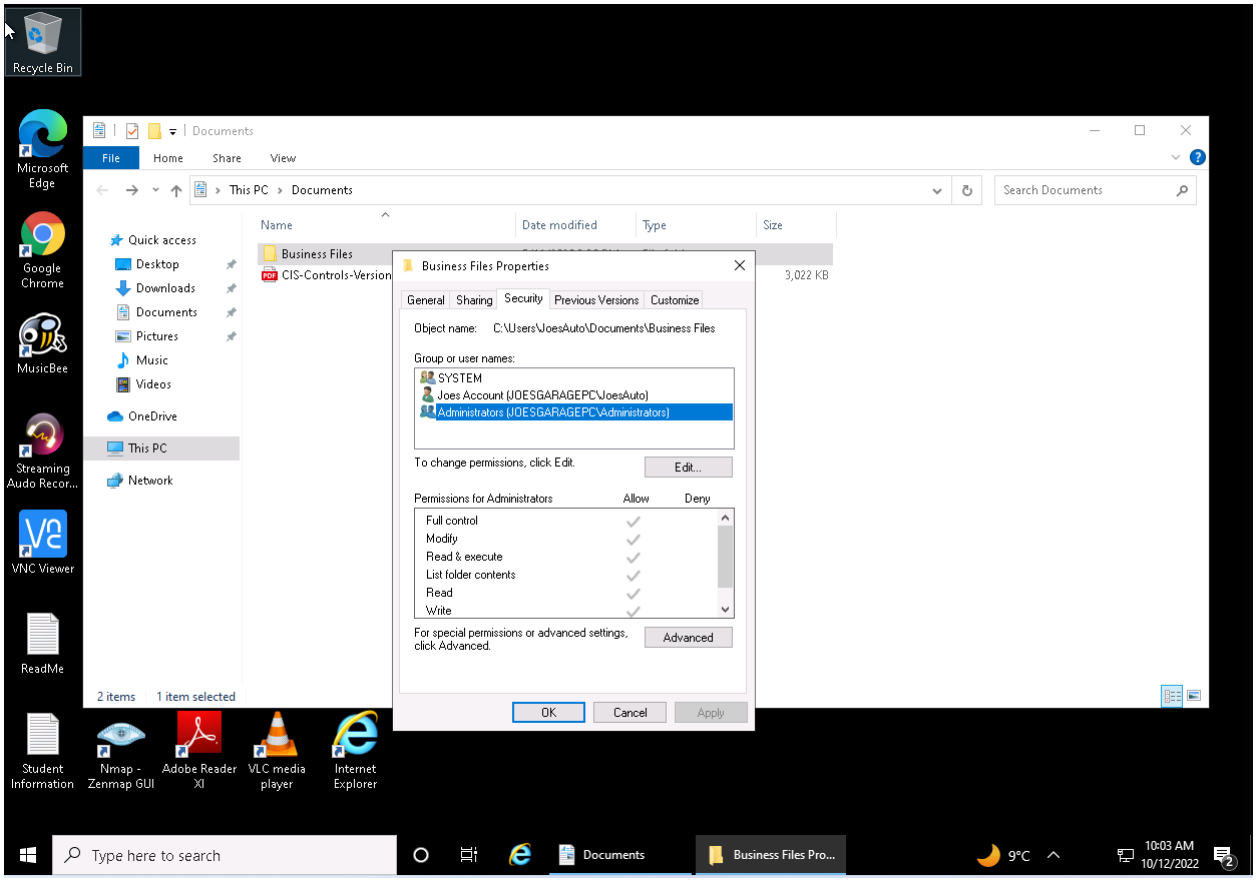
Joe has some work files in his Business folder that he wants to secure since they contain his customer information. They are labeled "JoesWork."

Joe suspects that other users on this computer beside him and Jane can see and change his business files. He wants you to check to make sure that only those two users have privileges to view or change the files.

