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: Emile Essosso

Date of completion: 24/07/2020

Scenario

Congratulations!

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

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

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

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

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

Account Name: JoesAuto
Password: @UdacityLearning#1

1. Reconnaissance

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

Complete each section below.

Hardware

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

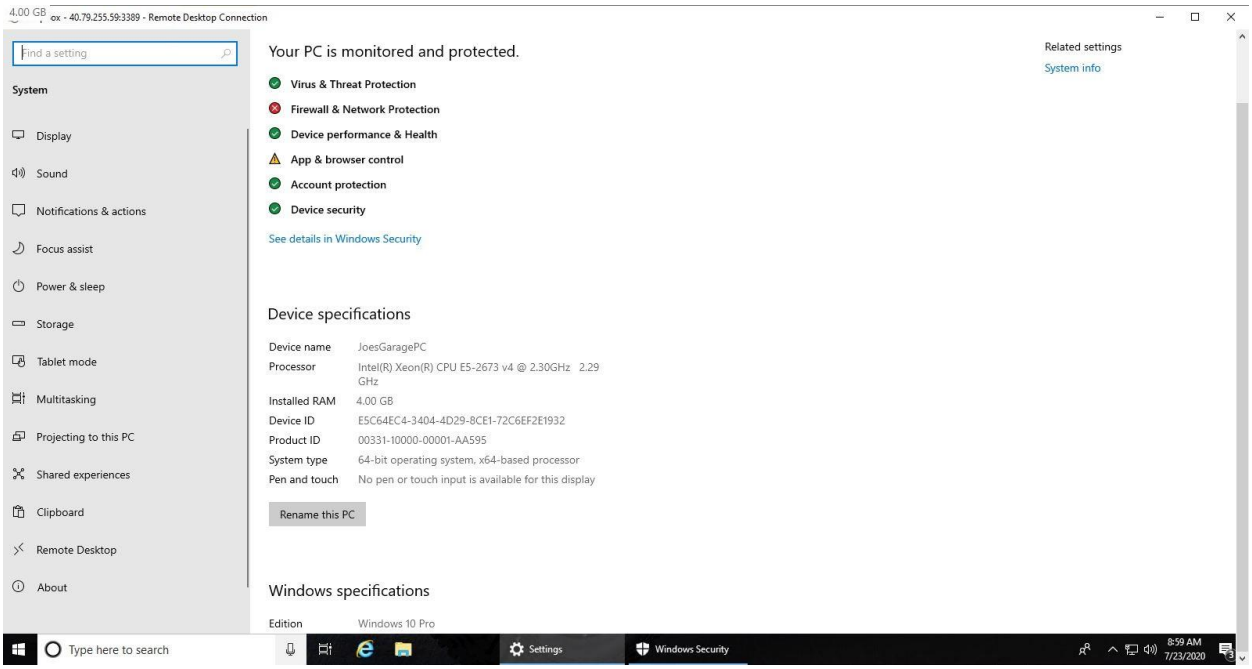
Device Name	JoesGaragePC
Processor	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30 GHz 2.29 GHz
Install RAM	1.00 GB
System Type	64-bit operating system, x64-based processor
Windows Edition	Windows 10 Pro
Version	1809
Installed on	5/11/2020
OS build	17763.1158

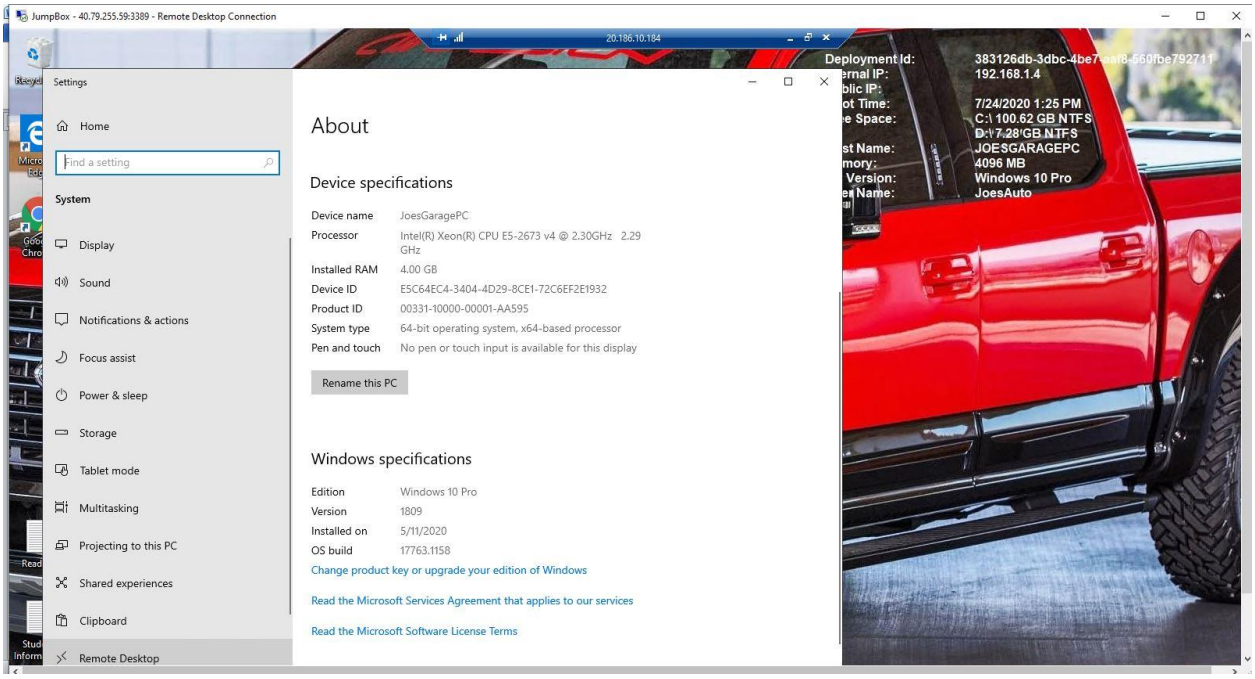
2. *Explain how you found this information:*

   The road map to this information is given bellow:

   Windows Start Button (Right Click) -> Click on System -> This information

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.

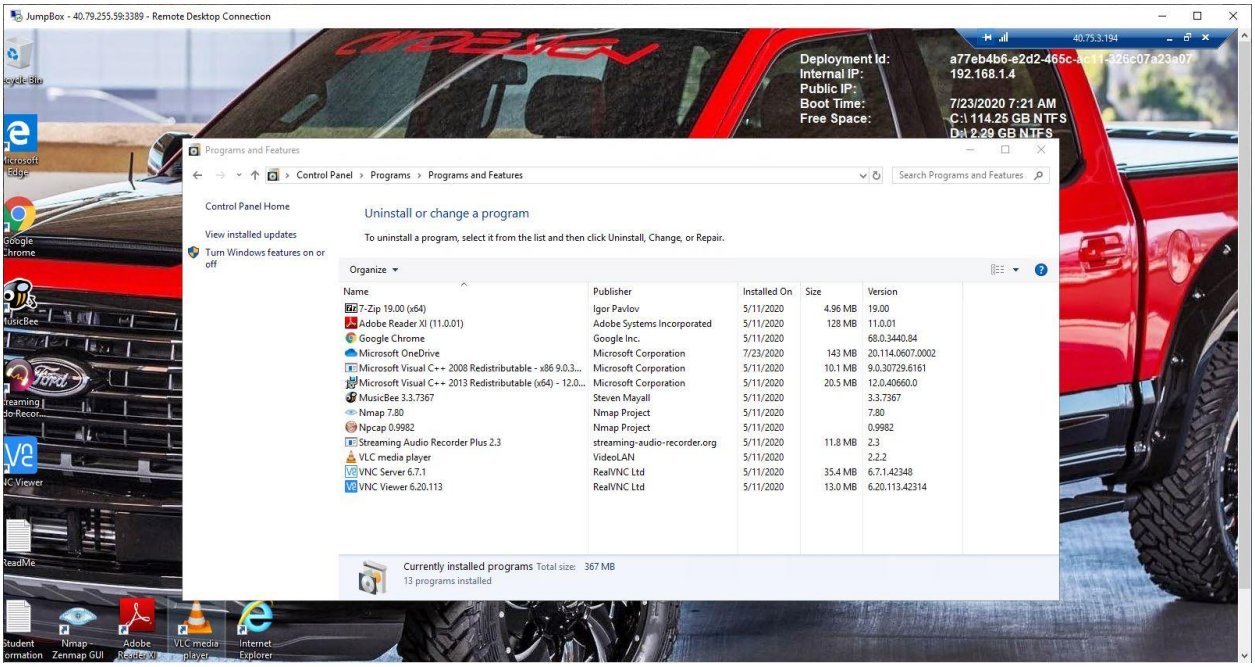
1. *List at least 5 installed applications on Joe's computer:*

- 7-Zip
- Google Chrome
- Nmap 7.80
- Npcap 0.9982
- MusicBee 3.3.7367
- VLC media player

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

   The road map to this information is given bellow:

   Click Windows Start Button - > Write Control Panel - > Select "Uninstall Program" under Program option -> This information



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

   ⇨ According to the Center for Internet Security Control (CIS Control), this falls under the "Inventory and control of Hardware Assets" and "Inventory and control of Software Assets" control of the "Basic Control" section.

Accounts

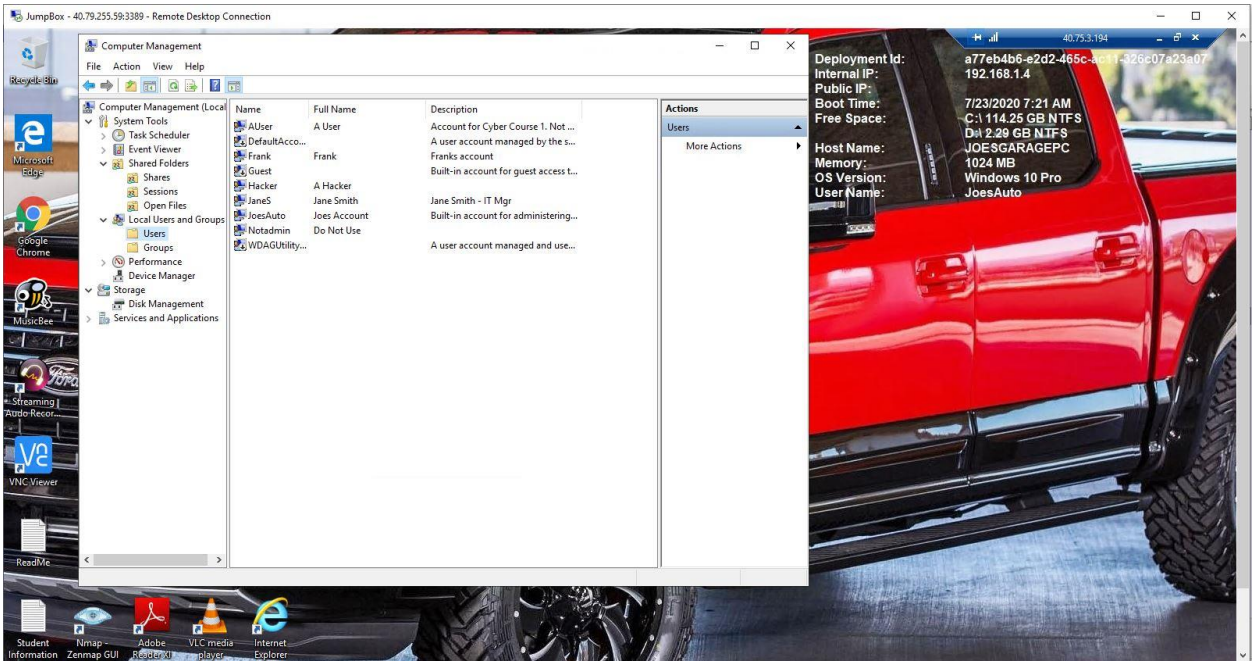
As part of your security assessment, you should know the user accounts that may access the PC.

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	Users
DefaultAccount		System Managed Accounts Group
Frank	Frank	Remote Desktop User, Users
Guest		Guests
Hacker	A Hacker	Administrative, Remote Desktop Users, Users
JaneS	Jane Smith	Administrative, Remote Desktop Users, Users
JoesAuto	Joes Account	Administrative

Notadmin	Do Not Use	Remote Desktop Users, Users
WDAGUtilityAccount		

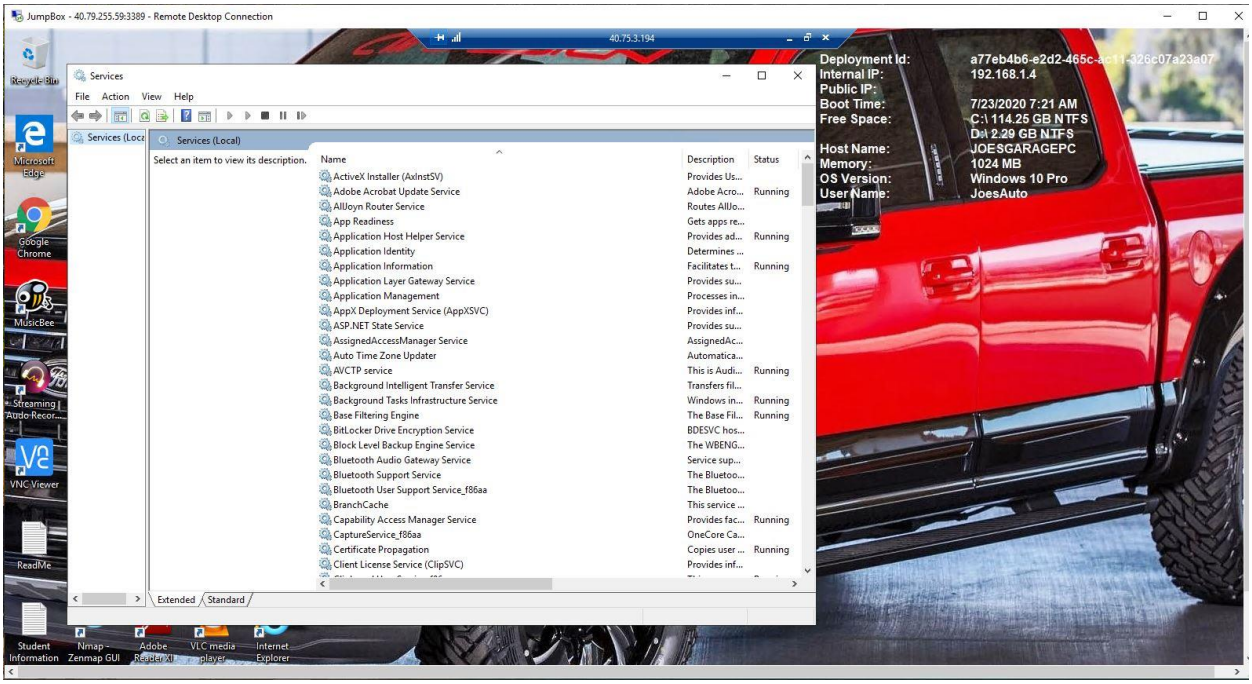
2. *Provide a screenshot of the Local Users.*



Services

Services are applications often running in the background. Most of them provide needed functionality for the PC. Some may also be used to violate security policies.

