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: Mohamed AbdelGawad Ibrahim

Date of completion: 28/10/2022

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

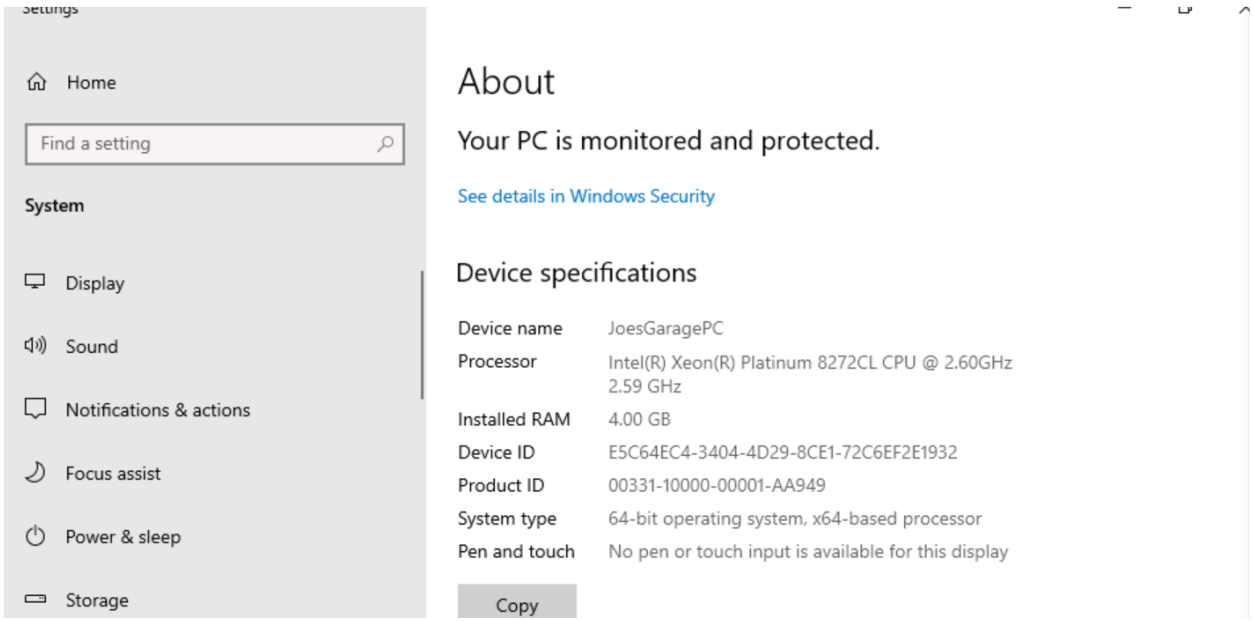
1. ***Fill in the following table with system information for Joe's PC.***

Device Name	JoesGaragePC
Processor	Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz 2.59 GHz
Install RAM	4.00 GB
System Type	64-bit operating system, x64-based processor
Windows Edition	Windows 10 Pro
Version	20H2
Installed on	11/23/2021
OS build	19042.1387

2. ***Explain how you found this information:***

   - Two ways:
     - Search on 'This PC' and click a right click on it, then choose 'properties'
     - OR search for 'About your PC'

