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: Ghira George-Bogdan

Date of completion: 30.01.2023

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

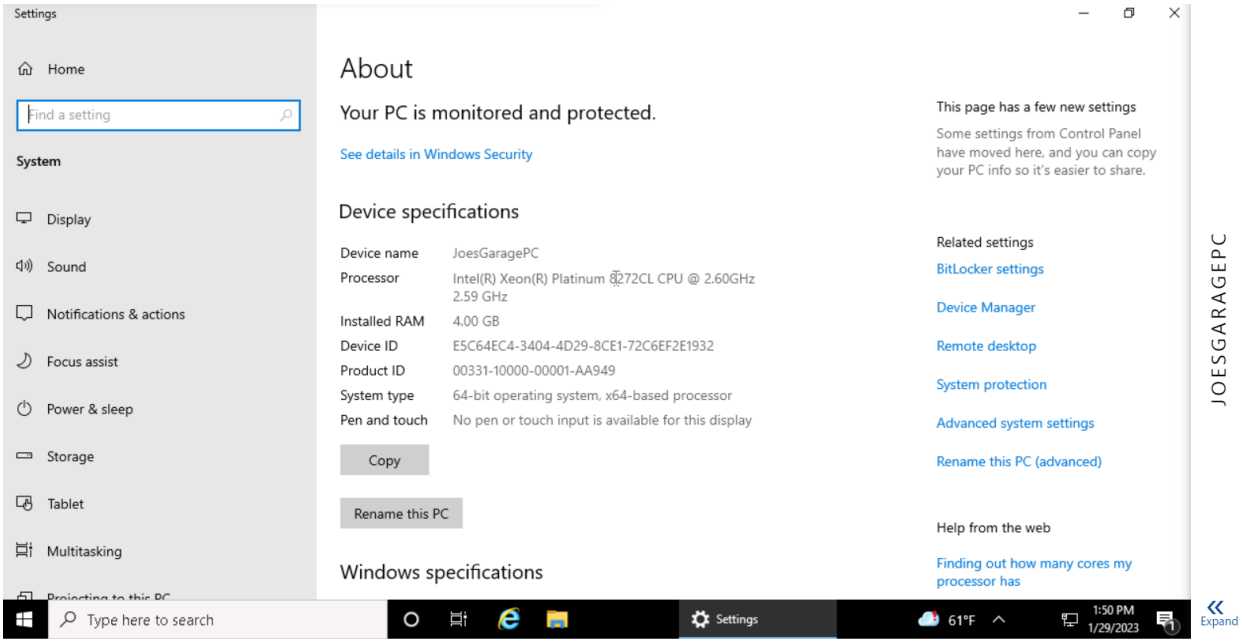
1. *Fill in the following table with system information for Joe's PC.*

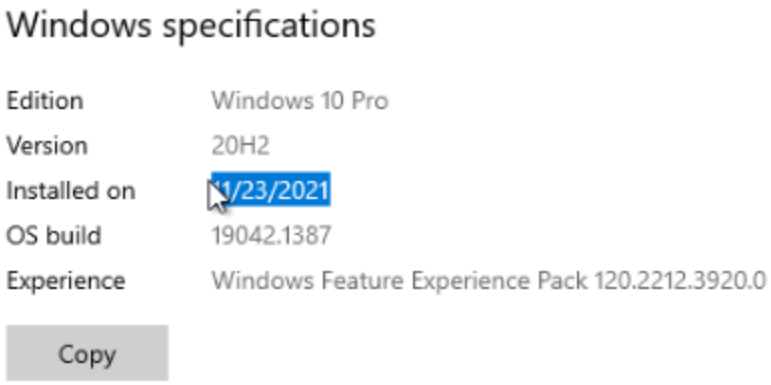
Device Name	JoesGaragePC
Processor	Intel(R) Xenon(R) Platinum
Install RAM	4 GB
System Type	64 bit, x64-based processor
Windows Edition	Windows 10 Pro
Version	20H2
Installed on	11.23.2021
OS build	19042.1387

2. *Explain how you found this information:*

In Control Panel>Settings>System>About. (Device specification and Windows specification)

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





Software

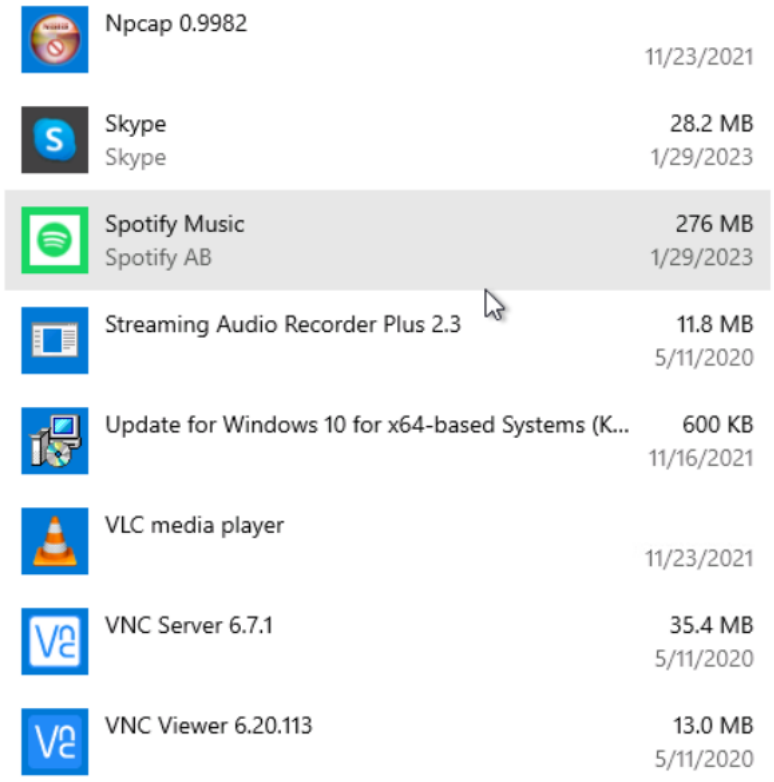
Another common early step in securing is taking an inventory of software or applications installed on a computer system. These are programs outside of the standard operating system.

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

- Npcap
- Skype
- Streaming Audio Recorder plus
- VLC
- VNC Server
- VNC Viewer

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

   Access Start button and look for Control Panel>Programs and features



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

   CIS Control 2: Inventory and Control of Software Assets

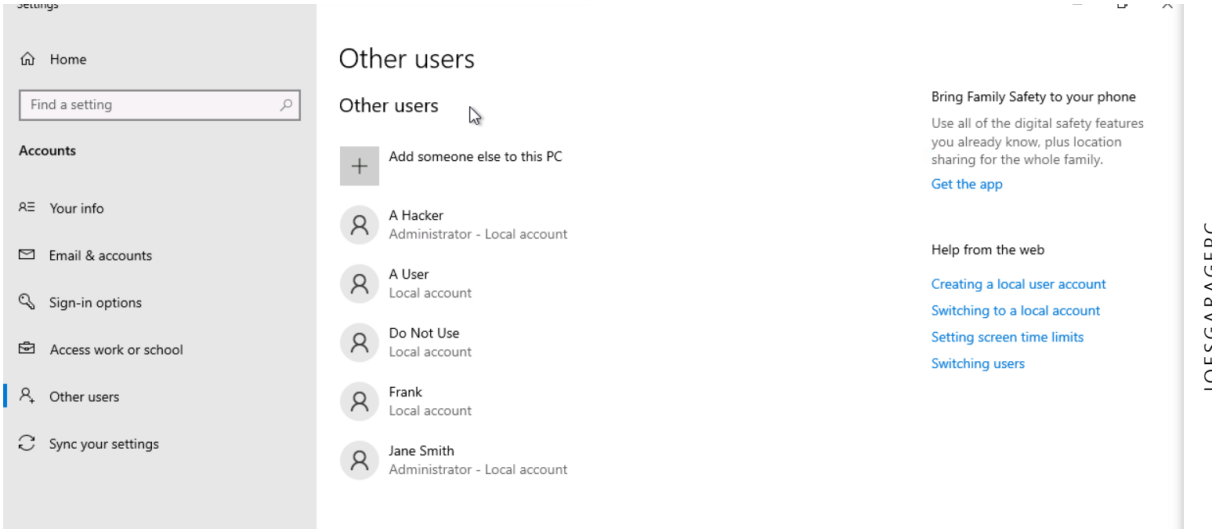
Accounts

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
A Hacker	A Hacker	Administrator
A User	A User	Local Account
Do not use	Do not use	Local account
Frank	Frank	Local account
Jane Smith	Jane Smith	Administrator
Joe	Joes Shop	Administrator

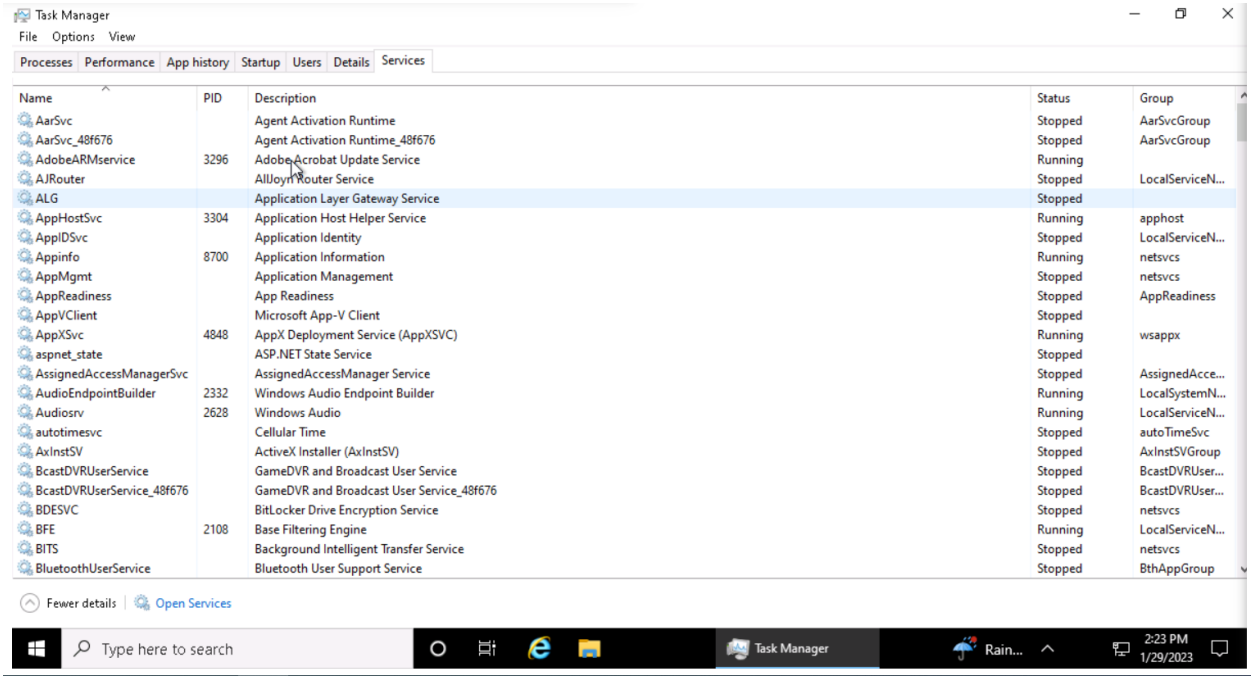
2. *Provide a screenshot of the Local Users.*



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.

