Cybersecurity 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: Kevin C Mejias

Date of completion: Tuesday May 18, 2021

Scenario

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.

1. Reconnaissance

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

Complete each section below.

Hardware

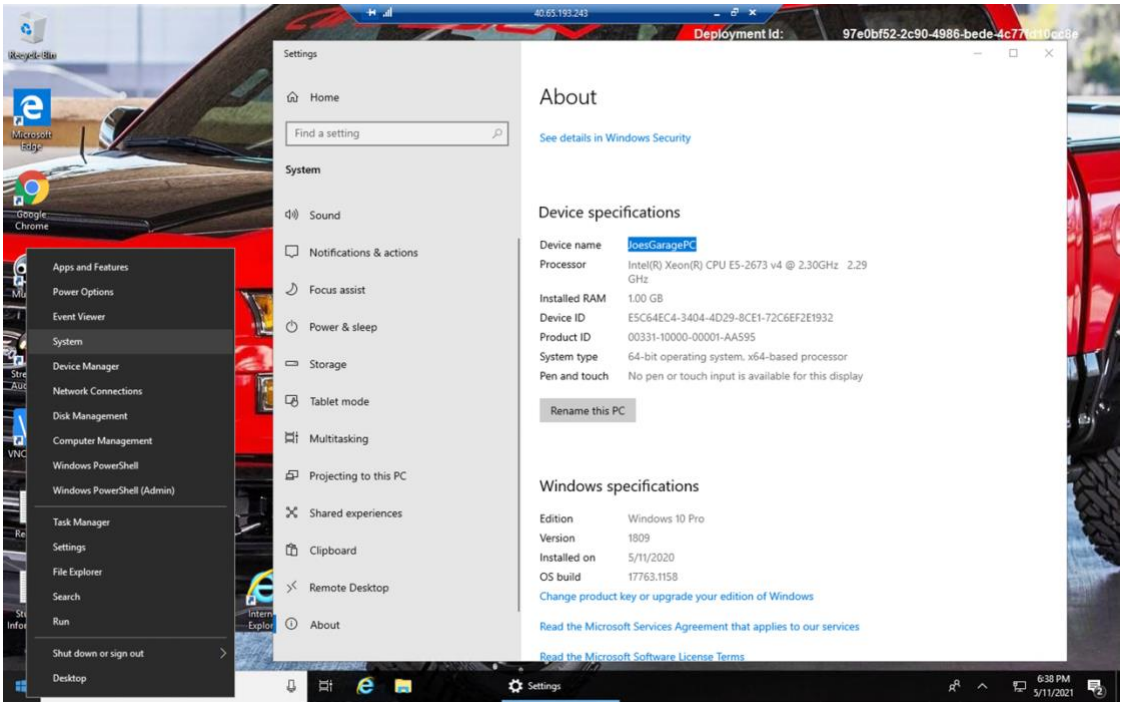
1. *Fill in the following table with system information for Joe's PC.*

Device Name	JoesGaragePC
Processor	Intel(R) Xeon(R) CPU E5-2673 V4 2.30 GHz 2.29 GHz
Install RAM	1.00 GB
System Type	64 bit operating system x64 based processor
Windows Edition	Windows 10 Pro
Version	1809
Installed on	05/11/2020
OS build	17763.1158

2. *Explain how you found this information:*

A: I initiated JoesGaragePC > Right Click on the Windows icon on the left-bottom corner of the screen > then pressed "System" : Opened Settings Panel > search "About" at the bottom of the list.

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



Software

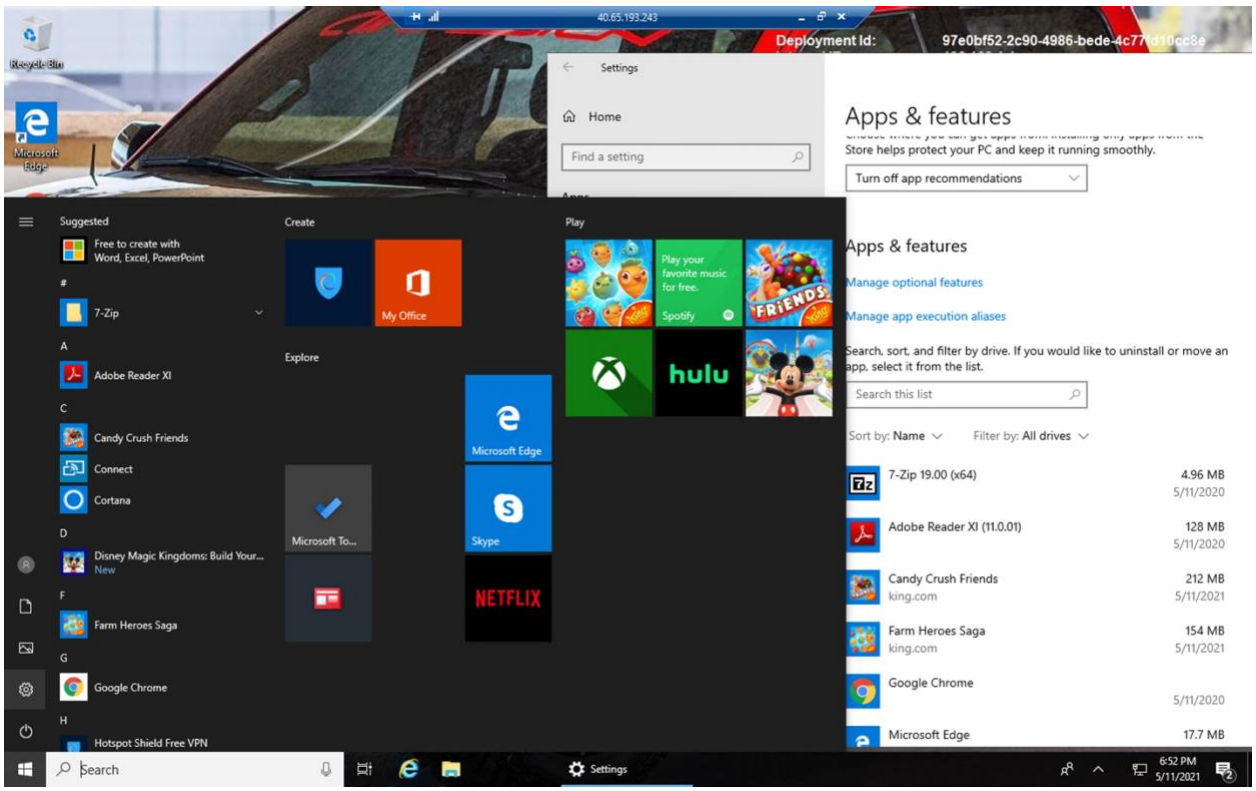
Another common early step in securing is taking an inventory of software or applications installed on a computer system. These are programs outside of the standard operating system.

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

- 7-ZIP
- Candy Crush
- Farm Heroes Saga
- Adobe reader
- Spotify

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

A: Press Windows icon in the left-bottom corner of the screen > press the 'Settings' : go to setting panel > Select 'Apps'



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

A: Step 2, Inventory and control of software assets.