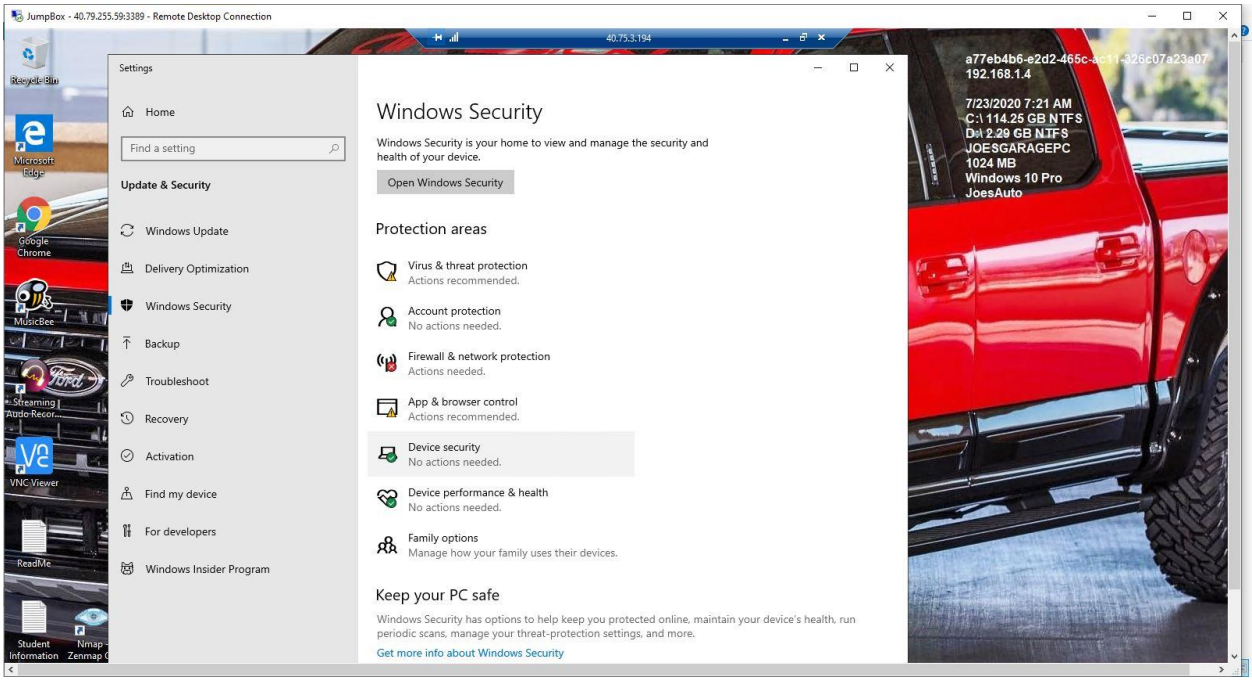
1. *Provide a screenshot of the services running on this PC.*



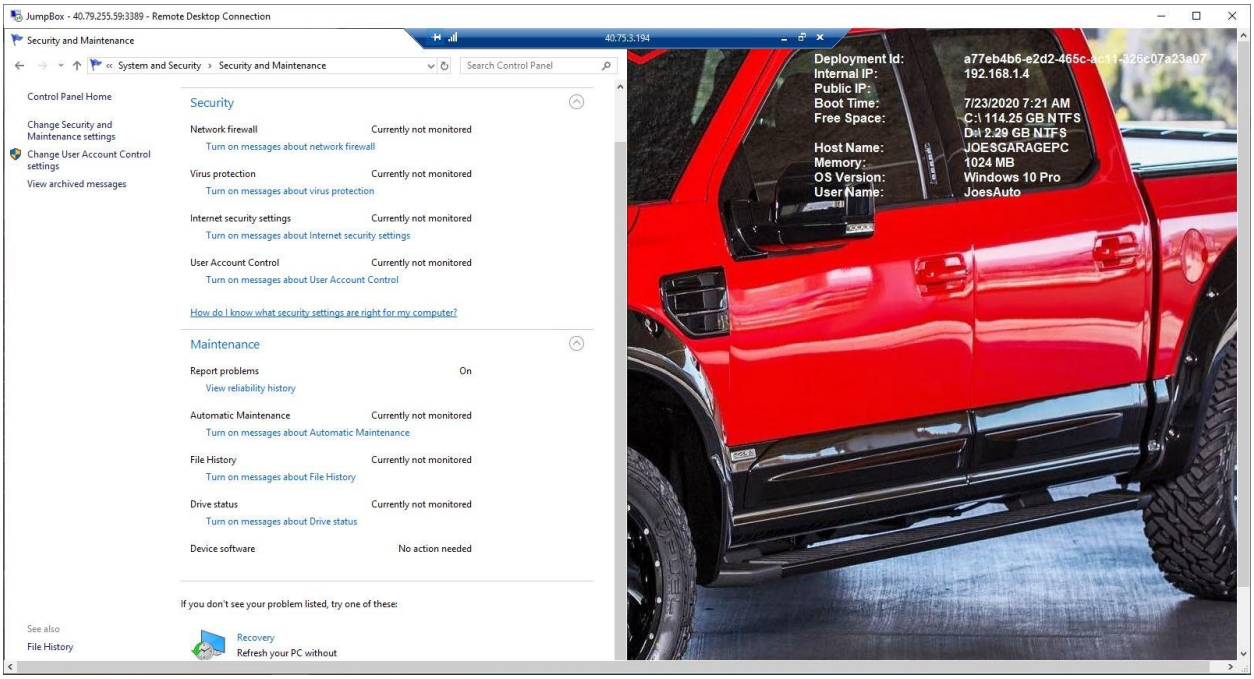
Security Services

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

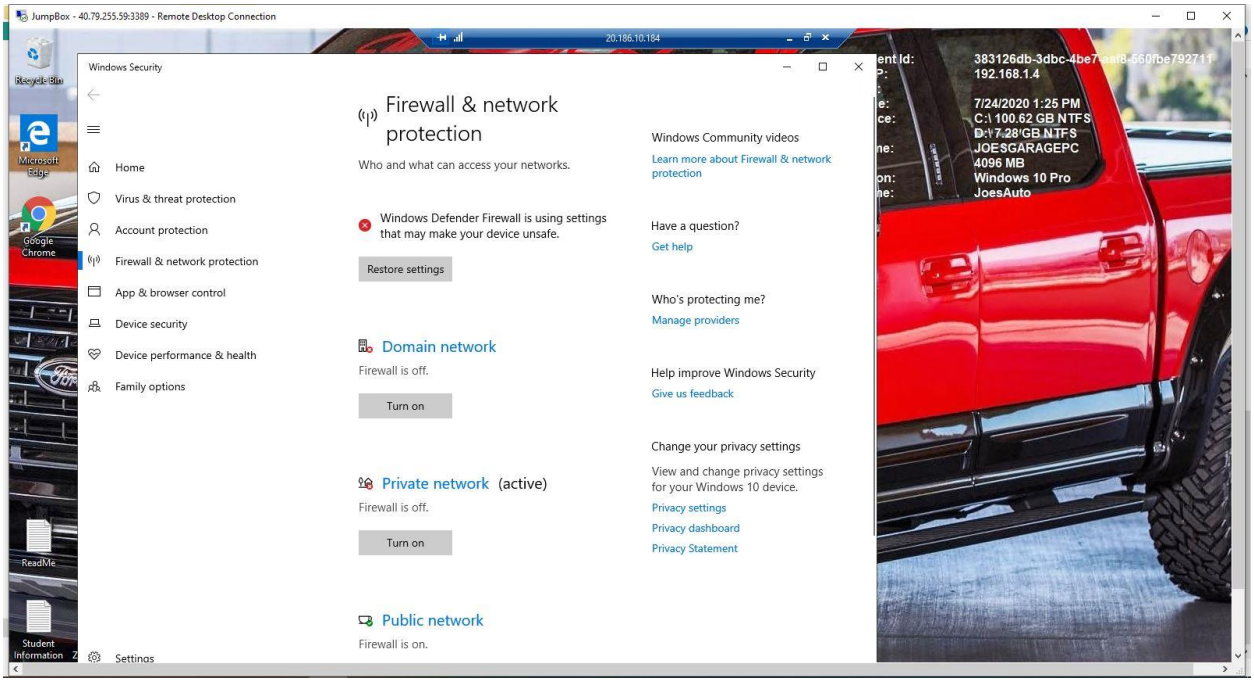
1. *To view a summary of security on Windows 10, start from the **Control Panel**. Use the "Find a setting" bar and search on Windows Defender. You can also search for Windows Defender using the Windows Run bar. Take a screenshot of what you see on the Windows Security screen and include it here:*



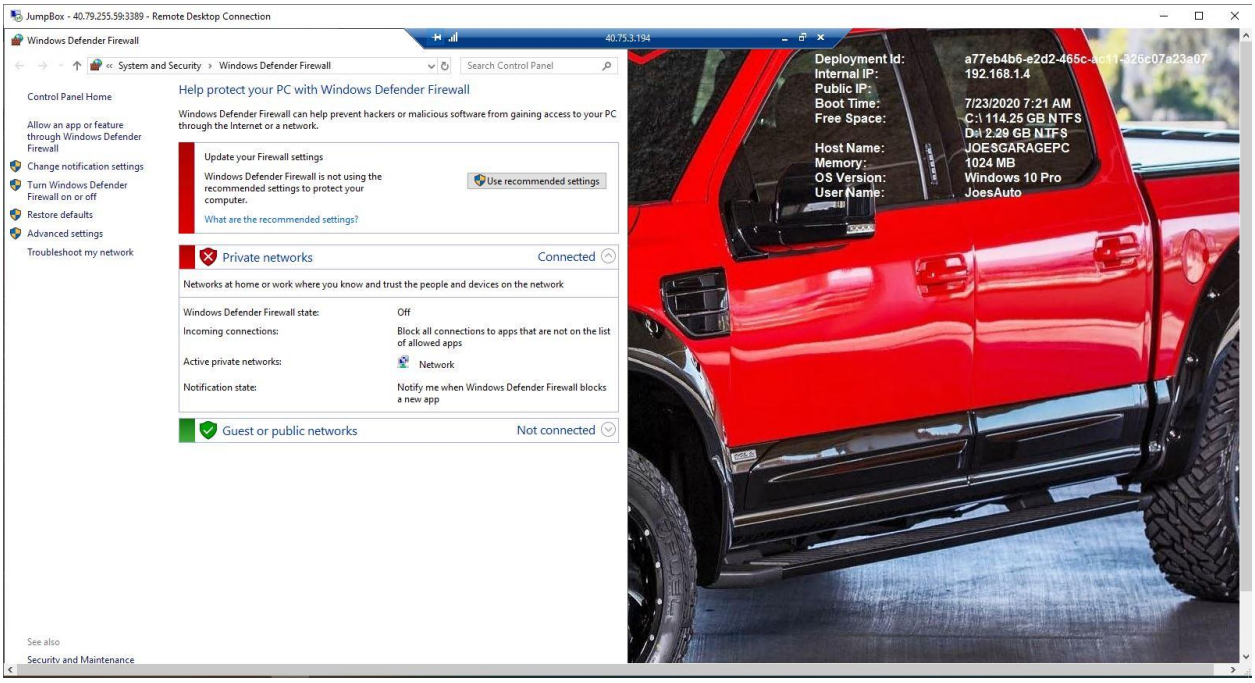
2. *The Windows 10 Security settings are also found from the* ***Control Panel > System and Security > Security and Maintenance****. Start by viewing* ***"Review your computer's status and resolve issues."*** *Provide a screenshot of this below:*



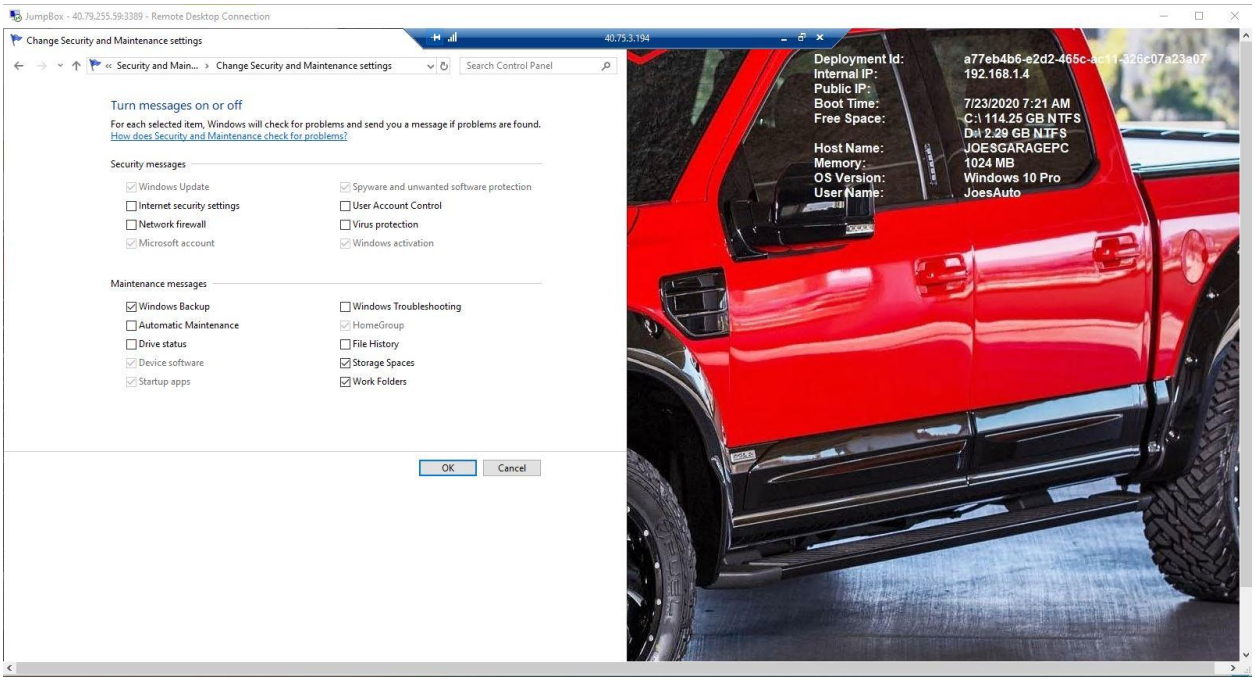
3. *Click on View in Windows Security to see the status there. Provide a screenshot of the* ***Firewall*** *settings.*



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



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



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

Security Feature	**Status**
Firewall product and status – Private network	Connected (Windows Defender Firewall State: OFF)
Firewall product and status – Public network	Not Connected (Windows Defender Firewall State: On)
Virus protection product and status	Actions Recommended
Internet Security messages	Unchecked
Network firewall messages	Unchecked
Virus protection messages	Unchecked
User Account Control Setting	Unchecked

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?*

⇨ The followings are the vulnerabilities and risks :

- Administrative privileges are given to several users which violates Least Privileges, according to CIS Controls. Also, any user having administrative privilege can modify even delete sensitive information of the company which can be catastrophic.
- As firewall is not activated on Private Network, bad actors can easily get access to the network and will try to take actions that might damage the company and users.