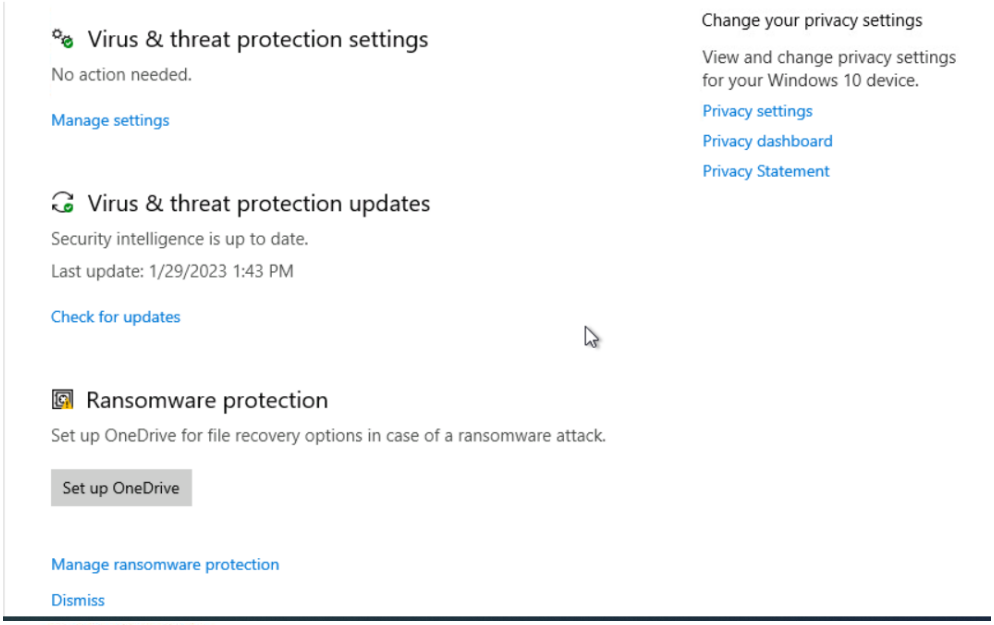
1. *Provide a screenshot of the services running on this PC.*

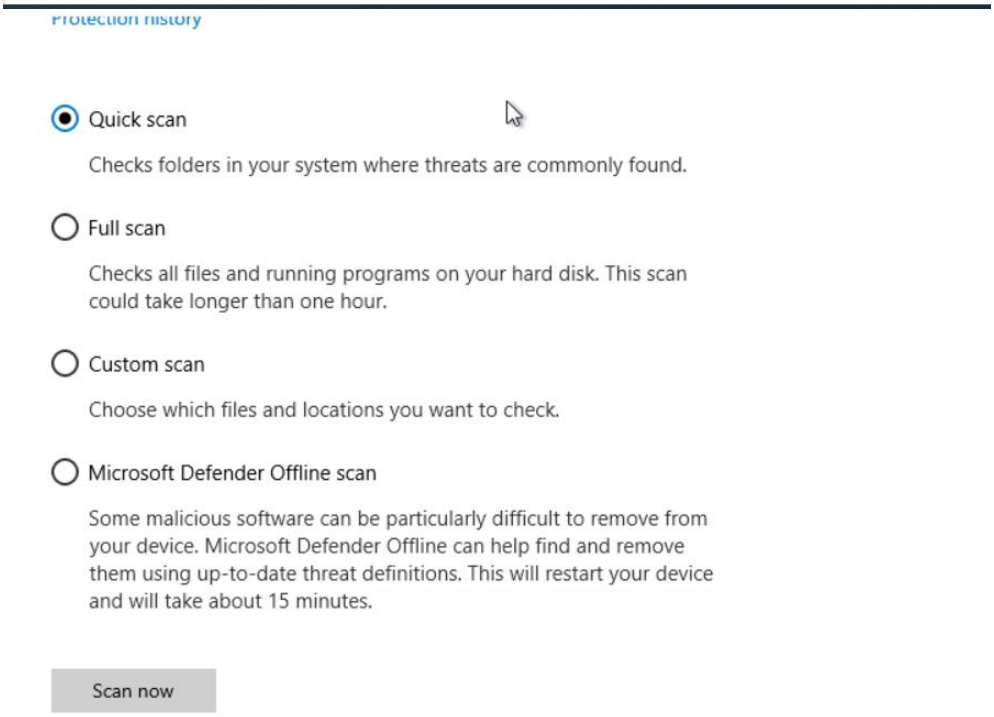


Security Services

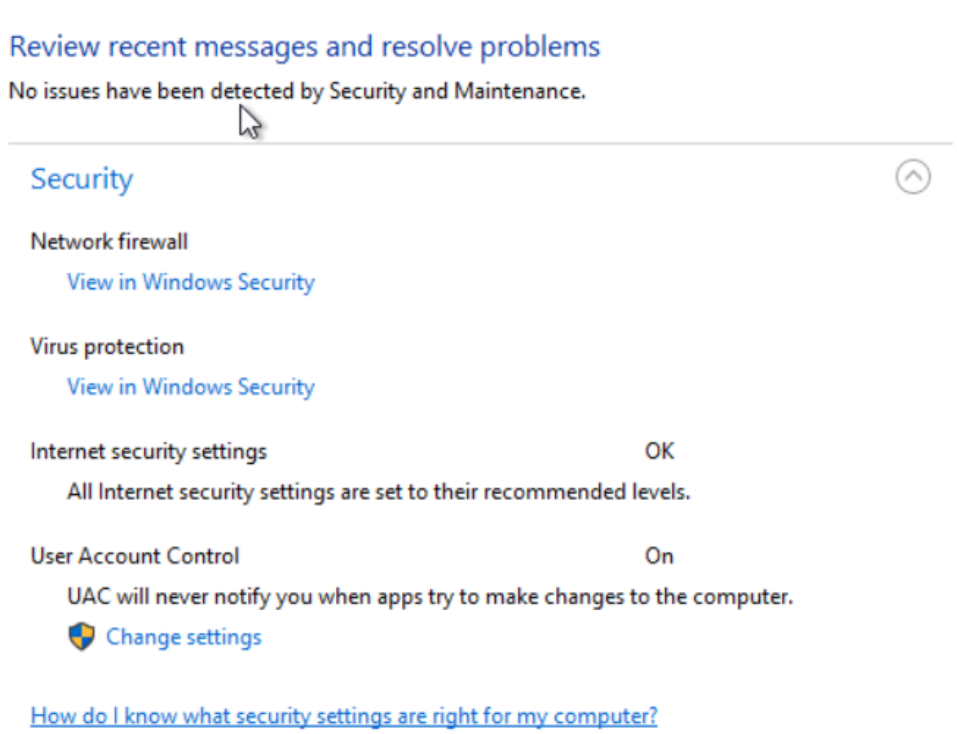
Joe wants to ensure that standard security services are running on his PC. He's content with using default Windows security settings and applications except for the rules outlined later. **Reminder that at this point you are just reporting what you observe. Do not make any changes to security settings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

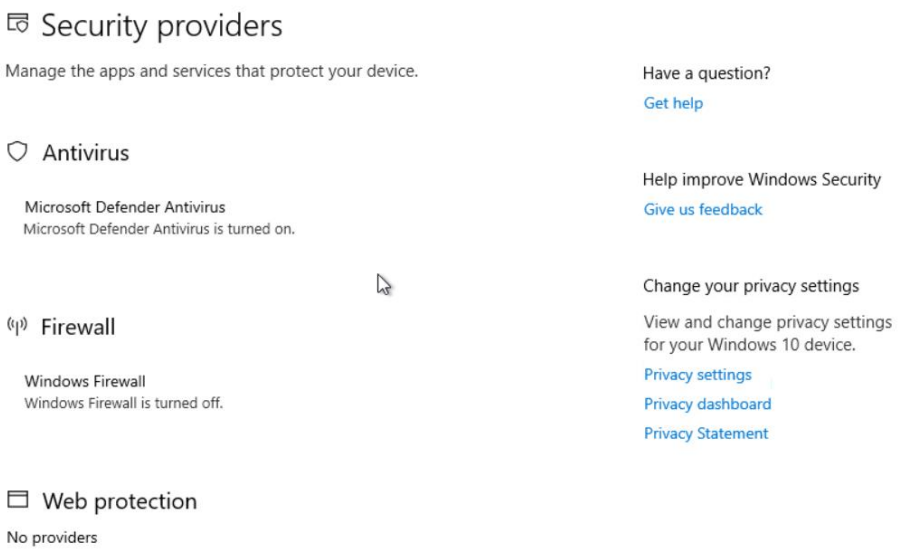




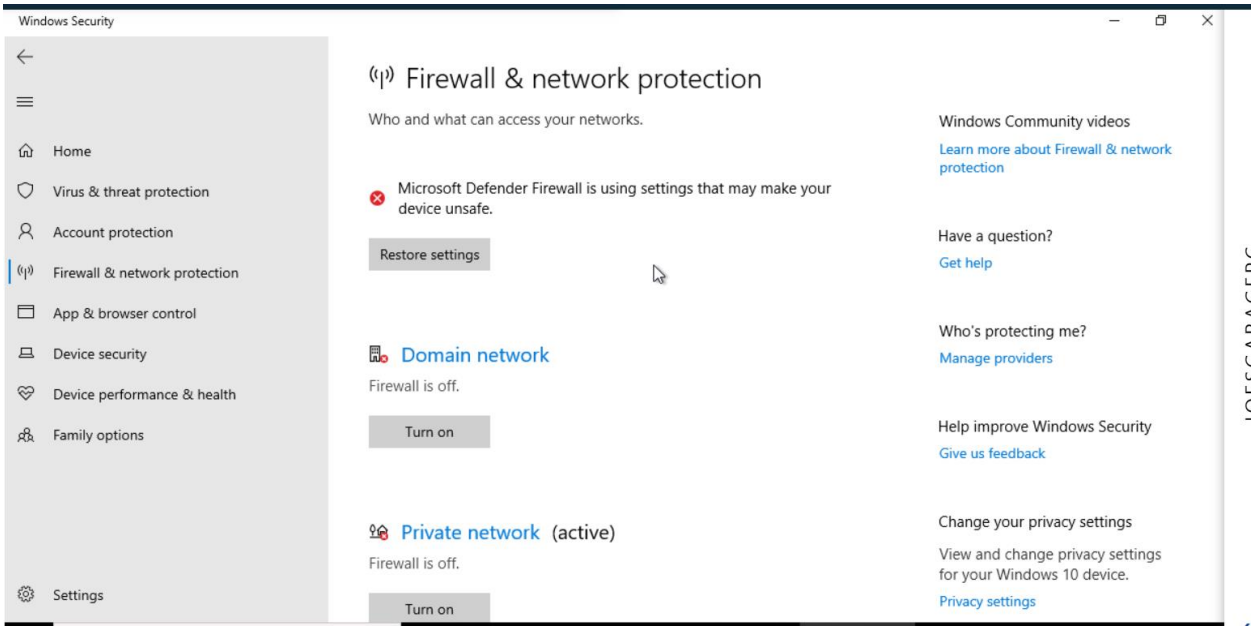
2. *The Windows 10 Security settings are also found from the **Control Panel > System and Security > Security and Maintenance**. Start by viewing **"Review your computer's status and resolve issues."** Provide a screenshot of this below:*



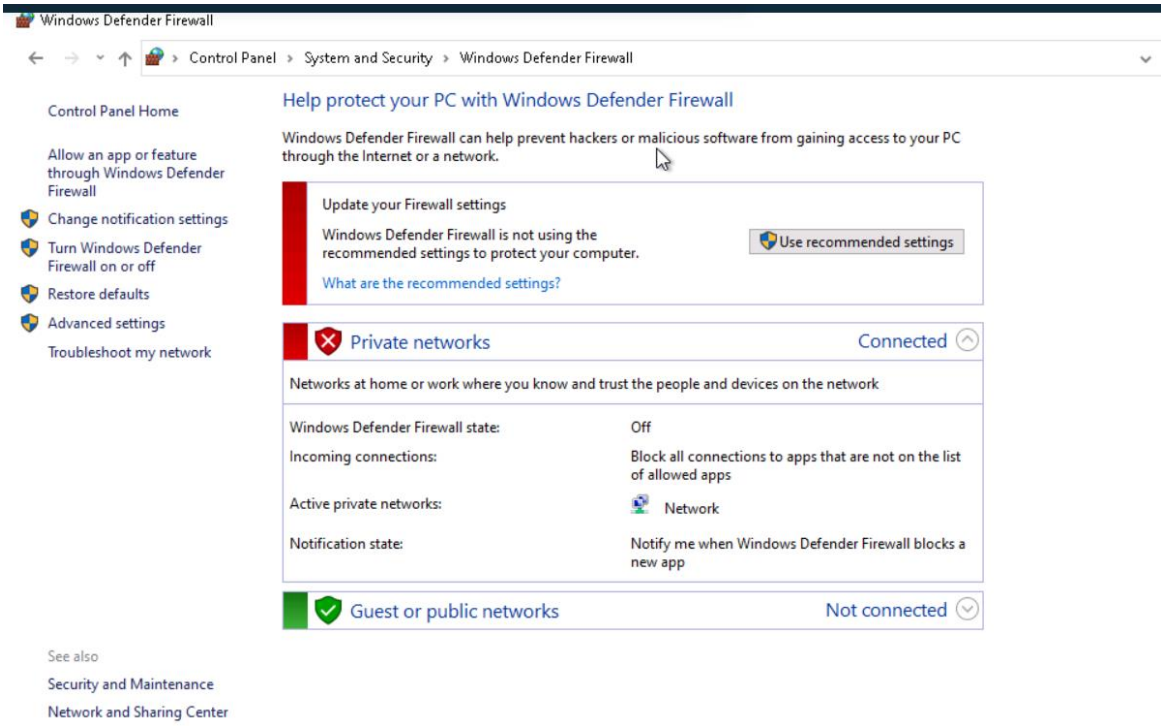
3. *Click on View in Windows Security to see the status there. Provide a screenshot of the **Firewall** settings.*



4.