Encrypting files and folders

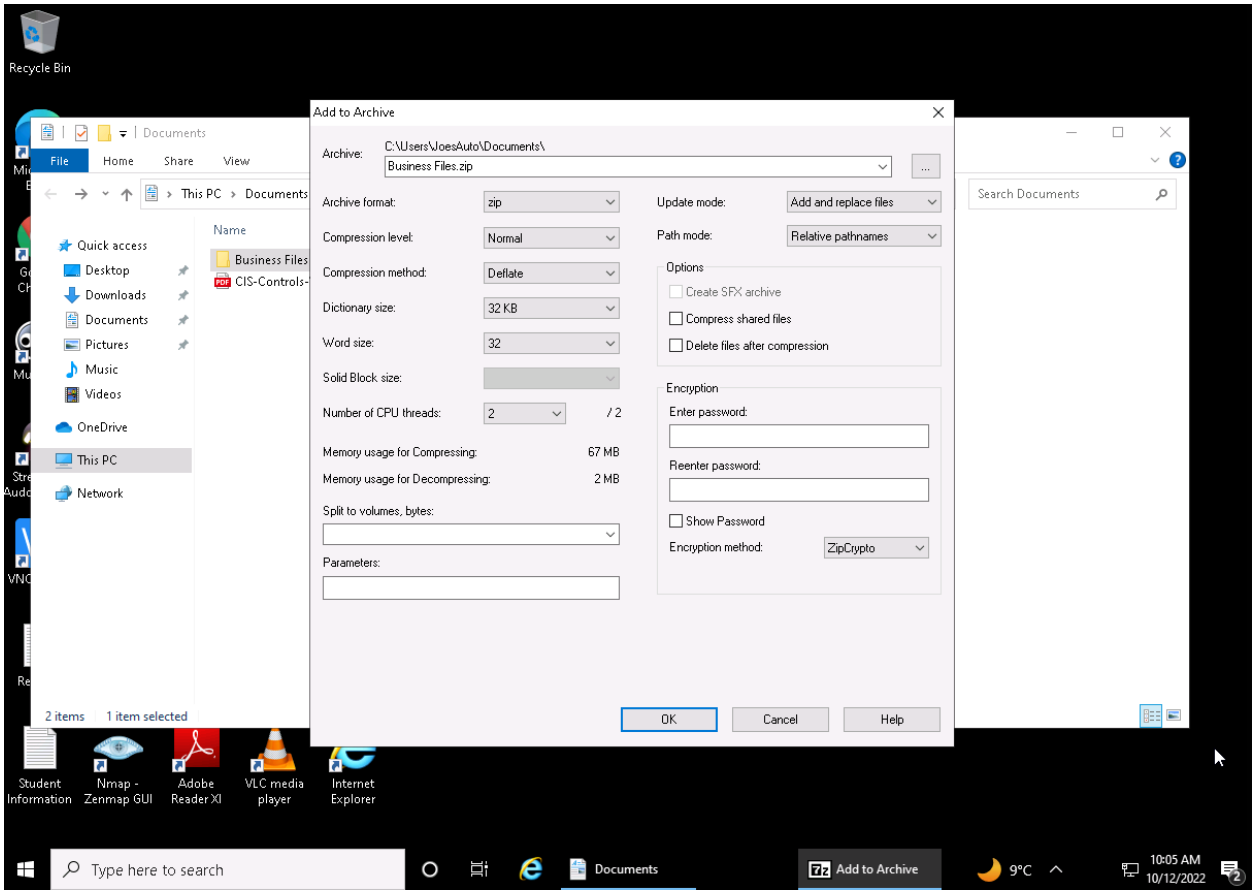
1. *Explain the process for checking this and changing any necessary settings on the file. Include screenshots showing that ONLY Joe and Jane have permissions to change Joes work files. [Hint: Right-click the folder and select Properties.]*

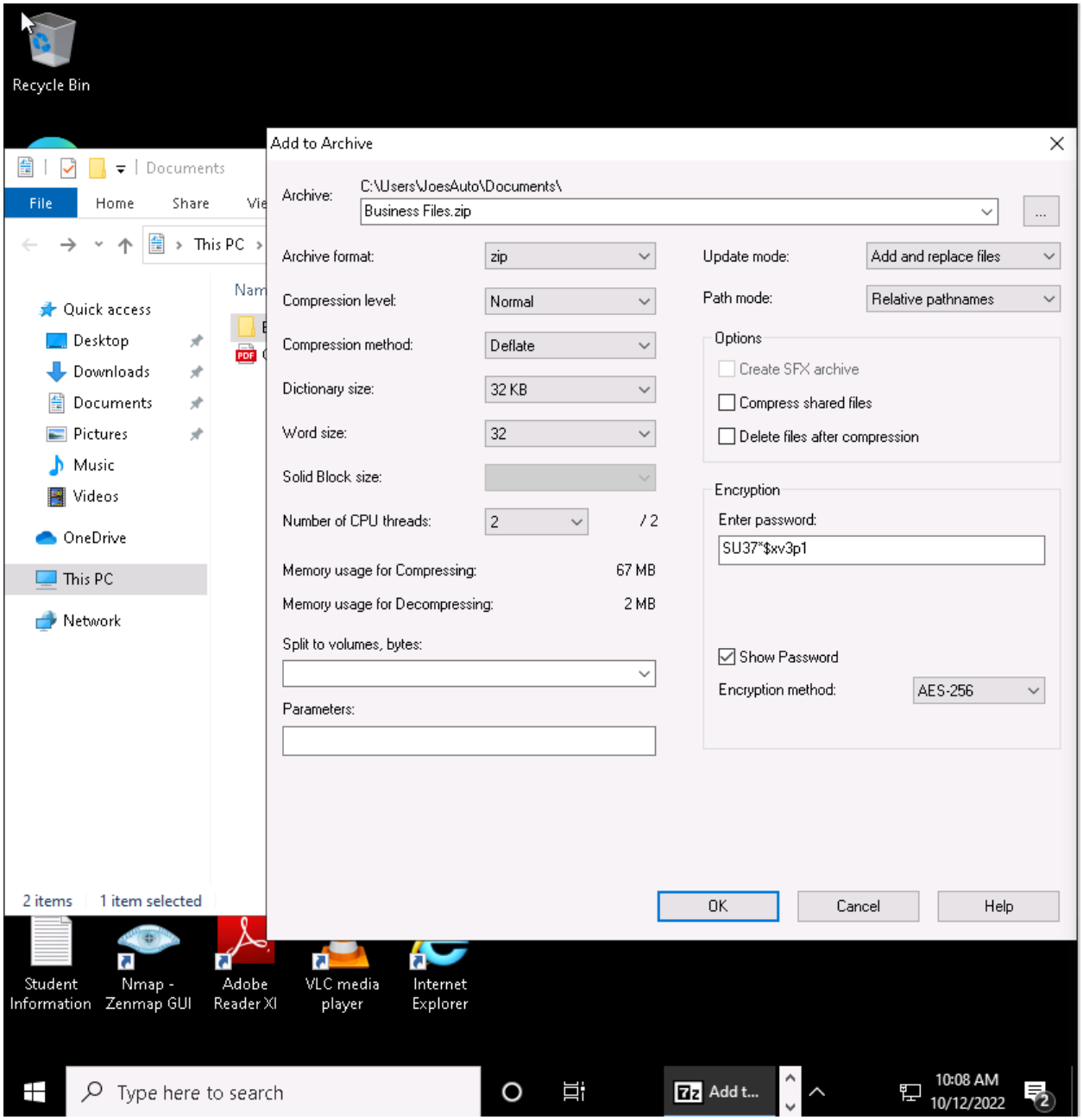
From the selected folder → right-click on the desired folder that needs changed and click on properties → Security tab → Advanced → remove all the unneeded users with permissions and only allow Joe and Jane.

