

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: Lathika Devanand

Date of completion: 11-04-2023

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 is on it, what it is used for and who uses it. That's the concept of systems reconnaissance and asset inventory. In this step, you will document the hardware, software, user access, system and security services on the PC.

Complete each section below.

Hardware

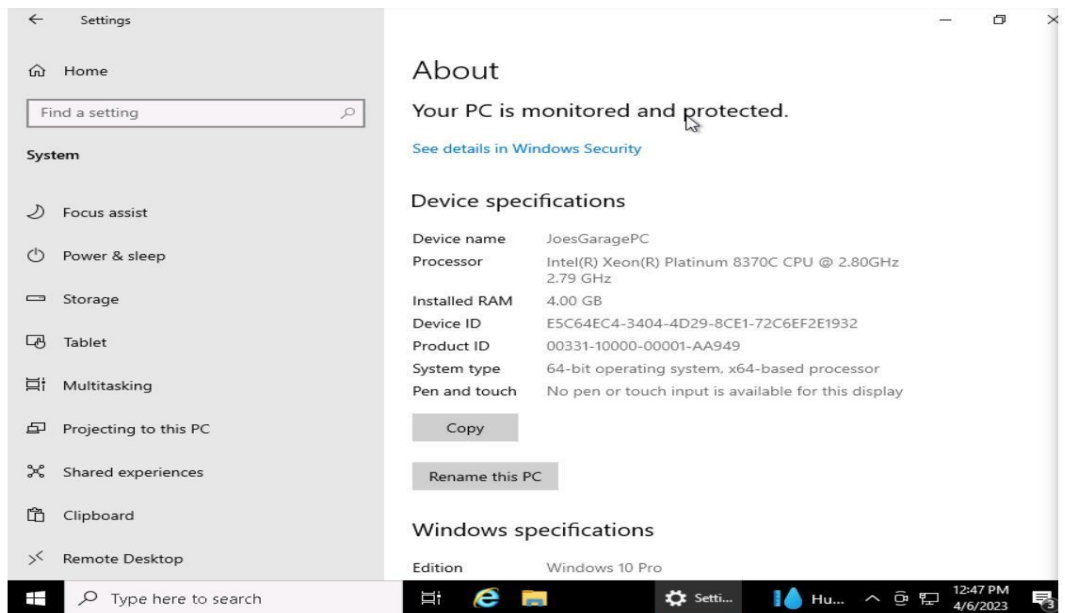
1. Fill in the following table with system information for Joe's PC.

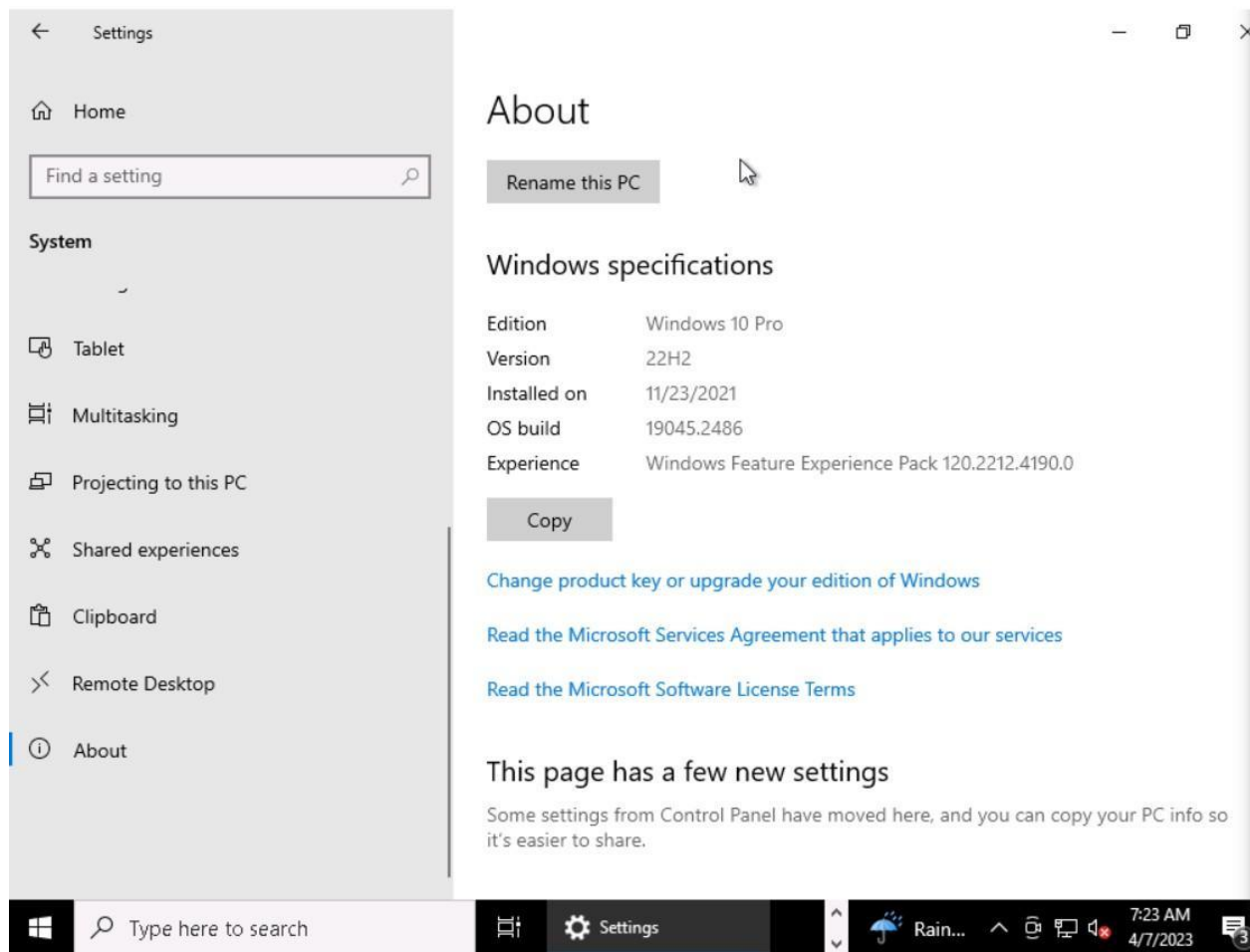
Device Name	JoesGaragePC
Processor	Intel(R) Xeon(R) Platinum 8370C CPU @ 2.80GHz 2.79GHz
Install RAM	4.00 GB
System Type	64-bit operating system, x64-based processor
Windows Edition	Windows 10 Pro
Version	22H2
Installed on	11/23/2021
OS build	19045_2486

2. Explain how you found this information:

I clicked on the windows button at the bottom left and clicked on settings. The settings panel opened and I clicked System. From the system I scrolled to the last available option that is named as "about" and this portion of the settings showed all the information about the system.

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



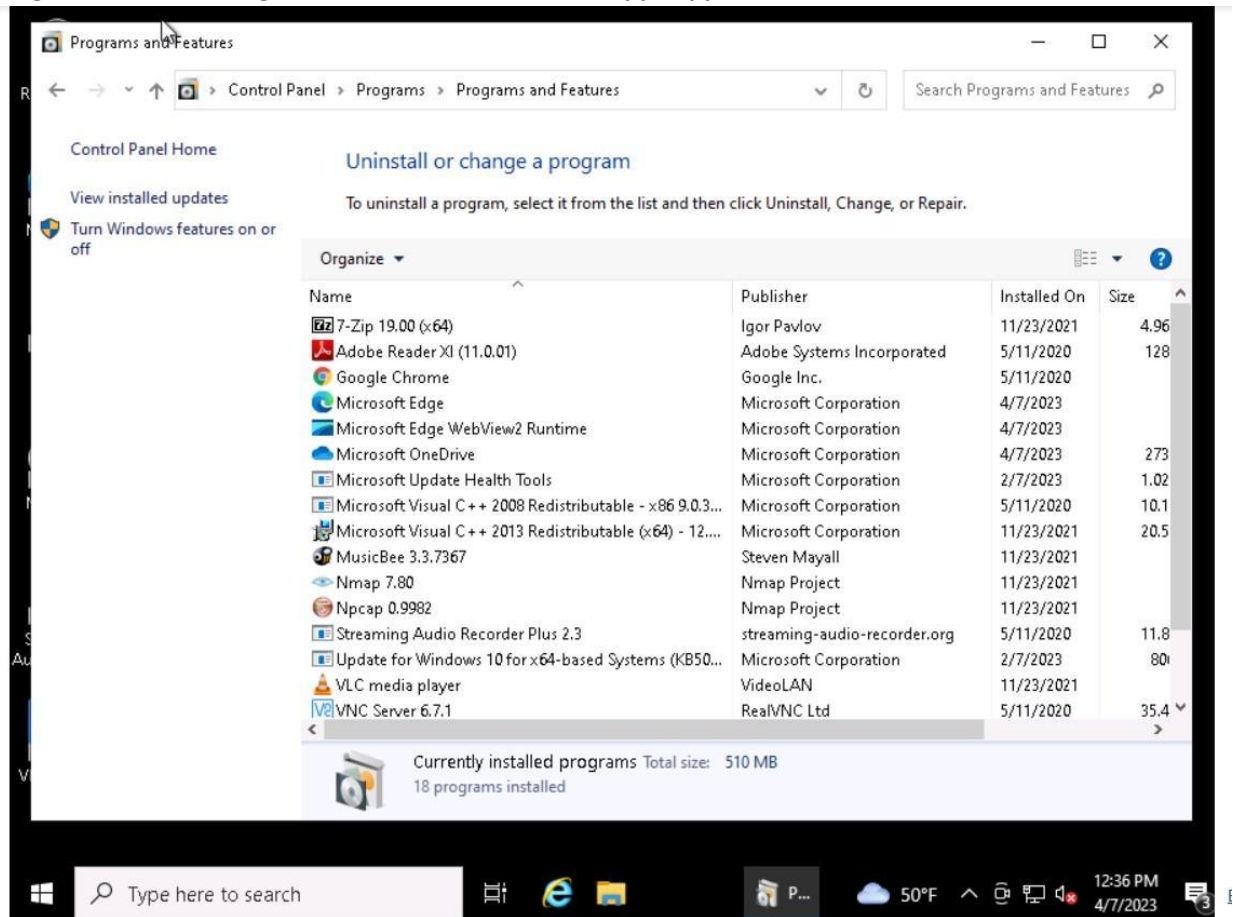


Software

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:*
 - **Adobe Reader XI**
 - **NMap 7.80**
 - **Npcap 0.9982**
 - **Google Chrome**
 - **Microsoft Edge**
2. *Explain how you found this information. Provide screenshots showing this information.*

I typed in the search bar to find the control panel. From the control panel, I clicked Program and then Program Features. Then a list of apps appeared



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

This step fulfills the CIS Critical Security Control 2: Inventory and Control of Software Assets. In this step, we need to distinguish the software that are required for an organization and remove any unauthorized software that are irrelevant to the business. We have to maintain the required software and update it to make sure most of its patches are fixed which makes it hard for hackers to exploit the software that the business intend to use for various sensitive data.

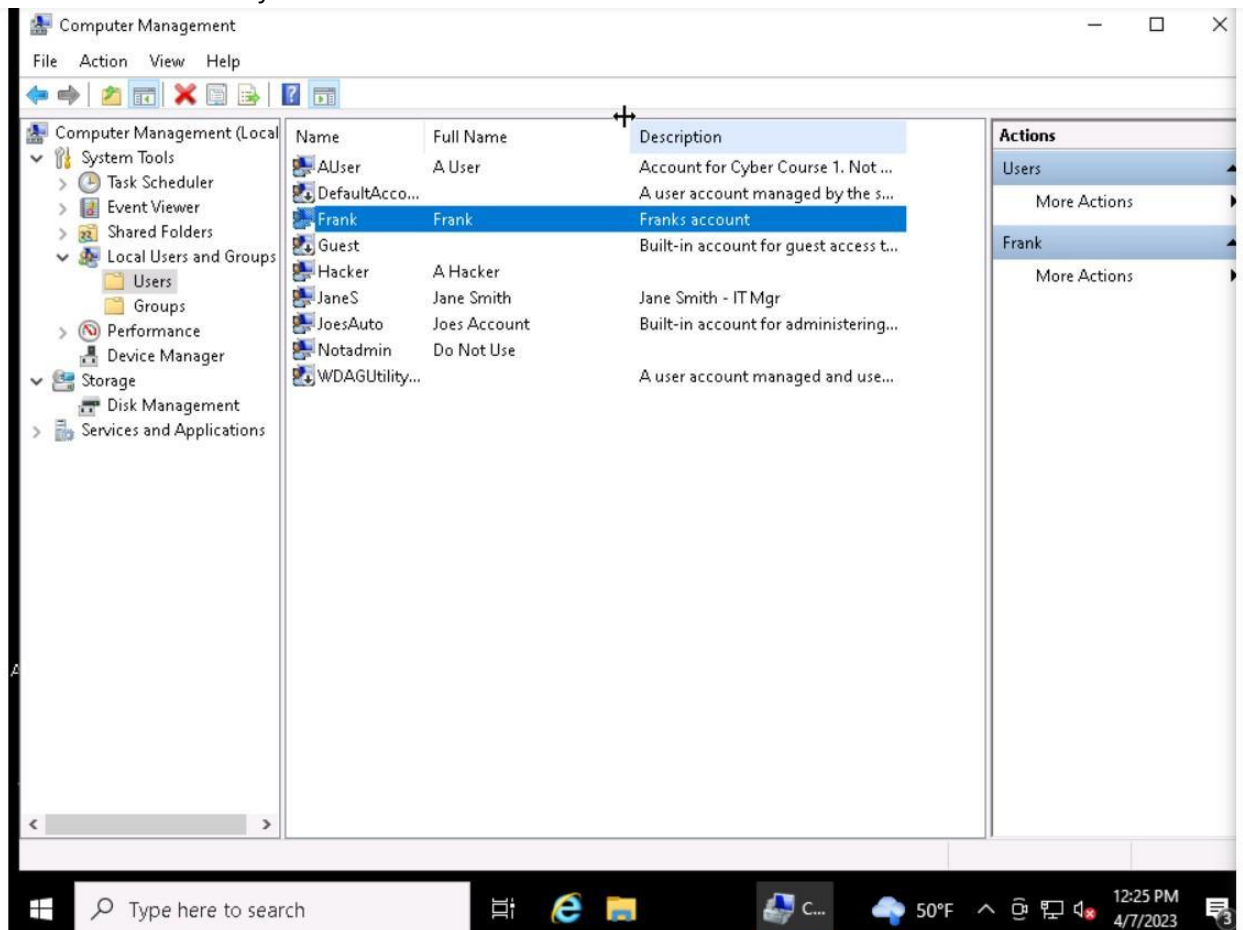
Accounts

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		
Guest		
Frank	Frank	
JaneS	Jane Smith	Administrator
Hacker	A Hacker	Administrator
JoseAuto	Joese Account	Administrator
Notadmin	Do Not Use	
WDAGUtility		

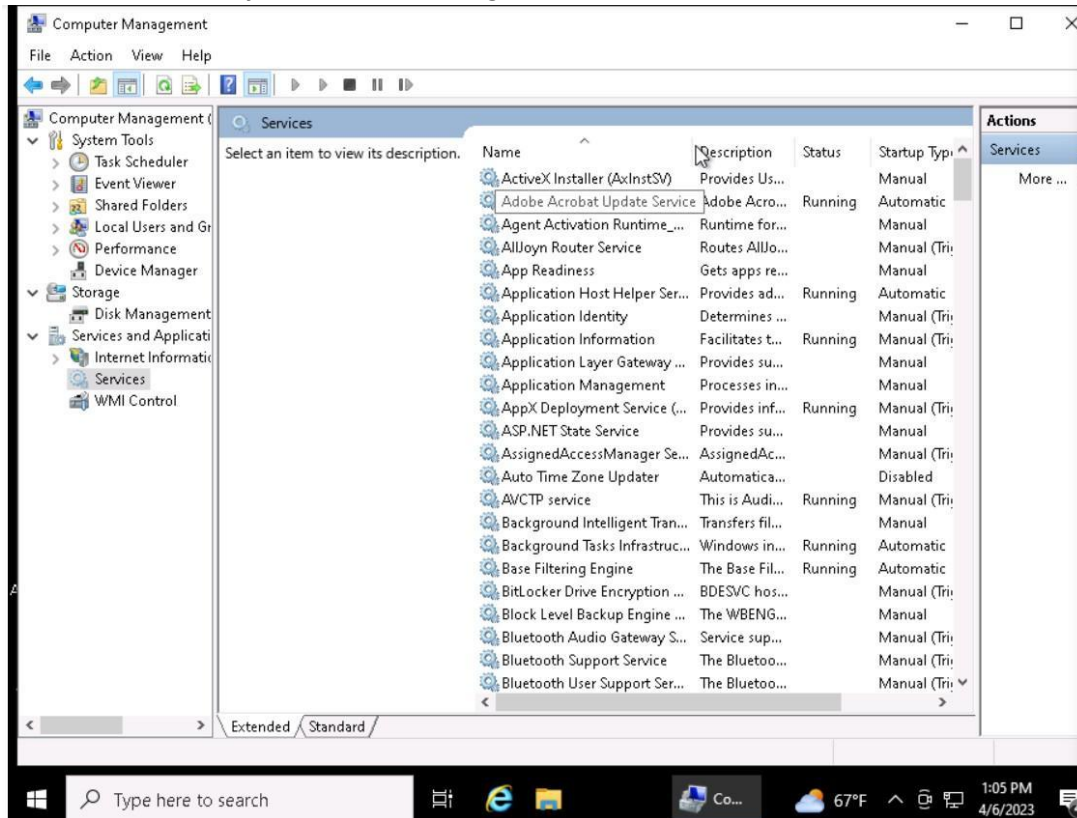
2. Provide a screenshot of the Local Users.



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.