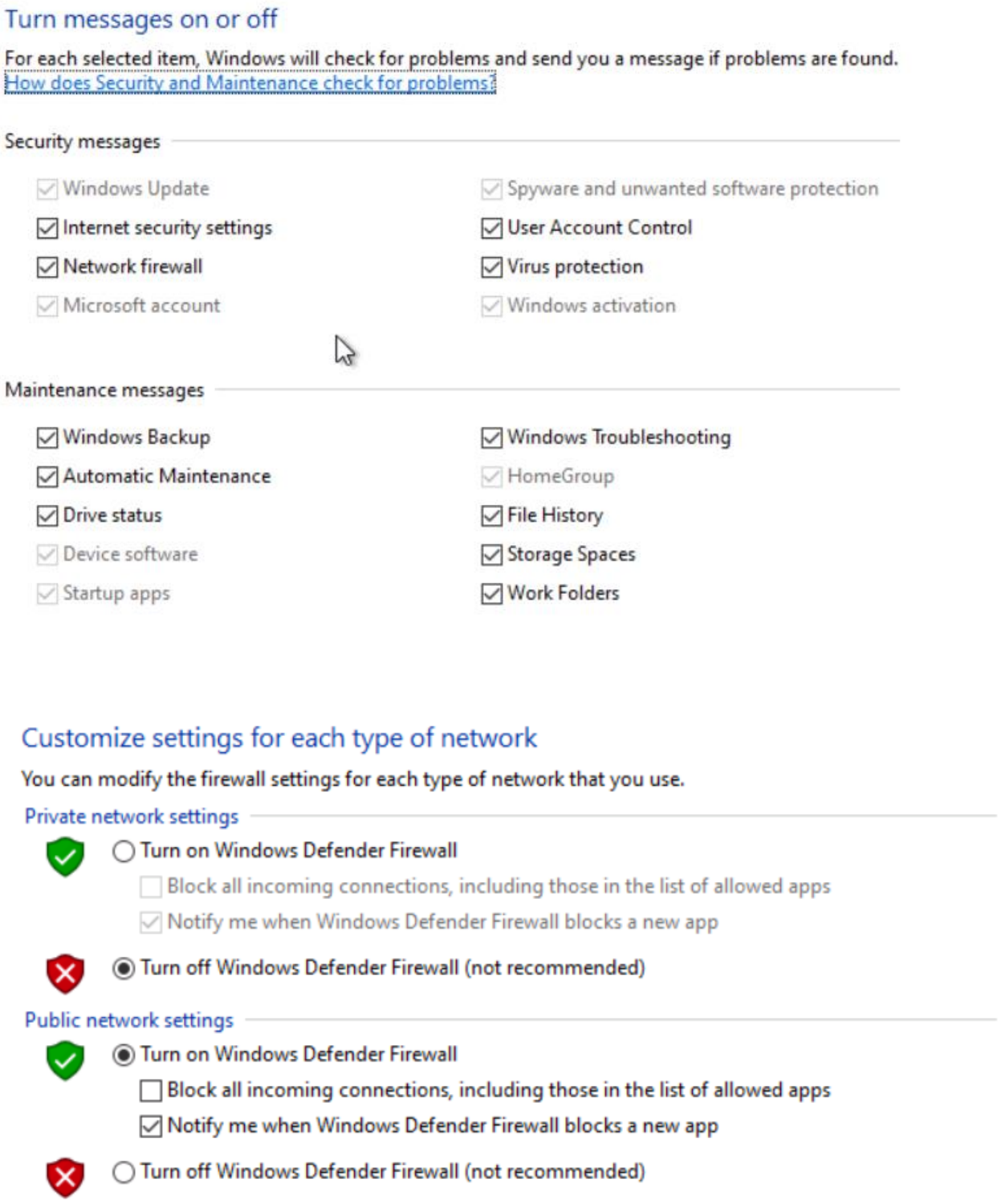


5. *From the **Control Panel**, go to **System and Security**. In that window, select **Windows Defender Firewall**. Provide a screenshot of it here:*



6. *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:



7. *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	Turn off Windows Defender Firewall
Firewall product and status – Public network	Turn on WDF >Notify me when WDF block a new app
Virus protection product and status	Windows Firewall, Windows Defender
Internet Security messages	Windows update-off Internet security settings-on Network firewall-on Microsoft account-on Spyware and unwanted software protection-off UAC-on Virus protection-on Windows activation-off
Network firewall messages	Block all incoming connections, including those in the list of allowed apps – OFF Notify me when WDF blocks a new app - ON
Virus protection messages	
User Account Control Setting	UAC will never notify when an app will make changes to your computer

8. *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.]

- Private network WDF is turned off > This could allow unwanted connection from outside of the network
- Domain network firewall is OFF > When a computer is connected to a domain network, this could also lead to unwanted connection from outside the domain.
- No malware software installed on machine > vulnerable to malware attacks
- No Hardware/Software inventory – It is difficult to keep up to dates components if you do not have an idea of what you must update.

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?*
   CIS Critical Security Controls

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

Giving the fact that Joe is using Windows suite, I would recommend using Microsoft Security baseline.

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?

Joes PC does not meet in a complete way any of the CIS controls.

System and Security

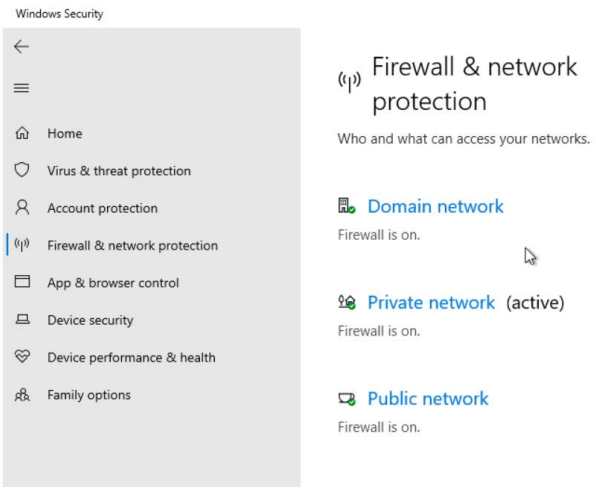
At this point, you need to enable security services for this PC. Pick at least 3 of the following 5 areas to secure in order to satisfactorily meeting the project requirements:

- 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.*
   Access windows security > firewall & network protection >
   Turn ON - Domain network
   Turn ON – Private network
2. *Include screenshots showing the firewall is turned on.*



3. *What protection does this provide?*

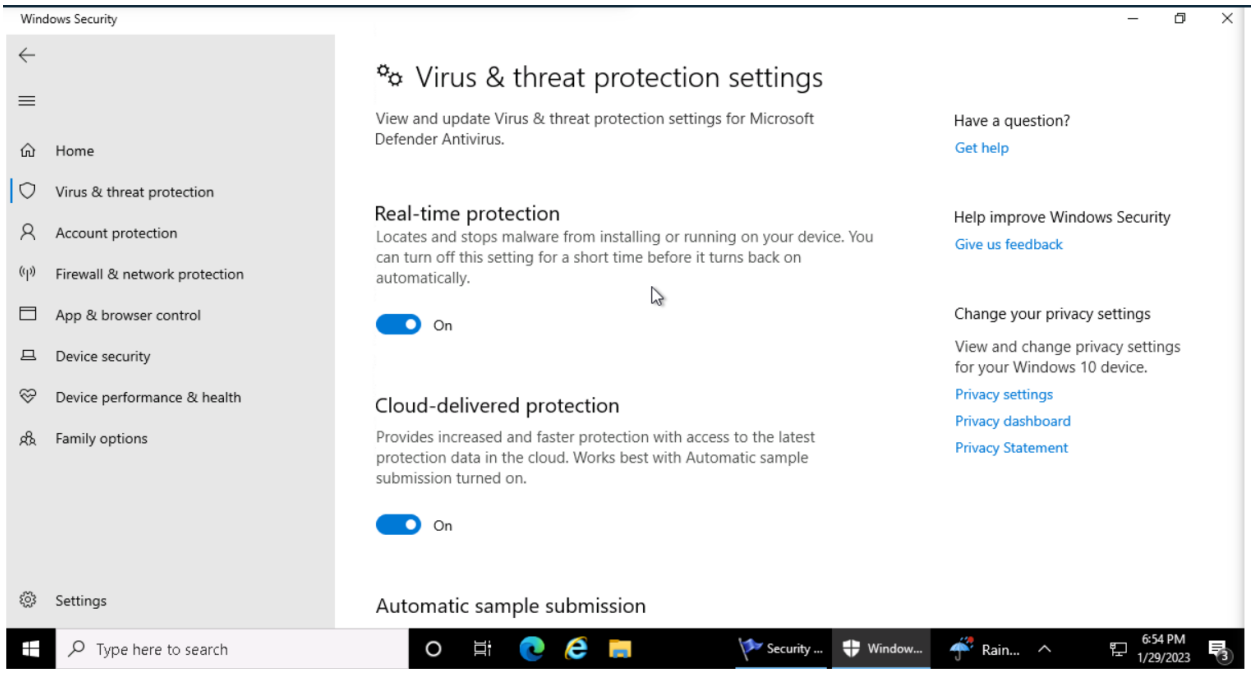
   A firewall offers protection of unwanted access on an internal network. It is a filter that does not allow suspicious activities inside the network/computer.

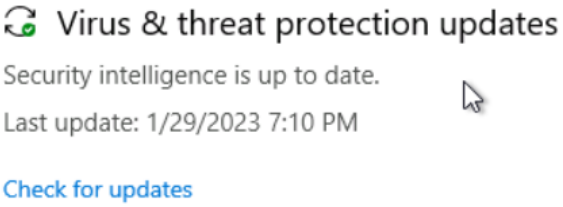
Virus & Threat Protection

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.*
   Settings>virus and threat protection > Set On for real-time protection/

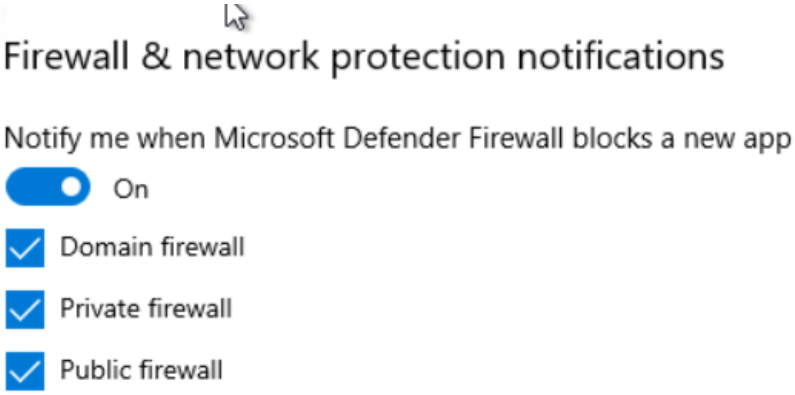
2. *Include screenshots to confirm that anti-virus is enabled.*





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



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

- Having an updated antivirus means that it can identify the latest viruses, which means a better protection.
- Having notification for when a app is blocked means that the user is informed in real time of a potential threat.

