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: Shrividya Ranjani Kaliyur NarayanaPrasad

Date of completion: 8/28/2020

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.

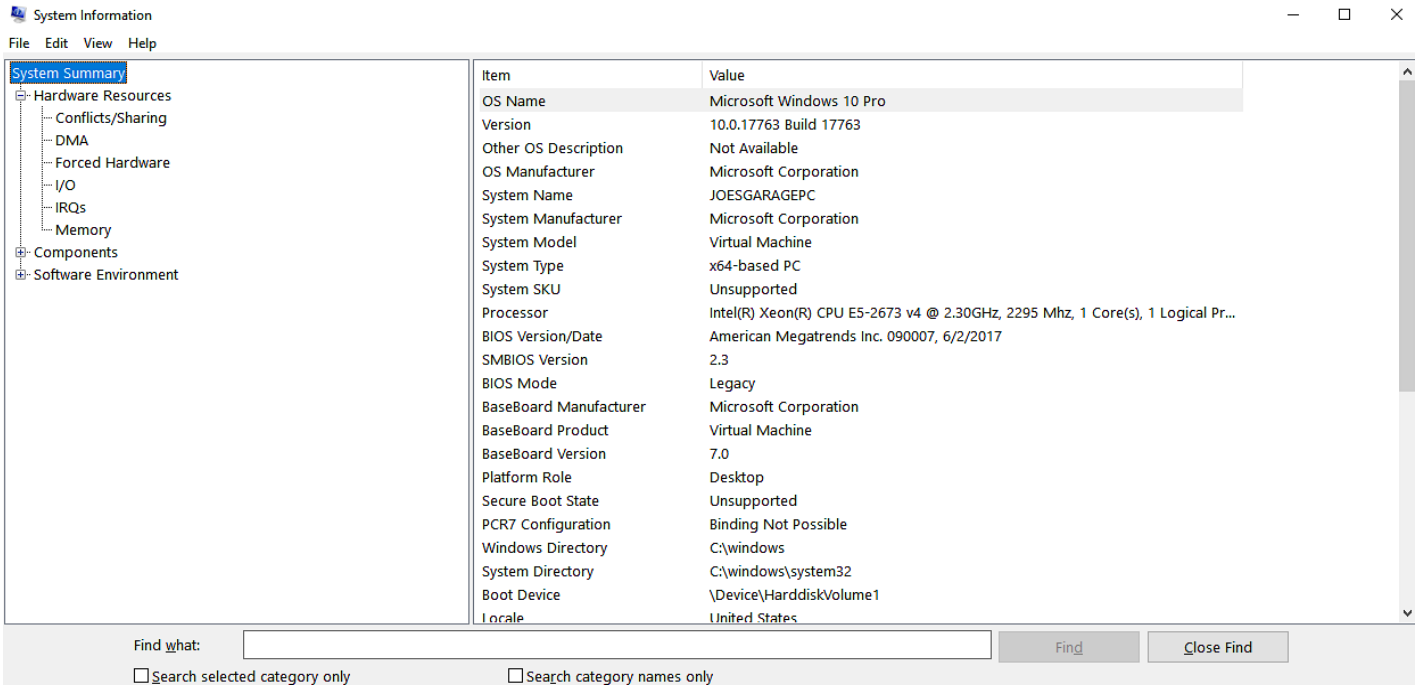
Hardware

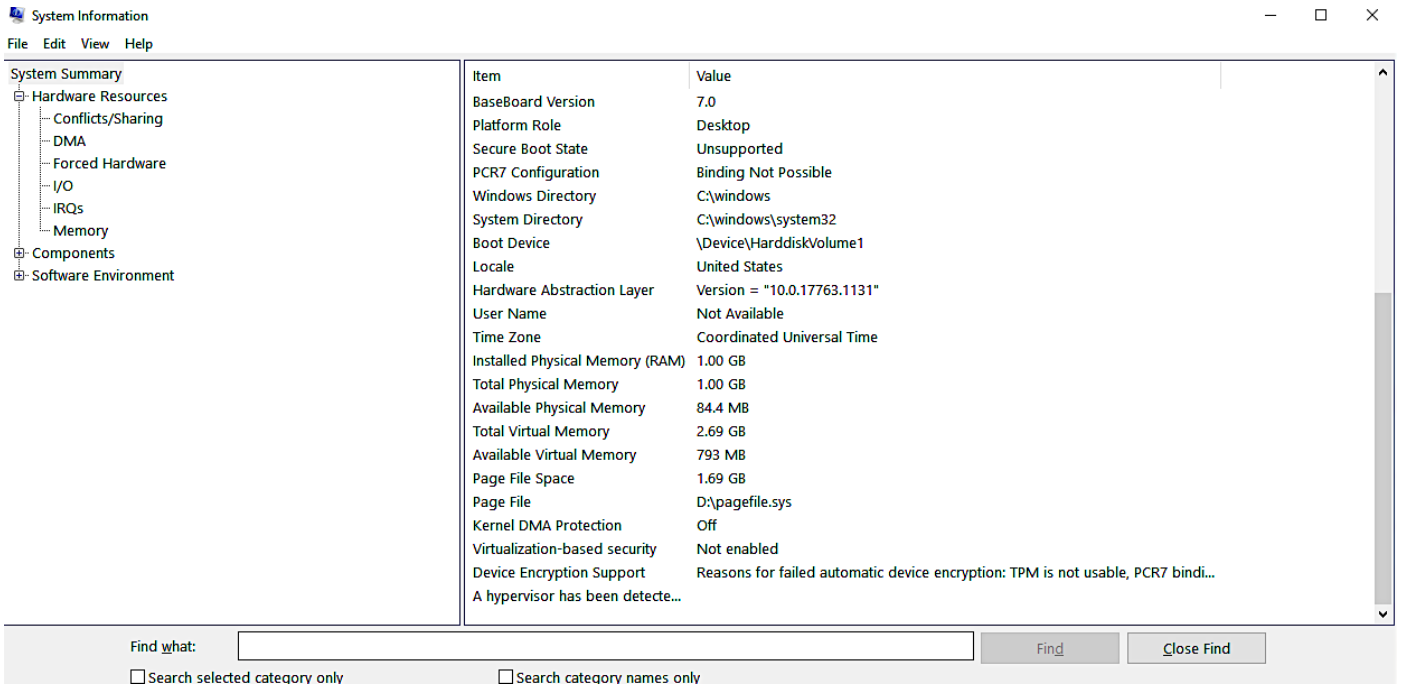
1. *Fill in the following table with system information for Joe's PC.*

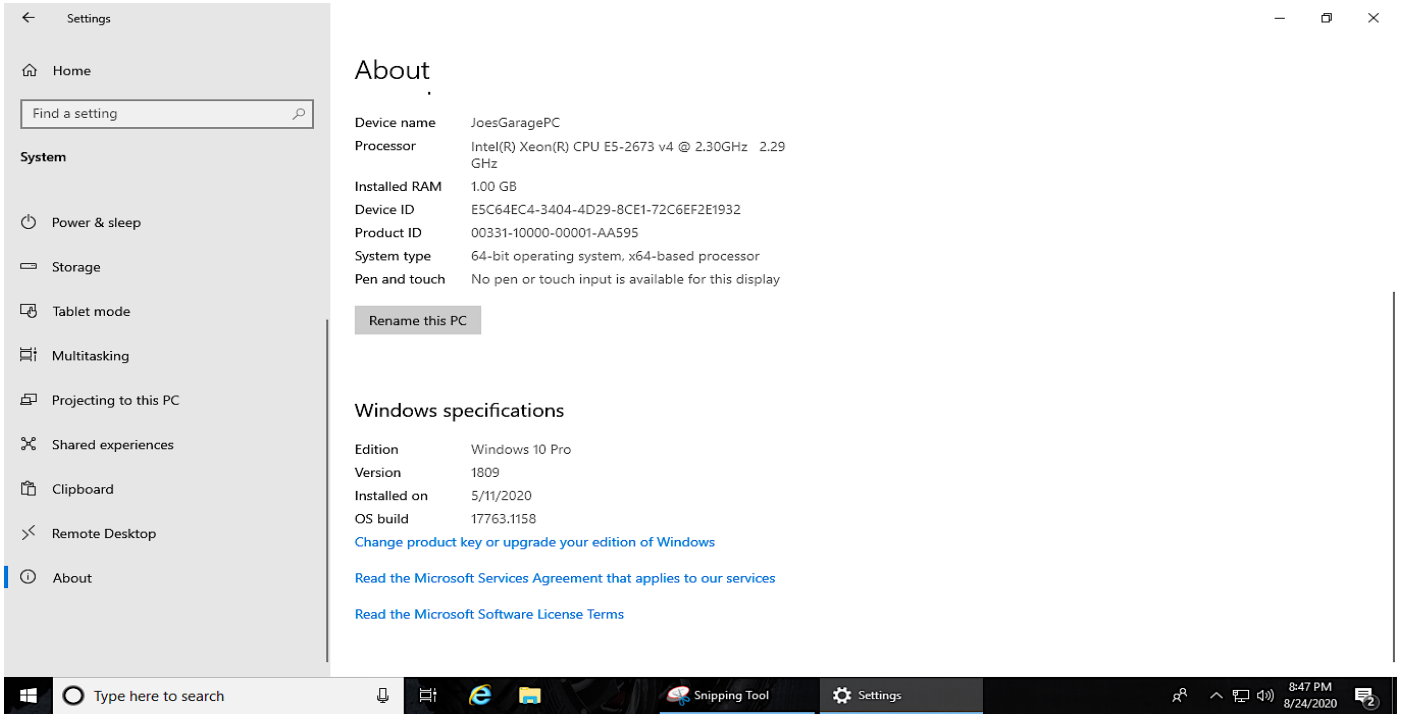
Device Name	**JoesGaragePC**
Processor	**Intel® Xeon® CPU E5-2673 v4 @ 2.30GHz, 2295 MHz, 1 core(s), 1 Logical Processor(s)**
Install RAM	**1.00 GB**
System Type	**X64-based PC**
Windows Edition	**Microsoft Windows 10 Pro**
Version	**10.0.17763**
Installed on	**5/11/2020**
OS build	**17763.1158**

2. *Explain how you found this information:*
   Click the search button and type "system information". Once inside the system information then click on "System Summary" which provides all the information about the PC. In order to find the installation date, go to settings and click "about" to find the installation date.

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




System Information
File Edit View Help
System Summary
Hardware Resources
Conflicts/Sharing
DMA
Forced Hardware
I/O
IRQs
Memory
Components
Software Environment
Item
Value
BaseBoard Version
7.0
Platform Role
Desktop
Secure Boot State
Unsupported
PCR7 Configuration
Binding Not Possible
Windows Directory
C:\windows
System Directory
C:\windows\system32
Boot Device
\Device\HarddiskVolume1
Locale
United States
Hardware Abstraction Layer
Version = "10.0.17763.1131"
User Name
Not Available
Time Zone
Coordinated Universal Time
Installed Physical Memory (RAM)
1.00 GB
Total Physical Memory
1.00 GB
Available Physical Memory
84.4 MB
Total Virtual Memory
2.69 GB
Available Virtual Memory
793 MB
Page File Space
1.69 GB
Page File
D:\pagefile.sys
Kernel DMA Protection
Off
Virtualization-based security
Not enabled
Device Encryption Support
Reasons for failed automatic device encryption: TPM is not usable, PCR7 bindi...
A hypervisor has been detecte...
Find what:
Find
Close Find
Search selected category only
Search category names only


Settings
Home
Find a setting
System
Power & sleep
Storage
Tablet mode
Multitasking
Projecting to this PC
Shared experiences
Clipboard
Remote Desktop
About
About
Device name
JoesGaragePC
Processor
Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz 2.29 GHz
Installed RAM
1.00 GB
Device ID
E5C64EC4-3404-4D29-8CE1-72C6EF2E1932
Product ID
00331-10000-00001-AA595
System type
64-bit operating system, x64-based processor
Pen and touch
No pen or touch input is available for this display
Rename this PC
Windows specifications
Edition
Windows 10 Pro
Version
1809
Installed on
5/11/2020
OS build
17763.1158
Change product key or upgrade your edition of Windows
Read the Microsoft Services Agreement that applies to our services
Read the Microsoft Software License Terms
Type here to search
Snipping Tool
Settings
8:47 PM
8/24/2020

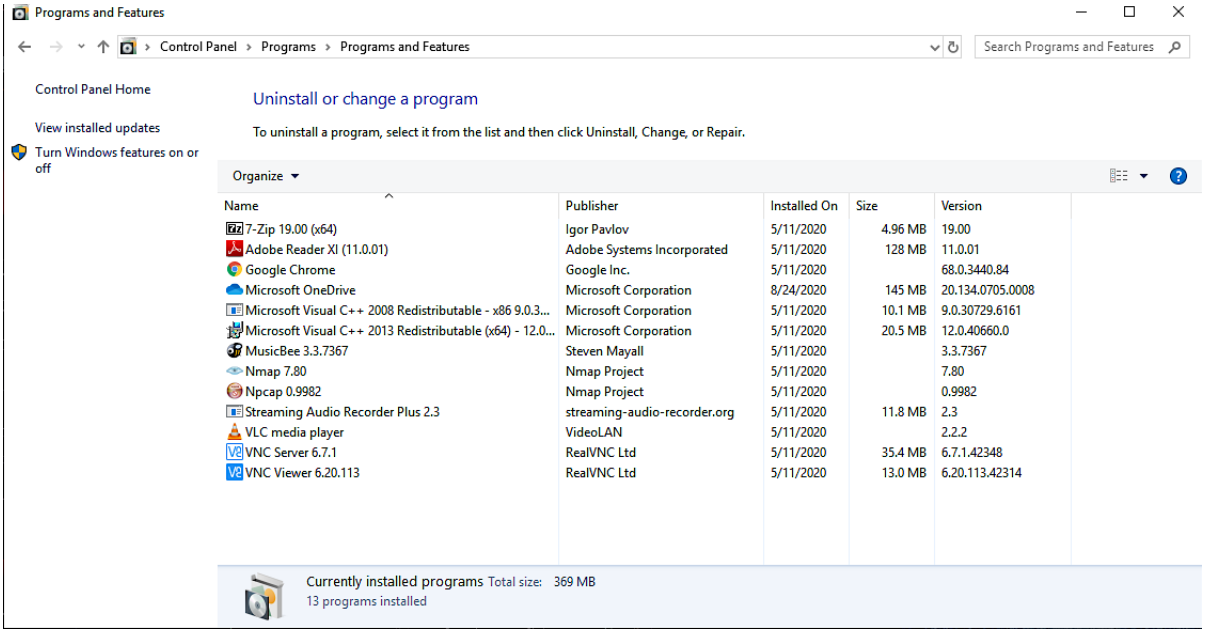
Software

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:*

- **Nmap 7.80**
- **MusicBee 3.3.7367**
- **Npcap 0.9982**
- **Google Chrome**
- **7-Zip 19.00 (x64)**