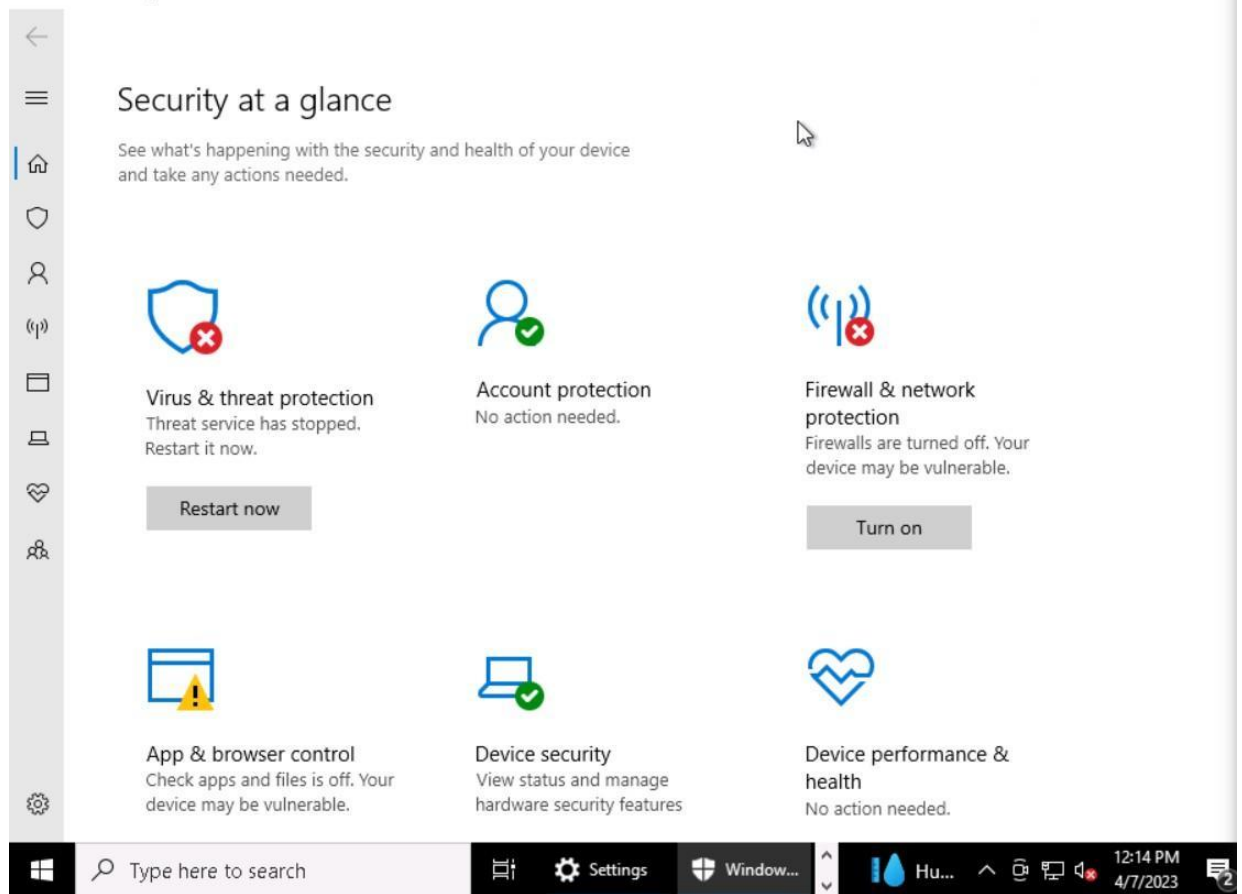


Security Services

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.**

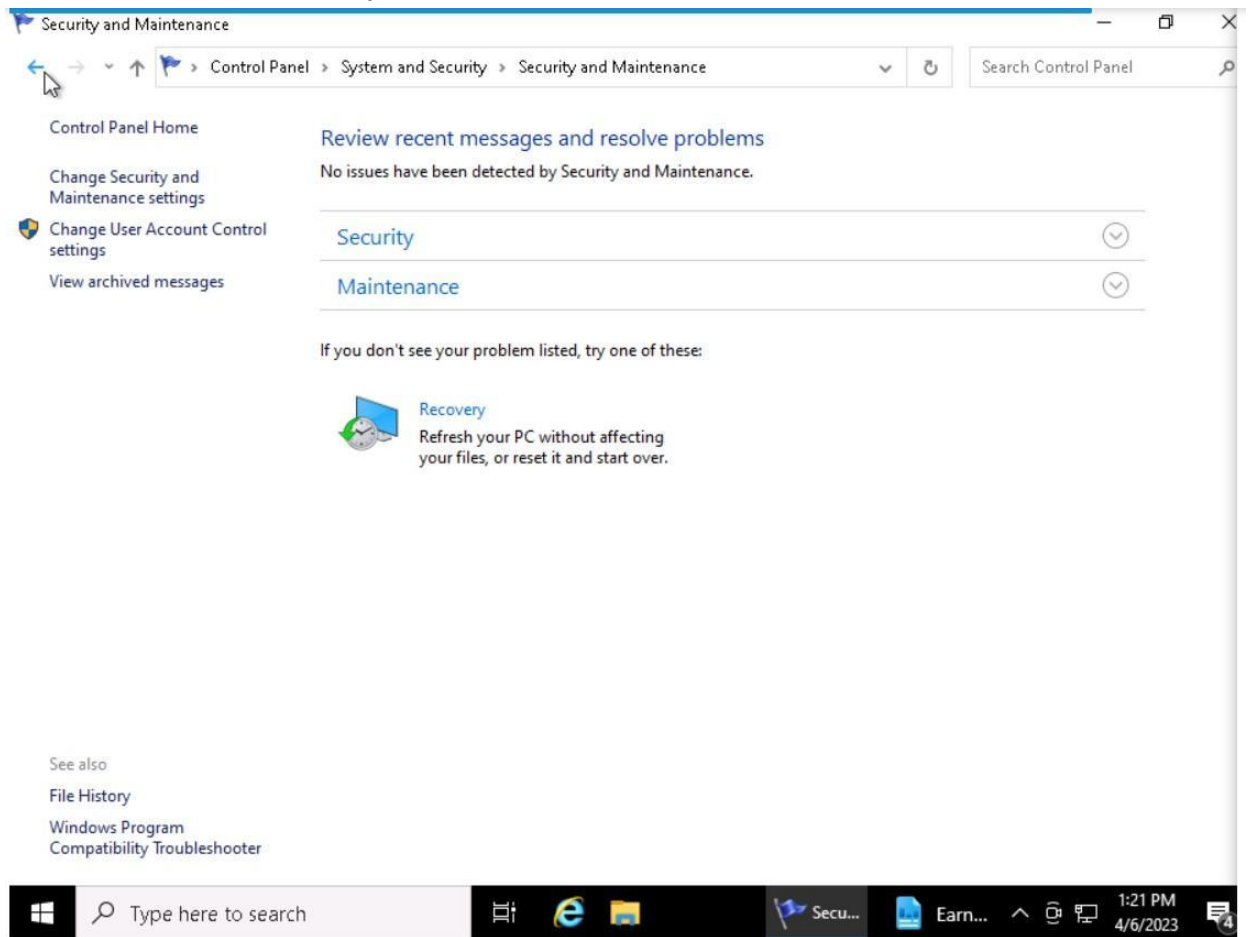
1. To view a summary of security on Windows 10, start from the **Control Panel**. Use the "Find a setting" bar and search on Windows Defender. You can also search for Windows Defender using the Windows Run bar. Take a screenshot of what you see on the Windows Security screen and

include it here:

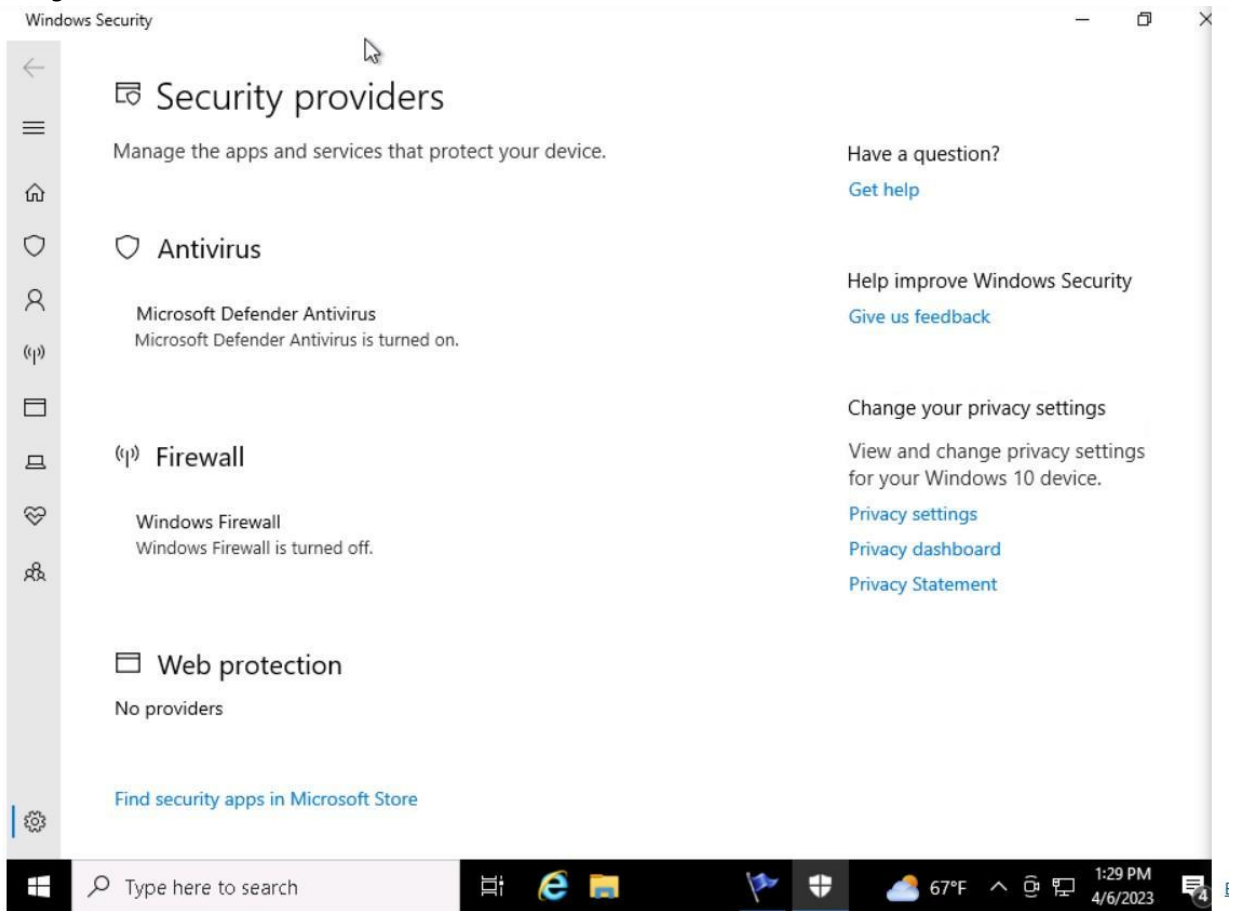


2. The Windows 10 Security settings are also found from the **Control Panel > System and Security > Security and Maintenance**. Start by viewing **"Review your computer's status and resolve**

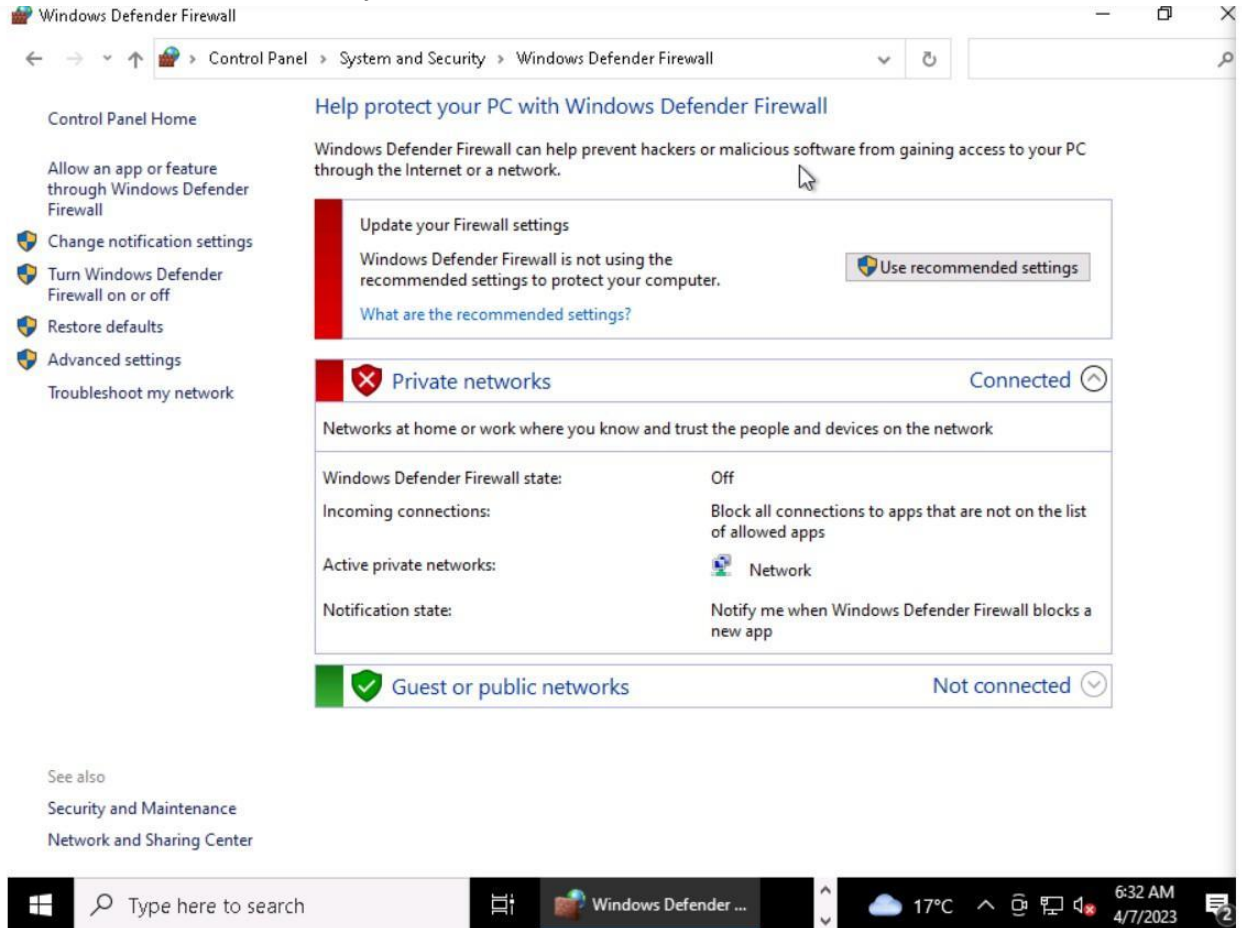
issues.” Provide a screenshot of this below:



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

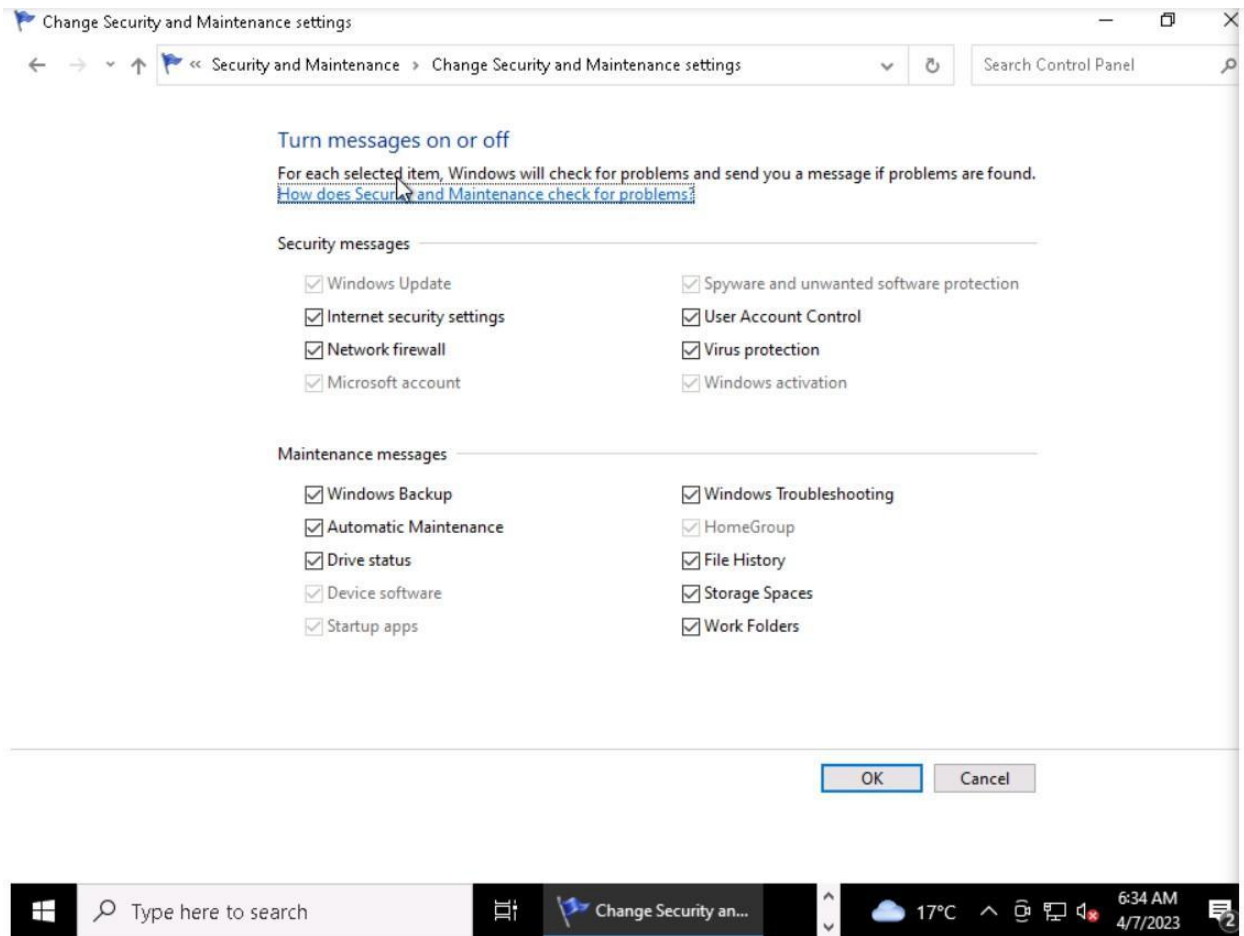


4. From the **Control Panel**, go to **System and Security**. In that window, select **Windows Defender Firewall**. Provide a screenshot of it here:


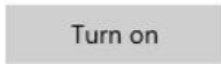



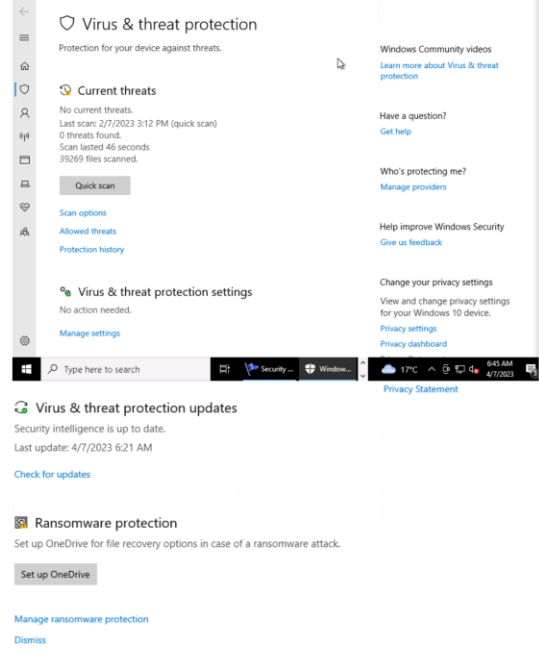
5. PC users should be notified whenever there is a security or maintenance message. In the Security & Maintenance window, click on Change Security and Maintenance settings and take a

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	 Private network (active) Firewall is off.  I opened settings and typed in firewall and a window opened giving information about the firewall
Firewall product and status – Public network	 Public network Firewall is on.

