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: Sahithi Charitha .Dindukuri

Date of completion: 07/23/2022

Scenario

Congratulations!

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

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

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

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

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

Account Name: JoesAuto
Password: udacityLearning.1!!

1. Reconnaissance

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

Complete each section below.

Hardware

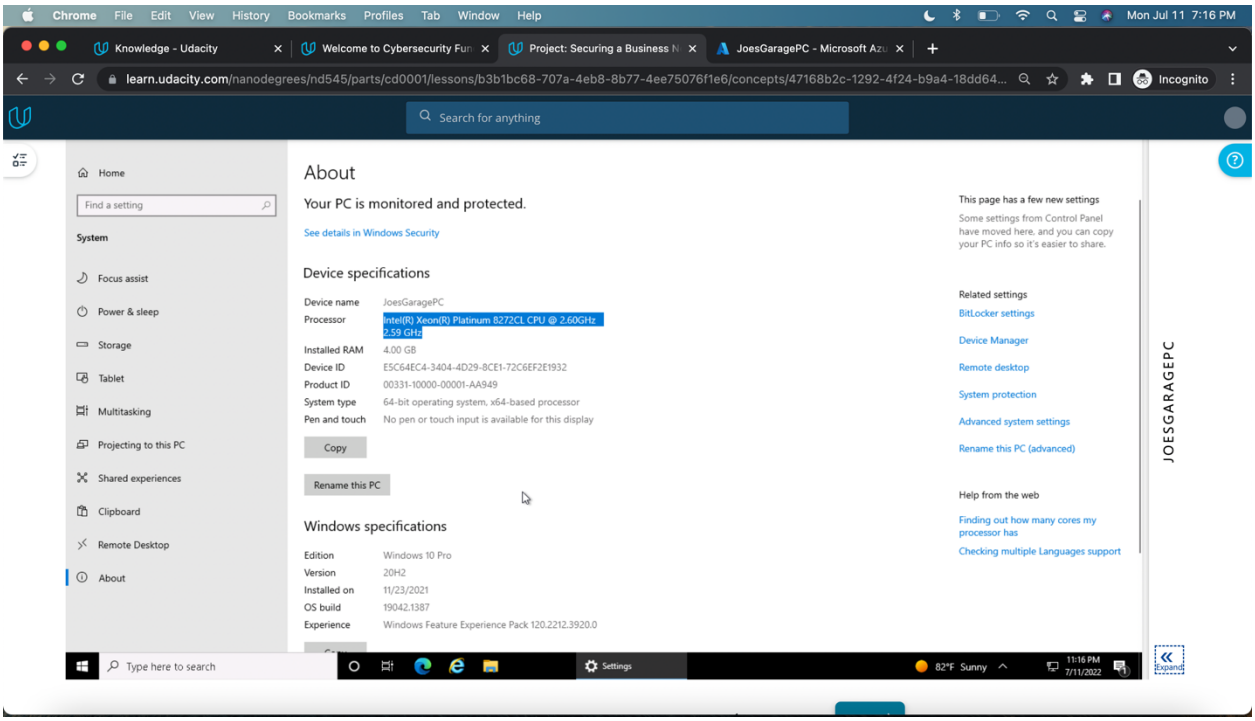
1. *Fill in the following table with system information for Joe's PC.*

Device Name	JoesGaragePC
Processor	Intel®Xenon®8272Cl CPU
Install RAM	4GB
System Type	64 bit os
Windows Edition	Windows 10pro
Version	20H2
Installed on	11/23/2022
OS build	19042.1387

2. *Explain how you found this information:*

   Home>>about>>Device specifications & Windows specifications

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



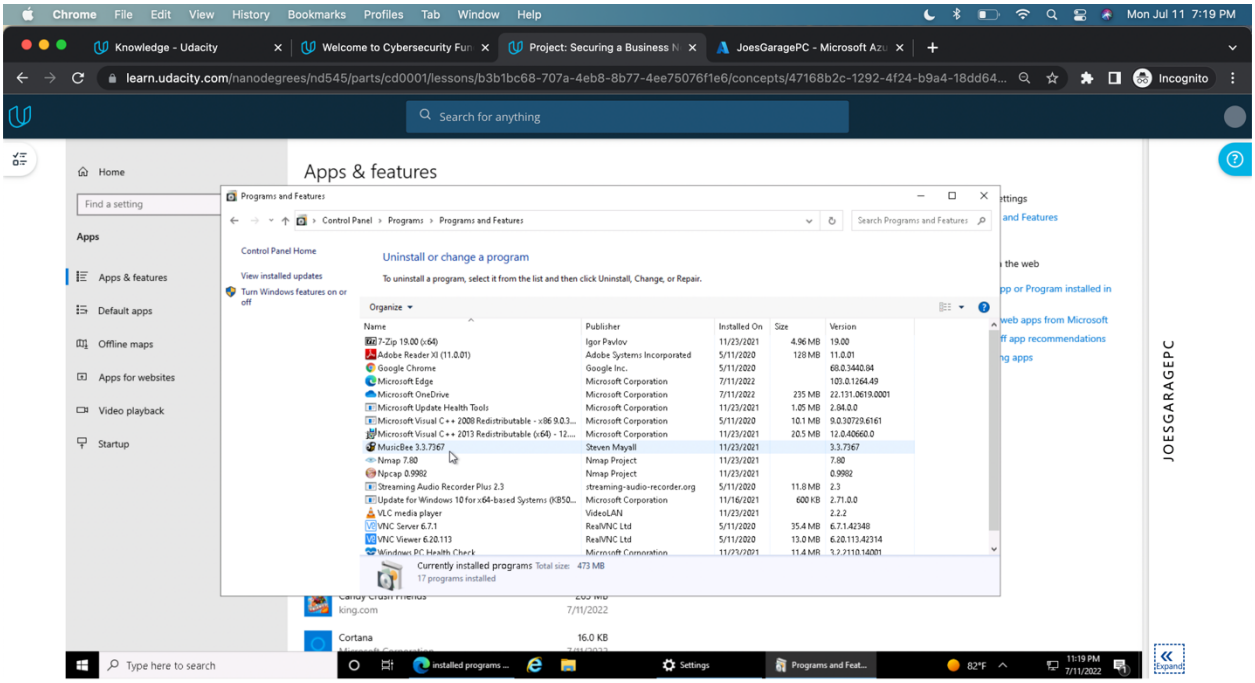
Software

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

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

- 7-Zip
- Adobe Reader
- N-Map
- Microsoft Visual C++
- Windows PC health check

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



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

A: CIS critical security control 2- Inventory and control of software assets

Accounts

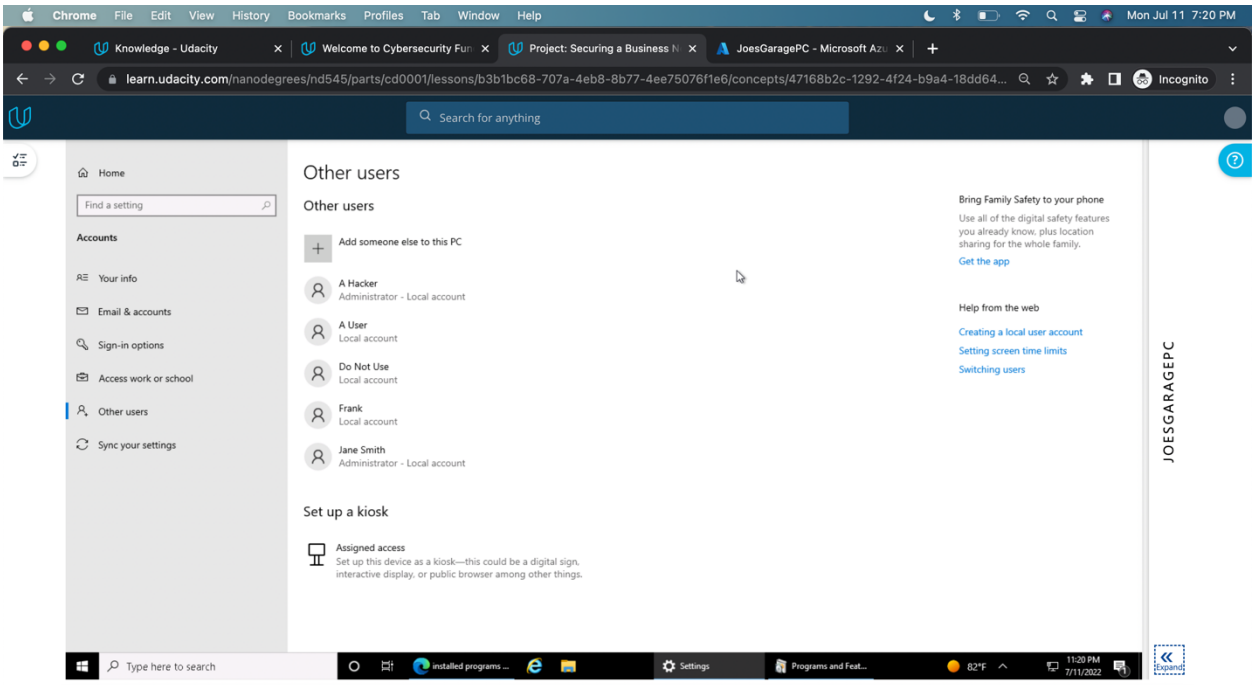
As part of your security assessment, you should know the user accounts that may access the PC.