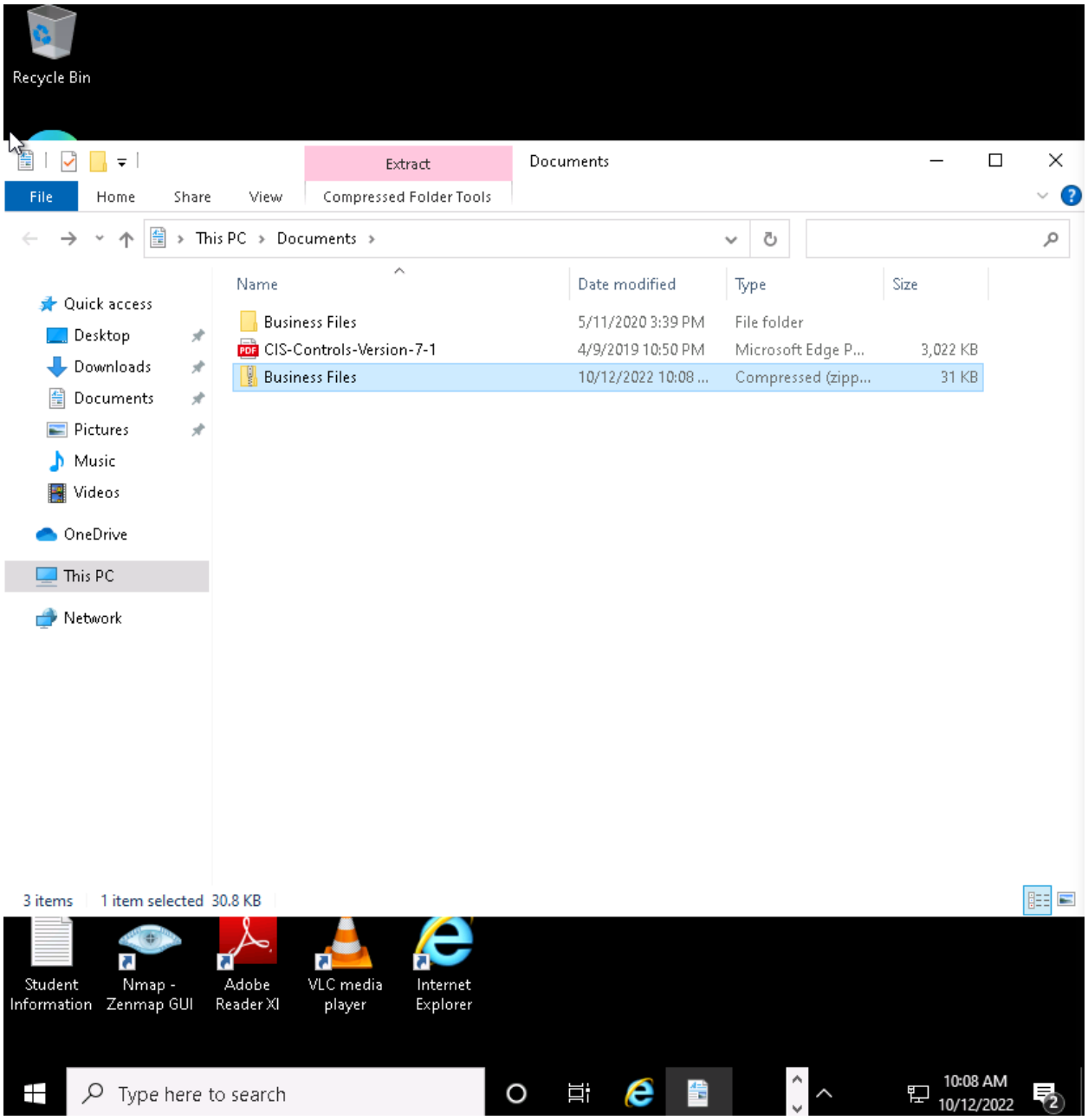


2. *Joe wants his work files encrypted with the password, "SU37*$xv3p1" Explain how you would do this. What encryption method do you recommend? You may use the pre-installed program 7-Zip for this.*

From the selected folder → right-click on the desired file that needs encryption with a password → Select 7-Zip → select Add to archive → Select the file type Zip then enter the password→ chose the desired encryption type(AES encryption is preferred to select) finally click on ok.