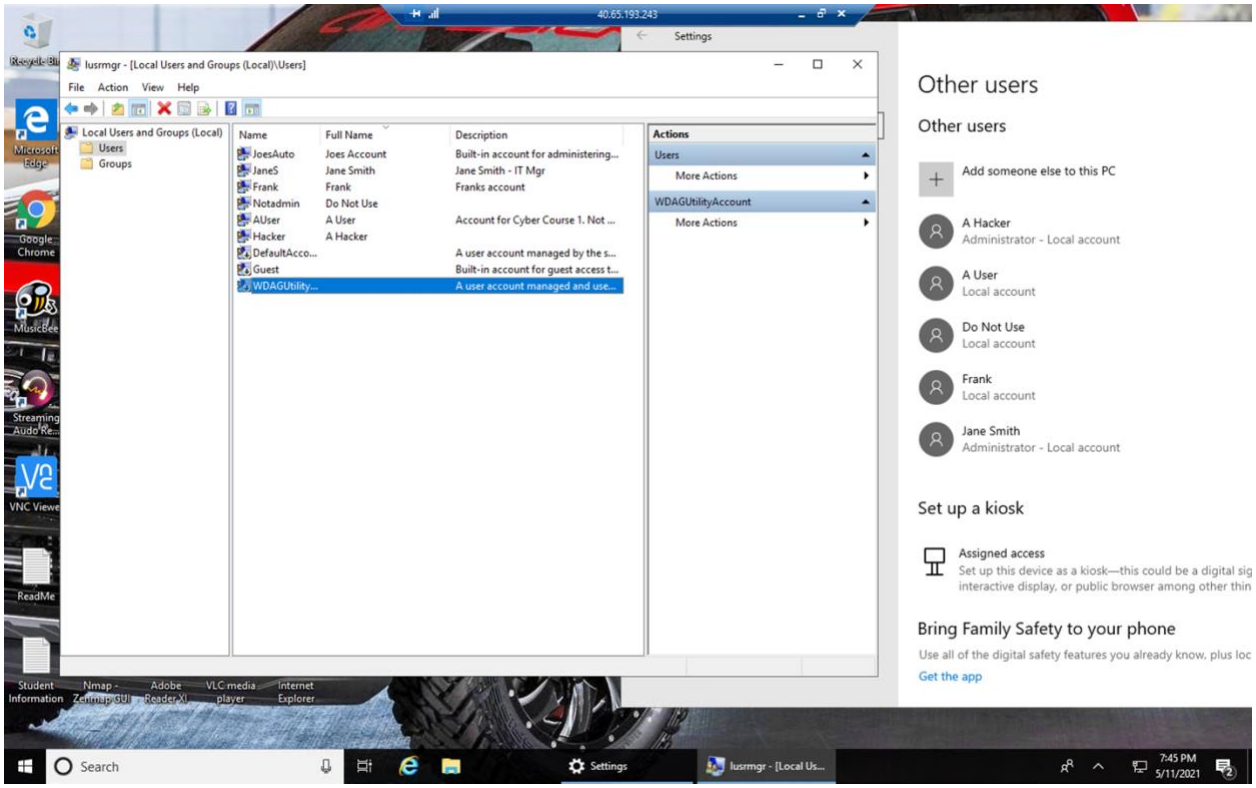
Accounts

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

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

Account Name	Full Name	Access Level
A user	User	User
Default account	NA	Account mangt group
Frank	Frank	User
Guest	NA	User
A hacker	A hacker	Administrator
JaneS	Jane Smith	Administrator
JoesAuto	Joes account	Administrator
Notadmin	Do not use	User
WDAG Utility account	NA	NA

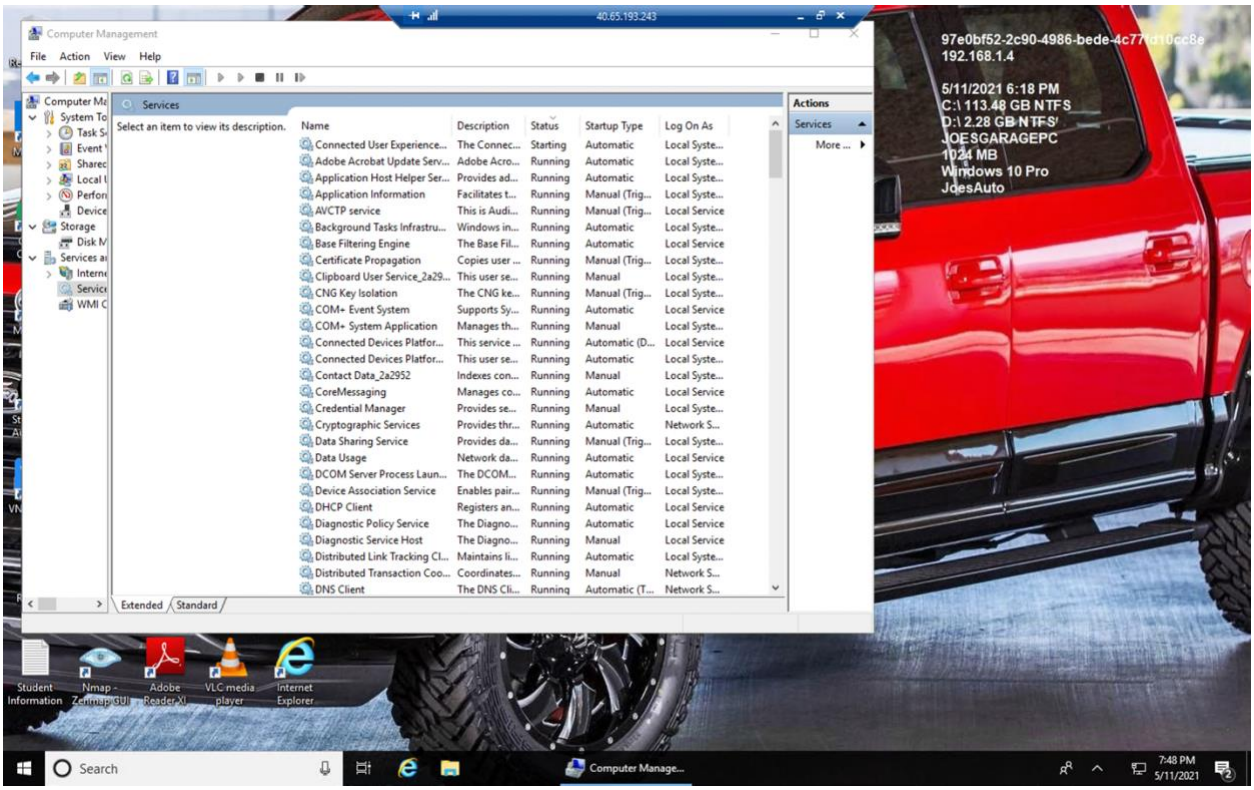
2. *Provide a screenshot of the Local Users.*



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.

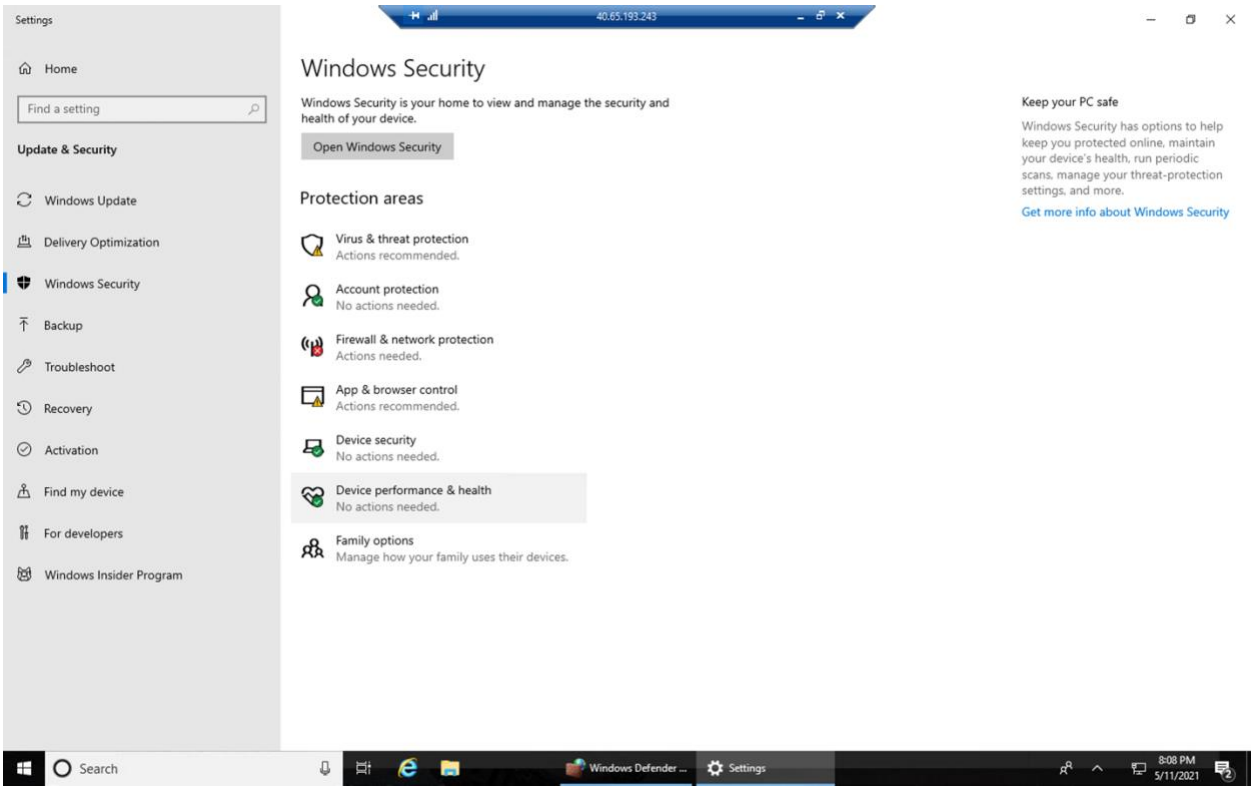
1. *Provide a screenshot of the services running on this PC.*