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

Account Name	**Access Level**
A hacker	Administrator -Local account

A User	Local account
Do Not Use	Local account
Frank	Local account
Jane smith	Administrator

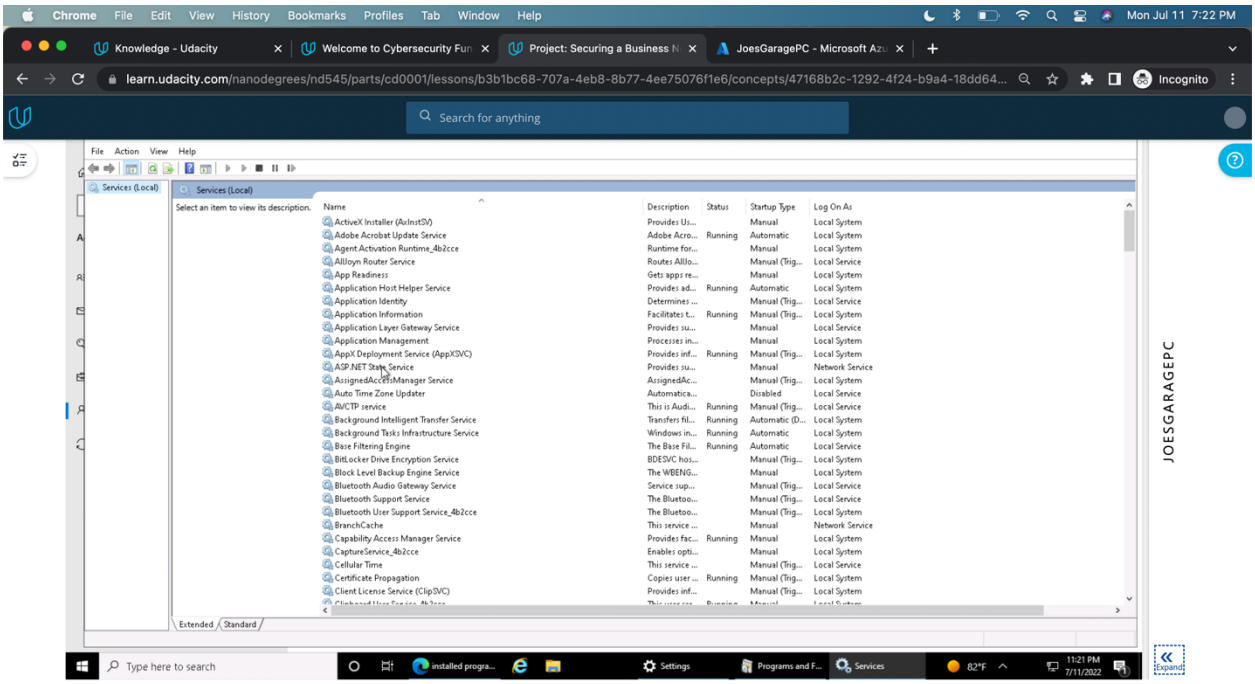
2. *Provide a screenshot of the Local Users.*



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.

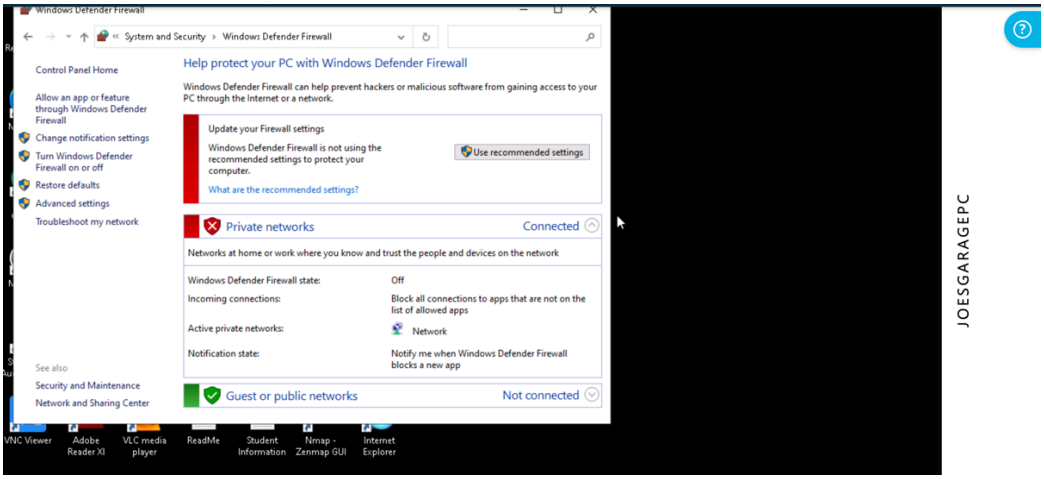
1. *Provide a screenshot of the services running on this PC.*



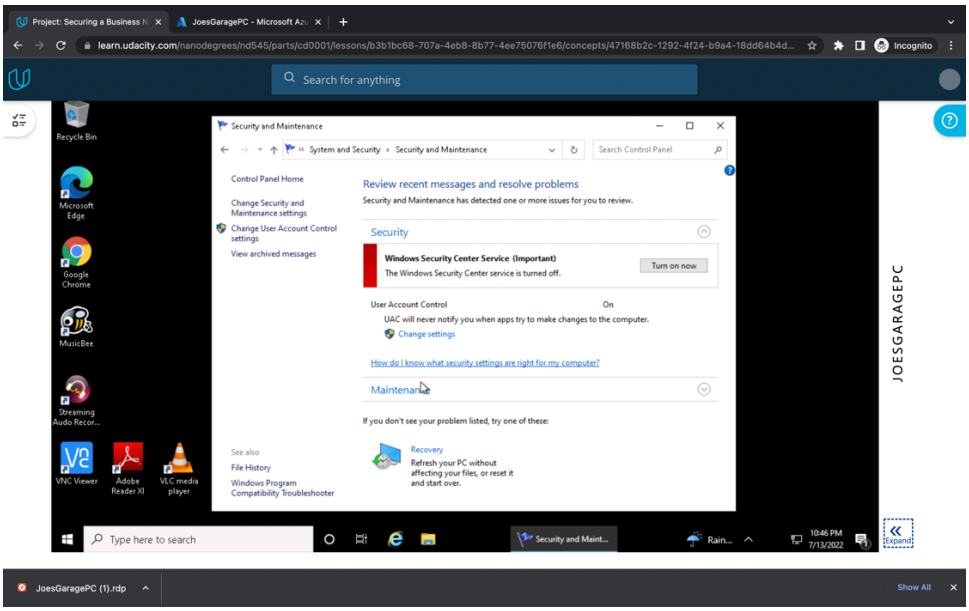
Security Services

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.**

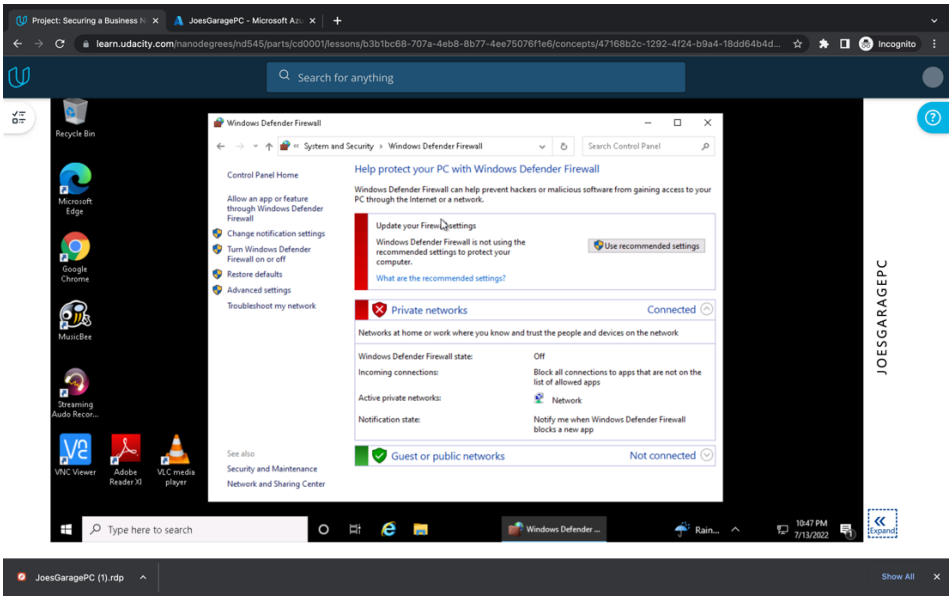
1. *To view a summary of security on Windows 10, start from the **Control Panel**. Use the "Find a setting" bar and search on Windows Defender. You can also search for Windows Defender using the Windows Run bar. Take a screenshot of what you see on the Windows Security screen and include it here:*



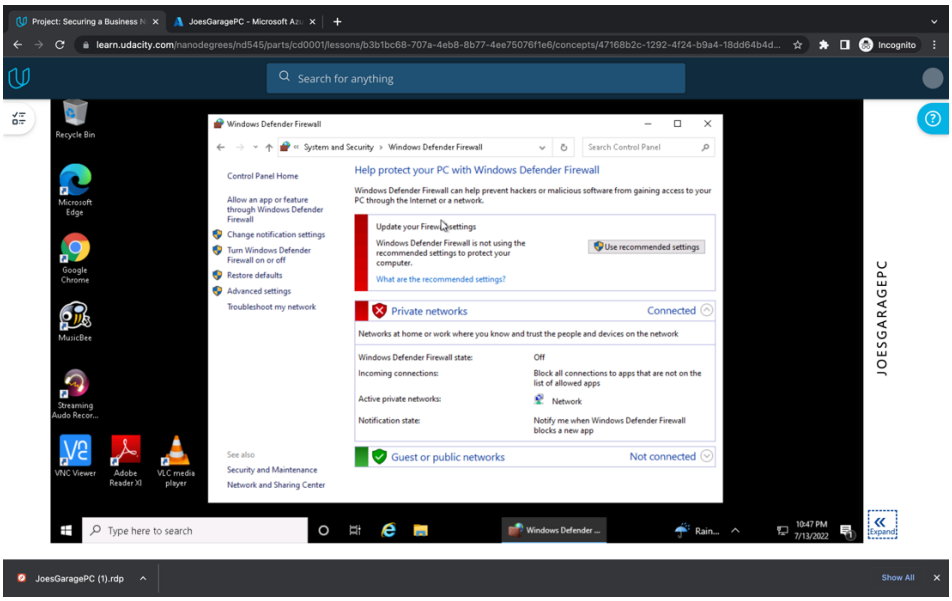
2. *The Windows 10 Security settings are also found from the **Control Panel > System and Security > Security and Maintenance**. Start by viewing **"Review your computer's status and resolve issues."** Provide a screenshot of this below:*