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



Click the search button on the desktop and search for "control panel". Once inside control panel click on "Programs". Inside Programs click "Programs and Features" which shows all the applications that are installed on 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 software assets***

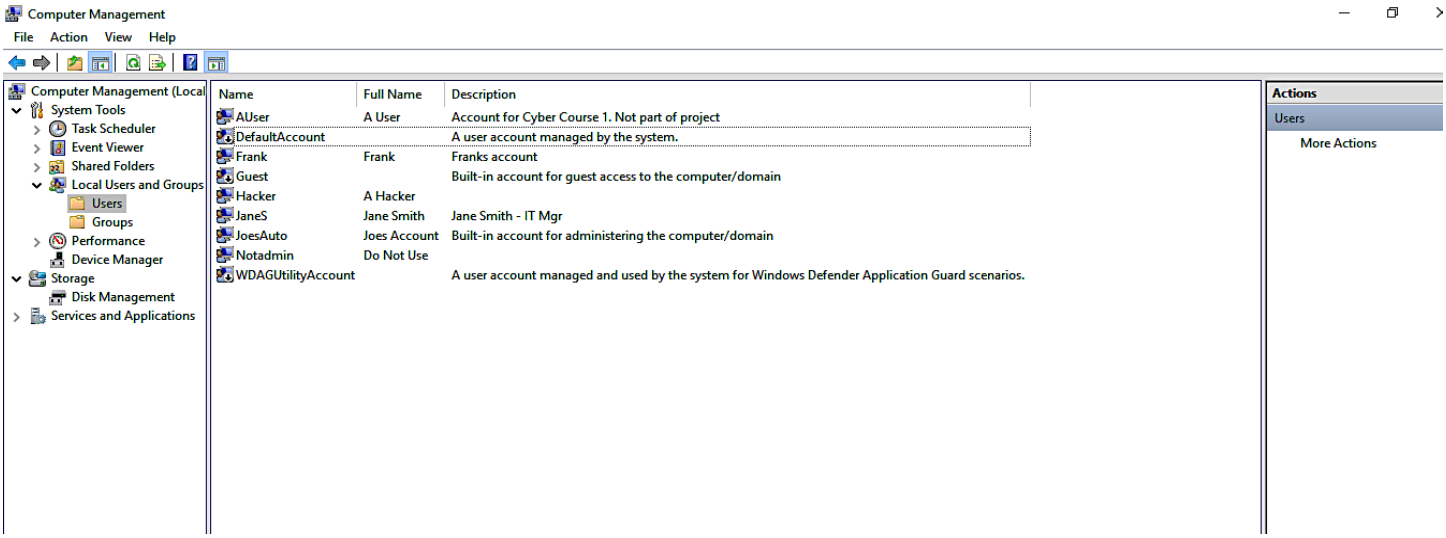
Accounts

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
AUser	A User	Standard
DefaultAccount		
Frank	Frank	Standard
Guest		
Hacker	A Hacker	Administrator
JaneS	Jane Smith	Administrator
JoesAuto	Joes Account	Administrator
Notadmin	Do Not Use	Standard
WDAGUtilityAccount		

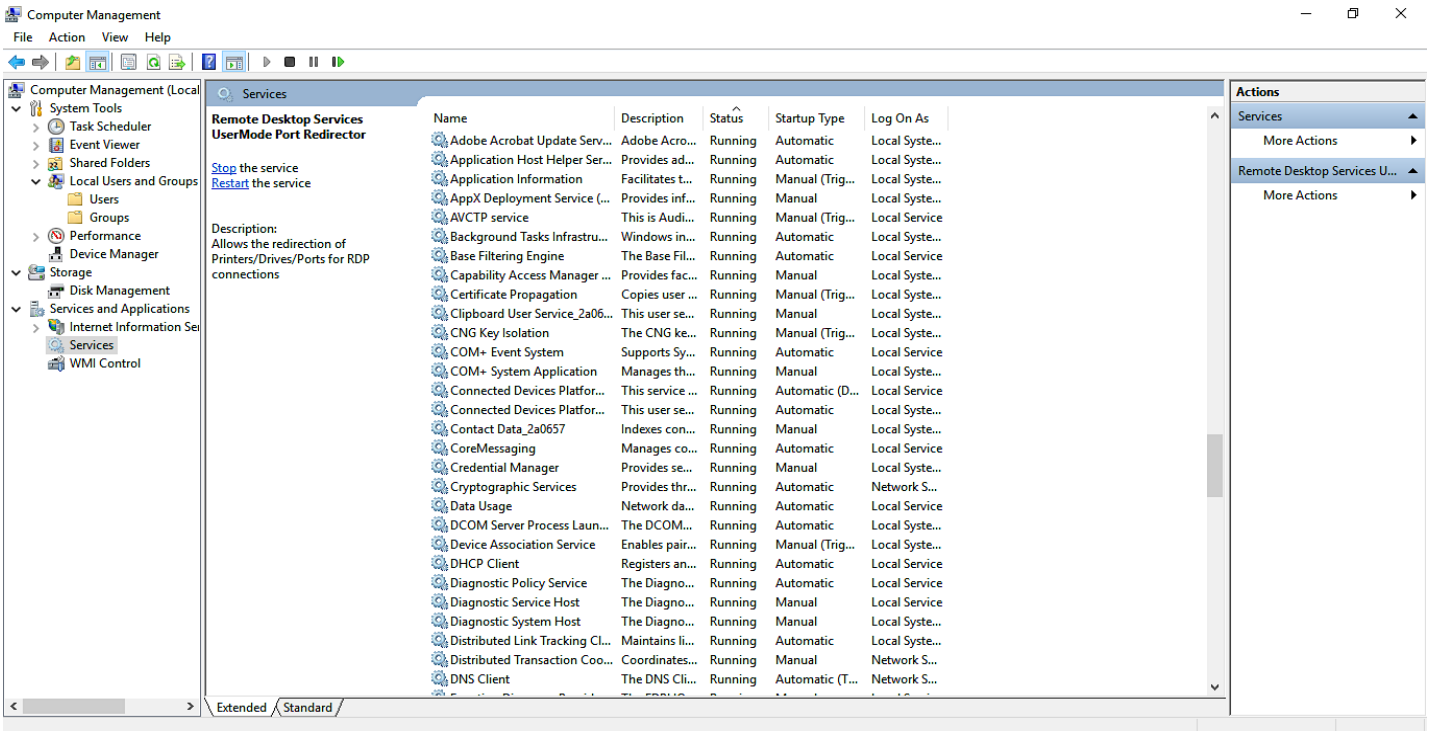
2. *Provide a screenshot of the Local Users.*

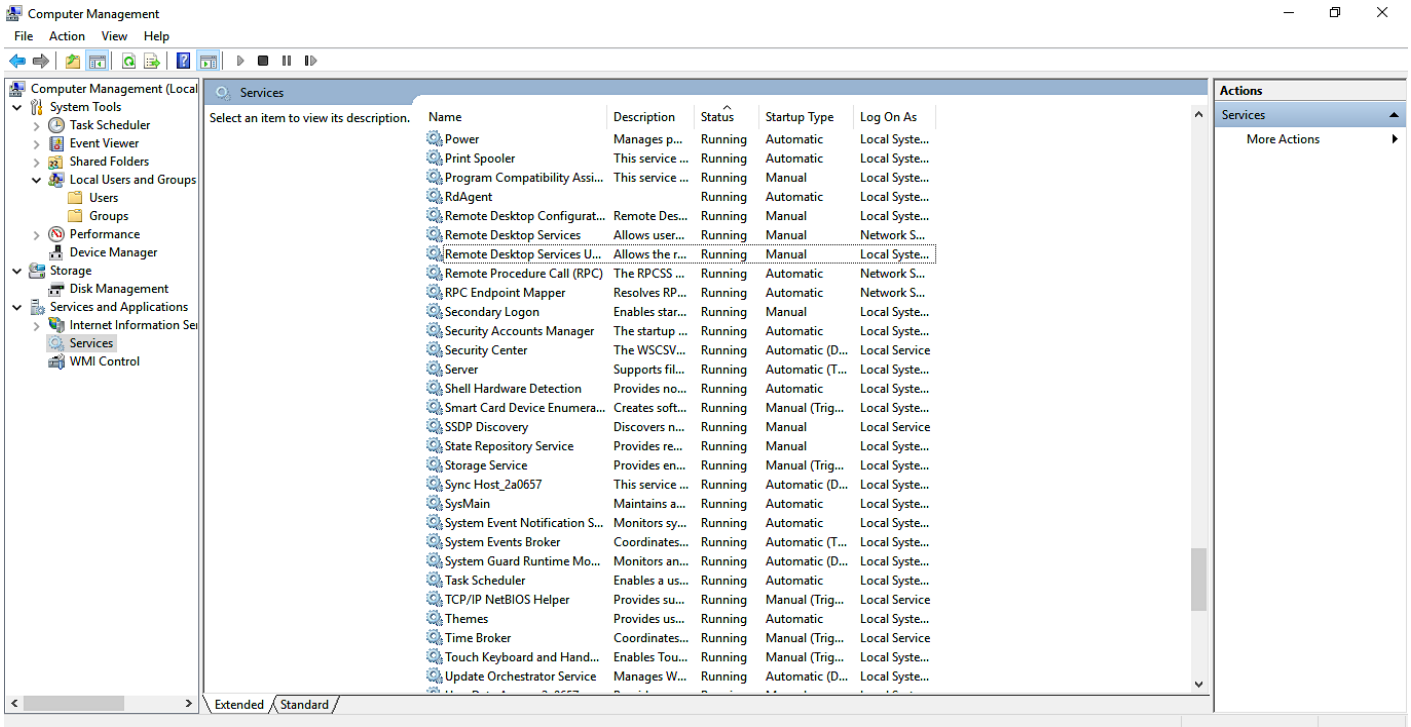


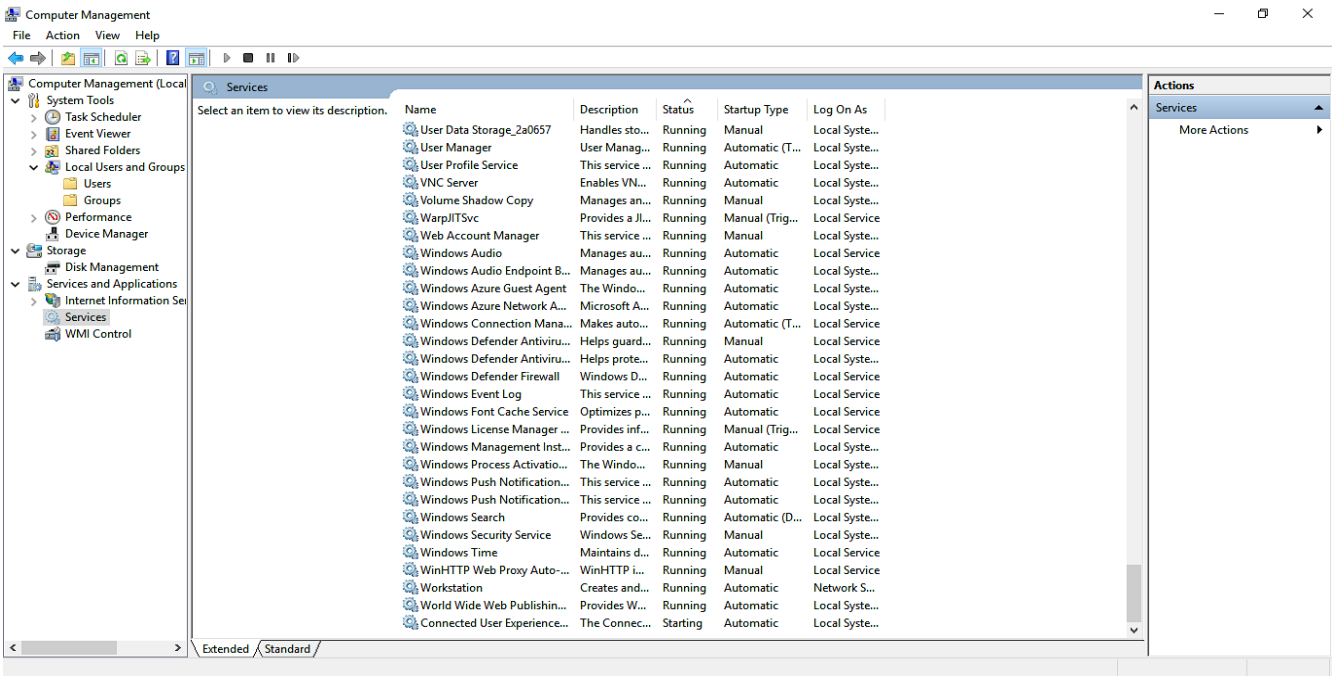
Services

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	**Off**
Firewall product and status – Public network	**On**
Virus protection product and status	**On**
Internet Security messages	**Currently not monitored**
Network firewall messages	**Currently not monitored**
Virus protection messages	**Currently not monitored**
User Account Control Setting	**Currently not monitored**

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.]

- **Unsecure configuration of network devices**
- **No proper access controls**
- **No proper monitoring**

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 to use NIST for setting the security policies. In order to protect something, they must know what can lead to the destruction. Once the vulnerabilities are known then policies and protection are set and then the business or device can be kept safe. And this process is neatly specified by NIST which is profitable to the ones who use it.