- User accounts are not monitored, bad actors might use this opportunity to gain access to the user account and perform damaging action. That's why according to the CIS Controls; users account has to be monitored.

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's Auto Body" works with customer's personal data and due to that fact, it should use industrial standards security policies such as:

- National Institute of Standards and Technology (NIST) Cyber-security framework provides computer security supervision for companies to evaluate and improve their ability to prevent, detect, and respond to cyber-attacks.
- General Data Protection Regulation (GDPR), which is regulation in EU law aims to regulate individuals over their data and simplify the governing environment for global businesses by joining the provision within the EU.
- Center of Internet Security Controls (CIS Controls), which is a short list of highly productive defensive procedures that enables an organization to gain defense in depth knowledge of their cyber security as well as prevent cyber-attacks.
- ISO 27000 Series contains information security standards, which are designed to assist companies in managing cyber-attack risks and internal data security threats.

2. *What industry baseline do you recommend to Joe?*

⇨ I would recommend Joe's Auto Body to embrace CIS Controls as it is easy to understand, maintain and implement in any level of organization. The CIS Controls has 20 simple but effective Steps to insure security for any company. The step also compliments NIST cyber security framework as well as principle of Least Privileges. Thus, embracing these controls will allow customer trust as well as will insure system security.

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?

⇨ According to CIS Controls, it meets “Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers” of “Basic Controls” and “Malware Defenses” of “Foundational Controls”.

System and Security

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

- Firewall
- Virus & Threat Protection
- App & Browser Control
- User Account Control settings
- Securing Removable Media

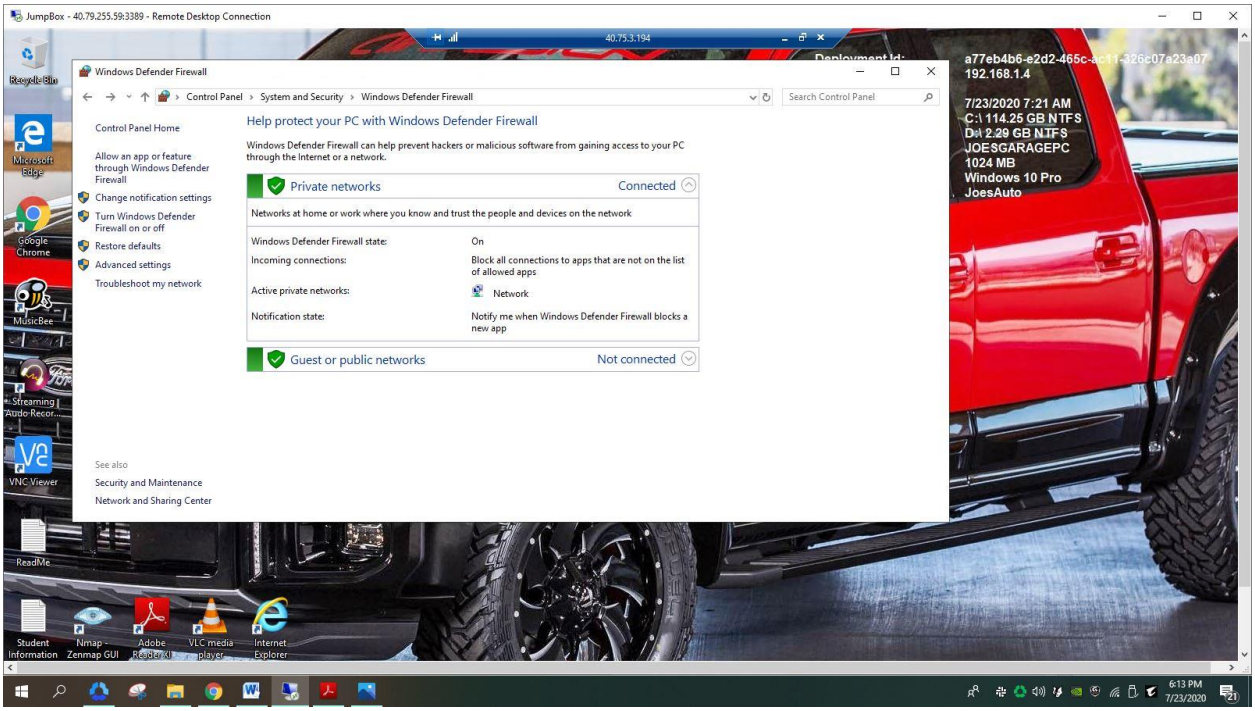
Firewall

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

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

⇨ Step 1: Click on the windows start button and type “Control Panel” and click on it.
Step 2: Click on “System and Security”
Step 3: Click on “Windows Defender Firewall”
Step 4: Click on “Turn Windows Defender Firewall on or off”
Step 5: Check “Turn on Windows Defender Firewall”

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



3. *What protection does this provide?*

⇨ Windows Defender Firewall protects the host device from unauthorized access over the network and filters network traffic permitted to enter or exit the device.

Virus & Threat Protection

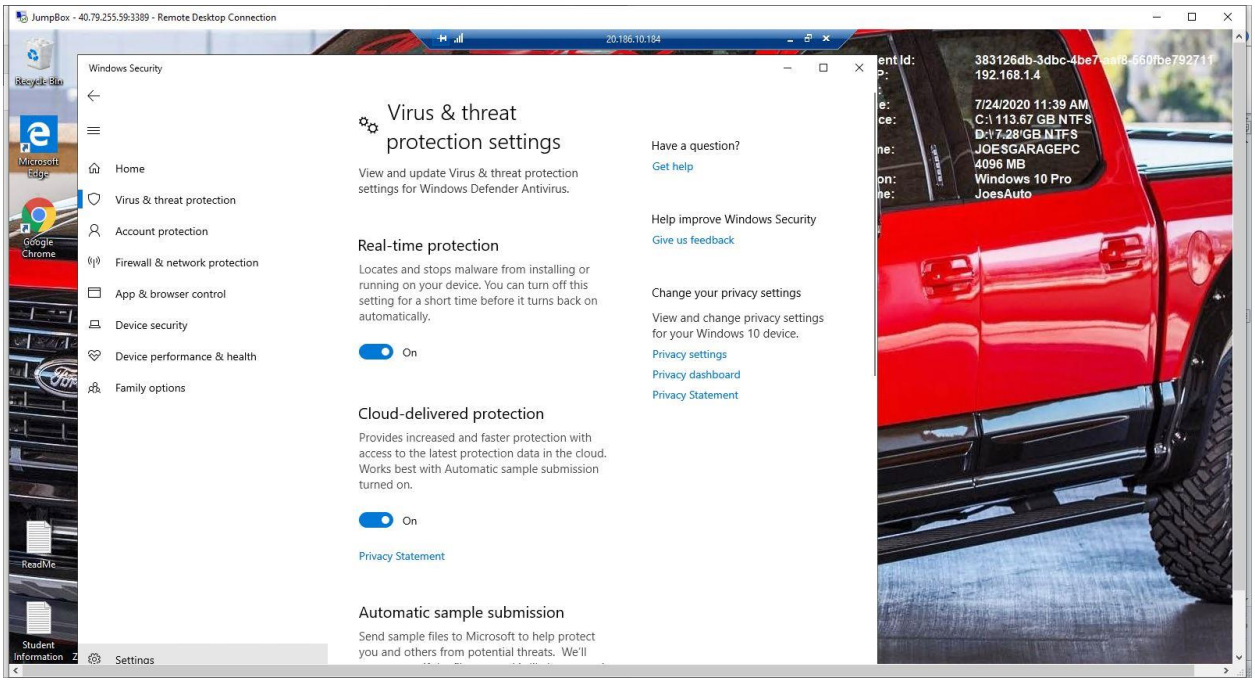
You need to ensure the Windows Defender anti-virus is enabled to always protect against current threats. It should be set to automatically update and continually scan the PC for malicious software. Note: Ignore any alerts about setting up OneDrive.

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

⇨ Step 1: Type “Virus and Threat Protection” on windows search bar and click on the option titling that. In the Virus and Threat Protection, click on “Manage setting” of “Virus & threat protection setting”. Turn on “Real-time Protection” and “Cloud-delivered protection” as well as “Automatic Sample Submission”.

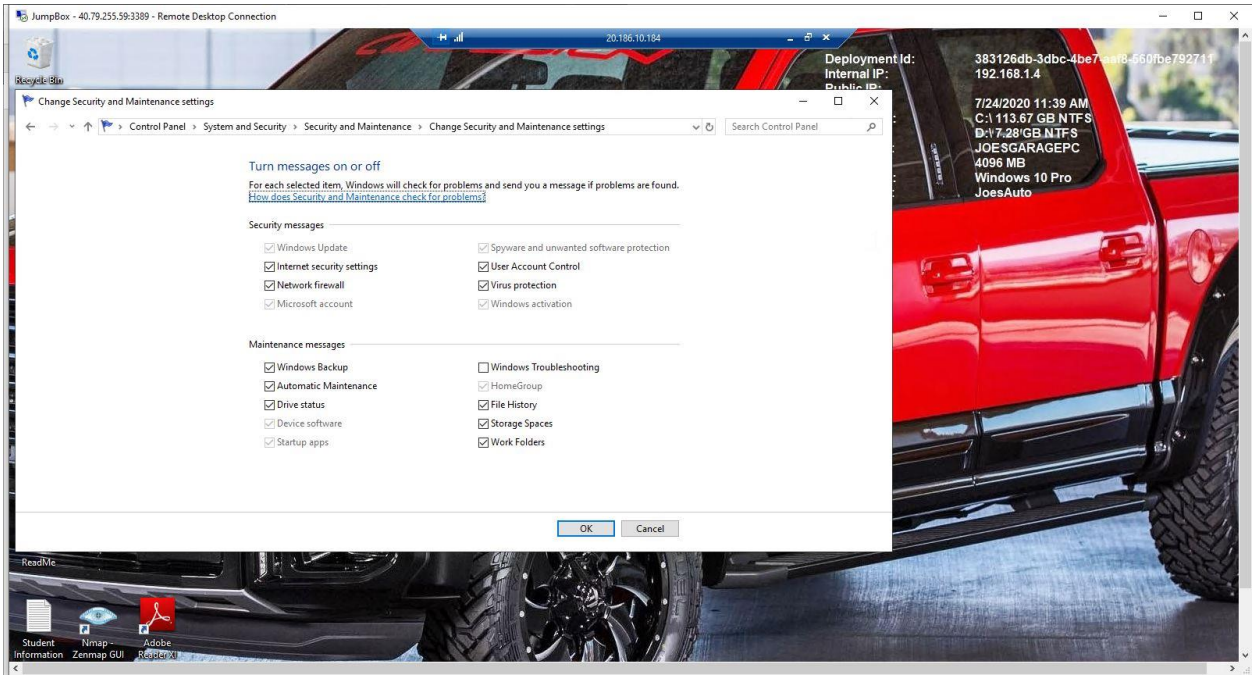
Step 2: On the virus “Virus & Threat Protection Setting” click on “Turn On”

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:*

- As Network firewall, it scans the Internet traffic and blocks outside user or unauthorized individual from accessing the network. Turning on the message for this will notify user that bad actors trying gain access to the network.
- As Virus Protection message is enabled, the host will get notified if malwares or viruses are trying to cause damage to the system.

