Udacity Cybersecurity Course #1 Project

Contents

Student Information	2
Scenario	3
1. Reconnaissance	4
2. Securing the PC	6
3. Securing Access	8
4. Securing Applications	10
5. Securing Files and Folders	13
6. Basic Computer Forensics (Advanced)	14
7. Project Completion	15

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: Nawaf Alyousef

Date of completion: 31/12/2022

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.

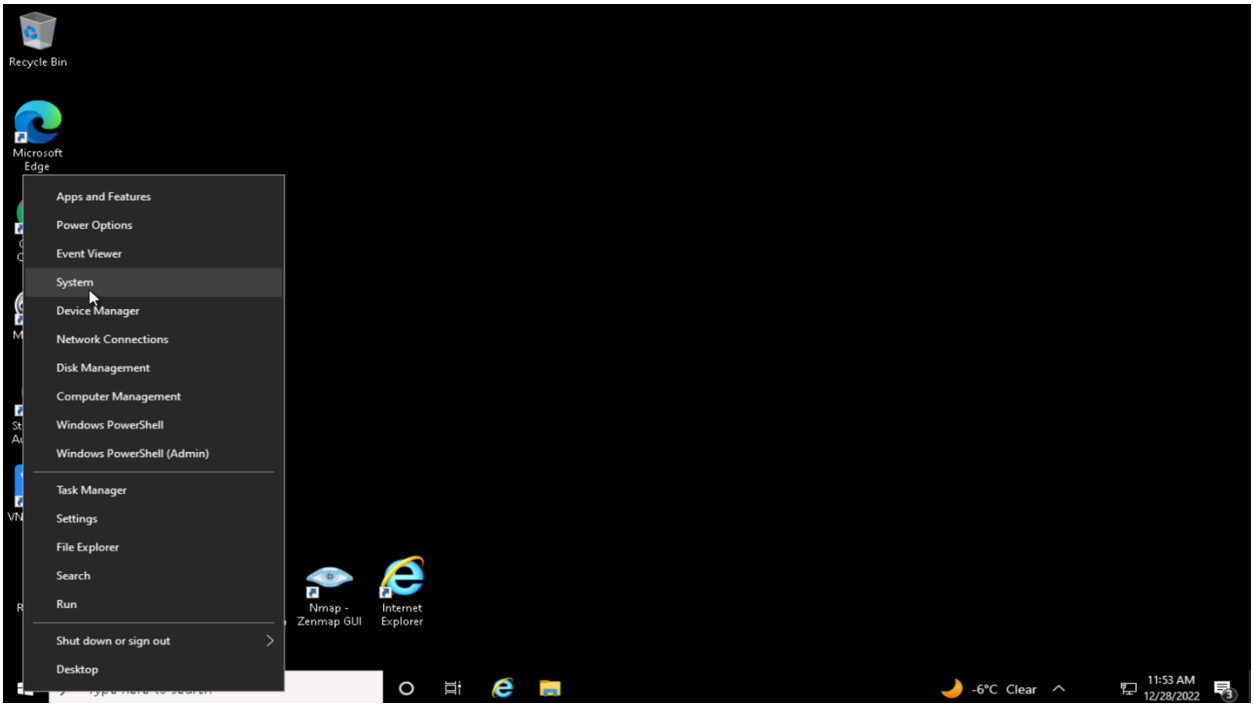
Complete each section below.

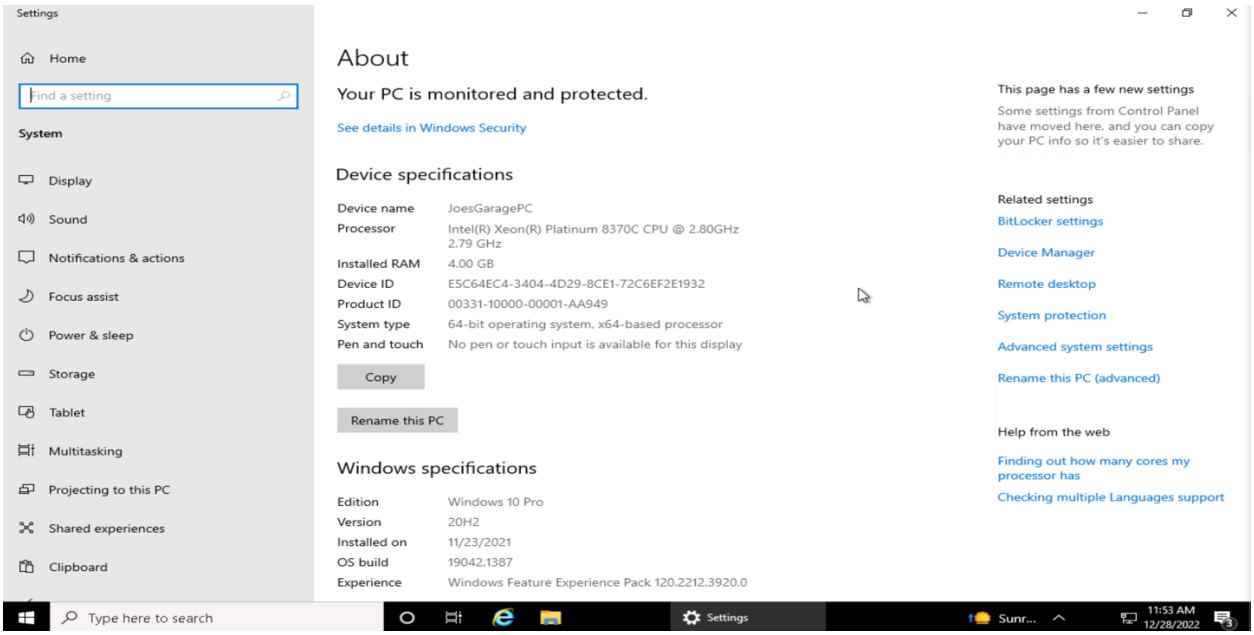
Hardware

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, x64-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:*
    - *Home >> right click >> system*
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), Date 11/23/2021
- Adobe Reader XI(11.0.01), Date 5/11/2020
- Candy Crush Friends, Date 12/28/2022
- Cortana, Date 12/28/2022
- Farm Herose Saga, Date 12/28/2022

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

    - *Home >> right click >> App & features*

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

    - *CIS Control 16: Application Software Security*

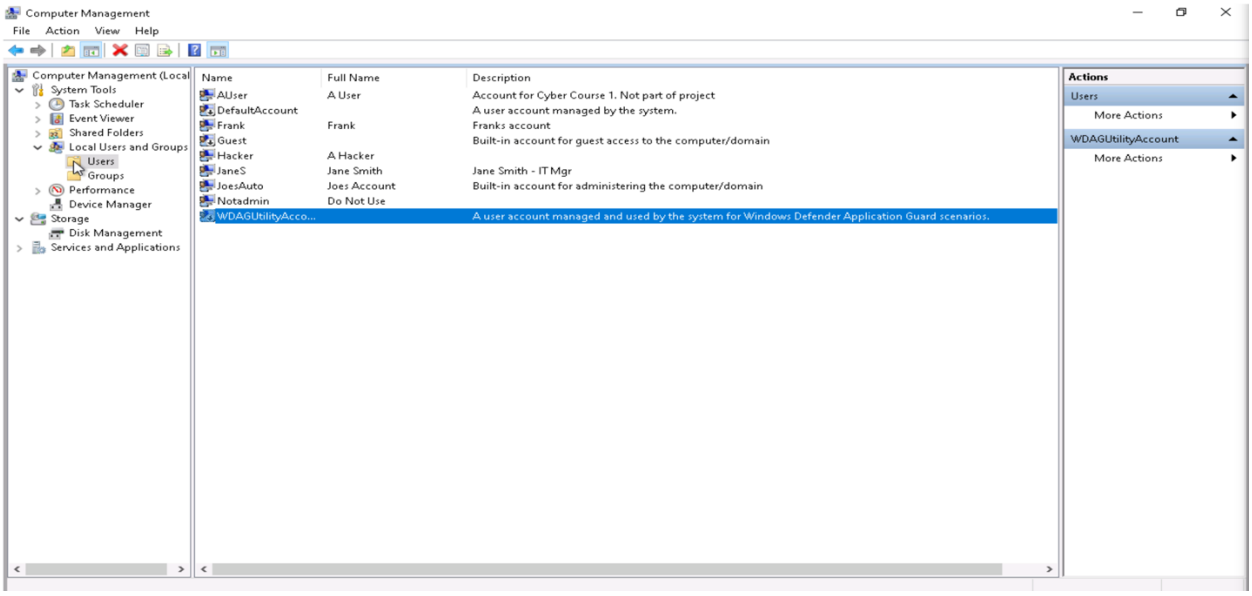
Accounts

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
AUser	A User	Account for Cyber Course 1. Not part of project
DefaultAccoount		A user account managed by the system
Frank	Frank	Frank accoount
Guest		Built-in account for guest access to the computer/domain
Hacker	A Hacker	
JaneS	Jane Smith	Jane Smith IT Mgr
JoesAuto	Joes Account	Built-in account for administering the computer/domain
Notadmin	Do Not Use	Do Not Use
WDAGUtilityAccount		A user account managed and used by the system for Windows Defender Application Guard scenarios.

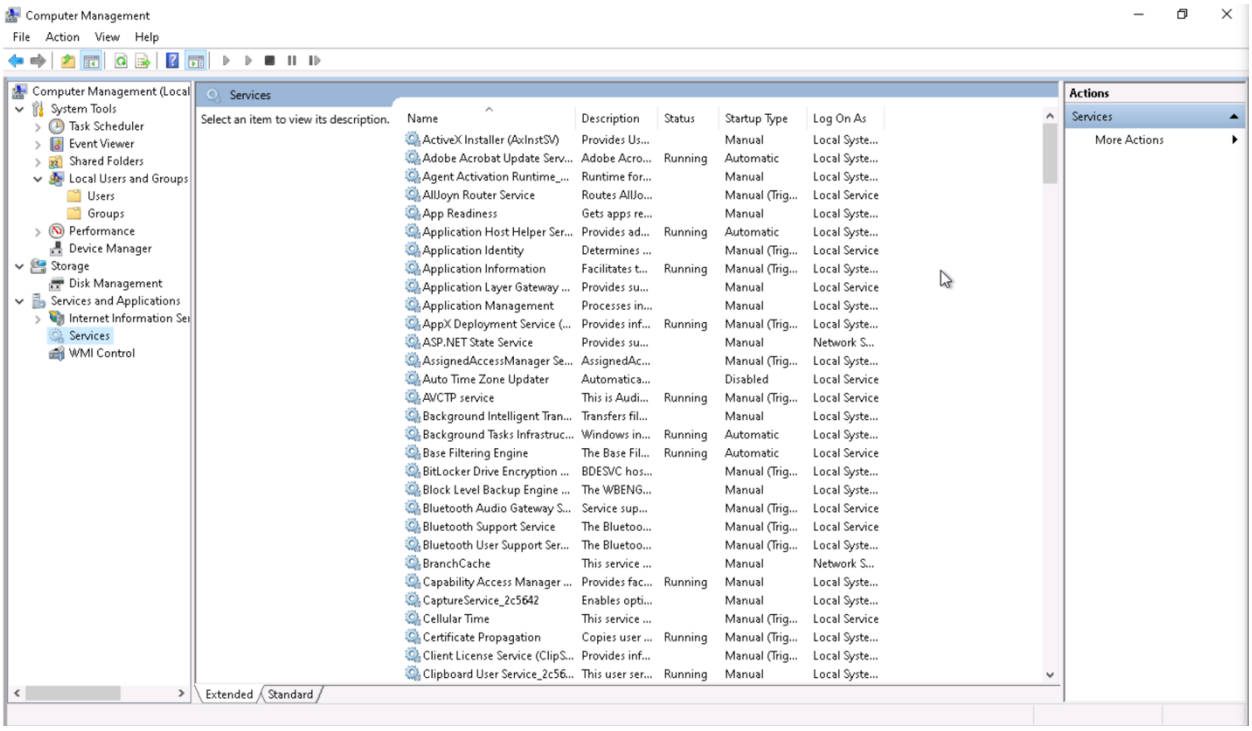
2. *Provide a screenshot of the Local Users.*



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.

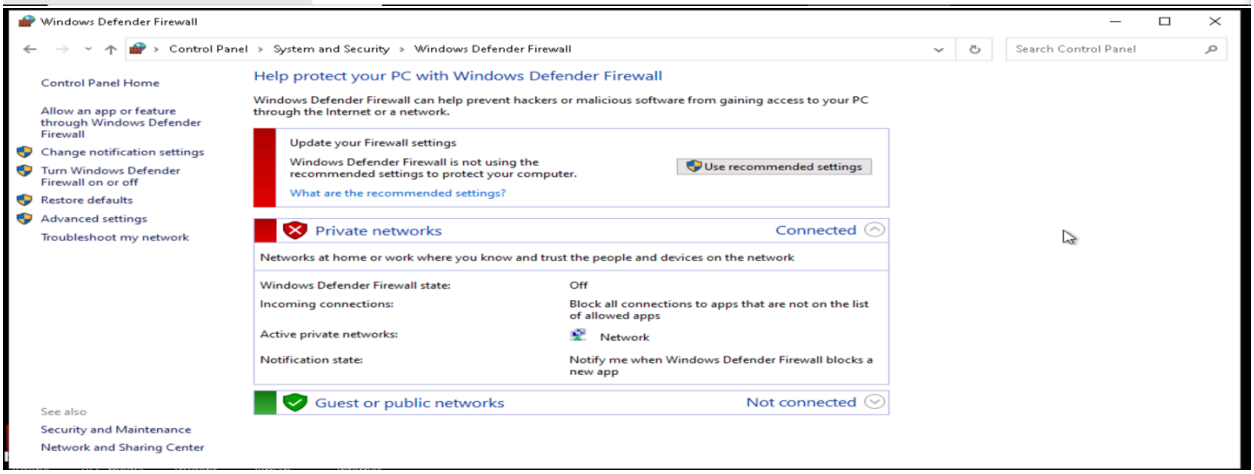
1. *Provide a screenshot of the services running on this PC.*



Security Services

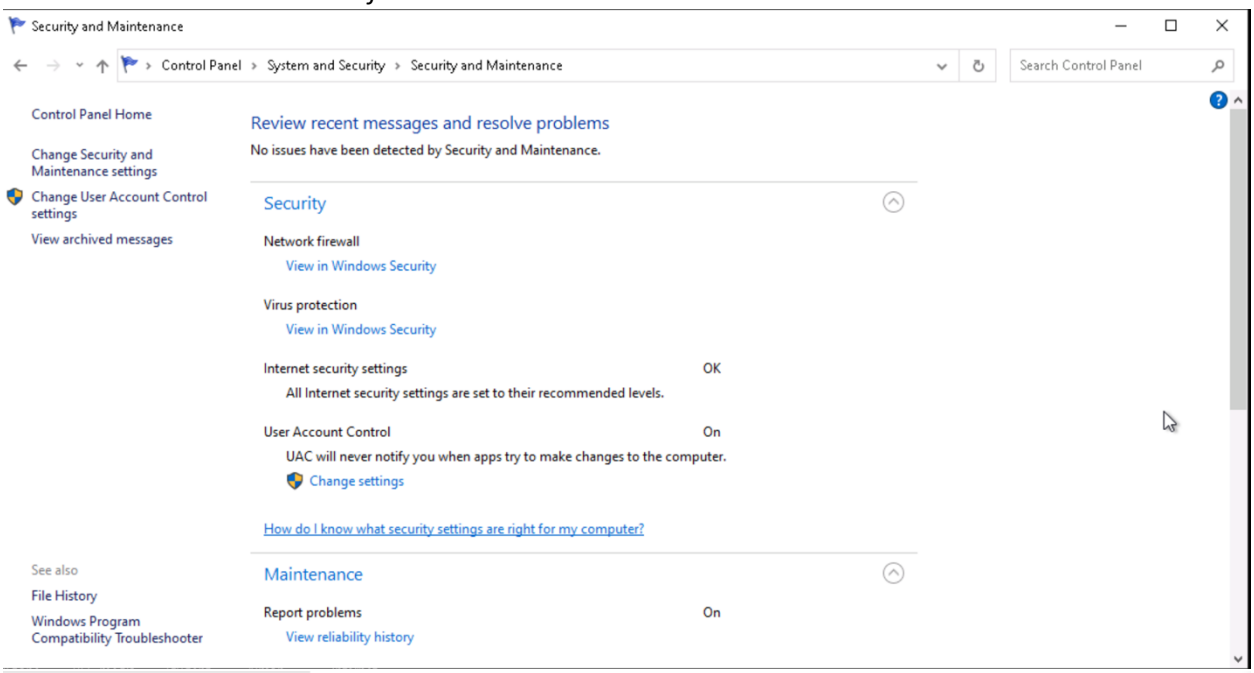
Joe wants to ensure that standard security services are running on his PC. He's content with using default Windows security settings and applications except for the rules outlined later. **Reminder that at this point you are just reporting what you observe. Do not make any changes to security settings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

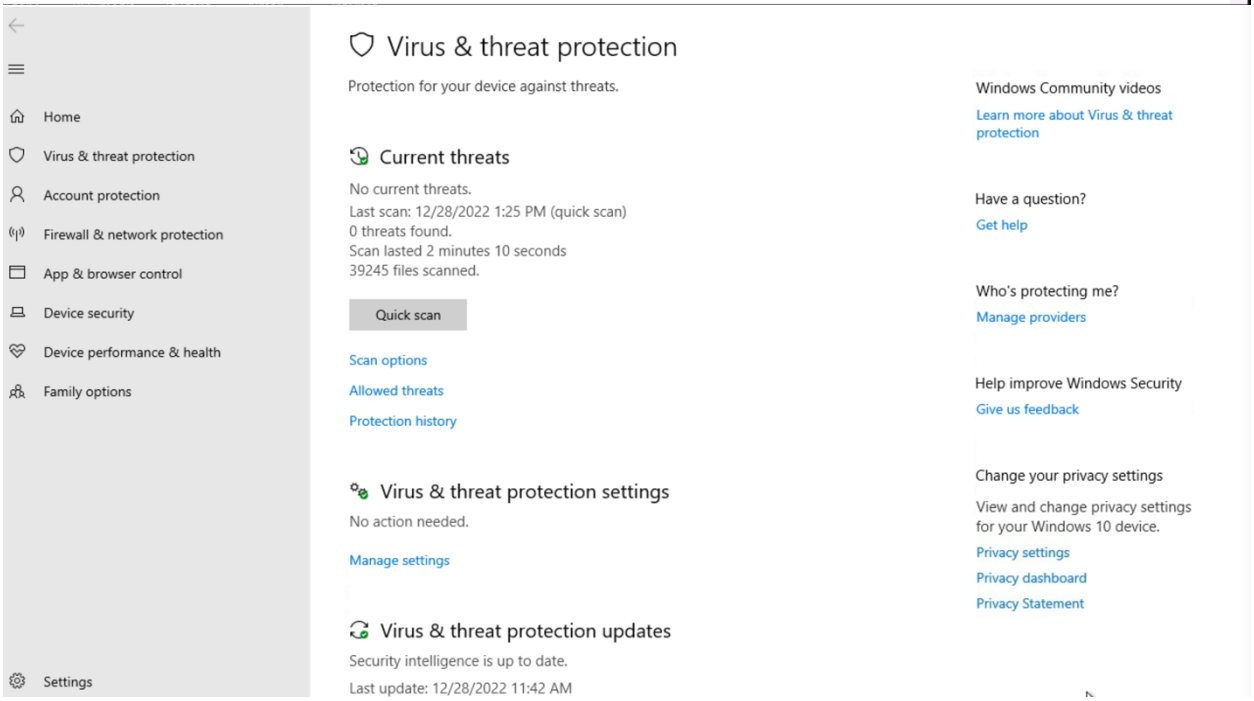
1. *To view a summary of security on Windows 10, start from the **Control Panel**. Use the "Find a setting" bar and search on Windows Defender. You can also search for Windows Defender using the Windows Run bar. Take a screenshot of what you see on the Windows Security screen and include it here:*