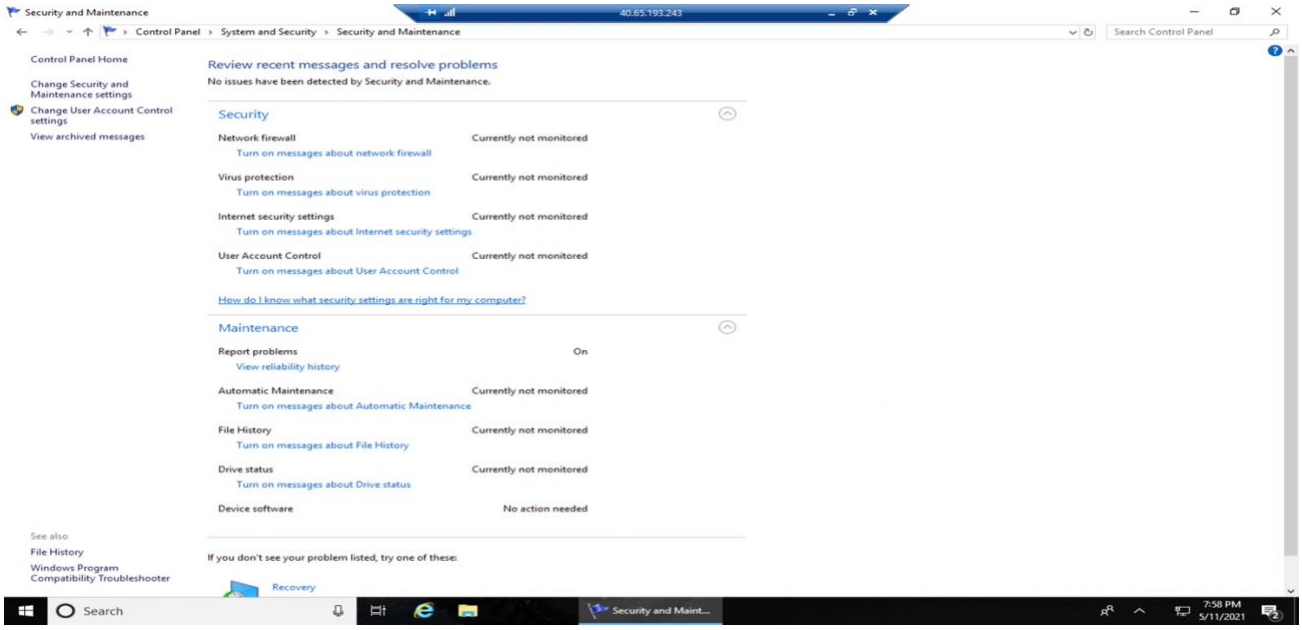
Security Services

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.**

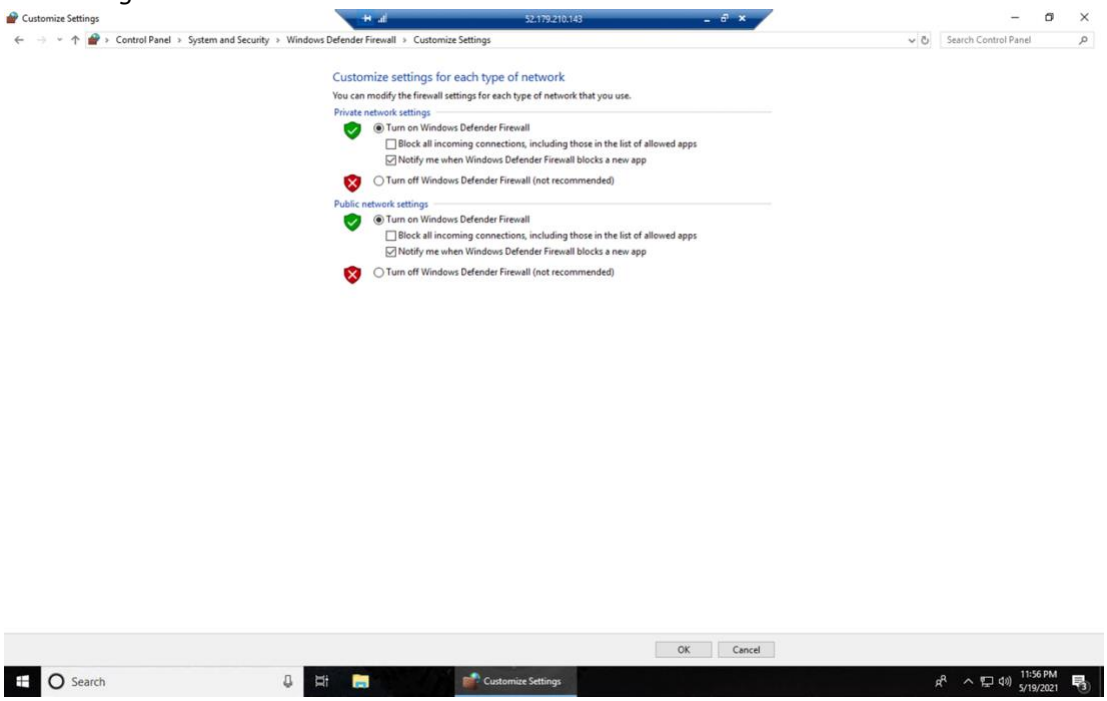
1. *To view a summary of security on Windows 10, start from the **Control Panel**. Use the "Find a setting" bar and search on Windows Defender. You can also search for Windows Defender using the Windows Run bar. Take a screenshot of what you see on the Windows Security screen and include it here:*



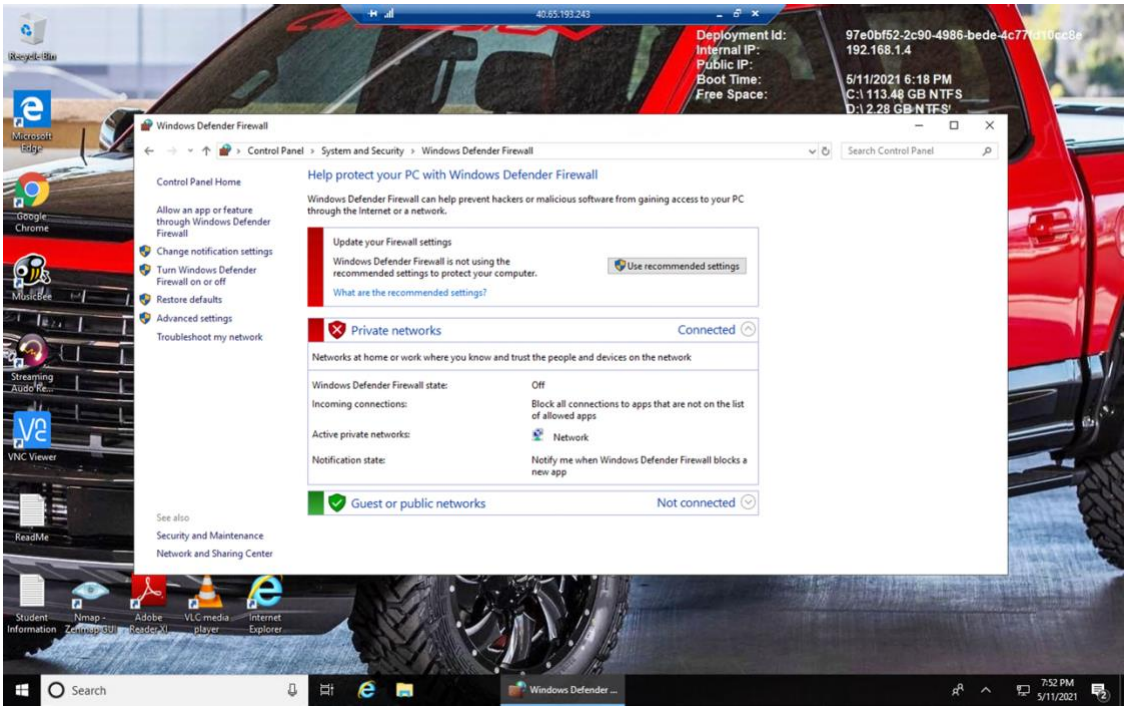
2. *The Windows 10 Security settings are also found from the* ***Control Panel > System and Security > Security and Maintenance****. Start by viewing* ***"Review your computer's status and resolve issues."*** *Provide a screenshot of this below:*