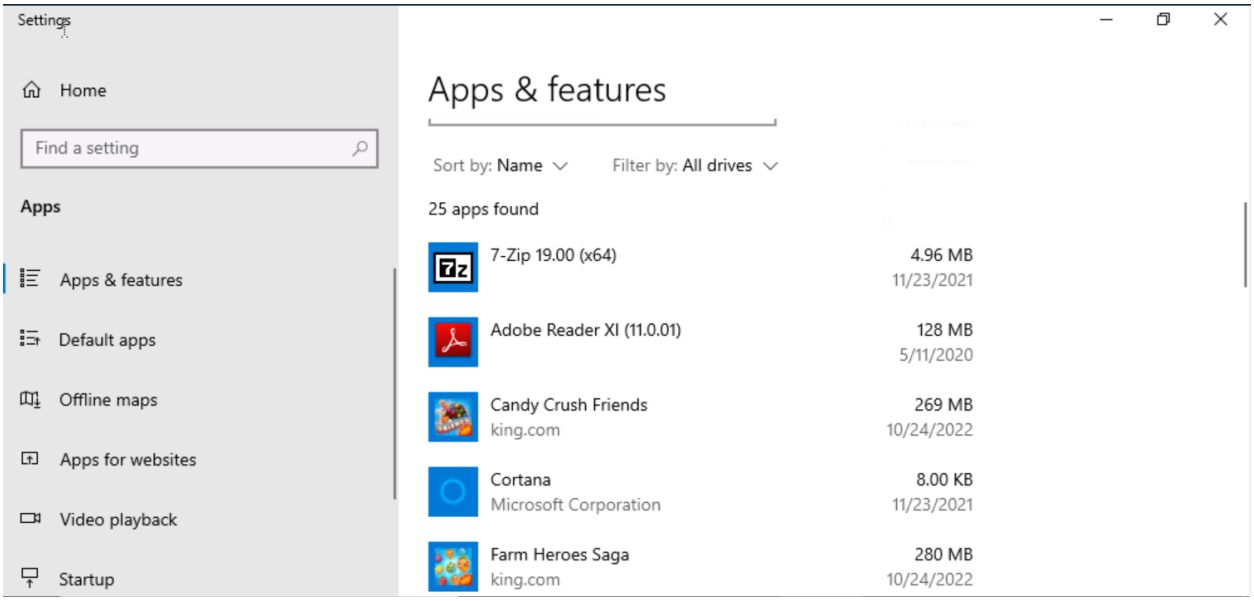
3. ***Provide a screenshot showing this information about Joe's PC:***



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 19.00 (x64)
   - Adobe Reader Xl (11.0.01)
   - Candy Crush Friends
   - Farm Heroes Saga
   - Google Chrome
2. ***Explain how you found this information. Provide screenshots showing this information.***
   - By searching on 'programs' then choose 'Apps & features'



3. ***The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?***
   - *Step2: Inventory and Control of Software Assets.*

Accounts

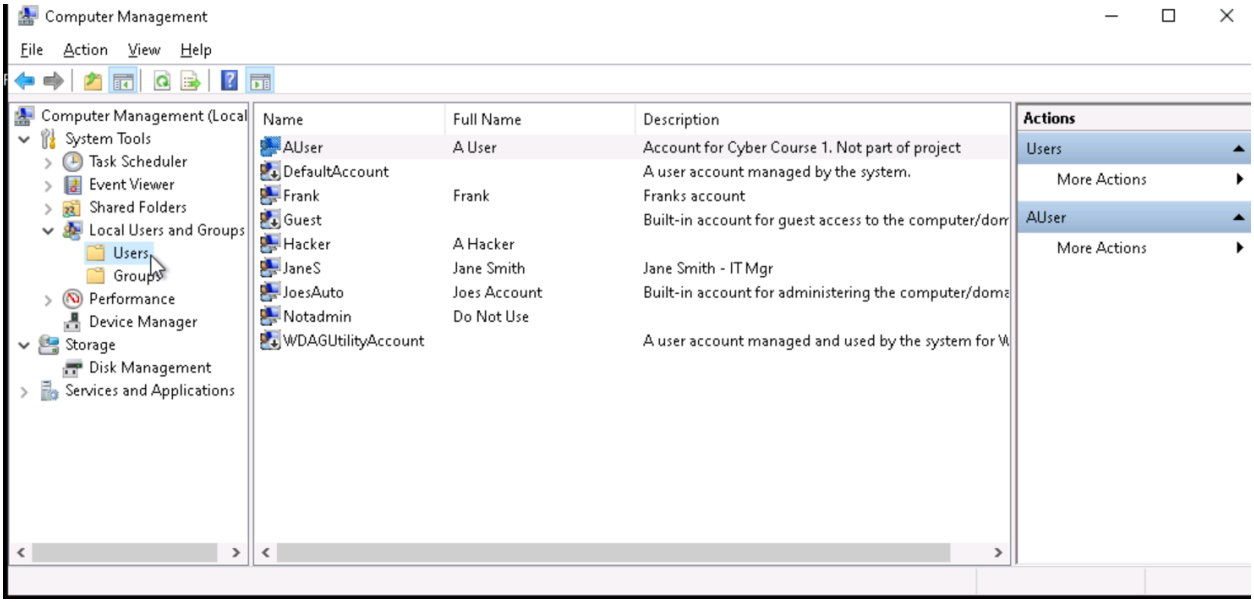
As part of your security assessment, you should know the user accounts that may access the PC.