	I opened settings and typed in firewall and a window opened giving information about the firewall
Virus protection product and status	 <p>I opened settings and typed in Virus Protection and I opened the Virus & threat protection window and was able to access these information</p>
Internet Security messages	None
Network firewall messages	None
Virus protection messages	None
User Account Control Setting	None

7. Now that you are familiar with the security settings on Joe's PC, explain at least three vulnerabilities and risks with these settings. In other words, what can happen to Joe's PC if these are not changed?

[Hint: Refer to the CIS Controls document for ideas.]

- The firewall was off for private networks. This is highly dangerous especially when a malicious hacker or even an insider gains access to the private network. They would have an easy path to hack through this PC and obtain all of the valuable information. By turning the firewall on, Joe would be able to prevent most of the attacks that could happen through the private network.
- There seems to be a problem with threat protection services. These allows us to prevent our Pc from being attacked by virus or an outside threat. It gives an option below the Virus & Threat Protection to restart it. I suggest Joe restart it and bring the protection service back to its original configurations to make sure it protects his PC
- There is a suspicious account called "A Hacker" that is given administrative privileges.

Managing access control for each of the account is important especially when it comes to a PC that holds business data and Joe should remove unnecessary accounts and give admin privileges to only the users that require the admin access.

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?*

Joe should be using NIST for setting security policies. NIST (national Institute of Standards and Technology) is used around various companies to withhold a strict security policy. Since many organizations use these policies, it would be safe for Joe to use these policies as well to further enhance his business security.

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

He should follow CIS rules as they are given an outline of all the security measures that must be taken within an organization.

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?

He should look at the following controls in CIS v7:

CIS Control 8: Malware Defense, CIS Control 5: Secure Configuration and CIS Control 11: Secure Configuration of Network Devices

He should look at the following controls in CIS v8:

CIS Control 10: Malware Defense, CIS Control 4: Secure Configuration of Enterprise Assets

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

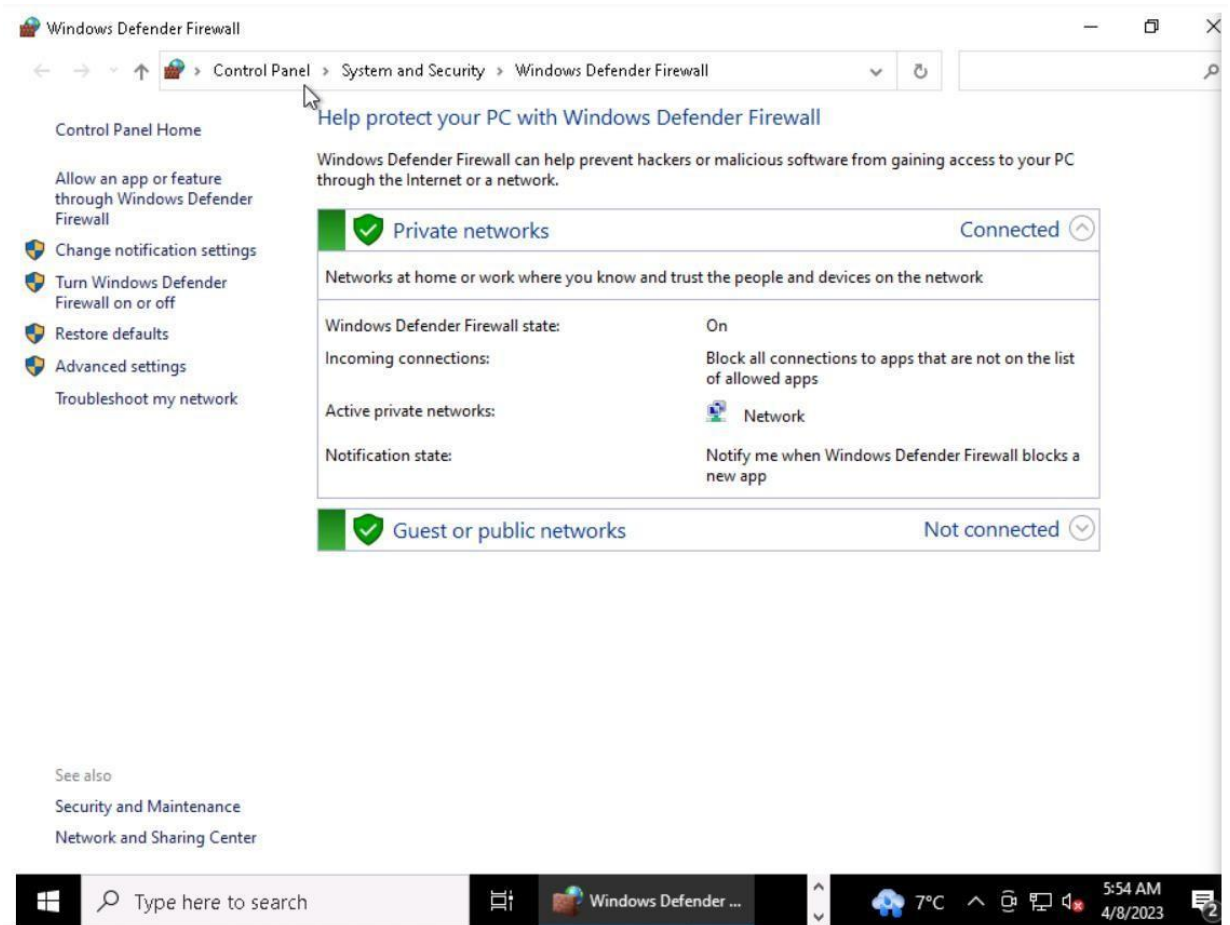
- Securing Removable Media

Firewall

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

1. *Explain the process you take to do this.*
2. *Include screenshots showing the firewall is turned on.*
3. *What protection does this provide?*

First, I clicked on the windows button at the bottom left and clicked settings. In the settings search bar, I searched window defender firewall and it gave me an option (Apply the recommended settings) and I clicked on it and the firewall for the private network was turned on



«p» 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.

Firewall would help our PC understand the good type of traffic and the bad type. It prevents any unauthorized access to our PC through the network we are connected in. Turning this on in our settings provides more security for our PC whether it is connected to private or public network.

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.

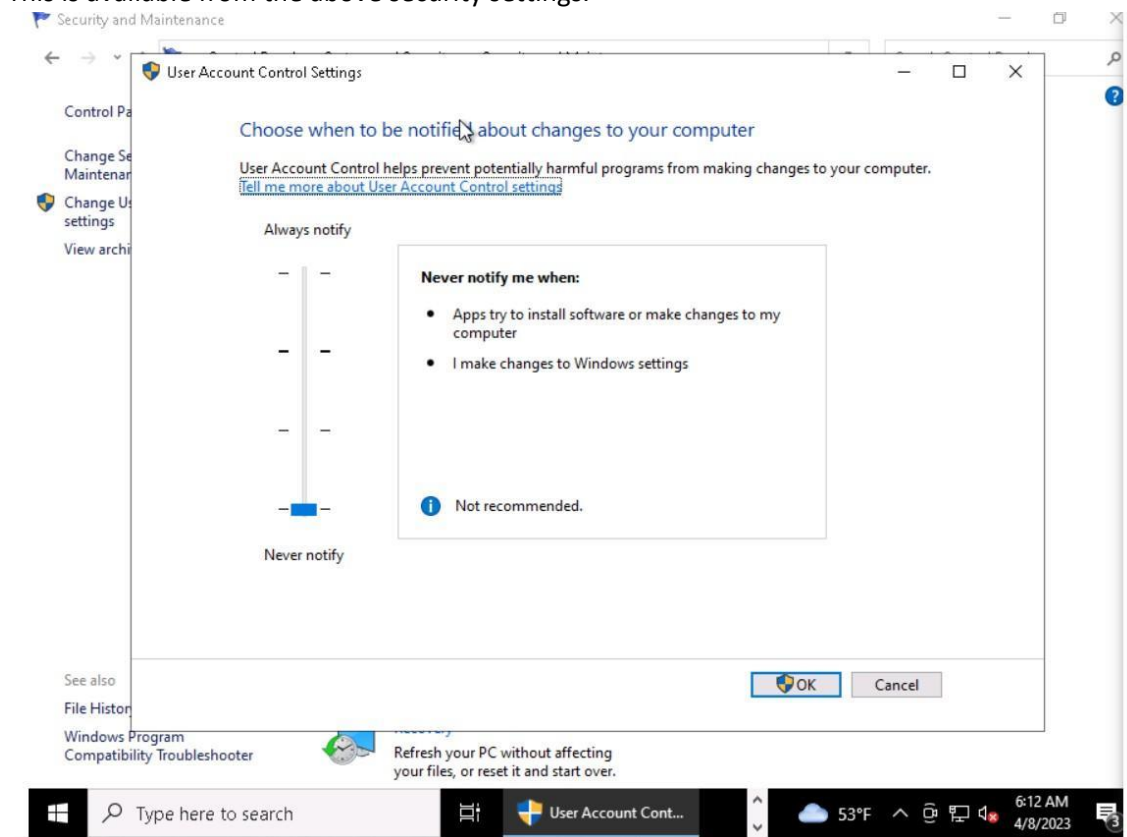
1. *Change the settings to provide **maximum** protection for Joe's PC and provide a screenshot of your results.*

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.

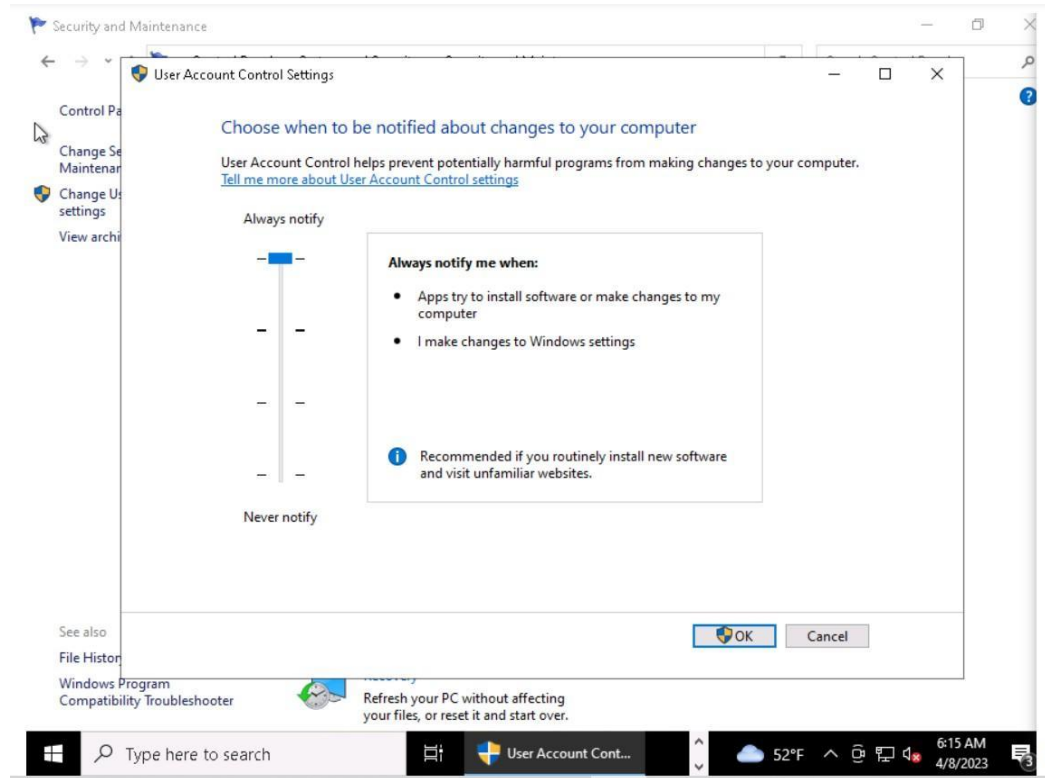
1. *What is the current UAC setting on Joe's computer?*

This is available from the above security settings.



Currently it is set to “never notify” when any setting in windows are changed and notifications that would come when installing a software in the PC

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

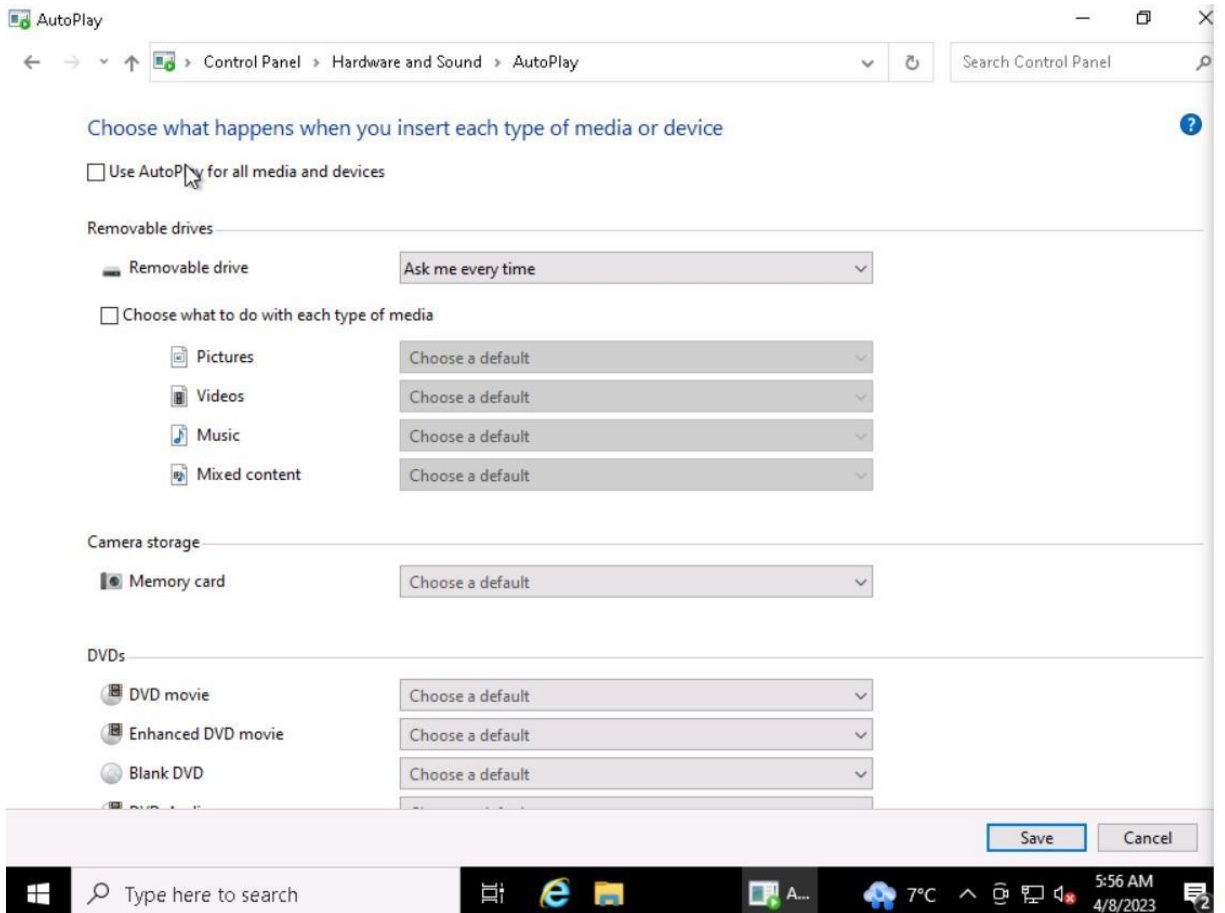


It should be set to notify me whenever any settings in the windows are changed and new software is installed in order to keep track of all the changes that have been made to the PC

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 and Hacker are the accounts that are not supposed to be in Joe PC

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

I right-clicked on the name that is present within the computer management app within the users file and it gave an option "delete". A pop up dialog box appeared and I clicked ok reading the terms and users was deleted

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

Unwanted users having access to sensitive data is harmful for any type of business information that are stored within the PC. It is possible that these data would be leaked so easily if these unauthorized accounts have access to them.