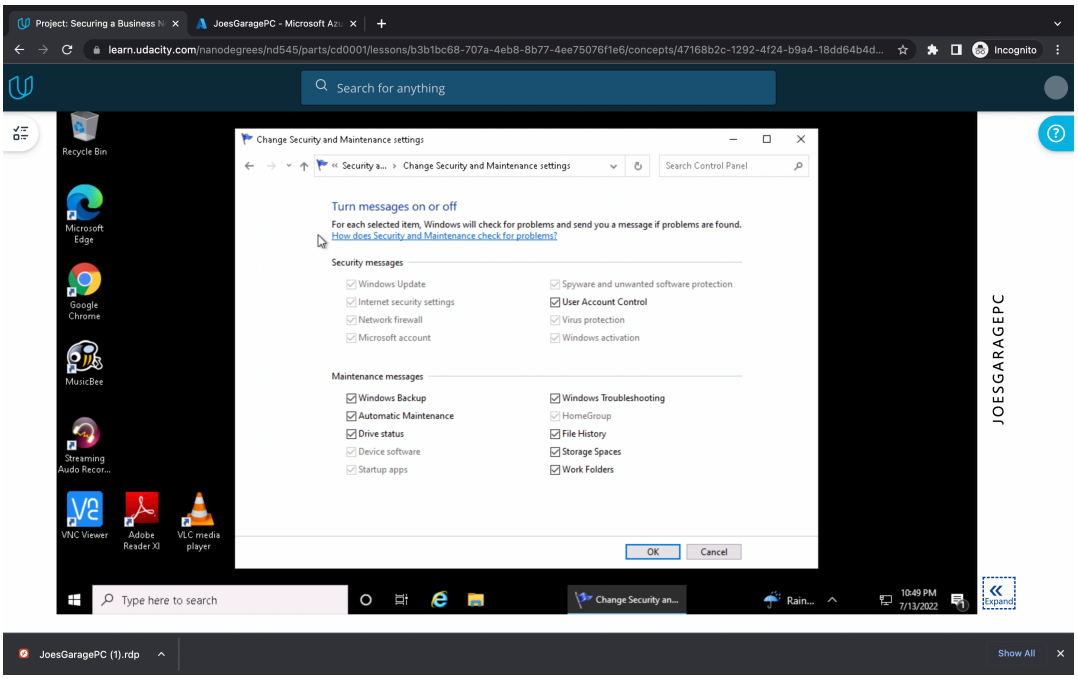
3. *Click on View in Windows Security to see the status there. Provide a screenshot of the* ***Firewall*** *settings.*



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



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



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

Security Feature	**Status**
Firewall product and status – Private network	connected
Firewall product and status – Public network	Not connected
Virus protection product and status	on

Internet Security messages	on
Network firewall messages	on
Virus protection messages	on
User Account Control Setting	on

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

- Windows defender is off – critical security control – as per CIS controls -secure configuration of Enterprise assets and software- it will help prevent access to hacker or malicious software from gaining access to your PC

- Windows Security Service is turned off – which will scan and notify about the malicious activity
- Do not give administrative access to untrusted user.
- User account control settings – never notify when apps try to install software, when making changes to the system
- File history is Off- you cannot get them back in case of lost/damage

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?*
   A:- ISO and CIS controls
2. *What industry baseline do you recommend to Joe?*
   [Hint: Look in the documents folder]

Ans: IG1(implementation group 1)

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?

   Inventory and control of hardware assets, secure configuration of hardware and software assets, data protection.

System and Security

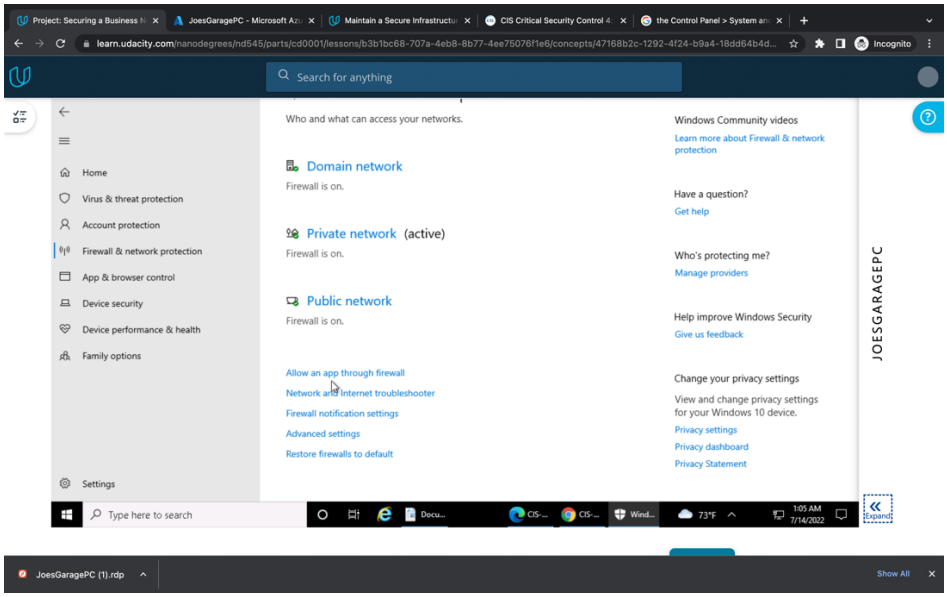
At this point, you need to enable security services for this PC. Pick at least 3 of the following 5 areas to secure to satisfactorily meeting the project requirements:

- 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.*
   Settings>>Firewall & network protection>> change domain network settings and private network settings
2. *Include screenshots showing the firewall is turned on.*



3. *What protection does this provide?*

It protects the organization/pc from malware attack and unnecessary traffic, according to CIS controls it comes under Malware Defense step 10.

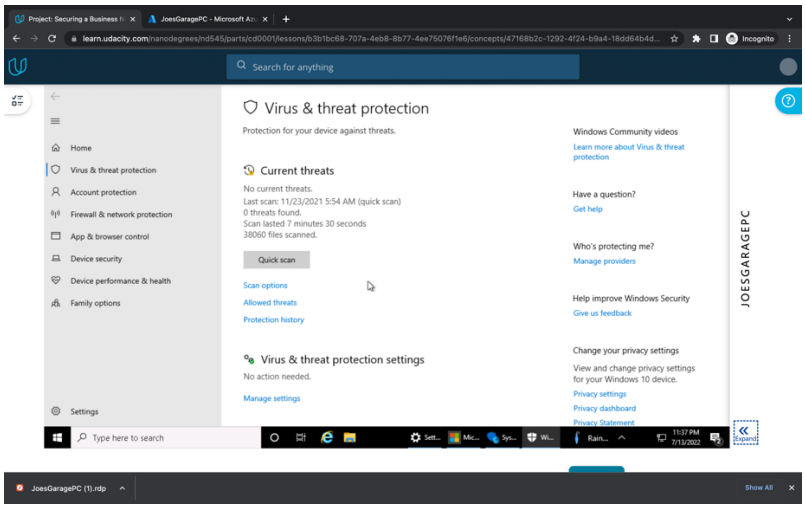
Virus & Threat Protection

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.*

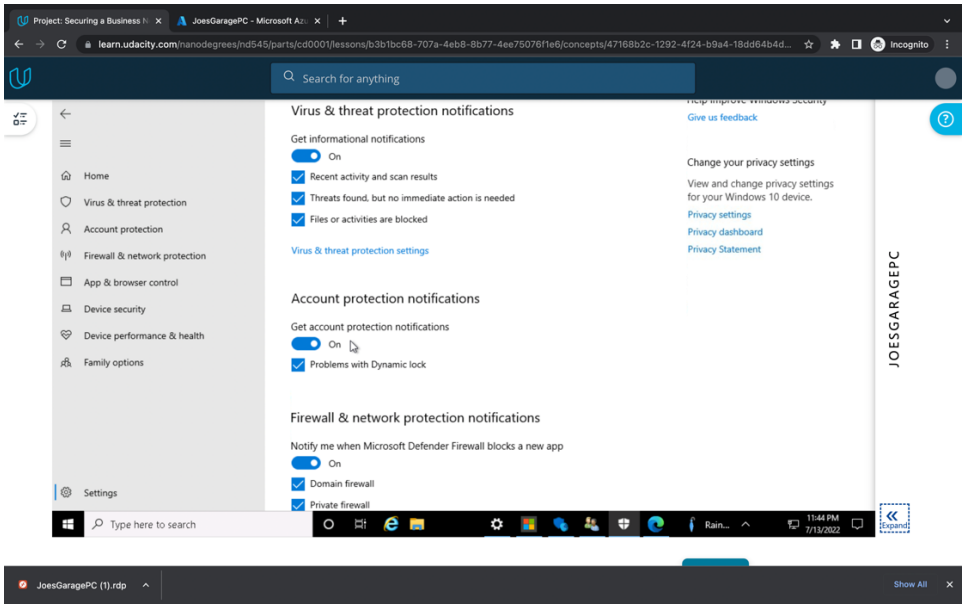
Settings>>Virus & Threat protection and manage virus and threat protection settings