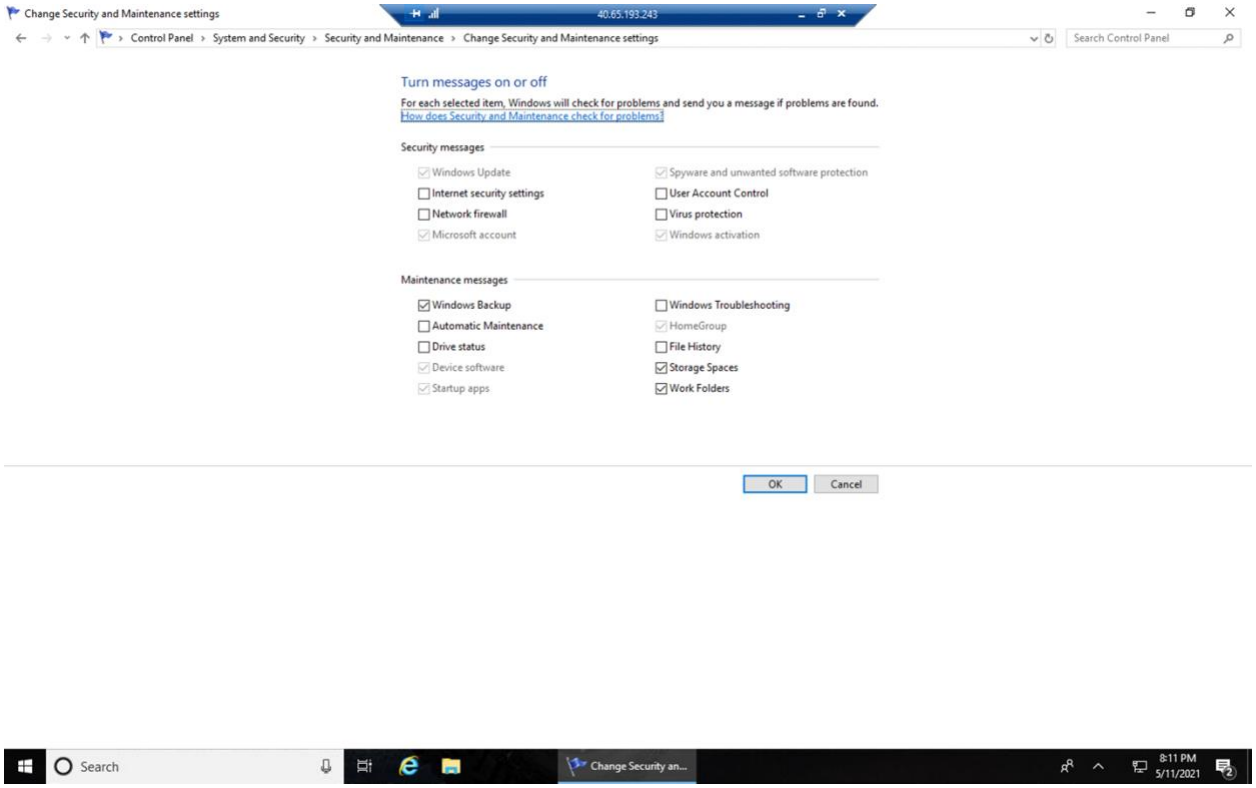
3. *Click on View in Windows Security to see the status there. Provide a screenshot of the* ***Firewall*** *settings.*



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	NO ACTION NEEDED
Internet Security messages	OFF
Network firewall messages	OFF
Virus protection messages	OFF
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.]

- Joes PC firewalls protection for private network is turned off, that represent a big risk since others networks and devices can have access to his system, even trusted devices can be a threat.
- Internet, network, and Virus messages notifications are turned off, losing the hablity to act immediately after a malicious program, virus or device is detected.
- User account is not being monitored and managed correctly allowing Other user to have full of the computer, this represent a huge risk since other user can accidentally download a malicious program to the system.

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: Joe should use the CIS benchmarks. The security benchmarks are best practices for the secure configuration of target system. CIS Benchmarks are developed through out a unique consensus-based process comprised of cybersecurity professionals and subject matter experts around the world CIS Benchmarks are the only consensus based, best- practice security configuration guides both developed and accepted by government, business industry and academia

2. *What industry baseline do you recommend to Joe?*
   -Inventory and control of hardware assets.

   -inventory and control of software assets

   -Continuous Vulnerability management

   -Controlled used of admin privileges

   -secure configurations for hardware and software on mobile devices, laptops, workstations and servers.

   -maintenance, monitoring and audit of logs.

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?

A: That step would meet the “Continuous Vulnerability management “.

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

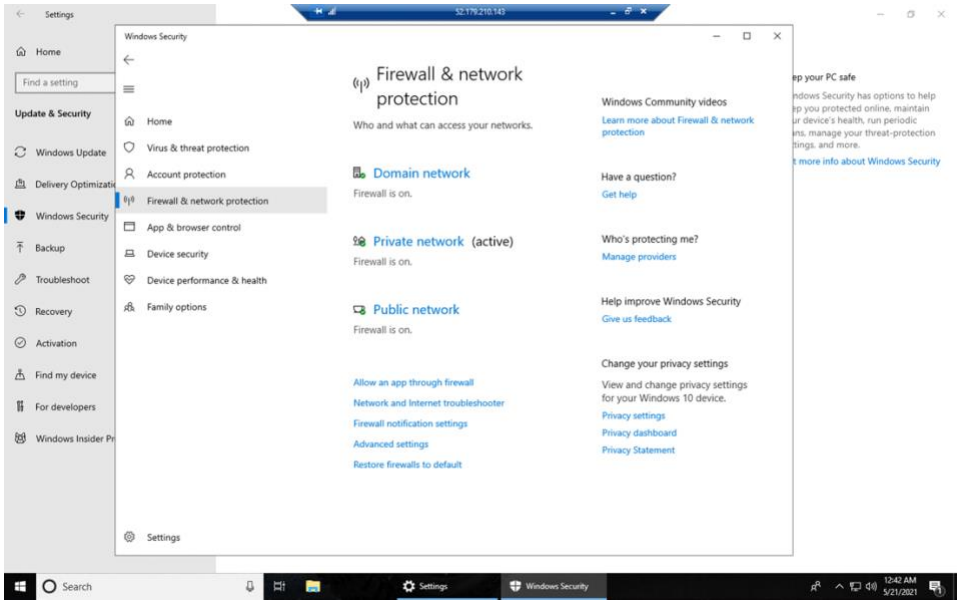
Firewall

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

1. *Explain the process you take to do this.*

A: In the "Windows Security" screen go to "Firewall & Network protection" then enable Microsoft defender firewall for the domain, public and private network, then go to firewall notifications settings to make sure we have the notifications on.