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

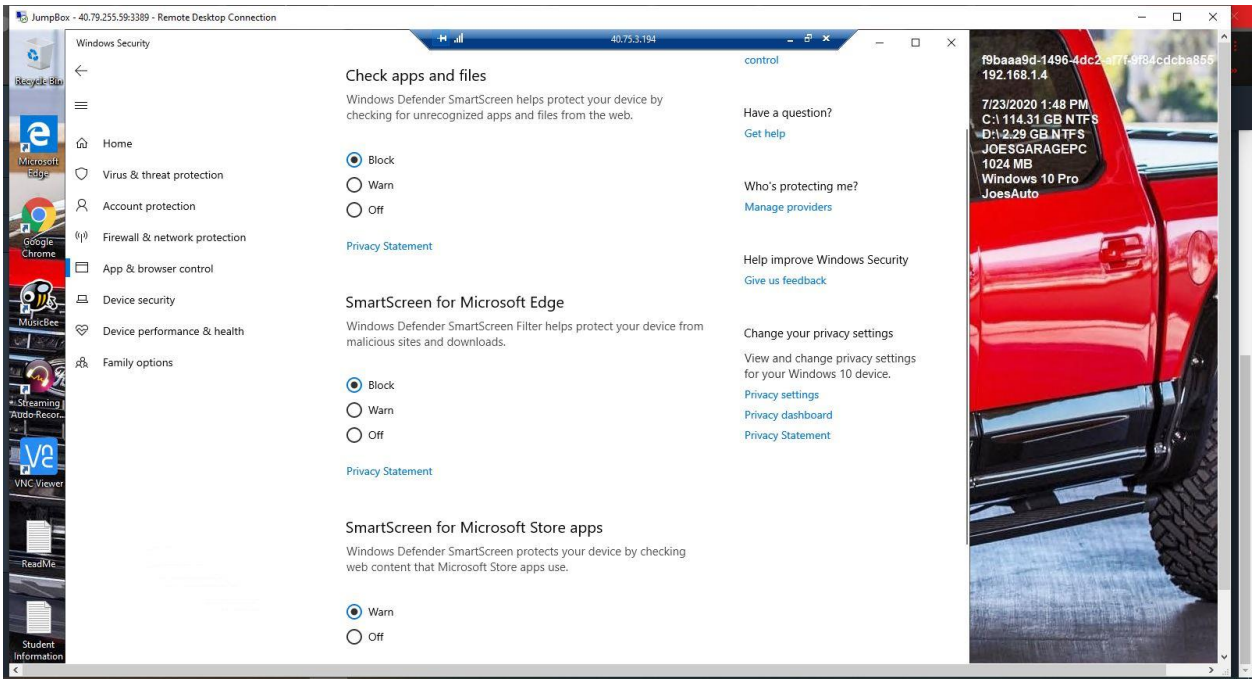
⇨ From CIS baseline controls, this actions satisfies “Malware Defenses” and “Secure Configuration for Network Devices, such as Firewalls, Routers and Switches” of “Foundational Control”

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?*

➢ The current UAC setting on Joe's computer is "Never Notify"

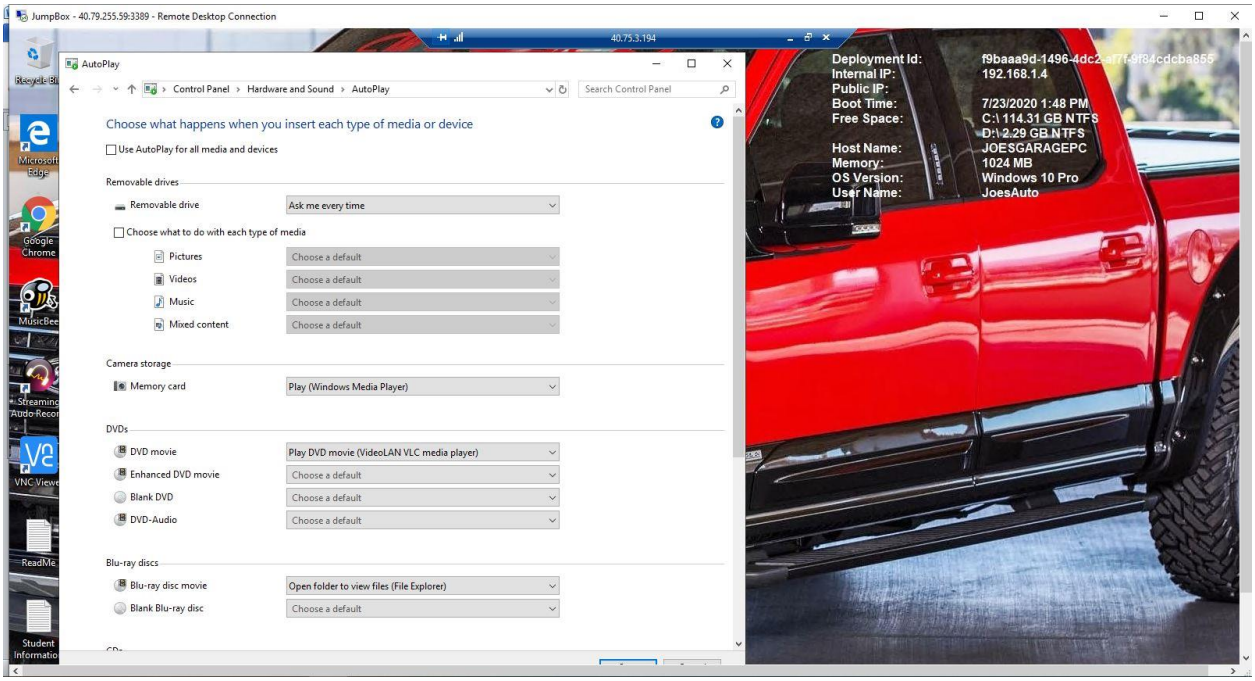
2. *What should it be set to? Include a screenshot of the new setting.*

➢ It should be at least set to "Notify me when apps try to make changes to my computer"

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?*

⇨ a. Frankb. Hacker

2. *Bonus questions: What is Hacker's password?*

⇨ The password of Hacker is : 3b80J8C2

3. *Explain the steps you take to disable or remove unwanted accounts.*

⇨ Step 1: Right click on the windows icon and go to Computer management
Step 2: Under "Local Users and Groups" double click on the "users" option
Step 3: Right click on the user that you want to remove and click the "Delete" option.

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

⇨ Unneeded accounts are one of the major reasons of security breach. An ex-employee (bad actor) could cause damage by leaking confidential data to a competitor. Also, if they had administrator privileges, they can install malware or delete the necessary software required for the system. This can cause the company catastrophic damage.

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

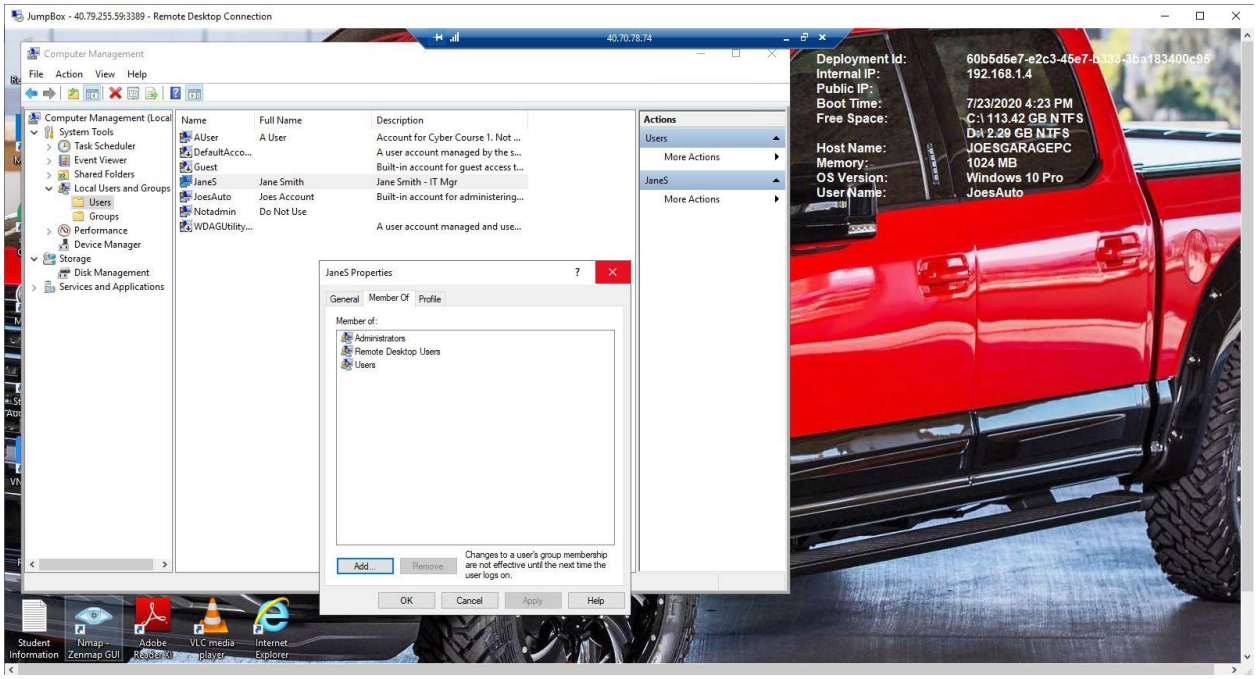
5. Which account(s) have administrator rights that shouldn't?

⇨ As the Hacker account is removed the only other account that has administrator rights apart from the "JoesAuto" and "AUser" is "JaneS" which shouldn't.

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

⇨ As we are on the computer management window and in "user" section, we want to see the privileges a specific user has. In order to do that we do the following:

- Right click on the user and select properties
- On properties windows, select the "Member of" tab. There we can see what privileges the user has.



Administrator privileges for too many users are another security challenge.

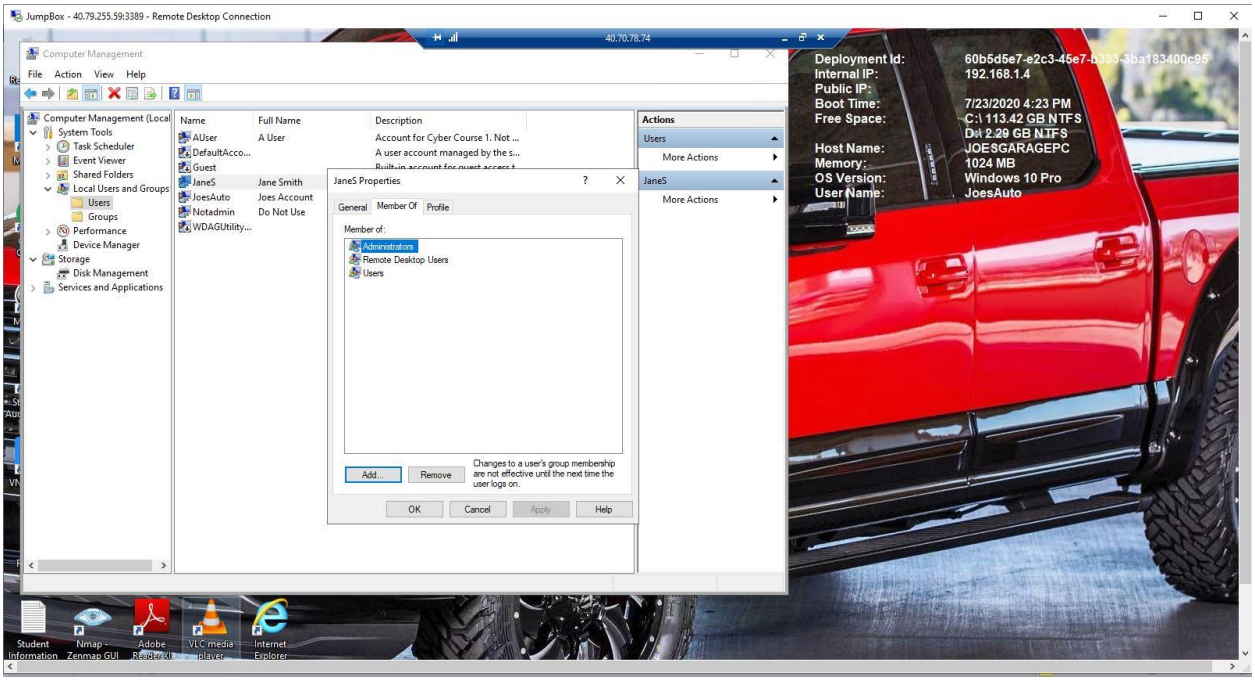
7. Provide at least three risks associated with users having administrator rights on a PC.

- If users want to damage the company for a reason and they have administrator privileges, they can delete sensitive information and install malware or uninstall necessary programs from device which can cause severe damage to the company.
- User (bad actor) can share confidential data to other competitor company if the user has administrator privileges.
- If users account is hacked by bad-actor then, hacker can damage the company by many means if that user has administrator privileges.

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.

⇨ Step 1: Right click on the user and click “Properties”.
Step 2: Select the “Member Of” tabs.
Step 3: Click on the “Administrator” in the “Member Of” box.
Step 4: Click on the remove button and click OK



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

⇨ The principle behind removing administrator privileges from users is “Least Privilege”.

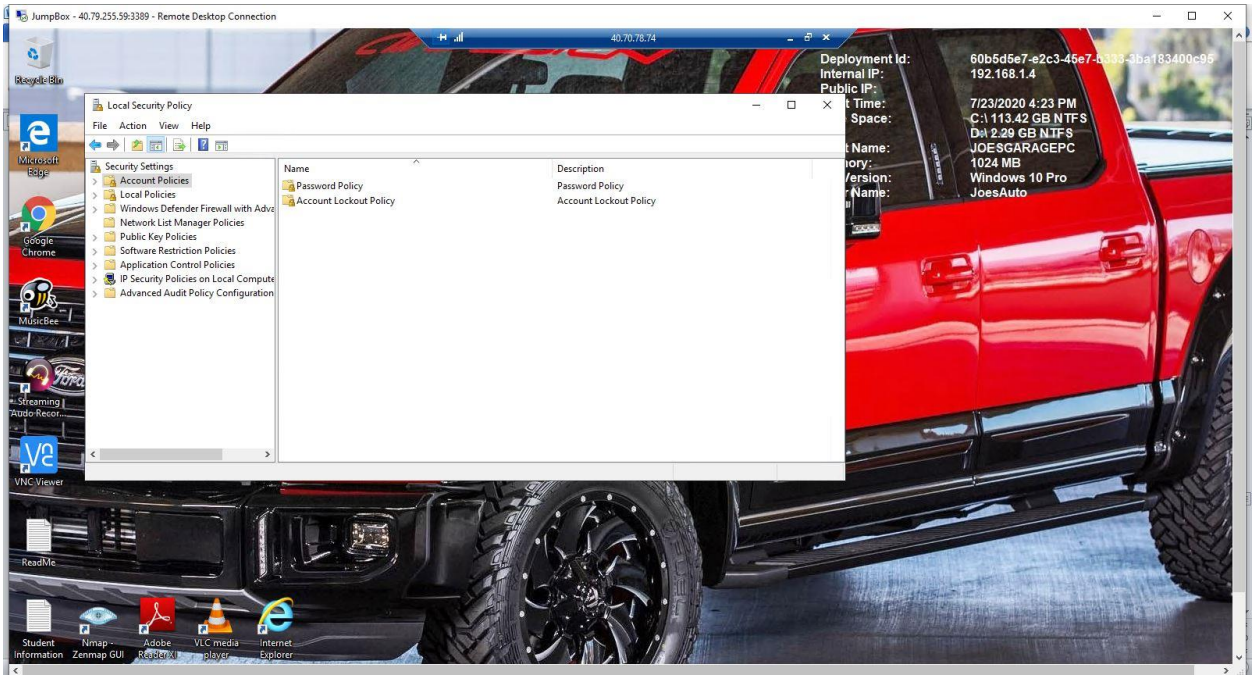
10. The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?