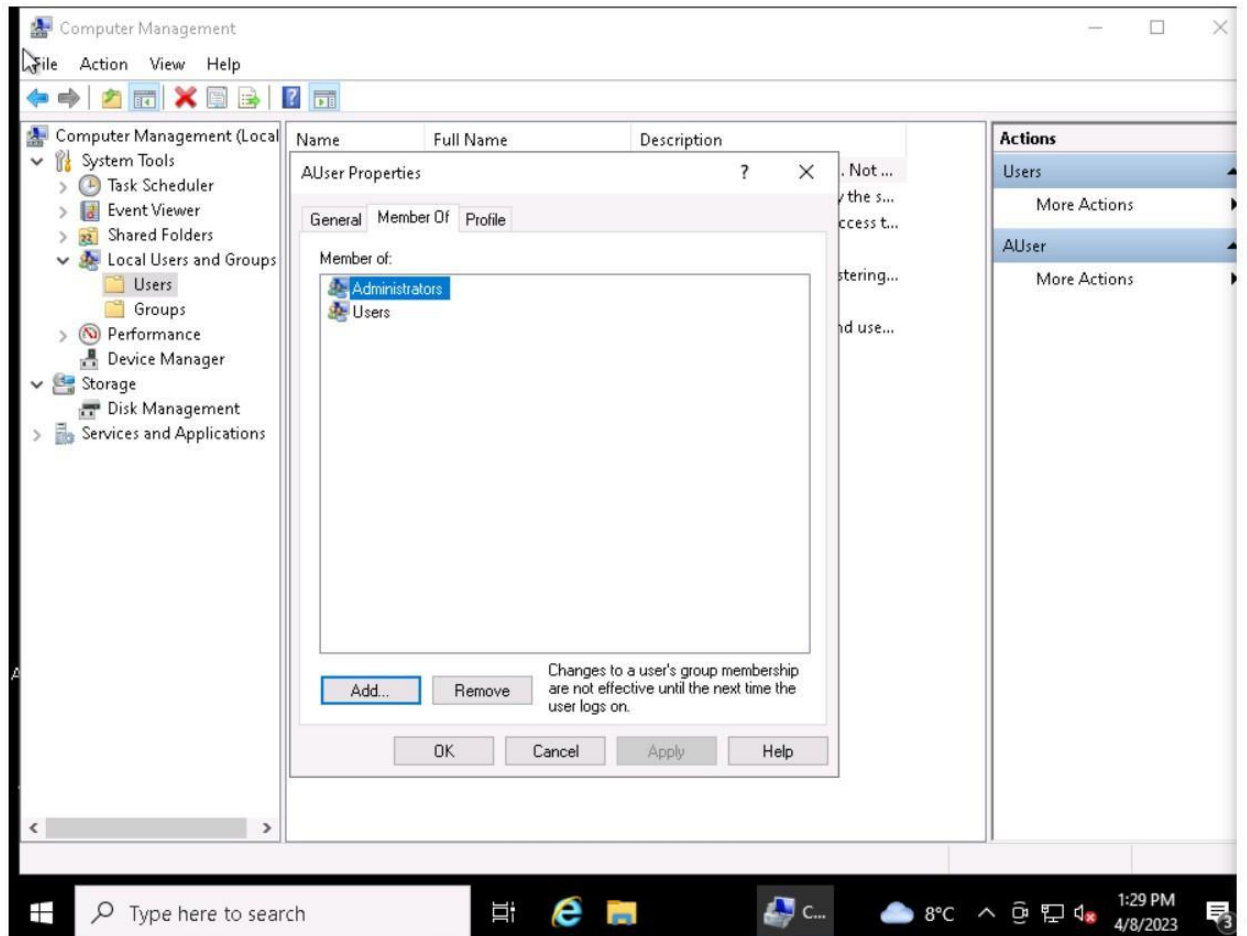
Only specific accounts should have administrator privileges. This reduces the ability for unwanted applications to be installed, including malware.

5. *Which account(s) have administrator rights that shouldn't?*

AUser and Hacker should not have admin rights

6. *Explain how you determined this. Provide screenshots as needed.*

I double clicked the account and in the Member of tab, I got their privilege info.



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.
 - **They would have the ability to change various business requirement settings and would also have the ability to install malicious software that could cause data loss**
 - **This would also lead to changes in business data or probably these data could be encrypted leading to ransomware**
 - **This opens a path for insider attacks as well and how they might take advantage of their privileges in the wrong manner**

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.*

I double clicked the user and within the pop up box, I selected "Member of" and it showed me what type of privileges they have. I clicked on the administrator and clicked the remove button
9. *What is the security principle behind this?*

Integrity is the security principle

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

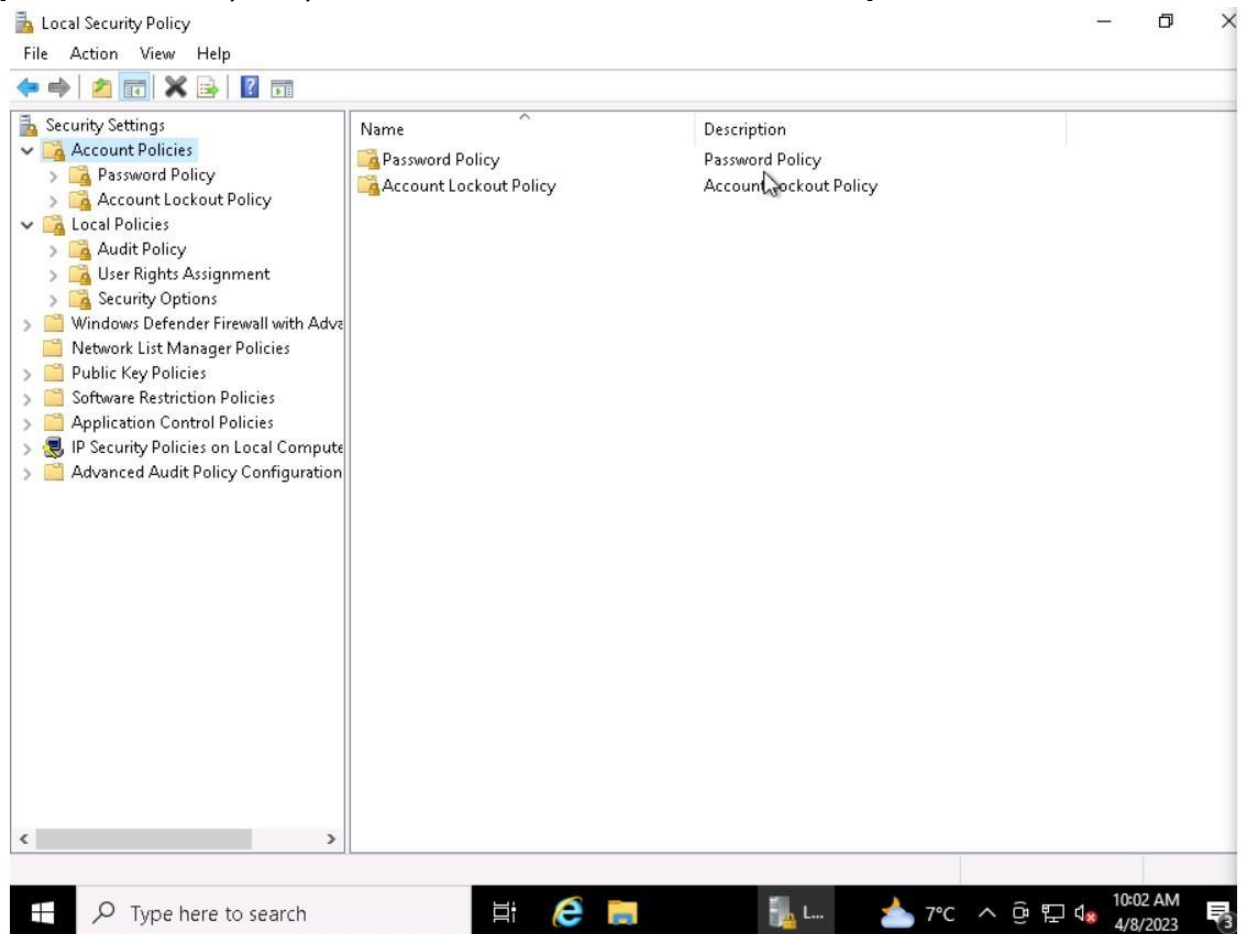
CIS Control 6 - Access Control Management is the control that this step fulfills. In this step, we are removing privileges to account that does not require it and giving only admin access to the ones that are authorized.

Setting Access and Authentication Policies

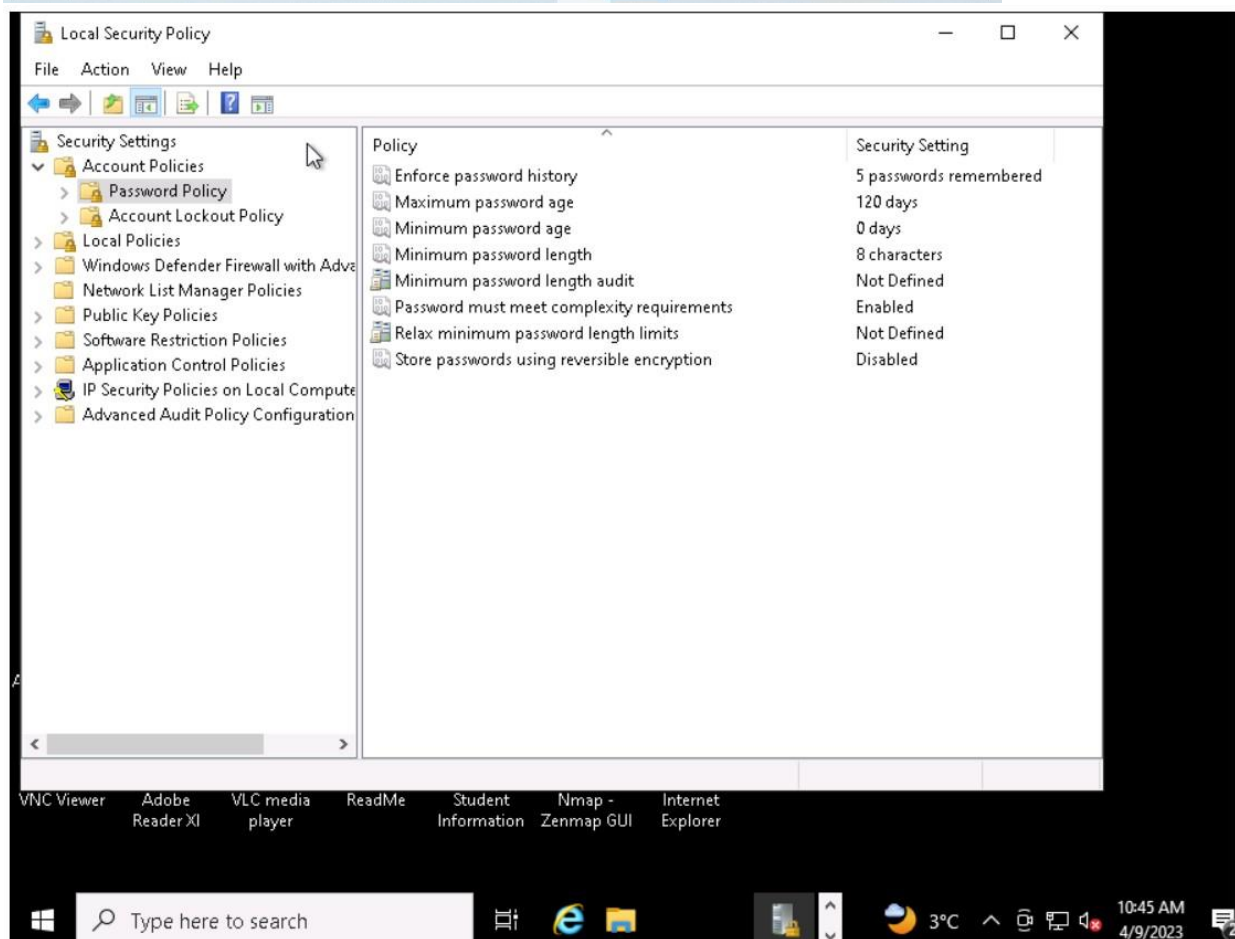
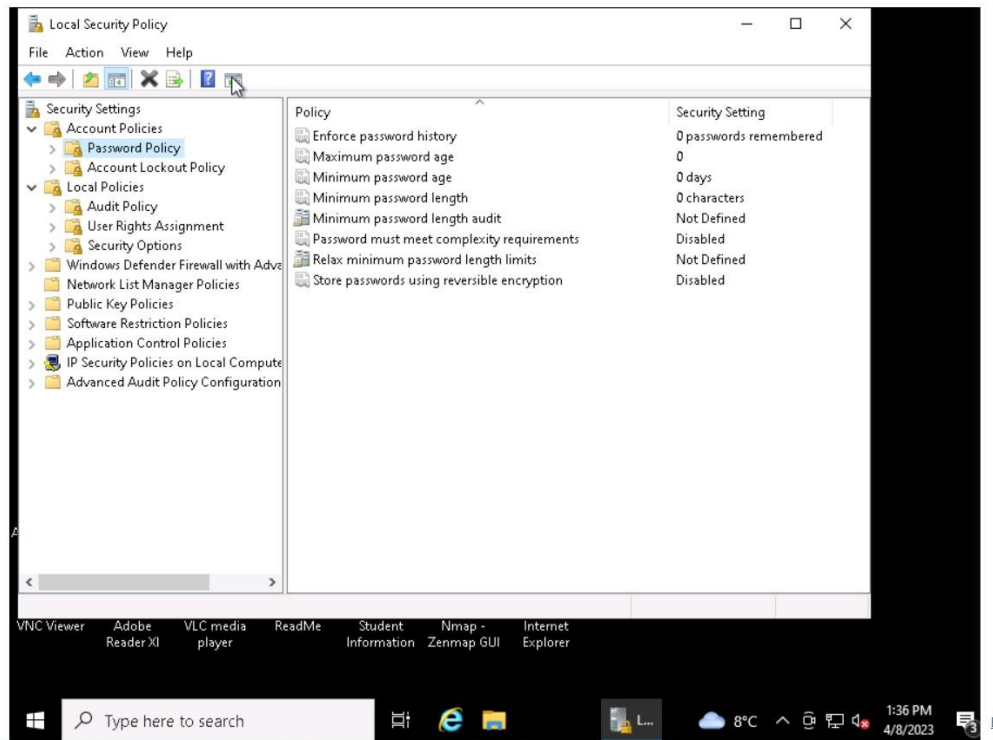
After you talked with Joe about security, he has asked that the access rules outlined above be in place on his PC. These are set using the Local Security Policy function in Windows 10. On the Windows search bar, type “Local Security Policy” to access it. Click the > arrow next to both “Account Policies”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

1. Provide a screenshot of the Local Security Policy window here.

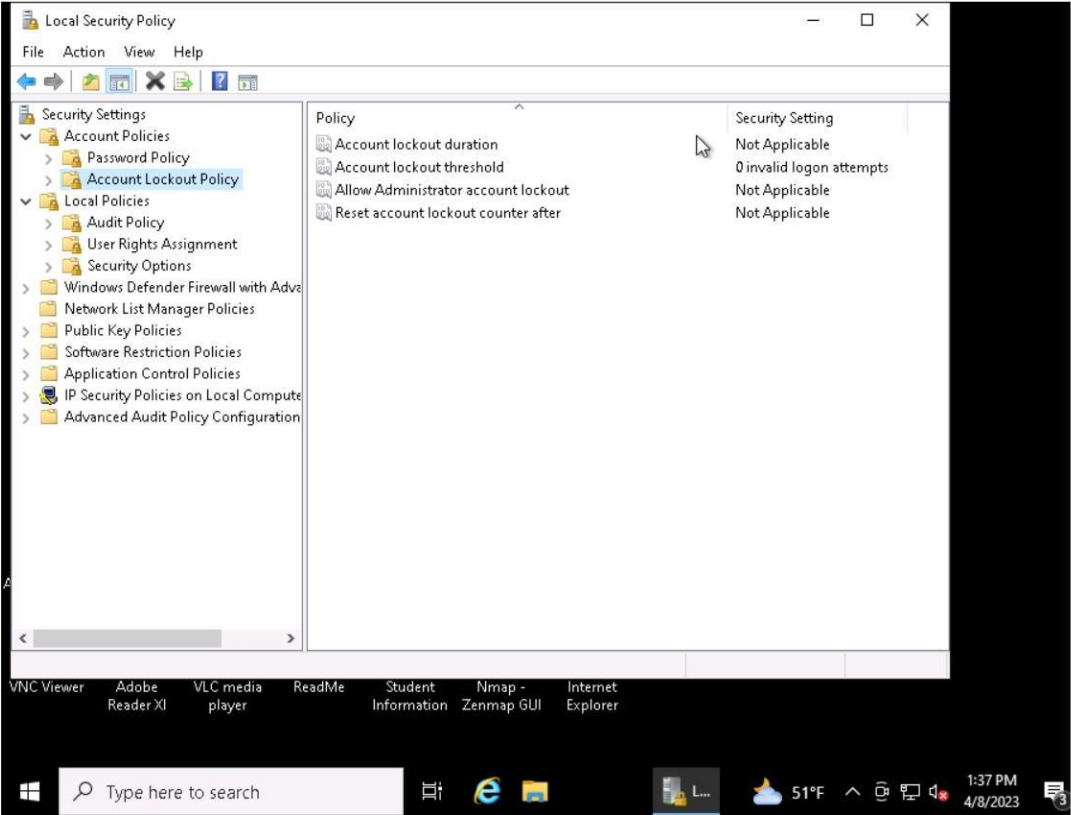
[Note: Local Security Policy is not available on Windows 10 Home edition.]

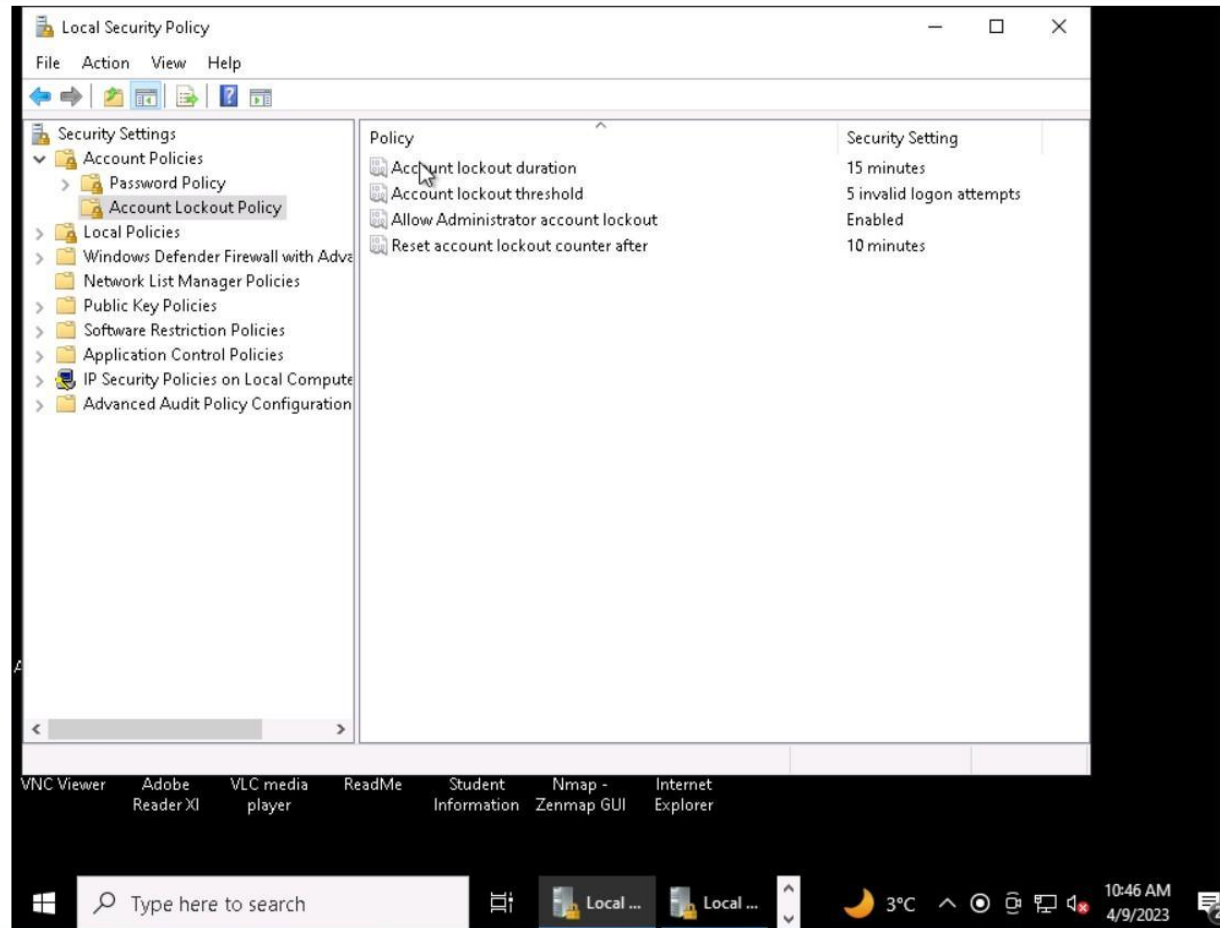


2. Explain the process for setting the password and access control policies locally on a Windows 10 PC. Provide screenshots showing how you set the rules on the PC.