2. *Include screenshots showing the firewall is turned on.*



3. *What protection does this provide?*

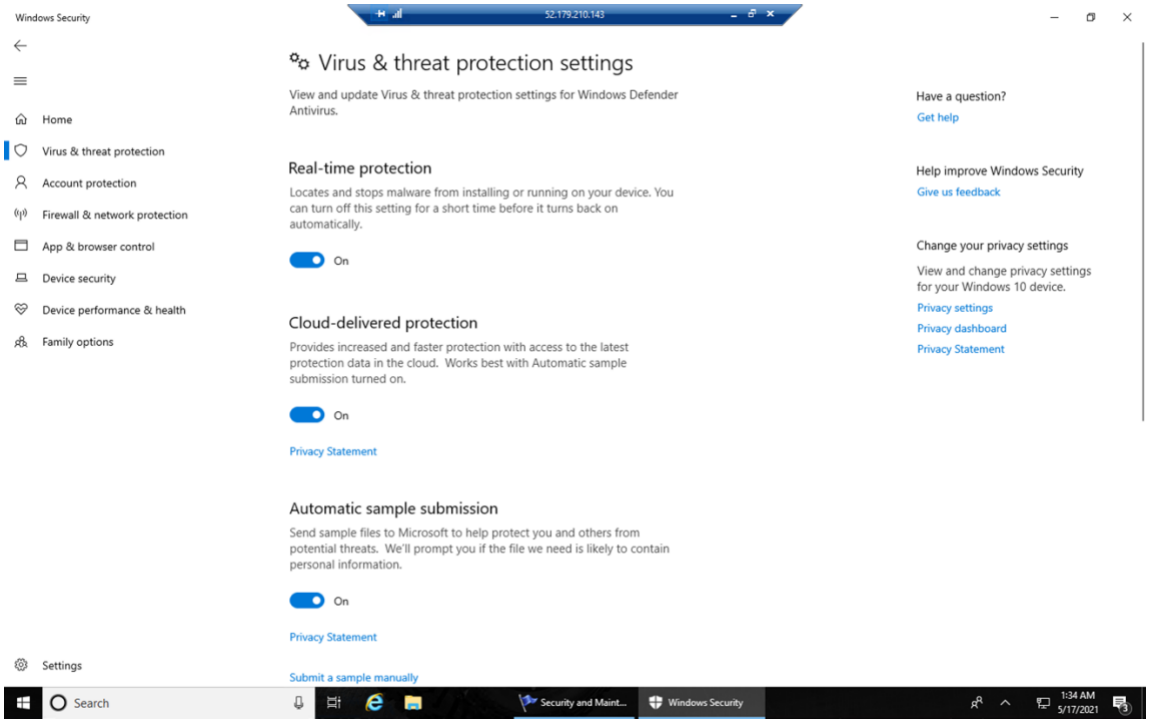
4. *A: this provide protection from public and private networks.*

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.*
   A: Go to the windows security screen, then click in the 'virus and threat protection' section, from there you will choose the 'virus and threat protection settings' option, I made sure to all the protection options were on.

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:*

- Malicious program installed
- Malicious browsers, websites, files, etc.

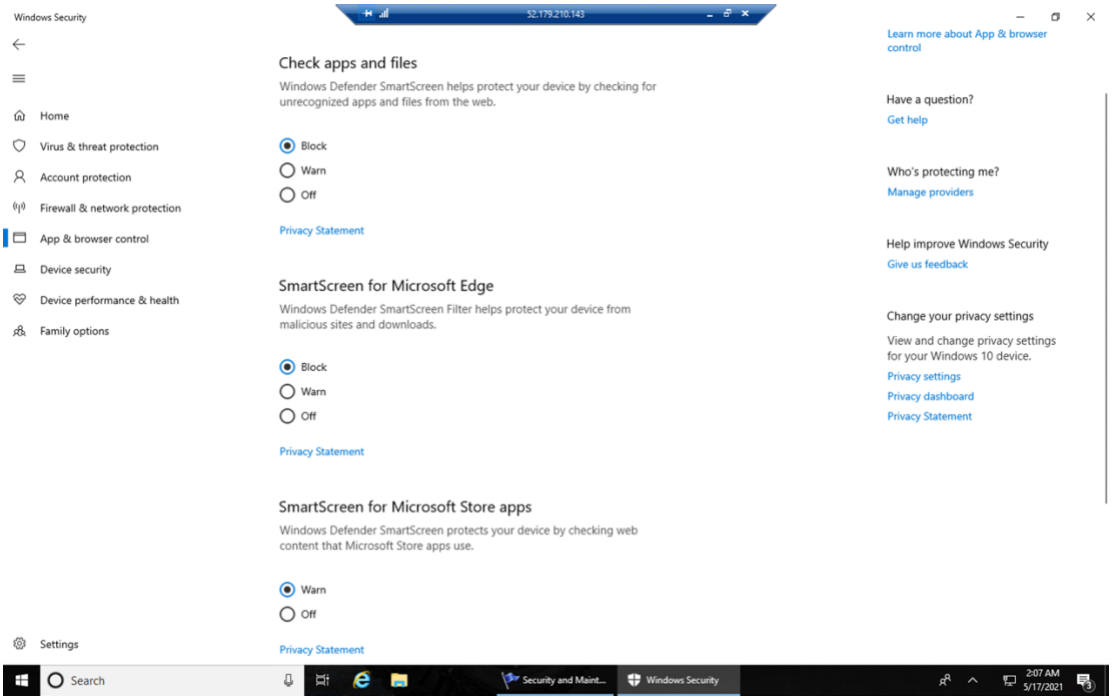
4. *From the CIS baseline controls, provide the controls satisfied by completing this.*

5. A: *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.

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)

ww

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?*
   *A: *Frank*
   ** A hacker*
2. *Bonus questions: What is Hacker's password?*
   A: I can change the password from the user configuration in the control panel

3. *Explain the steps you take to disable or remove unwanted accounts.*
   A: go to the control panel, then go to Users account, then manage accounts, then delete unwanted accounts

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

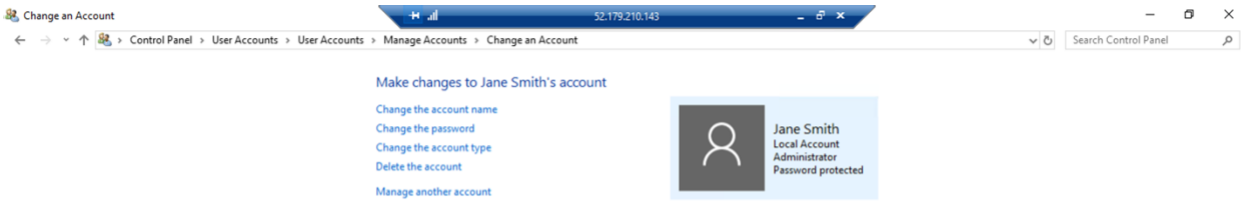
   A: It is very important to remove unneeded accounts because other users can installs malicious programs as well as change security configurations, access private information and use the computer for other activities not related to work which could lead to very serious problems as data breach or a virus infection.

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: *A hacker (shouldn't have admin privileges)
   *A User
   *Joes
   *Janes smith

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

   A: In the control panel/ user accounts / manage accounts:



Administrator privileges for too many users are another security challenge.

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

- Admin accounts can install or downland a malicious program
- Admin accounts can disable configurations creating vulnerabilities
- Admin accounts can change security configurations giving access to the computer to others.

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.*
   A: Control panel/ user accounts/ manage accounts/ change account type:

9. *What is the security principle behind this?*
   A: Principle of least privileges

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

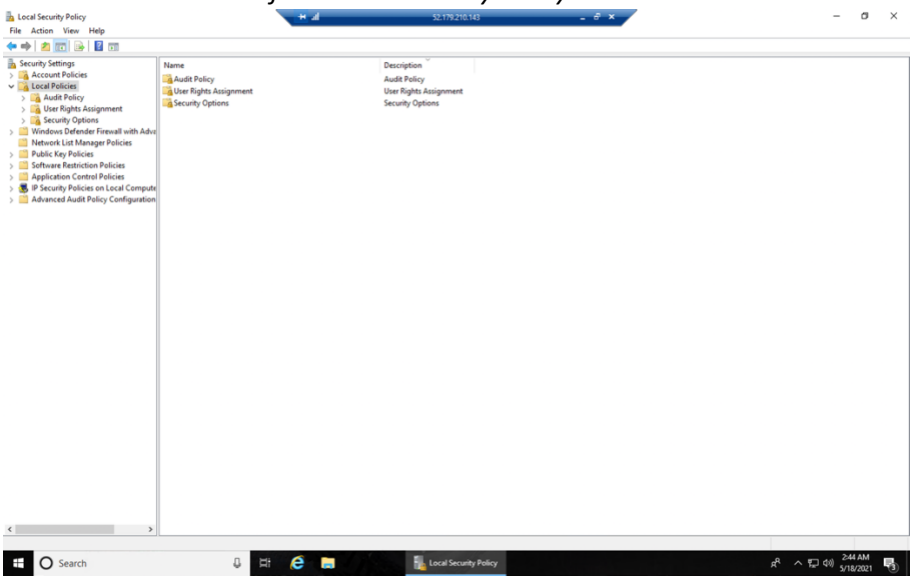
    A: Controlled Use of Administrative Privileges :

    The focus of this control is to ensure that all users with administrative level access use a dedicated or secondary account for any elevated activity. This administrator account should not be used for any other purpose, and should not be used for email, web-browsing, or similar activity.