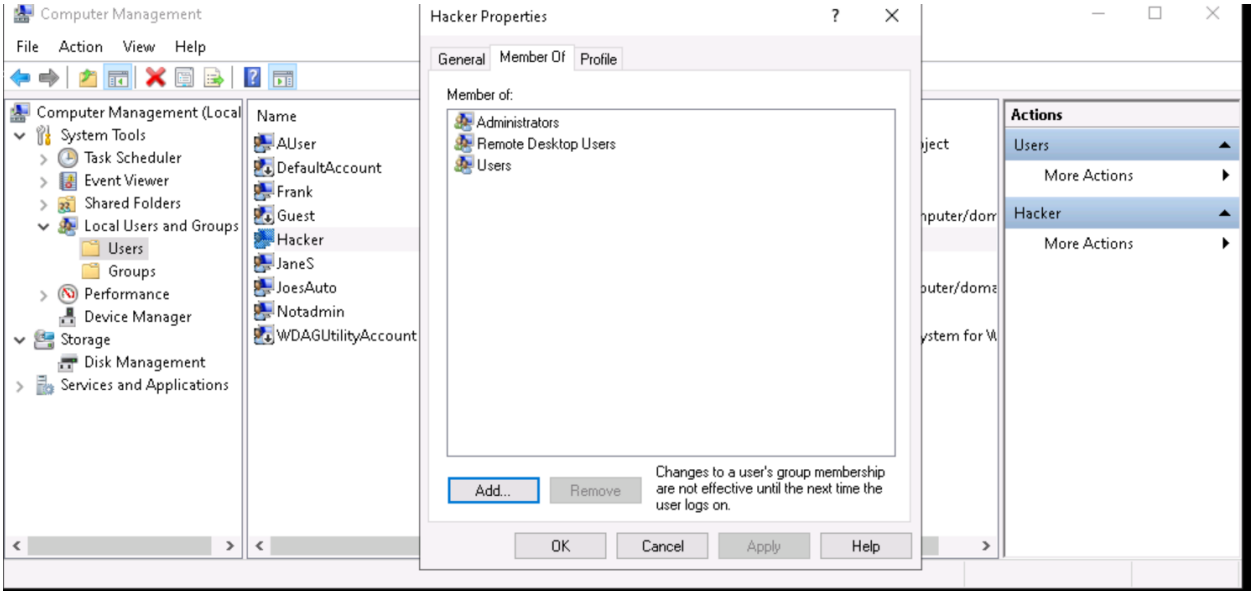
1. ***List the names of the accounts found on Joe's PC and their access level.***

Account Name	**Full Name**	**Access Level**
AUser	A User	Users Group
DefaultAccount	None	System Managed Accounts Group
Frank	Frank	- Users Group - Remote Desktop Users Group
Guest	None	Guests Group
Hacker	A Hacker	- Administrators Group - Remote Desktop Users Group - Users Group
JaneS	Jane Smith	- Administrators Group - Remote Desktop Users Group - Users Group
JoesAuto	Joes Account	- Administrators Group
Notadmin	Do Not Use	- Remote Desktop Users Group - Users Group
WDAGUtilityAccount	None	None

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

   - *By searching on 'Computer Management' then from the sidebar choose 'Local Users and Groups'. Then, Choose Users.*
   - *For viewing the groups of each account, right click on the account name then choose 'Properties'. Click on 'Member Of' tab to show the groups that the user account belongs.*