⇨ According to CIS Controls, this fits with “Controlled Use of Administrative Privileges” of “Basic Control” and “Controlled Access Based on the Need to Know” of “Foundational Control”.

Setting Access and Authentication Policies

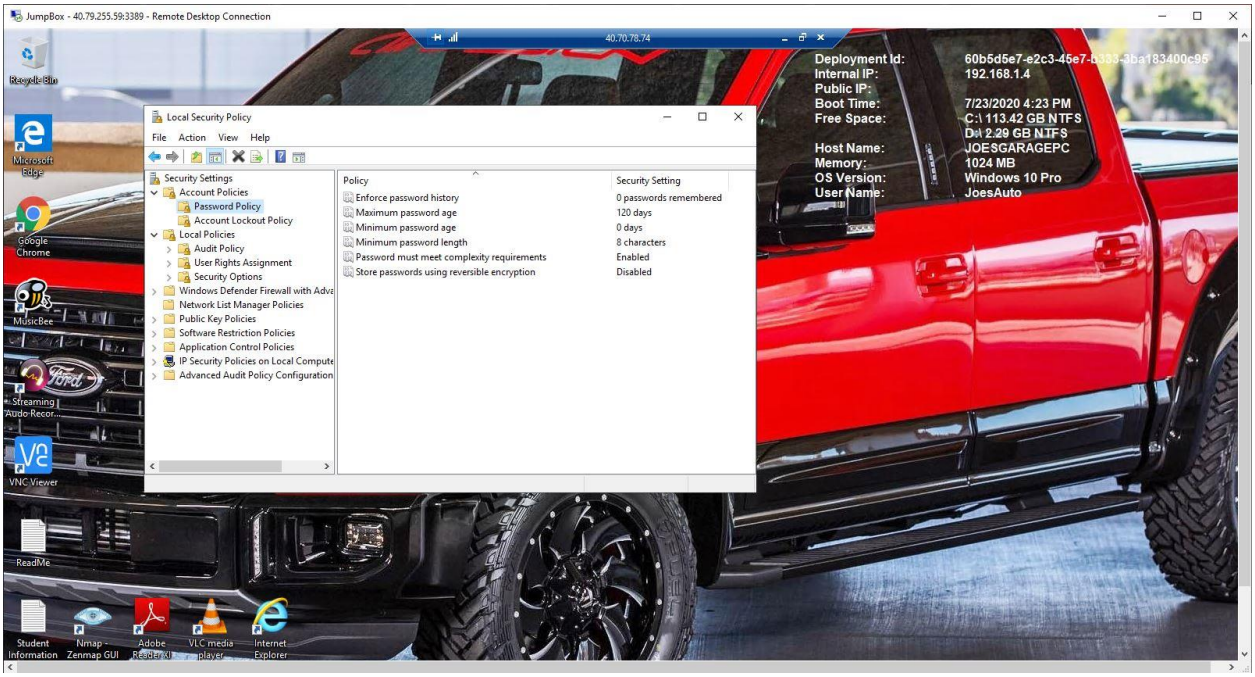
After you talked with Joe about security, he has asked that the access rules outlined above be in place on his PC. These are set using the Local Security Policy function in Windows 10. On the Windows search bar, type “*Local Security Policy*” to access it. Click the > arrow next to both “*Account Policies*”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

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



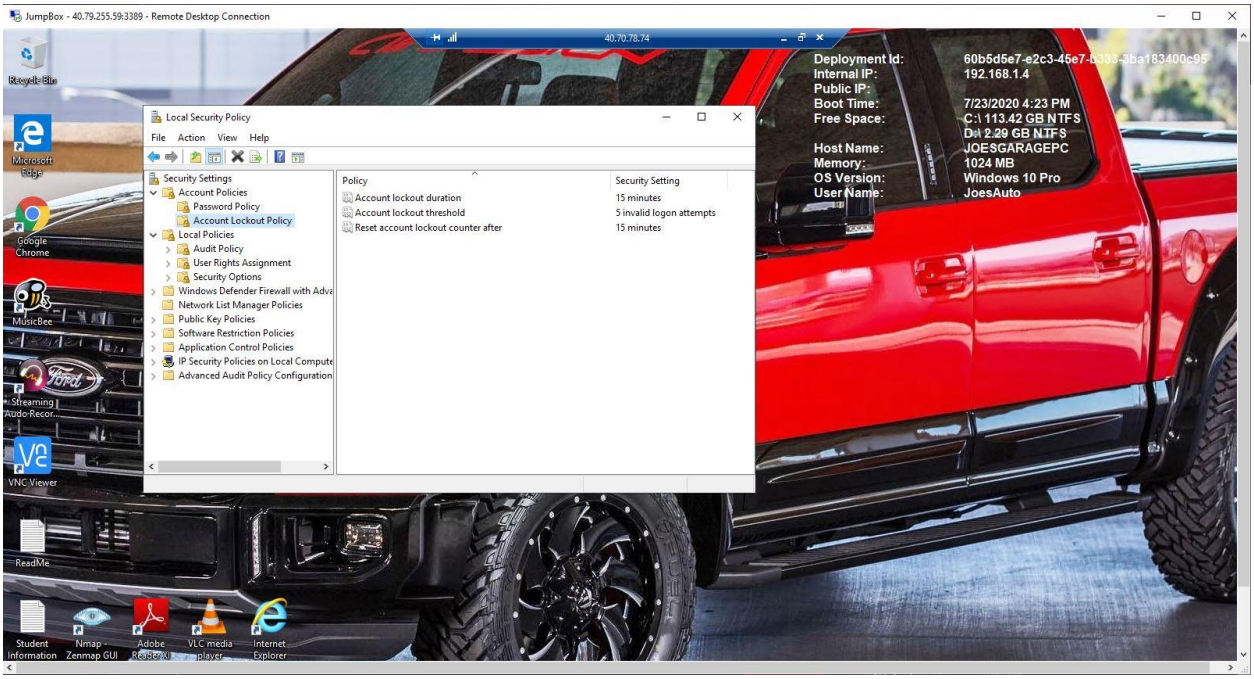
2. Explain the process for setting the password and access control policies locally on a Windows 10 PC. Provide screenshots showing how you set the rules on the PC.

- Setting the Password Policy:
  Step 1: On Local Security Window, Go to “Password Policy” under Account Policies.
  Step 2: Double Click on the Password Policy option.
  Step 3: Make Necessary changes according to the above scenario.



- Setting the Account Lockout Policy:

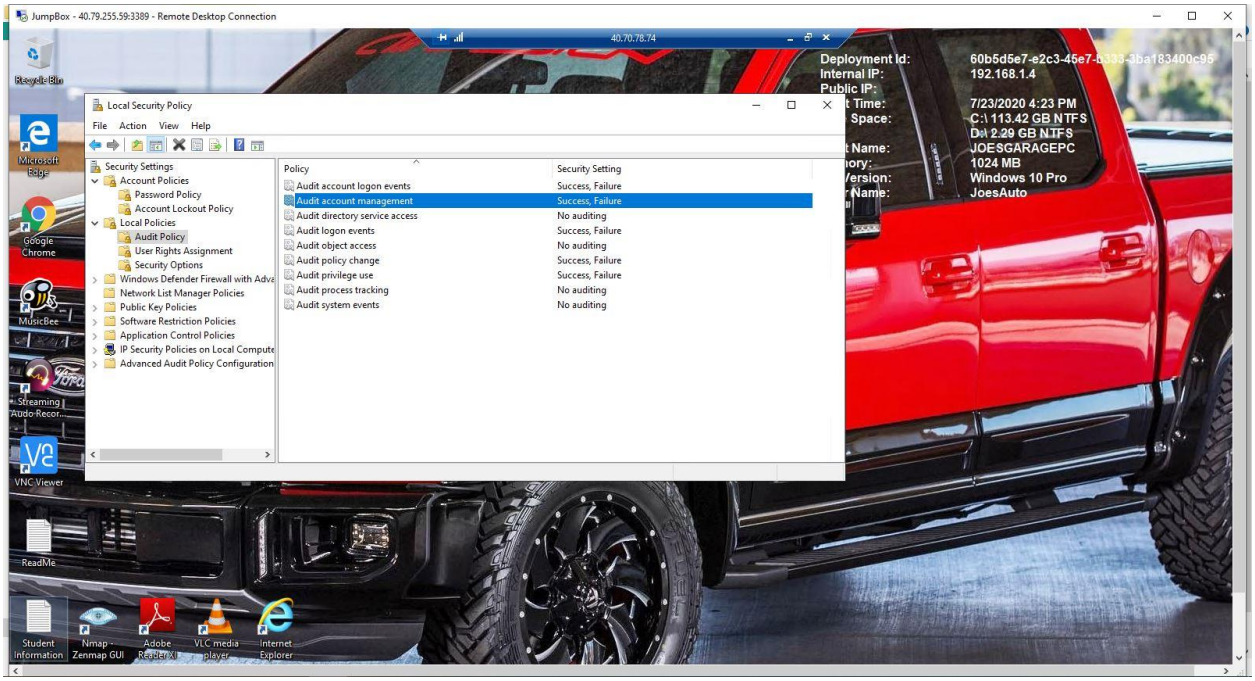
Step 1: On Local Security Window, Go to “Account Lockout Policy” under Account Policies.
Step 2: Double Click on the Account Lockout Policy option.
Step 3: Make Necessary changes according to the above scenario.



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.*

- Streaming Audo Recorder Plus
- VLC media player
- Candy Crush Friends

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

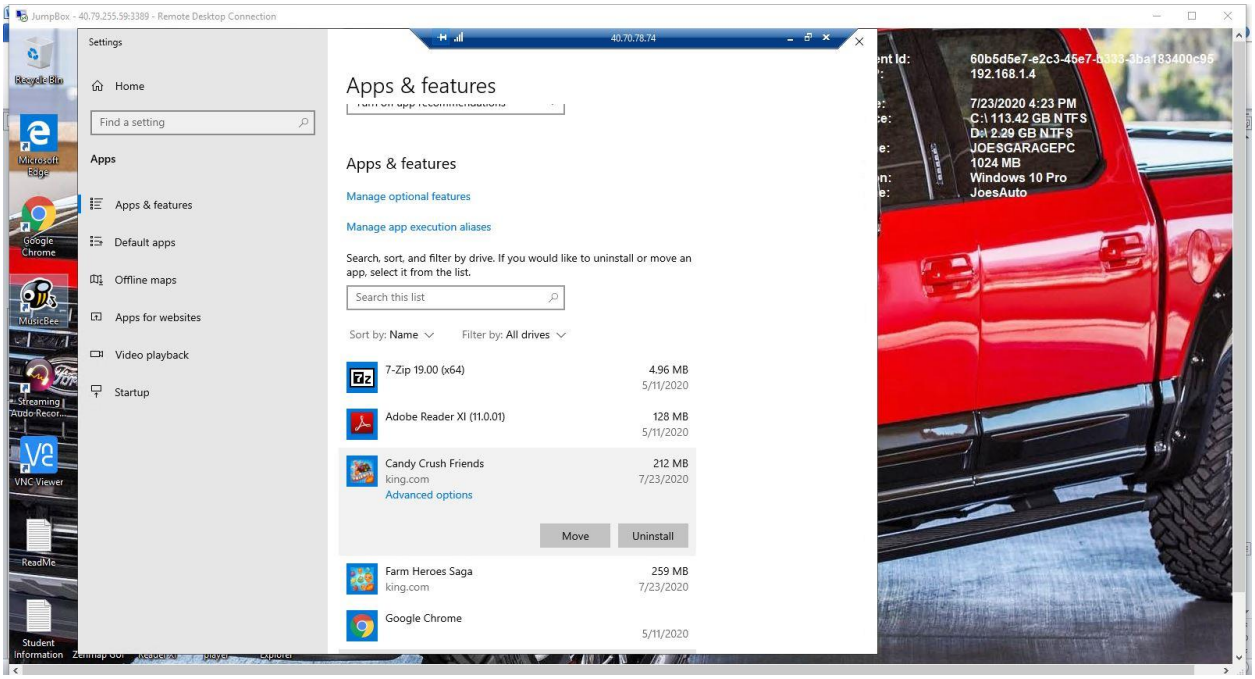
- Unwanted application can be the access point of bad actor to breach the system
- Using unwanted application, bad actor can steal data and damage the company

- Using unwanted application, bad actor can hack into user account and thus can perform action that can bring catastrophic damage to the company.

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.*

⇨ In order to remove unwanted application, do the following:

- ➢ Right click on the windows icon
- ➢ Click on the Apps & Features option
- ➢ Then on the Apps & Features window, click the app that has to removed and click uninstall. Again click uninstall on the pop up window.
- ➢ This can be done for all the unwanted apps.