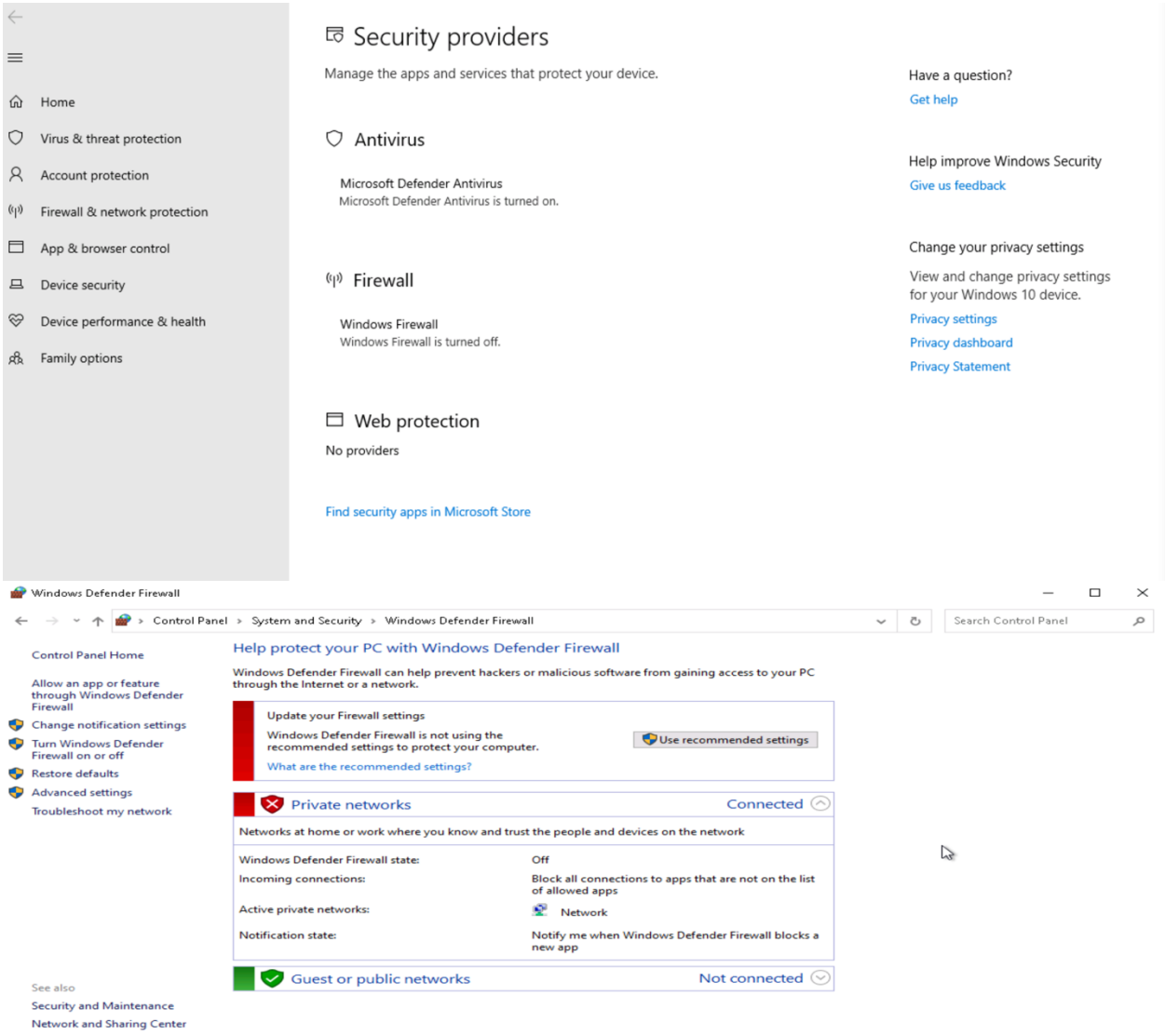
2. *The Windows 10 Security settings are also found from the* ***Control Panel > System and Security > Security and Maintenance****. Start by viewing* ***"Review your computer's status and resolve***

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

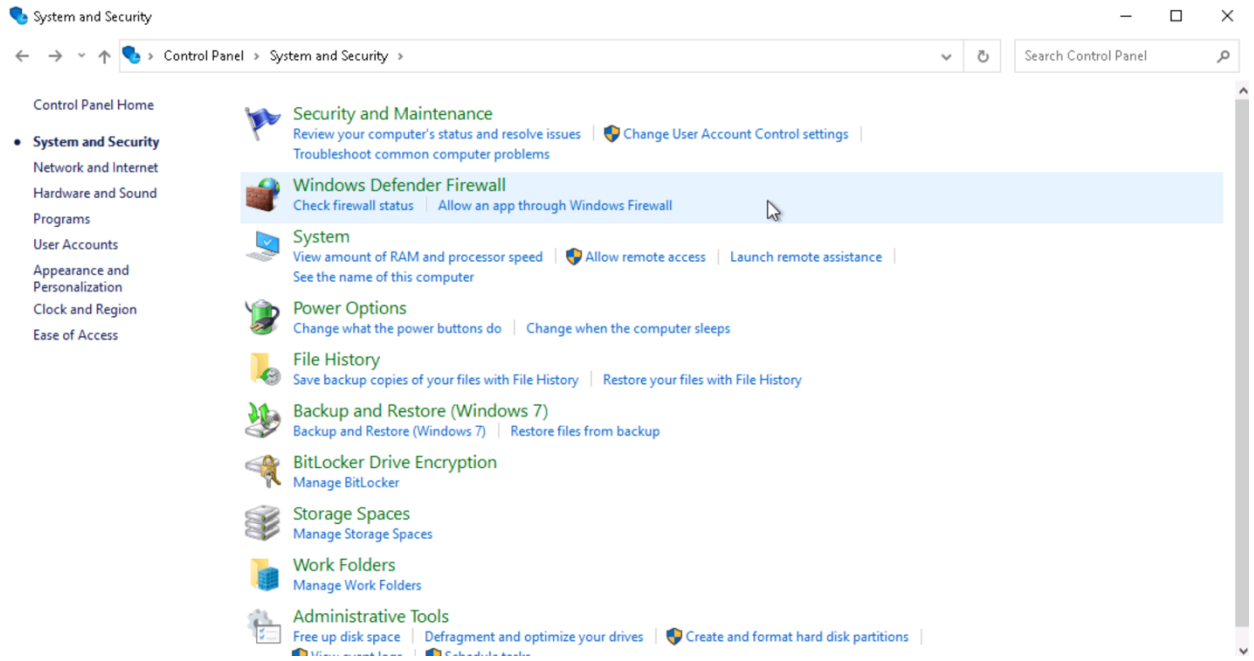


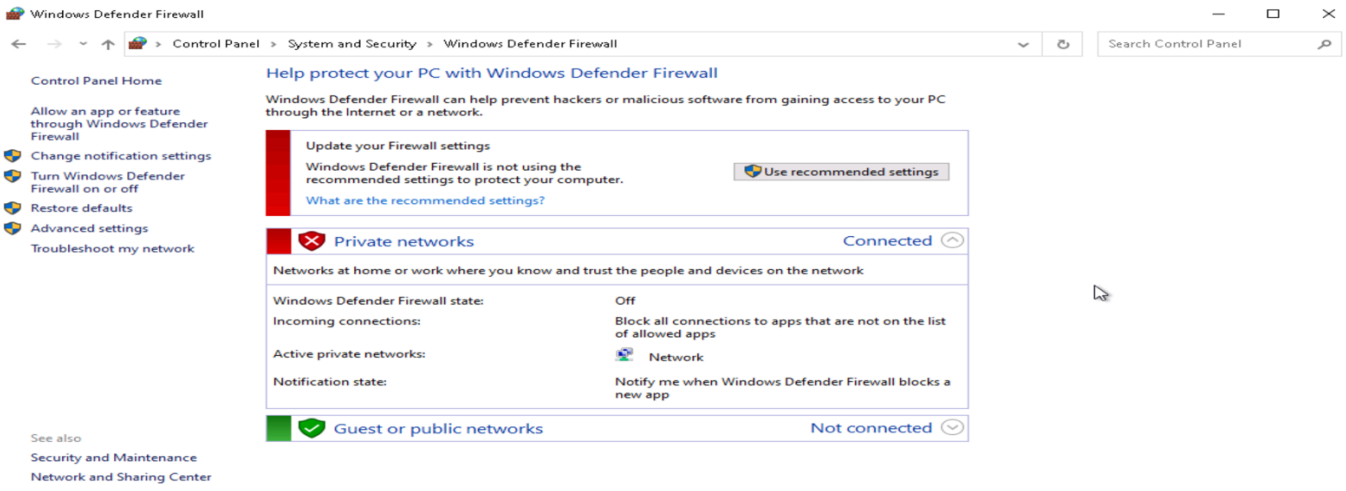


3. *Click on View in Windows Security to see the status there. Provide a screenshot of the **Firewall** settings.*

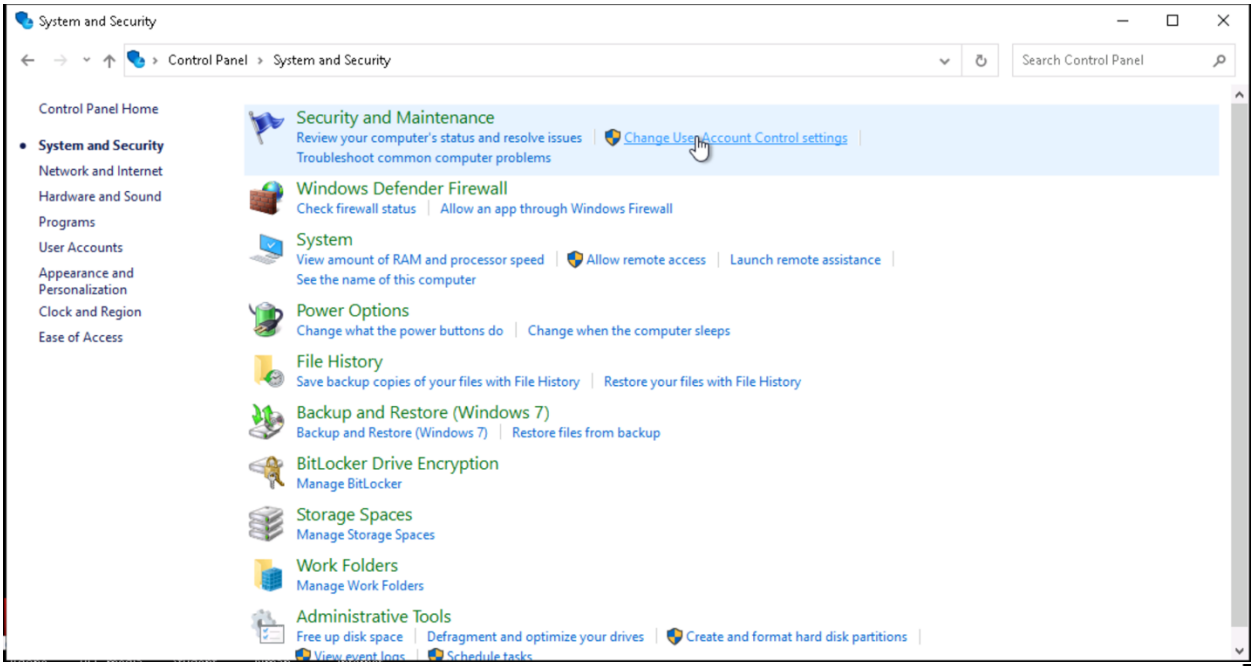


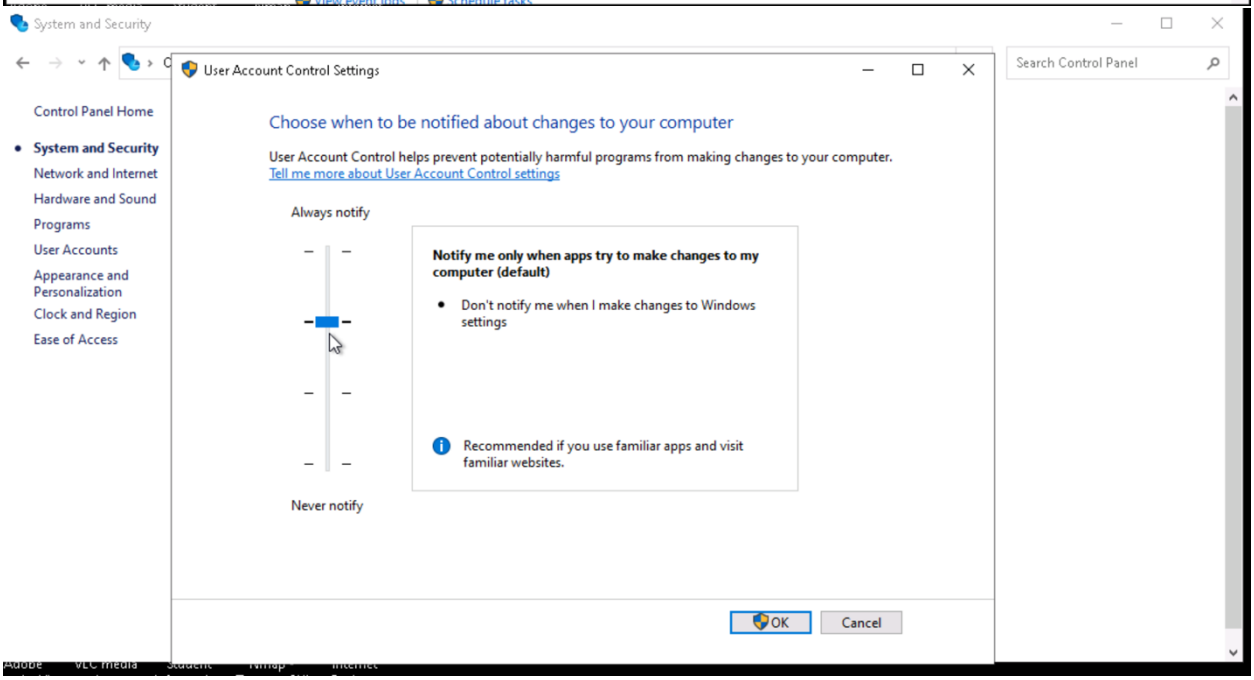
4. *From the **Control Panel**, go to **System and Security**. In that window, select **Windows Defender Firewall**. Provide a screenshot of it here:*





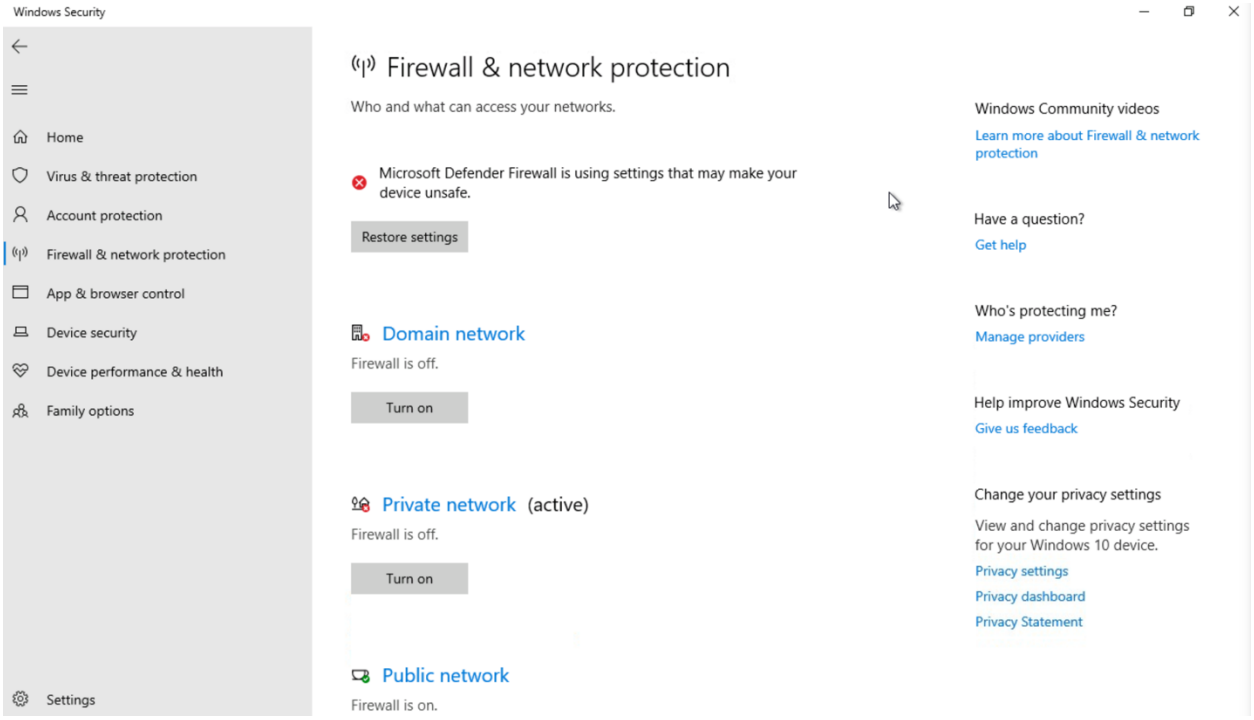
5. *PC users should be notified whenever there is a security or maintenance message. In the Security & Maintenance window, click on Change Security and Maintenance settings and take a screenshot. Paste it here:*

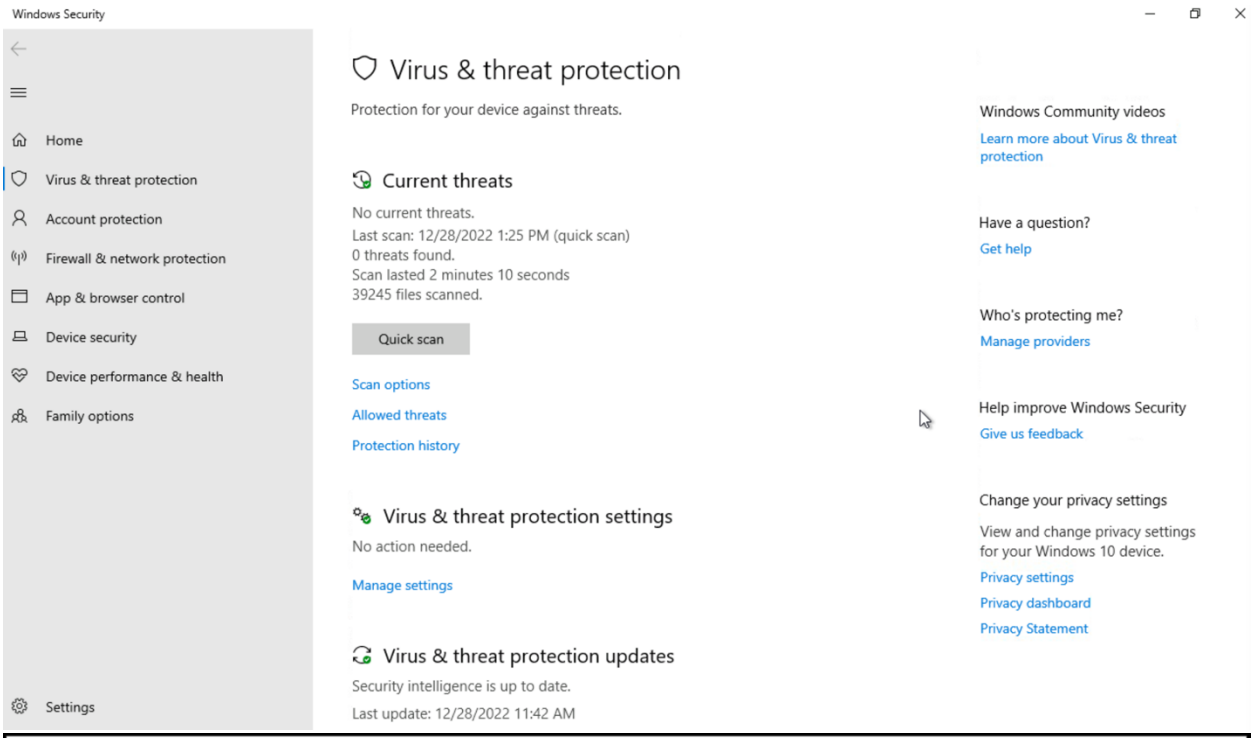


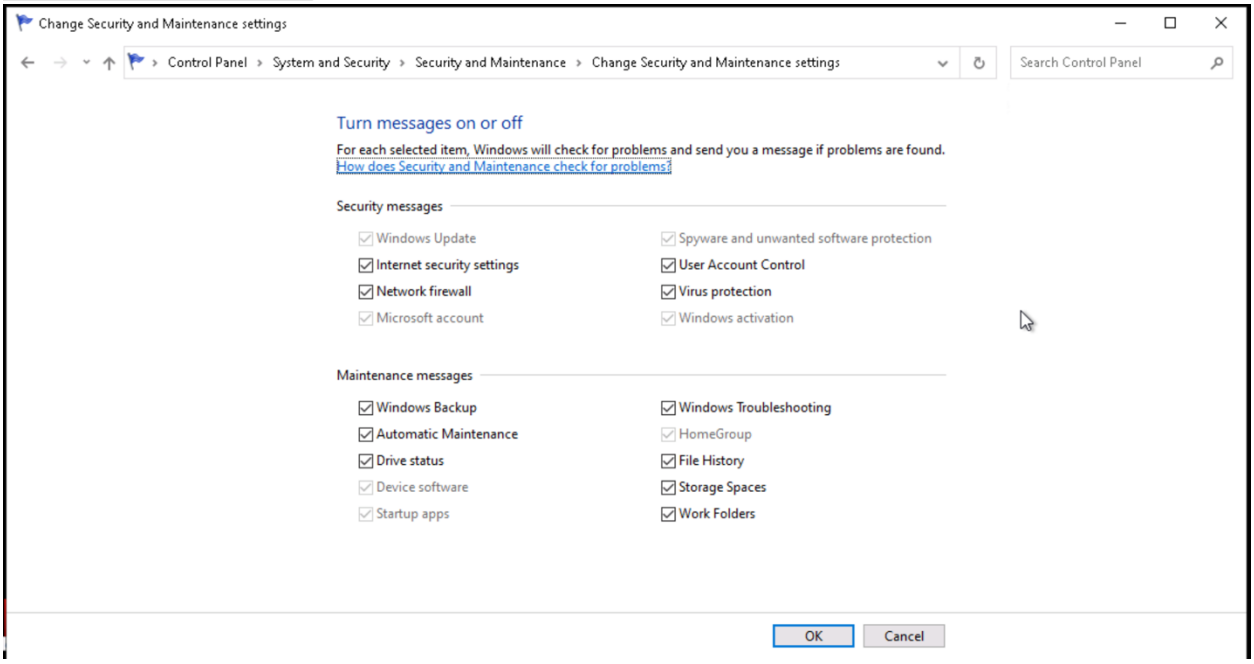


6. *Document the status of the PC's security settings listed below. Include the process you used to determine this information along with any screenshots. At this point, you are only documenting what you find. Do not make changes (yet).*

Security Feature	**Status**
Firewall product and status – Private network	Firewall is off
Firewall product and status – Public network	Firewall is on
Virus protection product and status	No current threats. last scan:12/28/2022 1:25 PM, No action needed
Internet Security messages	On
Network firewall messages	On
Virus protection messages	On
User Account Control Setting	On







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.]