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



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

- You will be notified for any threats/risk
- Account protection notifications

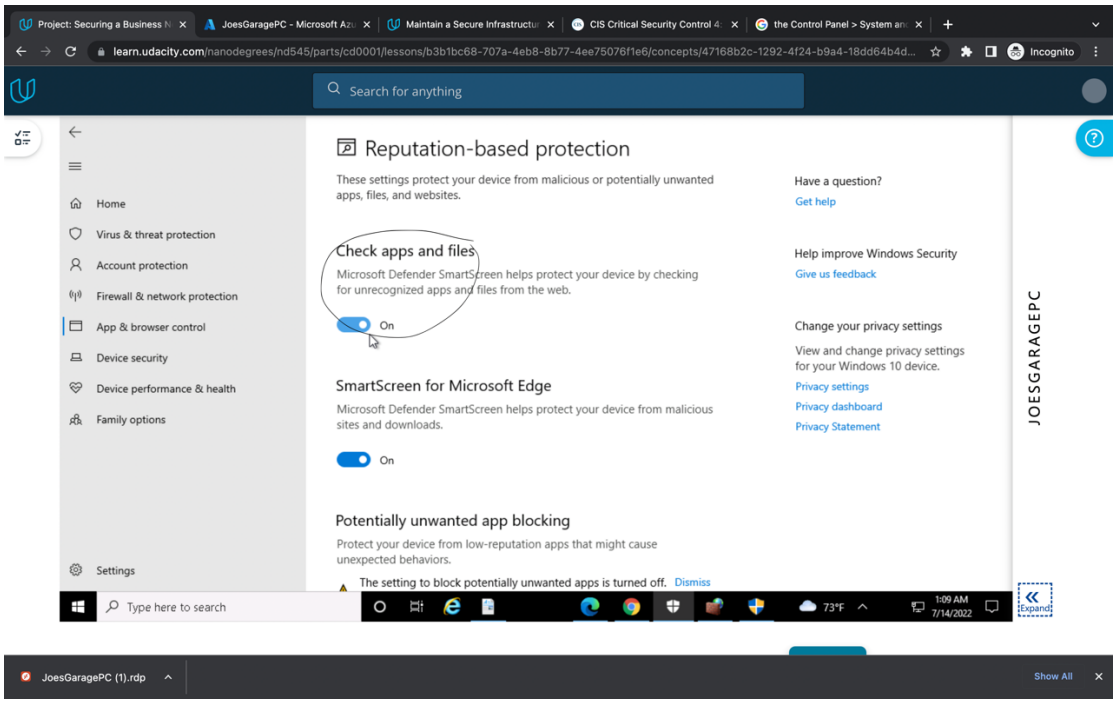
4. *From the CIS baseline controls, provide the controls satisfied by completing this.*

A: CIS critical security control 7: continuous vulnerability management

App & Browser Control

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

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



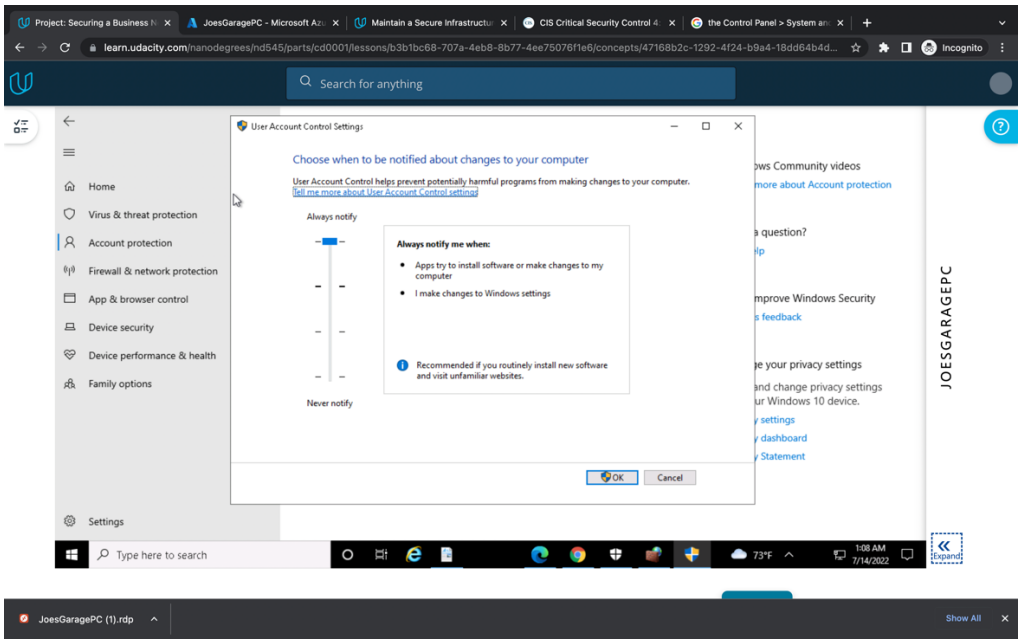
User Account Control Settings

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

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

This is available from the above security settings.
A: current setting is never notify but it should be “always notify”, it will help to prevent harmful programs from making changes to PC

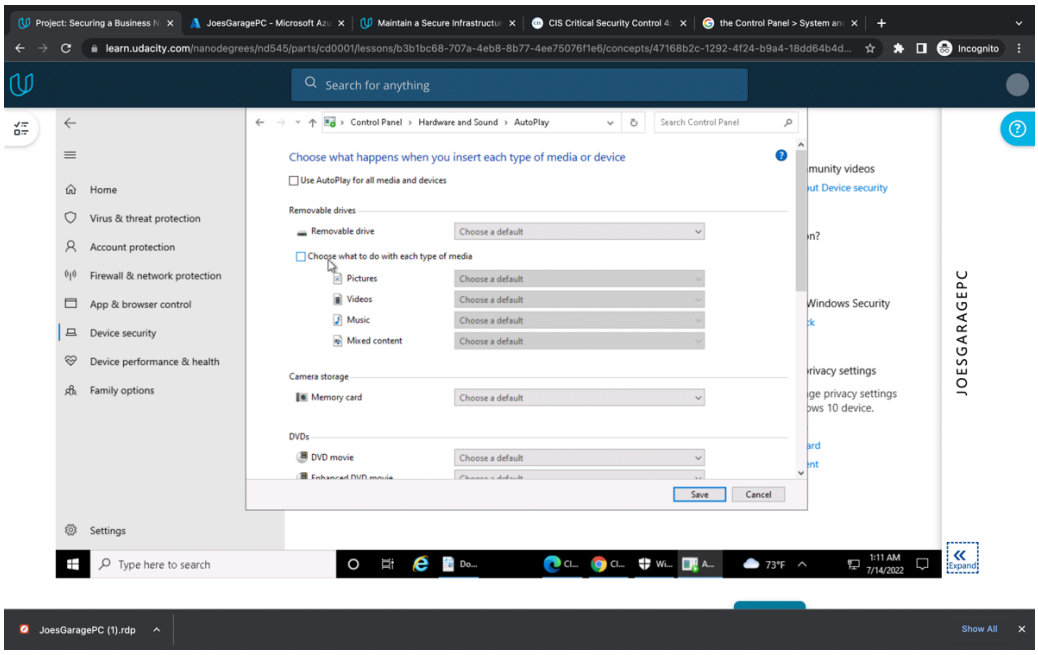
2. *What should it be set to? Include a screenshot of the new setting.*

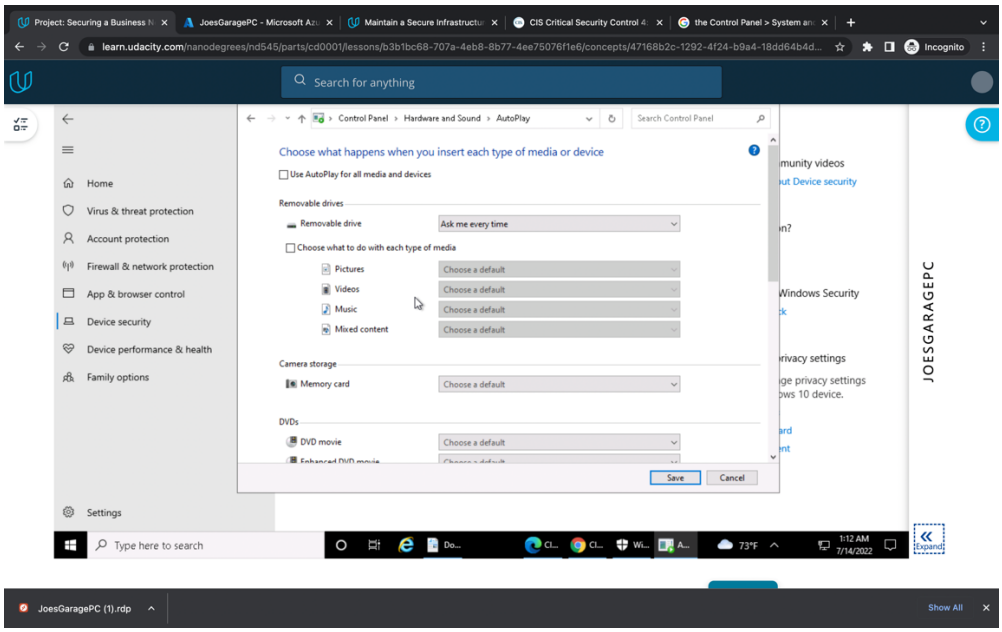


Securing Removable Media

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.”*
   A: done
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.

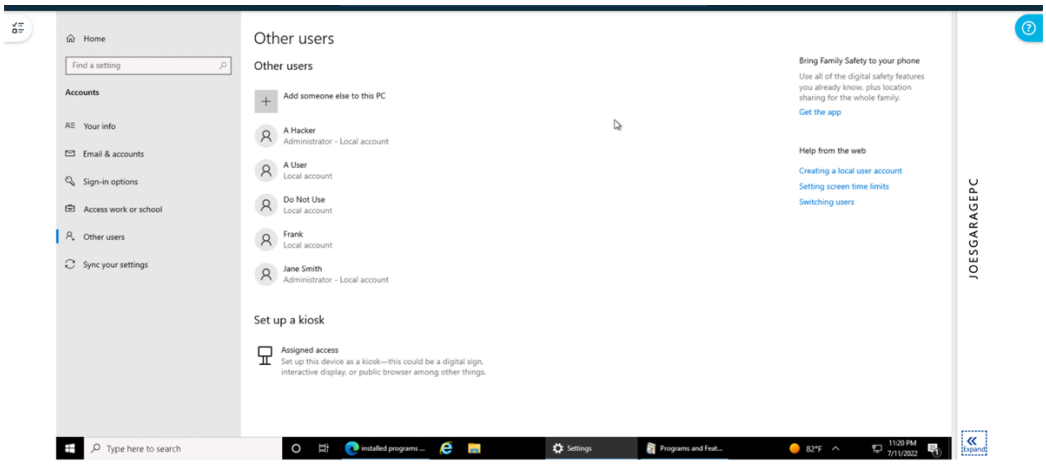
User Accounts

1. *What user accounts should not be there? Do not use, Franks account, A Hacker account*
2. *Bonus questions: What is Hacker's password?*
3. *Explain the steps you take to disable or remove unwanted accounts. Go to settings <<other user << select the account<<remove<<delete the account*
4. *Why is it important to disable or remove unneeded accounts from a PC or application? Include potential vulnerabilities and risks. All the people with the user accounts can access the pc and access data so removing unwanted accounts will help with the system security and privacy*

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 and Jane smith have administrative rights in the joes pc.
6. Explain how you determined this. Provide screenshots as needed.