Recycle Bin
Add to Archive
Archive: C:\Users\JoesAuto\Documents\
Business Files.zip
Archive format: zip
Compression level: Normal
Compression method: Deflate
Dictionary size: 32 KB
Word size: 32
Solid Block size:
Number of CPU threads: 2 / 2
Memory usage for Compressing: 67 MB
Memory usage for Decompressing: 2 MB
Split to volumes, bytes:
Parameters:
Update mode: Add and replace files
Path mode: Relative pathnames
Options
Create SFX archive
Compress shared files
Delete files after compression
Encryption
Enter password:
Reenter password:
Show Password
Encryption method: ZipCrypto
OK
Cancel
Help
Documents
File Home Share View
This PC › Documents
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Business Files
CIS-Controls-
2 items 1 item selected
Search Documents
Student Information
Nmap - Zenmap GUI
Adobe Reader XI
VLC media player
Internet Explorer
Type here to search
Documents
Add to Archive
9°C
10:05 AM
10/12/2022


Recycle Bin
Add to Archive
Archive: C:\Users\JoesAuto\Documents\
Business Files.zip
Archive format: zip
Compression level: Normal
Compression method: Deflate
Dictionary size: 32 KB
Word size: 32
Solid Block size:
Number of CPU threads: 2 / 2
Memory usage for Compressing: 67 MB
Memory usage for Decompressing: 2 MB
Split to volumes, bytes:
Parameters:
Update mode: Add and replace files
Path mode: Relative pathnames
Options
Create SFX archive
Compress shared files
Delete files after compression
Encryption
Enter password:
SU37"$xv3p1
Show Password
Encryption method: AES-256
OK
Cancel
Help
Documents
File
Home
Share
This PC
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
2 items
1 item selected
Student Information
Nmap - Zenmap GUI
Adobe Reader XI
VLC media player
Internet Explorer
Type here to search
Add t...
10:08 AM
10/12/2022