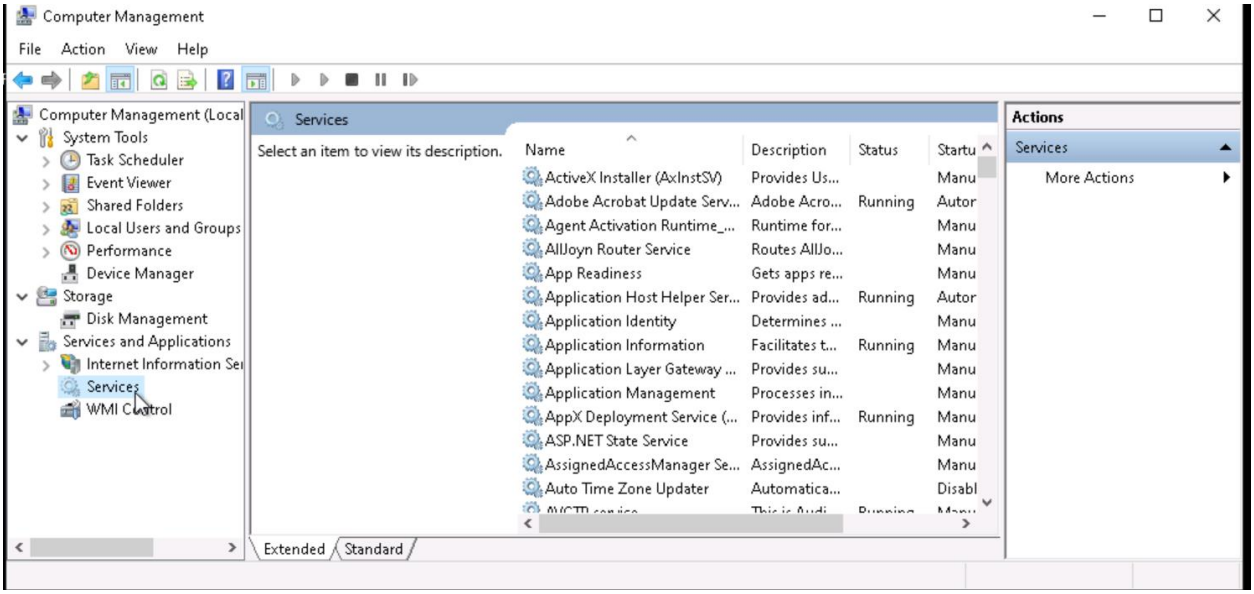


Services

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.***

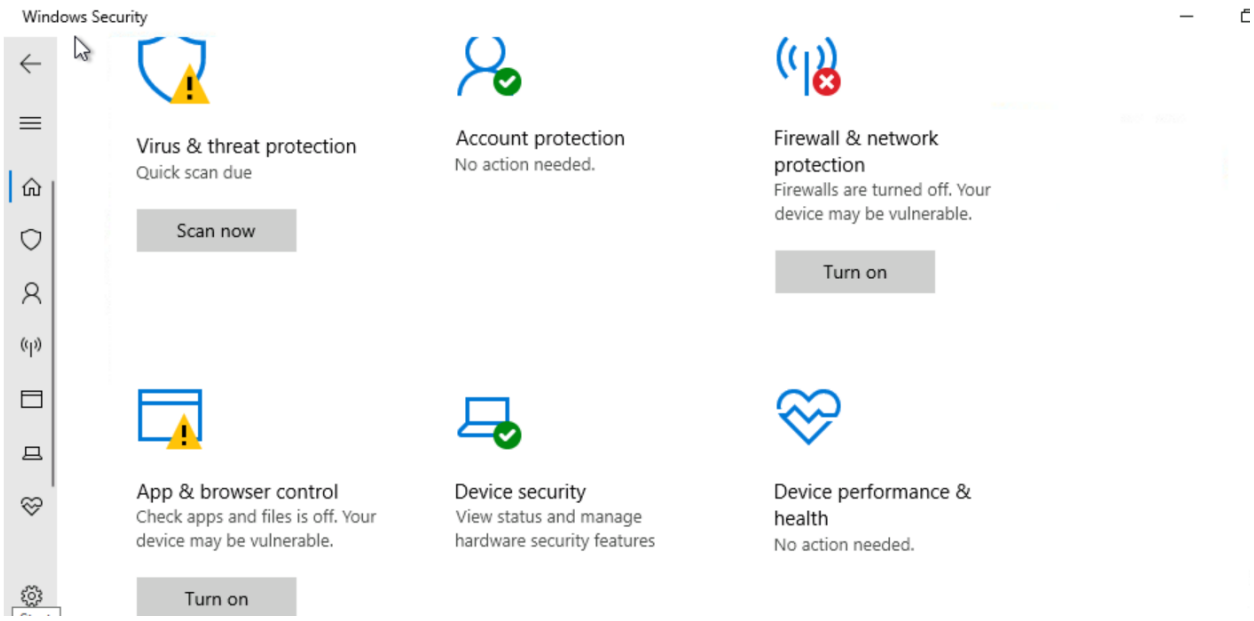
    - From 'Computer Management', click on 'Services and Applications' on the sidebar. Then click on 'Services'.