- In the Firewall& Network the domine and private networks are off may cause unfiltered and unrestricted for all connections that do not abide by those rules
- From the UAC the notification was off if there is an application that wants to make a change it will do the change without your knowledge, and this is more dangerous.

- In windows services, I have noted there are a lot of services running, which will represent a potential security threat in that running services can allow unauthorized access to the computer or its contents.
- "Games and Streaming" software on business machines
- "Update Frequency" specified by the IT contract.
- Shared folders and files, he threat is that you don't always know who may be able to see or change their content. Ransomware is another threat that will often try to lock file shares on a network until the ransom is paid. It's good to know what files and folders are shared on both a PC and across a network

- Windows Services, A potential security threat is that running services can allow unauthorized access to the computer or its contents.

- Windows and Application Updates, Malicious software is a continual threat to unpatched systems and applications. Other threats include unauthorized access to the system or data or the disclosure of sensitive data.

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?*
    - ISO/IEC 27001

    Standard ISO/IEC 27001, will help the Joe organization to achieve secure and highly confidential information asset management, as well as to protect them, By identifying risks and setting appropriate controls to manage or dispose of them, obtaining the confidence of stakeholders and customers that their data is protected. Compliance with controls gives the company customer confidence that it is the best supplier.
    - ISO/IEC 27002

    Standard ISO/IEC 27002, will help the Joe organization to provide best-practice guidance on how to develop and implement an ISMS to be used as a basis for developing a security program that meets the needs of a Joe organization and applying the controls listed in Annex A of ISO 2700.

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

    - *Follow the Least-Privilege principle*
    - *No Client Data on Personal Devices*
    - *Mandatory Anti-Virus Software*
    - *Only Work-Related Software*

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?

    - Secure Configuration of Enterprise Assets and Software

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:

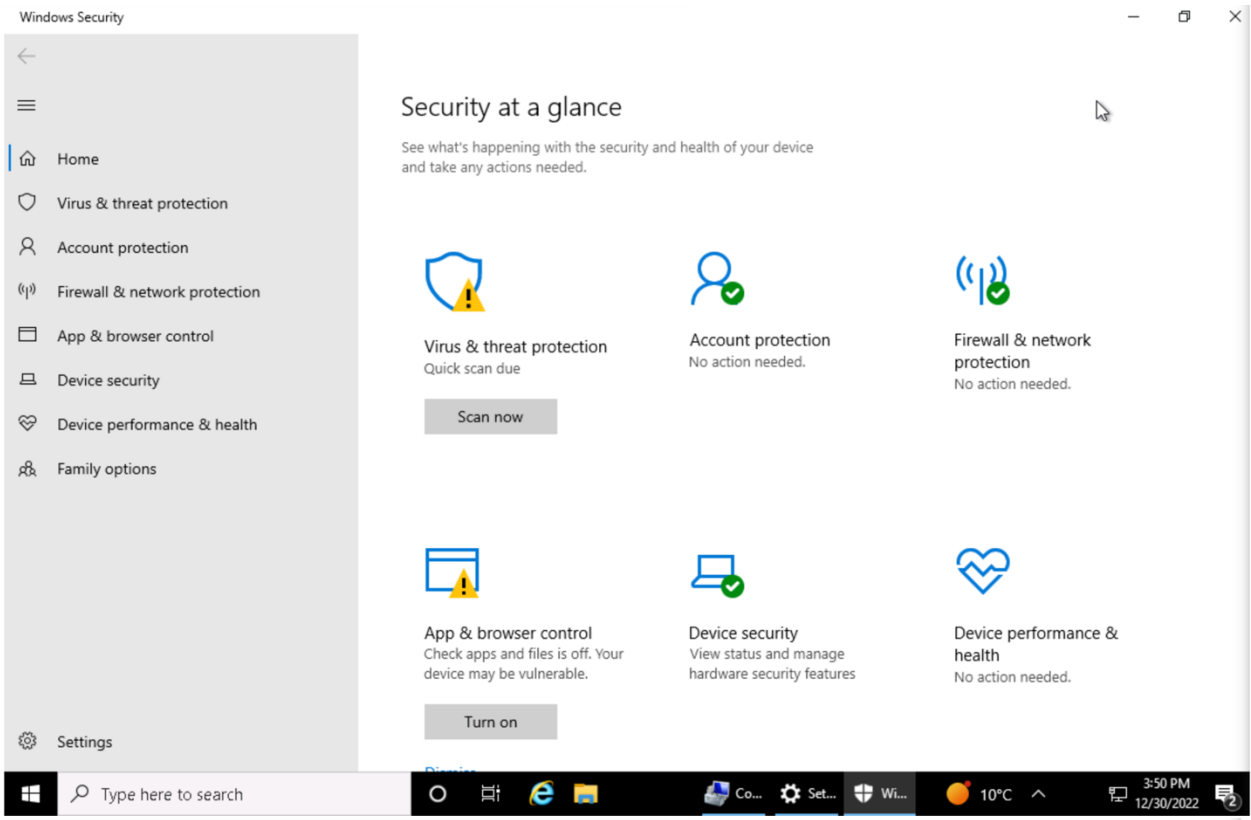
- Firewall
- Virus & Threat Protection
- App & Browser Control
- User Account Control settings
- Securing Removable Media

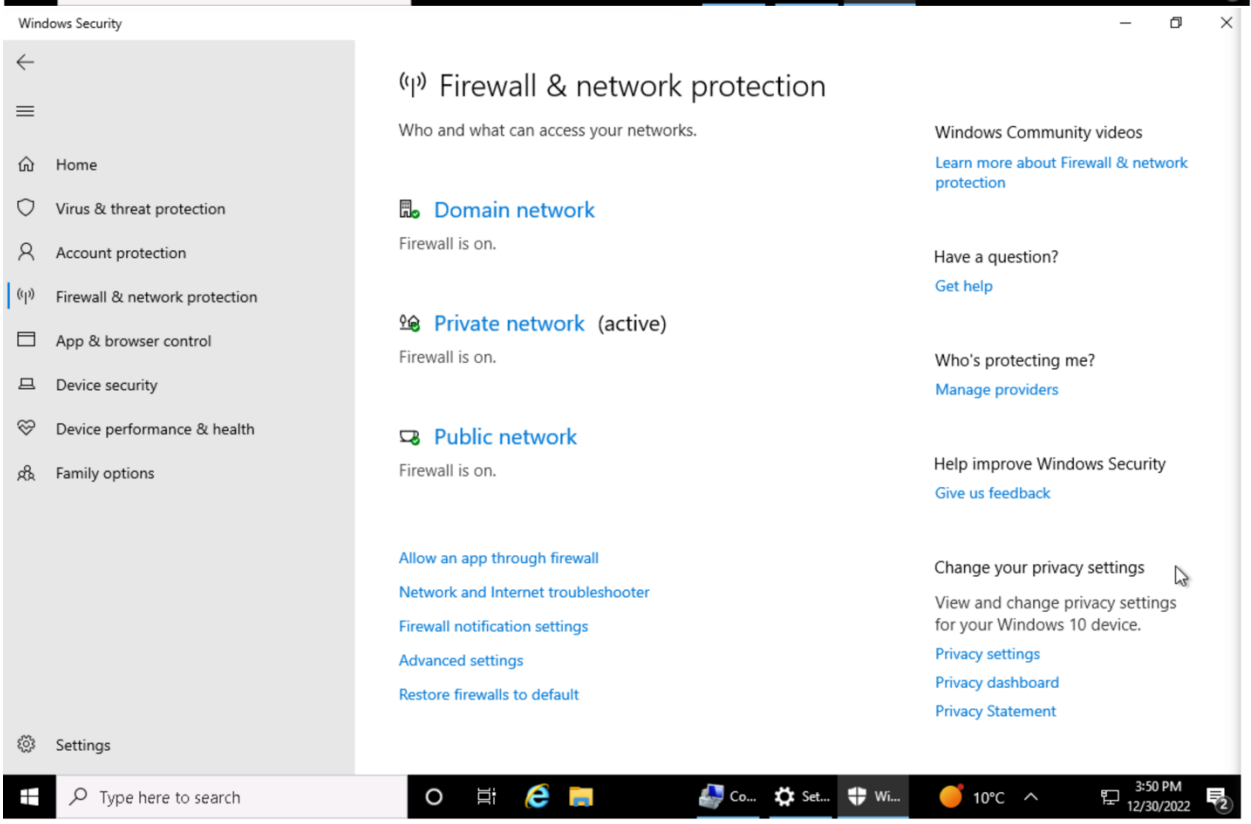
Firewall

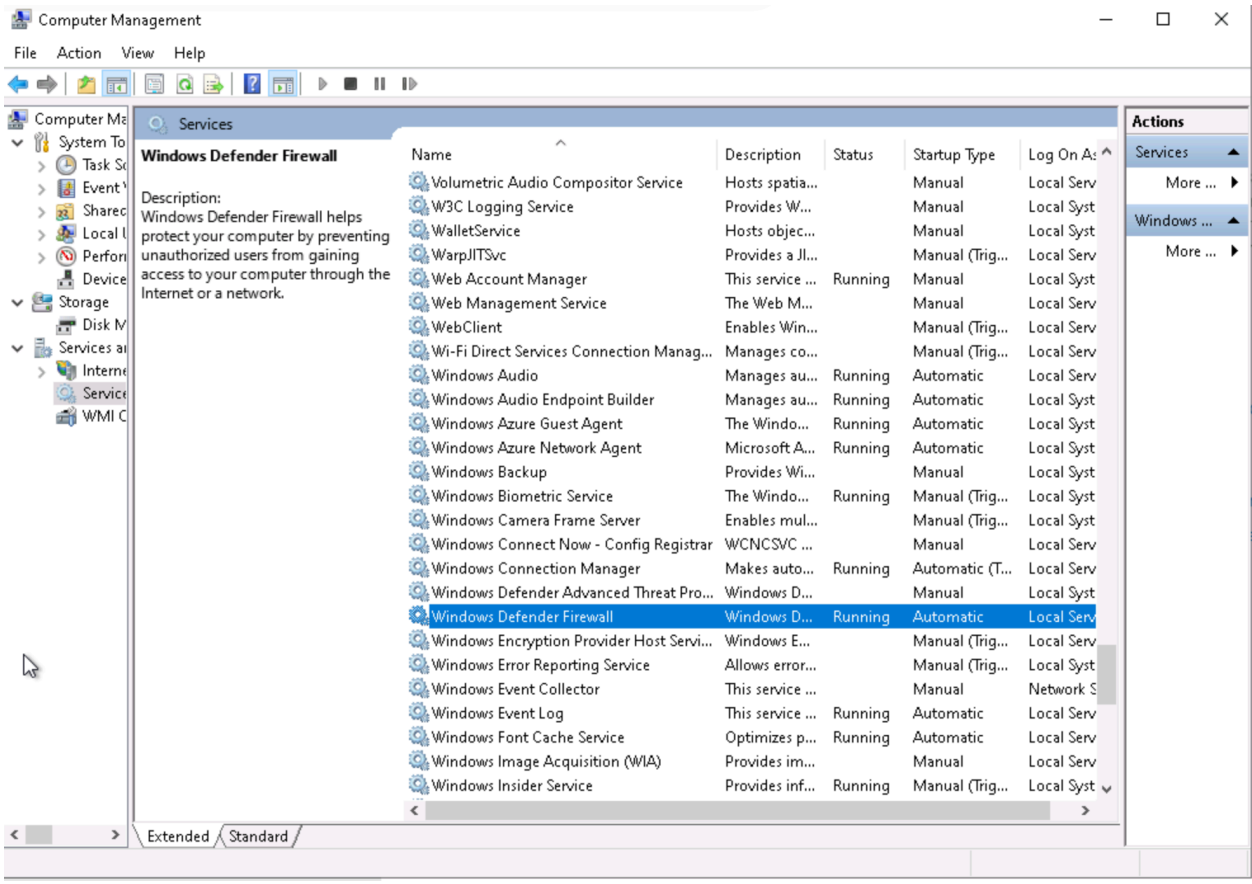
You need to ensure the Windows Firewall is enabled for all network access.

1. *Explain the process you take to do this.*
   By go to the setting >> update& security >> firewall& network protection
    - *Turn on:*
        - *Private network*
        - *Domain network*

      And to ensure it is running go to computer management >> services >> Windows defender is *running*
2. *Include screenshots showing the firewall is turned on.*


Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Security at a glance
See what's happening with the security and health of your device and take any actions needed.
Virus & threat protection
Quick scan due
Scan now
Account protection
No action needed.
Firewall & network protection
No action needed.
App & browser control
Check apps and files is off. Your device may be vulnerable.
Turn on
Device security
View status and manage hardware security features
Device performance & health
No action needed.
Type here to search
10°C
3:50 PM
12/30/2022


Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Firewall & network protection
Who and what can access your networks.
Domain network
Firewall is on.
Private network (active)
Firewall is on.
Public network
Firewall is on.
Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default
Windows Community videos
Learn more about Firewall & network protection
Have a question?
Get help
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
Type here to search
10°C
3:50 PM
12/30/2022



3. *What protection does this provide?*

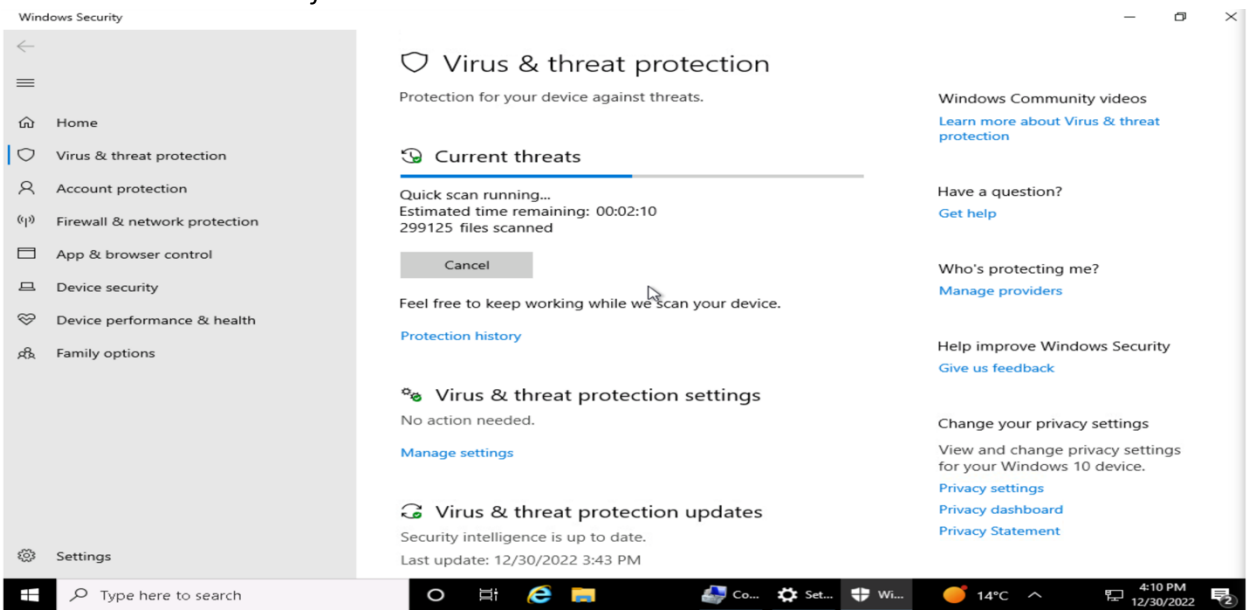
- *A firewall is needed because the internet is full of hackers and malicious traffic that wants access to your private network to cause harm. A firewall's main job is to prevent hackers and malicious traffic from entering your private network, protecting your private network from viruses and malware, so the firewall is especially important in a Joe organization with many computers. Joe doesn't want all his computers and servers to be vulnerable to hackers and accessible to everyone on the internet.*

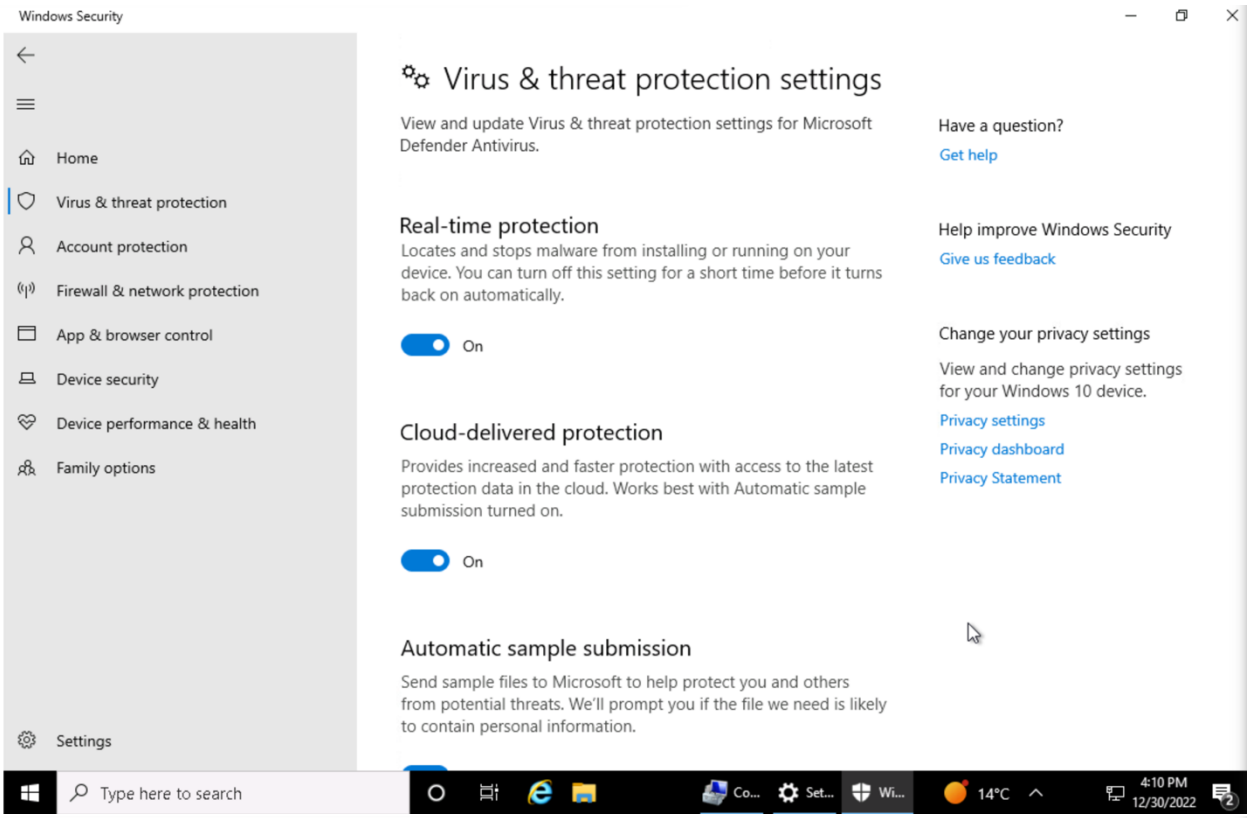
Virus & Threat Protection

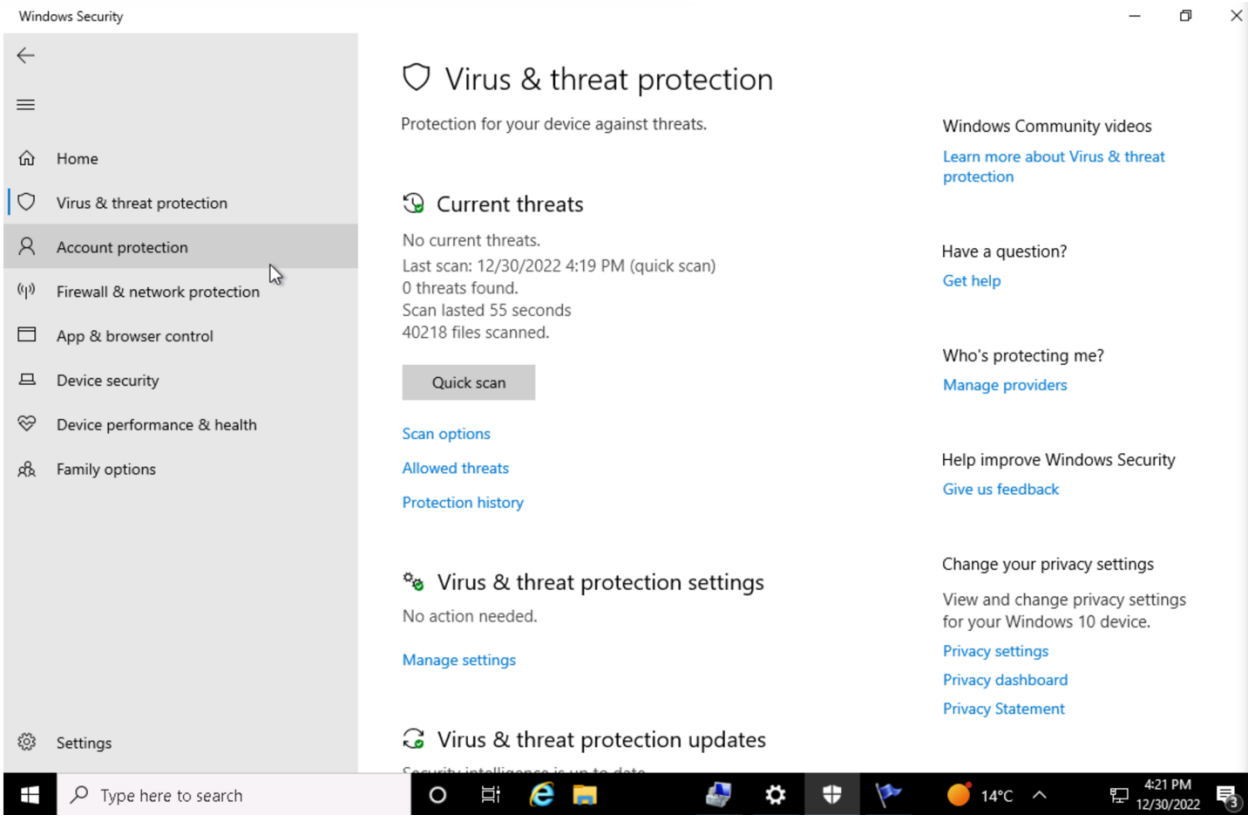
You need to ensure the Windows Defender anti-virus is enabled to always protect against current threats. It should be set to automatically update and continually scan the PC for malicious software. Note: Ignore any alerts about setting up OneDrive.