3. *What security fundamental does this provide?*

Confidentiality

4. *The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?*

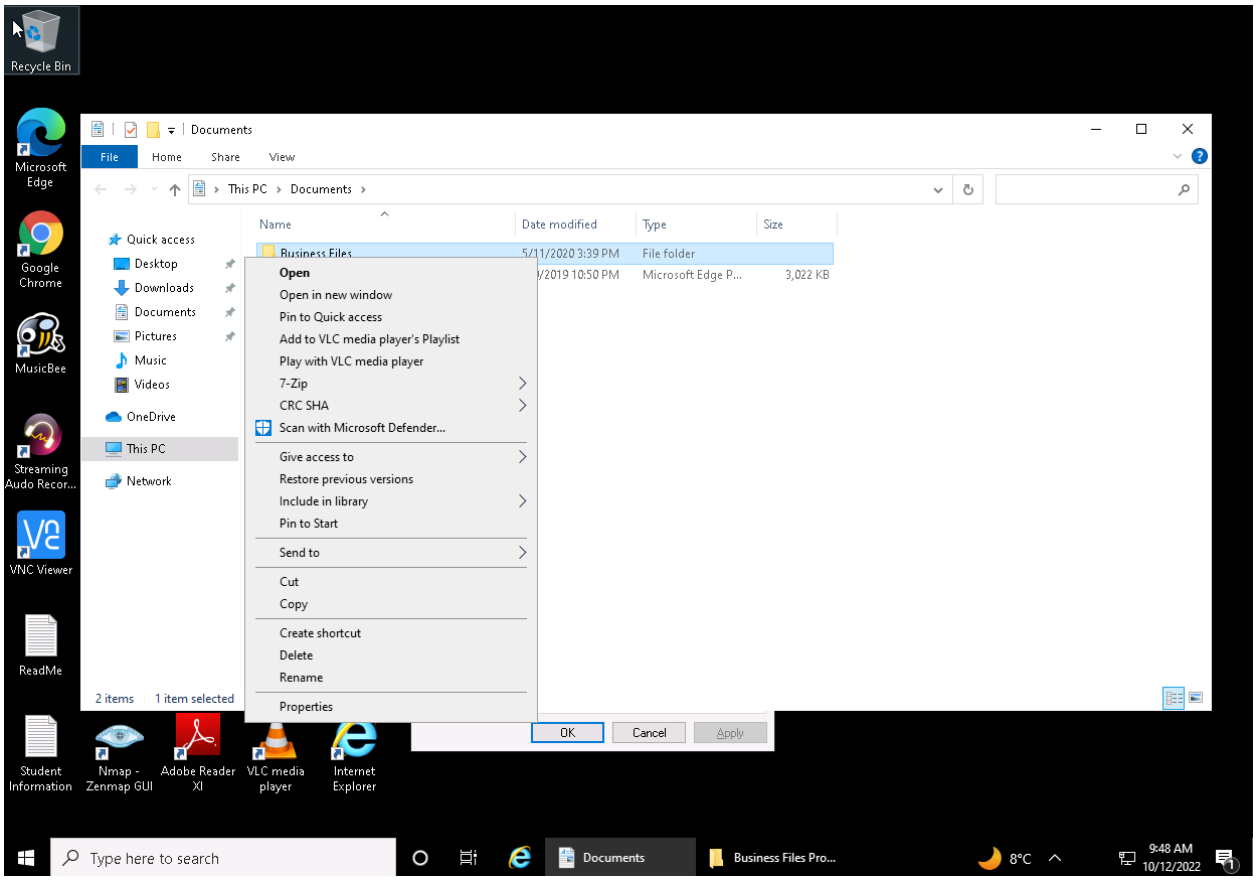
Data protection

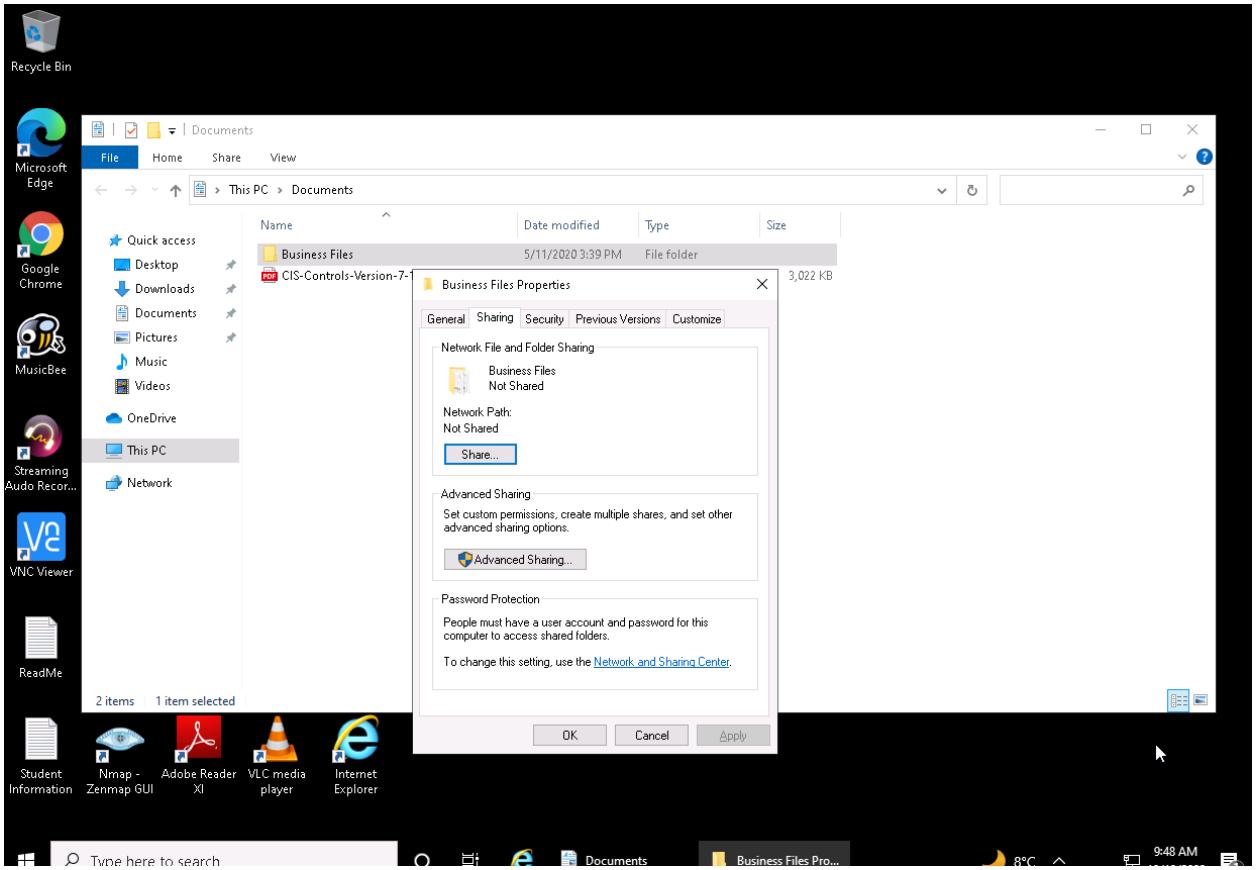
Shared Folders

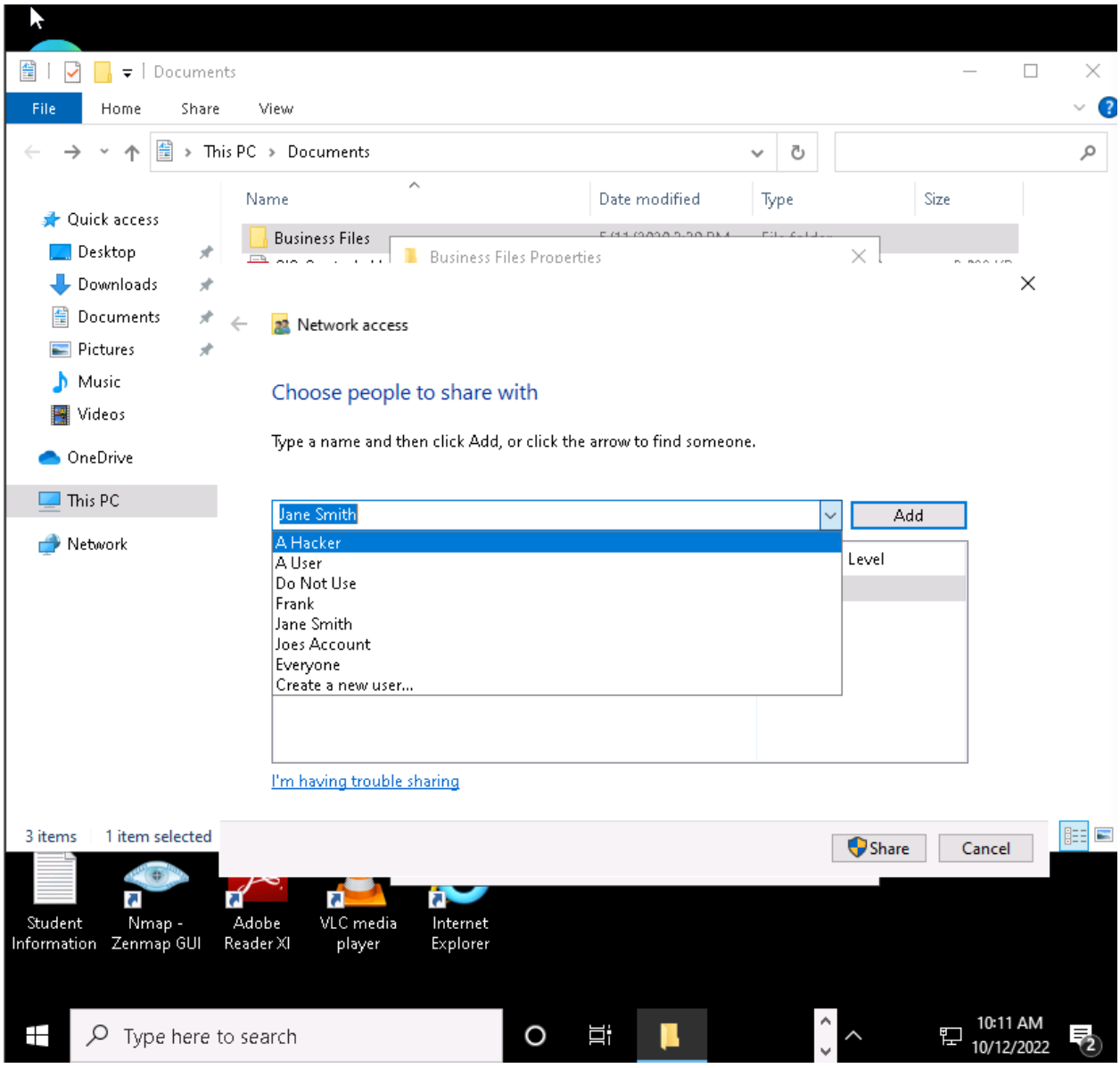
Shared folders are a common way to make files available to multiple users. There's a folder under Joe's documents called "Business Files" that Joe wants shared with his administrator Jane.