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

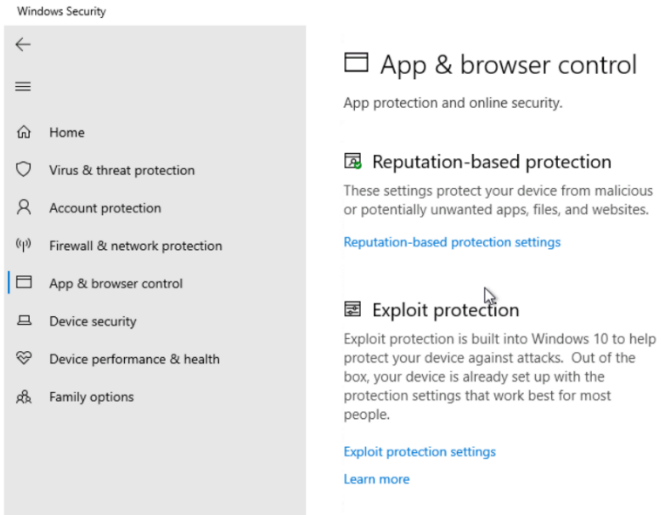
   - Continuous vulnerability management

   -Incident response and 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.*



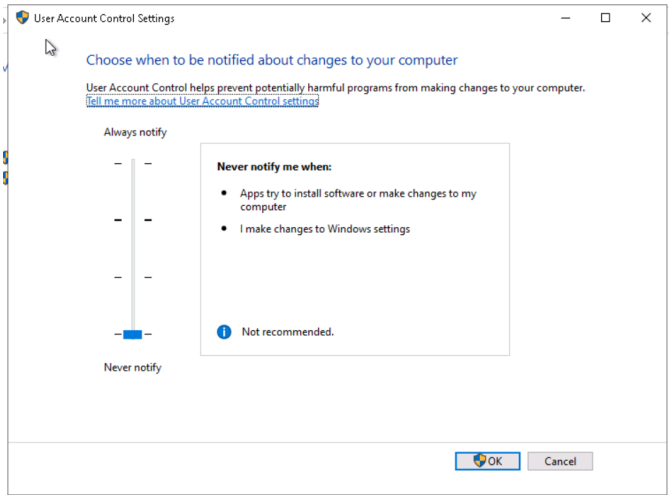
User Account Control Settings

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?*

   -Never notify

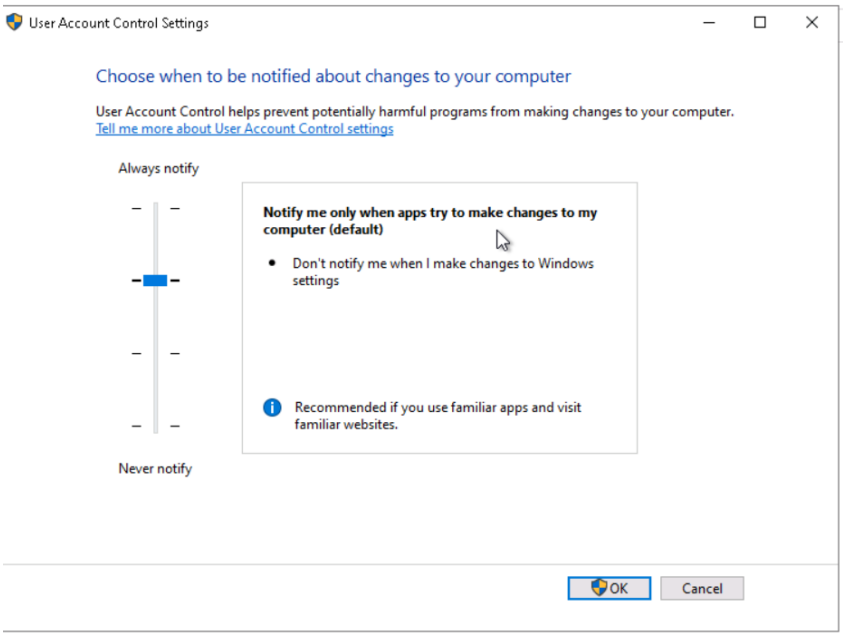
Before:



This is available from the above security settings.

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

   -Recommended

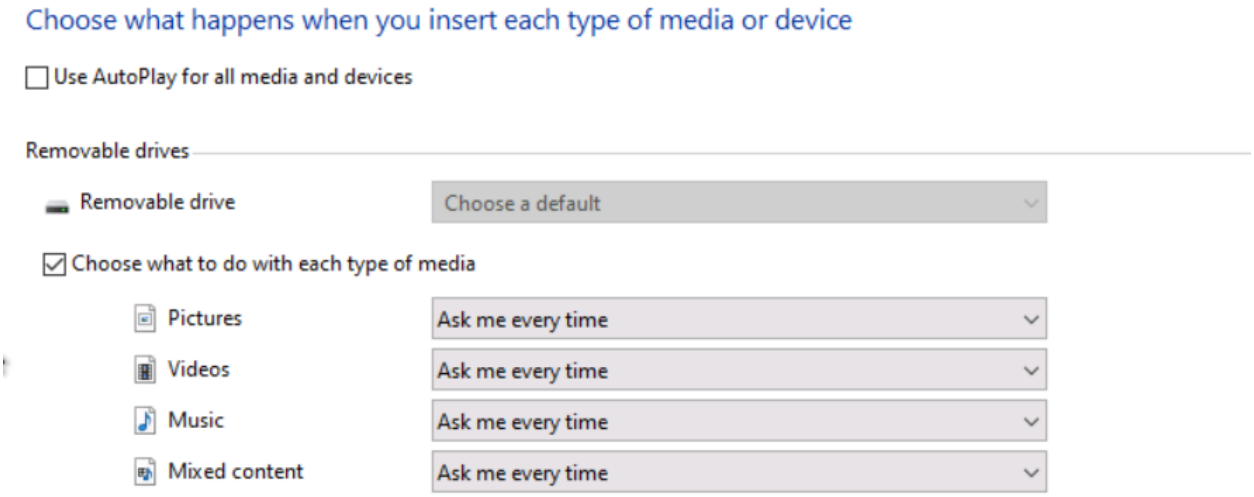


Securing Removable Media

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.

User Accounts

1. *What user accounts should not be there?*

-A Hacker (administrator)
-Do Not Use
-Frank

2. *Bonus questions: What is Hacker's password?*
3. *Explain the steps you take to disable or remove unwanted accounts.*

Control Panel>User Accounts>Manage Accounts>Delete Account> Select Unwanted Account> click on Delete the Account >Delete the files > Delete Account.

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

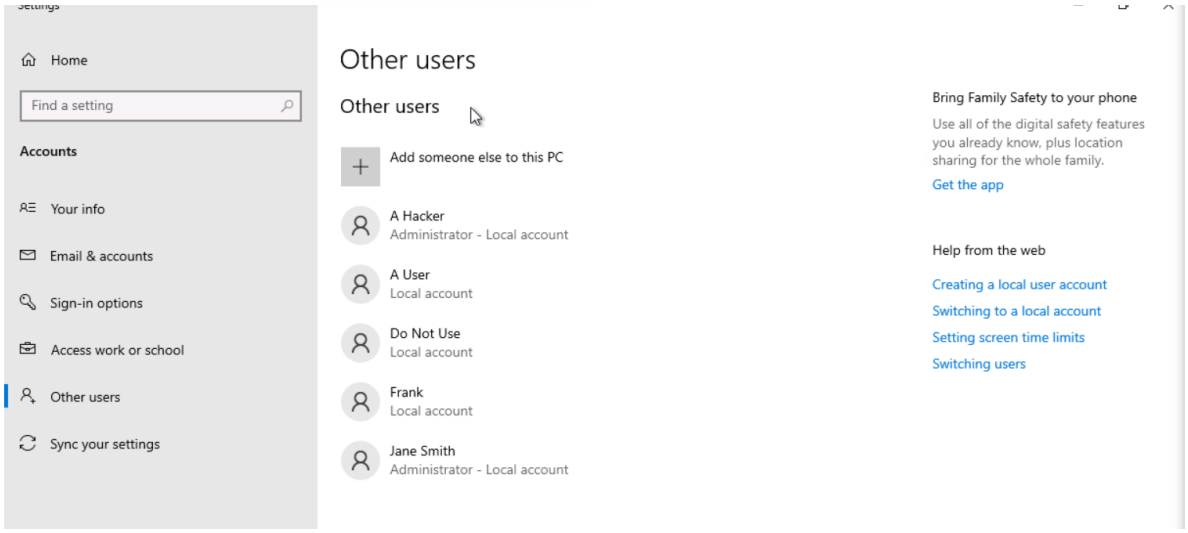
   -An account can be used be a bad actor to gain access to data/files, because these account are not in people eyes and their activity will go unnoticed.

   - an account has credentials that an employee knows, and sometimes, employees left the company being upsets and furious on manager/company and wants to do harm, to steal information, to delete files, to send emails to customers, etc.

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" account
   "Jane Smith" account
6. Explain how you determined this. Provide screenshots as needed.

   Accessing In Settings>Accounts >On Other Users page are listed all users that have an account on this PC, including their account status.



Administrator privileges for too many users are another security challenge.

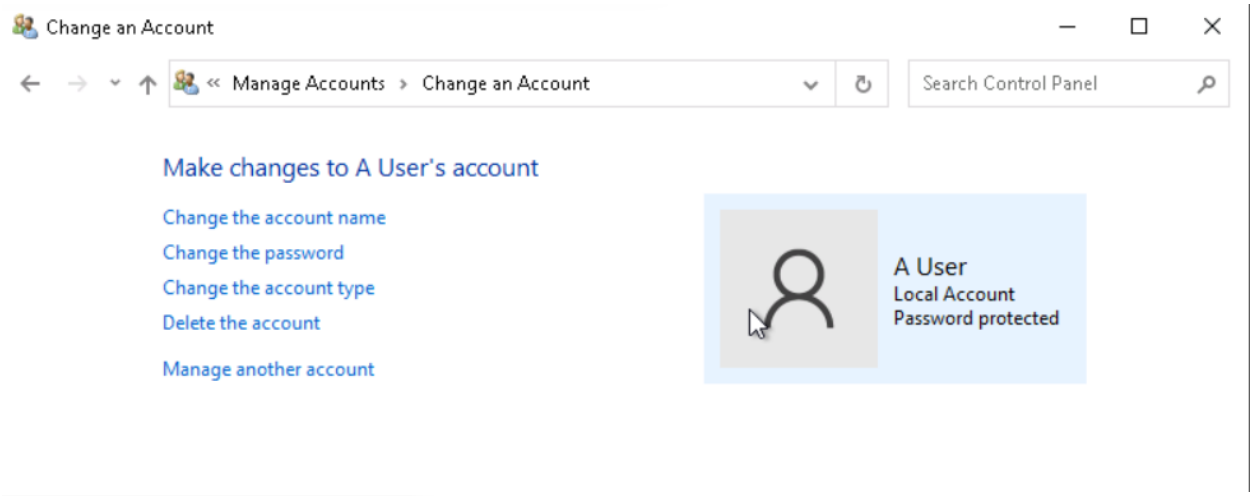
7. Provide at least three risks associated with users having administrator rights on a PC.

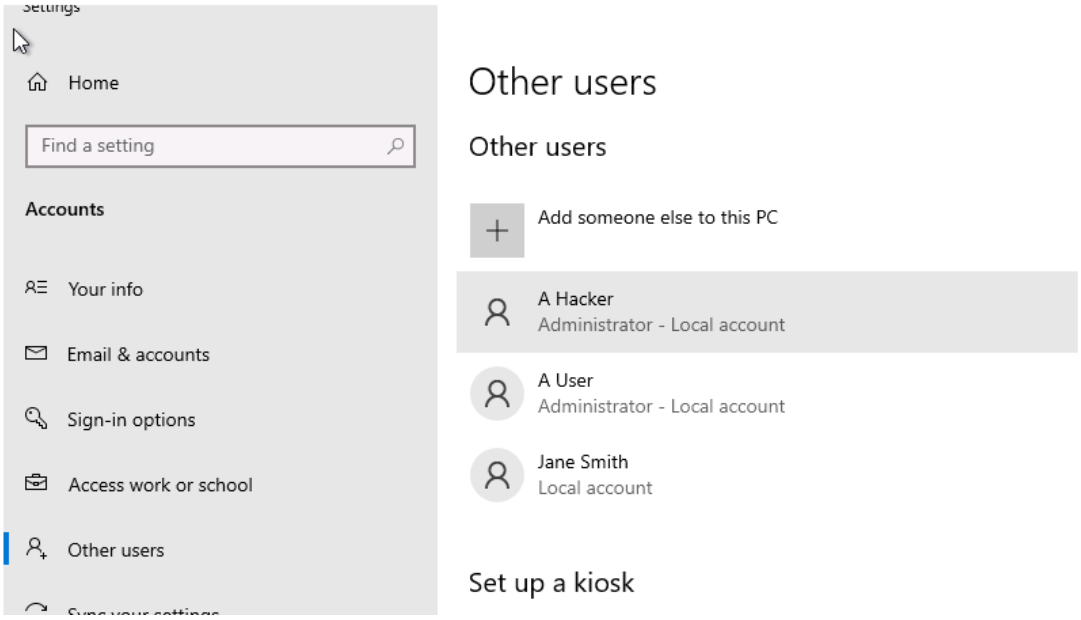
- Admin users can install software without auditing.
- Admin user can run software that are intended to do bad (steal data, money)
- Admin user can view other user data/information and steal it.
- Admin users can change the security setups of a computer, without being aware of the consequences of their action, posing a threat to a computer and of the entire network where that computer is connected to.

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.*

Control Panel>User Accounts> >Manage another account> Select "A user" Account >click on change the account type> Select Standard account>click on change Account Type.