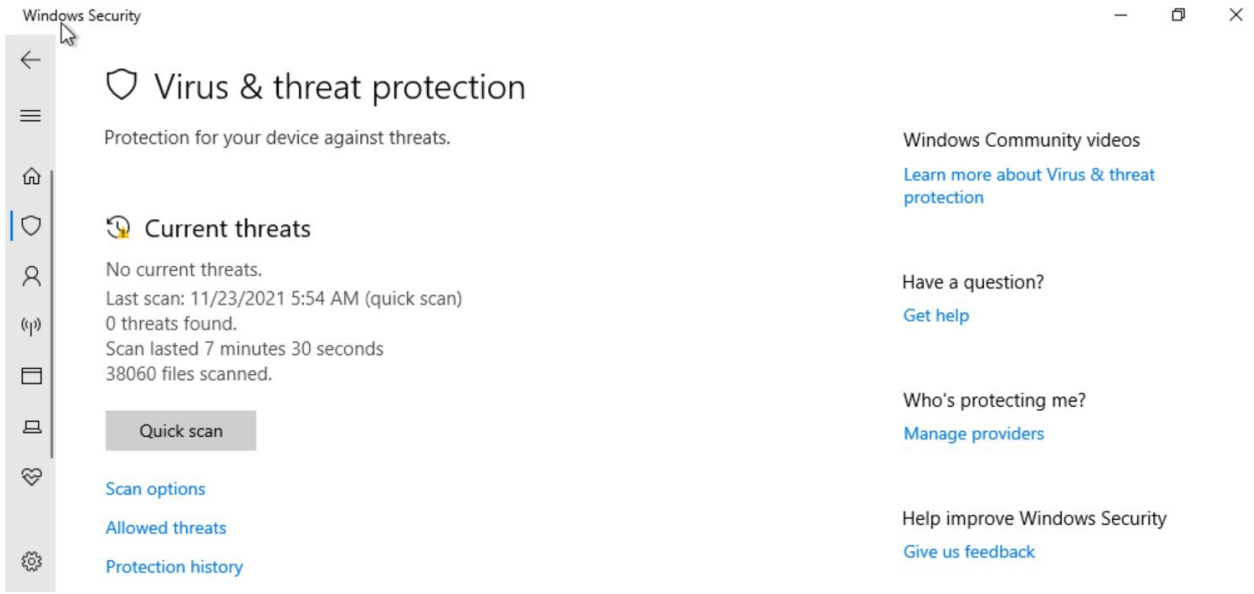


Security Services

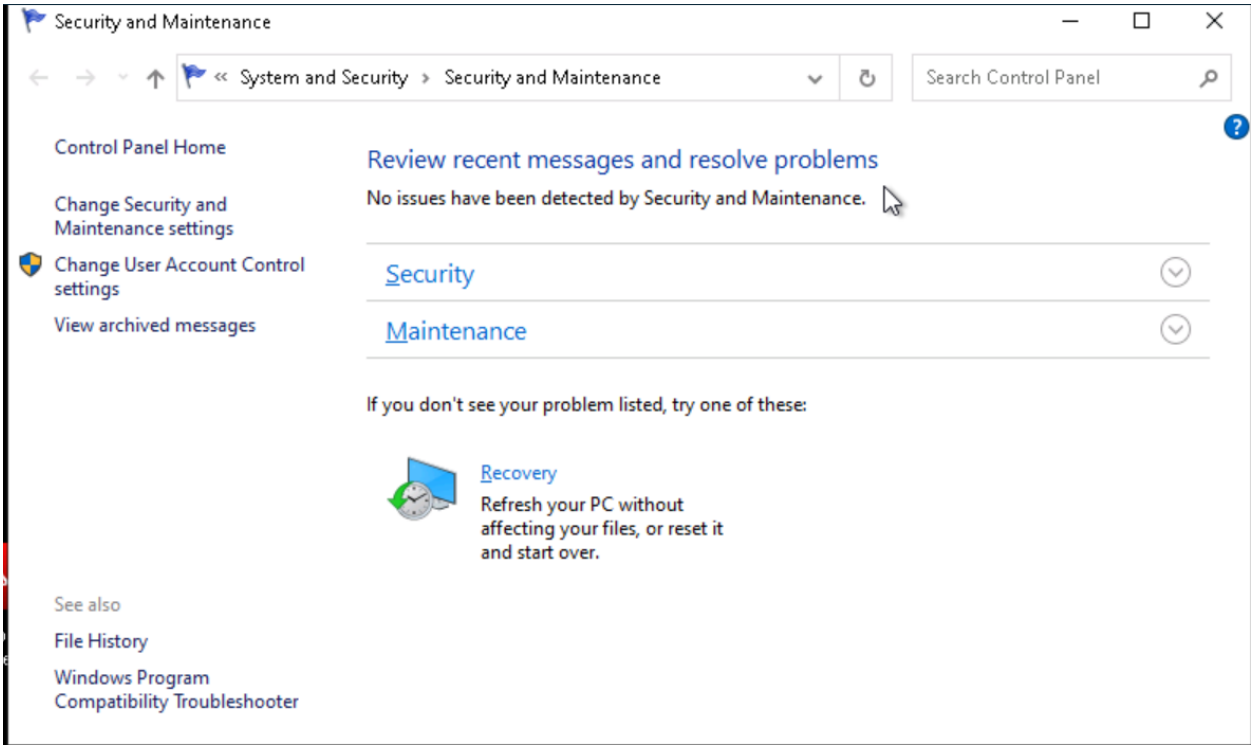
Joe wants to ensure that standard security services are running on his PC. He's content with using default Windows security settings and applications except for the rules outlined later. **Reminder that at this point you are just reporting what you observe. Do not make any changes to security settings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