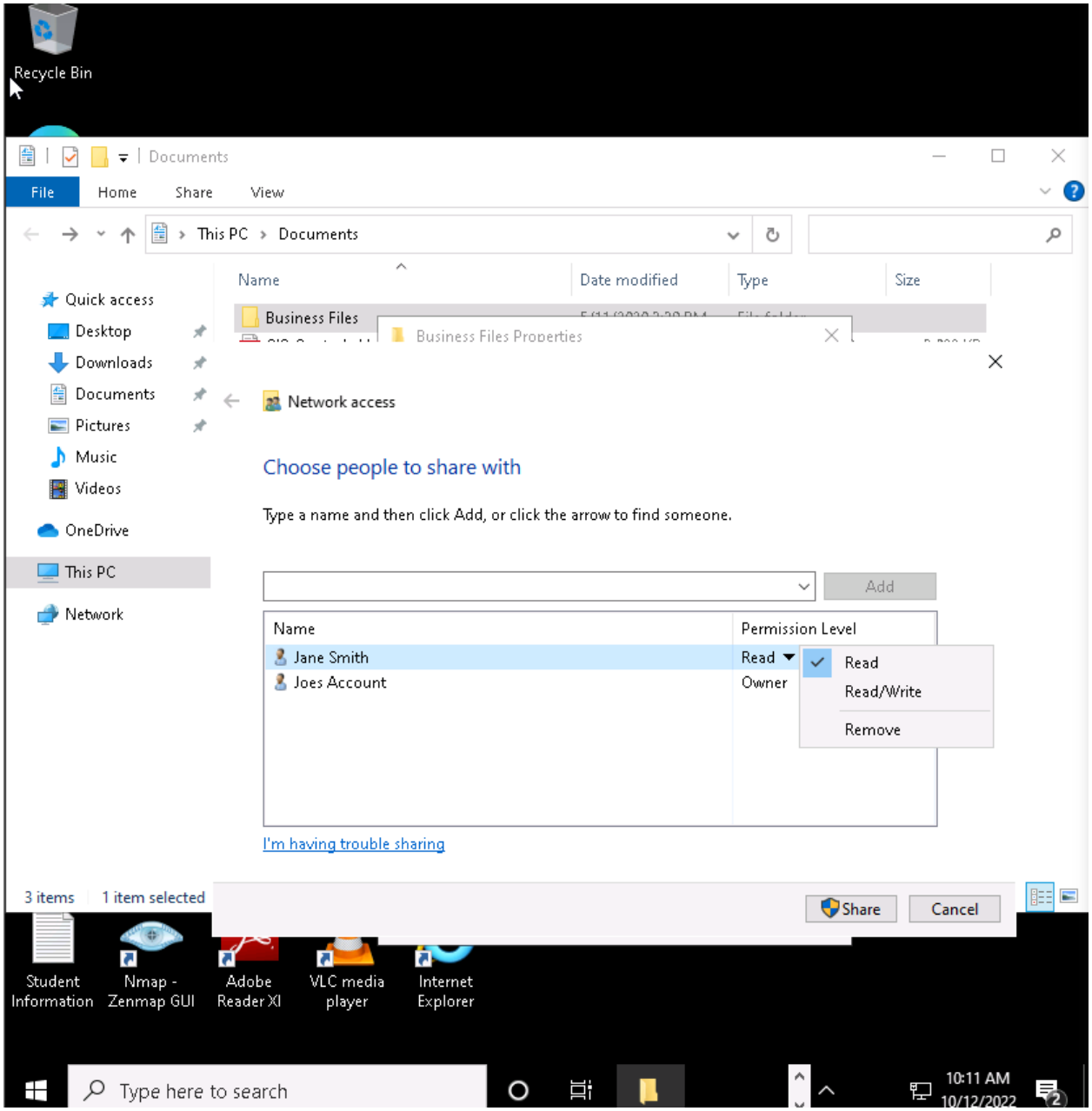
1. *Explain how you would do that and provide a screenshot showing how you can do it. Make sure it's only shared between Joe and Jane.*