   Home>> other users



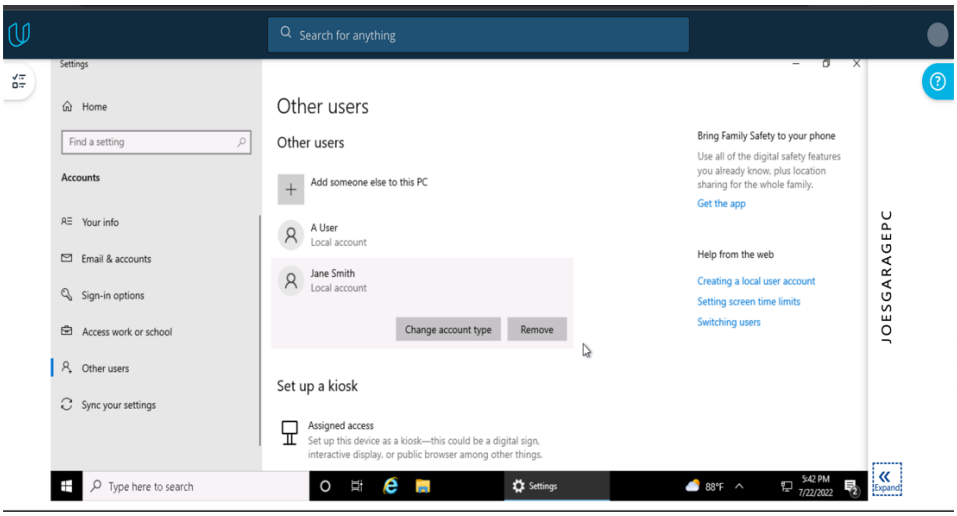
Administrator privileges for too many users are another security challenge.

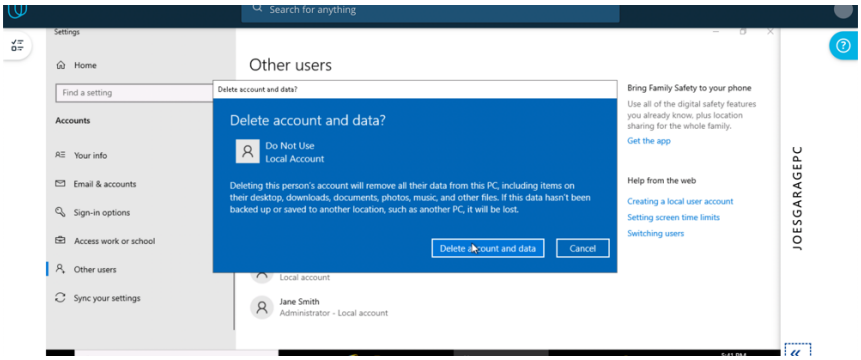
7. Provide at least three risks associated with users having administrator rights on a PC.

- There is a risk of malware/virus
- User with administration rights can modify security settings, disable firewall, threat protection….etc
- An administrator can added/ delete user accounts or mess-up the system and can delete important data in the pc

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.*
   Ans: go to settings>> other users>> remove>> delete account and data click on it. And change account type to standard account





9. *What is the security principle behind this?*
   Ans: CIS critical security control 5 & 6: account management and Account Access control management

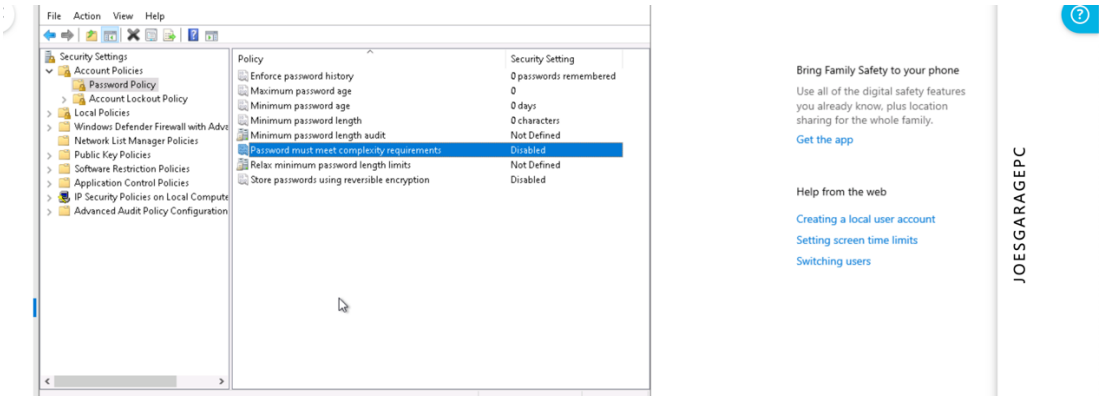
10. The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?

CIS critical security: Step5: Account Management

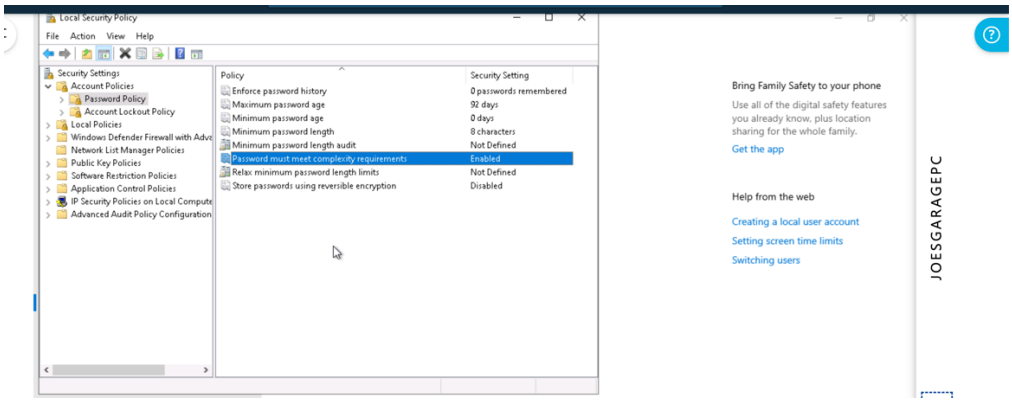
Setting Access and Authentication Policies

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

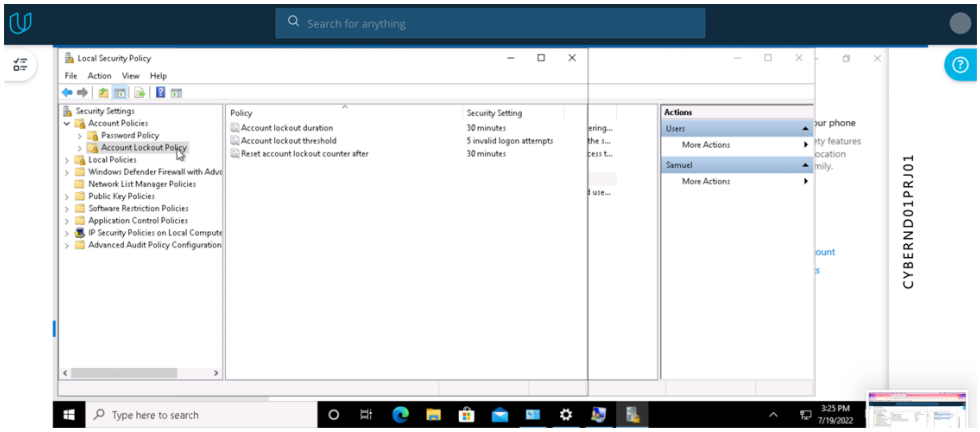
1. *Provide a screenshot of the Local Security Policy window here.*
   [Note: Local Security Policy is not available on Windows 10 Home edition.]



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



- Setting the Account Lockout Policy:

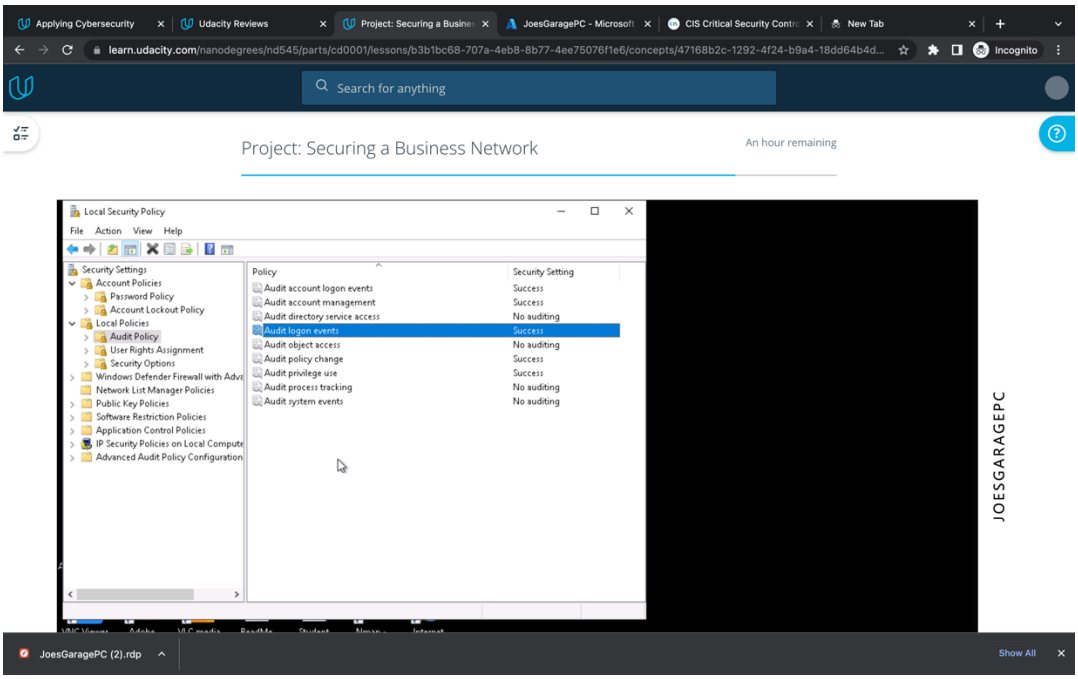


Auditing and Logging

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.
   Done

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.*

- *Candy crush, Hulu , Netflix*
- *VNS viewer*
- *VNC server*
- *Farm heros saga,*
- *Spotify*