Setting Access and Authentication Policies

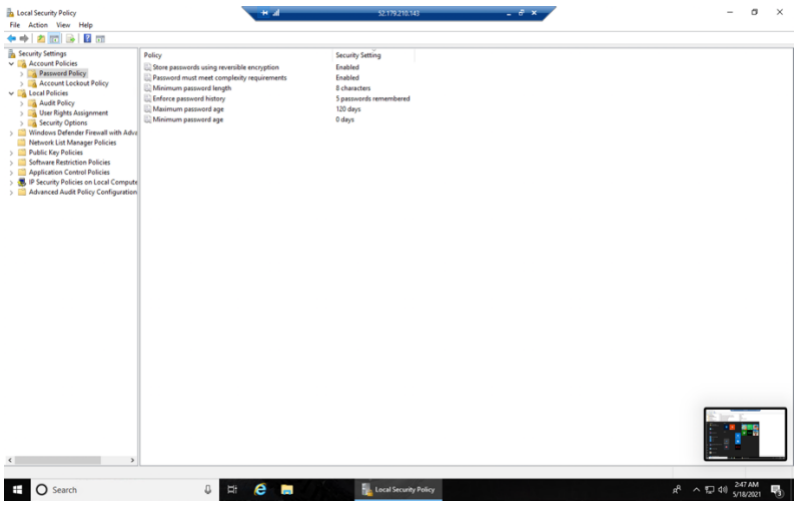
After you talked with Joe about security, he has asked that the access rules outlined above be in place on his PC. These are set using the Local Security Policy function in Windows 10. On the Windows search bar, type "*Local Security Policy*" to access it. Click the > arrow next to both "*Account Policies*"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

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

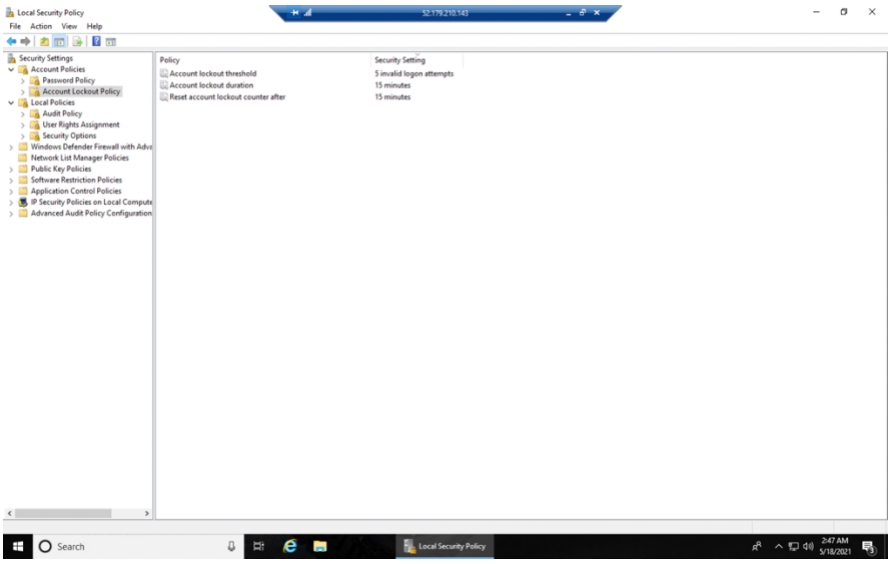


[Note: Local Security Policy is not available on Windows 10 Home edition.]

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: local security policy/ account policy/ password policy/ then set rules:



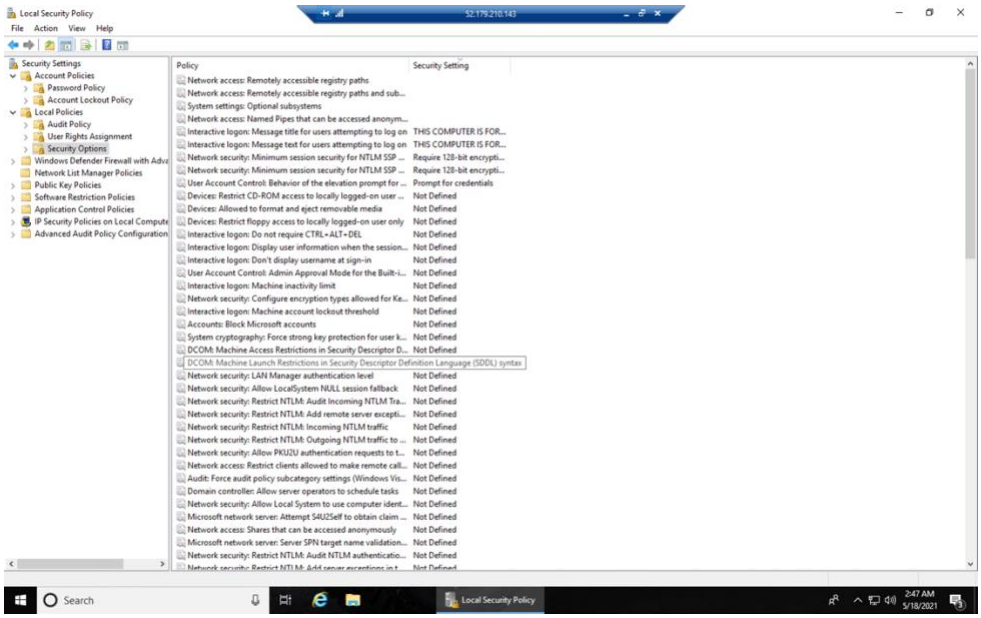
- Setting the Account Lockout Policy: local security policy/ account policy/ lockout policy/ then set rules:



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.*

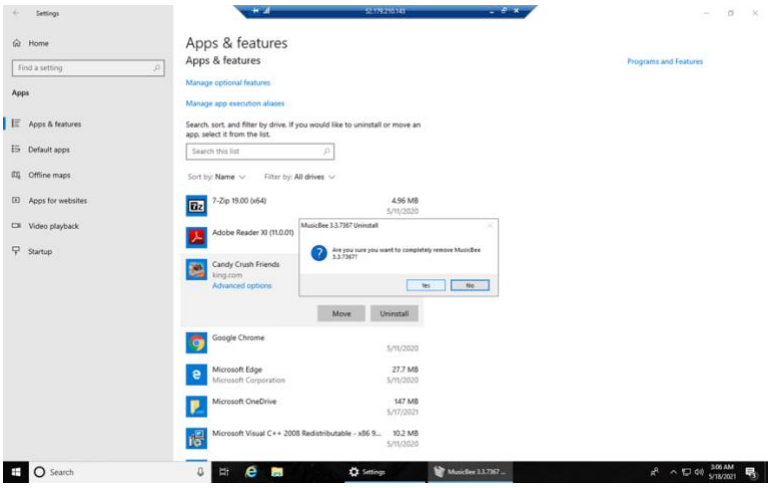
- *Farms heroes saga*
- *MusicBee*
- *Spotify*

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

- *Unnecessary Programs can allow access into the computer*
- *Unnecessary programs or applications can contain or download virus into the computer*
- *Unnecessary programs or applications can consume resources and slow down the system.*

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.*

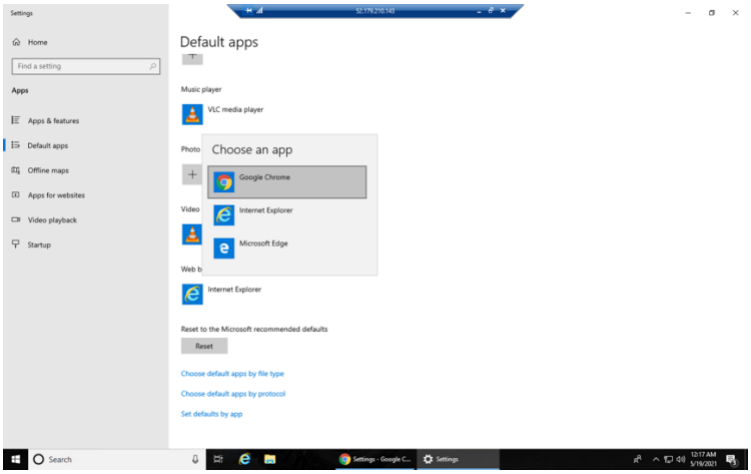
   A: Windows icon/ configuration icon/ Apps/ then choose app> uninstall:



Default Browser

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

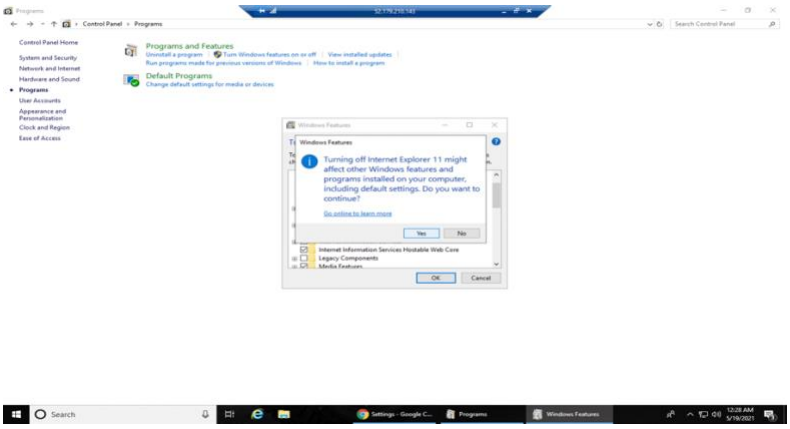
1. *Explain how you set default applications within the Windows 10 operating system. Include screenshots as necessary.*
   A: windows icon/ setting icon/ Apps/ Default apps/ then make select Google chrome as default 'web search'



2. *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
   - Internet explorer allow malicious website hijack computers, infect them with viruses and conduct identity theft
   - The lack of tech support has driven up the cost of web development and stifled innovation

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.

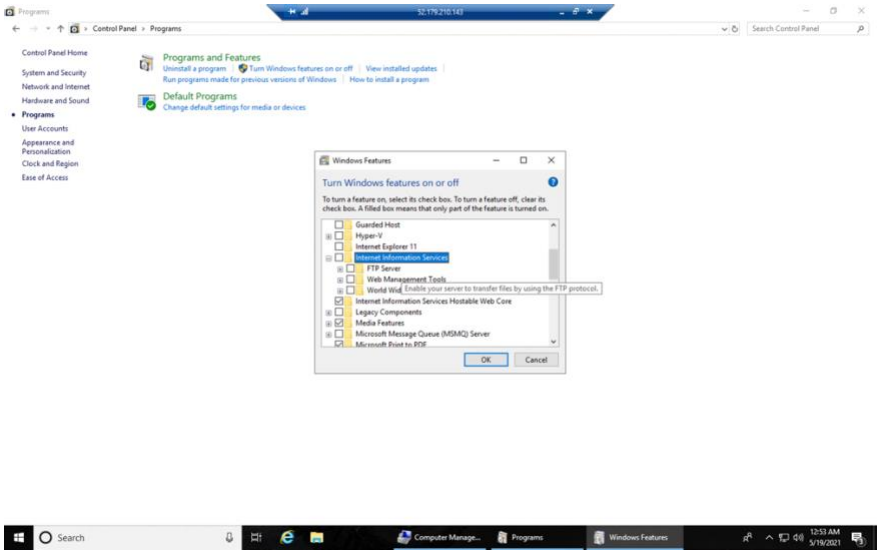
A: Windows icon/ right click/ computer management/ in the left panel click on services and applications.

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?

A: control panel/ programs/ 'turn windows features on'/ then select the internet information services so the square on the left is empty, then restart the pc and check.

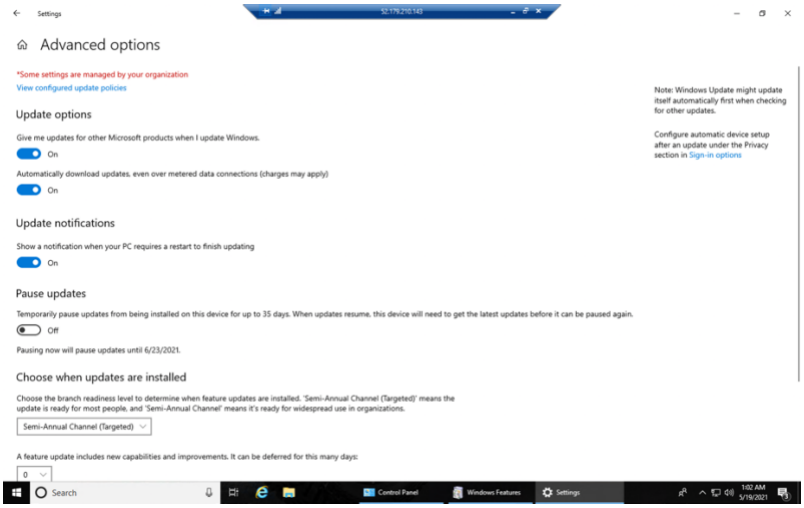
4. Advanced Users: The File Transfer Protocol FTP service is also running on this PC and shouldn't. Explain the process for disabling it and ensuring it is not automatically restarted.



Patching and Updates

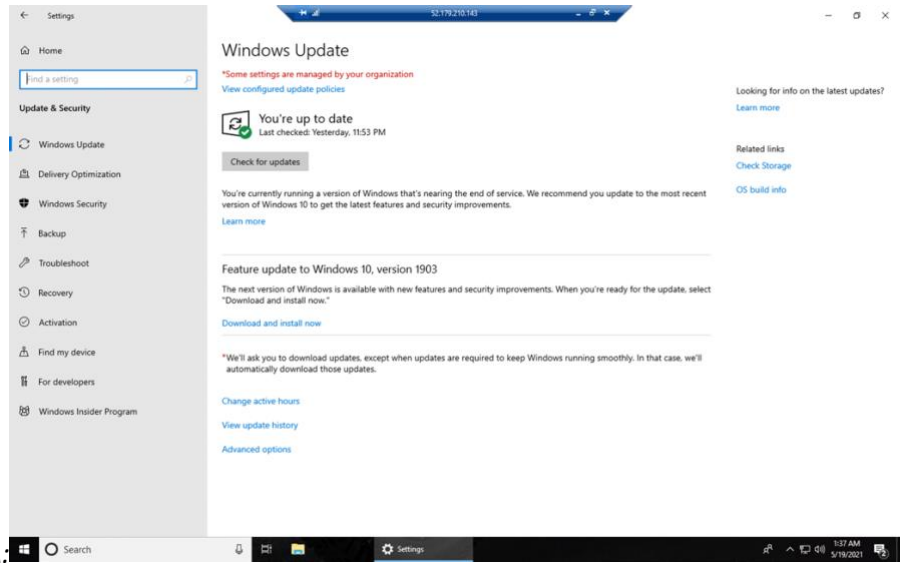
Keeping the operating system current on patches and fixes is a critical part of security. Joe wants his PC to be on the latest version of Windows 10. He also wants you to set it up for automated updates.

1. *Explain the process for doing this. Include screenshots as needed.*
   A: windows icon/ settings icon/ update and security/ advance settings:



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.*

A:



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:*

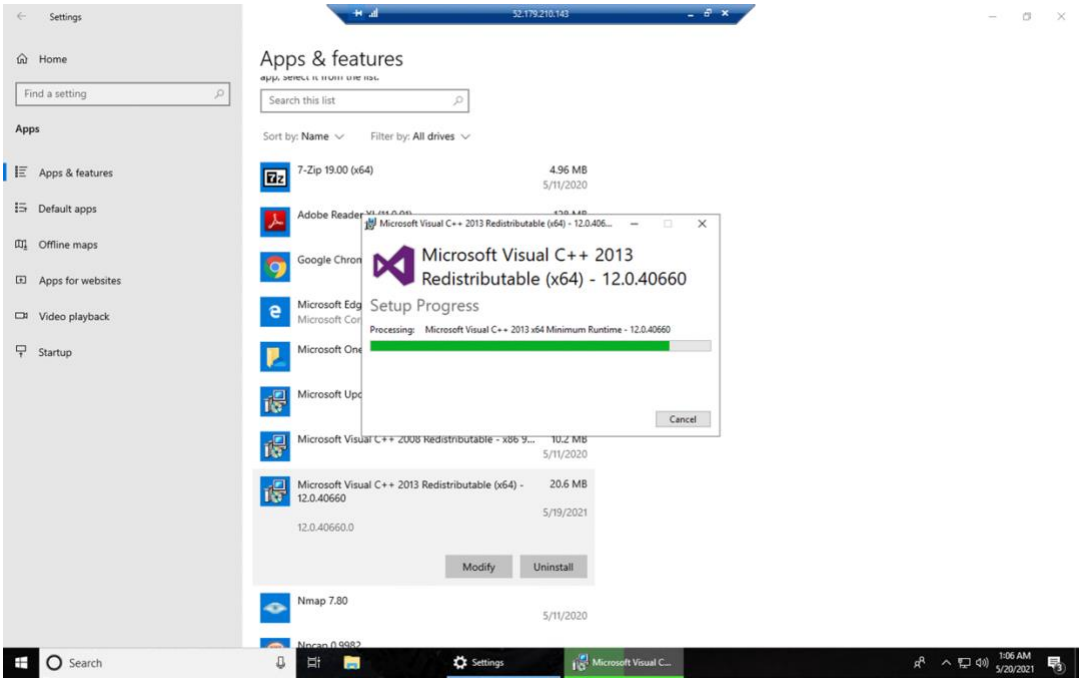
- Adobe reader

- Microsoft Visual C++

4. *Explain the steps you took to determine this information.*
   A: settings panel/ Apps/ then cheek if app needs to be modify

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

   A: Usually you can Update the apps in the "Microsoft store' but I couldn't find the store in this version of windows, so I went to settings/ Apps/ check apps that needs patches or updates/ then proceed to update them.



5. Securing Files and Folders

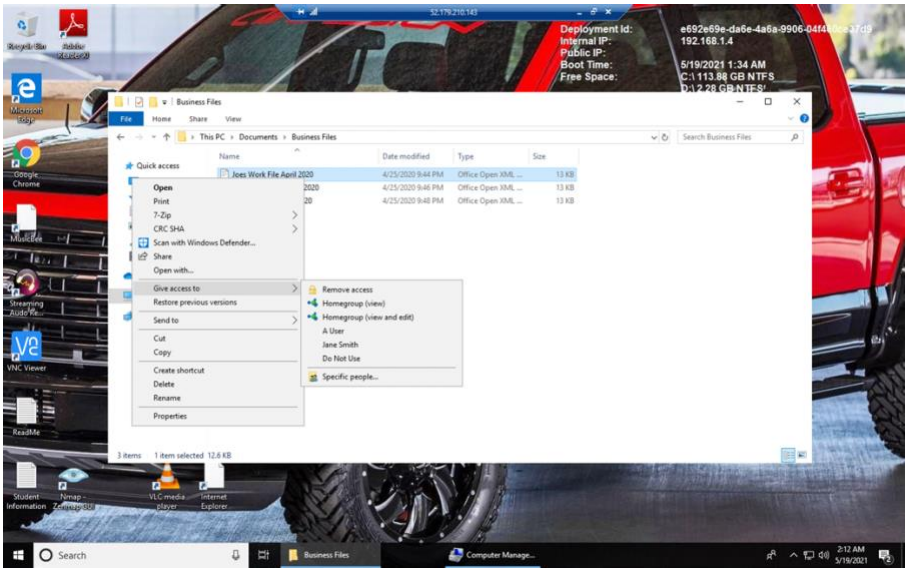
Joe has some work files in his Business folder that he wants to secure since they contain his customer information. They are labeled “JoesWork.”

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.]*

A: right click in the file, then select 'give access to' then choose the user you want to give access to.



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.*

A: click the 7zip app, then select all files, click add, then select your criteria and add your password. I would recommend The AES method

3. *What security fundamental does this provide?*

   A: Confidentiality

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

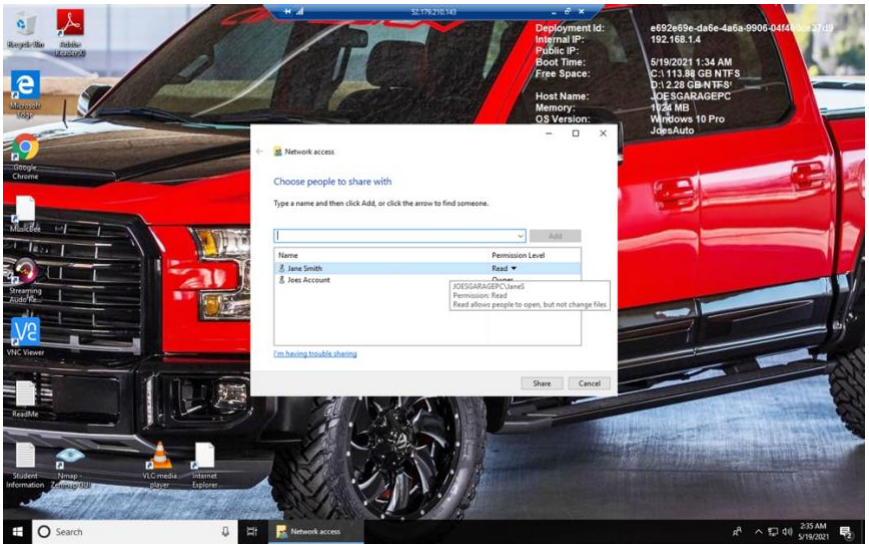
   A: *step 13: Data Protection*

Shared Folders

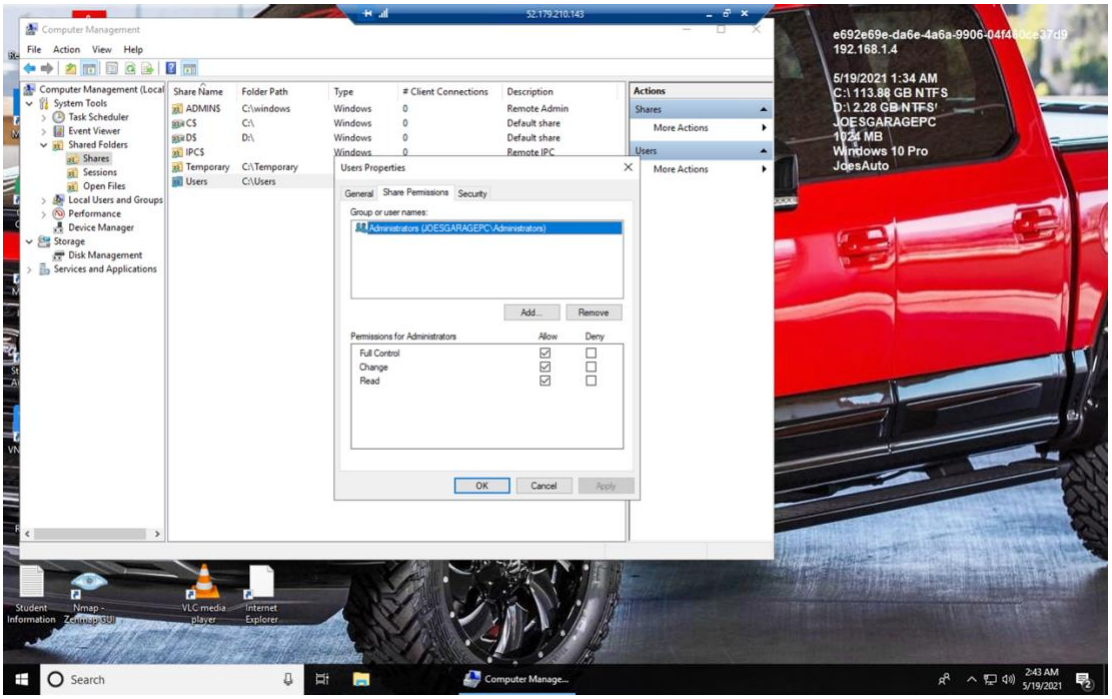
Shared folders are a common way to make files available to multiple users. There's a folder under Joe's documents called "Business Files" that Joe wants shared with his administrator Jane.

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.*

A: right click in the folder/ give access to/ add Jane/ share with Jane.



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]

- Hackers folder
- This pc/ hacker folder/Hidden file
- This pc/ hacker folder/ new bitmap
- This pc/ program Data/ shh
- This pc/ lnetup/ wwwroot

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.