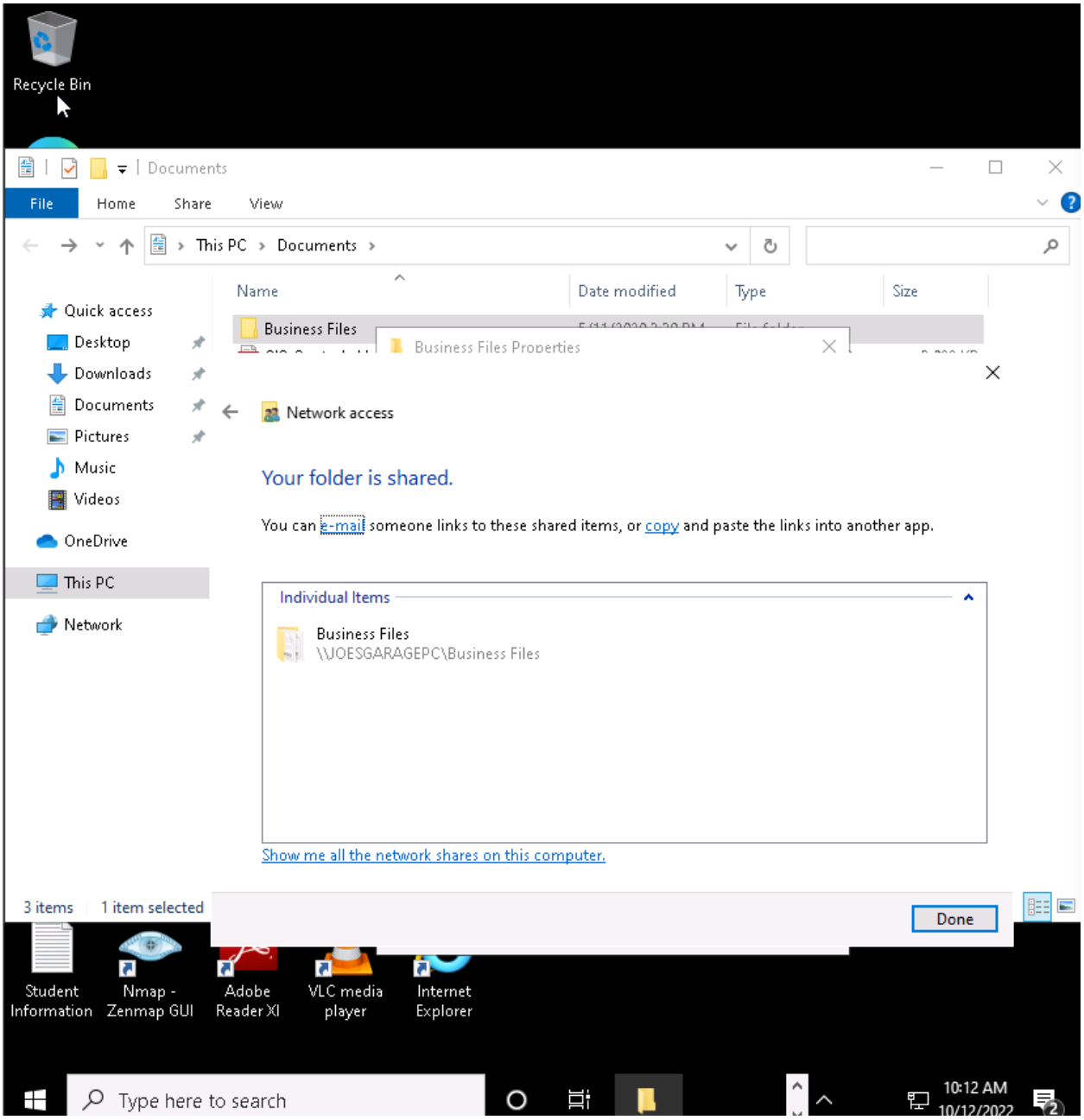
From the selected folder → right-click on the folder(*Business Files*) → click on sharing → click on advanced sharing → Select the Jane account file → chose the permissions for the folder → click on share then done.