Setting the Account Lockout Policy:

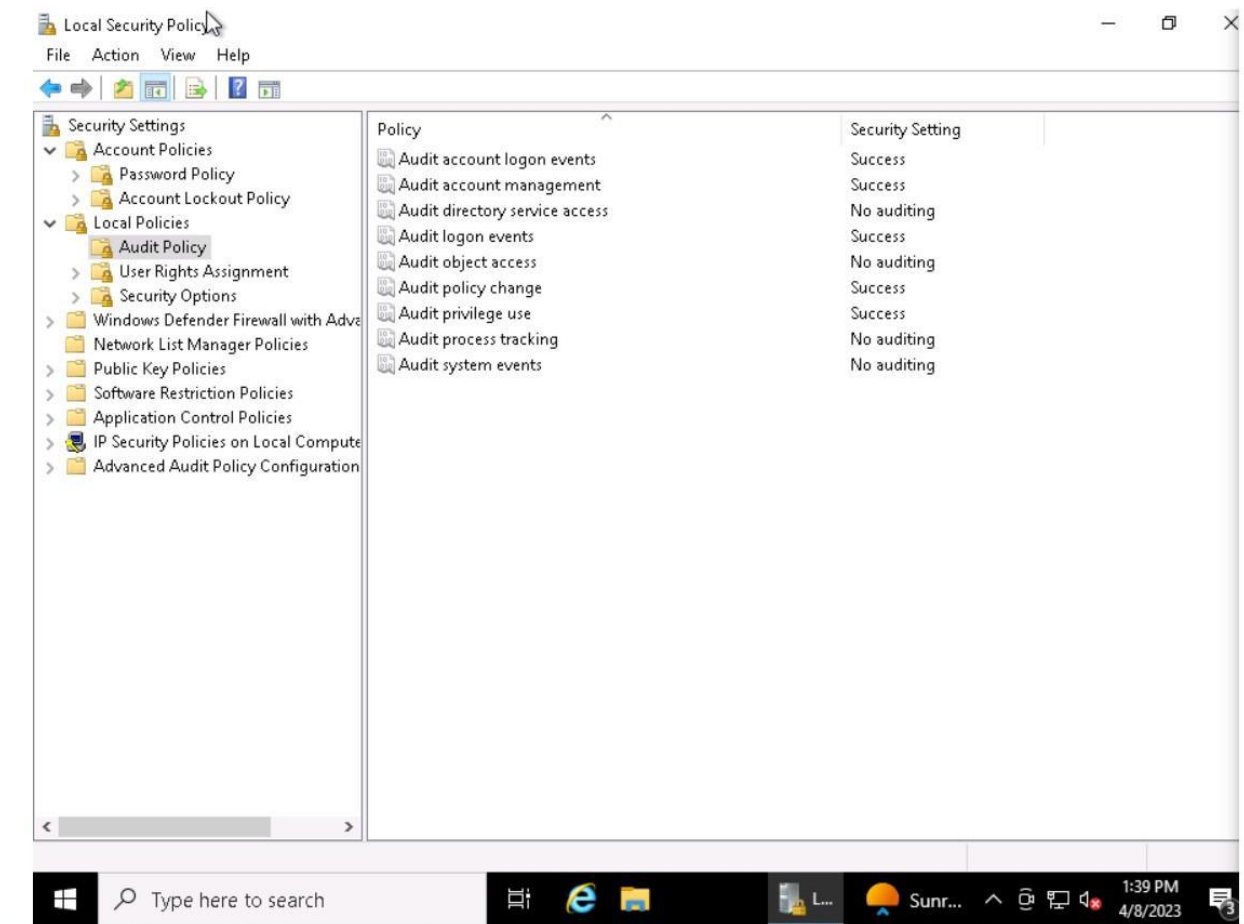




Auditing and Logging

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

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



4. Securing Applications

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

Joe has established the following rules regarding PC applications:

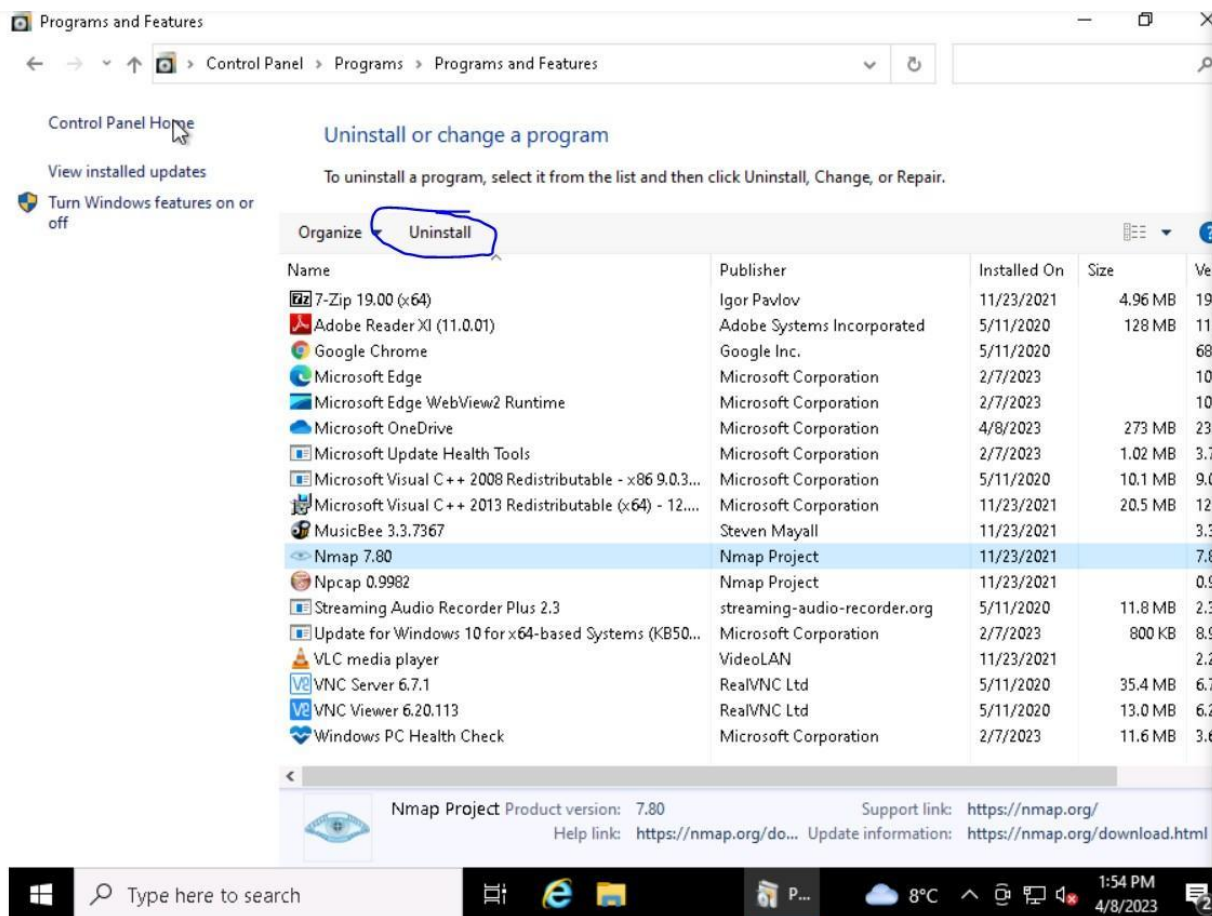
- Joe wants everyone to use the latest version of the Chrome browser by default.
- There should be no games or non-work-related applications installed or downloaded.
- Joe is also concerned that there are “hacking” programs downloaded or installed on the PC that should be removed.
- This PC is used for standard office functions. The auto-body has a separate service they use for their website and to transfer files from their suppliers.

Remove unneeded or unwanted applications

1. *List at least three application(s) that violate this policy.*
 - **NMap 7.80**

- Npcap 0.998
 - 7-Zip 19.00
2. Name at least three vulnerabilities, threats or risks with having unnecessary applications:
 - Unauthorized apps would make the PC more vulnerable because it could have malware code infested in the app which is a major threat
 - These apps could also have a backdoor for the hackers to find easy access to the system
 - These apps would also be like running in the background and they collect a large amount of data from users
 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.

From the control panel we would be able to see the apps present in Programs and Features. From here, select one app and there is an option above to uninstall

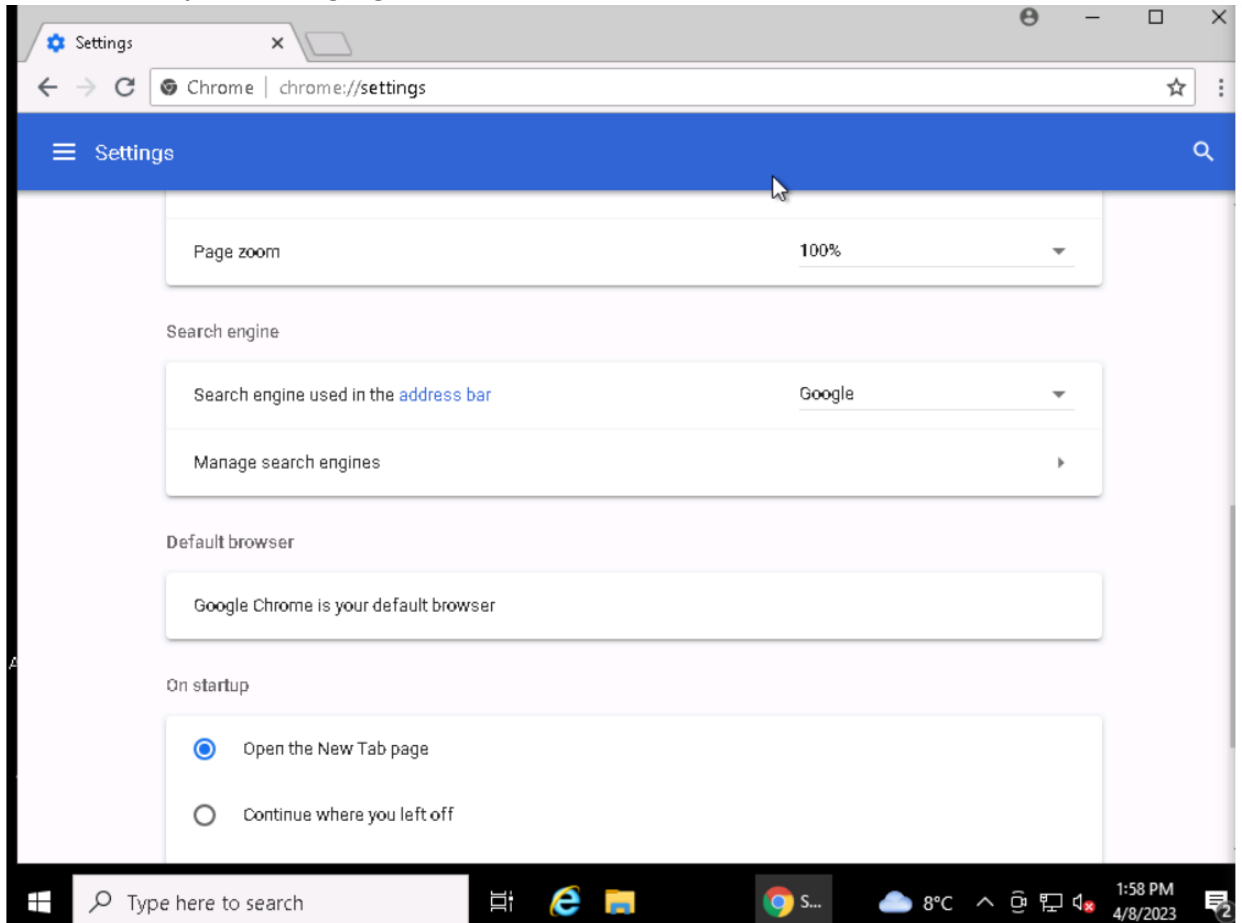


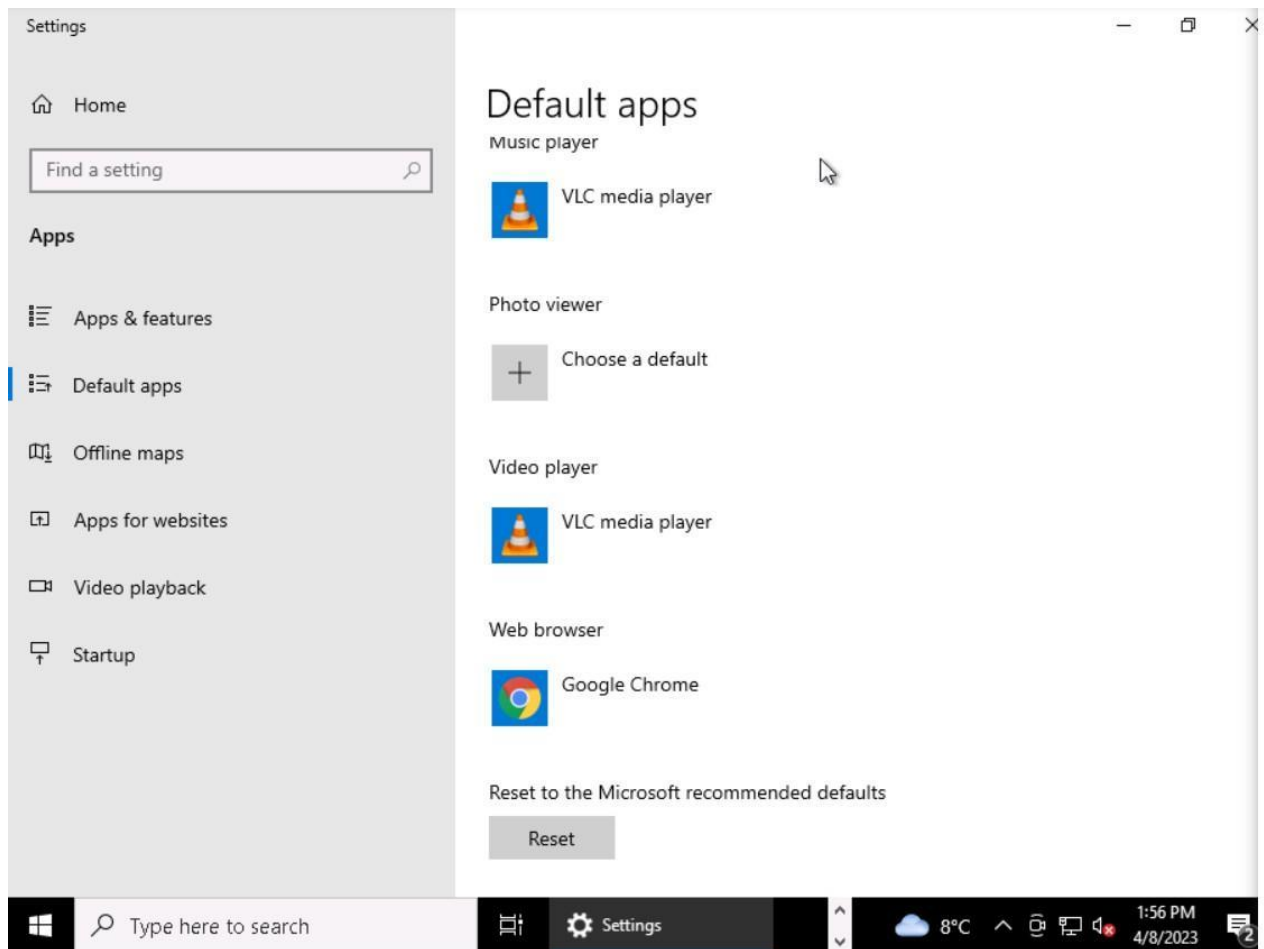
Default Browser

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.