2. *What industry baseline do you recommend to Joe?*
   [Hint: Look in the documents folder] **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?
   Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
   Malware Defenses

Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Boundary Defense

System and Security

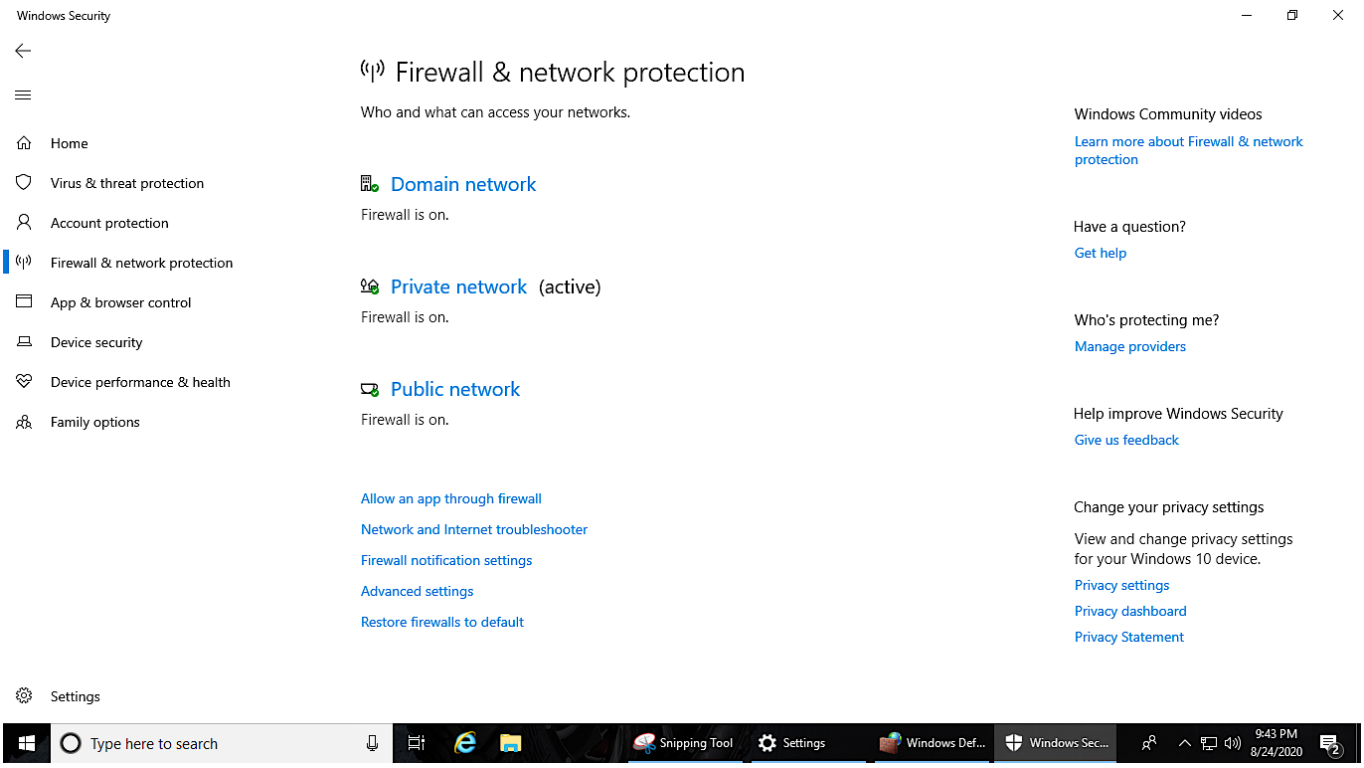
At this point, you need to enable security services for this PC. Pick at least 3 of the following 5 areas to secure in order to satisfactorily meeting the project requirements:

- 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.*
   Click the search button on the desktop. Type "Windows Security". Click "Firewall and network protection" then click on switch on the different types of firewalls.
2. *Include screenshots showing the firewall is turned on*



3. *What protection does this provide?*

   Prevents unauthorized access to the network, prevents unauthorized internet users from accessing private networks connected to 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.*
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:*

-
-

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

App & Browser Control

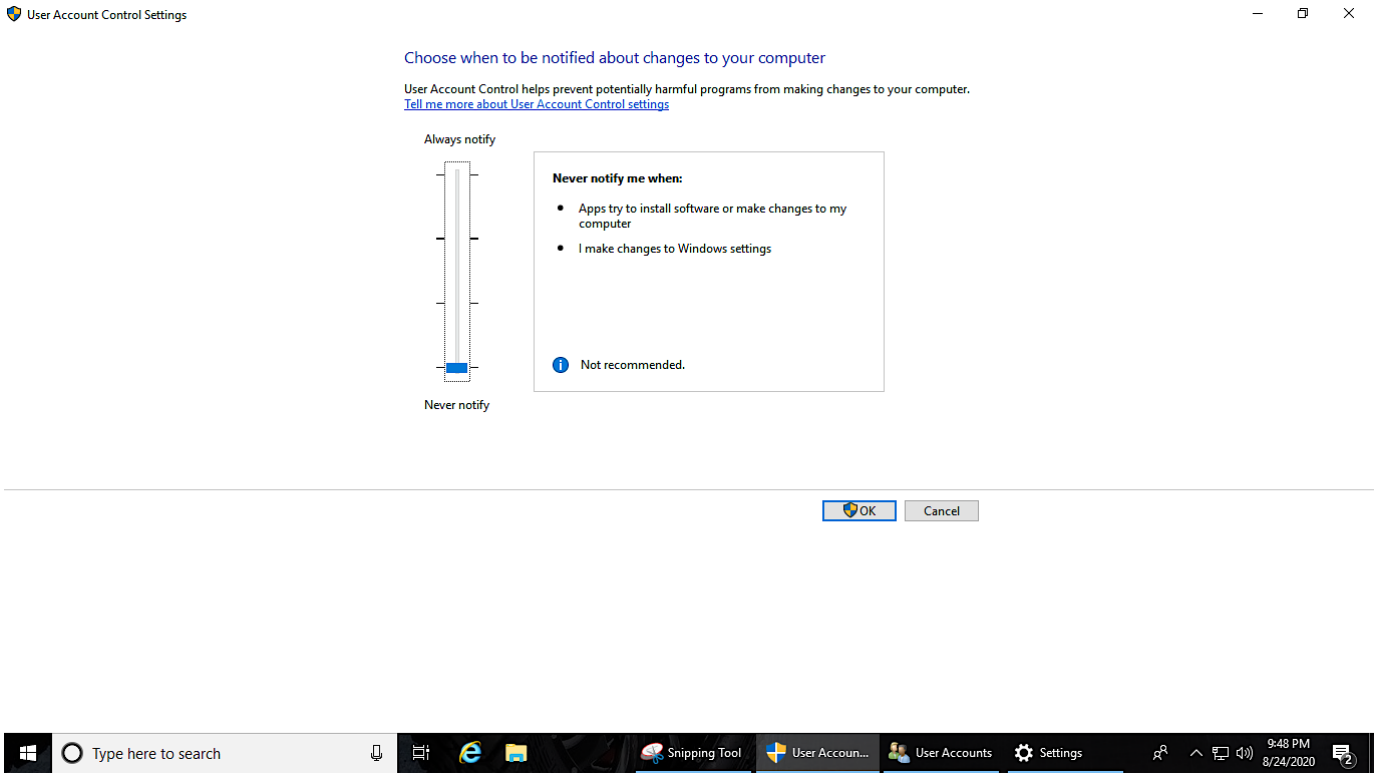
The App protection within Windows Defender helps to protect your device by checking for unrecognized apps and files and from malicious sites and downloads. Review the settings found within the *Account protection window, and App & browser control windows* found on the *Windows Defender Security page*.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

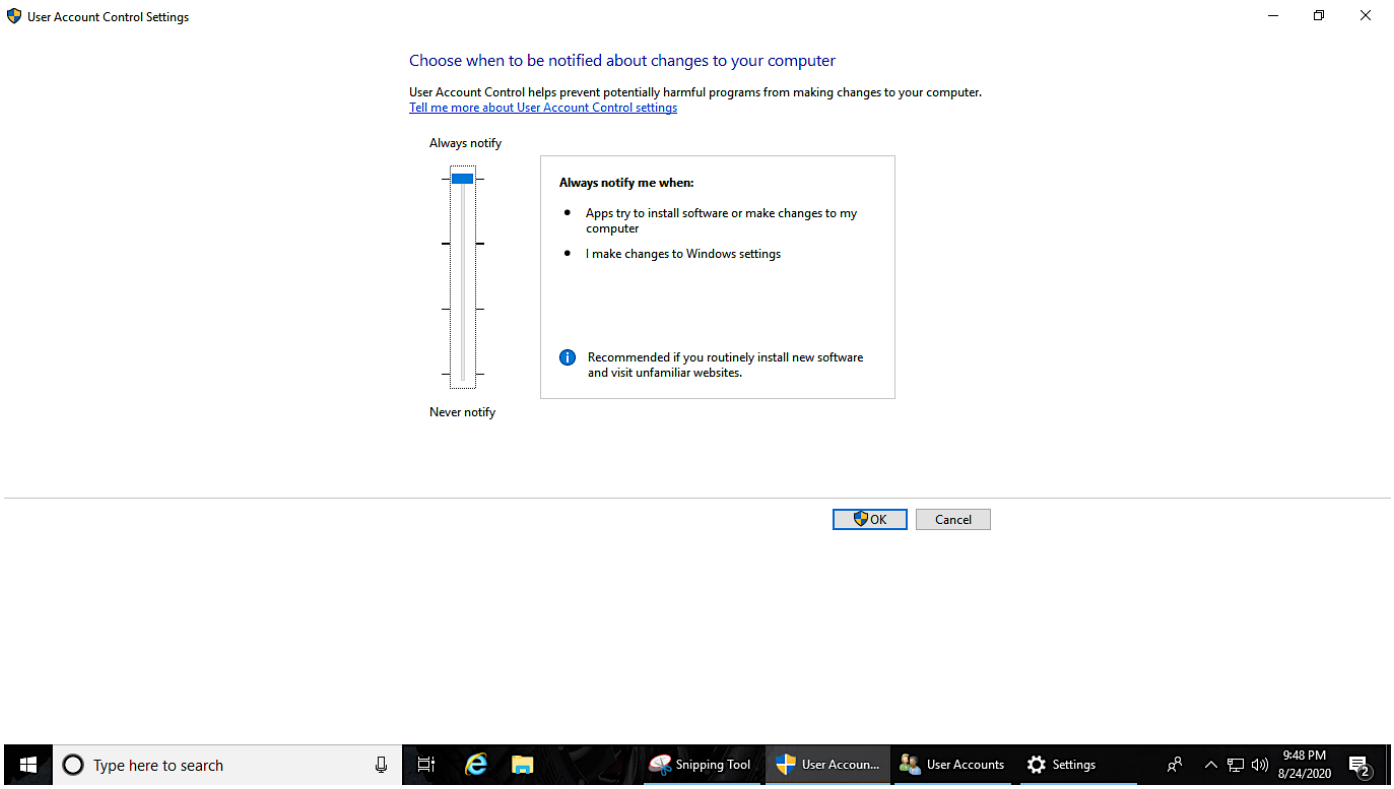
User Account Control Settings

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.
   The current UAC setting on Joe's computer is set to never notify me when apps install or make changes to the computer or when I make changes to the settings.



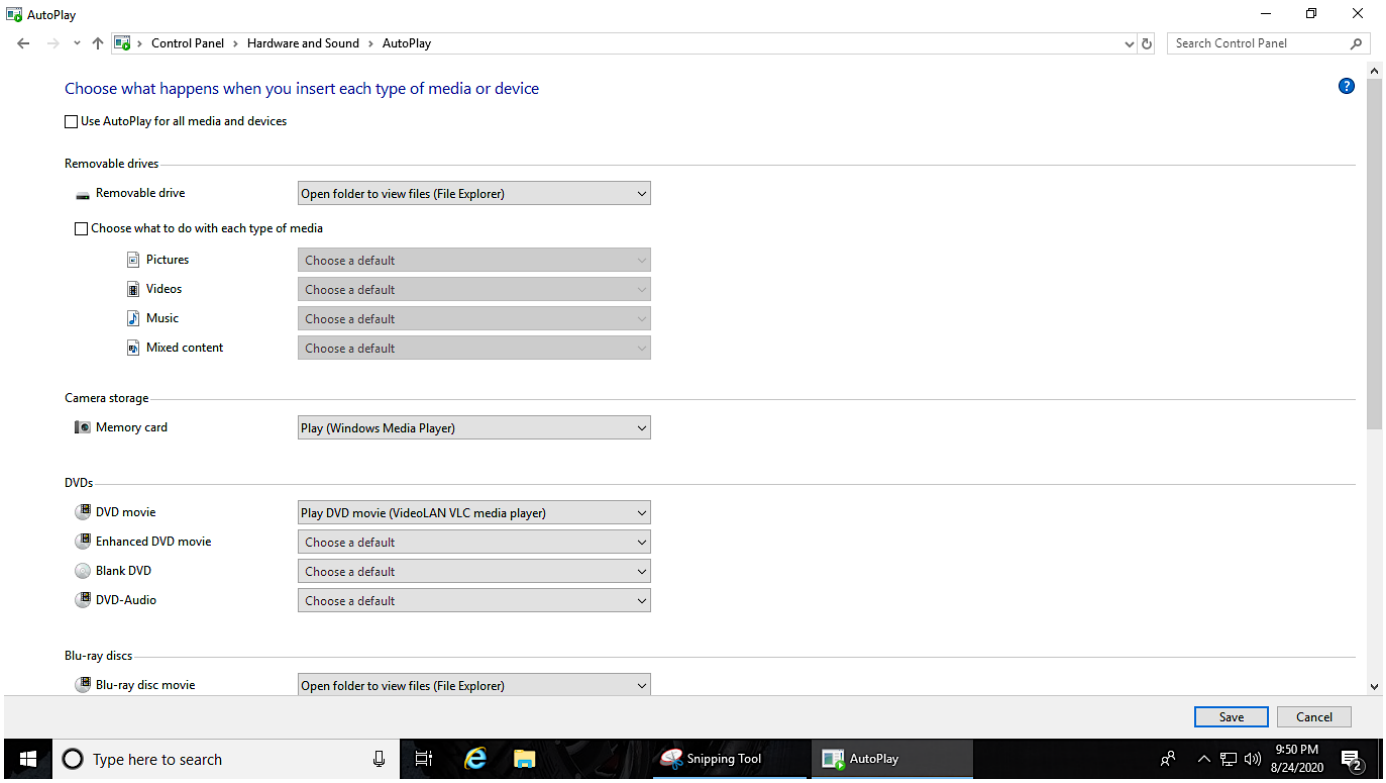
2. *What should it be set to? Include a screenshot of the new setting.*