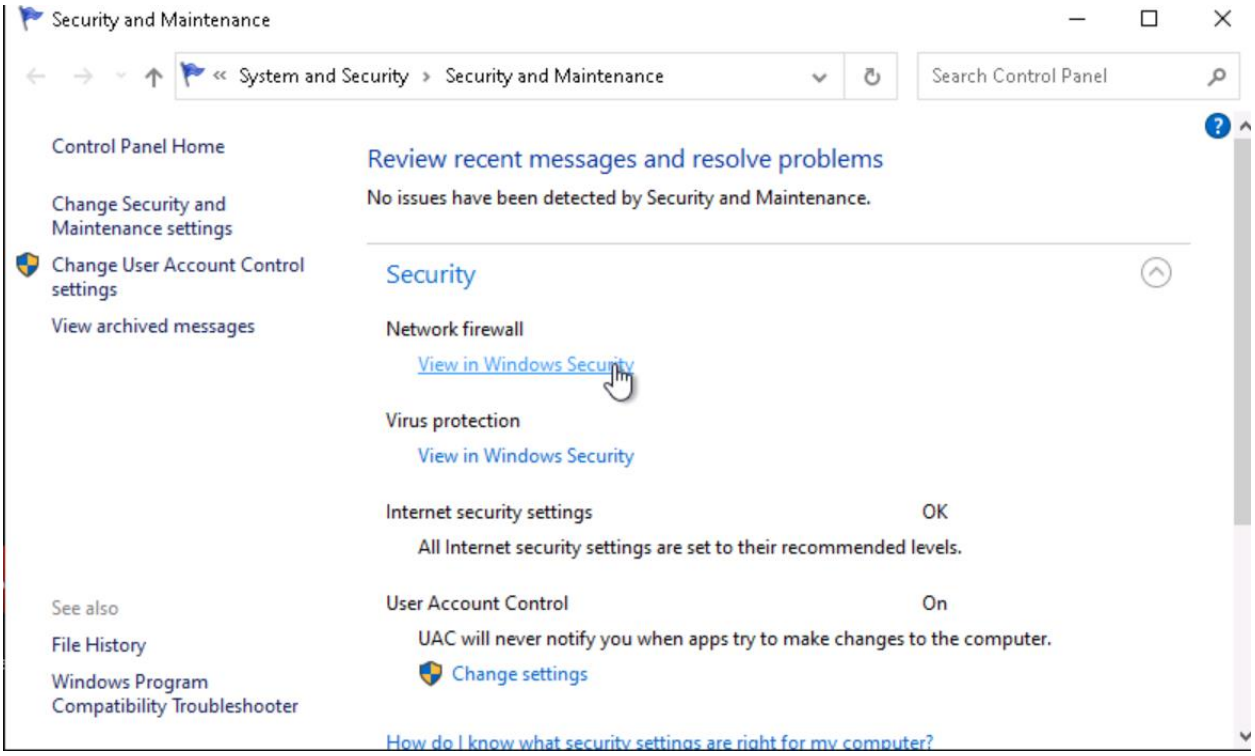


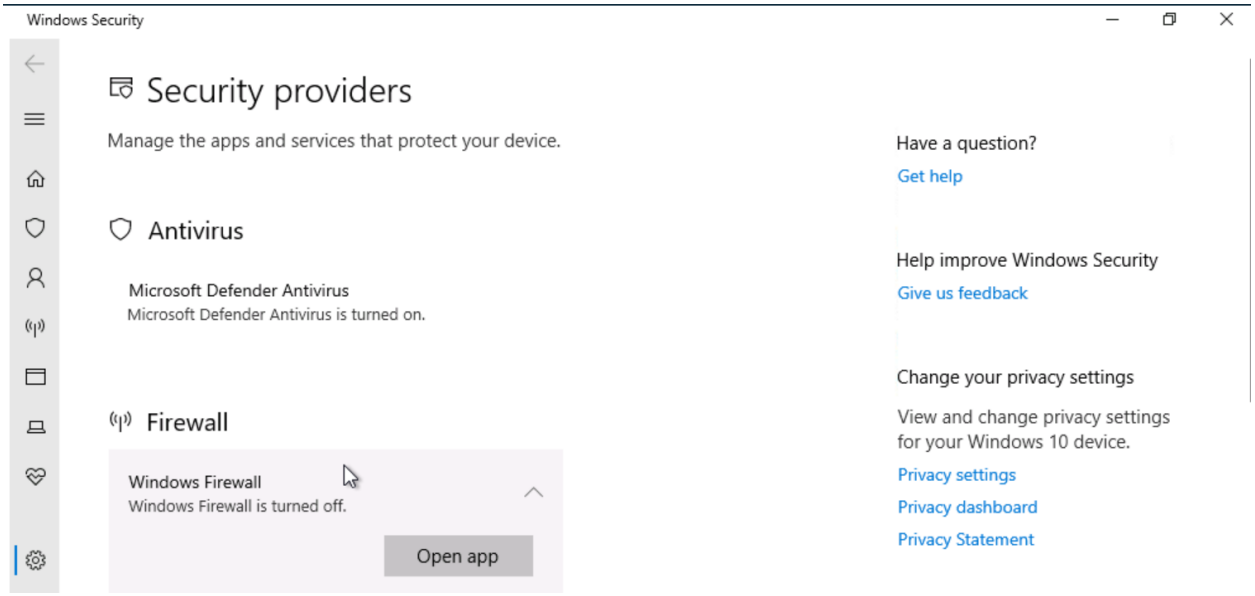


2. *The Windows 10 Security settings are also found from the* ***Control Panel > System and Security > Security and Maintenance****. Start by viewing* ***"Review your computer's status and resolve issues." Provide a screenshot of this below:***