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

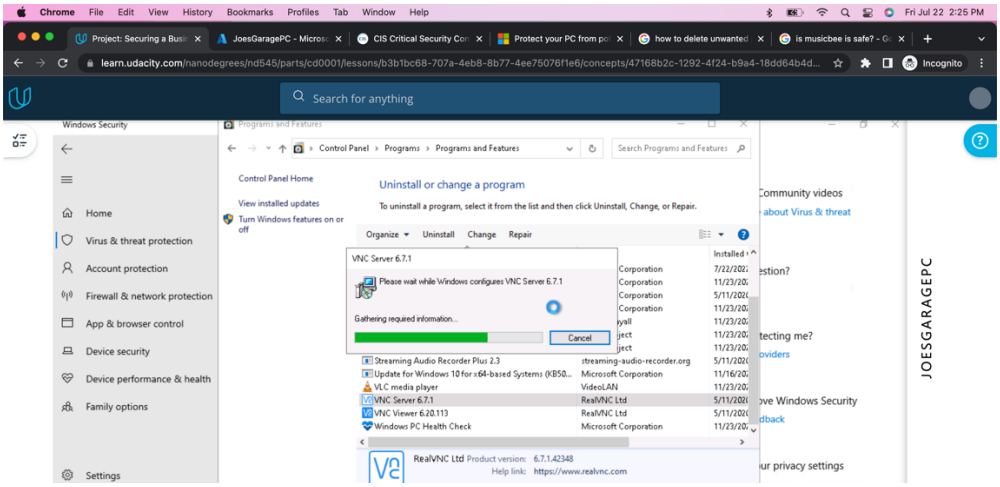
- *VNC viewer, VNC server will provide remote access, people can remotely check pc input (keyboard, mouse) which will allow access to hacker*

- *Some games /3rd party applications may have malware,*
- *the applications are harmful and makes system run slow*

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.*

   Go to settings>> app& features select the unwanted app and remove it:- done removed candy crush, farm heros, spotify

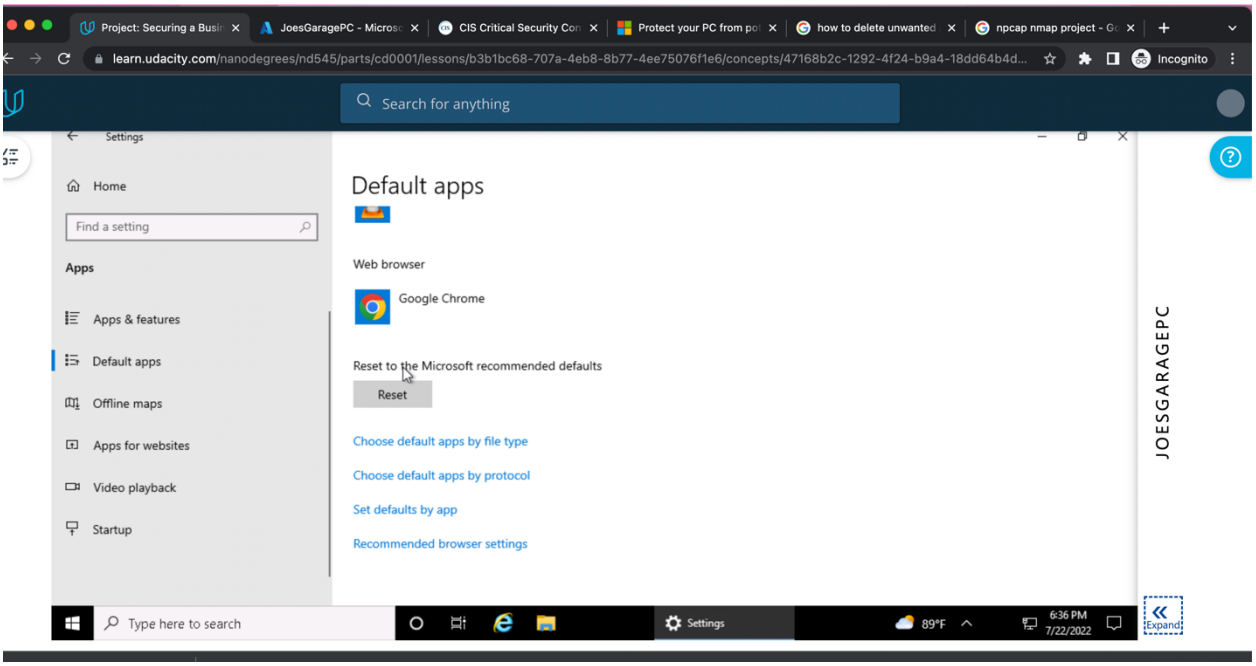
   Go to control panel >>Programs>> uninstall unwanted programs



Default Browser

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

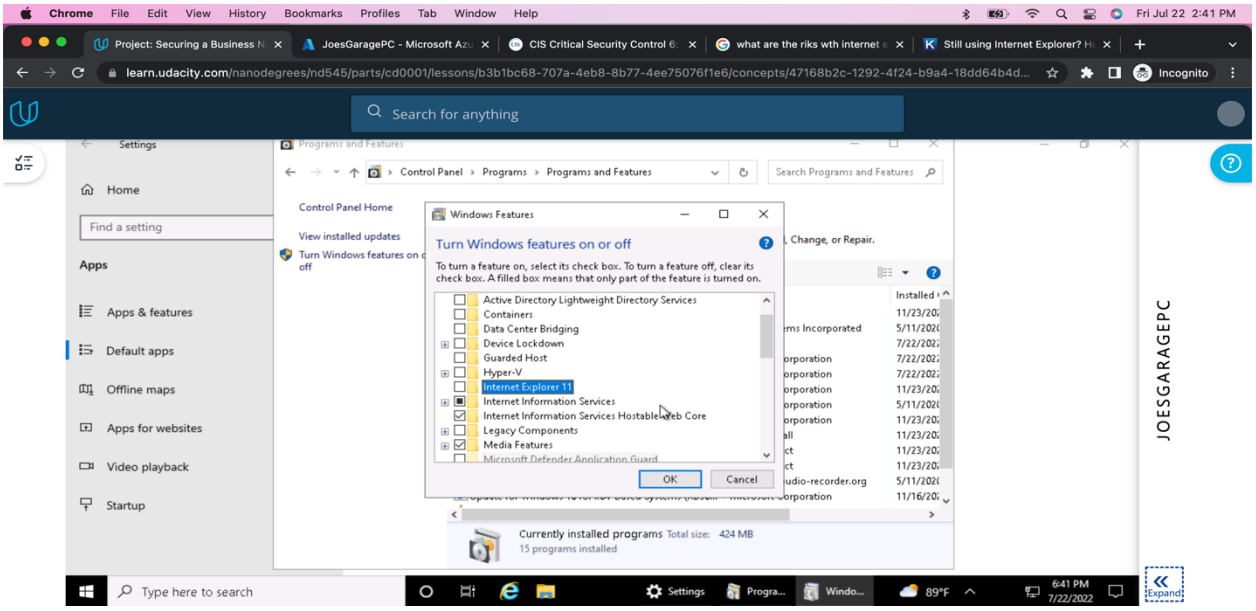
1. *Explain how you set default applications within the Windows 10 operating system. Include screenshots as necessary.*
   Go to settings>>Default apps>> set default browser as chrome.



2. *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
    - Internet explorer is old web browser that does not have many security updates and patches, so hackers may take the advantage of it and can hack the computer
    - And experts found many vulnerabilities in this browser

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**."