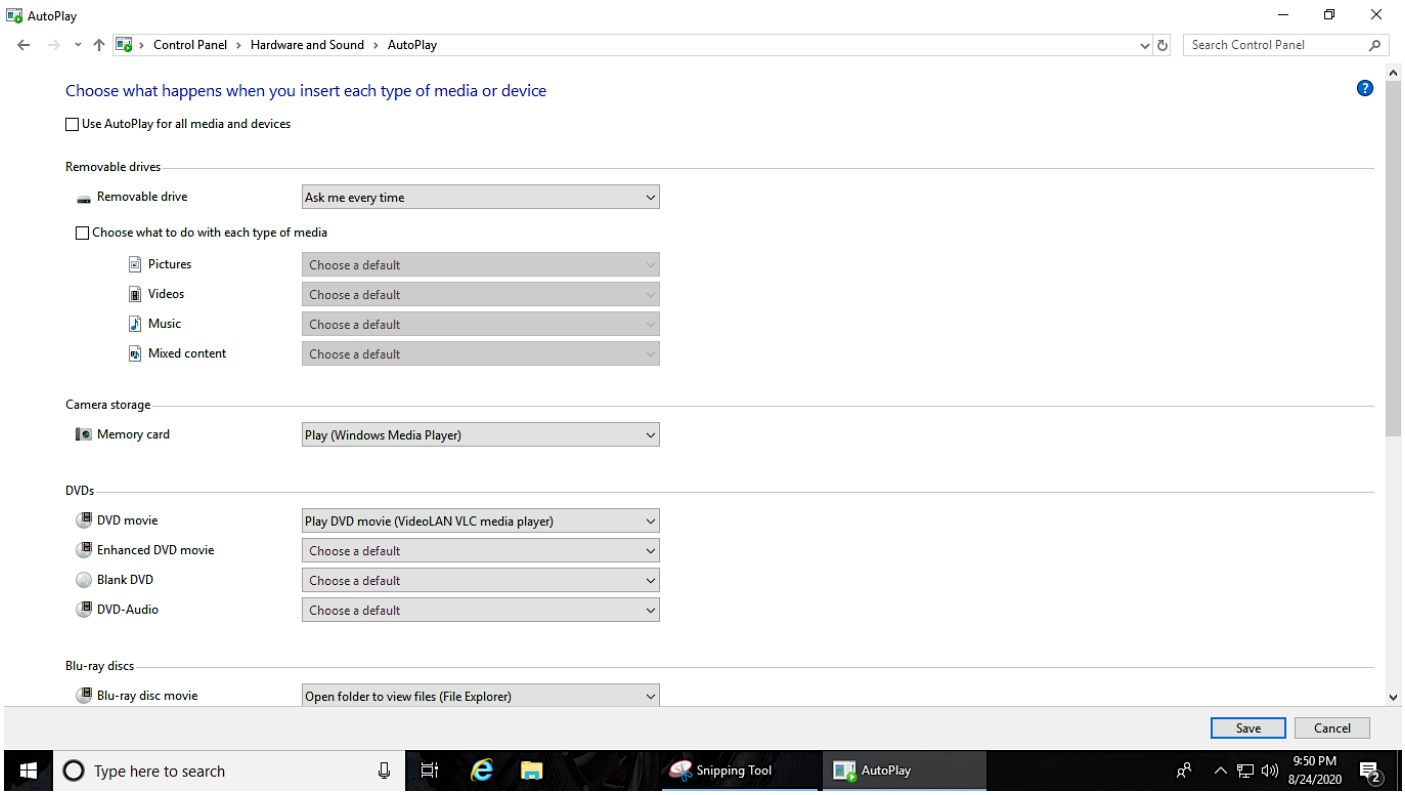
Securing Removable Media

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

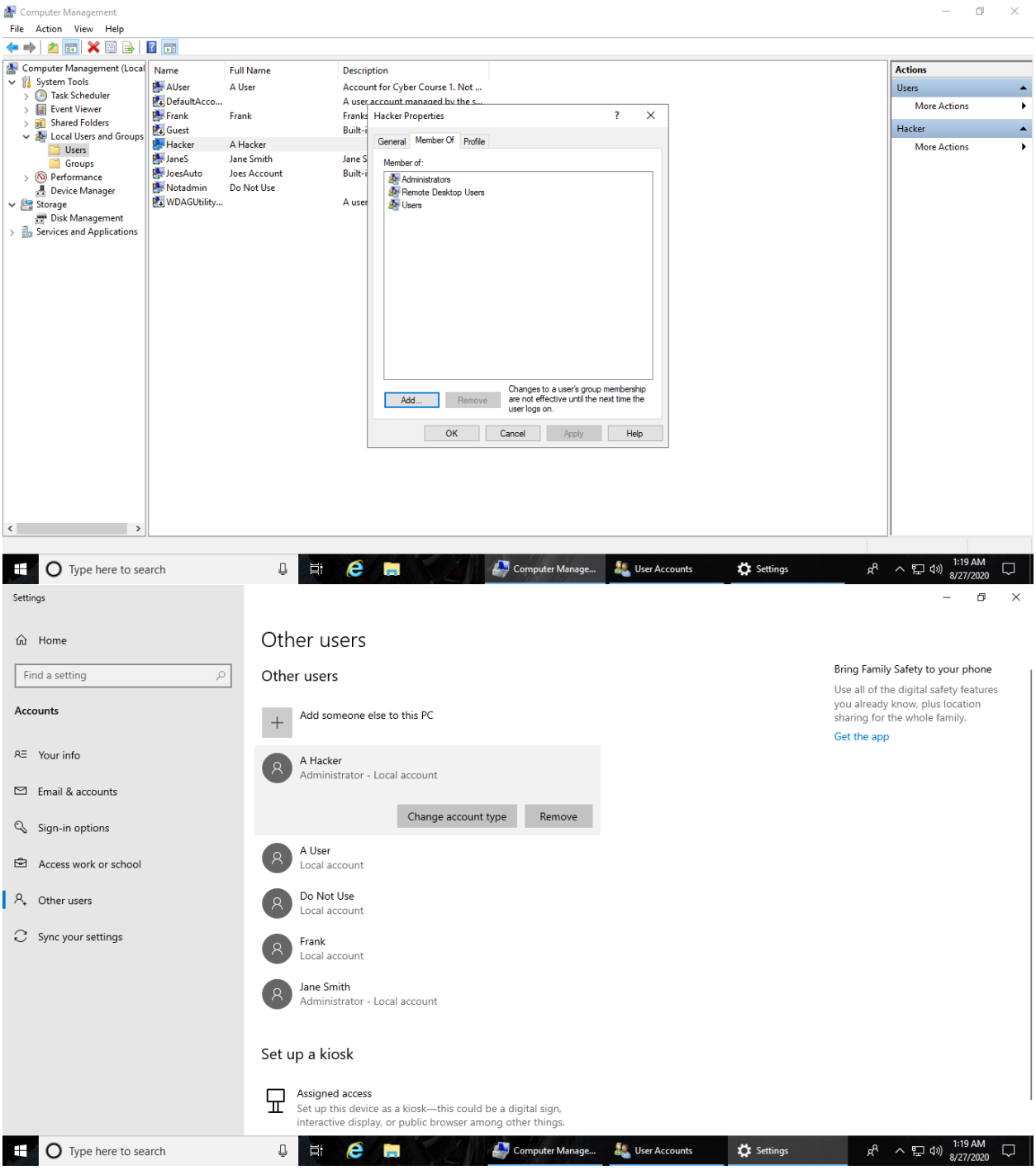
1. *What user accounts should not be there?*
   Frank, Hacker
2. *Bonus questions: What is Hacker's password?*

3. *Explain the steps you take to disable or remove unwanted accounts.*
   Click the search button on the desktop and type "Control Panel"
   Then click "User Accounts" and click "Make changes to my account in PC settings"
   Click "Other users"
   And select the unwanted account and click remove

4. *Why is it important to disable or remove unneeded accounts from a PC or application? Include potential vulnerabilities and risks.*
   It is necessary to delete unwanted accounts on PC because it removes the risk of unauthorized user to get access to one of the unused accounts to fulfil their goals.
   Potential vulnerabilities:
   Unauthorized access
   Risk of data being 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
6. Explain how you determined this. Provide screenshots as needed.
   According to JoesAuto access rule only JoesAuto and AUser must have the admin privileges. But when we go to settings and looking at the user accounts or by looking at the computer management -> Users; A Hacker also has admin 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.

- **Misuse of authority**
- **Users intentionally or unintentionally installing malicious software**
- **When multiple users have admin access then one user can access data of another user**

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

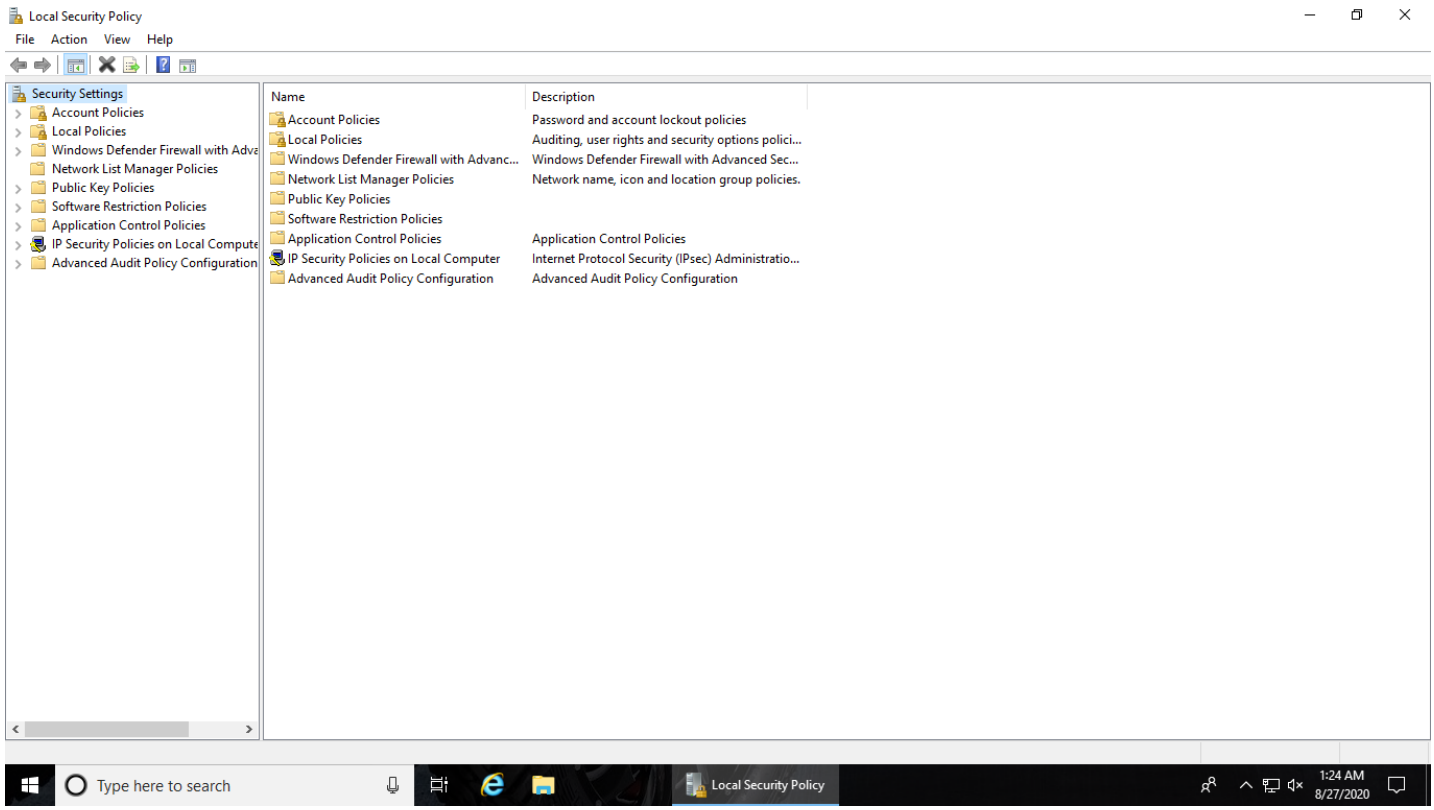
8. *Explain the process for doing this. Include screenshots to show your work.*
   Click the search button on the desktop and type "Control Panel"
   Click on "User Accounts"
   Then select "Make changes to my account in PC settings" and select "Other users"
   Click on "Select the account whose privileges must be changed "
   Click on "change account type "
   Then click "Select Standard account which gives only local privileges 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 Administrative 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.]