1. *Explain the process you take to do this.*
   By go to the setting >> update& security >> virus& threat protection

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



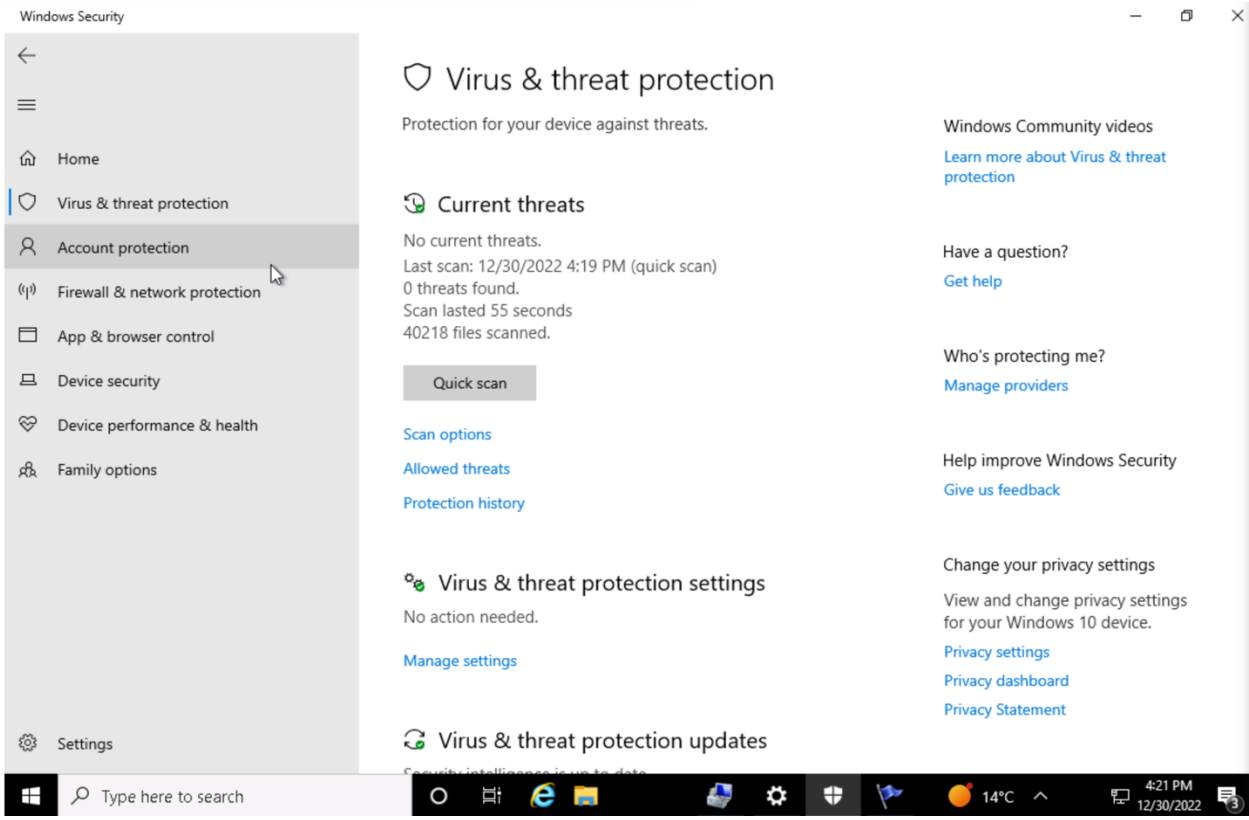

Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Virus & threat protection settings
View and update Virus & threat protection settings for Microsoft Defender Antivirus.
Real-time protection
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.
On
Cloud-delivered protection
Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.
On
Automatic sample submission
Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
Type here to search
14°C
4:10 PM
12/30/2022

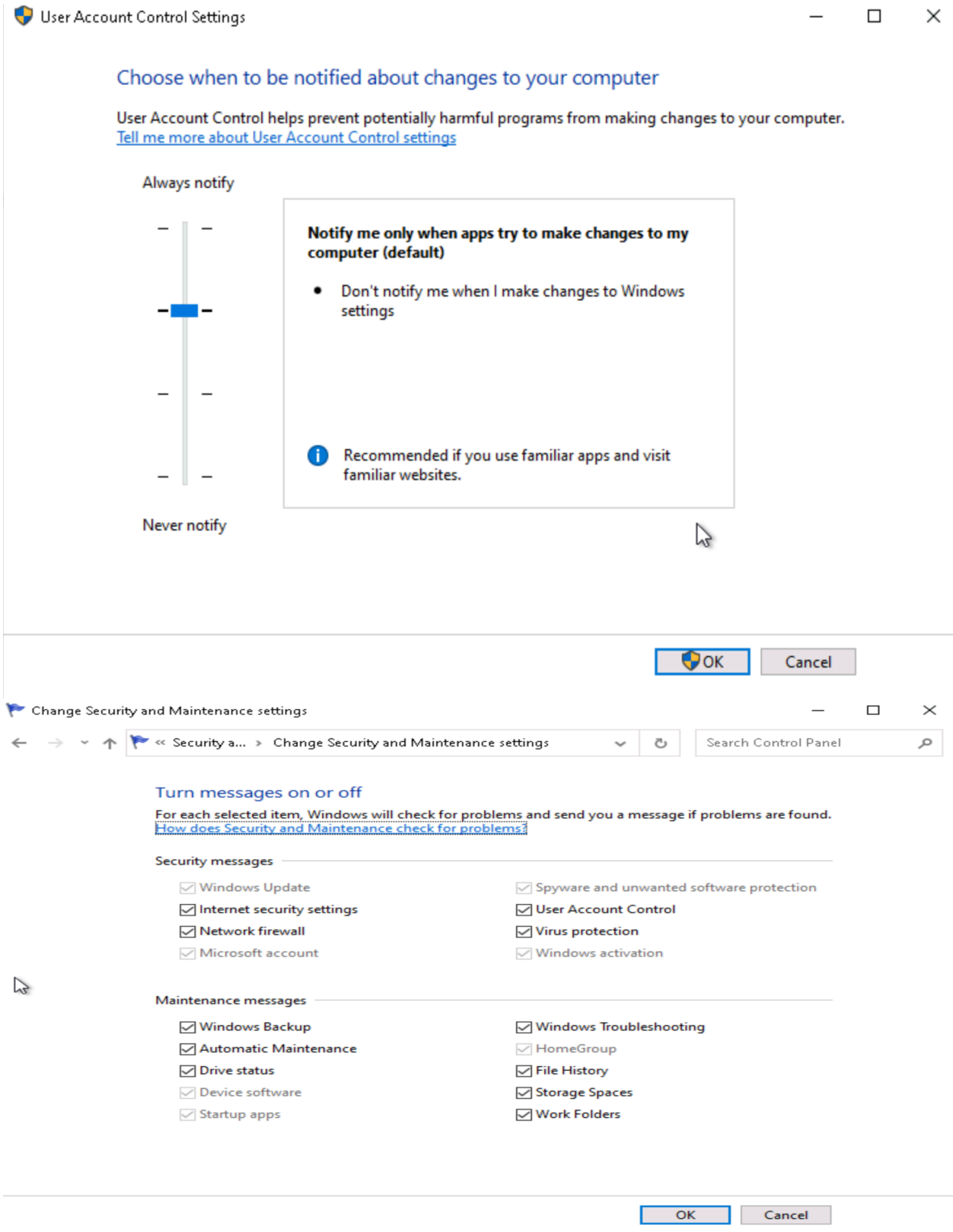

Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Virus & threat protection
Protection for your device against threats.
Current threats
No current threats.
Last scan: 12/30/2022 4:19 PM (quick scan)
0 threats found.
Scan lasted 55 seconds
40218 files scanned.
Quick scan
Scan options
Allowed threats
Protection history
Virus & threat protection settings
No action needed.
Manage settings
Virus & threat protection updates
Windows Community videos
Learn more about Virus & threat protection
Have a question?
Get help
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
Type here to search
14°C
4:21 PM
12/30/2022

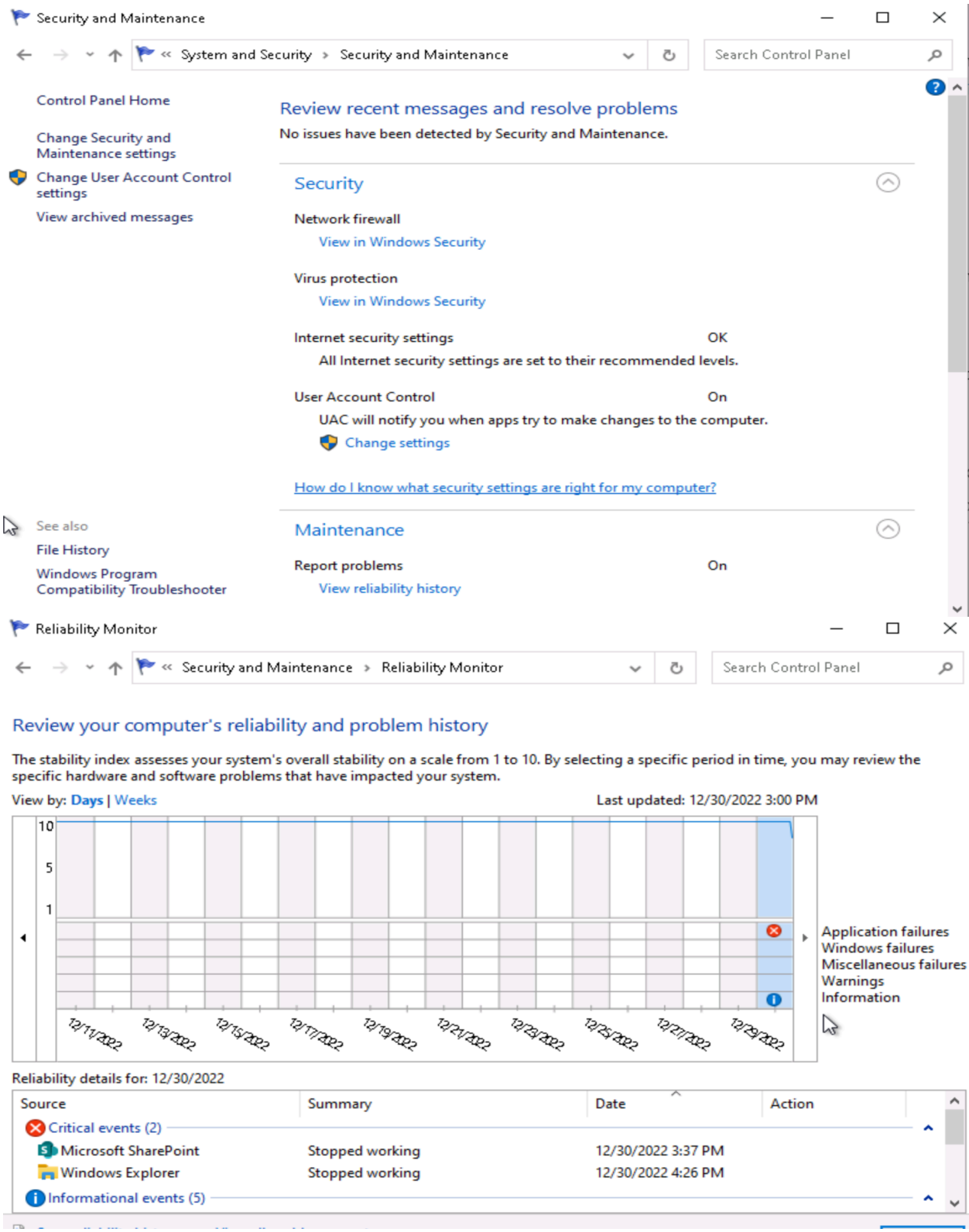
Once you determine that virus & threat protection is on and updated, you need to turn on messages about the Network firewall and Virus protection. Refer to the instructions above for viewing the settings within Security and Maintenance, Review recent messages and resolve problems.

1. *Turn on the Network firewall and Virus protection messages using Change Security and Maintenance Settings.*
   - ***Control Panel > System and Security > Security and Maintenance**>> **Security>>** Network firewall >> View in windows **Security (ensure it is tourn on)***
   - ***Control Panel > System and Security > Security and Maintenance**>> **Security>>** Virus protection >> View in windows **Security (ensure it is tourn on)***
   - ***Control Panel > System and Security > Security and Maintenance**>> **change Security and Maintenance settings (ensure** Network firewall, Virus protection is on)*
   - ***Control Panel > System and Security > Security and Maintenance**>> **view achieved massage***
   - ***++ Control Panel > System and Security > Security and Maintenance**>> **change UAC (ensure it is default notified)***

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




User Account Control Settings
Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Notify me only when apps try to make changes to my computer (default)
Don't notify me when I make changes to Windows settings
Recommended if you use familiar apps and visit familiar websites.
Never notify
OK
Cancel
Change Security and Maintenance settings
Security a... > Change Security and Maintenance settings
Search Control Panel
Turn messages on or off
For each selected item, Windows will check for problems and send you a message if problems are found.
How does Security and Maintenance check for problems?
Security messages
Windows Update
Internet security settings
Network firewall
Microsoft account
Spyware and unwanted software protection
User Account Control
Virus protection
Windows activation
Maintenance messages
Windows Backup
Automatic Maintenance
Drive status
Device software
Startup apps
Windows Troubleshooting
HomeGroup
File History
Storage Spaces
Work Folders
OK
Cancel



3. *Provide at least two risks mitigated by enabling these security settings:*
   - *Mitigate the risk of Block spyware*
   - *Mitigate the risk of Direct virus attacks*

- *Mitigate the risk of Maintain privacy*

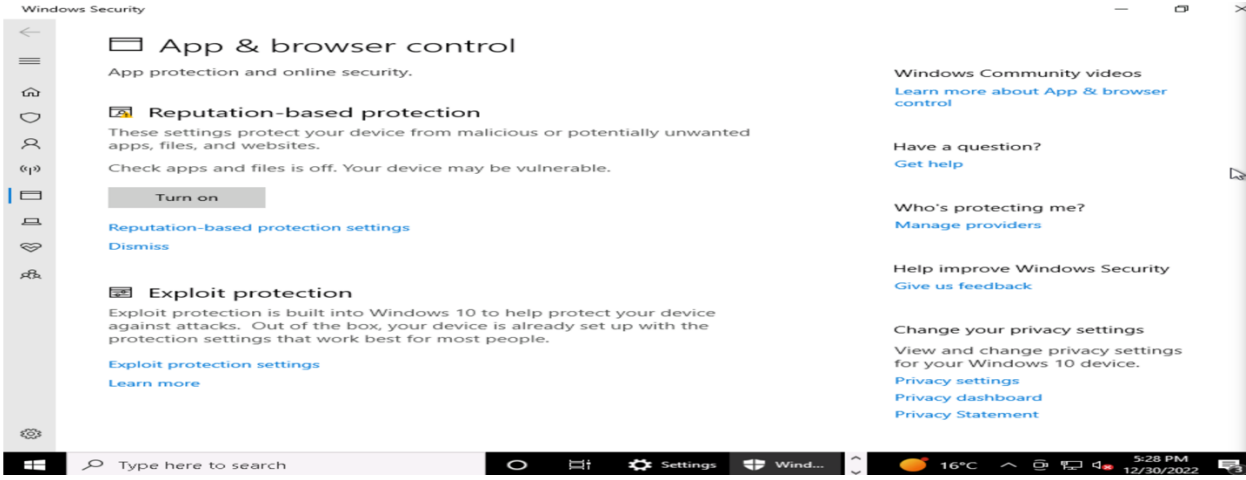
4. *From the CIS baseline controls, provide the controls satisfied by completing this.*

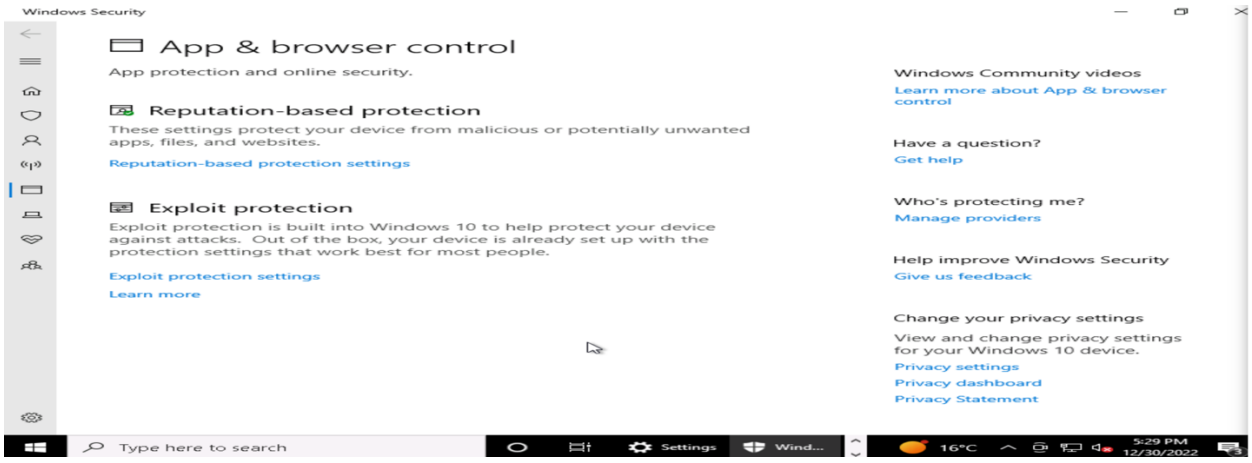
- Malware Defenses
- Network Infrastructure Management
- Network Monitoring and Defense
- Inventory and Control of Software Assets
- Data Protection

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.