I clicked onto google and went to their settings and below that they had an option to make google default so I clicked it and it opened in settings window and I was able to swap out internet explorer with google

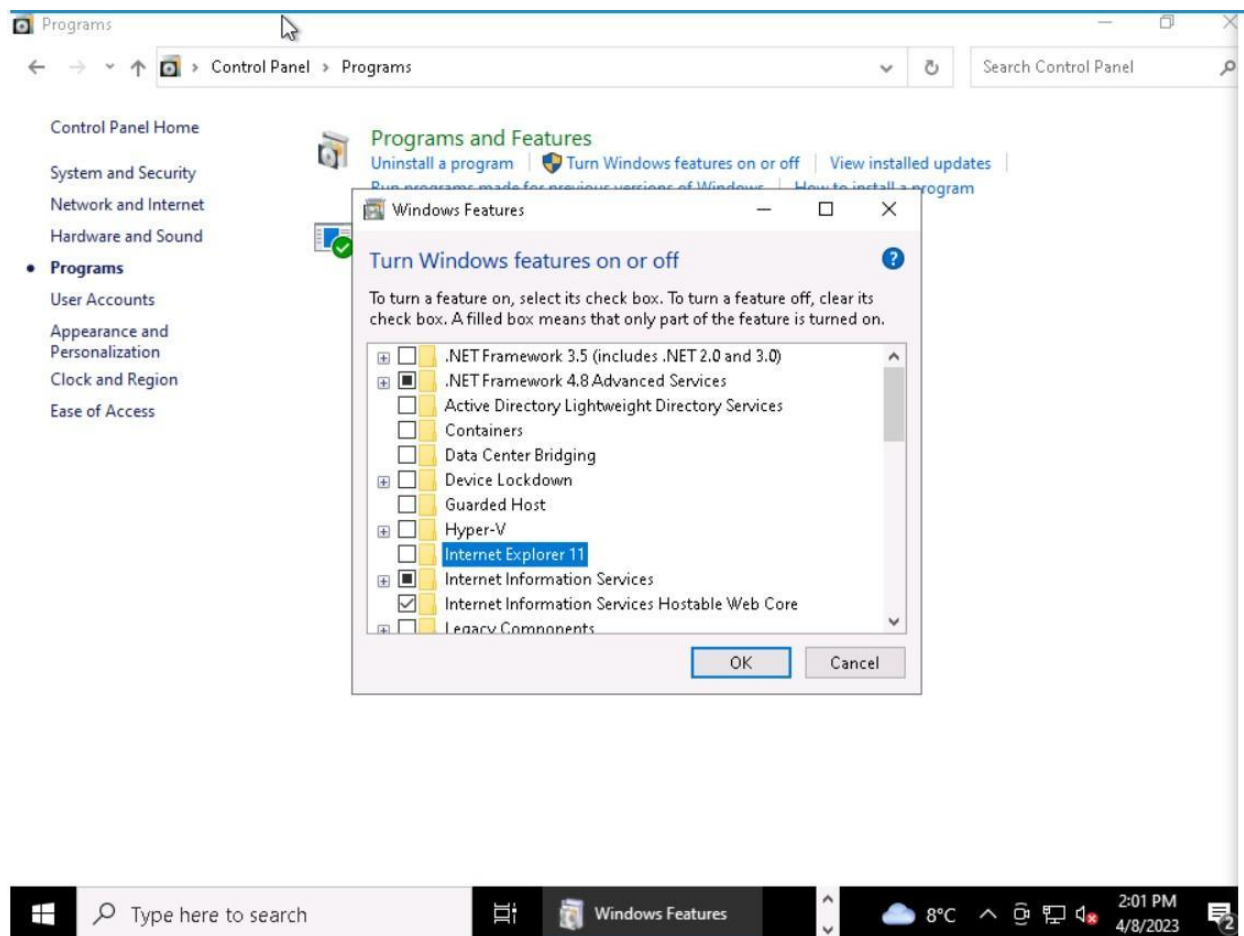




2. *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
 - **It does not have any more updates so it could cause PC to be vulnerable**
 - **An outdated web browser have multiple patches that are not fixed. So using this browser could cause unauthorized access to PC**

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.*

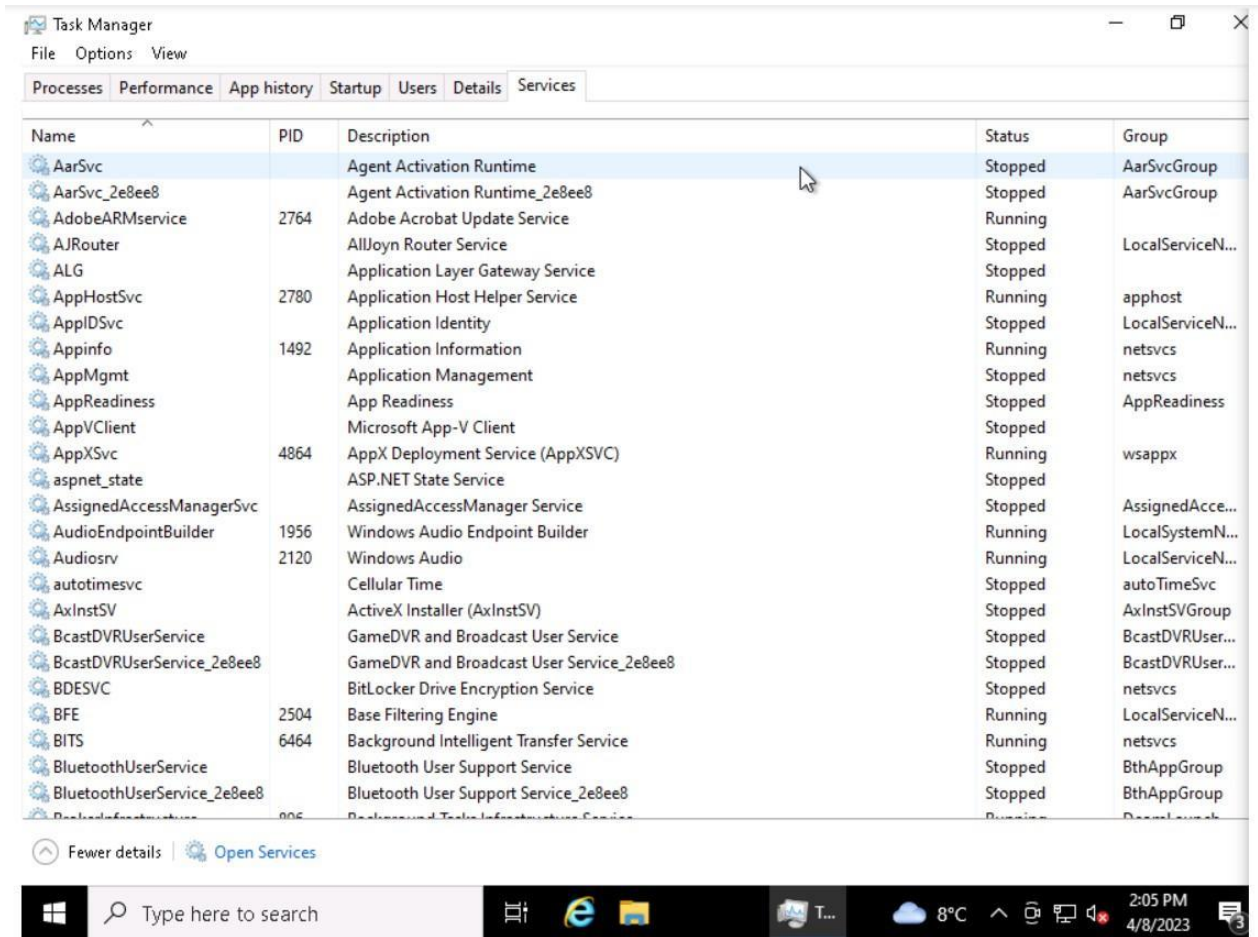


Windows Services

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.

In the search bar, I typed in services and the services window opened up.



- Advanced users should provide at least two methods for determining a web server is running on a host

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name	PID	Status	User name	CPU	Memory (a...	UAC virtualizat...
svchost.exe	5492	Running	LOCAL SE...	00	508 K	Not allowed
svchost.exe	672	Running	LOCAL SE...	00	604 K	Not allowed
svchost.exe	6824	Running	LOCAL SE...	00	416 K	Not allowed
svchost.exe	2384	Running	SYSTEM	00	2,012 K	Not allowed
svchost.exe	1592	Running	LOCAL SE...	00	1,872 K	Not allowed
svchost.exe	7124	Running	LOCAL SE...	00	656 K	Not allowed
svchost.exe	5744	Running	LOCAL SE...	00	1,292 K	Not allowed
svchost.exe	5248	Running	SYSTEM	00	2,208 K	Not allowed
svchost.exe	3696	Running	SYSTEM	00	596 K	Not allowed
svchost.exe	2772	Running	SYSTEM	00	1,268 K	Not allowed
svchost.exe	6600	Running	SYSTEM	00	452 K	Not allowed
svchost.exe	5876	Running	JoesAuto	00	2,340 K	Not allowed
svchost.exe	7108	Running	JoesAuto	00	4,992 K	Not allowed
svchost.exe	5564	Running	SYSTEM	00	868 K	Not allowed
svchost.exe	6748	Running	SYSTEM	00	1,716 K	Not allowed
svchost.exe	7536	Running	JoesAuto	00	1,556 K	Not allowed
svchost.exe	9064	Running	SYSTEM	00	1,276 K	Not allowed
svchost.exe	2208	Running	JoesAuto	00	1,952 K	Not allowed
svchost.exe	2200	Running	SYSTEM	00	3,248 K	Not allowed
svchost.exe	8308	Running	SYSTEM	00	928 K	Not allowed
svchost.exe	7356	Running	LOCAL SE...	00	1,124 K	Not allowed
svchost.exe	1492	Running	SYSTEM	00	1,248 K	Not allowed
svchost.exe	6464	Running	SYSTEM	00	5,372 K	Not allowed
svchost.exe	7732	Running	SYSTEM	00	1,140 K	Not allowed
svchost.exe	6032	Running	SYSTEM	00	3,848 K	Not allowed

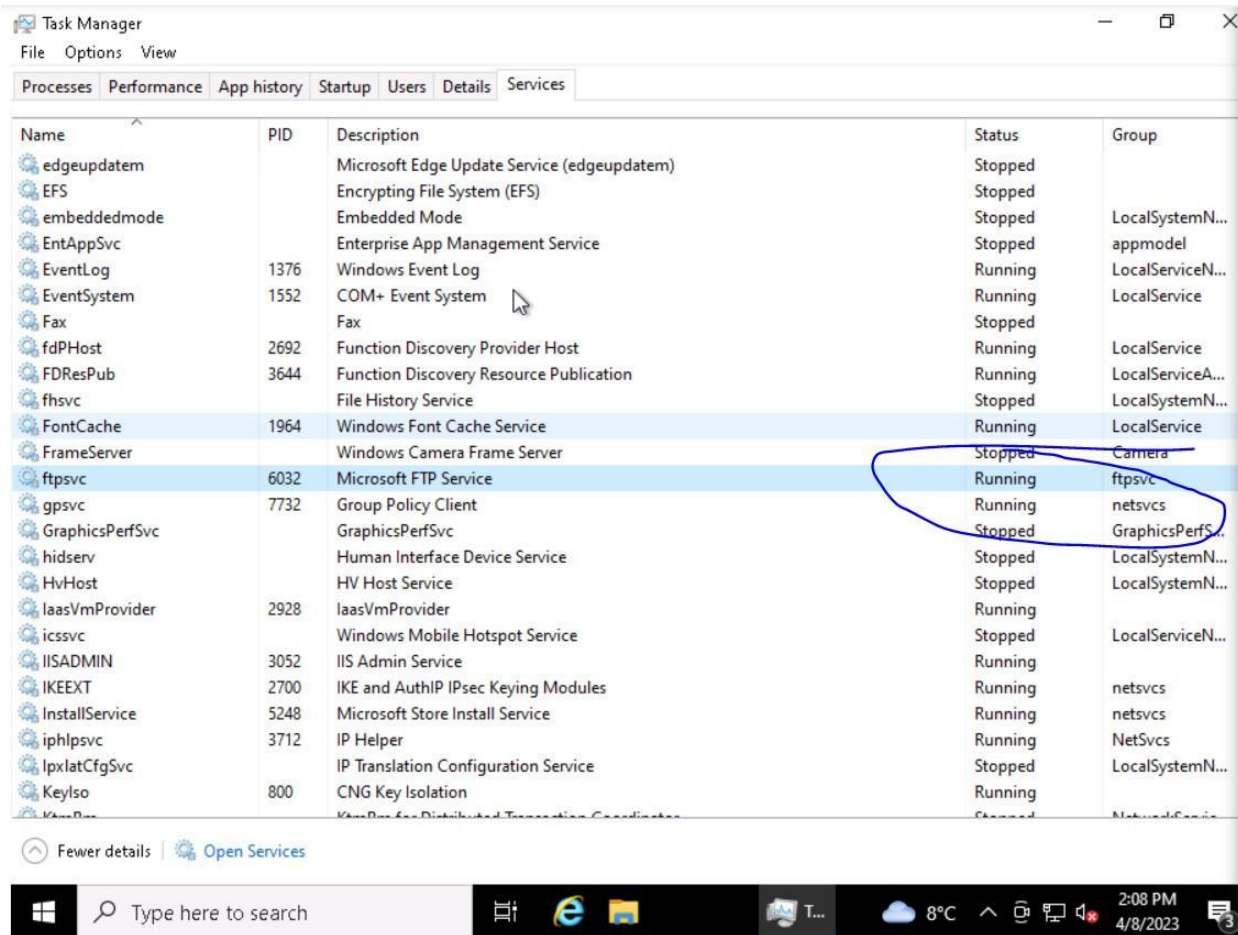
Fewer details

End task

Type here to search

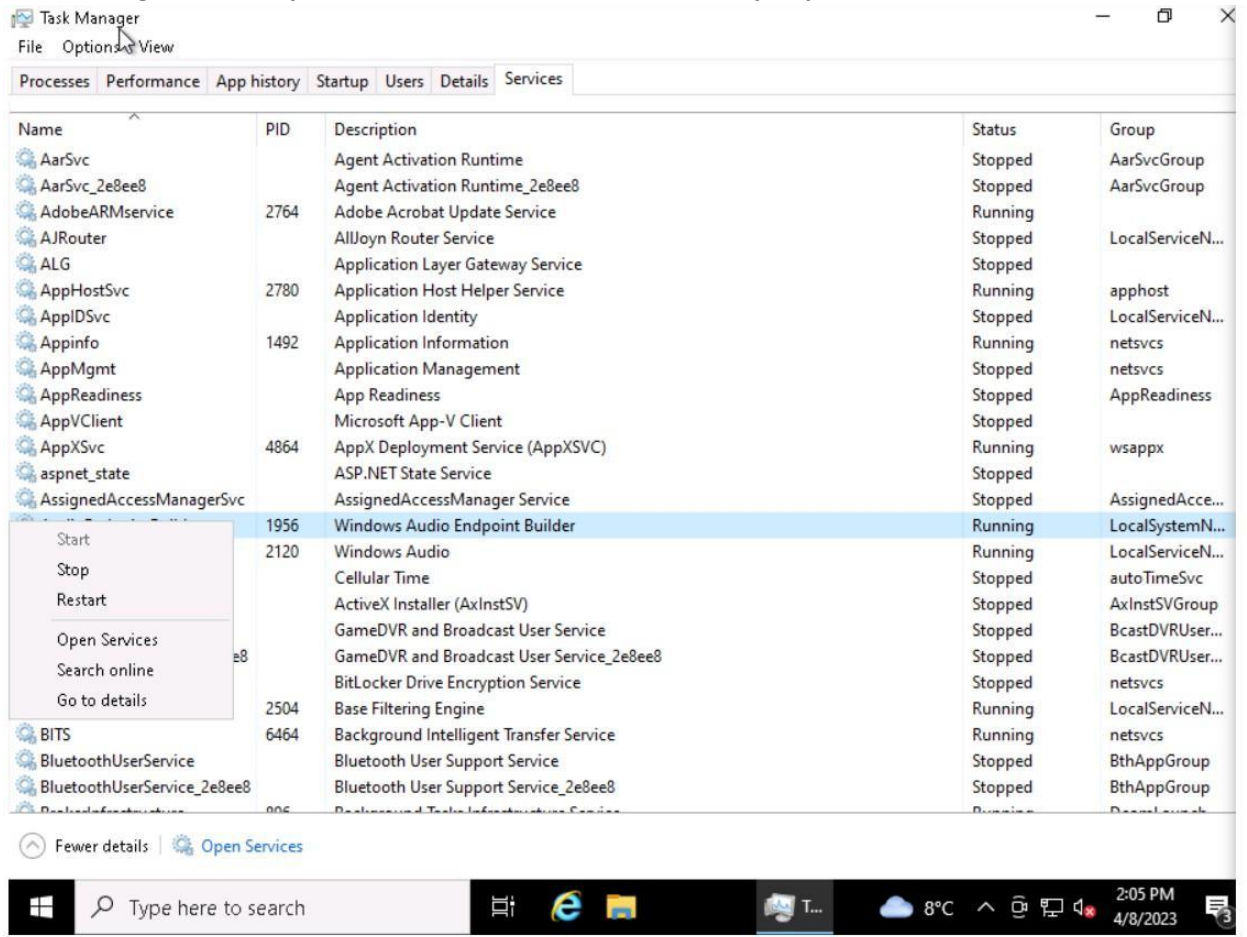
8°C

2:07 PM
4/8/2023

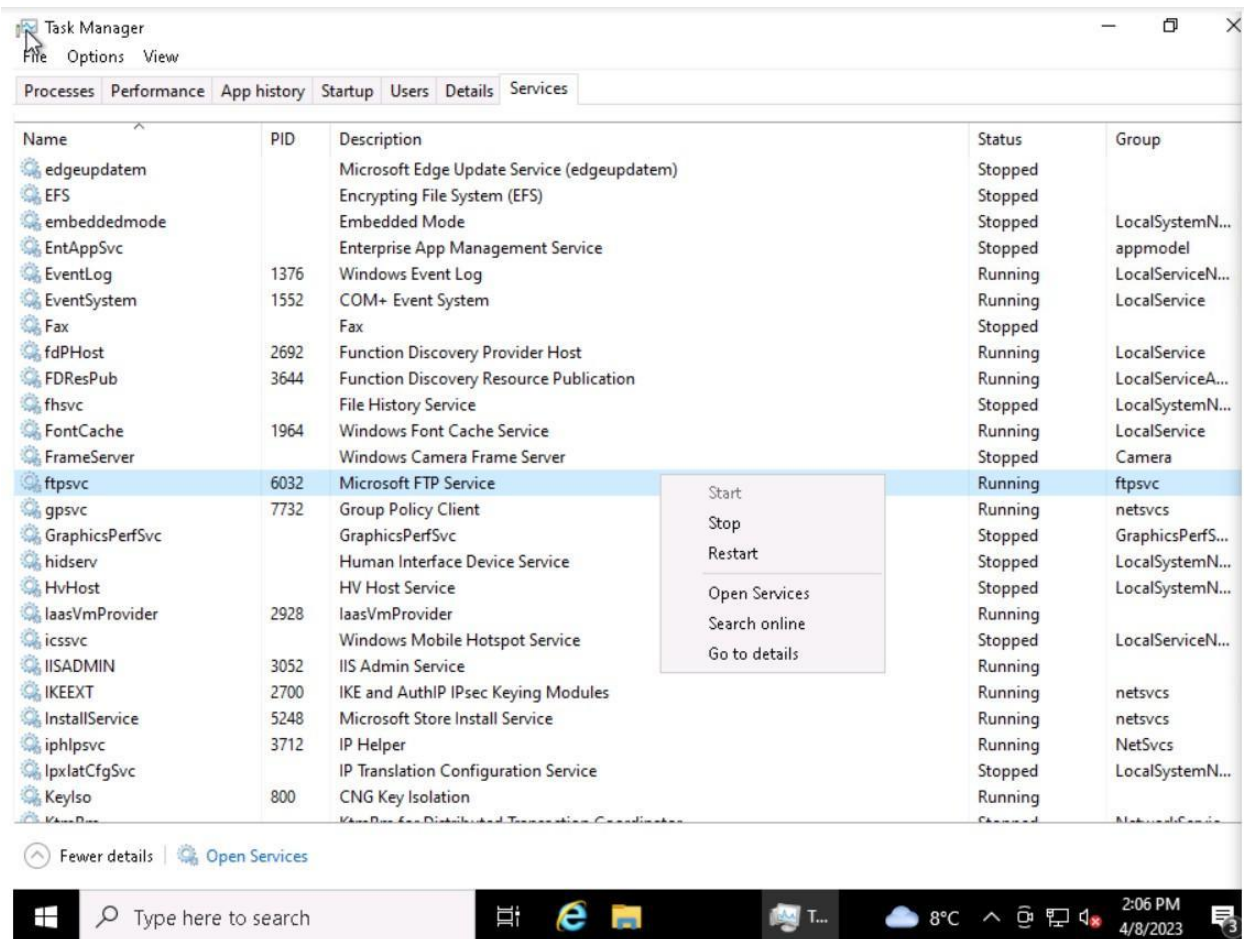


3. How do you disable them and make sure they are not restarted?

Right click the particular service and click on the “stop” option



- 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.