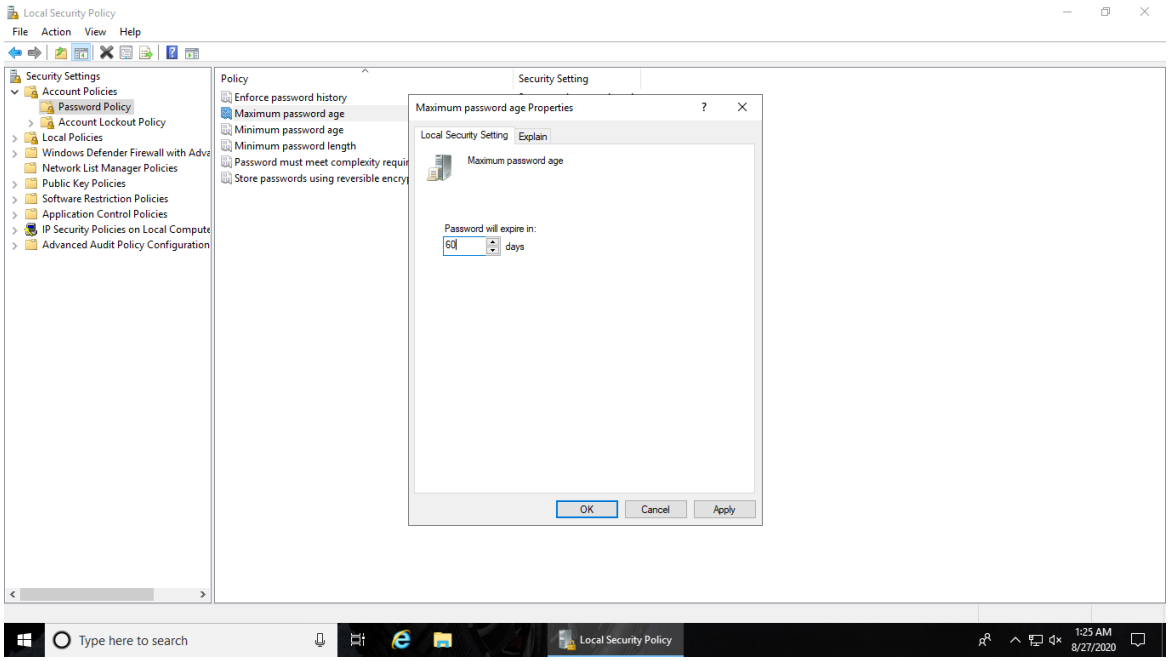


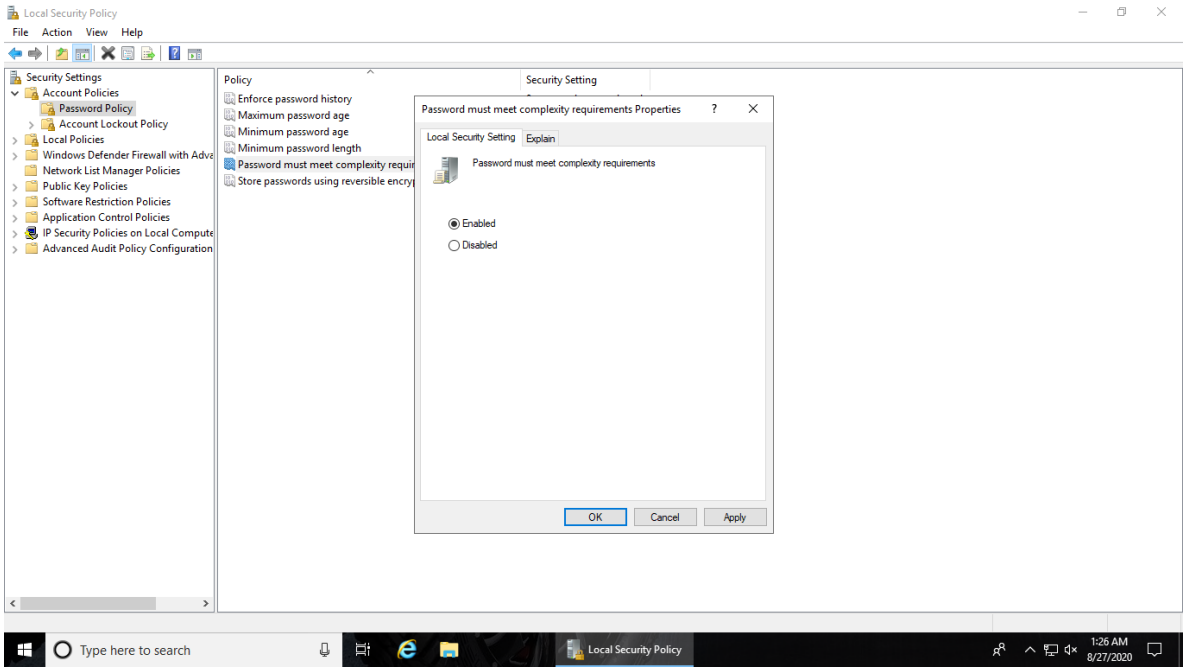
2. Explain the process for setting the password and access control policies locally on a Windows 10 PC.

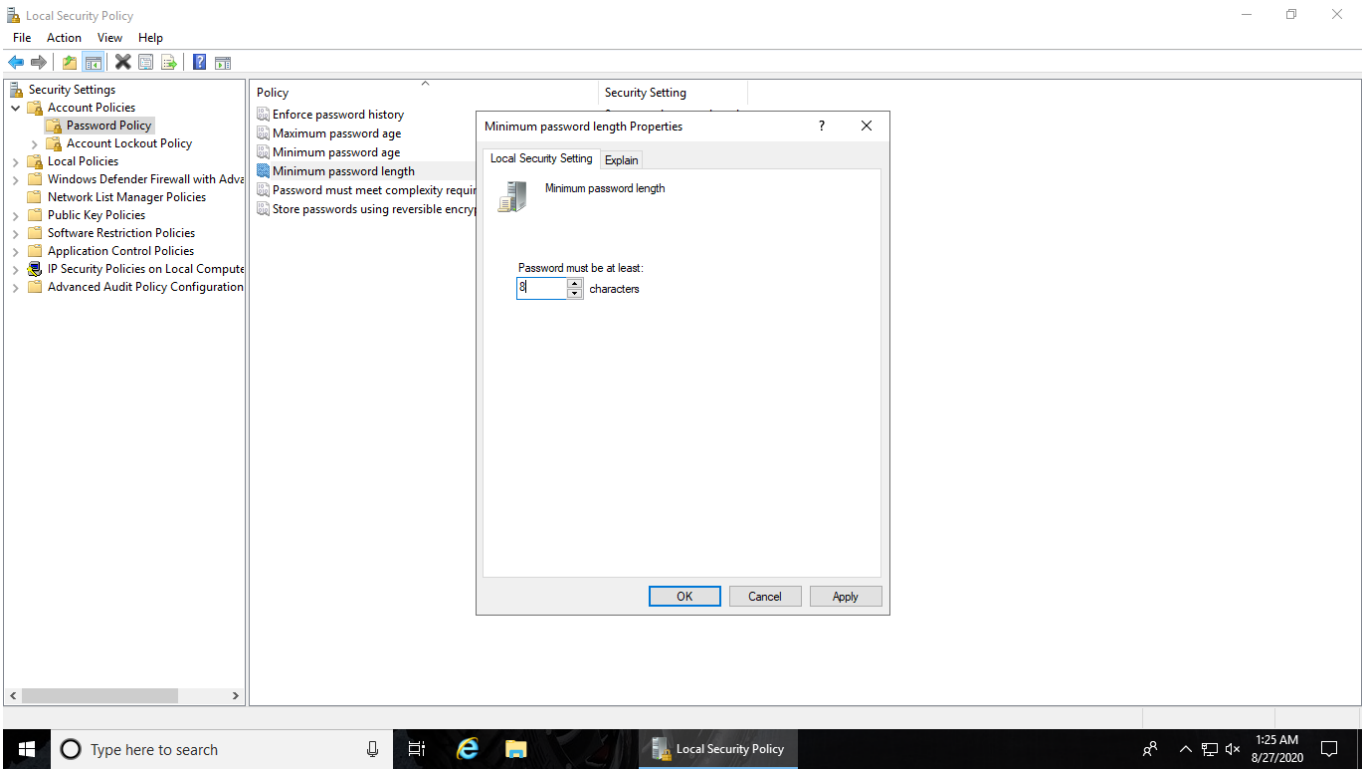
Click the search button on the desktop and type "Local Security Policy" and then click on "Account policies" and then select "Password Policy" and select the "policy settings" and change the values.

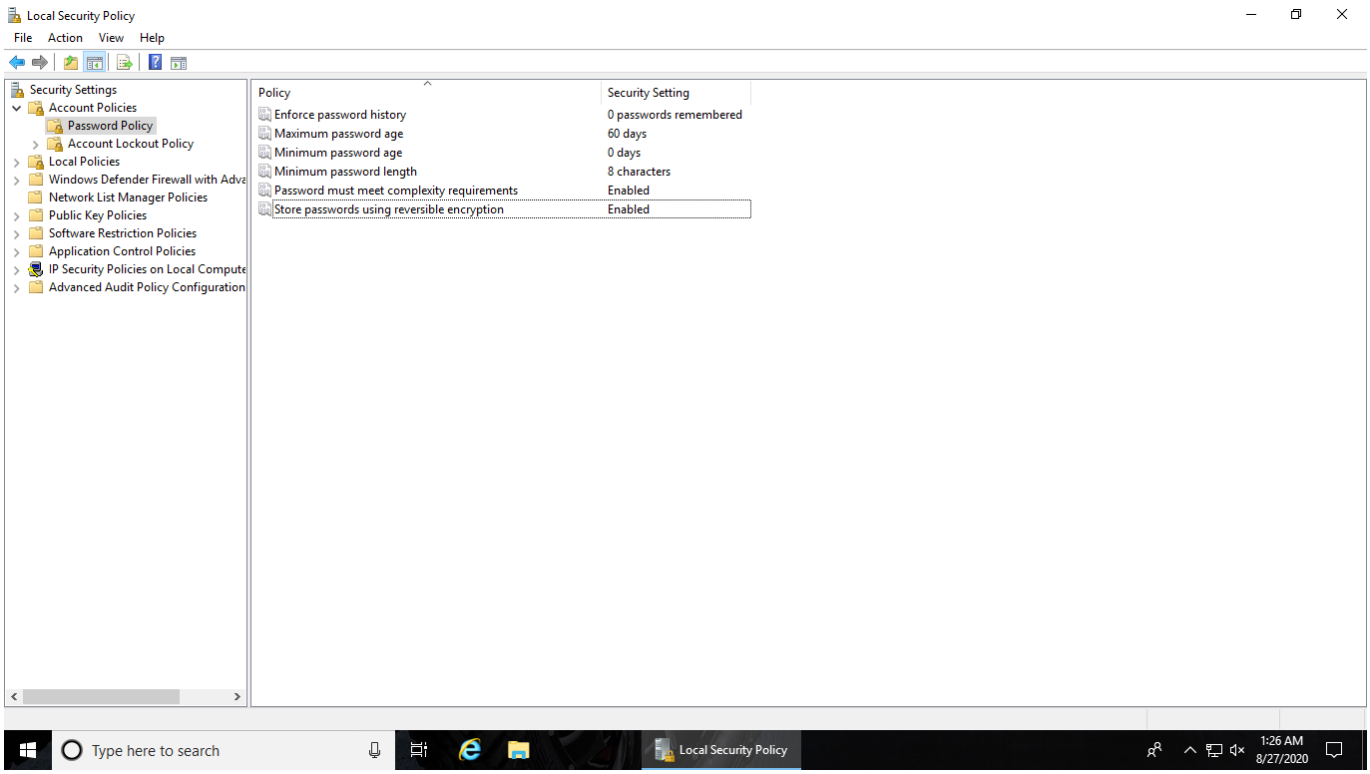
Provide screenshots showing how you set the rules on the PC.

- Setting the Password Policy:

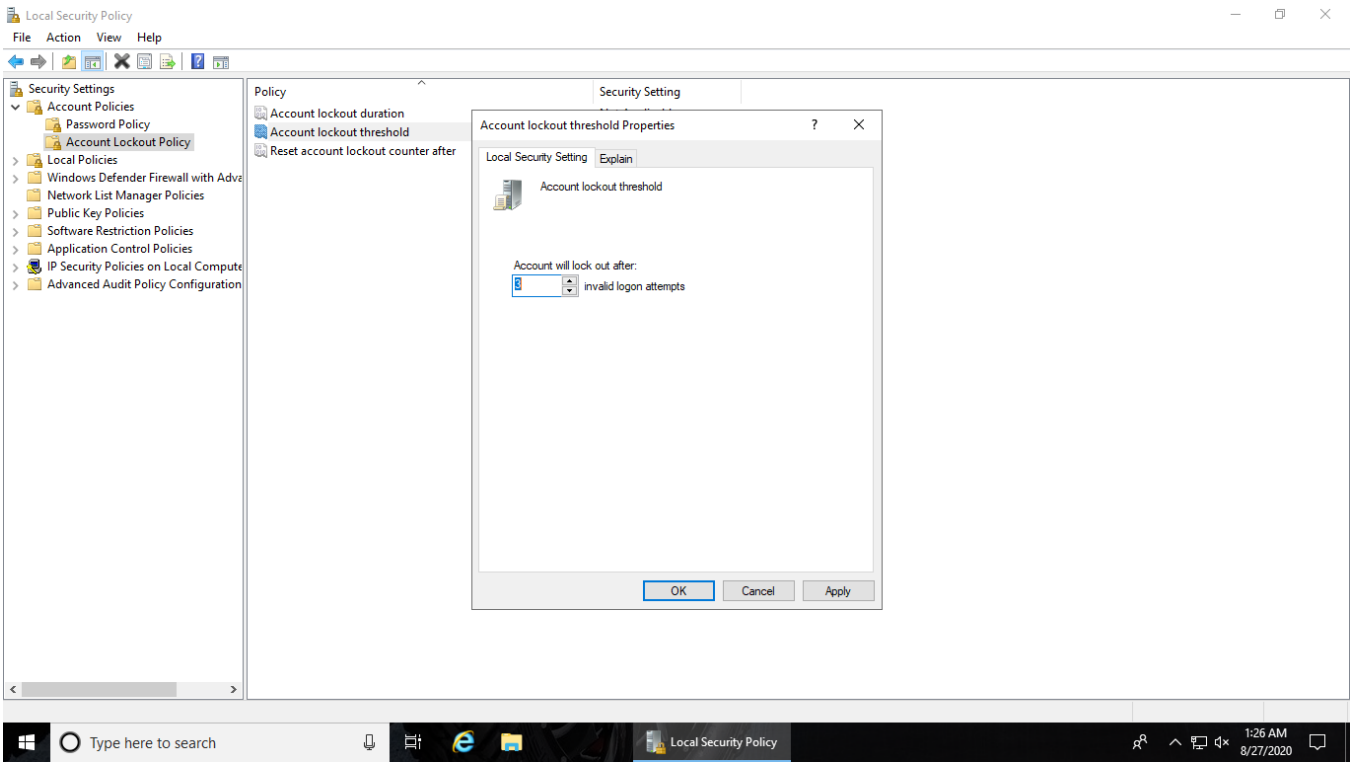


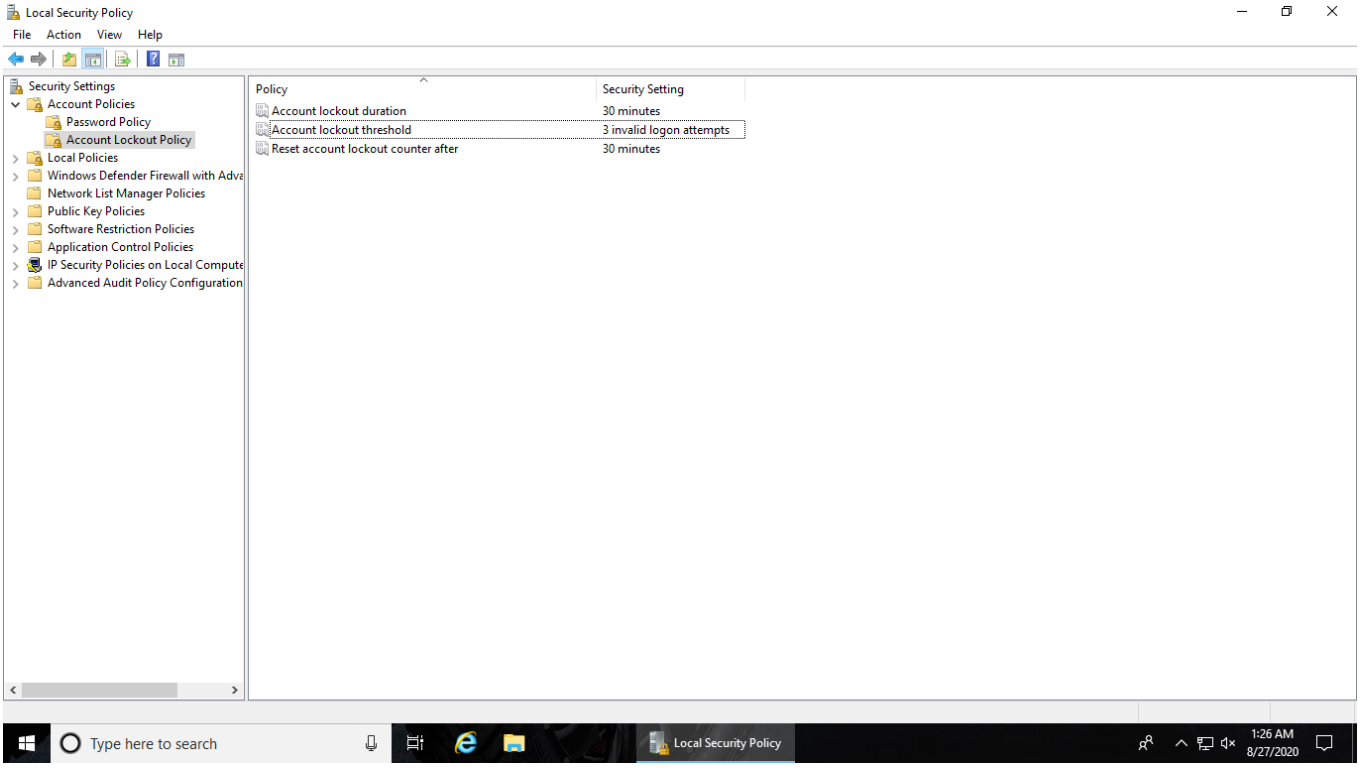






Setting the Account Lockout Policy:

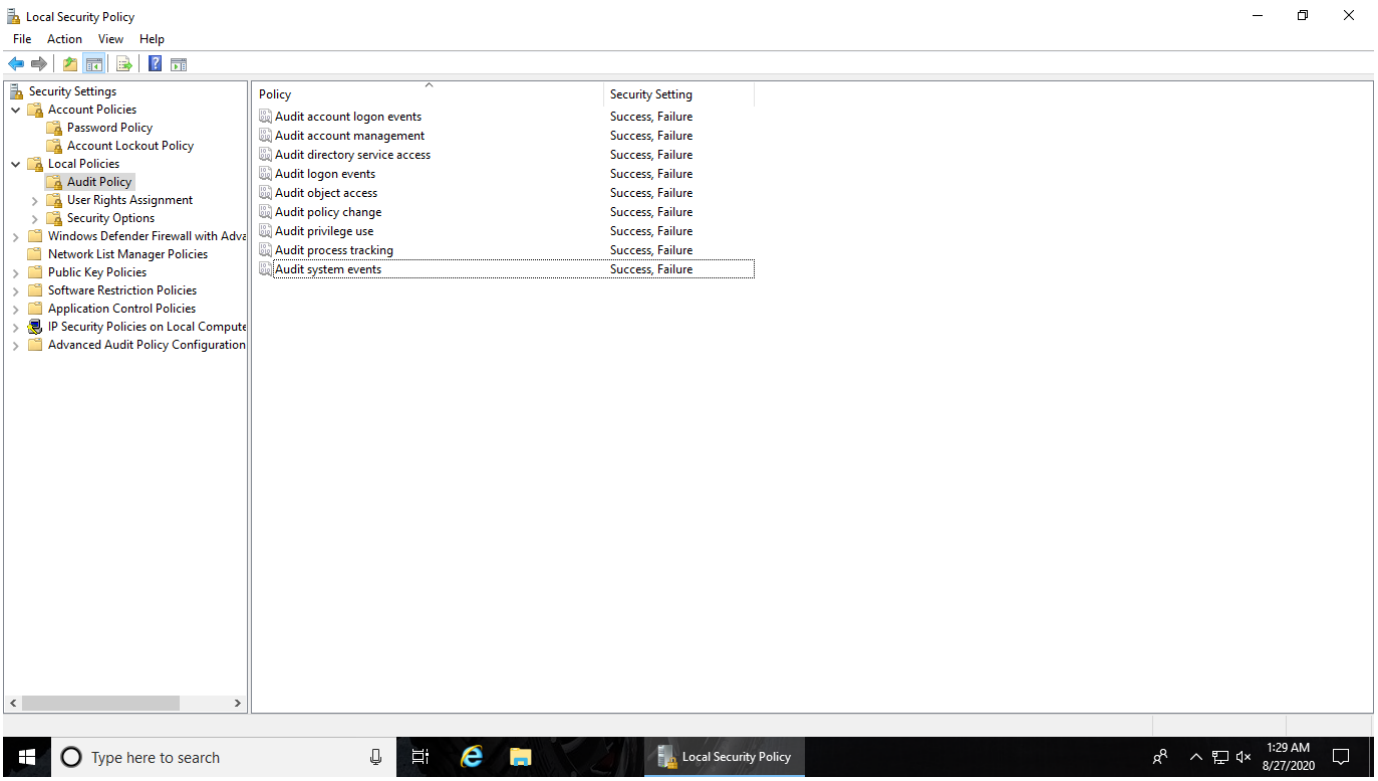

Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Account lockout duration
Account lockout threshold
Reset account lockout counter after
Account lockout threshold Properties
Local Security Setting
Explain
Account lockout threshold
Account will lock out after:
0
invalid logon attempts
OK
Cancel
Apply
Type here to search
Local Security Policy
1:26 AM
8/27/2020


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
Account lockout duration
30 minutes
Account lockout threshold
3 invalid logon attempts
Reset account lockout counter after
30 minutes
Type here to search
Local Security Policy
1:26 AM
8/27/2020

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

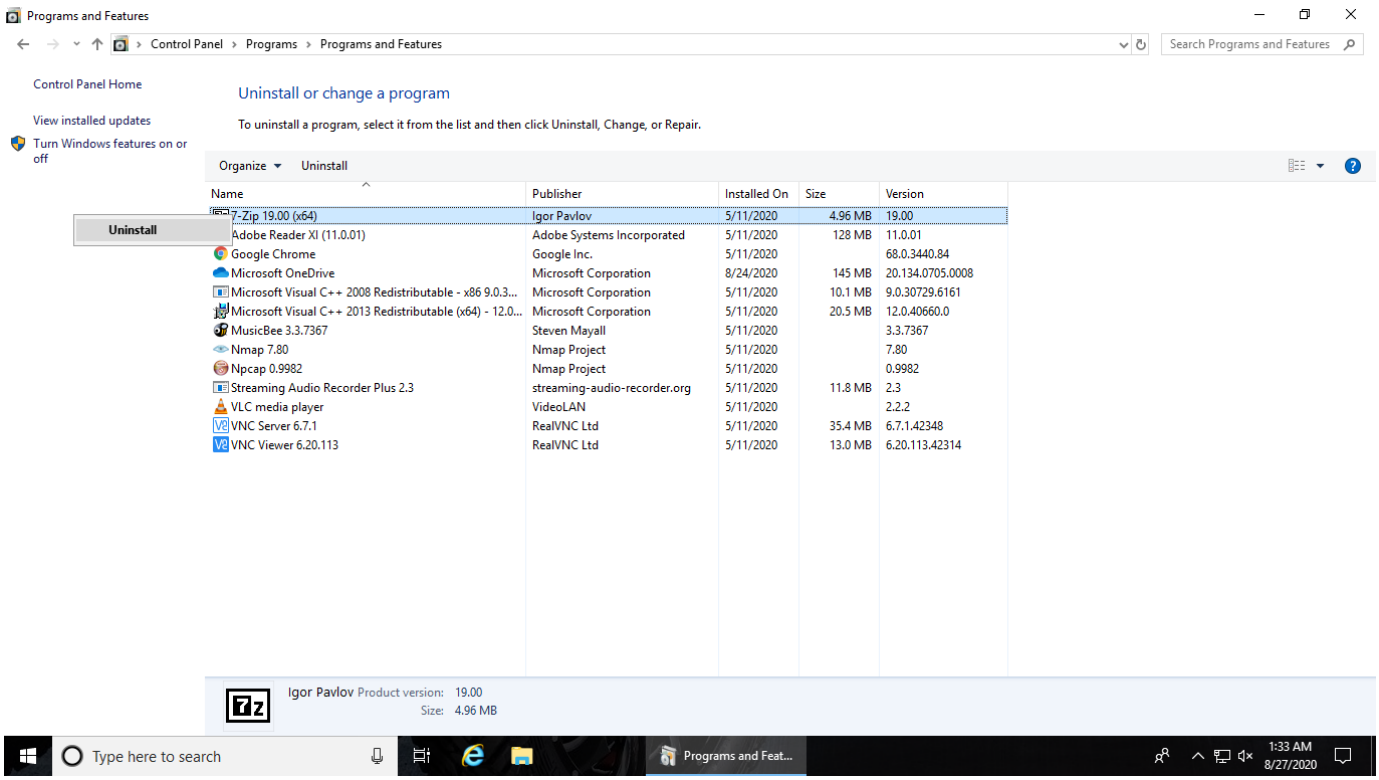
1. *List at least three application(s) that violate this policy.*

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

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

- **Apps may contain backdoors**
- **Collect user data in the background**
- **Download unnecessary plugins which might cause a problem**

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.*

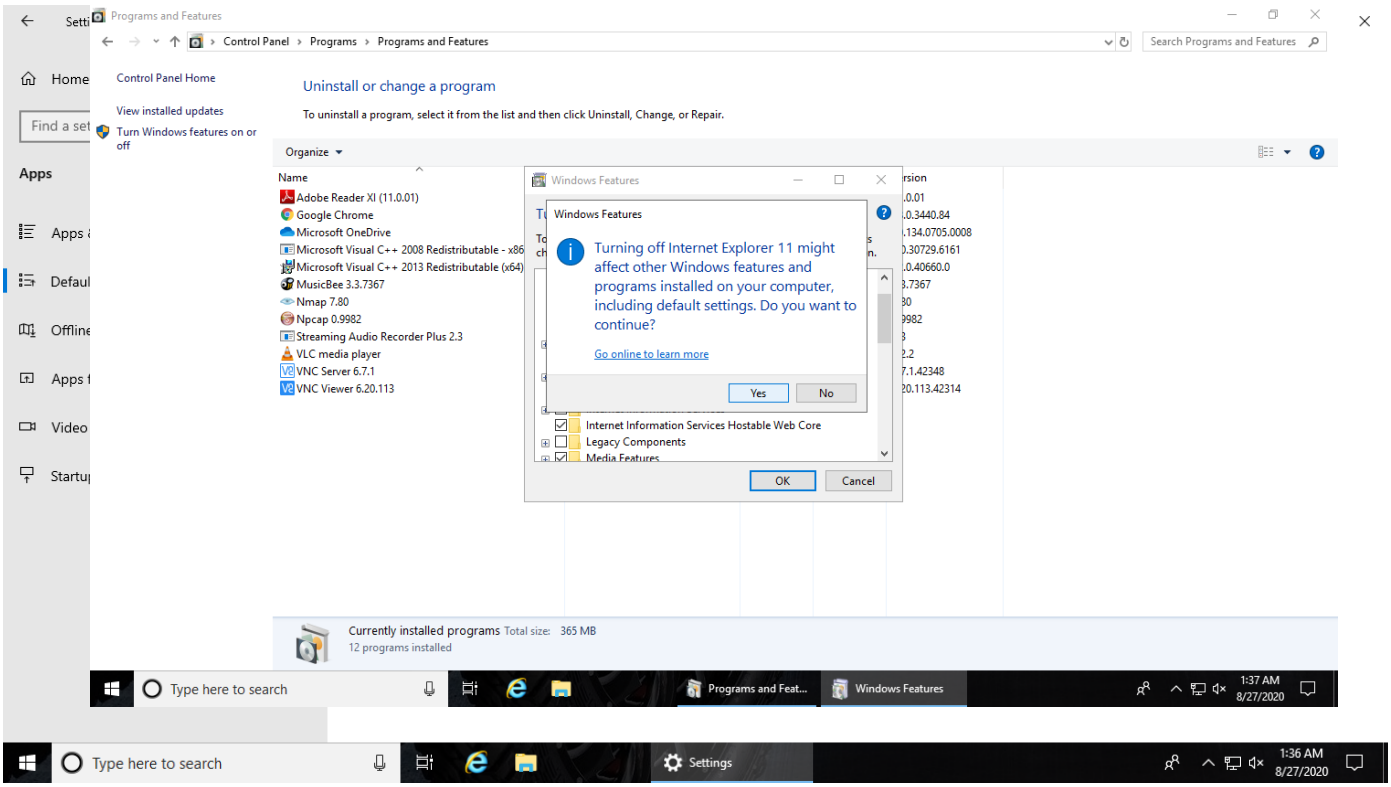


Select the search button on the desktop and type “control panel”. Select “programs”, then “programs and features”. In programs and features all the applications that are installed on the PC are shown. In that select the unnecessary applications and click uninstall.