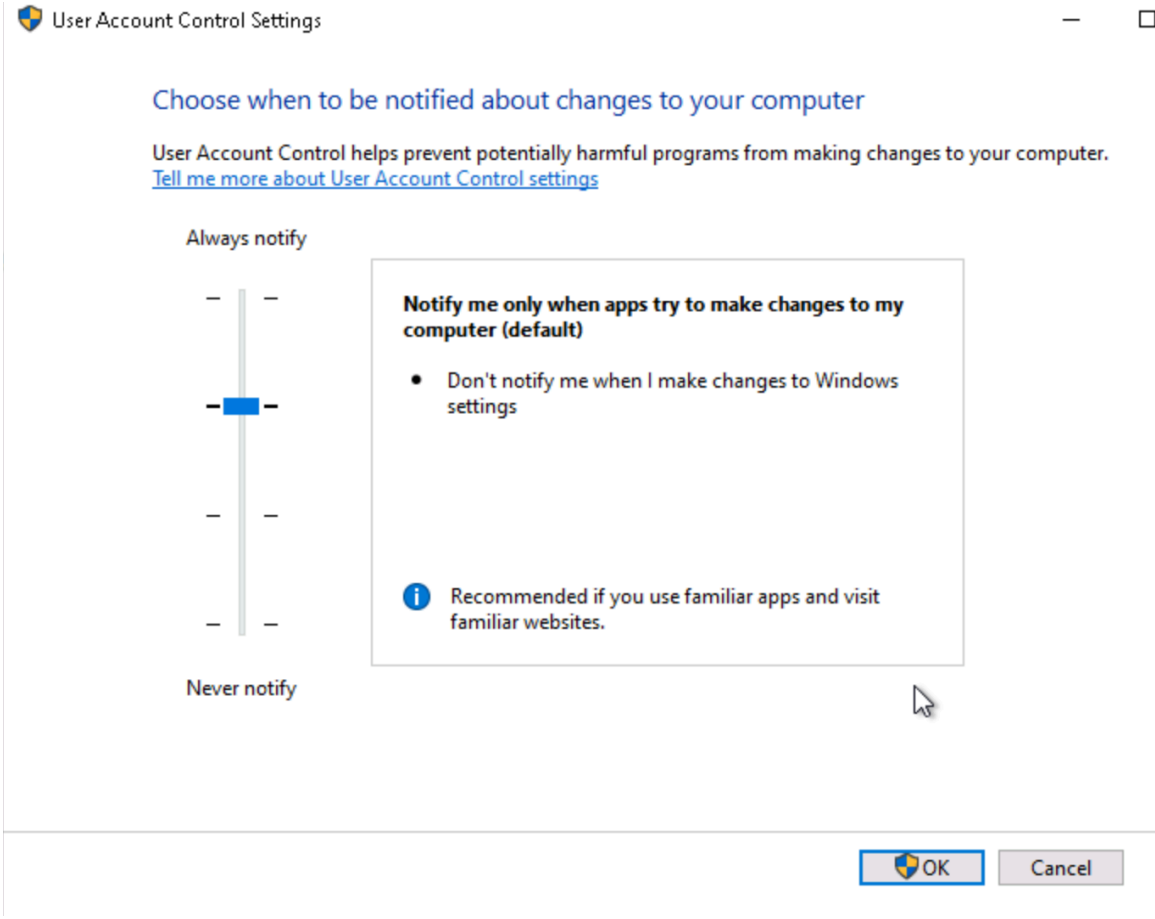
1. *What is the current UAC setting on Joe's computer?*

   This is available from the above security settings.

   - Will it was neve notify, I replace it to the default

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

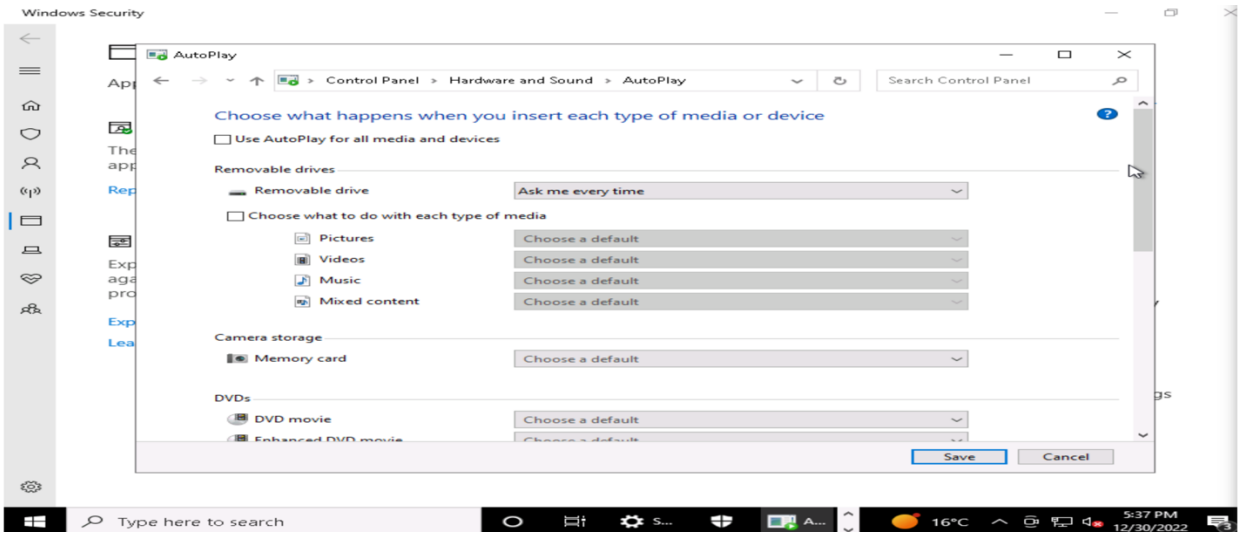
   - *should the* default



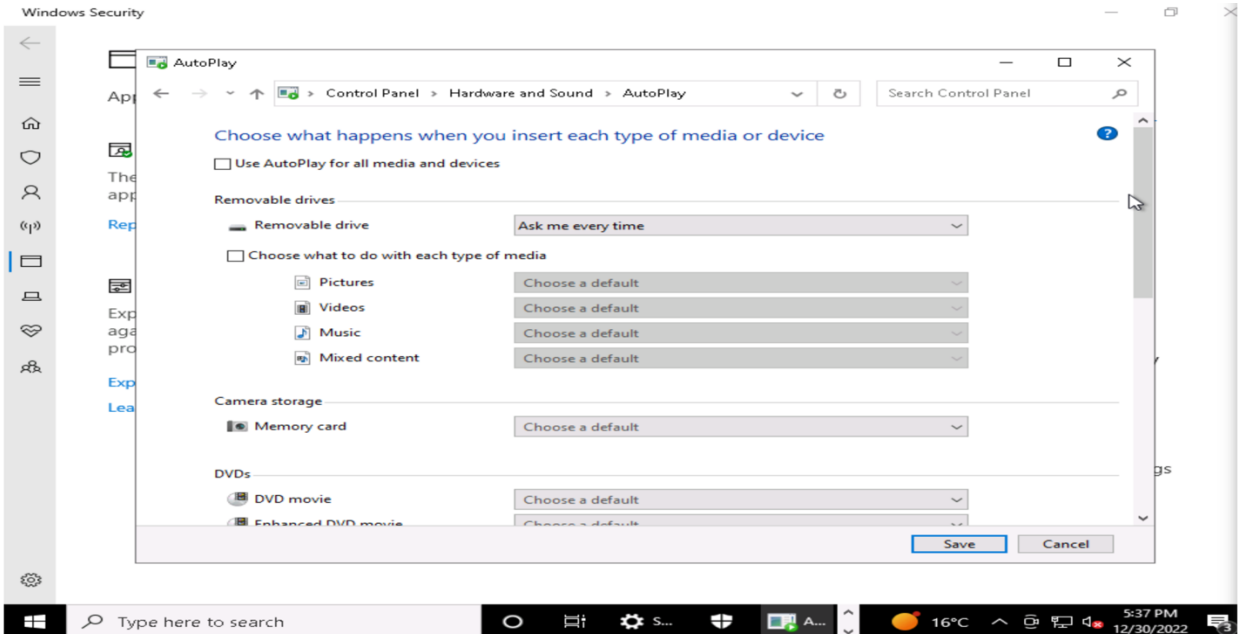
Securing Removable Media

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.*



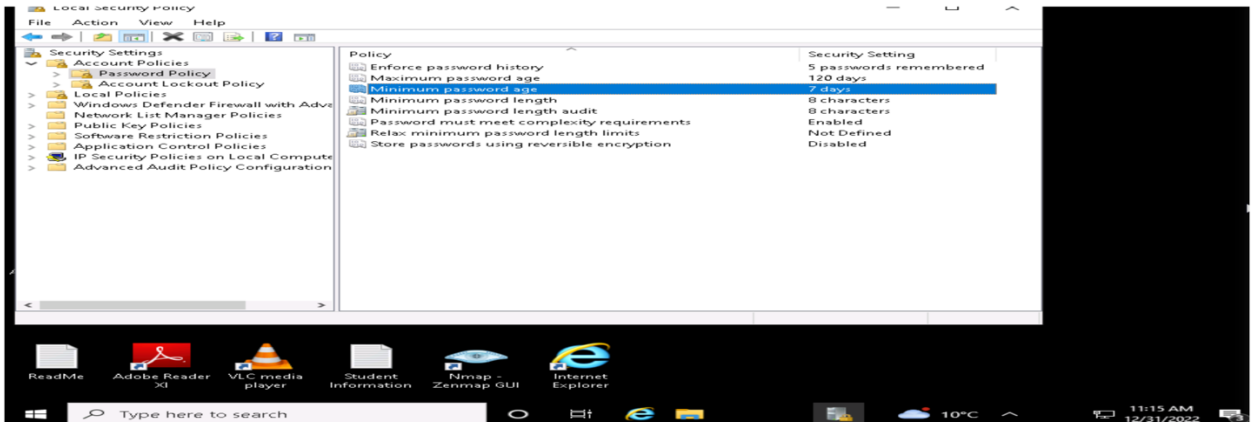
3. Securing Access

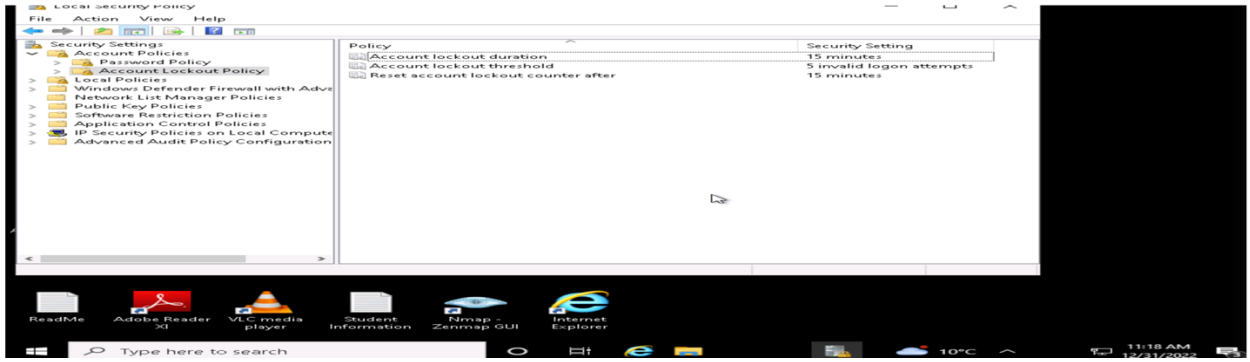
Ensuring only specific people have access on a computer system is a common step in information security. It starts by understanding who should have access and the rules or policies that need to be followed.

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

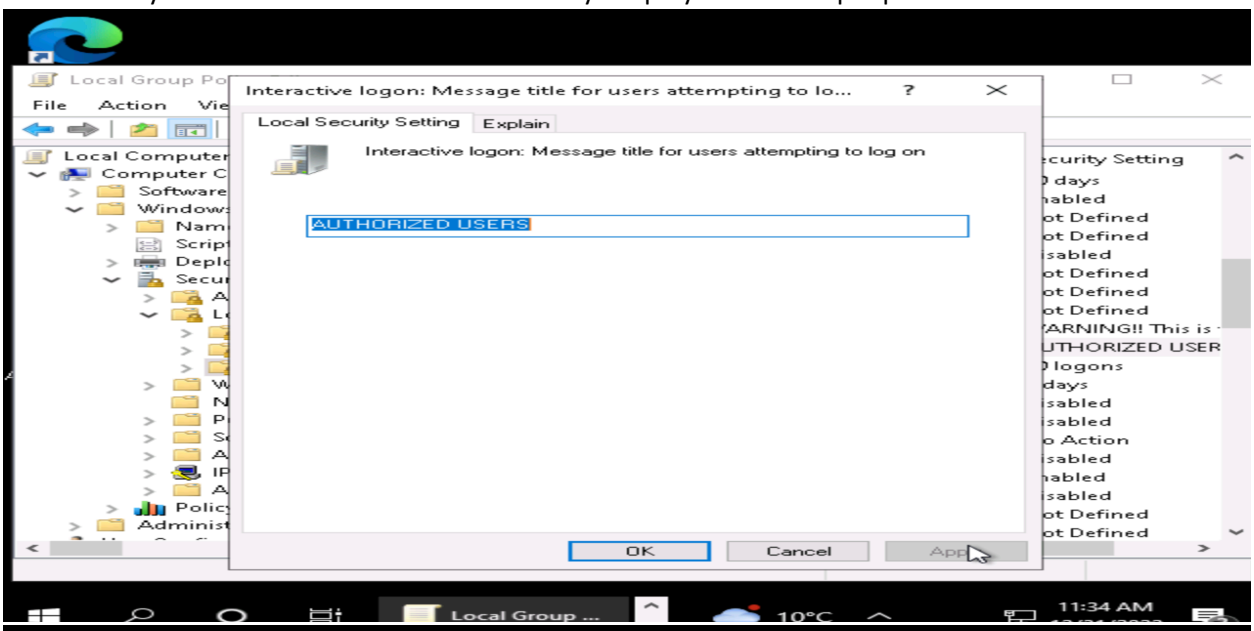
- JoesAuto
- Jane Smith (Joe's assistant)
- A User - Used for exercises (Not used in this project)
- Notadmin - Built-in administrator account (Not used for this project)
- Windows built-in accounts: Guest, DefaultAccount, and WDAGUtility (Not used for this project)

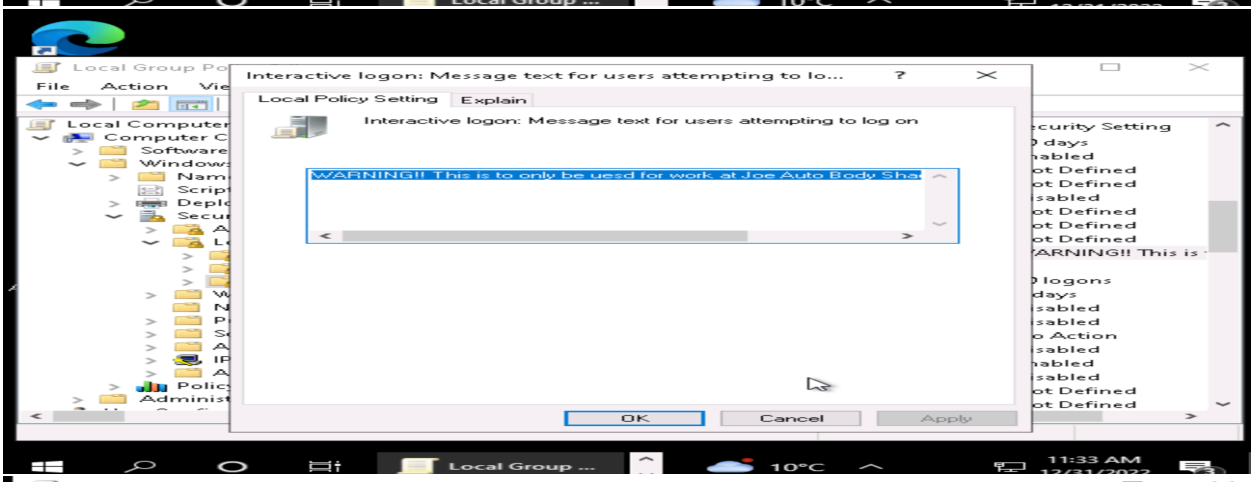
Joe's Auto Access Rules:

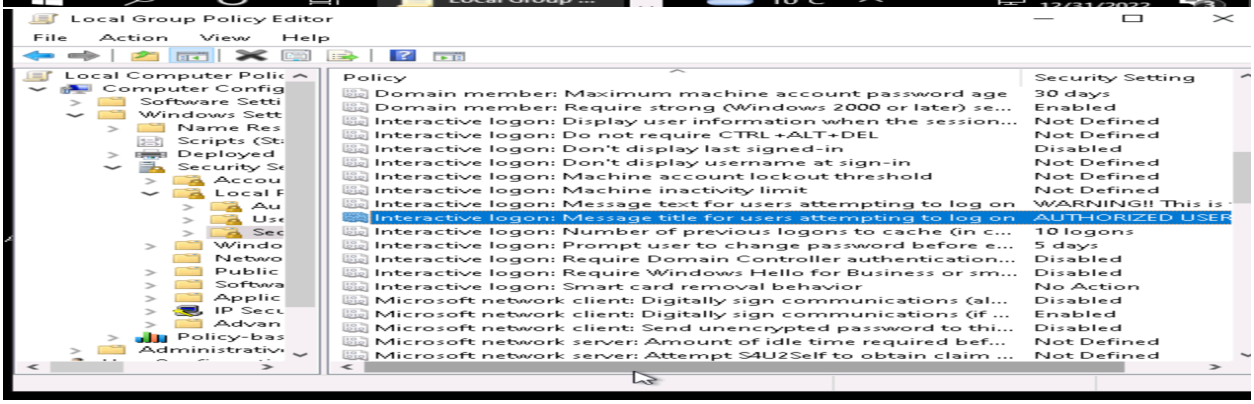
- Only JoesAuto and A User should have administrative privileges on this PC.
- Joe wants to prevent potentially harmful programs from making changes and wants to be notified whenever apps try to make changes to his computer.
- All valid users should have a password following Joe's password policy below
    - At least 8 characters
    - Complexity enabled
    - Changed every 120 days
    - Cannot be the same as the previous 5 passwords
    - 

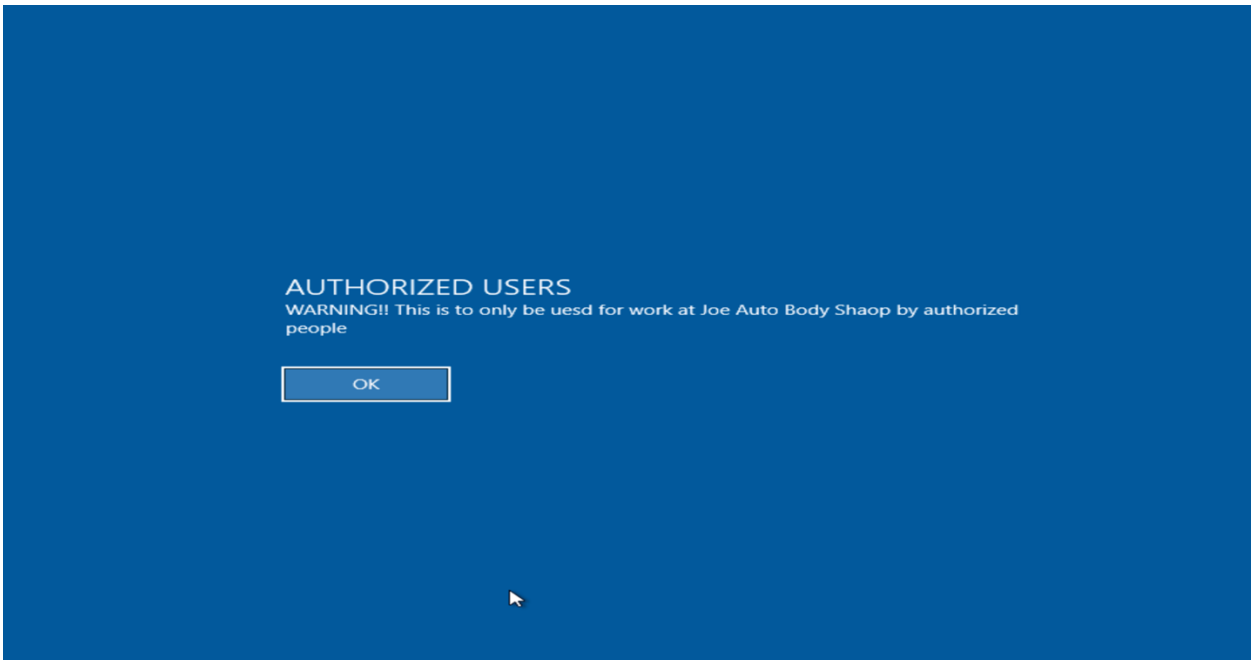
- Account should be automatically disabled after 5 unsuccessful login attempts. The account should be locked for 15 minutes and then should automatically unlock.
- 

- 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.