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

   -security principle of least privilege

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

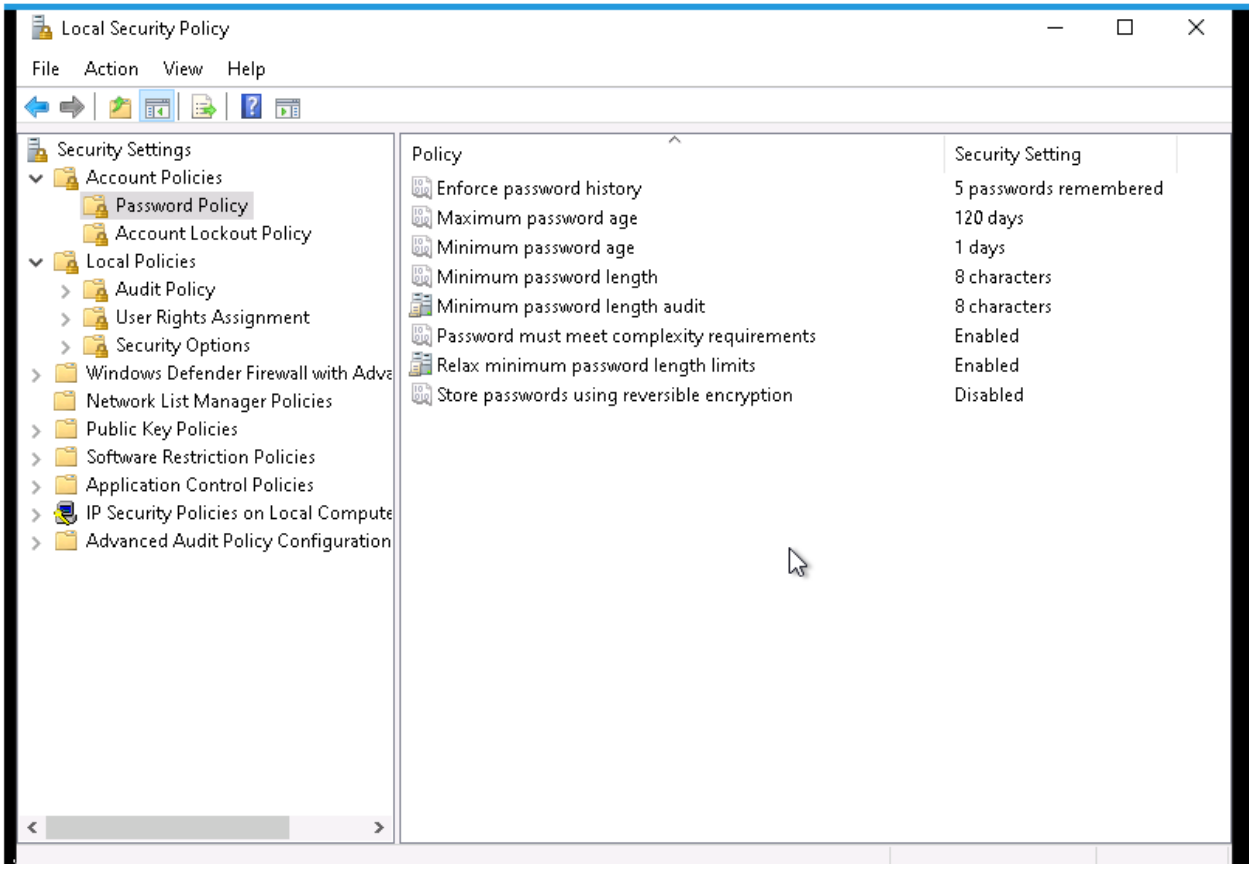
    CIS Critical Security Control 6: Access Control Management

Setting Access and Authentication Policies

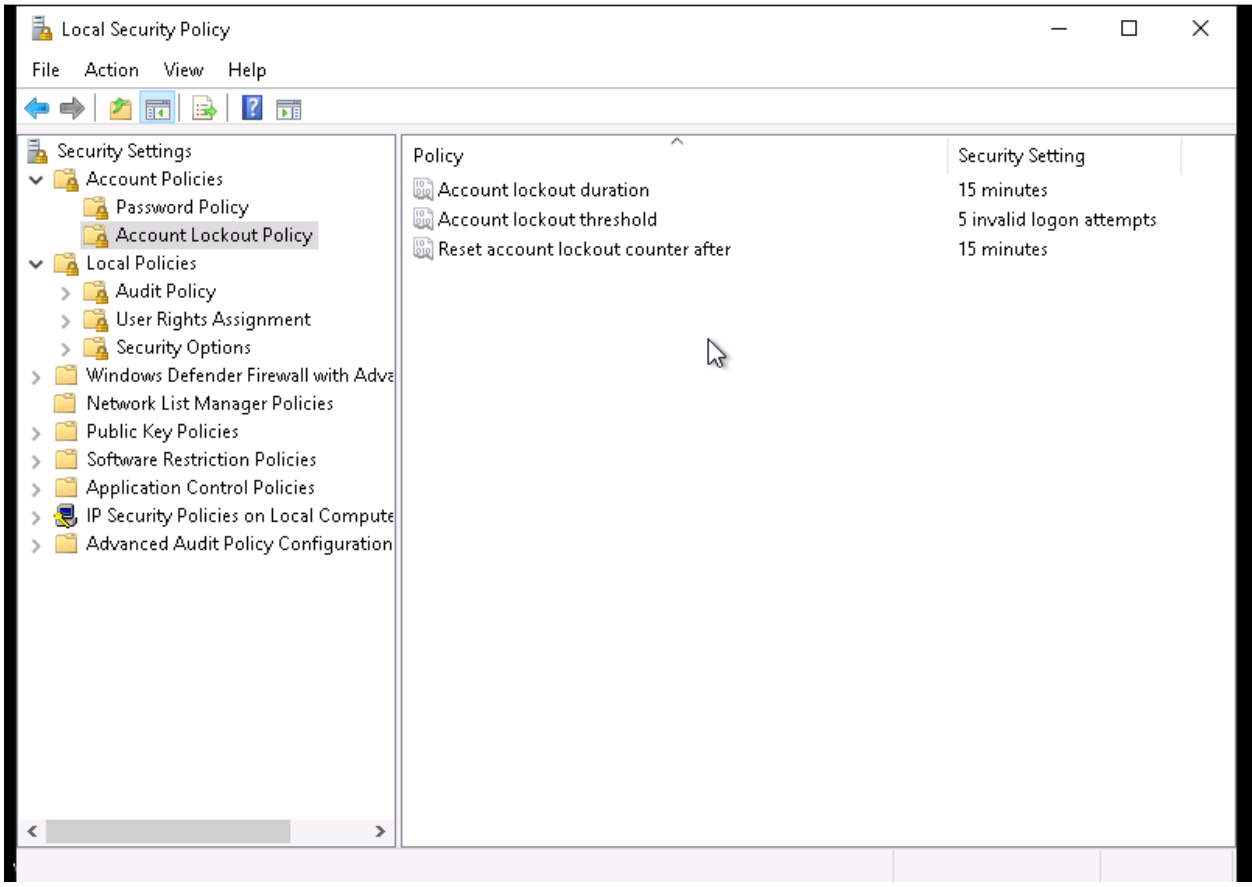
After you talked with Joe about security, he has asked that the access rules outlined above be in place on his PC. These are set using the Local Security Policy function in Windows 10. On the Windows search

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:



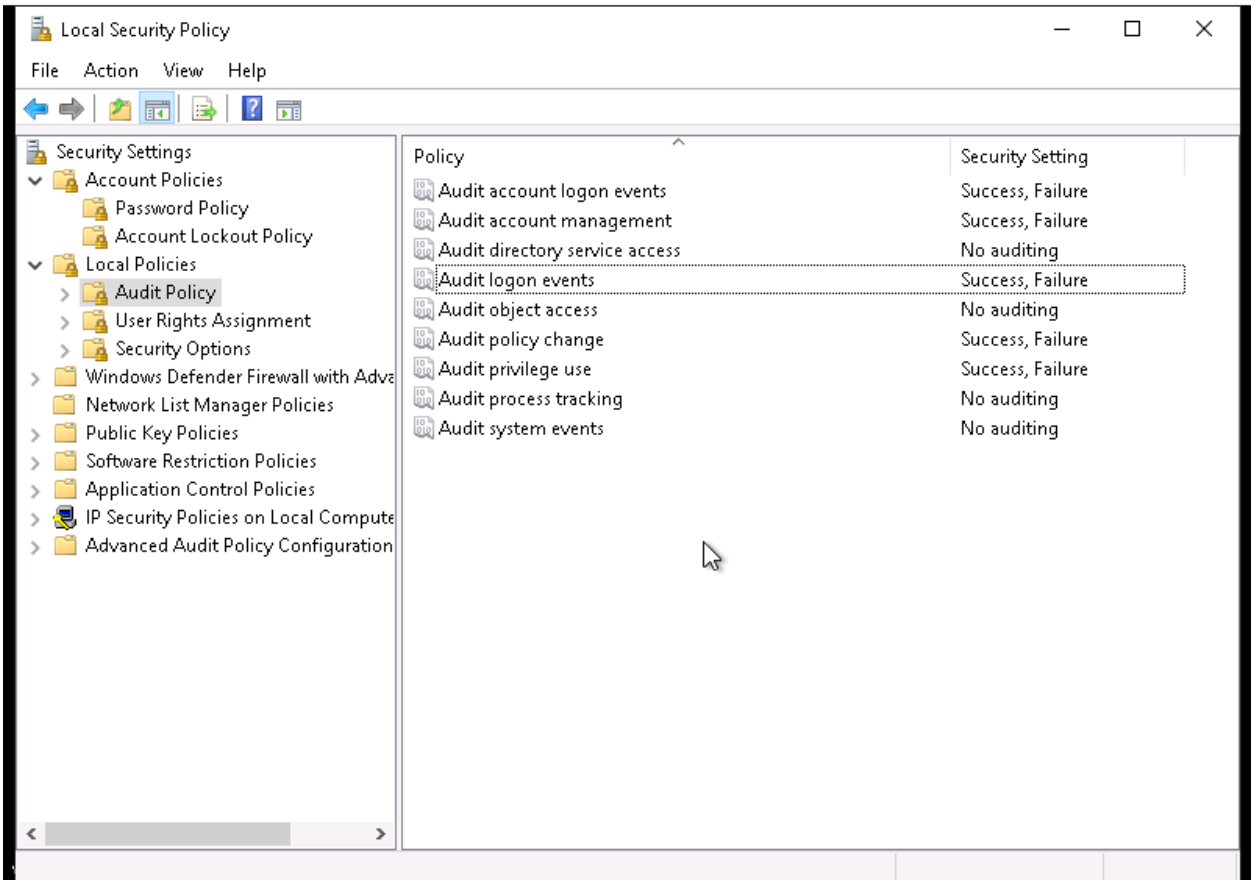
- Setting the Account Lockout Policy:



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.

Remove unneeded or unwanted applications

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

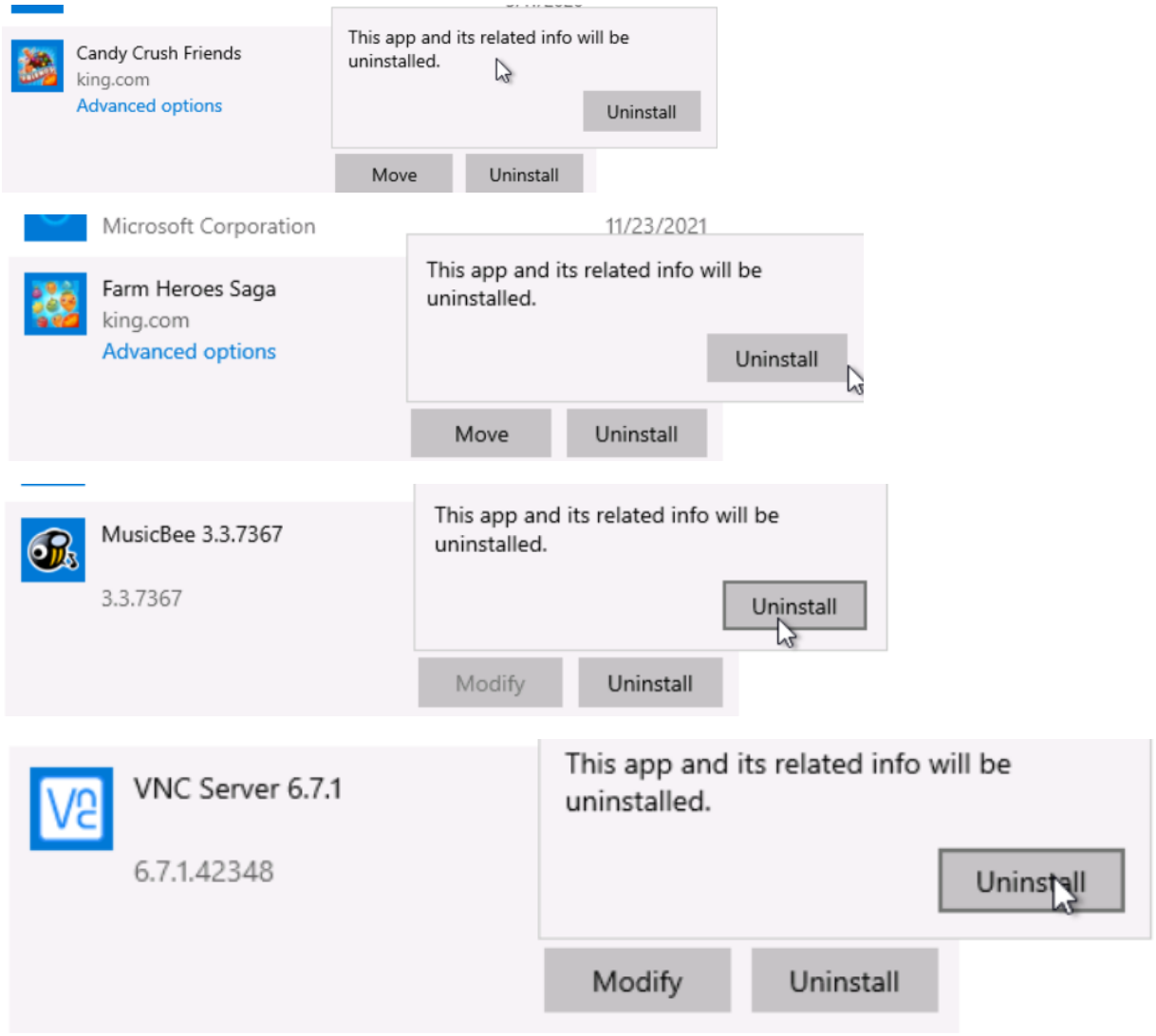
- *Candy Crush Friends*
- *Farm Heros Saga*
- *MusicBee*

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

- *It increases the chances of being accessible to hacking*
- *It consumes hardware resources*
- *It makes difficult to manage an inventory and review it.*

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.*

   Setting > Apps>App & feature > Click on Uninstall button for unwanted app > Confirm by clicking on Uninstall.