Default Browser

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

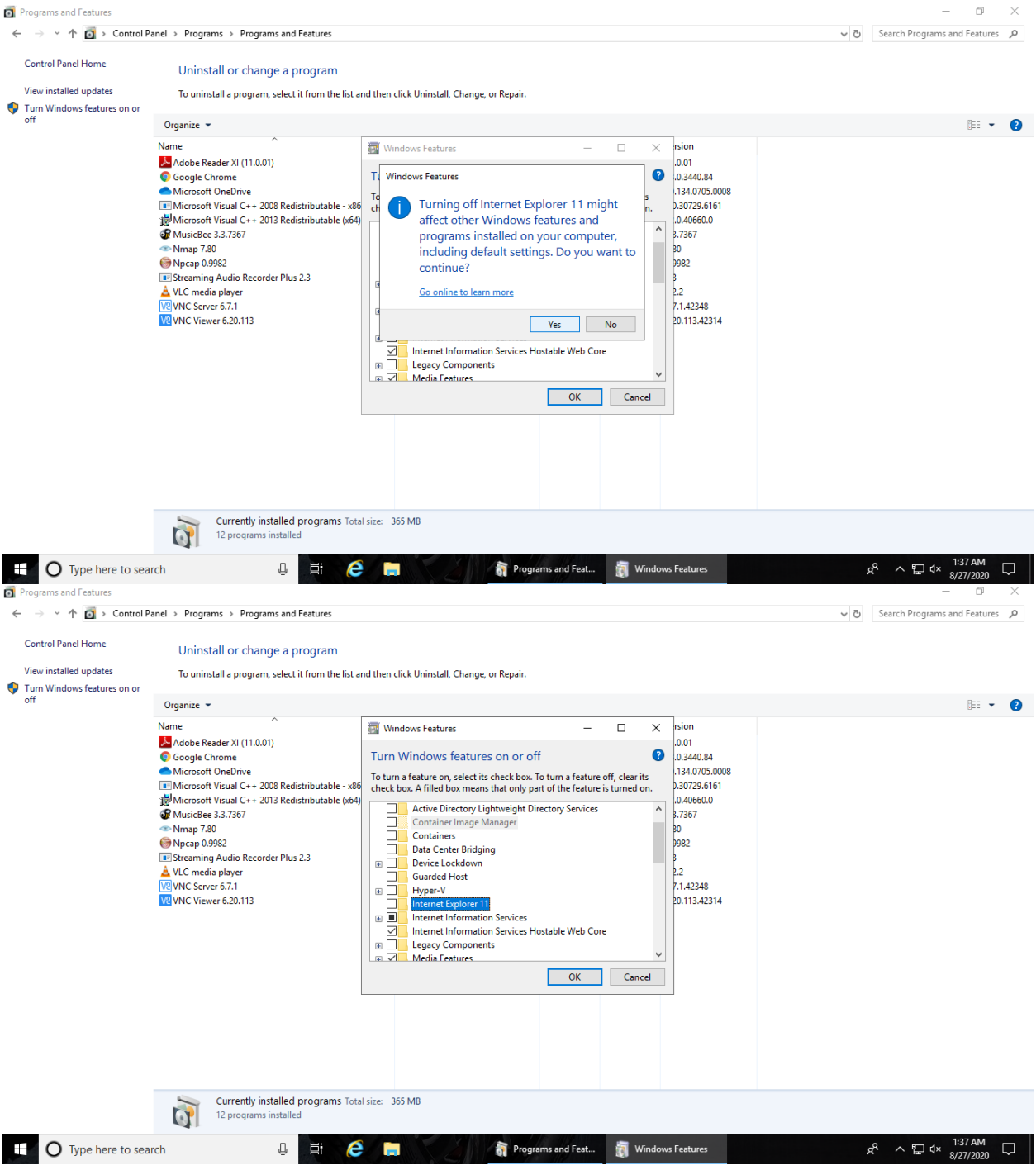
1. *Explain how you set default applications within the Windows 10 operating system. Include screenshots as necessary.*
   Click the start button on the desktop and select “Settings” and then select “Apps”. Go to “Default apps “. Click on the default web browser and change it to Google Chrome.



2. *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
    - **Outdated web browser becomes vulnerable to harmful viruses**
    - **Critical vulnerability in the browser allows malicious actors to hijack the computers**

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**."

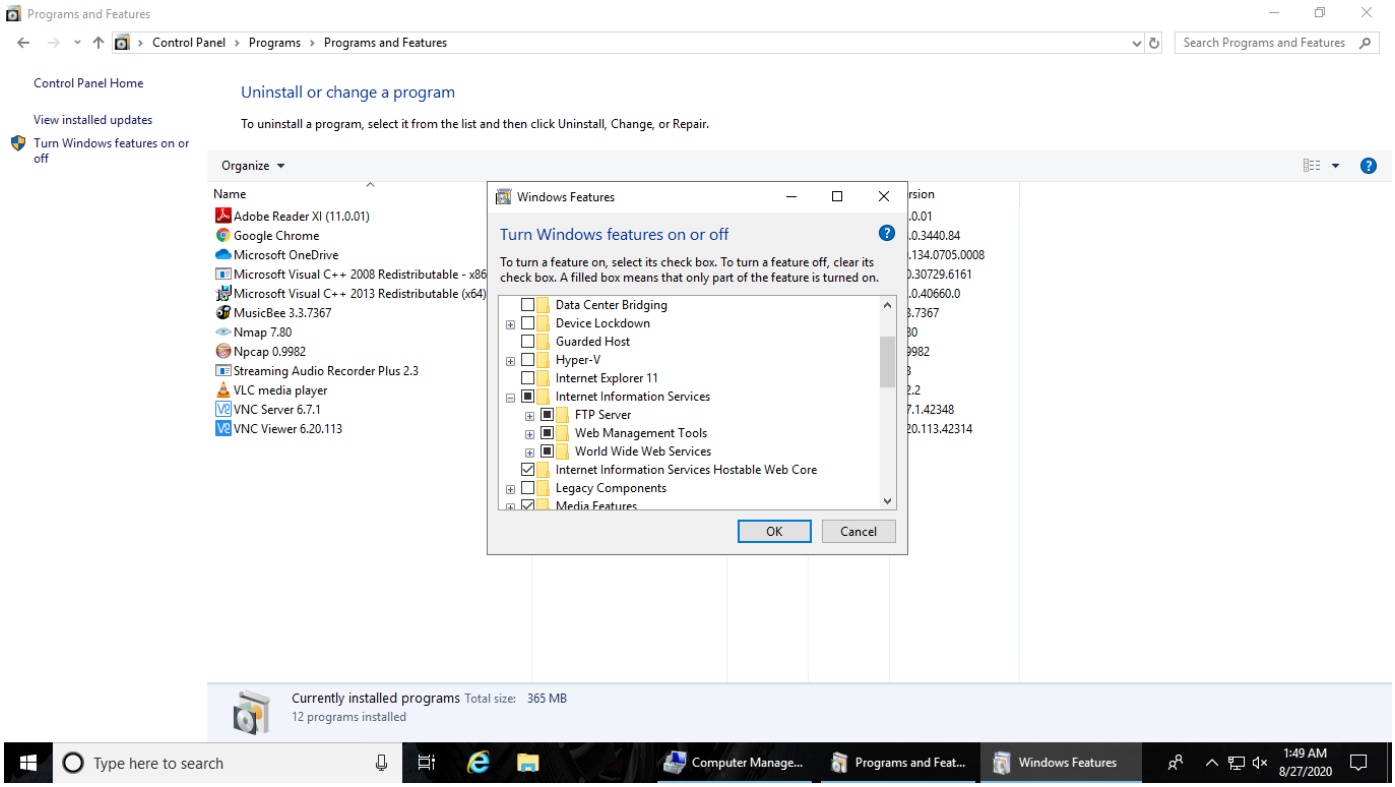
3. *Provide a screenshot showing Internet Explorer 11 is off.*



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.

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

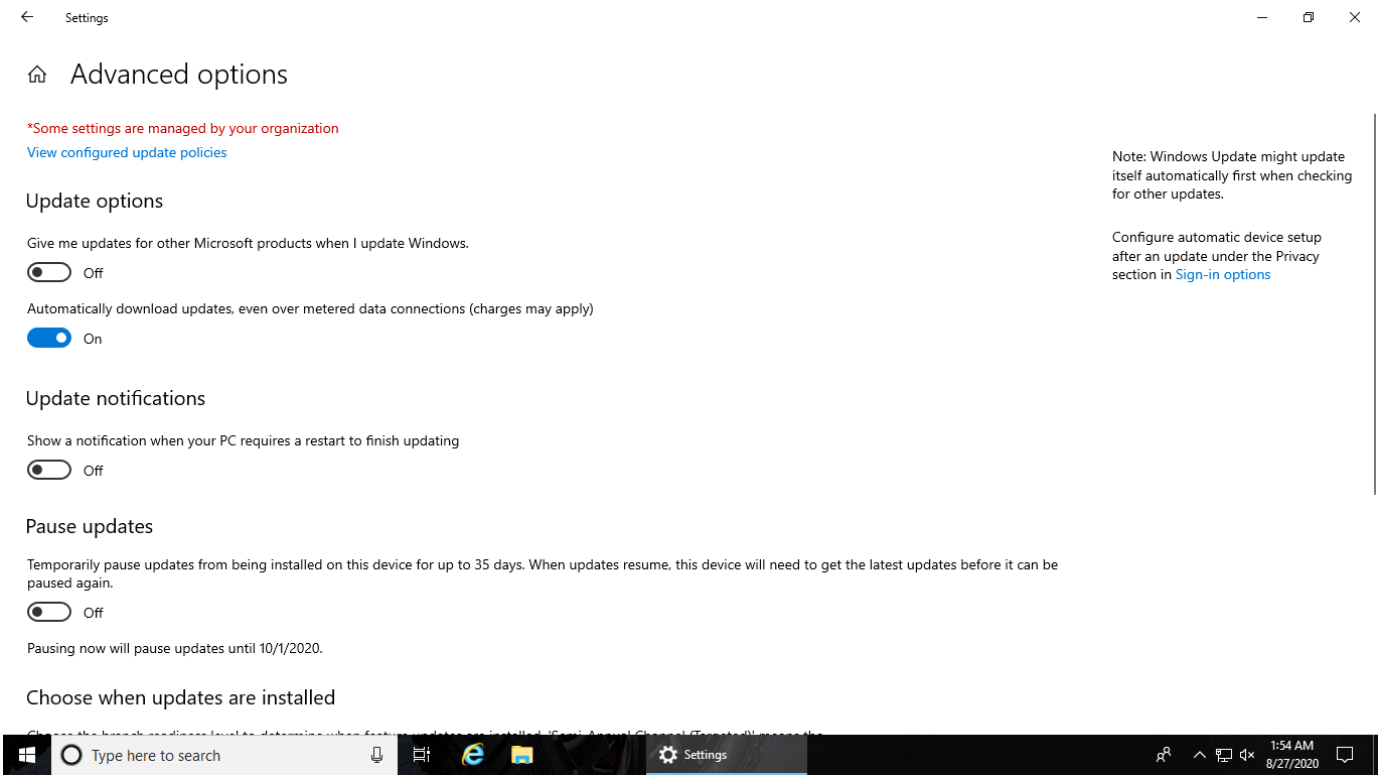


2. Advanced users should provide at least two methods for determining a web server is running on a host
3. How do you disable them and make sure they are not restarted?
   Go to the control panel and select programs -> programs and features. In program features search for Internet Information Services. 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.