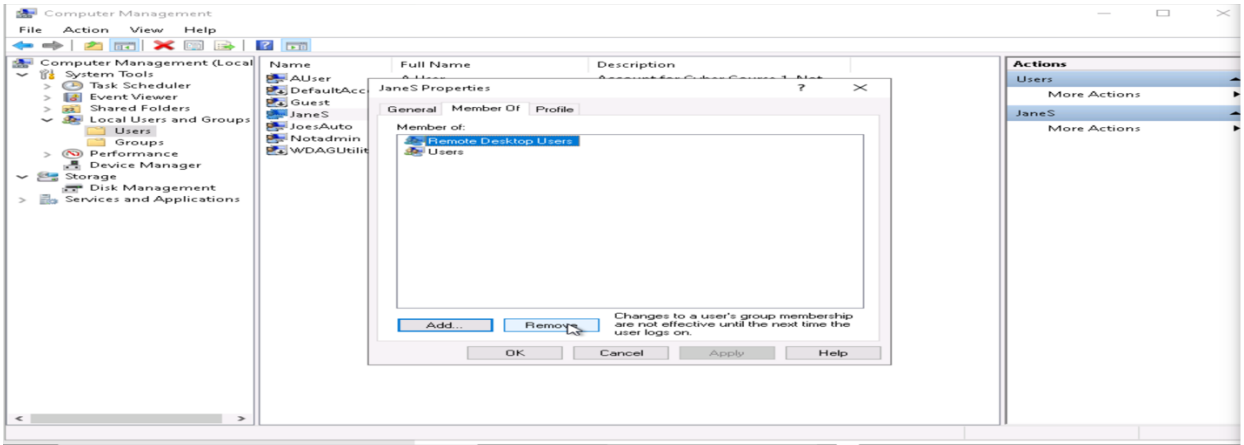








- There is to be no remote access to this computer.
    - It is can be done by go to setting >> Update& security >> For devolves >> remote desktop
    - Or be go to specific user and remove him from member of remote desktop users



User Accounts

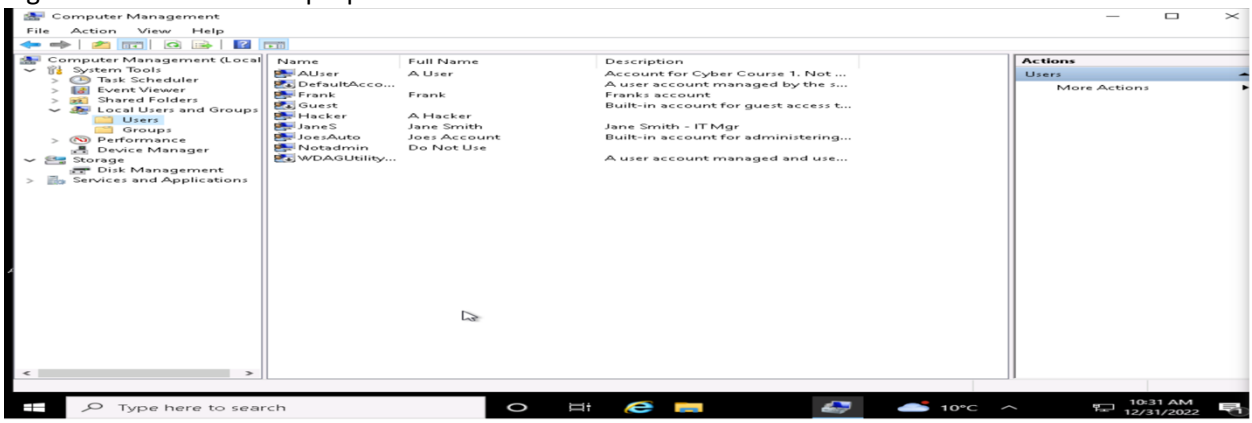
1. *What user accounts should not be there?*
    - *Frank account*
    - *Hacker account*
2. *Bonus questions: What is Hacker's password?*
3. *Explain the steps you take to disable or remove unwanted accounts.*
    - Right click on account>> *remove*
4. *Why is it important to disable or remove unneeded accounts from a PC or application? Include potential vulnerabilities and risks.*

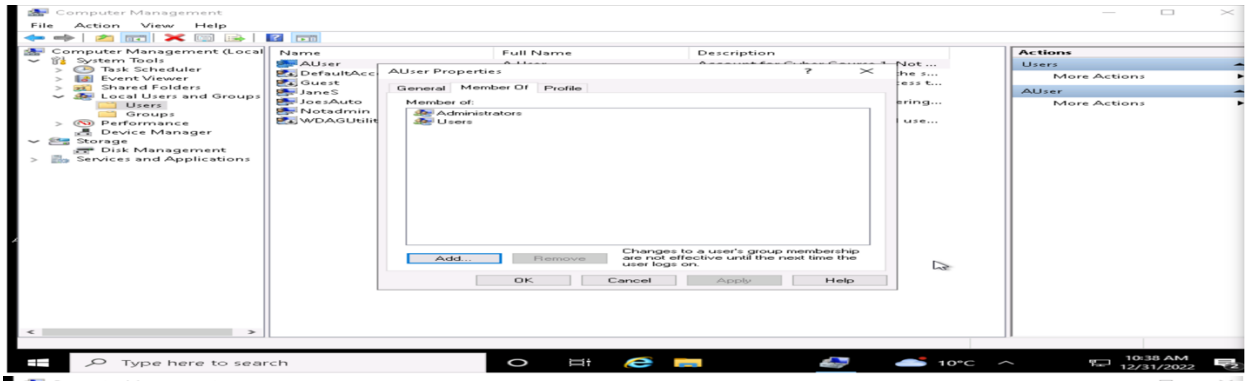
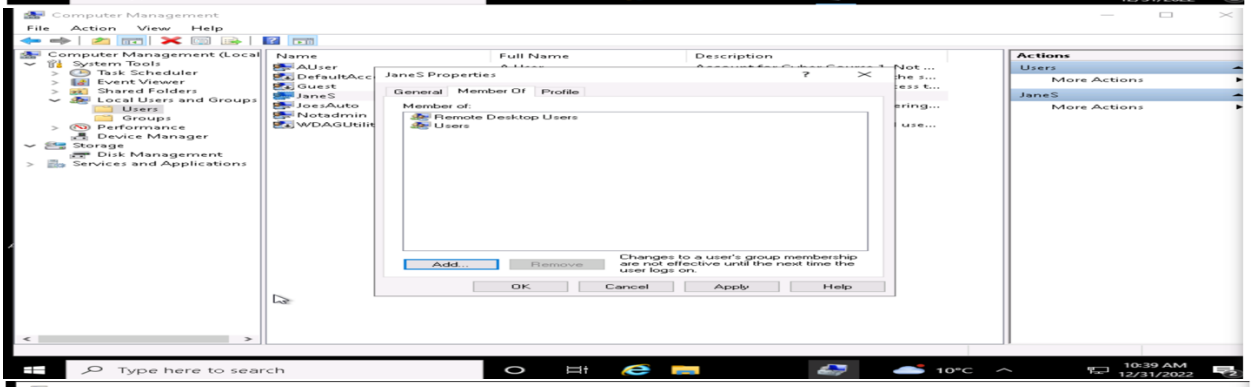
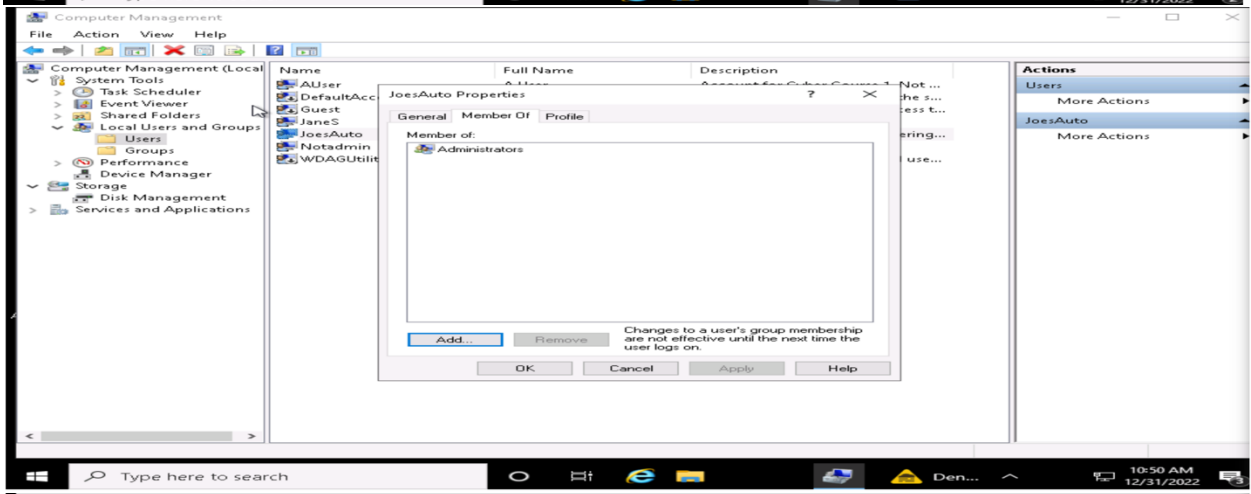
    - *In general, it is always best to reduce your attack surface, Stale user accounts in Active Directory are a significant security risk since they could be used by an attacker or a former employee. These inactive accounts also consume reclaimable database space.*
    - *CIS Control 5: Account Management,CIS Control 6: Access Control Management, CIS Control 8: Audit Log Management.*

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?
    - Will the only accounts that should have administrator user is JoesAuto and A User
    - I was find the Jane Smith account have administrator, which shouldn't have a administrator
6. Explain how you determined this. Provide screenshots as needed.

    - Right click on account >> properties>> Member of



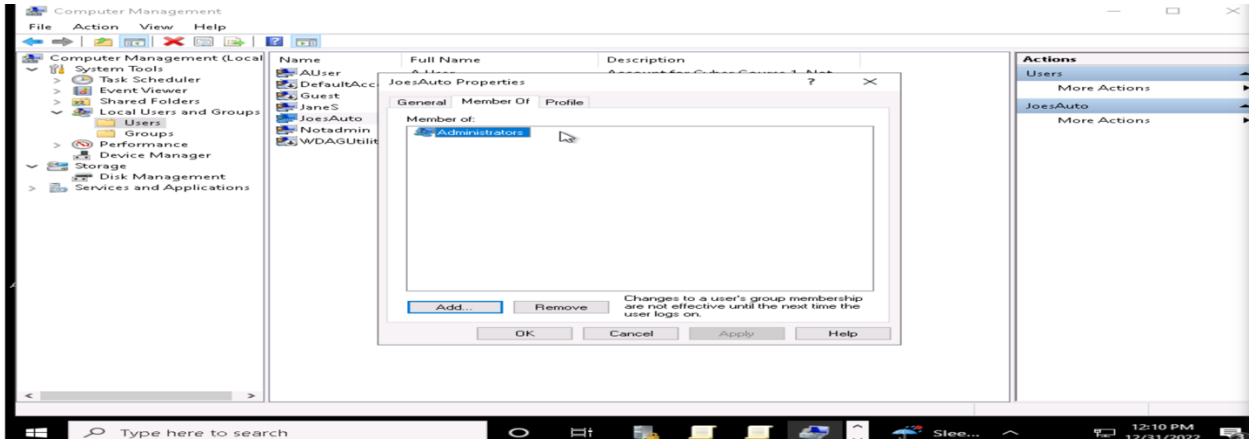
- 
Computer Management
File Action View Help
AUser Properties
General Member Of Profile
Member of:
Administrators
Users
Add... Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK Cancel Apply Help
Type here to search
10:38 AM
12/31/2022

Computer Management
File Action View Help
JaneS Properties
General Member Of Profile
Member of:
Remote Desktop Users
Users
Add... Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK Cancel Apply Help
Type here to search
10:39 AM
12/31/2022

Computer Management
File Action View Help
JoesAuto Properties
General Member Of Profile
Member of:
Administrators
Add... Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK Cancel Apply Help
Type here to search
10:50 AM
12/31/2022

Computer Management
Type here to search
10:50 AM
12/31/2022

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.
   - Administrator accounts on a computer allow the user to install software, make any change to the system settings, and override local folder permissions:
   - Unauthorized software can be installed on the computer, leading to non-work-related activities and possible computer slowdowns or shutdowns.
   - Unlicensed software can be installed, opening your business up to potentially hefty fines from software vendors.
   - Users can intentionally or unintentionally execute a malicious program, leading to infections that could potentially span many computers on your network. These are often undetectable by anti-virus programs (frequently because the user specifically allows them to execute).
   - If multiple users use a single PC, the administrator account can be used to access data in other user profiles. This could allow for data breaches, theft, and privacy concerns.

Now, you need to remove administrator privileges for any user(s) that should not have it.

8. *Explain the process for doing this. Include screenshots to show your work.*
   - *Computer management >> Local users>> Users >> Right click on account >> properties >> member of.*
   - 

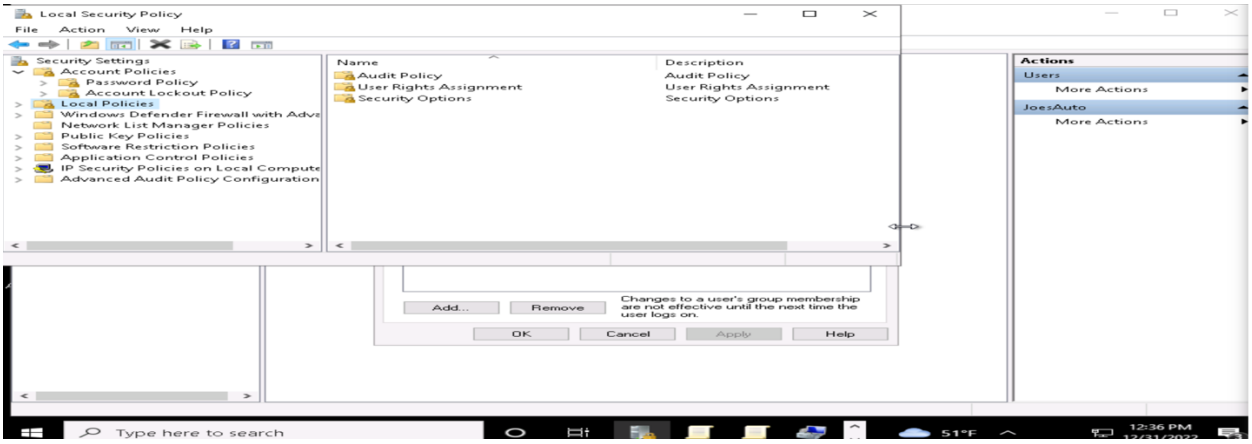
9. *What is the security principle behind this?*
   - *In general, it is always best to reduce your attack surface, because the administrator accounts on a computer allow the user to install software, make any change to the system settings, and override local folder permissions*
10. The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?

    - CIS Control 5: Account Management

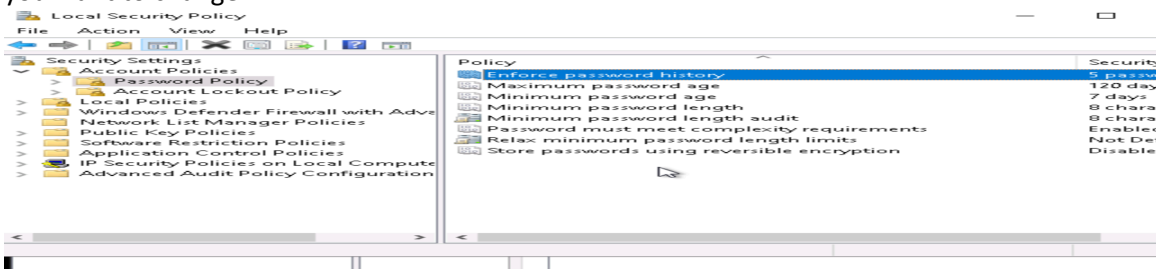
Setting Access and Authentication Policies

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.

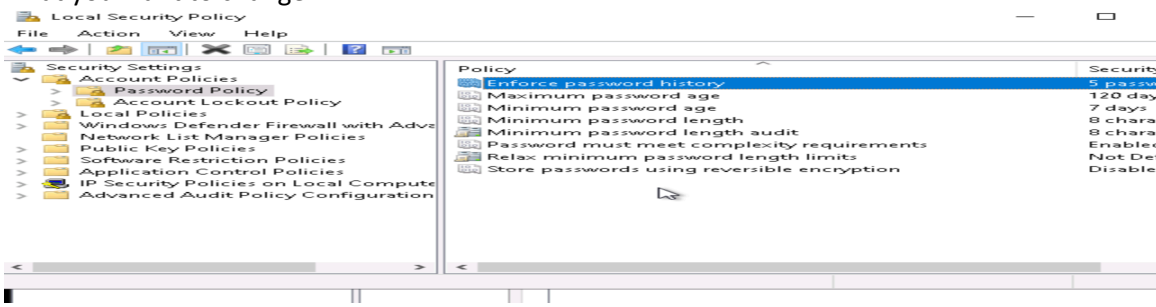
1. *Provide a screenshot of the Local Security Policy window here.*
   [Note: Local Security Policy is not available on Windows 10 Home edition.]



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.
   - Setting the Password Policy:
     - By go to *Local Security Policy>> Account Police>>* Password Policy >> find what you want to change



     -
   - Setting the Account Lockout Policy:
     - By go to *Local Security Policy>> Account Police>>* Account Lockout Policy >> find what you want to change

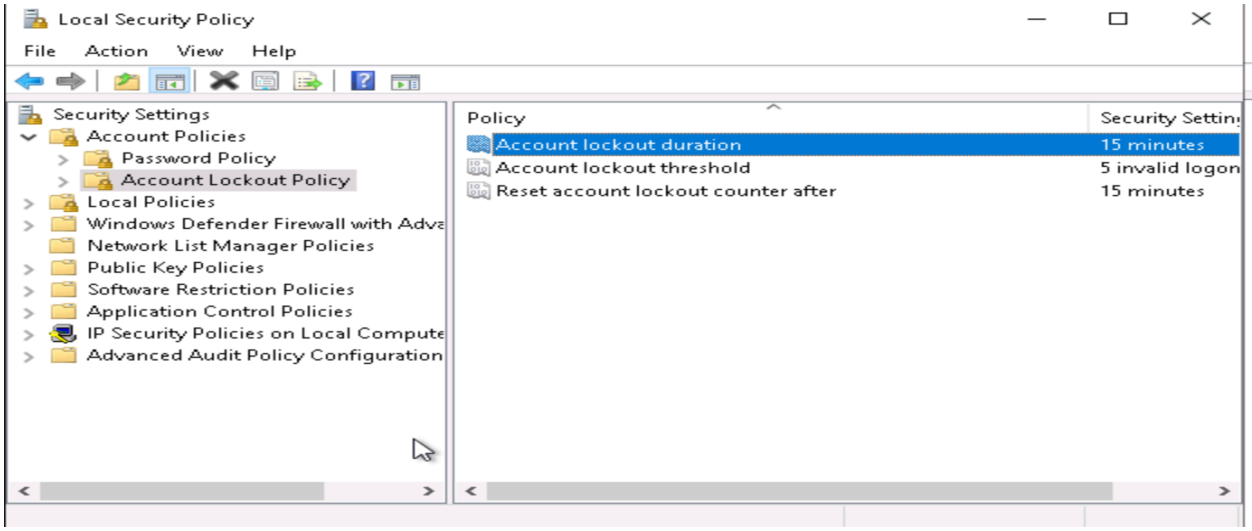


     -

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.

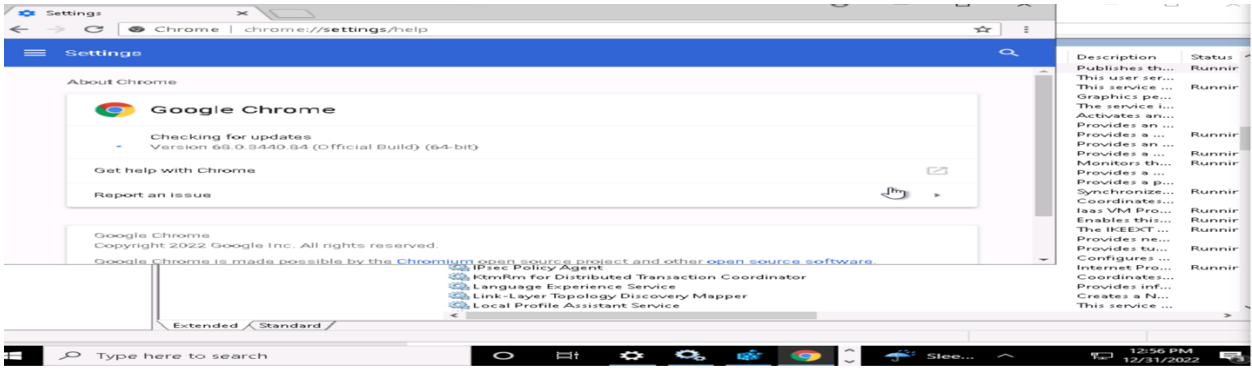
- 

4. Securing Applications

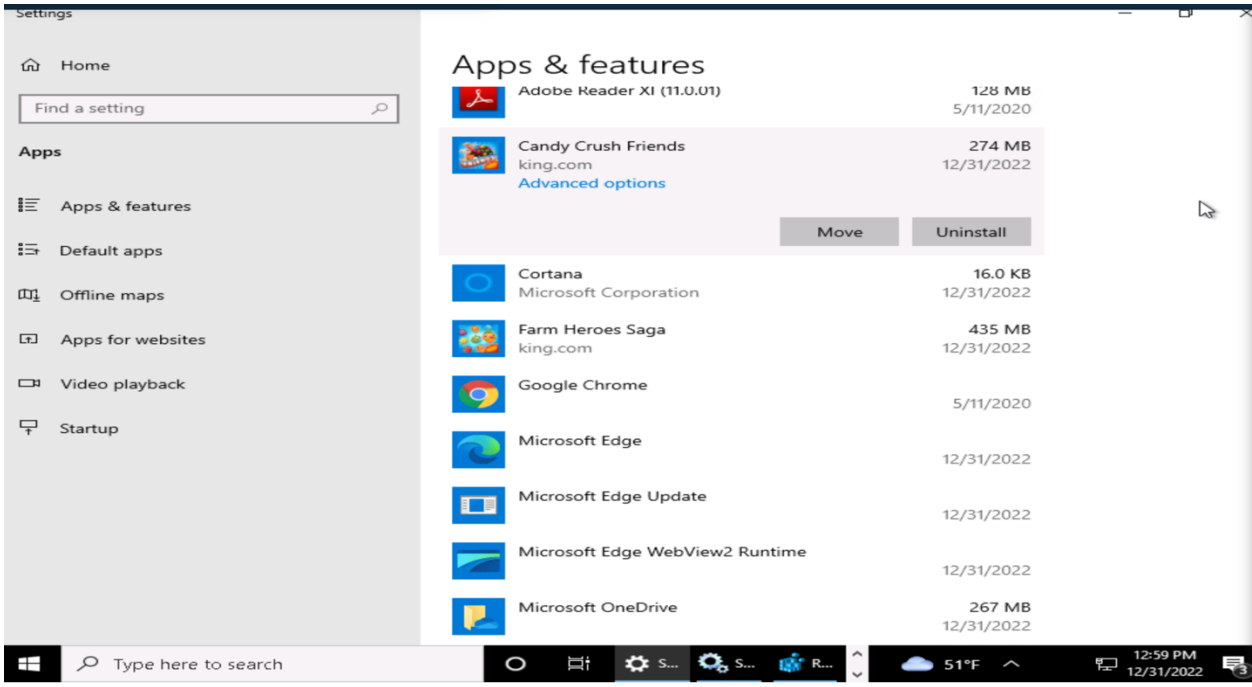
As part of the inventory process, you determined computer programs or applications on the PC. The next step is to decide which ones are needed for business and which ones should be removed. Unneeded programs could be vulnerable to attacks and allow unauthorized access into the computer. They also consume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