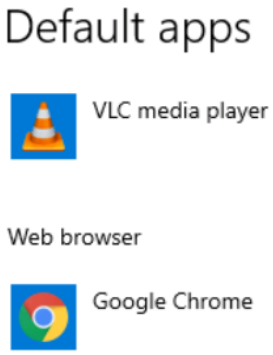


Default Browser

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.*

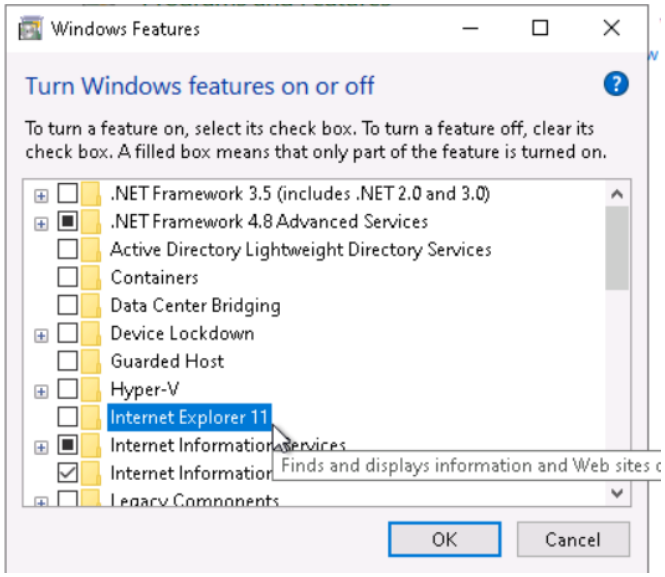
Setting > Apps>Default Apps>click on Plus button and select Chrome Browser from the list.



2. *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
    - It is no longer supported by Microsoft
    - It is based on an old architecture, and it is prone to much to many 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.*

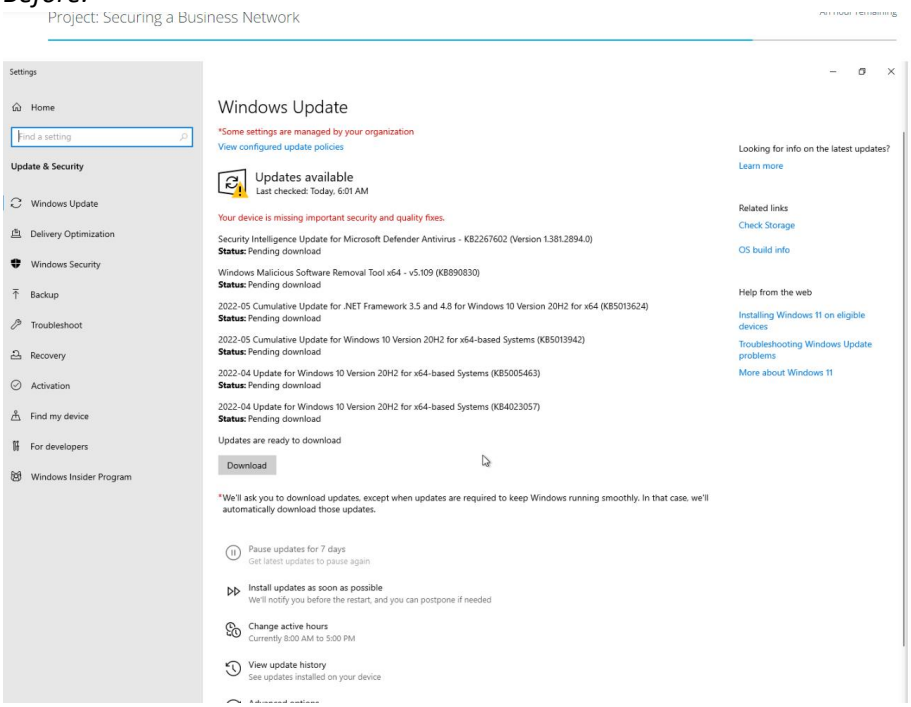
4. 

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.*
   Control Panel>Settings>Update & Security >Windows Update.

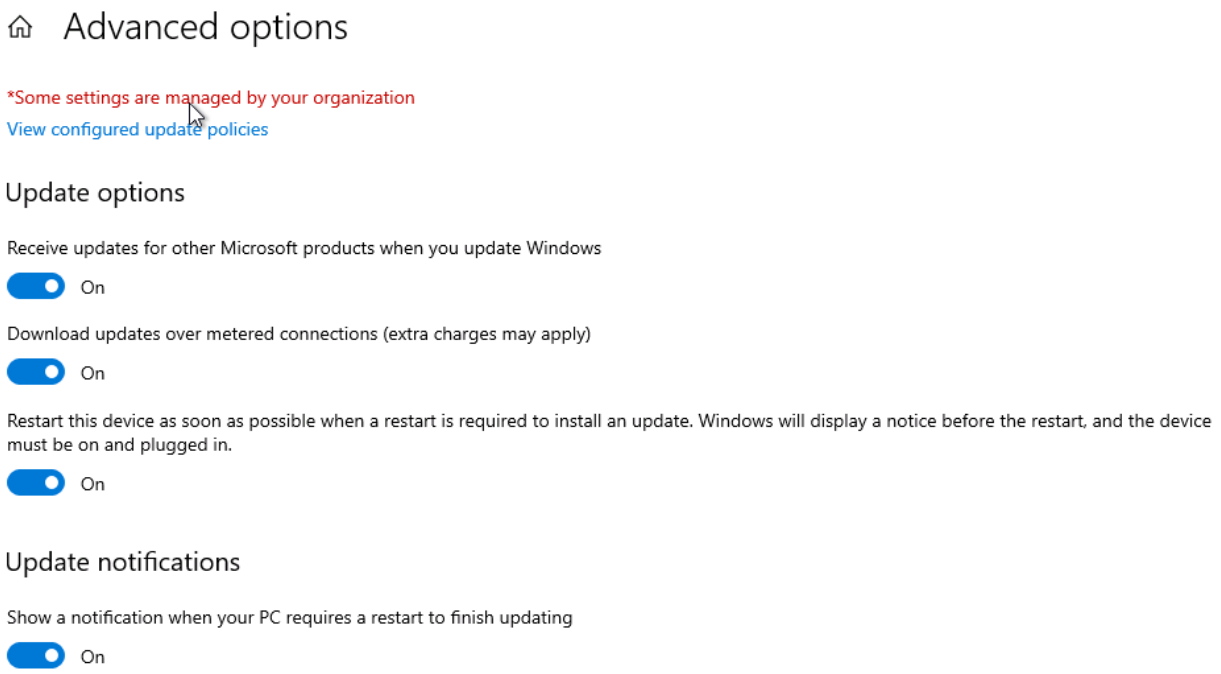
Before:



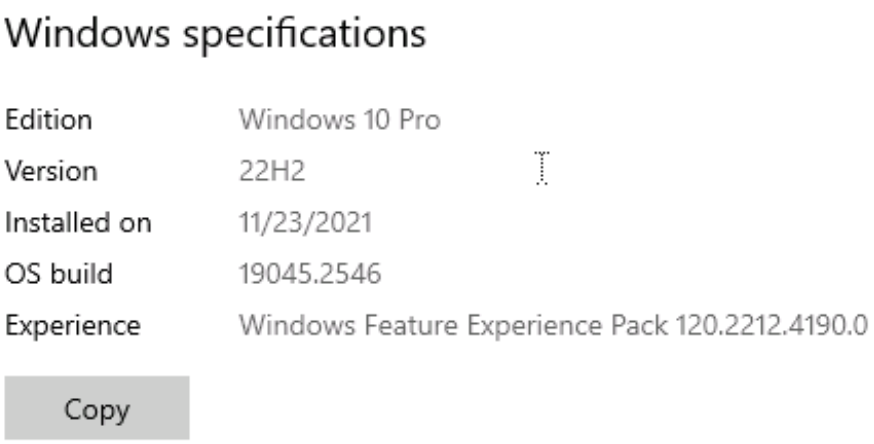
After:

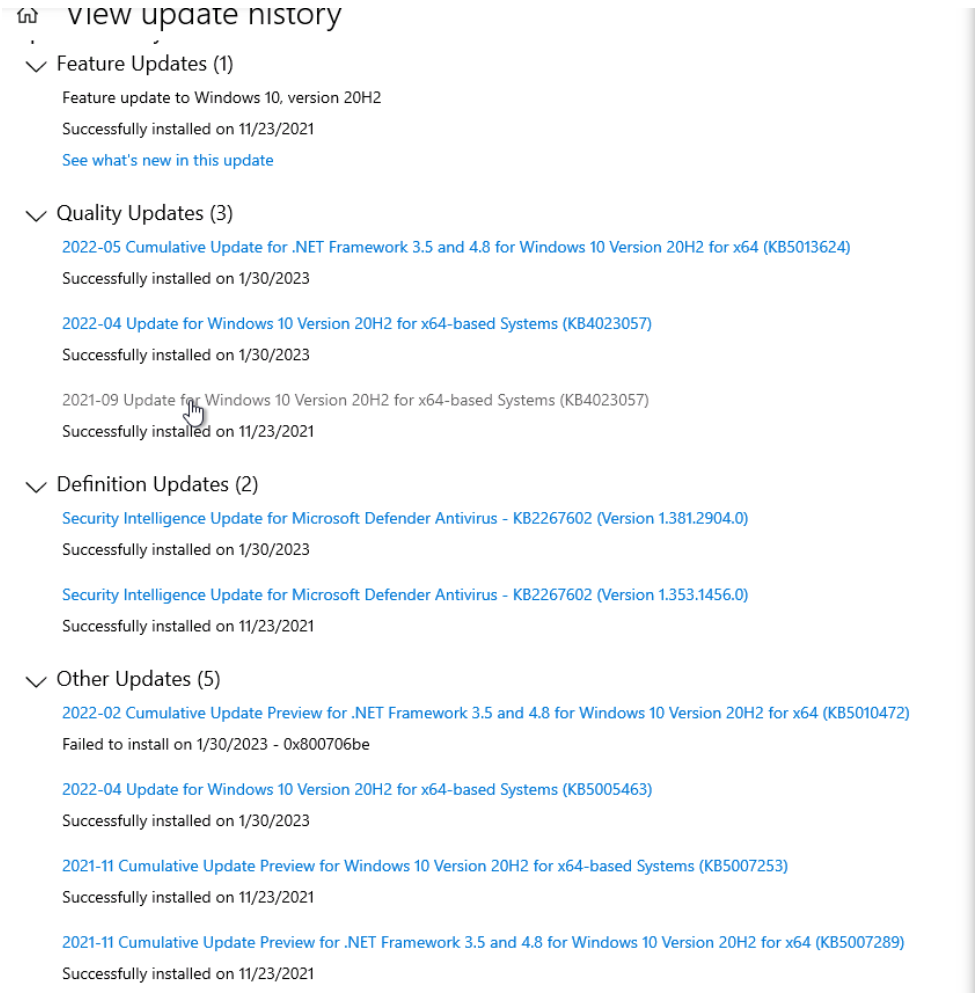
Control Panel>Settings>Update & Security >Windows Update > Click on download button under updates available section.