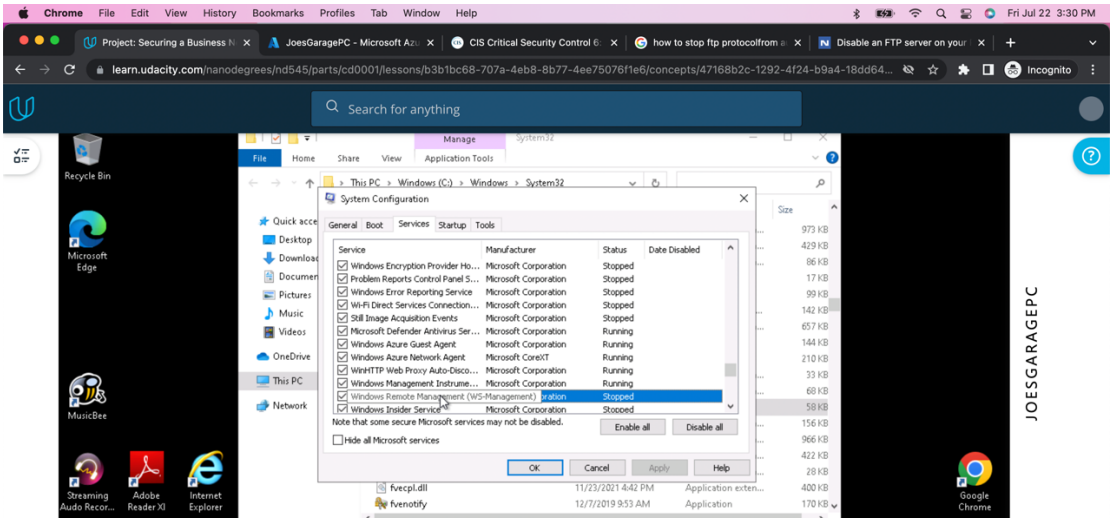
3. *Provide a screenshot showing Internet Explorer 11 is off.*

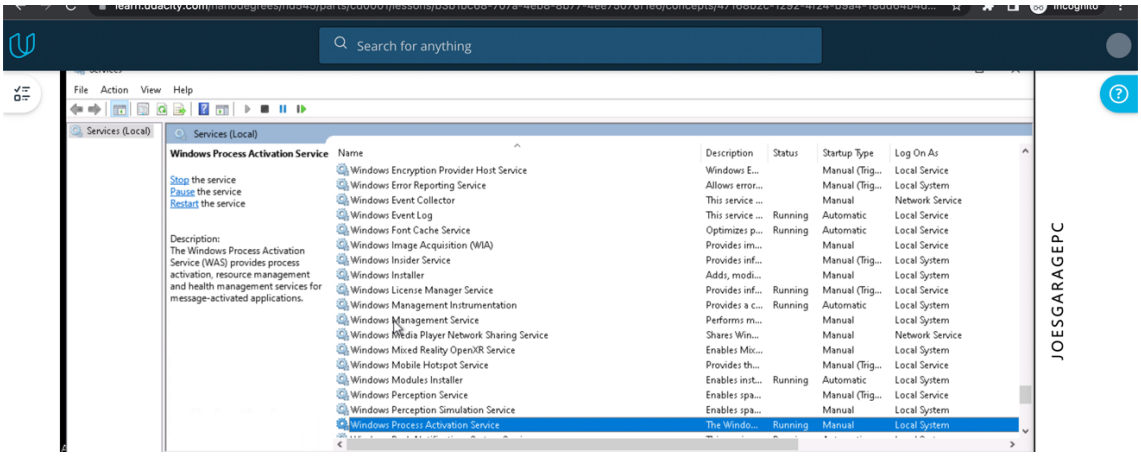


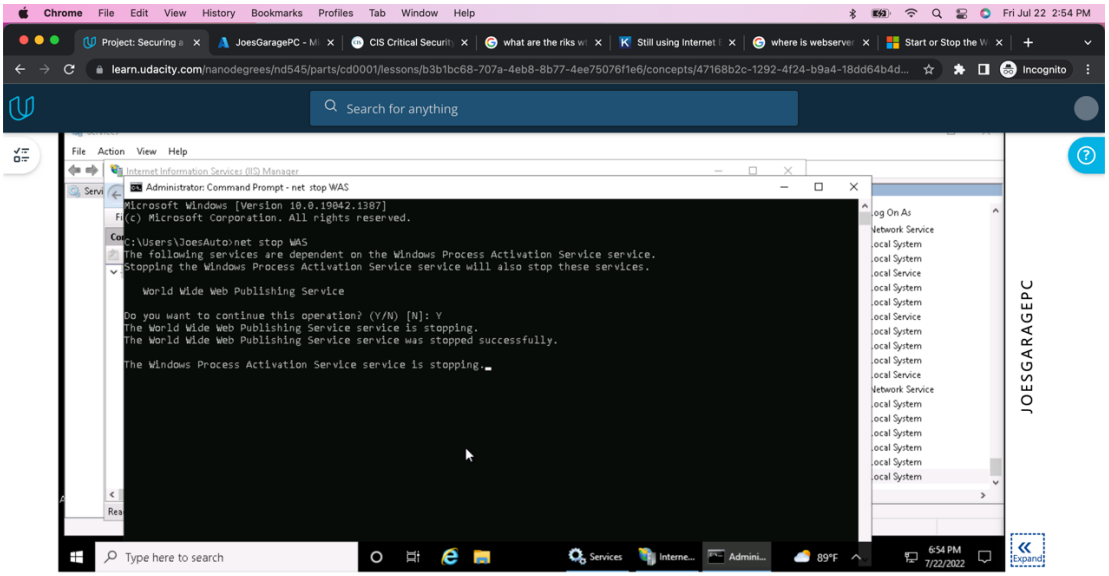
Windows Services

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.
   go to services(local) and check automatically running programs and manually running programs







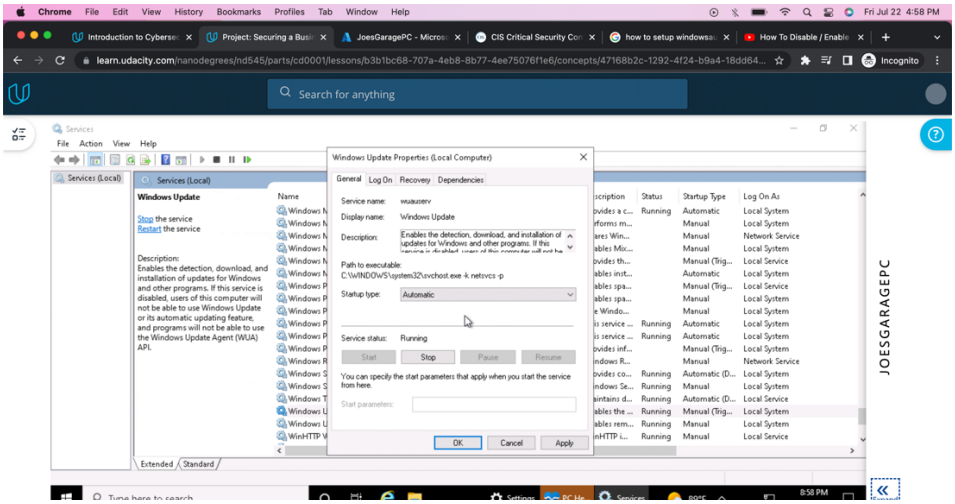
2. Advanced users should provide at least two methods for determining a web server is running on a host
   Check active web servers from services (or) from command prompt using command netstat -na or from system configuration
3. How do you disable them and make sure they are not restarted?
   Using command net stop WAS in command prompt or manually disable from system config
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.

   System configuration>> services>> Microsoft ftp services disable it.

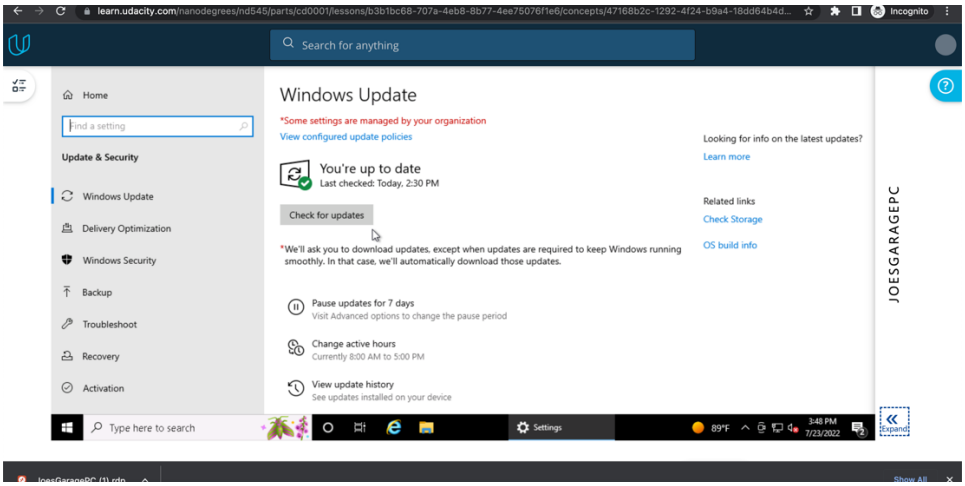
Patching and Updates

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

1. *Explain the process for doing this. Include screenshots as needed.*
   Go to services>>windows update>> click on it select automatic and apply



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



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

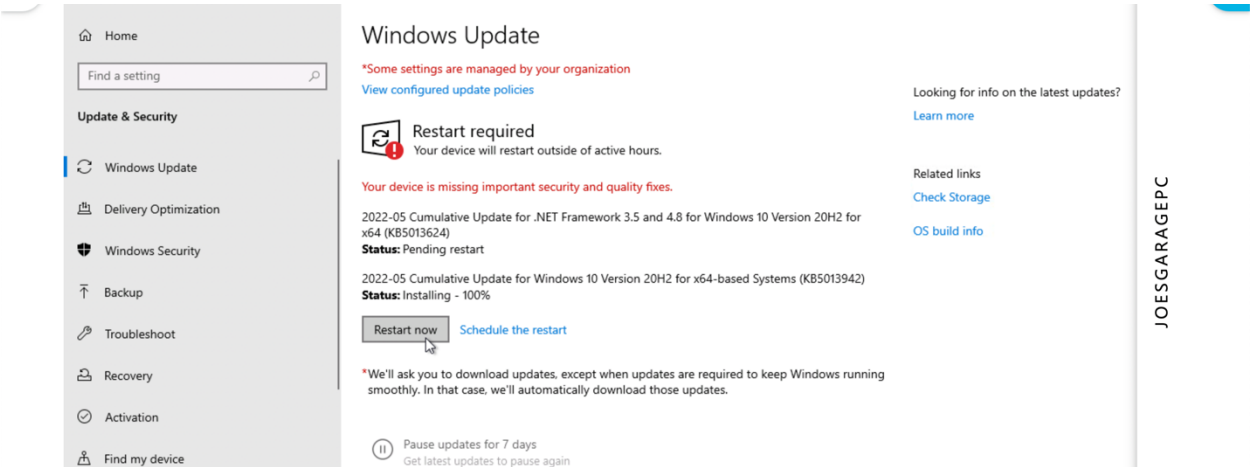
3. *List at least two applications on Joe's PC that are out of date. List them below:*

- Adobe reader
- Google Chrome (before updating)
- This Pc has recorder which is out if date.