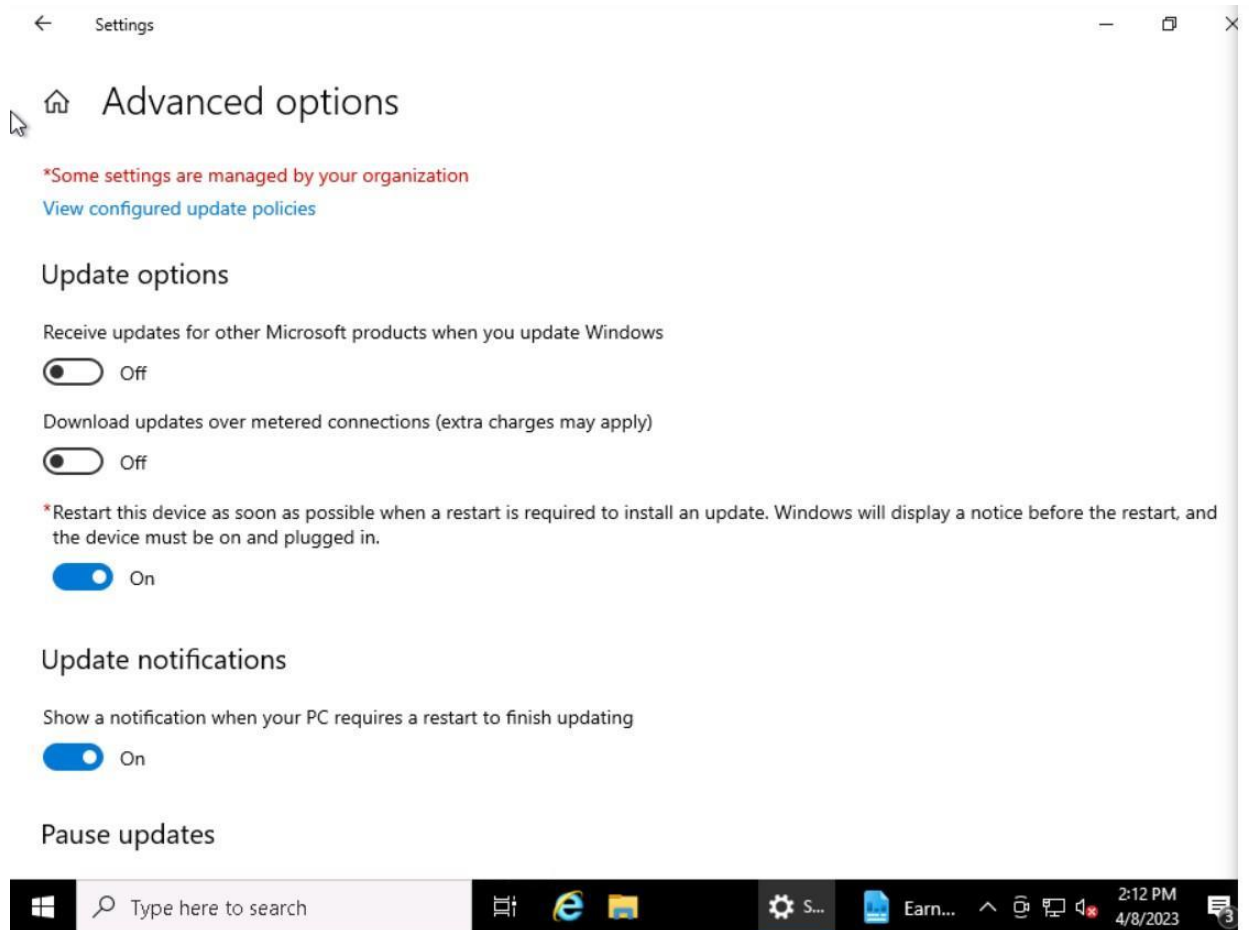


Patching and Updates

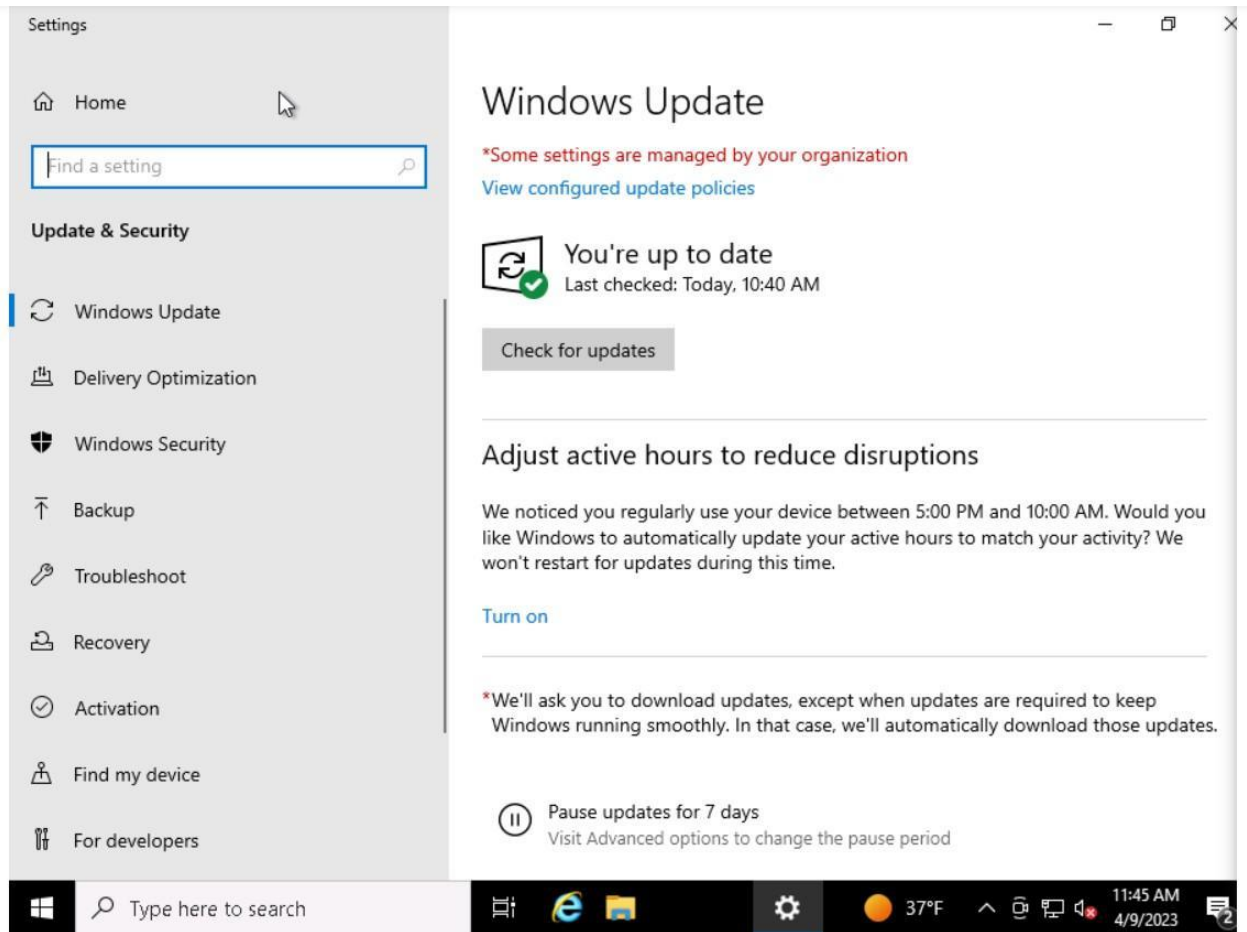
Keeping the operating system current on patches and fixes is a critical part of security. Joe wants his PC to be on the latest version of Windows 10. He also wants you to set it up for automated updates.

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

I clicked on the windows at the left bottom and then clicked the settings button.
After the setting panel open, I clicked on Updates & Security. I clicked on Advanced Settings, and turned on automatic update



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.

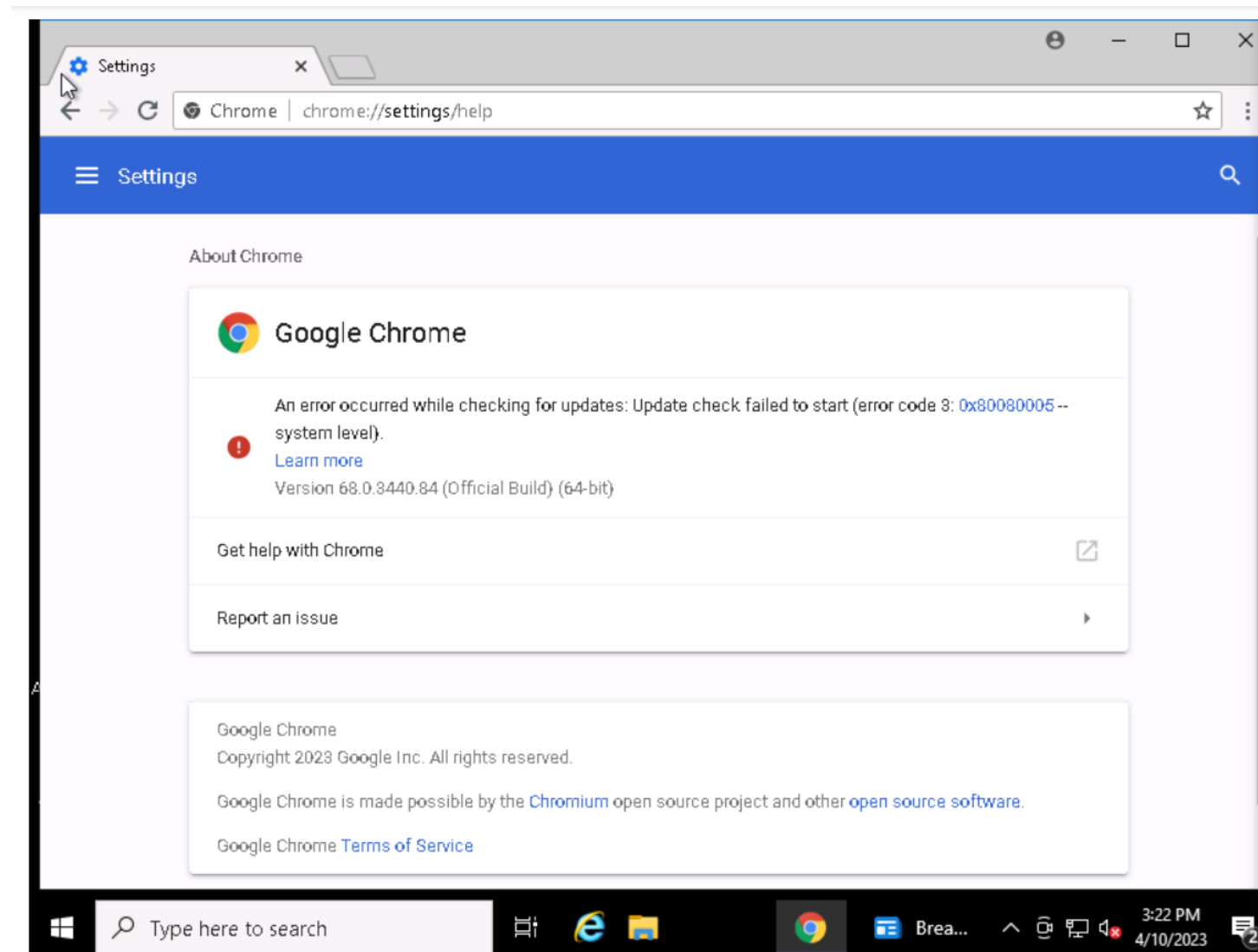
3. *List at least two applications on Joe's PC that are out of date. List them below:*

- Google Chrome
- NMap 7.80

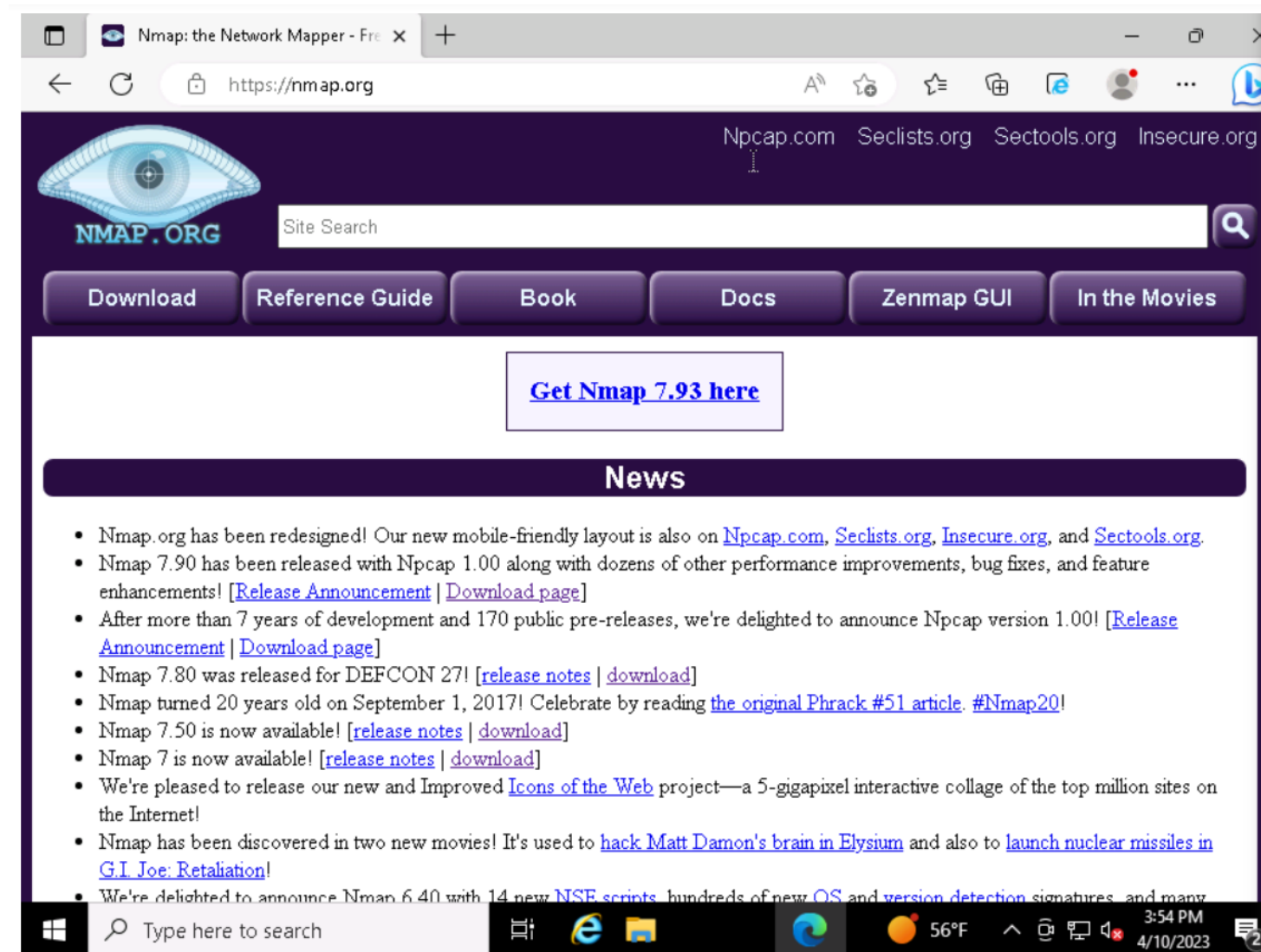
4. Explain the steps you took to determine this information.