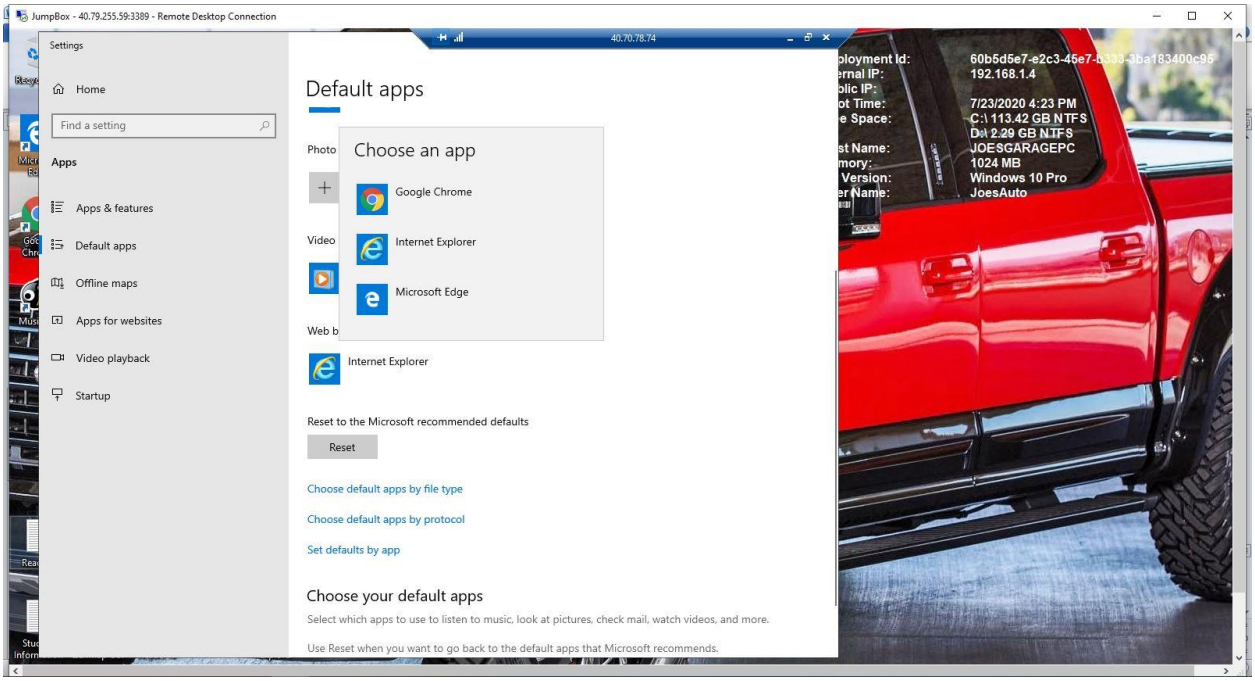


Default Browser

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.*

⇨ In order to set default apps, do the following:
Step 1: Click on the windows icon and click setting
Step 2: Click on “Apps” on Windows Setting window.
Step 3: Click on the default apps and choose default app as “Chrome” for browser.
Step 4: Same thing can be done for other apps as well for other sectors.

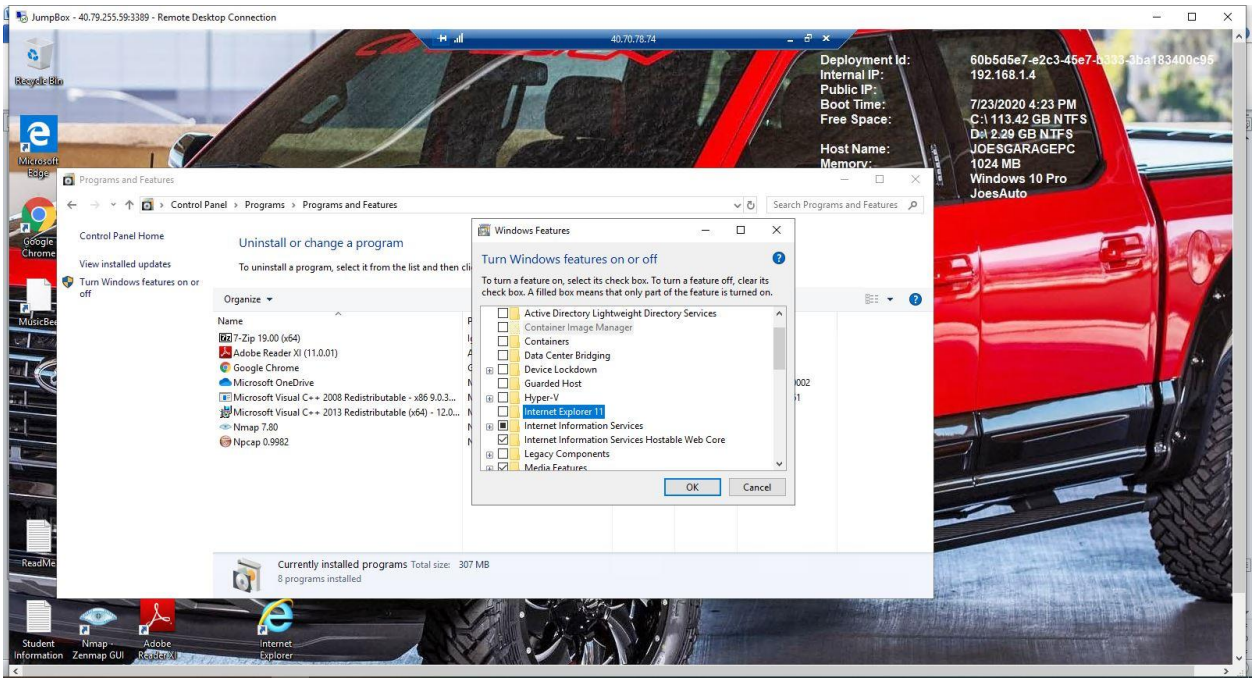


2. *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
    - According to security researcher John Page, Internet explorer has a severe security flaw that allows hacker to breach the system.
    - Hackers can also steal personal data from the host device through Internet Explorer.

    Information collected from:
    https://www.forbes.com/sites/jasonevangelho/2019/04/15/warning-internet-explorer-just-became-a-silent-but-serious-threat-to-every-windows-user/#299cadd386d8

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.

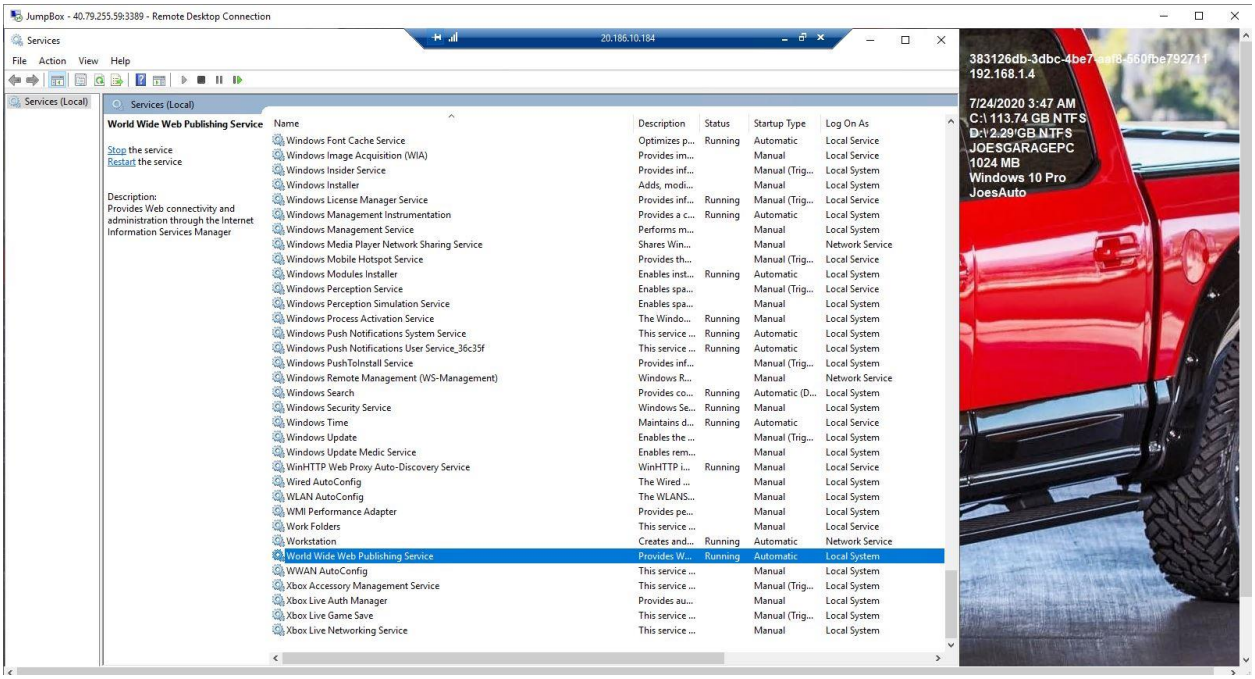
1. How did you determine these services were running? Include screenshots to show how you found them.

⇨ In order to find the web services, do the following:

i. On Windows Search bar (in Windows Taskbar) type "Services" and click the icon titling it.

ii. When the Services window pops up, search for "World Wide Web Publishing Service".

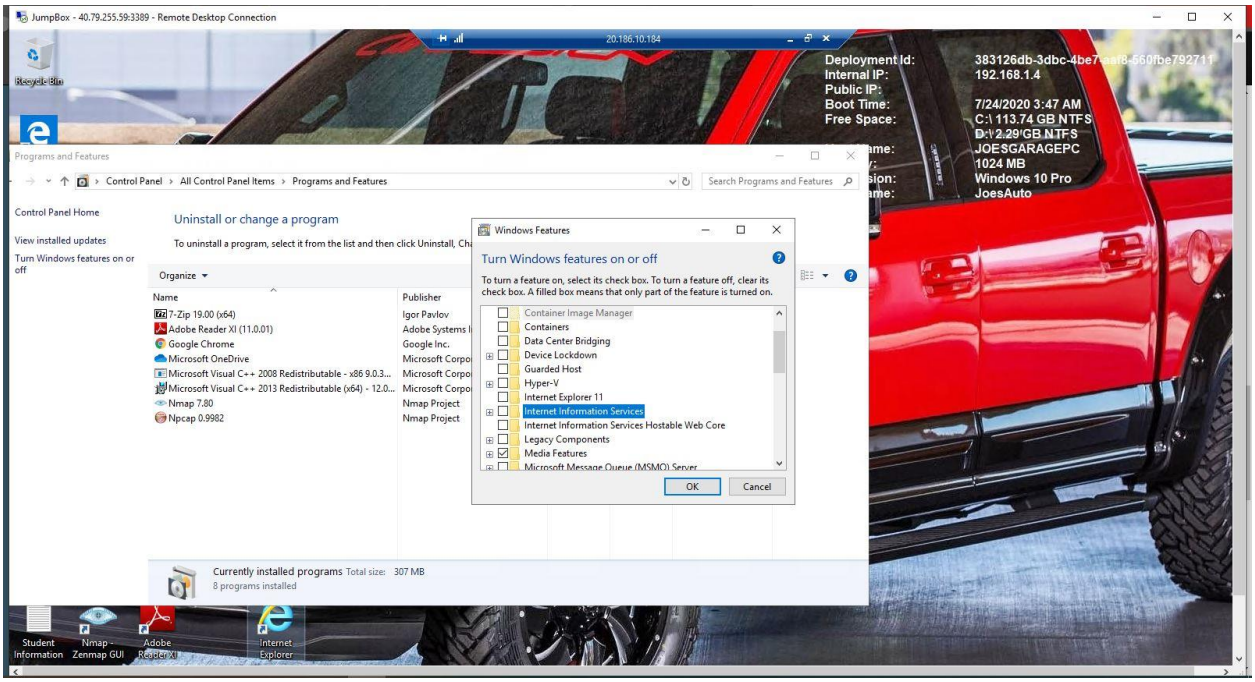
iii. Upon finding the "World Wide Web Publishing Service", you can see "Status" column saying that it is running and also "Status Type" column says that it is automatic, meaning it will start as soon as user logs on to the computer.



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

⇨ Another way to check if the web server are running or not is to do the following:

i. Go to “Control Panel”
ii. Click on “Programs and Features”
iii. Click on “Turn Windows features on or off”
iv. On the pop up window, scroll down until you find “Internet Information Services” (IIS).
v. Uncheck “Internet Information Services” and “Internet Information Services Hostable Web Core”.
vi. This is will prevent web server to be installed as well as will uninstall if it is already installed.

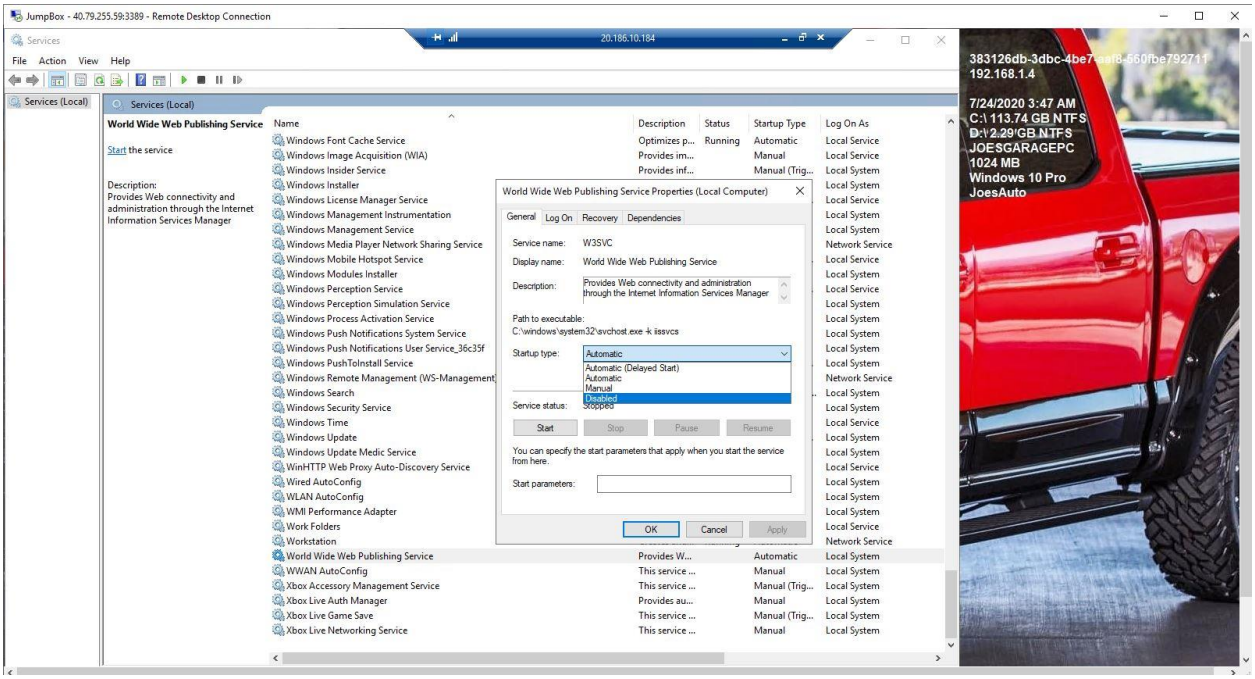


3. How do you disable them and make sure they are not restarted?

⇨ In order to stop and disable web-server do the following:

i. Double click on "World Wide Web Publishing Service"