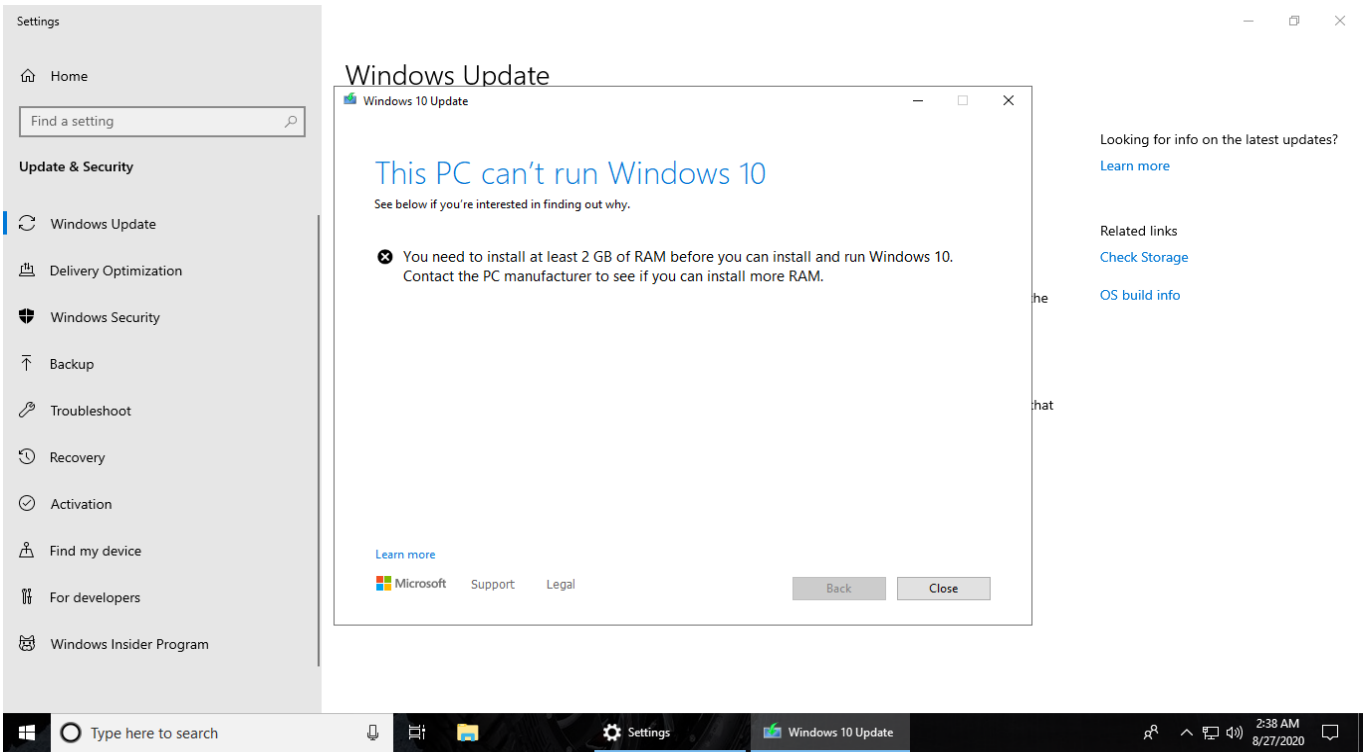
Patching and Updates

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.*



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:*

- Couldn't determine as the update was not possible
-

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

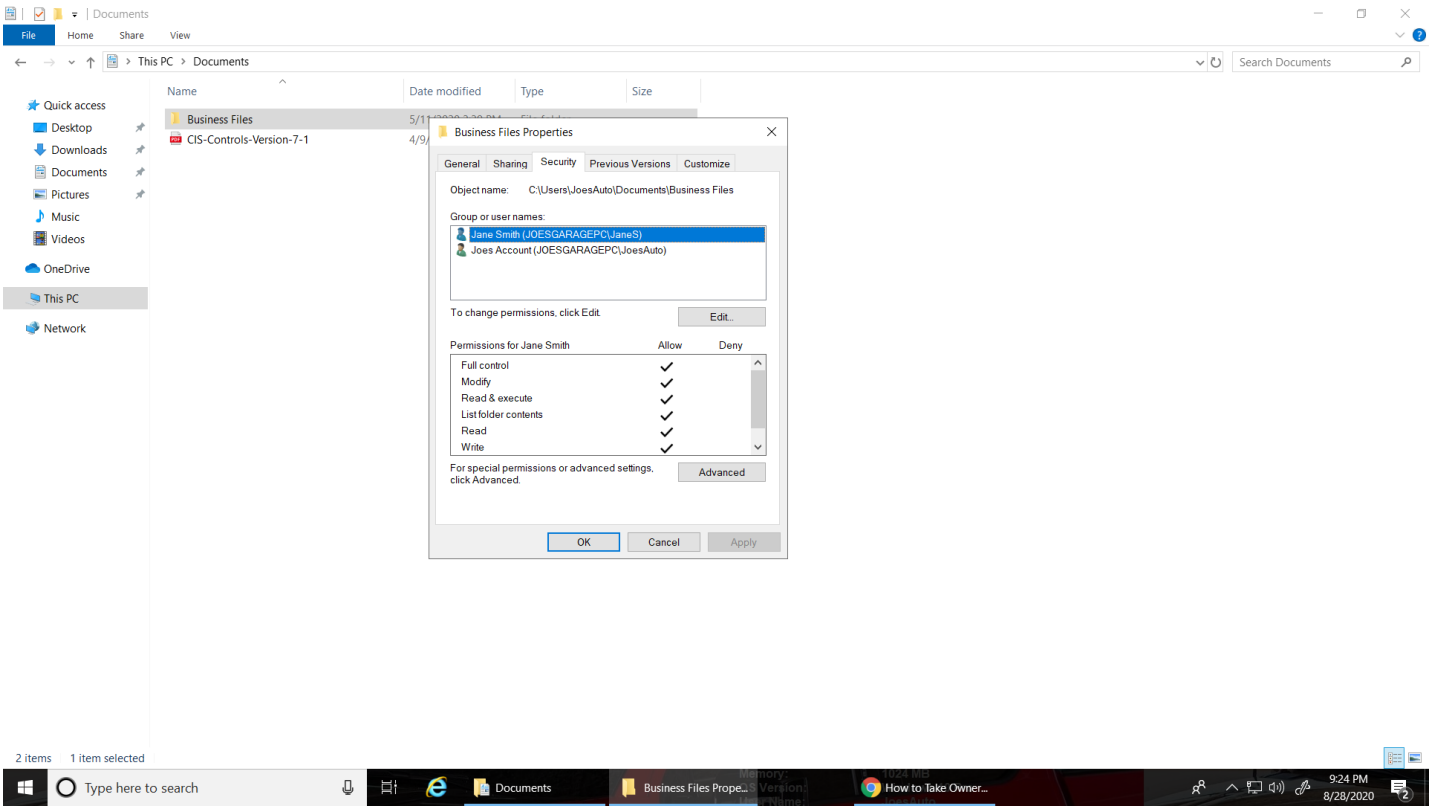
5. Securing Files and Folders

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.]*



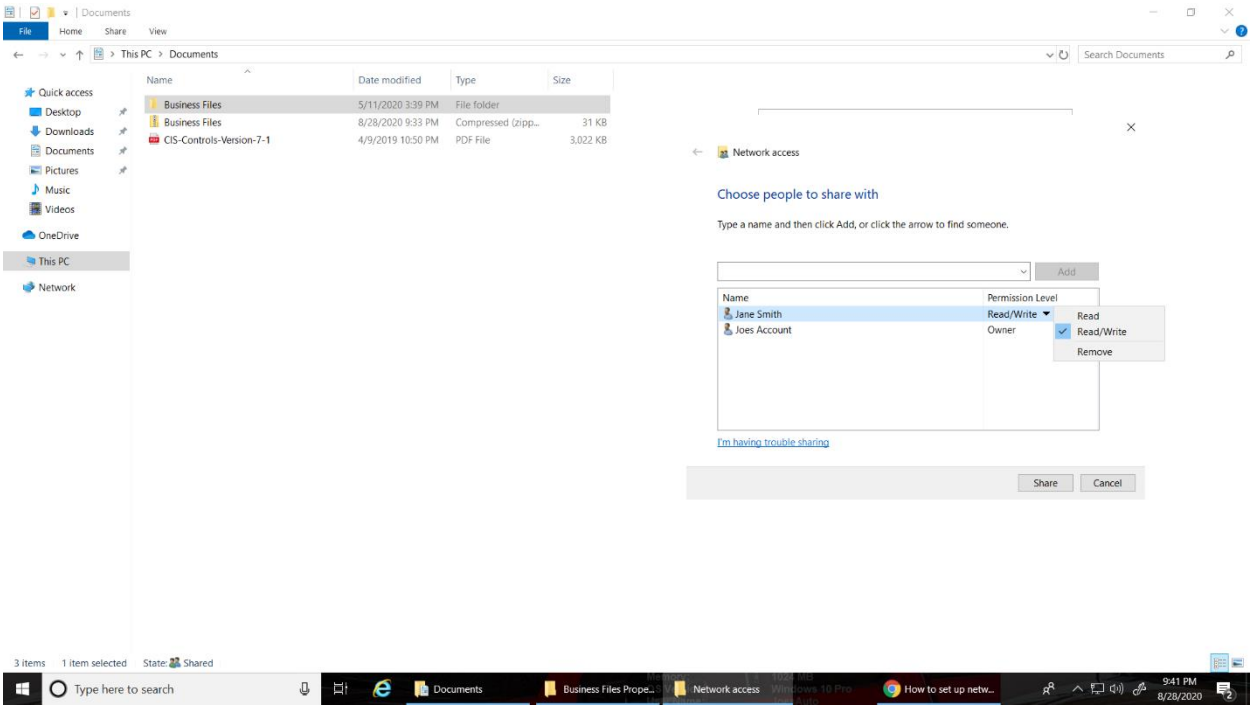
Go to the folder whose permissions are to be changed. Right click on the folder and select properties. Go to the "Security" tab and click "Advanced". Remove all the inheritance from the accounts and then select the accounts that need to be given permissions.

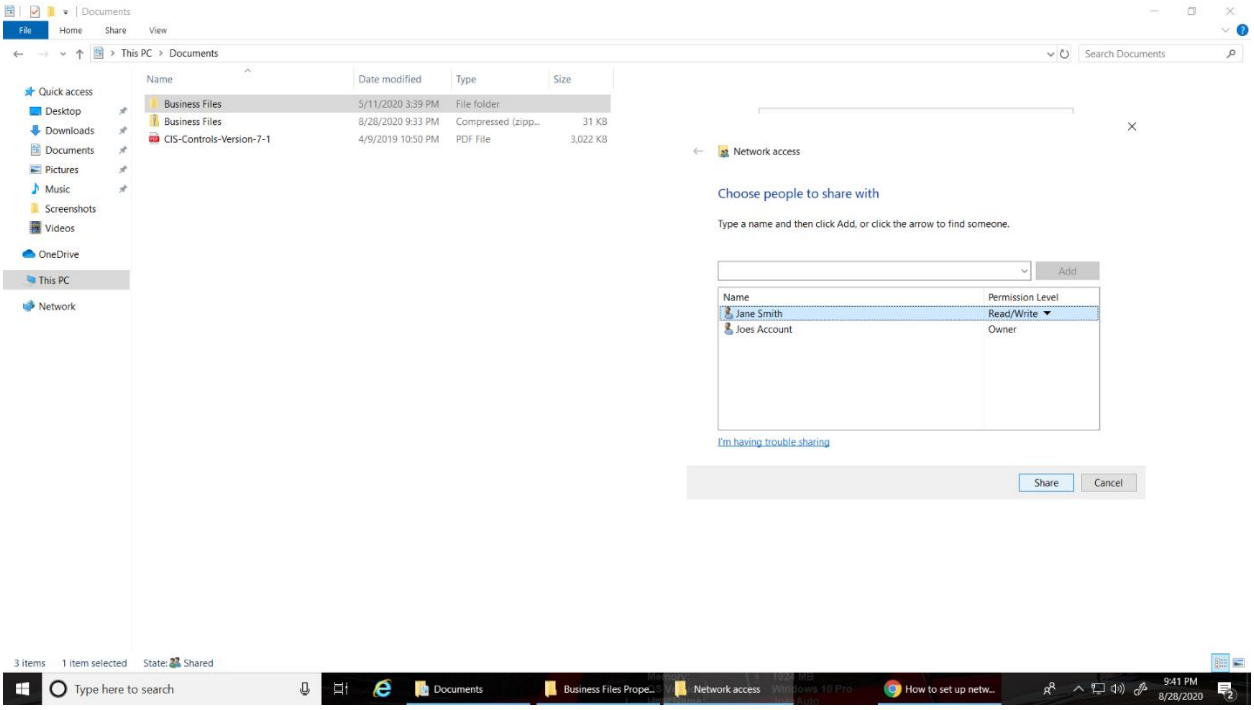
2. *Joe wants his work files encrypted with the password, "SU37*$xv3p1" Explain how you would do this. What encryption method do you recommend? You may use the pre-installed program 7-Zip for this.*
   Go to the folder that needs to be password protected and right click on the file. Select "7-zip "and then select "Add to archive". Select the file type as zip and enter the desired password. Select the desired encryption type and then click ok.
   I would recommend "AES" encryption type.
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**

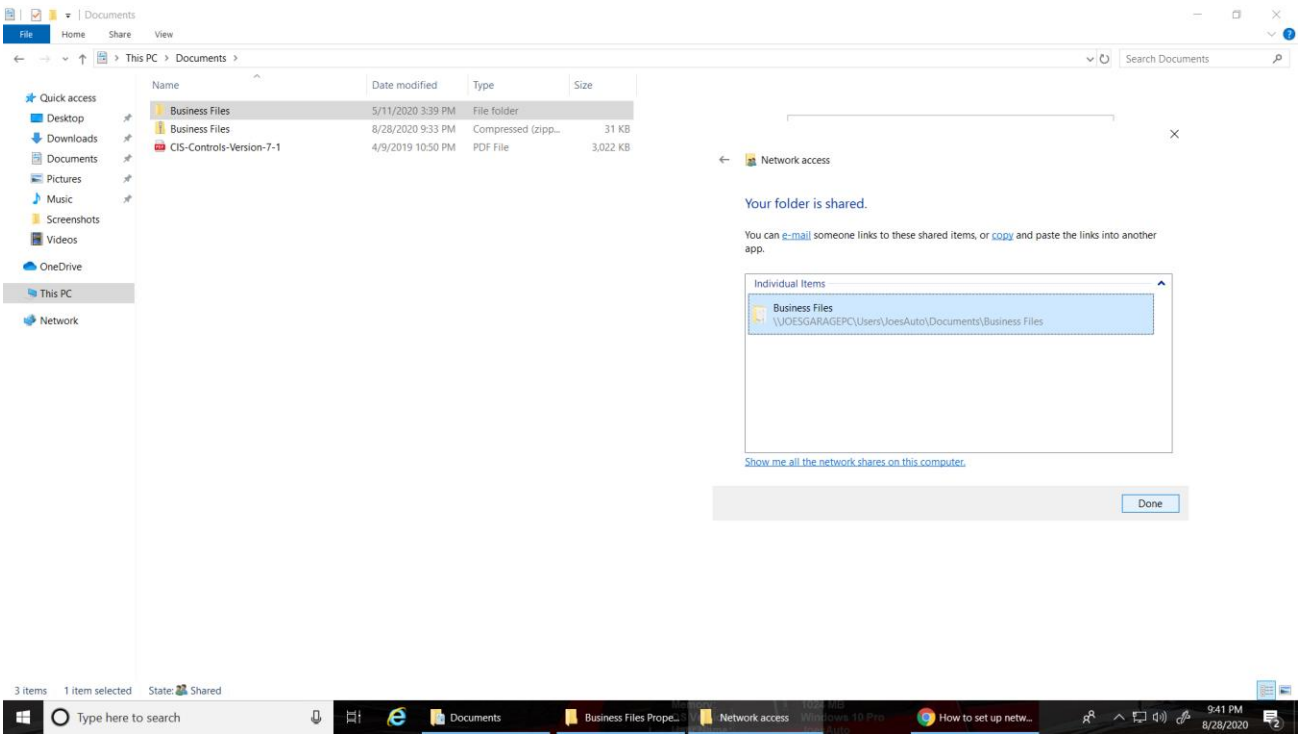
Shared Folders

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.*
   Select the folder that is to be shared and right click on it. Select "Properties" and click on "Sharing" and then click on "Advanced Sharing". Select the accounts to whom the folder is to be shared and then select the permission and then share the folder.







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.