I checked the apps that first even existed in the Programs and Features in the Control Panel. It displayed the version of each app on the far right. Based on that, I searched a few of the apps on the internet and found their official vendors. Newer version about that apps are displayed in their respective websites and hence helped me analyze which of the application was outdated

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

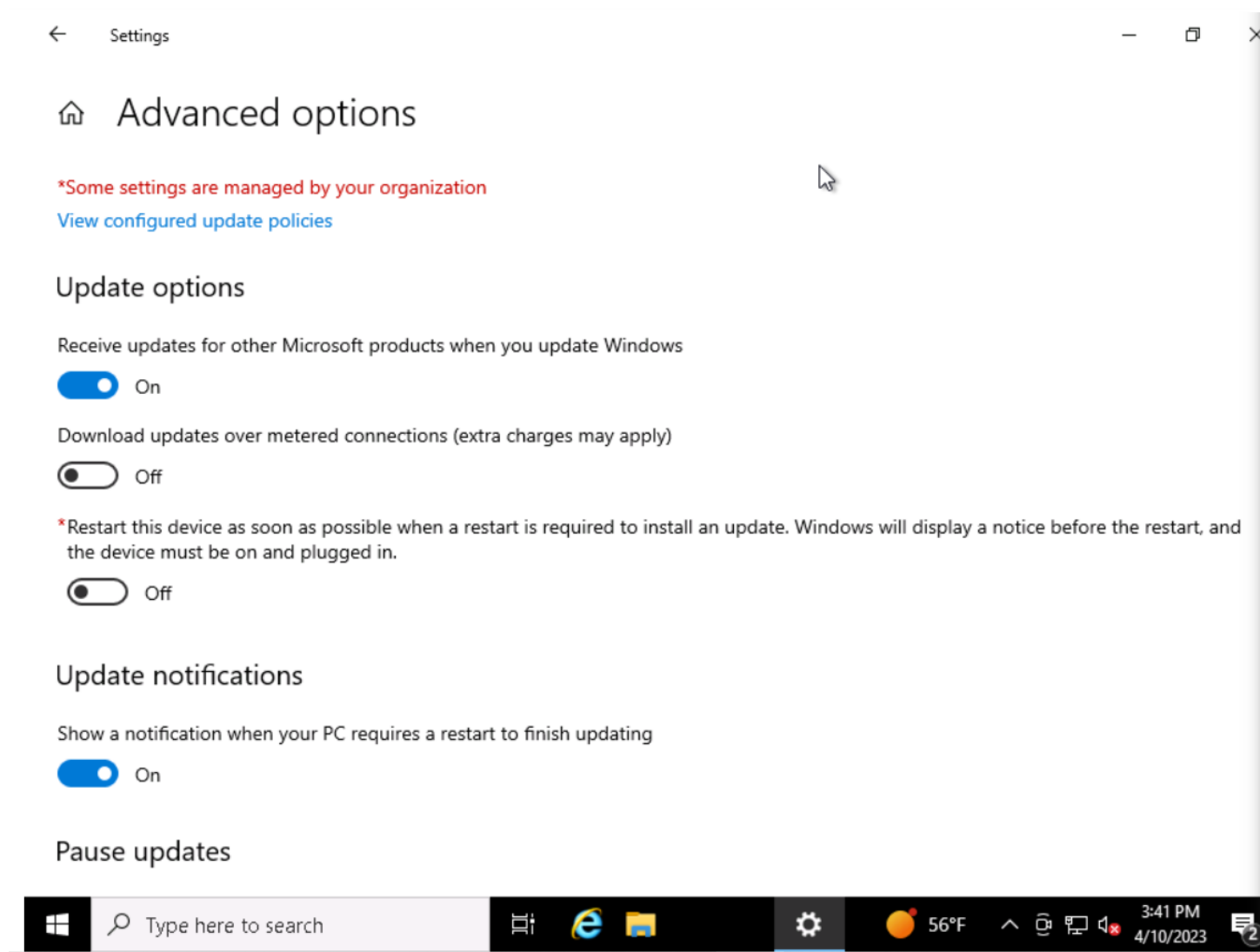


Google is showing some error for checking about its update. The current version in Joe's PC is 68.0.3440.84 but the newest latest version of google is 110.0.5481.178. But here when a user open google chrome they should click the three dots at the top right and click settings and click "about google"



For Nmap i visited their official website and based upon their latest version we would be able to download them and update our application as often as needed.

Additionally, we can turn on automatic updates for other microsoft apps when you update windows



5. Securing Files and Folders

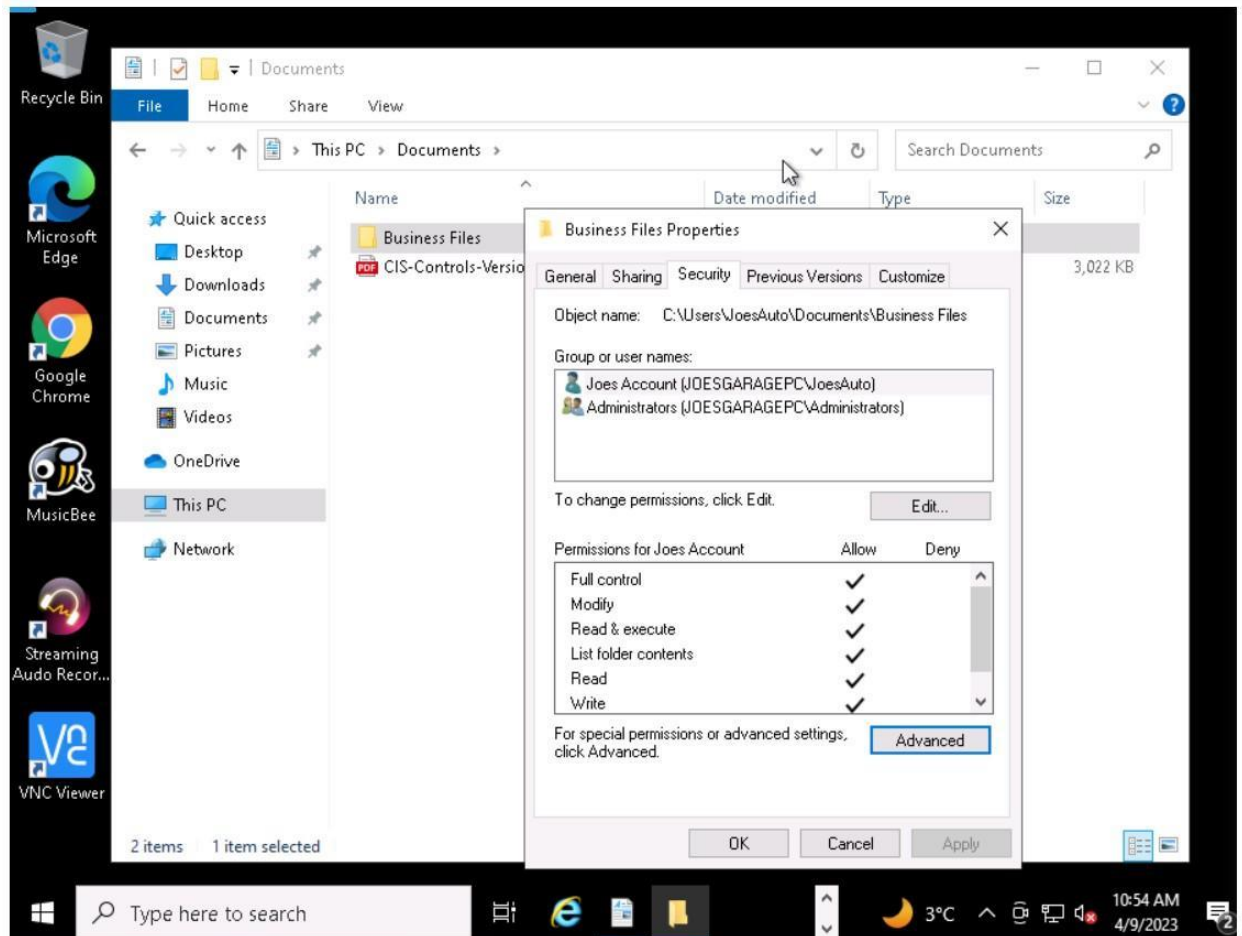
Joe has some work files in his Business folder that he wants to secure since they contain his customer information. They are labeled "JoesWork."

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

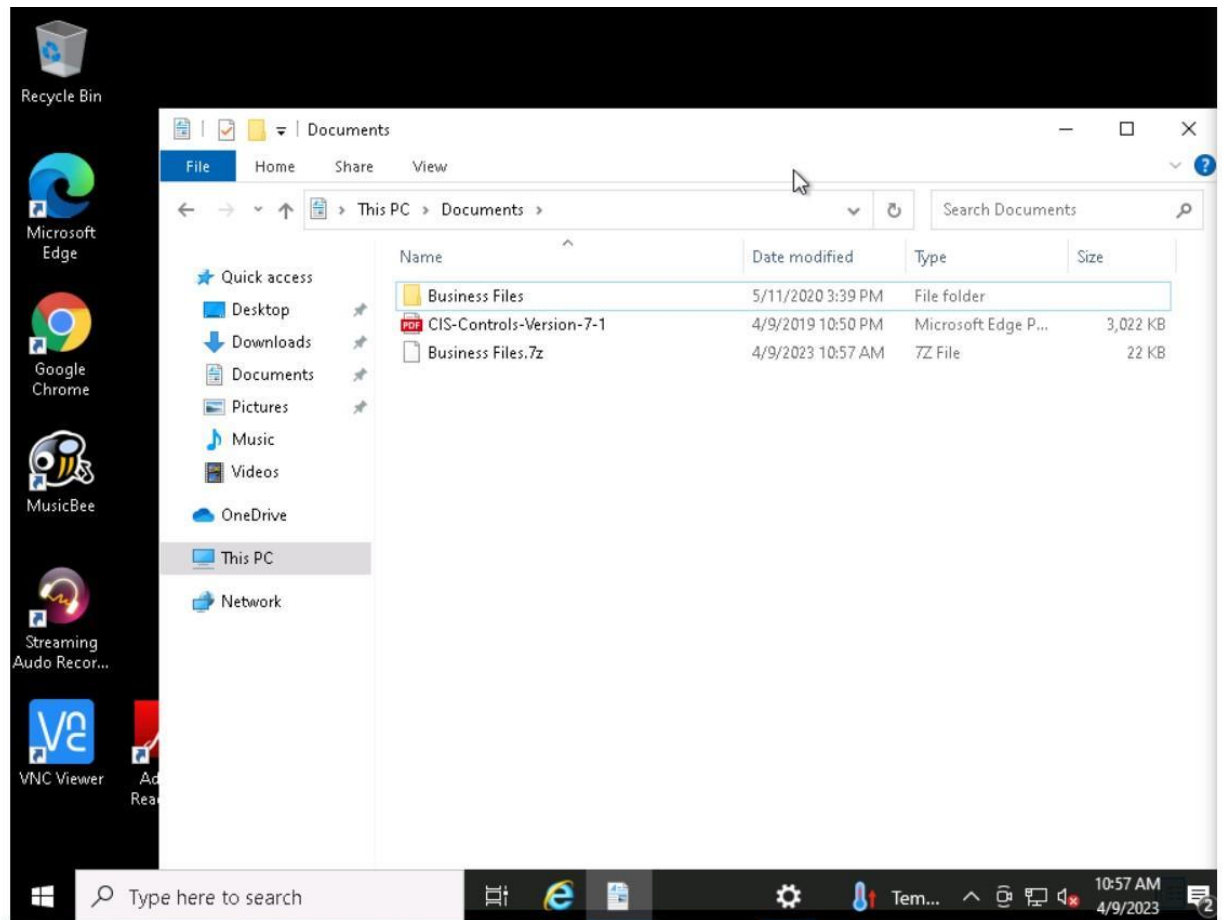
1. Explain the process for checking this and changing any necessary settings on the file. Include screenshots showing that **ONLY** Joe and Jane have permissions to change Joes work files. [Hint: Right-click the folder and select Properties.]

I right clicked on the folder and in the properties there was a security tab. In there, it showed a list of people who had access to the file and I simply removed them



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.

I right clicked the file and with a 7-ZIP option I was able to click on the "Add to archive" and then entered the password at the bottom and encrypted the file



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?

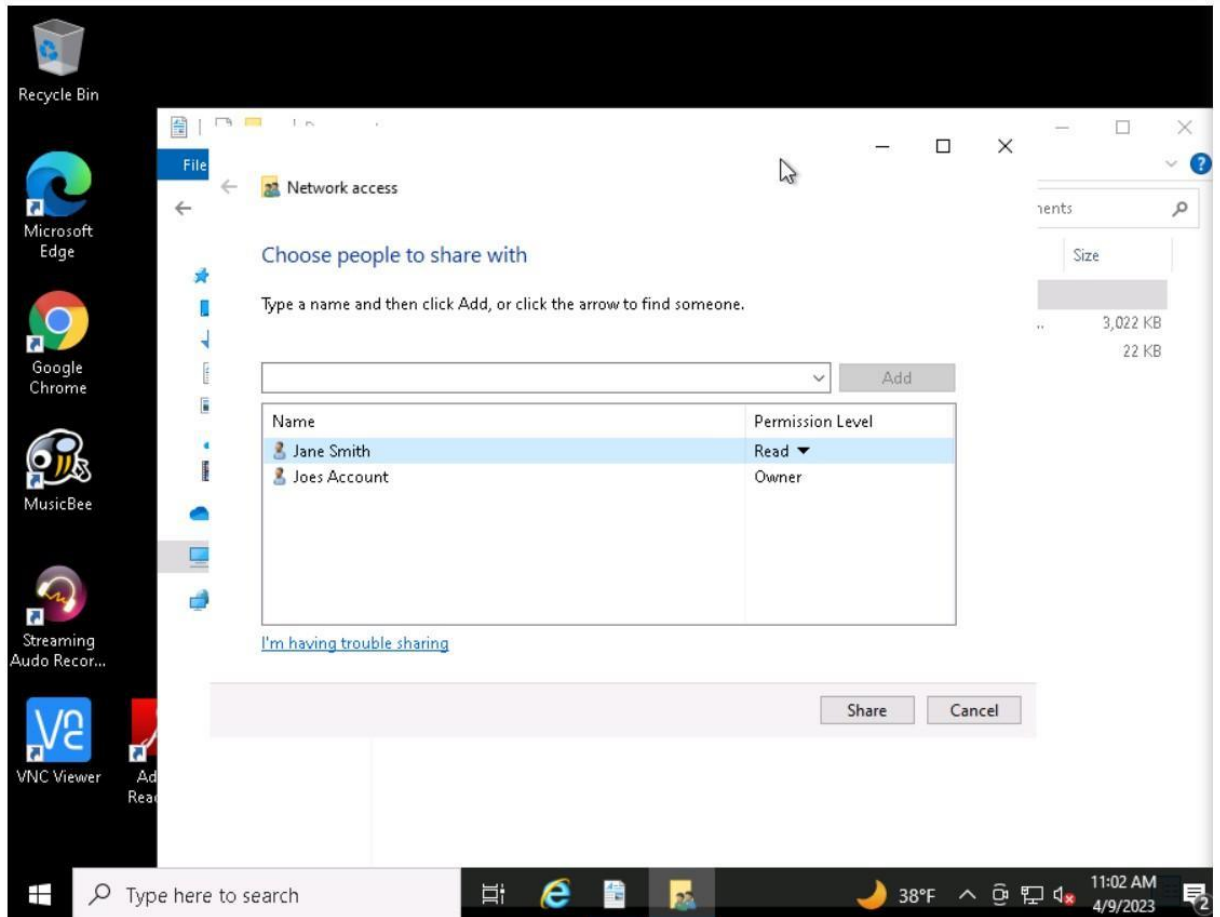
CIS Control 3: Data Protection

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.

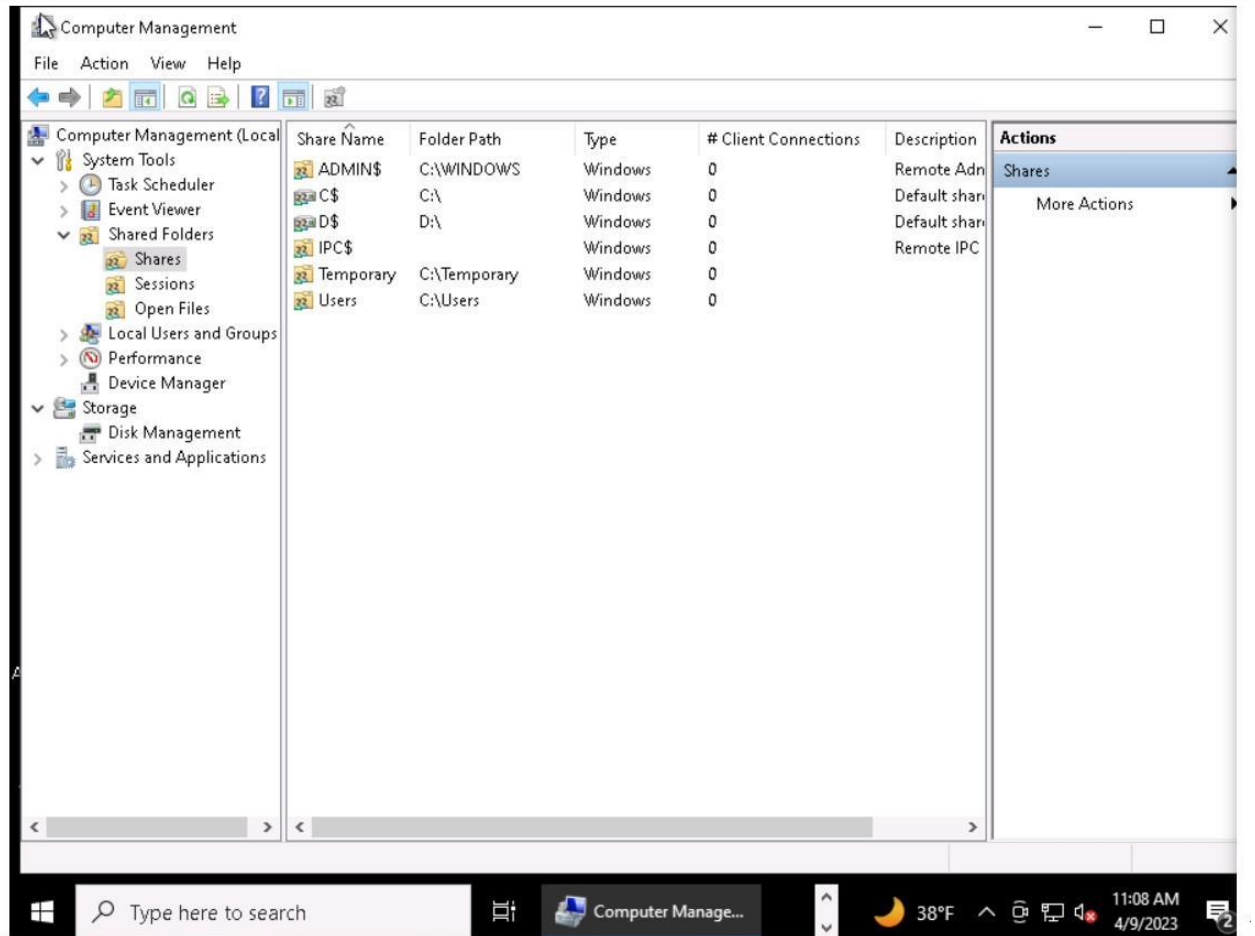
1. Explain how you would do that and provide a screenshot showing how you can do it. Make sure it's only shared between Joe and Jane.

I right clicked on the file and there was option to give access to. I added Jane to the given list and shared the file with her.



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.*

I typed in computer management in the search bar. I clicked the option shared folders and then clicked 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.