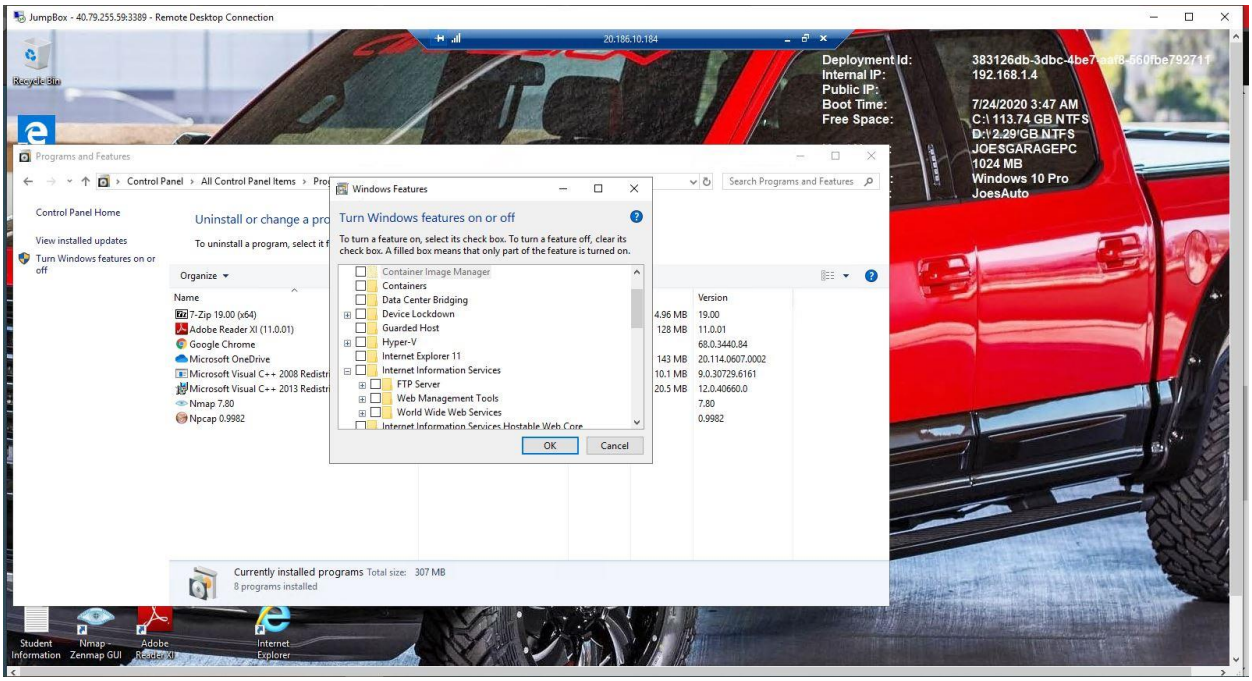
ii. If it is running, then click the "Stop" button, after that click on the status type dropdown menu. Select "Disable" from the dropdown menu.



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.

⇨ In order to stop FTP services do the following:

- ➢ Go to "Control Panel"
- ➢ Click on "Programs and Features"
- ➢ Click on "Turn Windows features on or off"
- ➢ On the pop up window, scroll down until you find "Internet Information Services" (IIS).
- ➢ There is a "+" sign on the left of the check box of "Internet Information Services", click on that.
- ➢ Upon clicking among several options there is a option called "FTP Server". In the previous instruction we unchecked the "Internet Information System", and for that all the internal options of Internet Information System should be unchecked. If not then uncheck "FTP Server". This will stop the FTP services.



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.

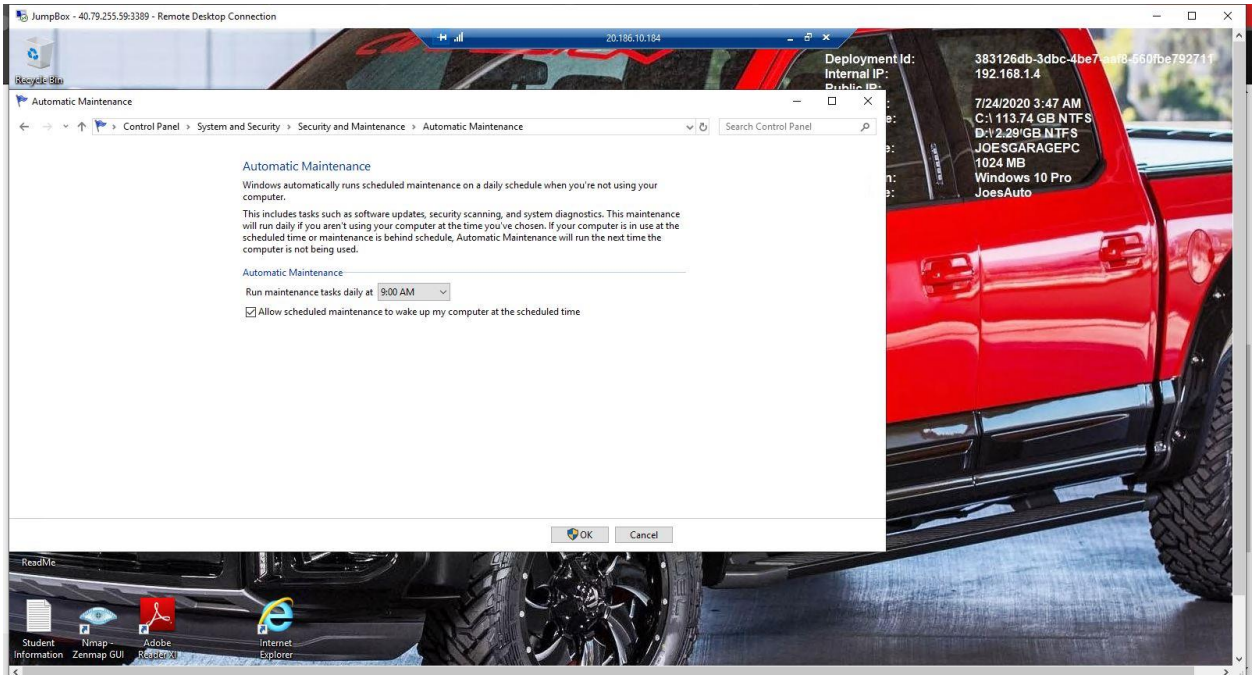
1. *Explain the process for doing this. Include screenshots as needed.*

⇨ In order to set "automatic updates" do the following:

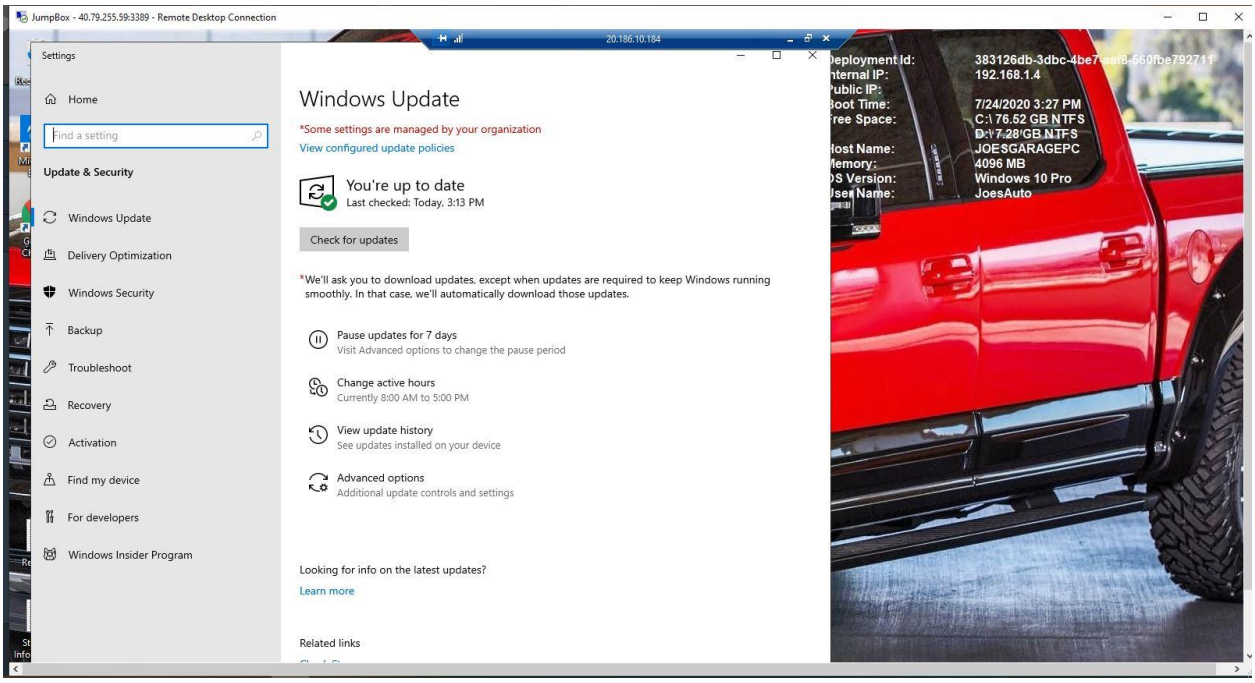
- ➢ Go to "Control Panel"
- ➢ Click on "System and Security"

- Click on “System and Maintenance”
- Open the “Maintenance” tab
- Click on the “Change Maintenance Setting”
- Set a maintenance time.
- Click on OK.

This will set an automatic update daily on that specific time.



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
- Npcap 0.9982

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

⇨ In order to get this information, first go to the "Control Panel" and under "Programs", click "Uninstall a Program". On the new window there will be all the apps installed in the computer with corresponding publisher, installed date, size, version displayed in a table.

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

⇨ In order to update an app, go to the apps publishers website to check whether there is a new update available or not. If an update is available then we can download the newest version of the app and install it. This installation will remove the previous update and will install the newest one.
For example, in order to update Google Chrome, there are two ways.

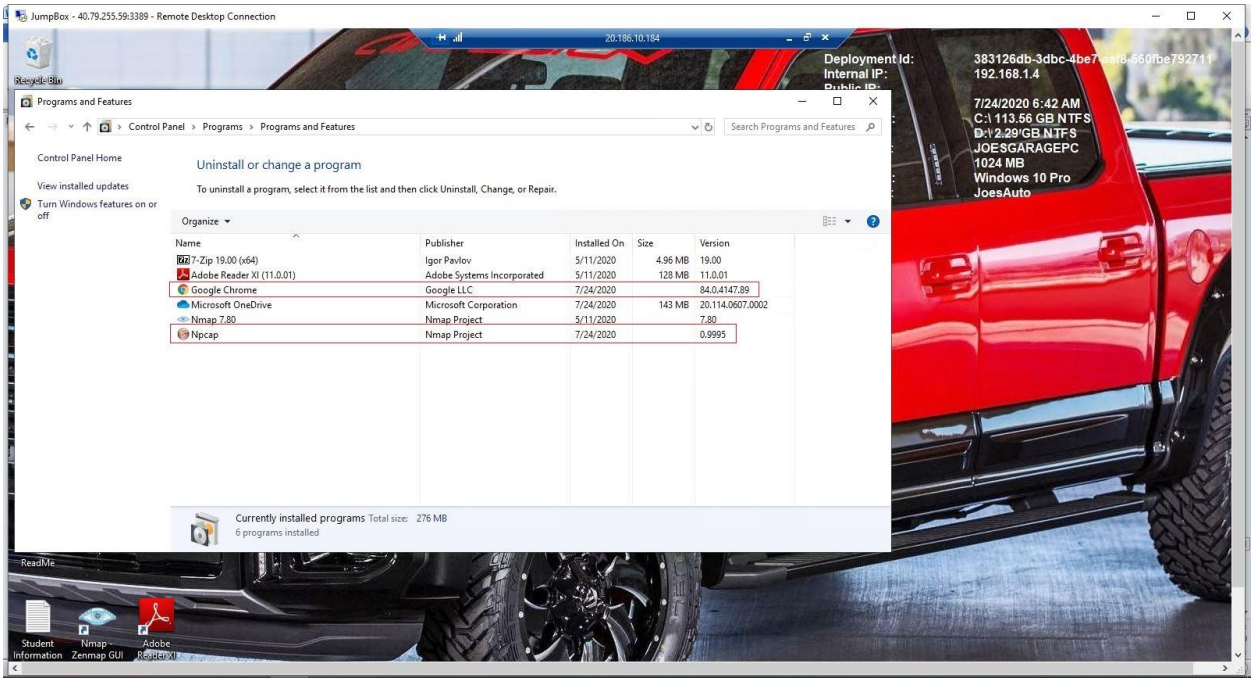
- Open Google Chrome and on the right corner click on the three dots of the address bar. Go to help and click "About Google Chrome". There we can see if it is the updated version or not. Google chrome can automatically update, so upon finding new update it will automatically update itself.
- On your browser search for "Google Chrome Download" and click on the first item titling that. From there download the latest version.

https://www.google.com/chrome/?brand=CHBD&gclid=Cj0KCQjwjer4BRCZARIsABK4QeUngOooCJvgrOTEYxJUf4wK2EjBQmlRvcFyROlZG8e2QQ_o031nwKgaAvPiEALw_wcB&gclsrc=aw.ds

In order to update Npcap, go to browser and search for npcap. In the page's navigation bar go to Download. In Download page, go to "Microsoft Windows Binaries" section and click on option that has a label called "Latest Npcap release self-installer". It will download the new version of the npcap.

https://nmap.org/download.html

As we can see in the screenshot, Google Chrome and Npcap are both updated.