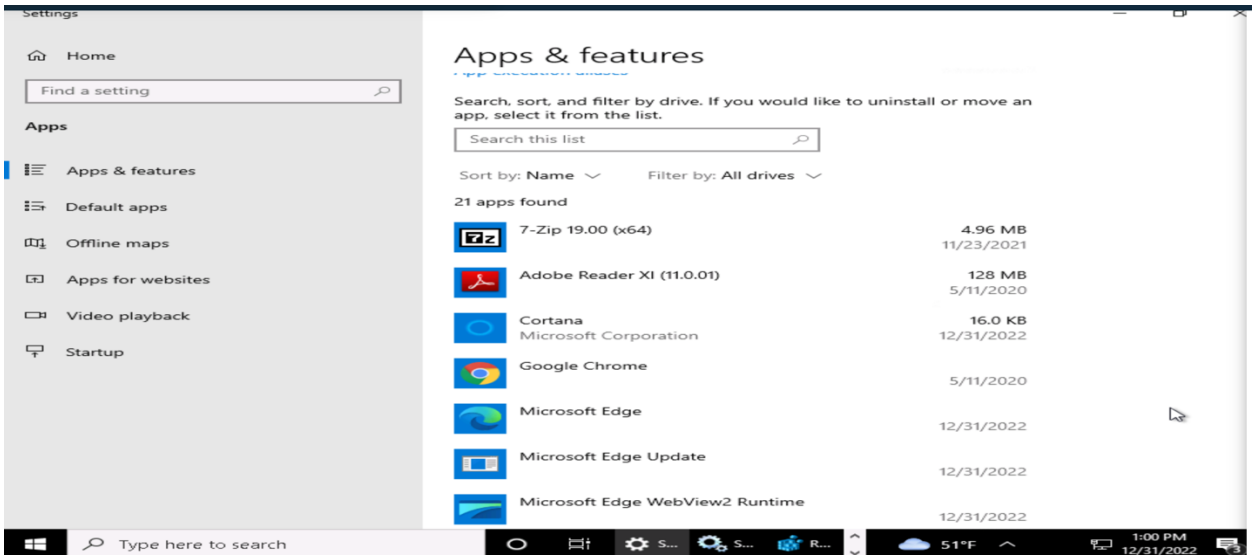
Joe has established the following rules regarding PC applications:

- Joe wants everyone to use the latest version of the Chrome browser by default.
    a. Open Chrome>> control Chrome >> Help >> about Chrome >> update
    b.



- There should be no games or non-work-related applications installed or downloaded.

a. 



- Joe is also concerned that there are “hacking” programs downloaded or installed on the PC that should be removed.

- 

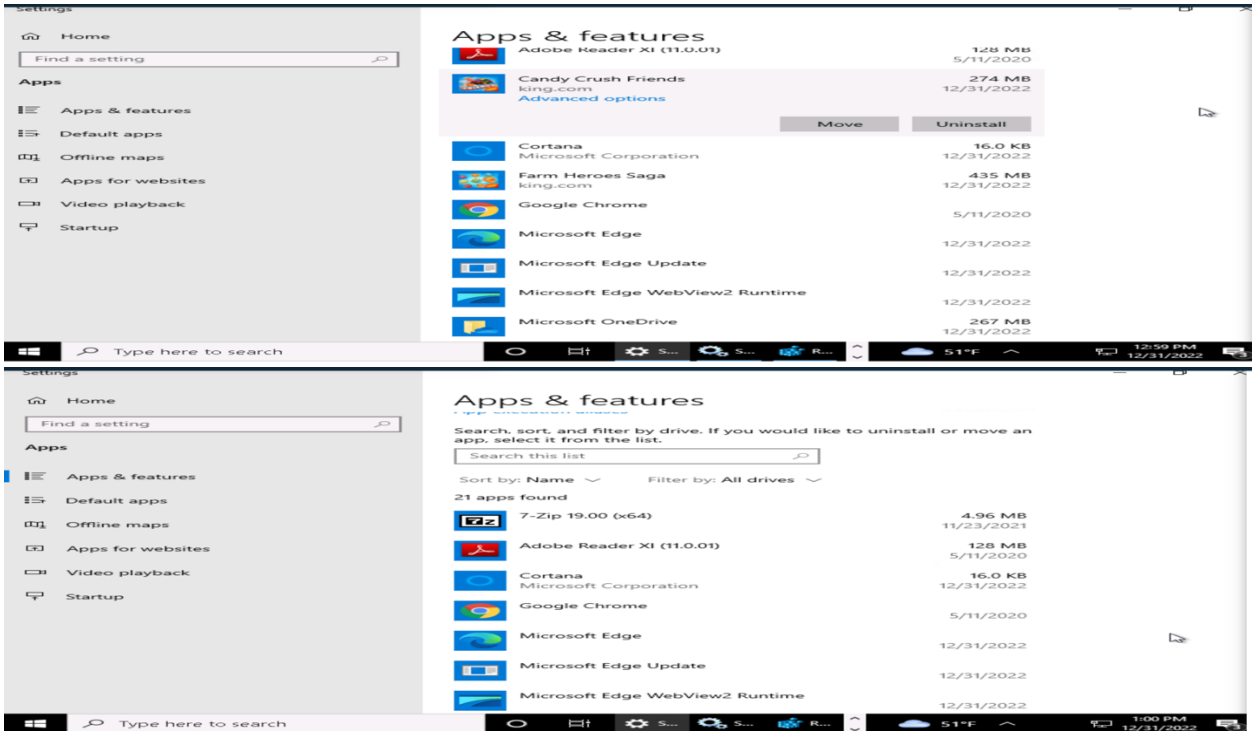
- This PC is used for standard office functions. The auto-body has a separate service they use for their website and to transfer files from their suppliers.

Remove unneeded or unwanted applications

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

- *Candy Crush Frindes*
- *Farm Heroes Sage*
- *Spotify Music*
- *Windows PC Health check*

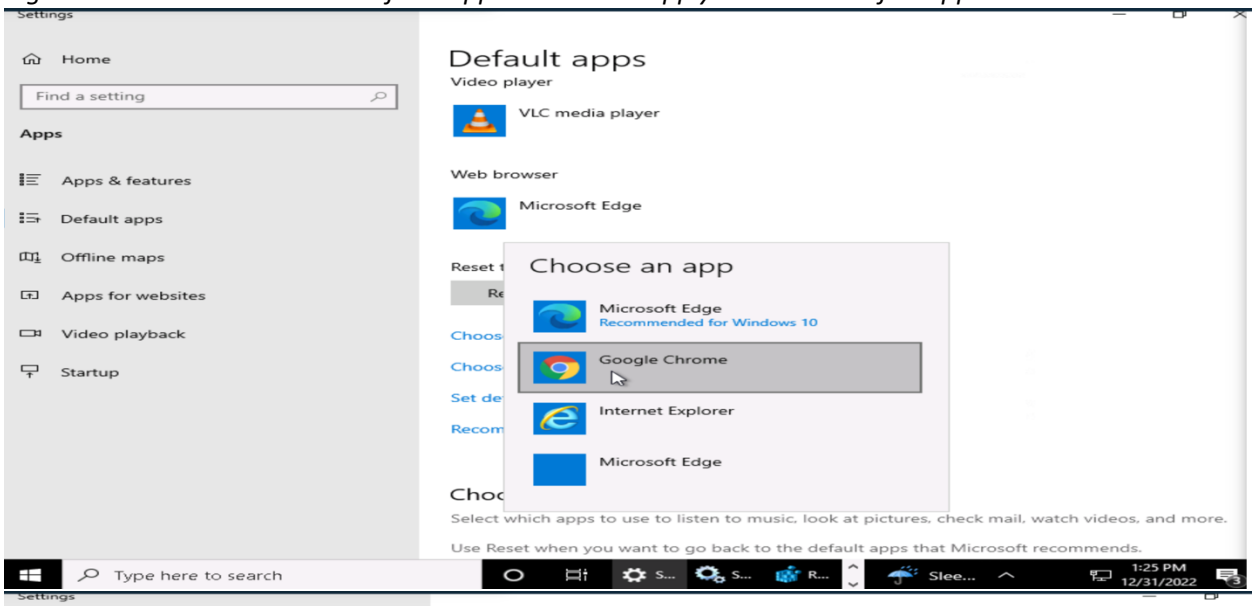
2. *Name at least three vulnerabilities, threats or risks with having unnecessary applications:*
    - *Increase in malware attacks*
    - *Njection Attacks*
    - *Broken Authentication*
    - *Missing Function Level Access Control*
3. *Joe wants you to make sure unneeded applications or programs are no longer on the PC. Explain the steps you take to disable or remove them. Include screenshots to show your work.*

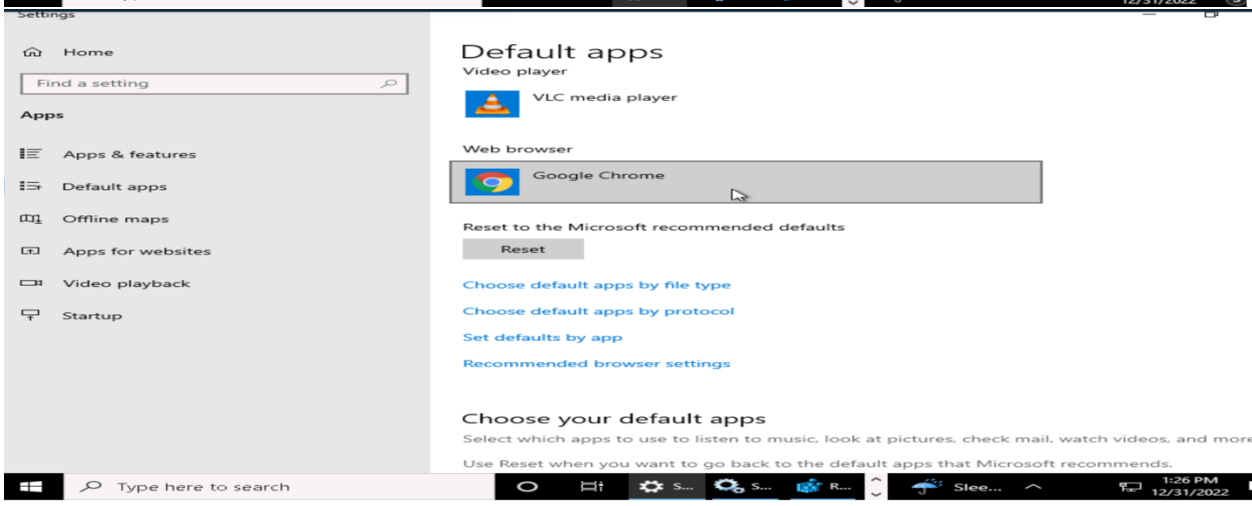
- *Right click on home button>> app& features >> install App*
- 

-

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.*
    - *Right click on home button>> default app>> make the app you want as defult app*
    - 

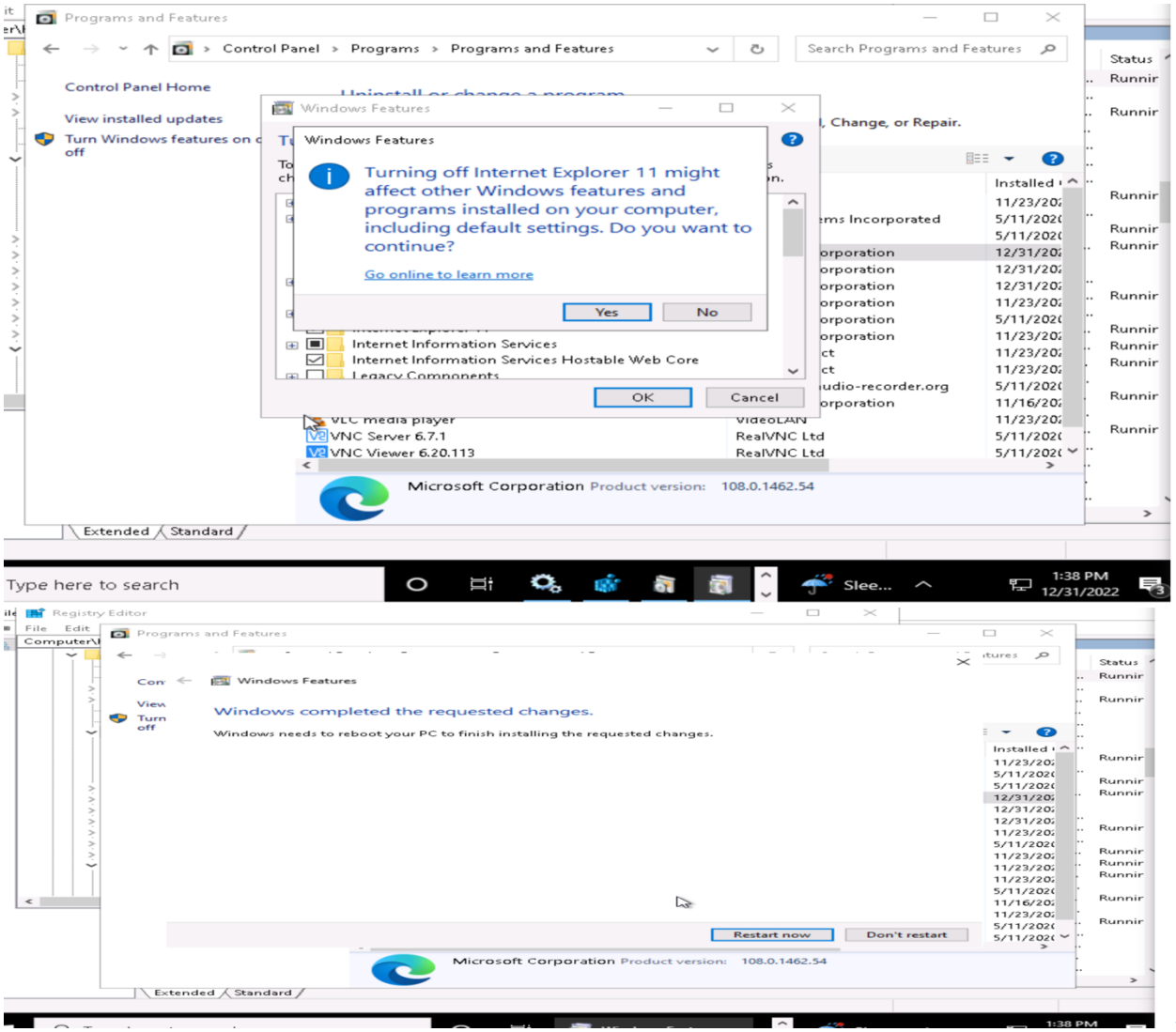
    - 

2. *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
    - Frequent Vulnerabilities
    - Lack of Support
    - A use-after-free vulnerability has been reported in Internet Explorer, which could allow a remote attacker to execute arbitrary code on a targeted system. Experts have advised users to opt for alternate browsers like Firefox and Google Chrome
    - Microsoft has found a security flaw in its popular web browser — Internet Explorer — which could allow hackers to gain control of a computer, and there have already been

targeted attacks to exploit the bug. This has prompted government security response teams from various countries, including India urging Windows users to consider Chrome or Firefox as their default browser until Microsoft fixes the flaw.

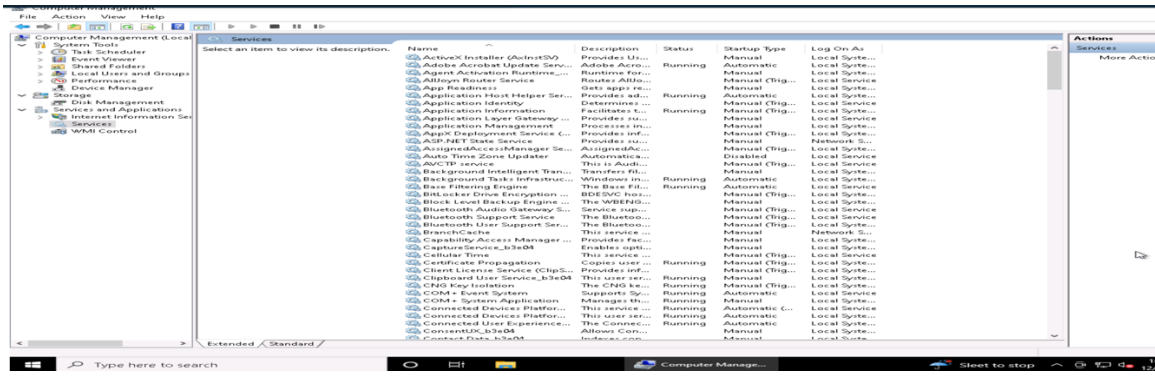
Because of the reasons you give above, Internet Explorer should be removed. To do that, go to the **Control Panel**, select **Programs**. On the **Programs and Features** window, select "**Turn Windows features on or off**."

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

- 

Windows Services

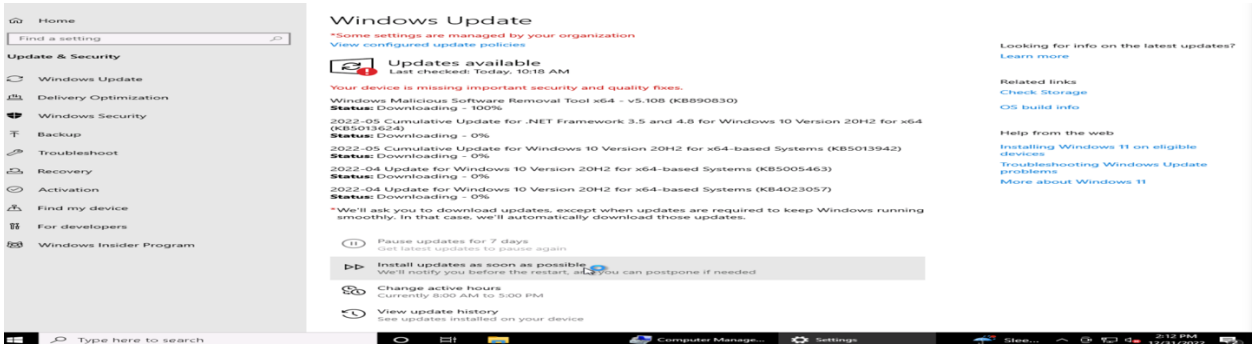
There are Windows features running on Joe's computer that could allow unwanted activity or files. He suspects that someone may have used the PC as a web server in the past. Joe wants you to confirm if web services are turned on, stop it if it is and make sure it is not running whenever the computer restarts.

- How did you determine these services were running? Include screenshots to show how you found them.
    i. Right click on widows home >> Computer Management >> services
    ii. 
- Advanced users should provide at least two methods for determining a web server is running on a host
- How do you disable them and make sure they are not restarted?
    i. Right click on widows home >> Computer Management >> services>> click on the service and press stop.

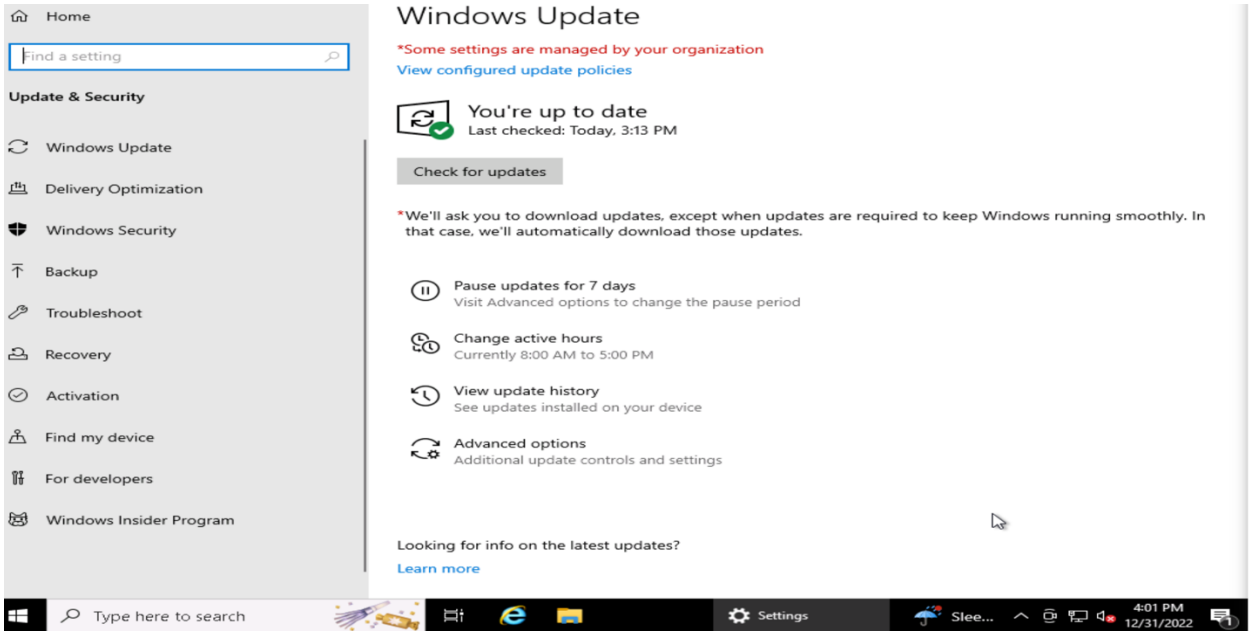
- Advanced Users: The File Transfer Protocol FTP service is also running on this PC and shouldn't. Explain the process for disabling it and ensuring it is not automatically restarted.