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

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

   Ans: Go to settings >> windows update >>install all the updates available



5. Securing Files and Folders

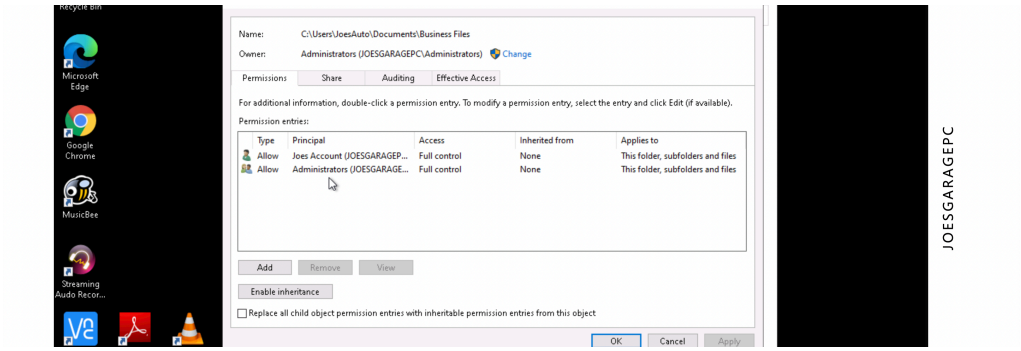
Joe has some work files in his business folder that he wants to secure since they contain his customer information. They are labeled “JoesWork.”

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.

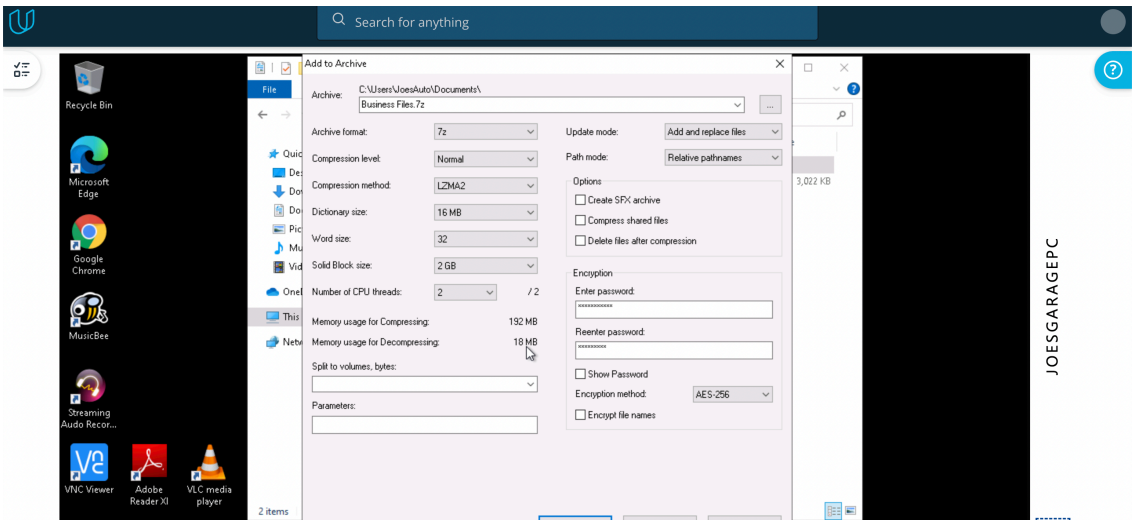
Encrypting files and folders

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.]*

   Ans: only Joe and Jane smith are administrators.



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?*
   By encrypting the files and limiting the access, it will be protected from unauthorized access (from modify ,delete ,copy the data)

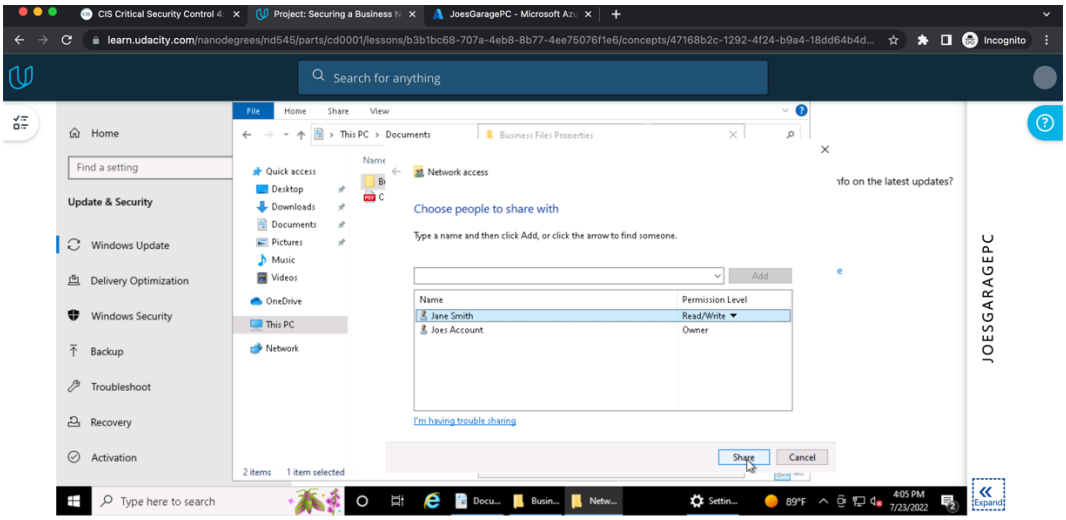
4. *The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?*

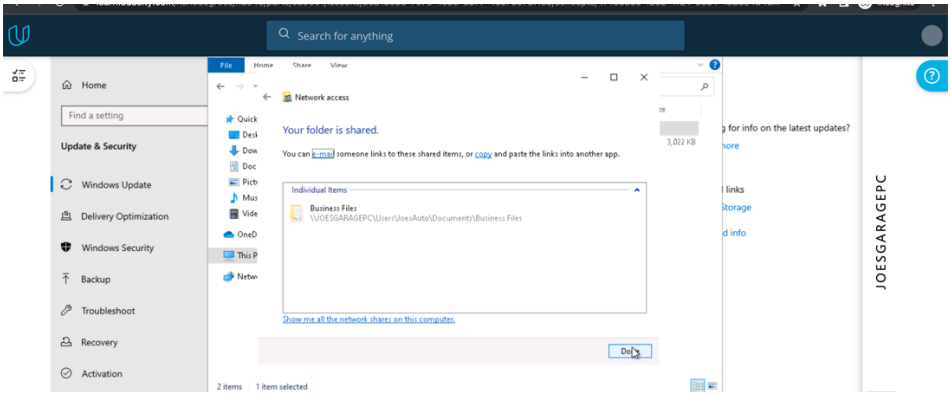
   CIS critical security control step4: Secure configuration of Enterprise assets and Software, Cis critical security control 3: data protection, step6: Access control management

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.

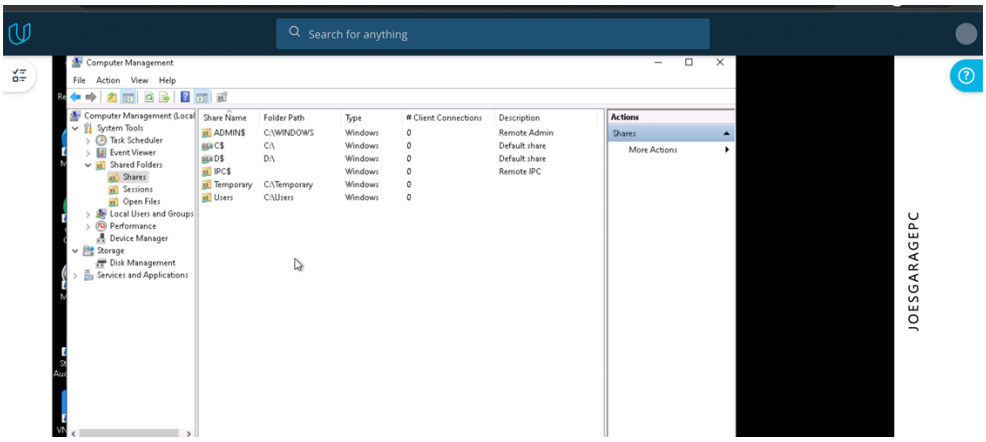
1. *Explain how you would do that and provide a screenshot showing how you can do it. Make sure it's only shared between Joe and Jane.*
   Right clock on document>> properties>>sharing or right click>> give access to specific people.

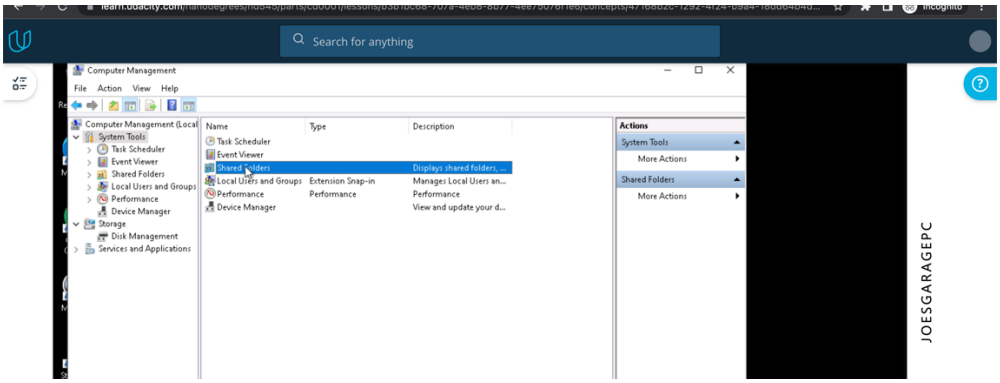




2. *For advanced students: Joe wants to make sure there are no other folders shared on the PC. Explain how you view all shared files and folders on a Windows 10 PC. Include a screenshot as proof.*

   System tools>> shaared folders>>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]

- Hacker folder has a bitmap image folder which may be vulnerable
- Frank folder have some Xbox games which are violating the standard principles, 3rd party applications sometimes have malware/virus
  And some other unwanted accounts like Do not use and Franks have access to 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.