5. Securing Files and Folders

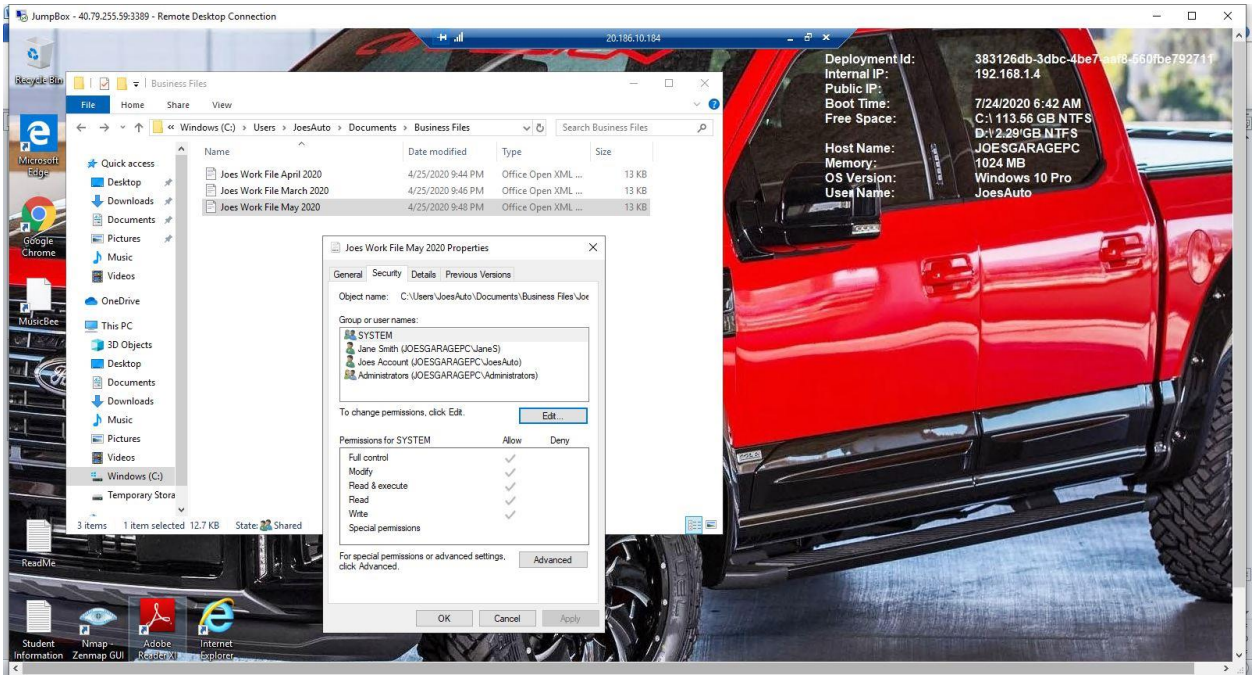
Joe has some work files in his Business folder that he wants to secure since they contain his customer information. They are labeled "JoesWork."

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.*

⇨ In order to ensure that only Joe and Jane has access to those work files, first go to the Business folder that contains these files. Right click on a file and click on “Properties”. On the Properties window, select “Security” and click on “Edit”. There we can add new user how can access the file as well as remove existing user.



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.*

⇨ In order to encrypt Joe’s work files, select all the files and right click on one of the Joe’s work files. On the option 7-zip click “add to Archive”. On the new popped up window, set the “Archive Format” to “zip” and on the password section put the above password. On the “options” section check “Delete after file compression”. Finally, set the “Encryption Method” to “AES-256” as it is the most latest and the most secure among the other existing encryption methods. Next, click ok. After the files are encrypted in a folder, the files that are unprotected will be deleted automatically.

3. *What security fundamental does this provide?*

⇨ The above scenario provides the following security fundamental:

- ⇨ Least Privileges
- ⇨ Data Protection

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

⇨ According to CIS Controls, this step matches the following:

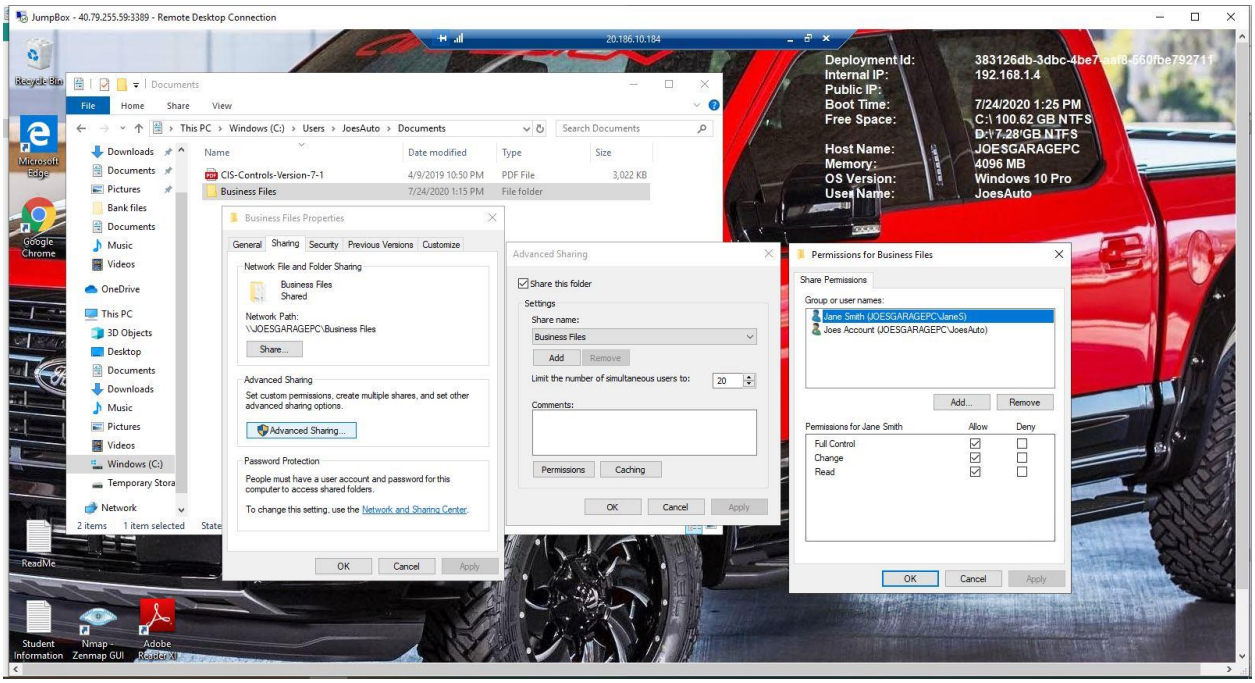
- ⇨ Basic Control: Continuous Vulnerability Management (Step 3), Controlled Use of Administrative Privileges (Step 4)
- ⇨ Foundational Control: Controlled Access Based on the Need to Know (Step 14), Data Protection (Step 13)

Shared Folders

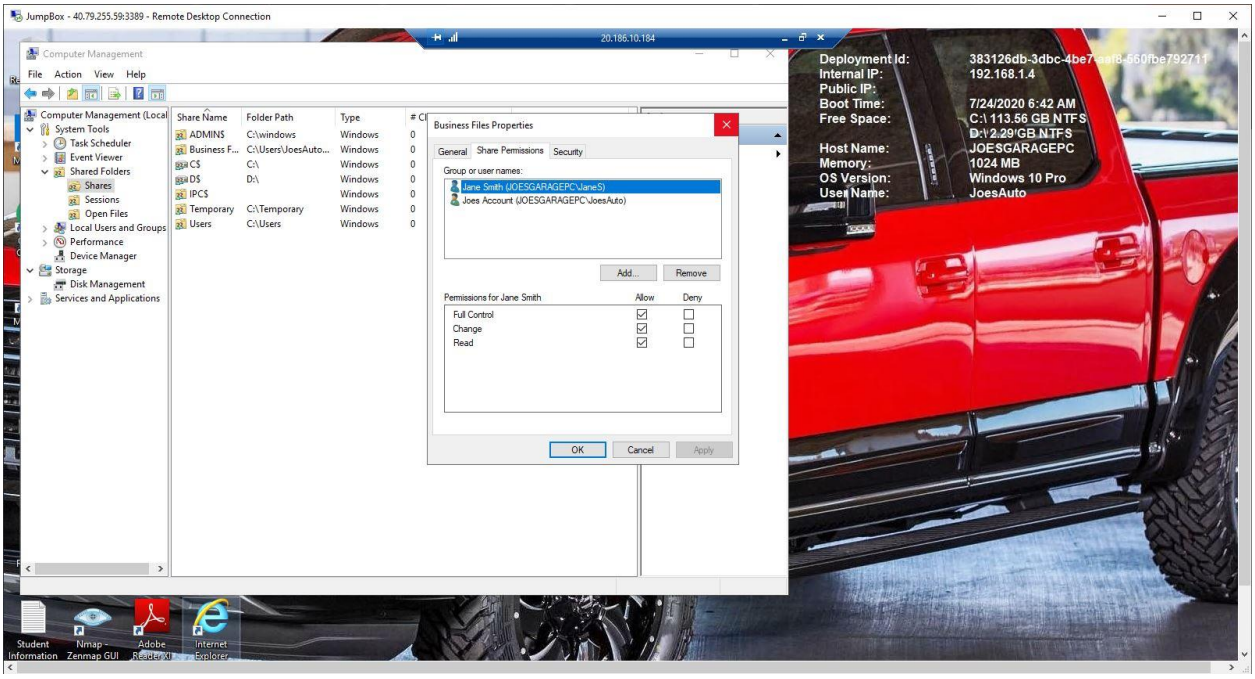
Shared folders are a common way to make files available to multiple users. There's a folder under Joe's documents called "Business Files" that Joe wants shared with his administrator Jane.

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.*

⇨ At first go user "JoesAuto" and go to its Document folder. Right click on the Business Folder and select properties. On the properties window, select "Sharing" tab. Click on "Advanced Sharing" button. On the Window, check "Share this folder". Then click on the "Permission". On the new window, click on the "Add" button to add specific user who can access this folder. Also check the "Full Control" option on the Permission box. Then will allow the folder to display on "Computer Management".

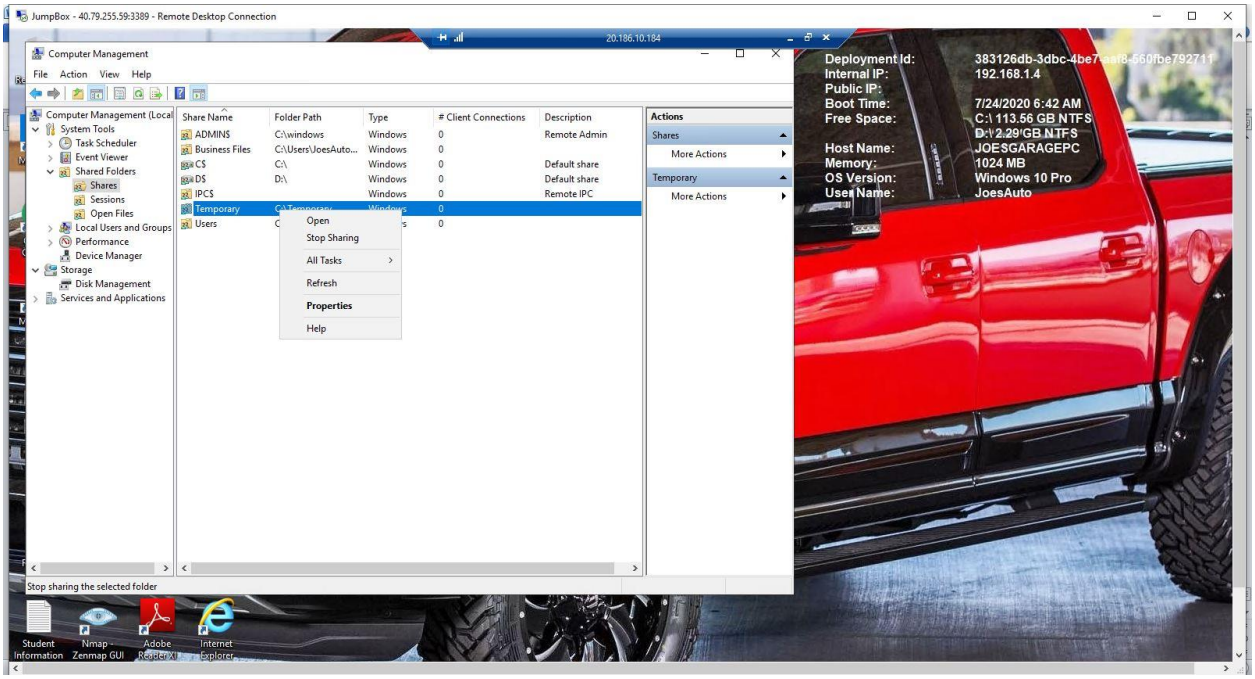


Next, Right Click on the windows icon and click on "Computer Management". On the left menu, click on "Shared Folders". Double click on "Shares" under the "Shared Folder". On the table, we can see that the "Business Folder" is available. Right click on it and click properties. On the properties window, click on Share Permissions tab. Here we can add new user and give that user appropriate privileges or we can remove user and also take away certain privileges.



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.*

⇨ In order to make sure there are no other shared folder, go to Computer Management's Share option and see the table to check if there is any other Folder shared or not. As we can see in the table that there is only Business folder that is shared with Jane Smith and Joe (Owner). There is another folder called Temporary. If we want to stop it then right click on it and click Stop Sharing.



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]

- In the Hackers Documents folder, there is a folder called "Bank Files" containing two text files. One is Bank Accounts and other is Pete Letter. The Bank account file contains Bank Transaction credential as well as users saving and checking information. Hacker can use that information to steal money from user. The Pete Letter confirms that these account credentials have been stolen by hacker.
- Stealing Bank Account information can also lead to employee suing law suit against Joe as he didn't take any precaution to prevent Cyber-attacks.
- In the Hackers Documents folder, there is an invoice and a letter. The invoice is to fake Joe into paying a customer, as Joe never pays attention to these things. So Pete Letter confirms that Pete will send this to Joe when Jane is on vacation. Thus, will steal money from Joe.

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.