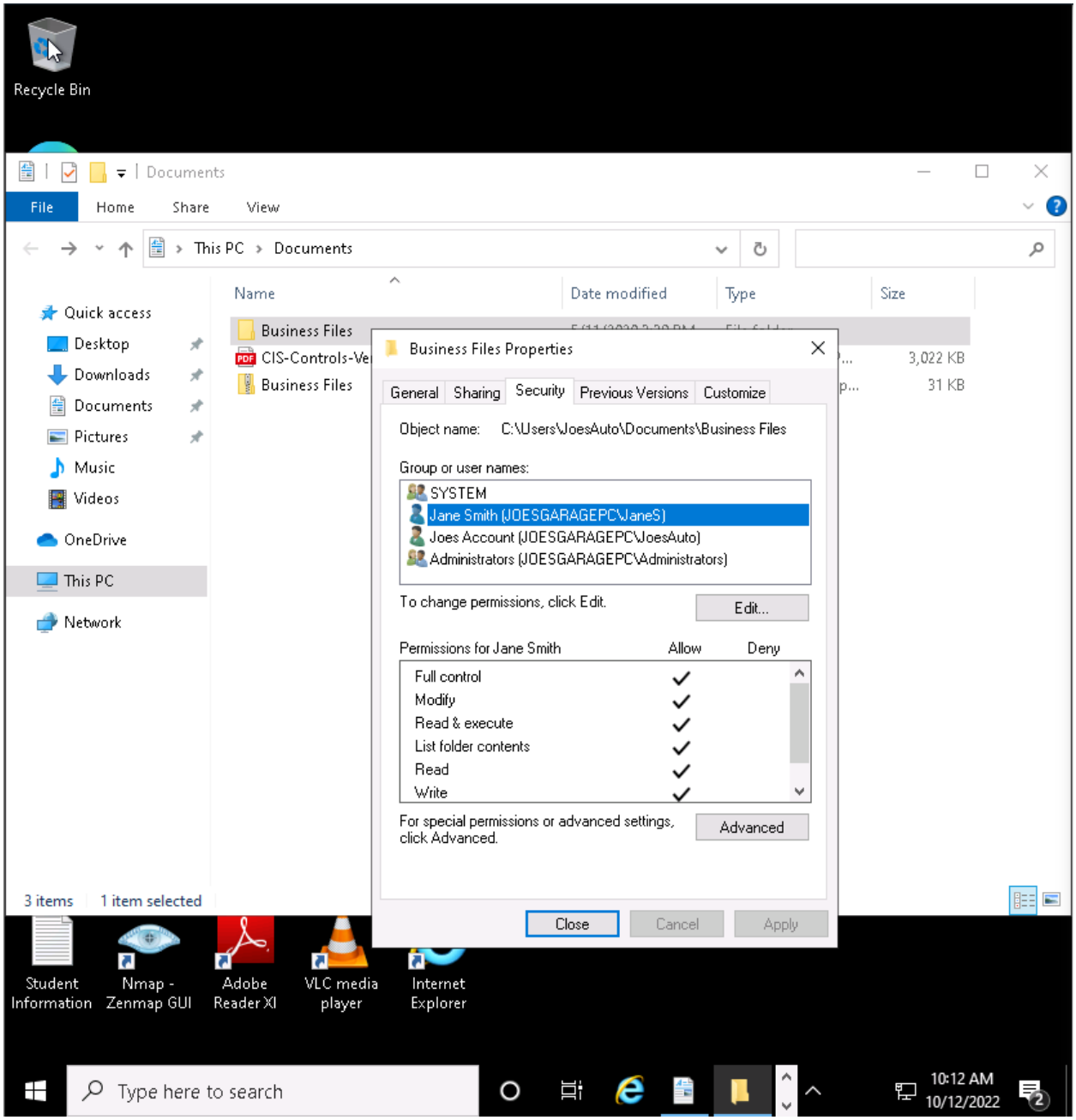



Recycle Bin
Microsoft Edge
Google Chrome
MusicBee
Streaming Audo Recor...
VNC Viewer
ReadMe
Student Information
Nmap - Zenmap GUI
Adobe Reader XI
VLC media player
Internet Explorer
Documents
File
Home
Share
View
This PC › Documents
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Business Files
5/11/2020 3:39 PM
File folder
CIS-Controls-Version-7-1
3,022 KB
2 items
1 item selected
Business Files Properties
General
Sharing
Security
Previous Versions
Customize
Network File and Folder Sharing
Business Files
Not Shared
Network Path:
Not Shared
Share...
Advanced Sharing
Set custom permissions, create multiple shares, and set other advanced sharing options.
Advanced Sharing...
Password Protection
People must have a user account and password for this computer to access shared folders.
To change this setting, use the Network and Sharing Center.
OK
Cancel
Apply
Type here to search
Documents
Business Files Pro...
8°C
9:48 AM


Documents
File
Home
Share
View
This PC
Documents
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Business Files
Business Files Properties
Network access
Choose people to share with
Type a name and then click Add, or click the arrow to find someone.
Jane Smith
Add
A Hacker
A User
Do Not Use
Frank
Jane Smith
Joes Account
Everyone
Create a new user...
Level
I'm having trouble sharing
3 items
1 item selected
Share
Cancel
Student Information
Nmap - Zenmap GUI
Adobe Reader XI
VLC media player
Internet Explorer
Type here to search
10:11 AM
10/12/2022


Recycle Bin
Documents
File
Home
Share
View
This PC
Documents
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Business Files
Business Files Properties
Network access
Choose people to share with
Type a name and then click Add, or click the arrow to find someone.
Add
Name
Permission Level
Jane Smith
Read
Joes Account
Owner
Read
Read/Write
Remove
I'm having trouble sharing
3 items
1 item selected
Share
Cancel
Student Information
Nmap - Zenmap GUI
Adobe Reader XI
VLC media player
Internet Explorer
Type here to search
10:11 AM
10/12/2022


Recycle Bin
Documents
File
Home
Share
View
This PC
Documents
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Business Files
Business Files Properties
Network access
Your folder is shared.
You can e-mail someone links to these shared items, or copy and paste the links into another app.
Individual Items
Business Files
\\JOESGARAGEPC\Business Files
Show me all the network shares on this computer.
3 items
1 item selected
Done
Student Information
Nmap - Zenmap GUI
Adobe Reader XI
VLC media player
Internet Explorer
Type here to search
10:12 AM
10/12/2022



2. *For advanced students: Joe wants to make sure there are no other folders shared on the PC. Explain how you view all shared files and folders on a Windows 10 PC. Include a screenshot as proof.*

6. Basic Computer Forensics (Optional)

Joe has asked that you investigate his PC to see if there are any other files left behind by previous unwanted users that may show they wanted to harm Joe's business. Look through the unwanted users' folders and list suspicious files. General students should document three issues and advanced students at least five issues. Include a brief explanation of their contents and their risks. [Hint: there is a "Hacker" in the PC]

-
-

7. Project Completion

Take the following steps when you are done answering the challenges and securing Joe's PC:

- Save your answer template as both a Word document and PDF. Make sure your name and date are on it.
- Shutdown the virtual Windows 10 PC.
- Submit the PDF to Udacity for review.