For automated updates:



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:*

- .NET Framework 3.5 and 4.8
- Windows Defender Antivirus

4. *Explain the steps you took to determine this information.*
   In Settings>Update & Security > Under Updates available, .NET Framework and Windows Defender antivirus were available updates > click on download button for those updates to download on local computer > Click on Install updates as soon as possible option (bellow)

5. *Explain the steps for updating each of these applications. Include screenshots as needed.*

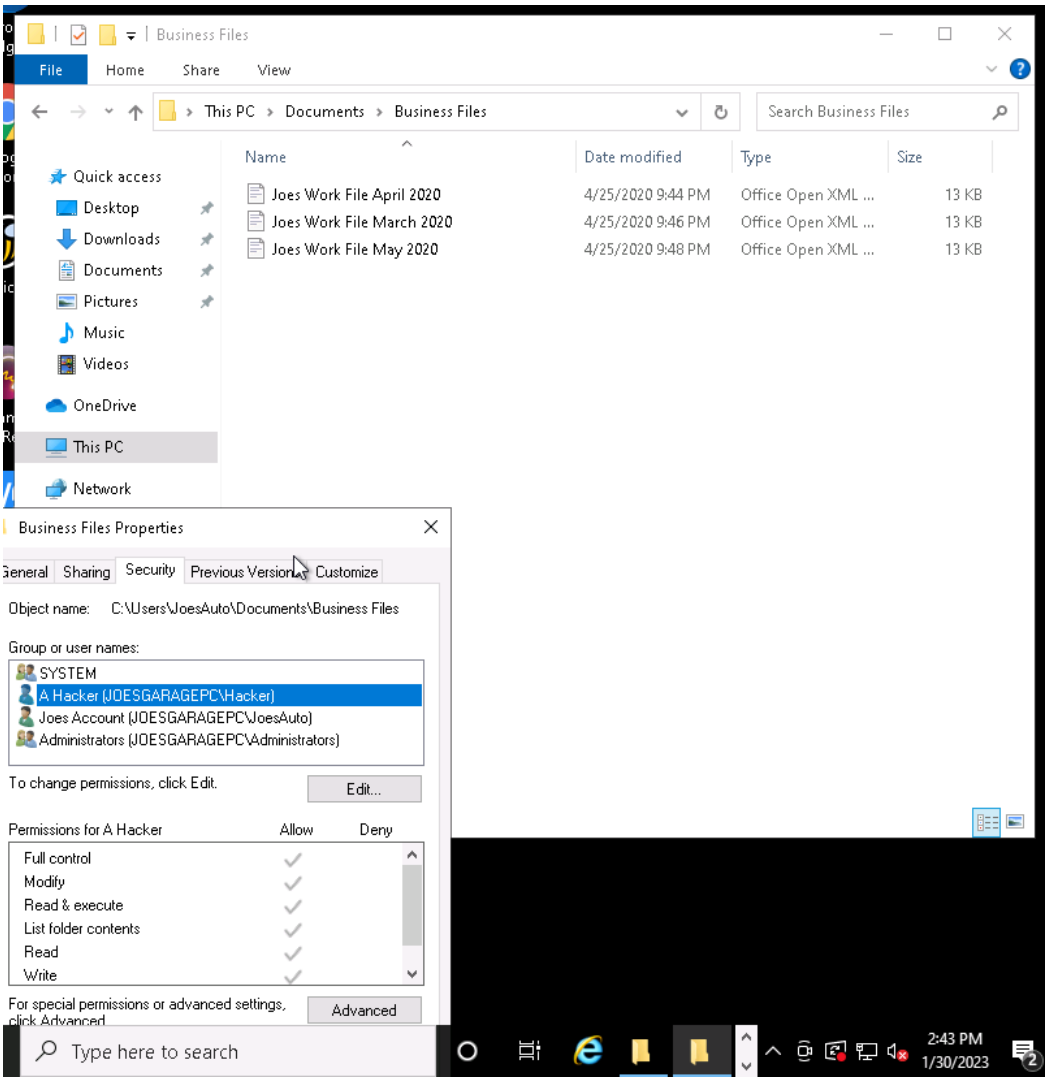
5. Securing Files and Folders

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

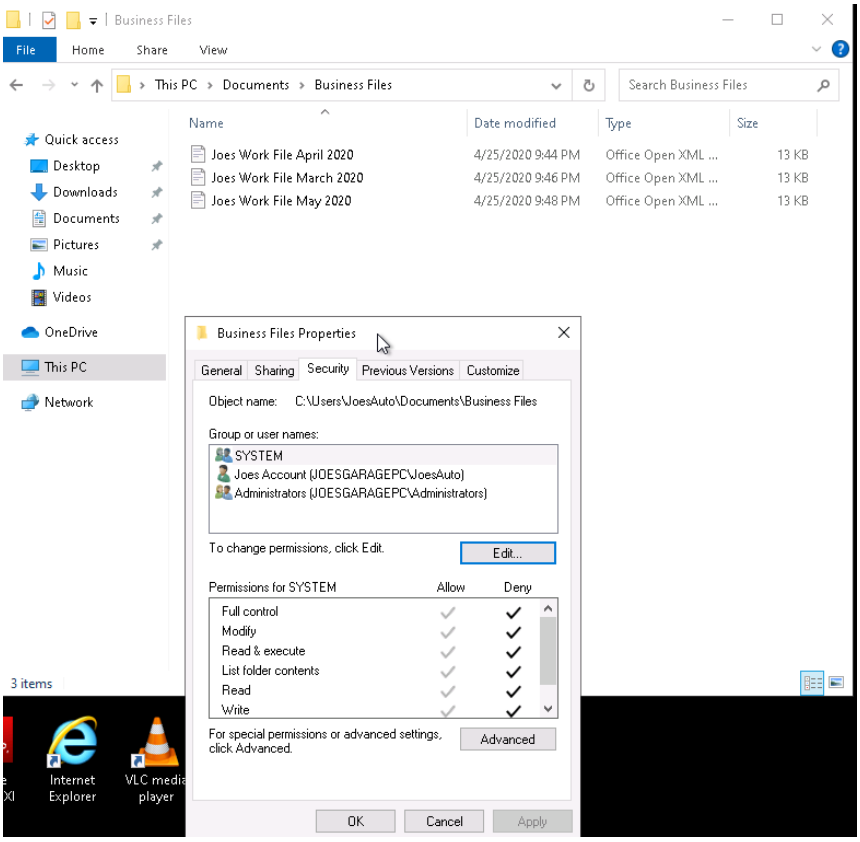
Joe suspects that other users on this computer beside him and Jane can see and change his business files. He wants you to check to make sure that only those two users have privileges to view or change the files.

Encrypting files and folders

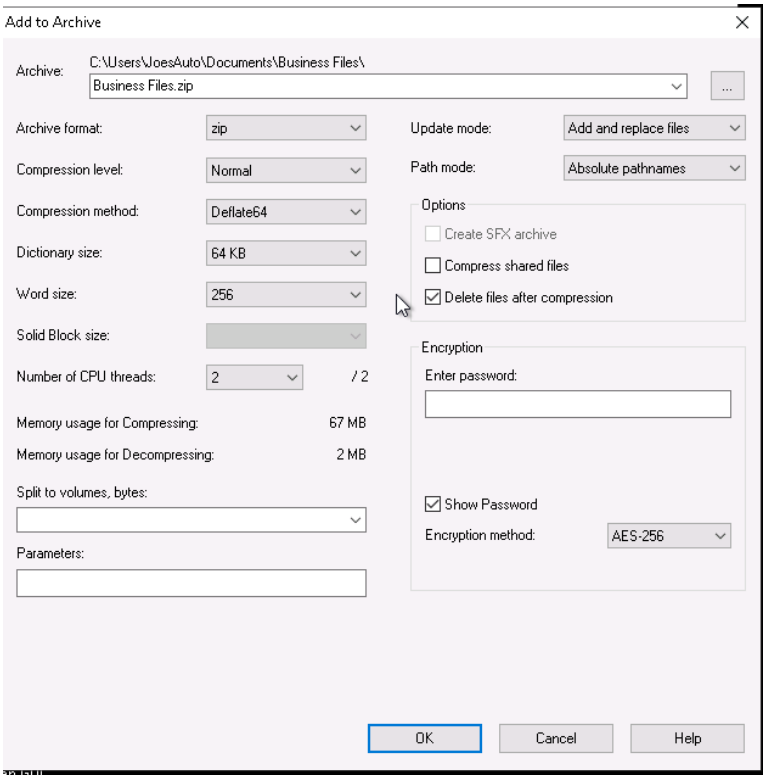
1. *Explain the process for checking this and changing any necessary settings on the file. Include screenshots showing that ONLY Joe and Jane have permissions to change Joes work files. [Hint: Right-click the folder and select Properties.]*

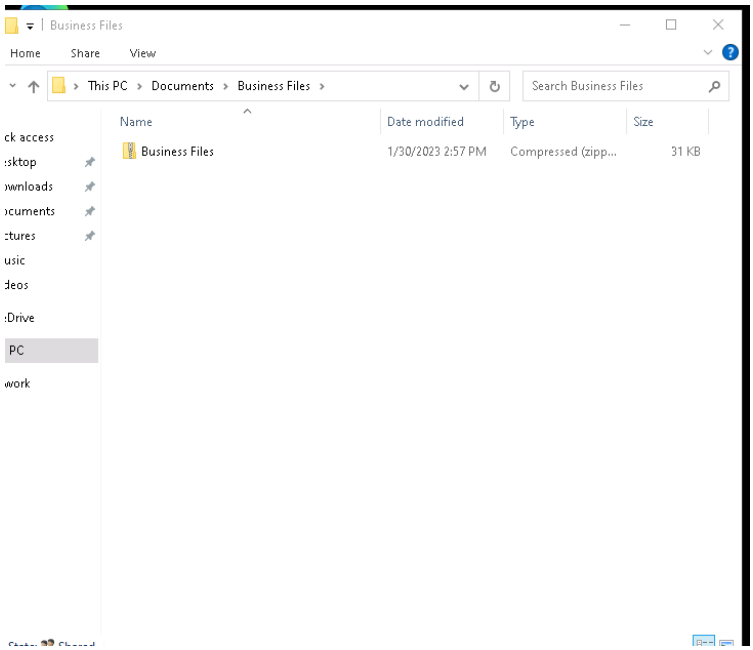

Business Files
File
Home
Share
View
This PC › Documents › Business Files
Search Business Files
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Joes Work File April 2020
4/25/2020 9:44 PM
Office Open XML ...
13 KB
Joes Work File March 2020
4/25/2020 9:46 PM
Office Open XML ...
13 KB
Joes Work File May 2020
4/25/2020 9:48 PM
Office Open XML ...
13 KB
Business Files Properties
General
Sharing
Security
Previous Versions
Customize
Object name: C:\Users\JoesAuto\Documents\Business Files
Group or user names:
SYSTEM
A Hacker (JOESGARAGEPC\Hacker)
Joes Account (JOESGARAGEPC\JoesAuto)
Administrators (JOESGARAGEPC\Administrators)
To change permissions, click Edit.
Edit...
Permissions for A Hacker
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
Type here to search
2:43 PM
1/30/2023

After:



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?*
   Protecting and Performing Timely Backups of Files and Documents

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

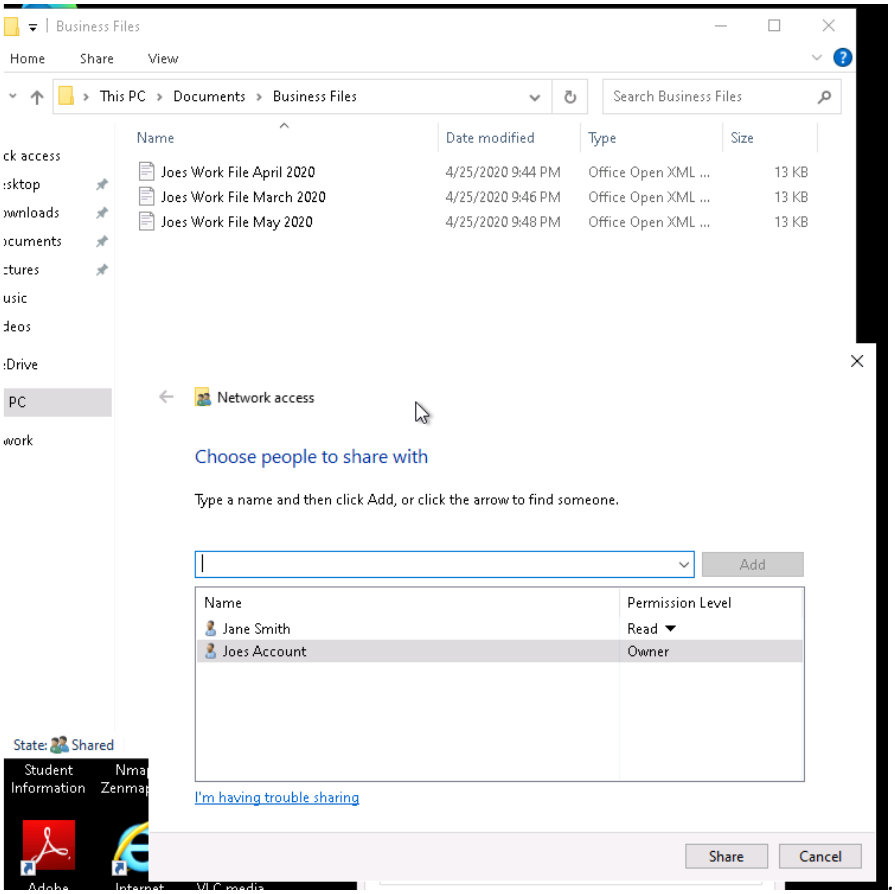
CIS Critical Security Control 3: Data Protection

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.