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.*
    - *Go to setting >> update& security>>* Windows *update(https://msrc.microsoft.com/update-guide)*
    - 

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.*

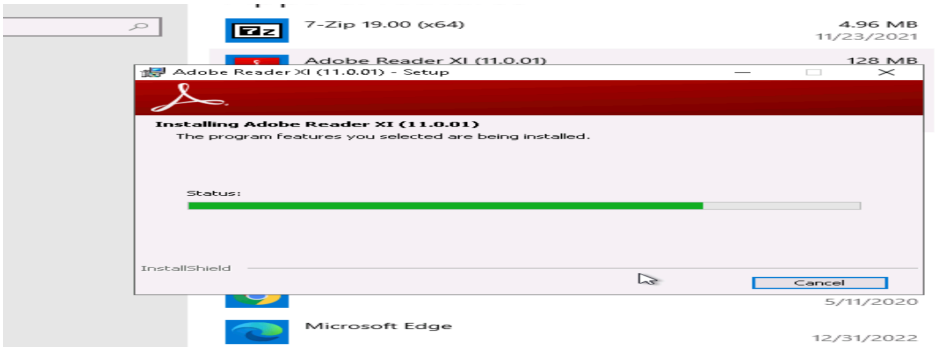


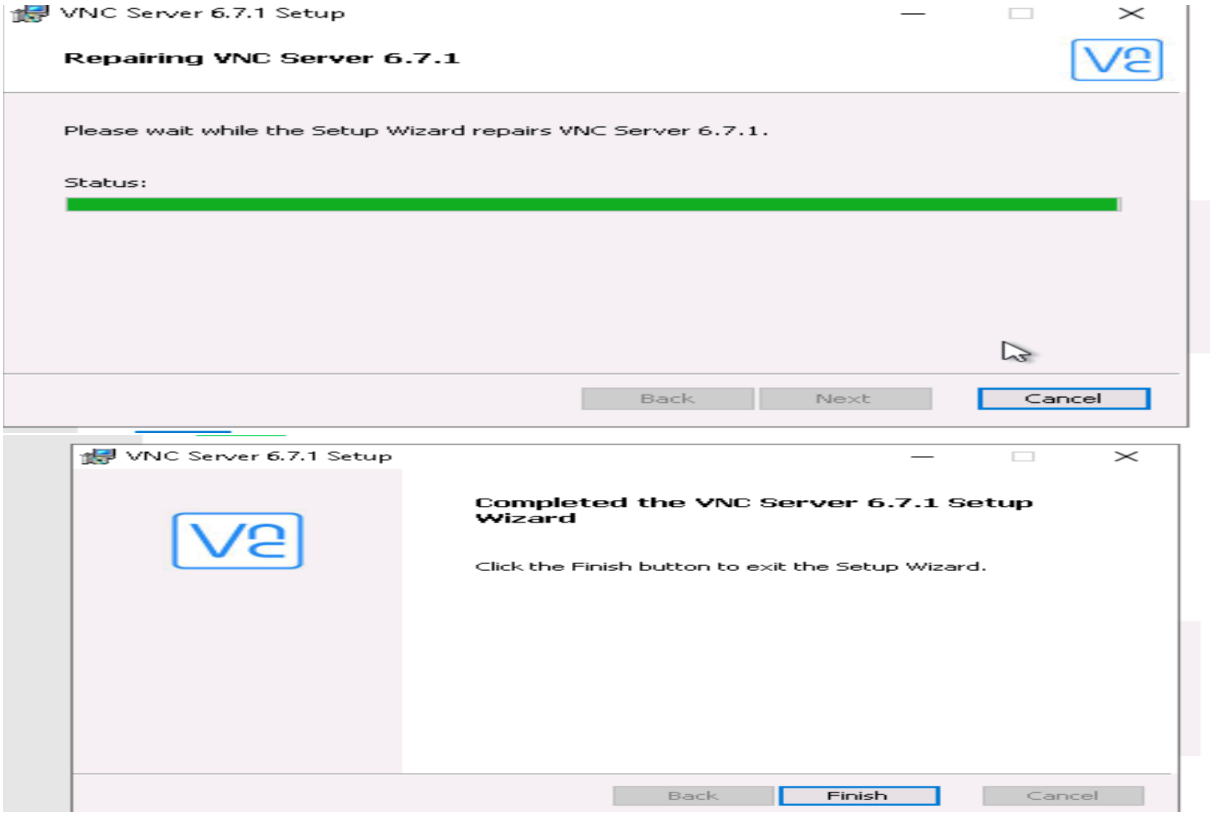
All applications should also be up to date on patches or fixes provided by the manufacturer. Any old versions of software should be uninstalled.

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

- Adobe
- VAC

4. *Explain the steps you took to determine this information.*
    - *By going to the owner of the app and search for the last version*
    - *And from the app in computer see exist version*
    - *Note Microsoft store dose not work*
5. *Explain the steps for updating each of these applications. Include screenshots as needed.*





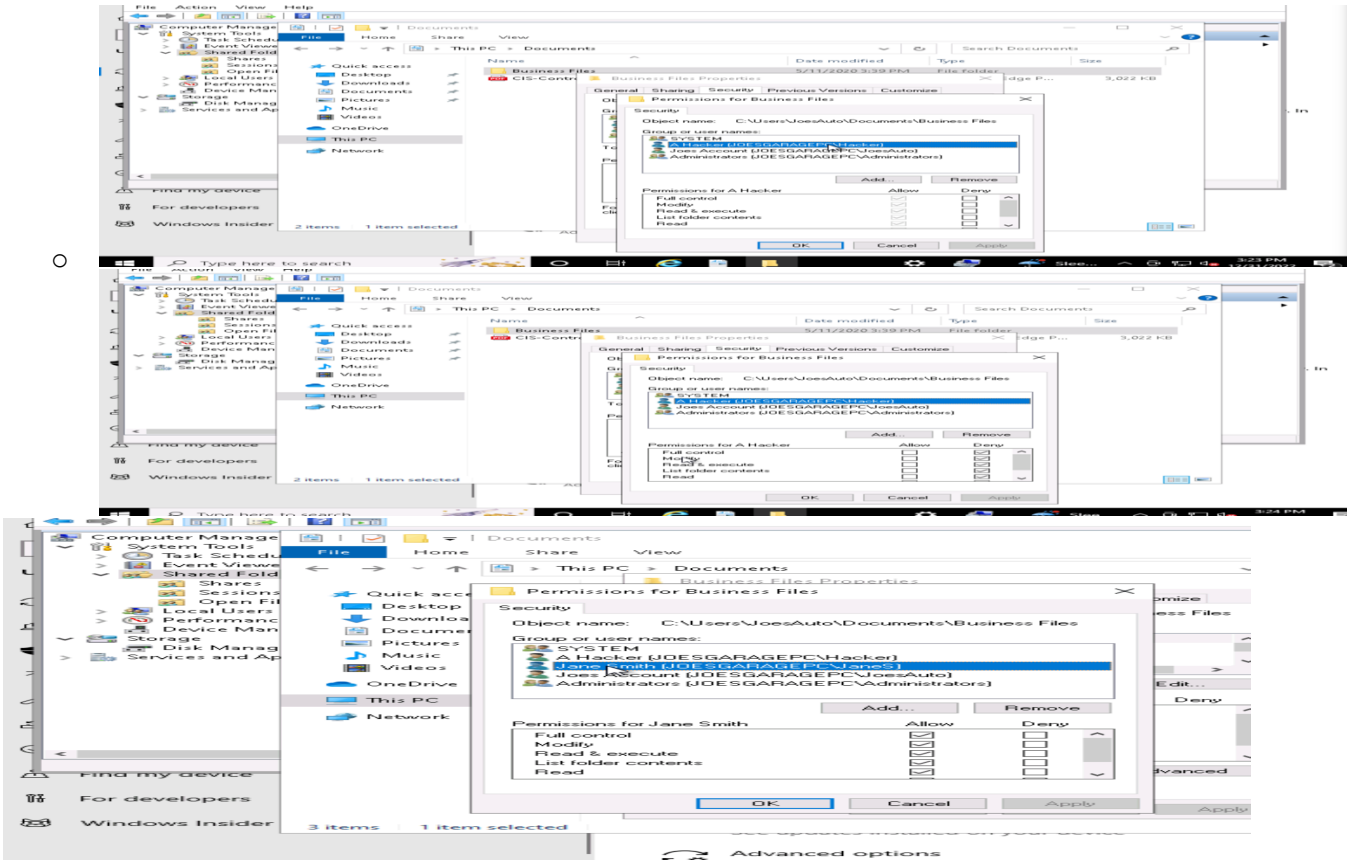
5. Securing Files and Folders

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

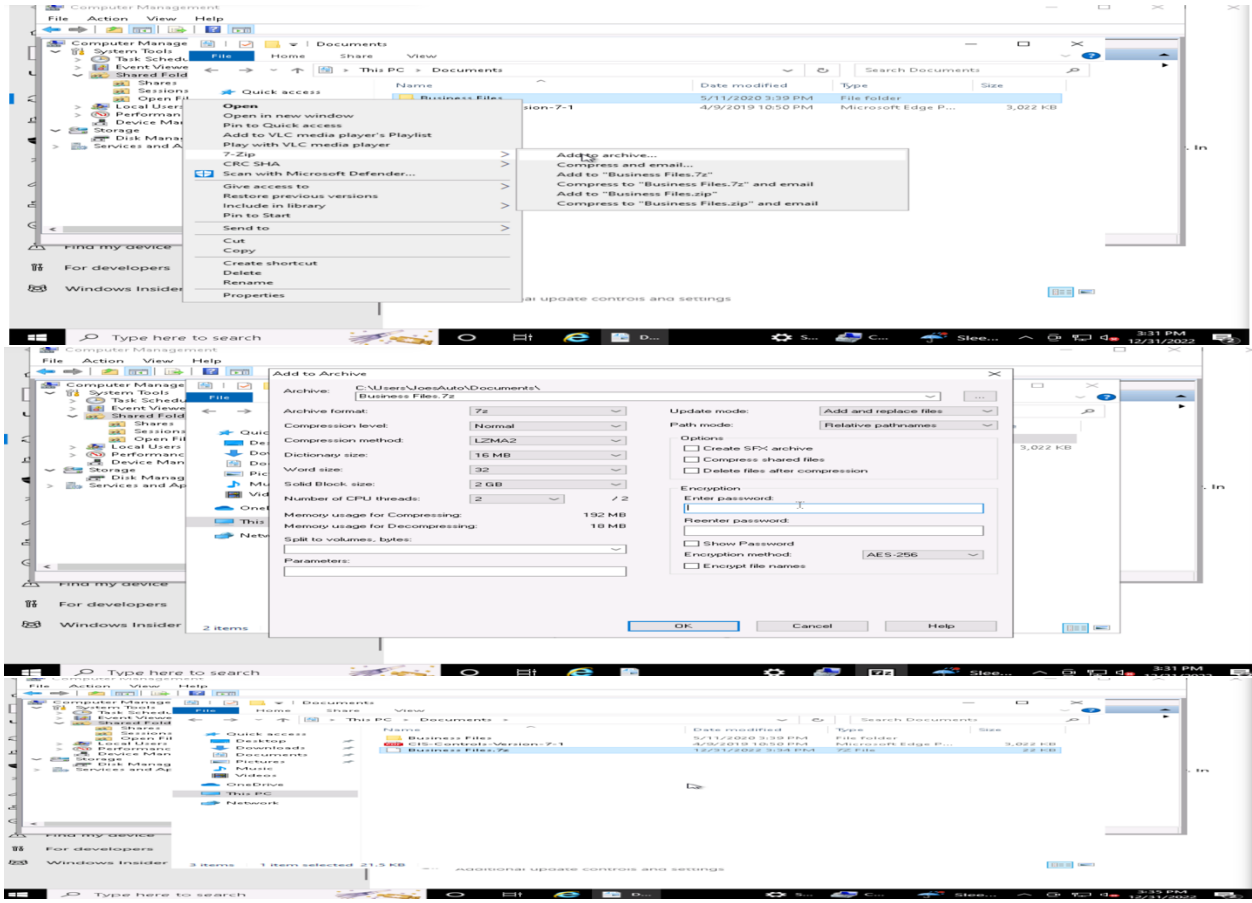
Joe suspects that other users on this computer beside him and Jane can see and change his business files. He wants you to check to make sure that only those two users have privileges to view or change the files.

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.]*
    - *Right-click the folder and select Properties>> Security*

- 

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.*

- 

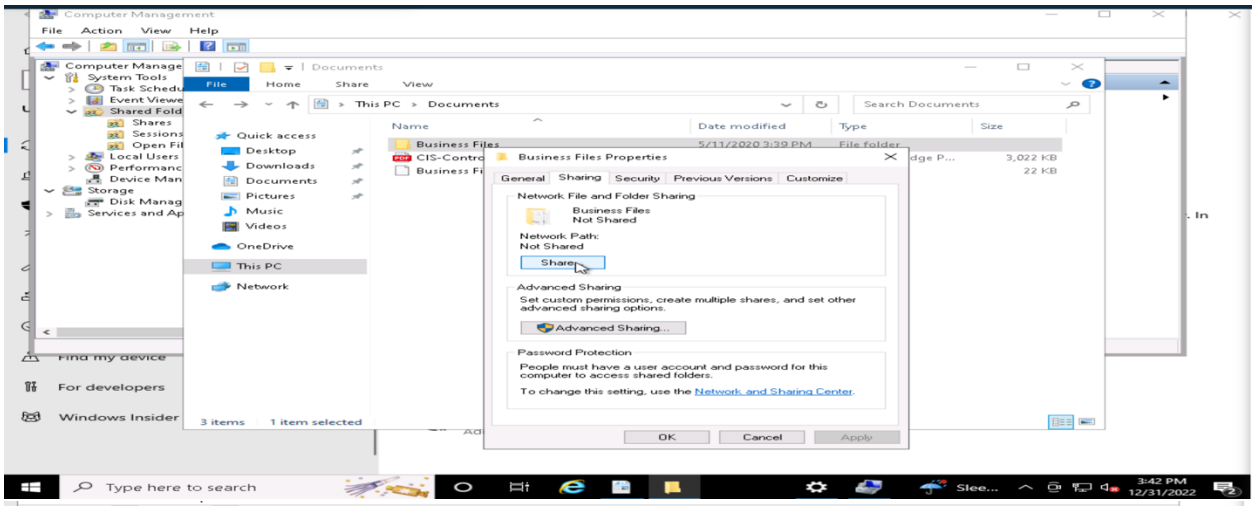
3. *What security fundamental does this provide?*
    - *Confidentiality*
    - *Will save* JoesWork *from unauthorized users and It will prevent data leakage>*
4. *The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?*

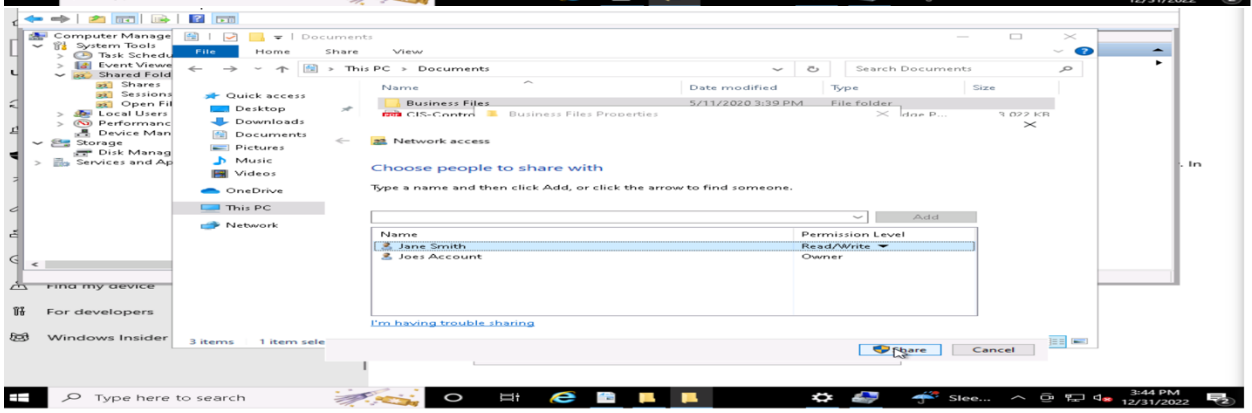
    - *CIS Control 6: Access Control Management*
    - *CIS Control 3: Data Protection*

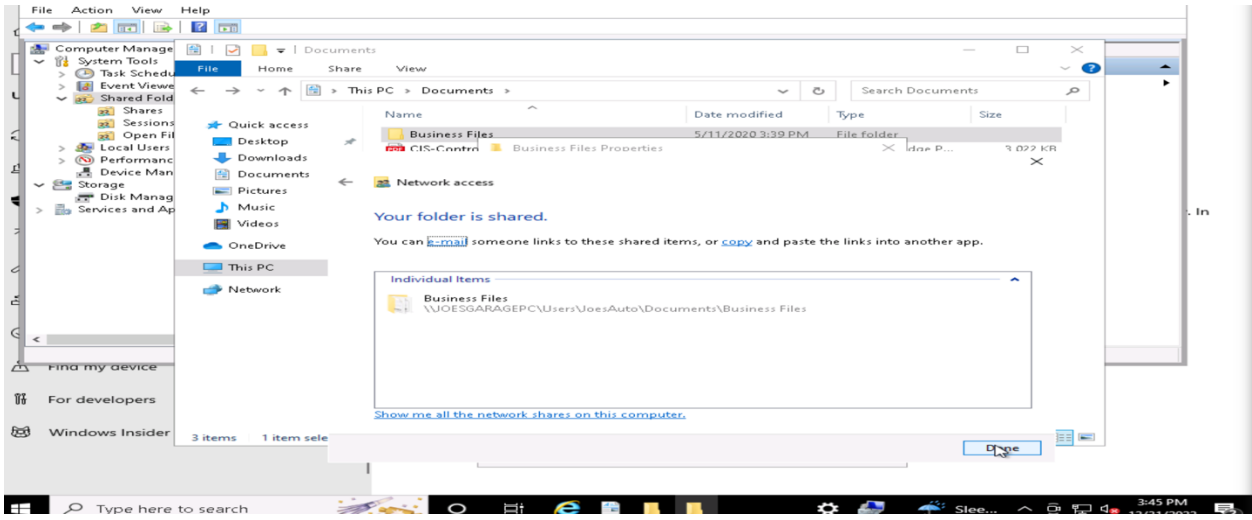
Shared Folders

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.*
    - *By go to the* Business *folder>> right click >> Properties>>*

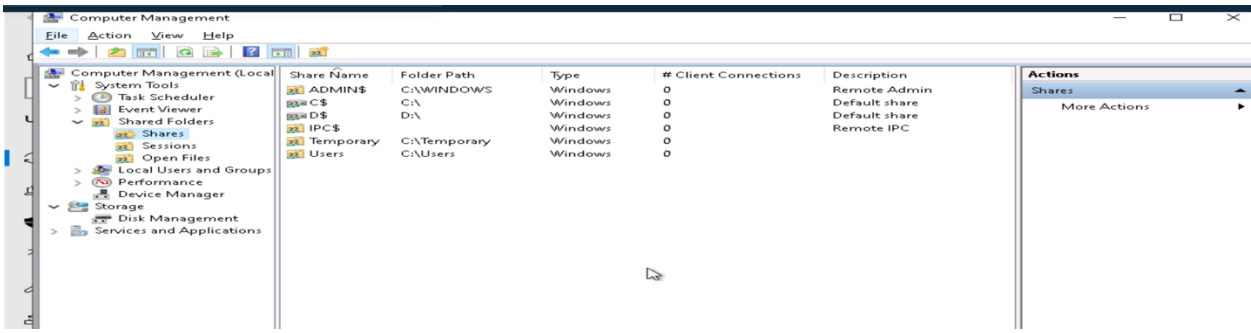
- 

- 

- 

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.*

    - *By going to computer management >> Shared folder>> shares*

- 

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.

8. Recourses:

- https://www.fortra.com/
- https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations
- https://www.cisecurity.org/controls/cis-controls-list
- https://www.simplilearn.com/top-5-ethical-hacking-tools-rar313-article
- https://www.itgovernanceusa.com/iso27002
- https://www.one.com/en/website-security/what-is-a-network-firewall
- https://diligex.com/
- https://www.loginradius.com/