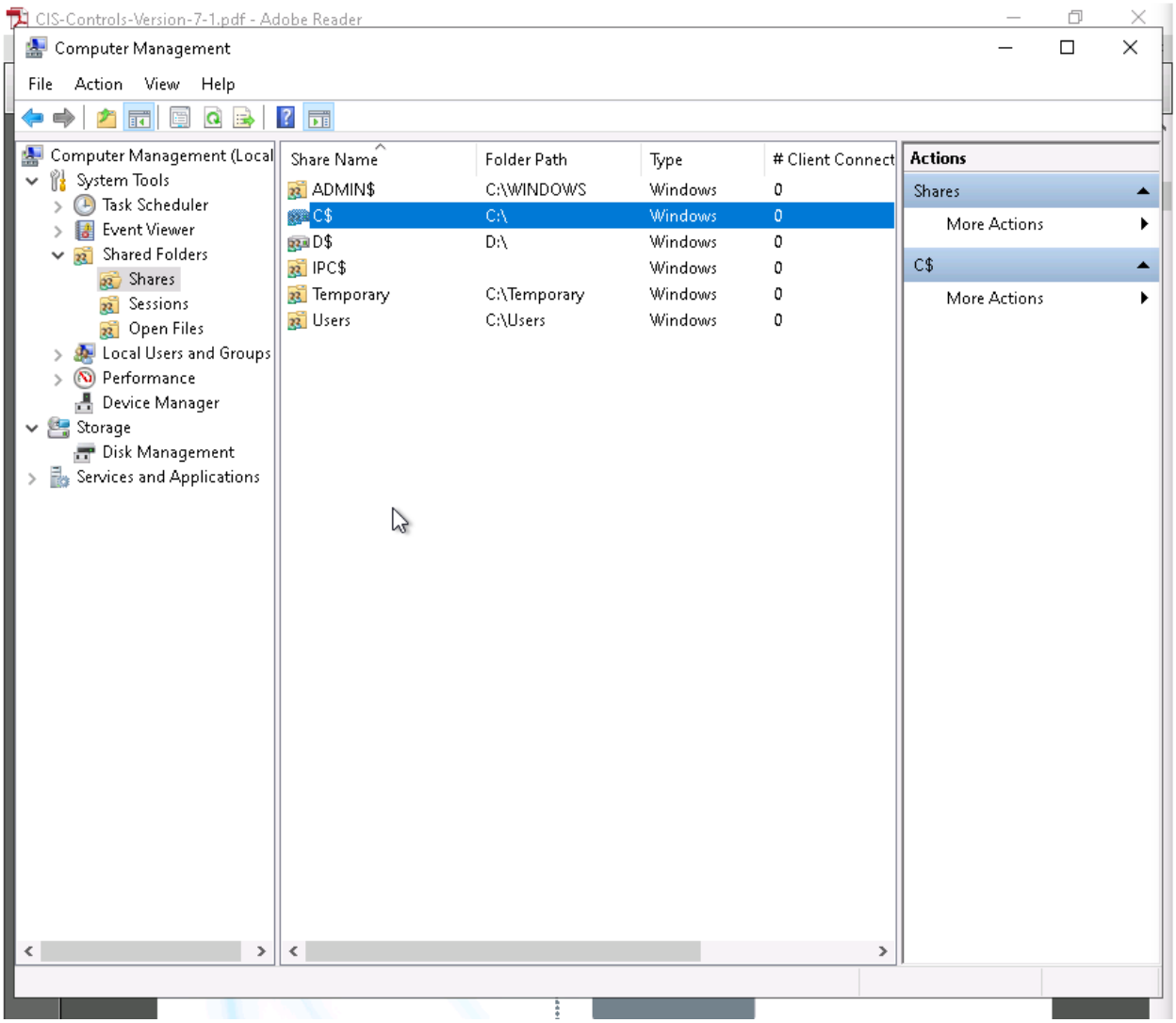
1. *Explain how you would do that and provide a screenshot showing how you can do it. Make sure it's only shared between Joe and Jane*

Right-click on the file/folder which you want to share. > Select Share > In the file sharing window select the Jane accounts and click on Share button.



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.*

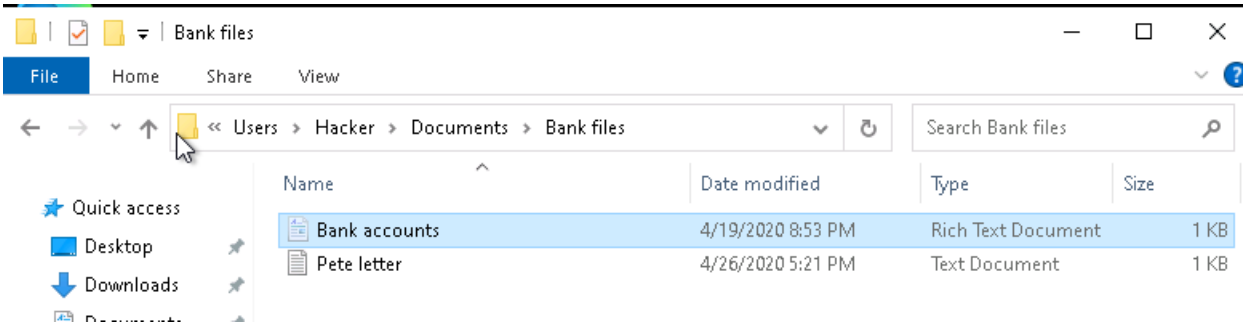
   Right-click or tap-and-hold the *Start* icon. In the menu that appears, choose *Computer Management*.



6. Basic Computer Forensics (Optional)

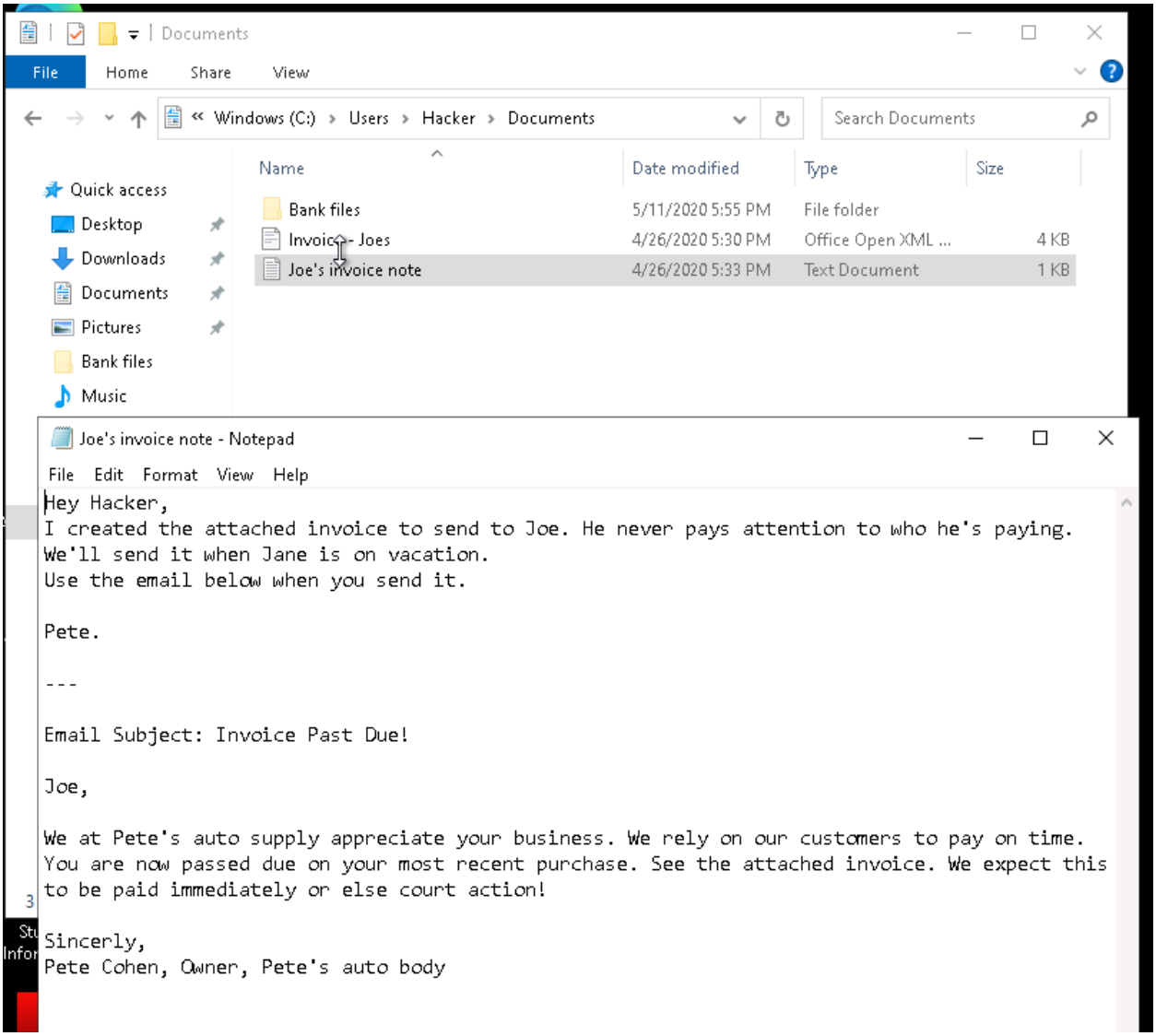
Joe has asked that you investigate his PC to see if there are any other files left behind by previous unwanted users that may show they wanted to harm Joe's business. Look through the unwanted users' folders and list suspicious files. General students should document three issues and advanced students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

- Bank account of Joes customers. That means that the hacker has access to Pete customers money

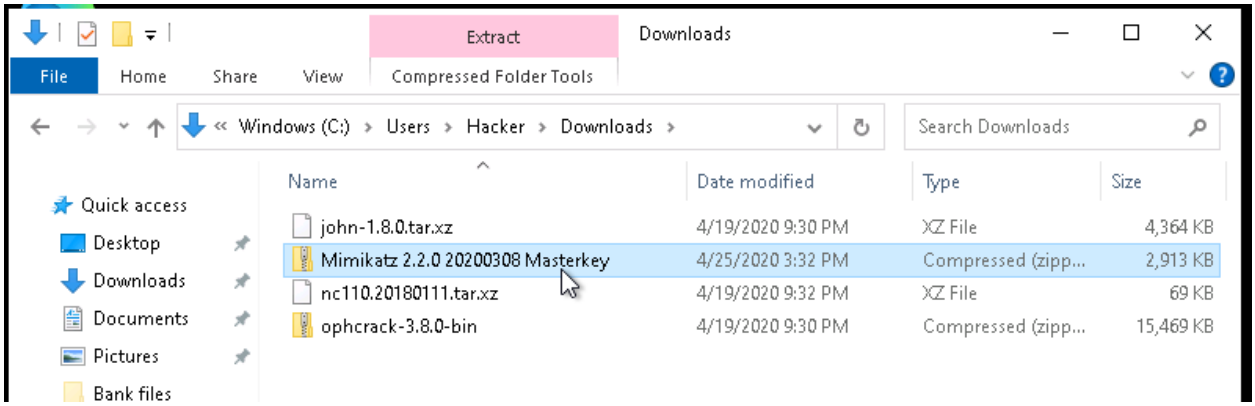


- Joes invoice and some social engineering would do some financial damage.

-



- Software to decode passwords > Hacker gain access to other user's accounts, as well as at their email/ website's accounts, bank accounts, etc.



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.