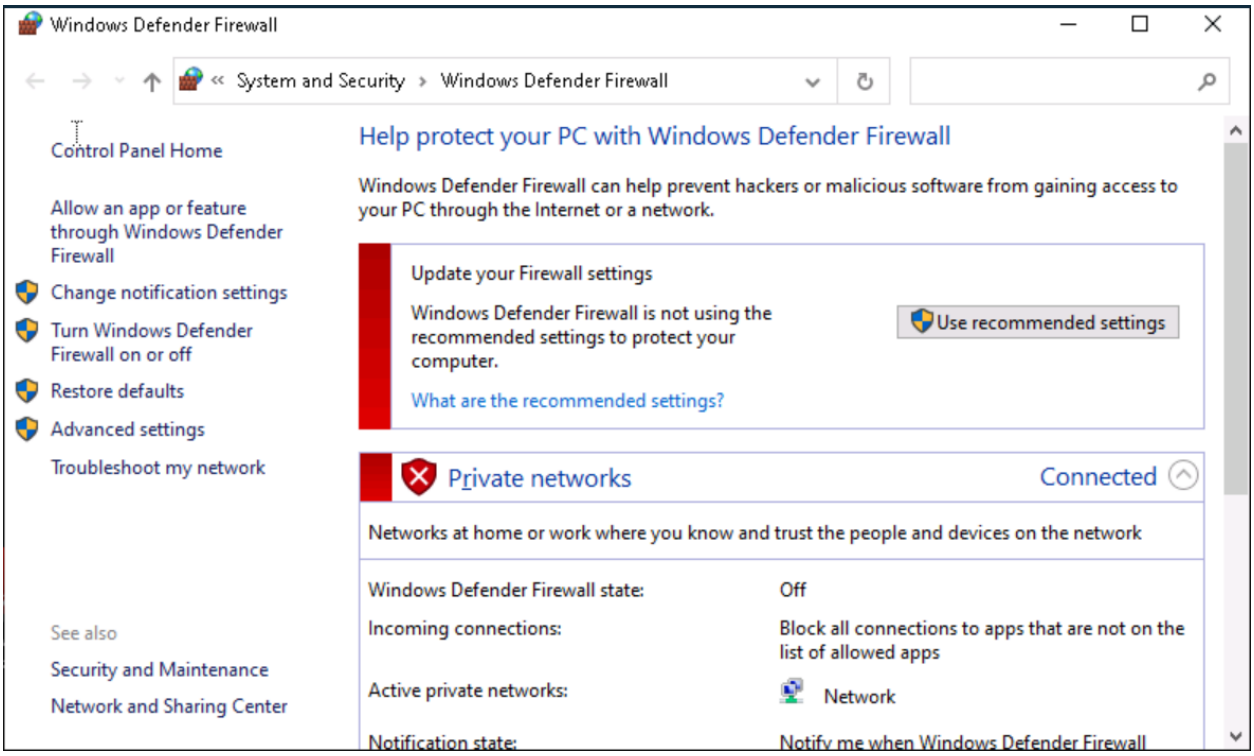


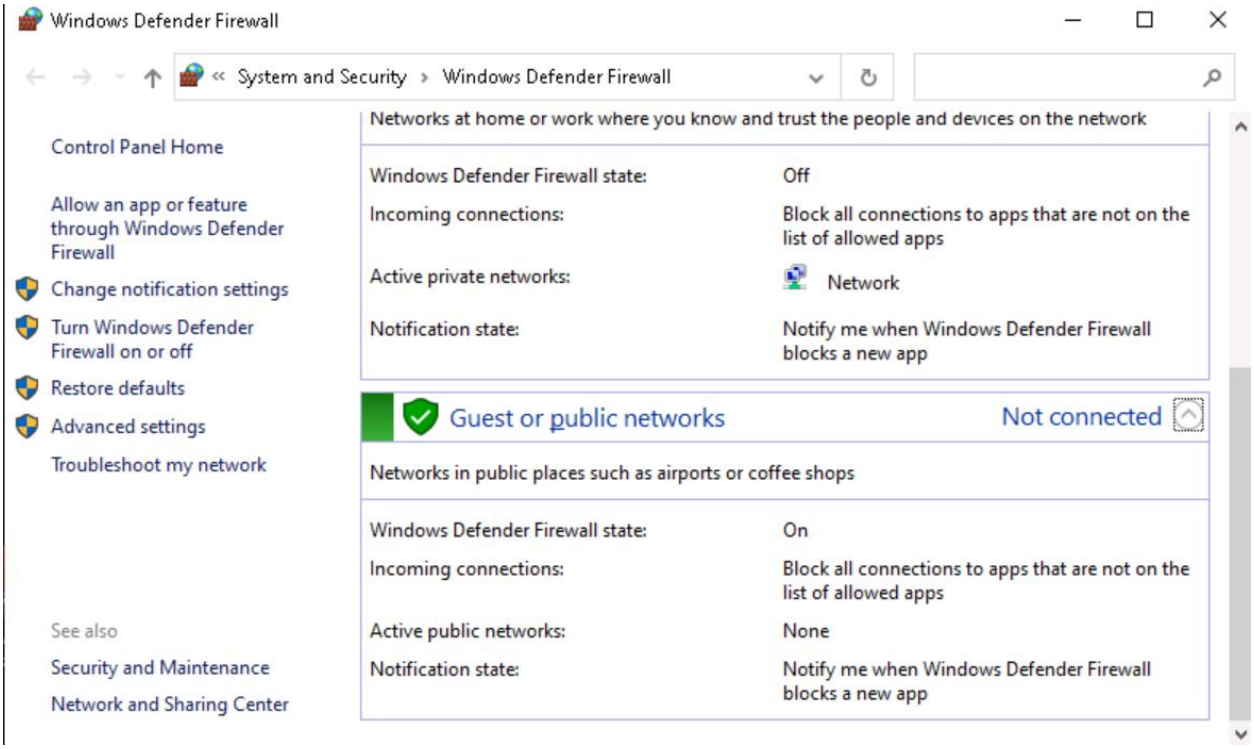
3. *Click on View in Windows Security to see the status there.* ***Provide a screenshot of the Firewall settings.***



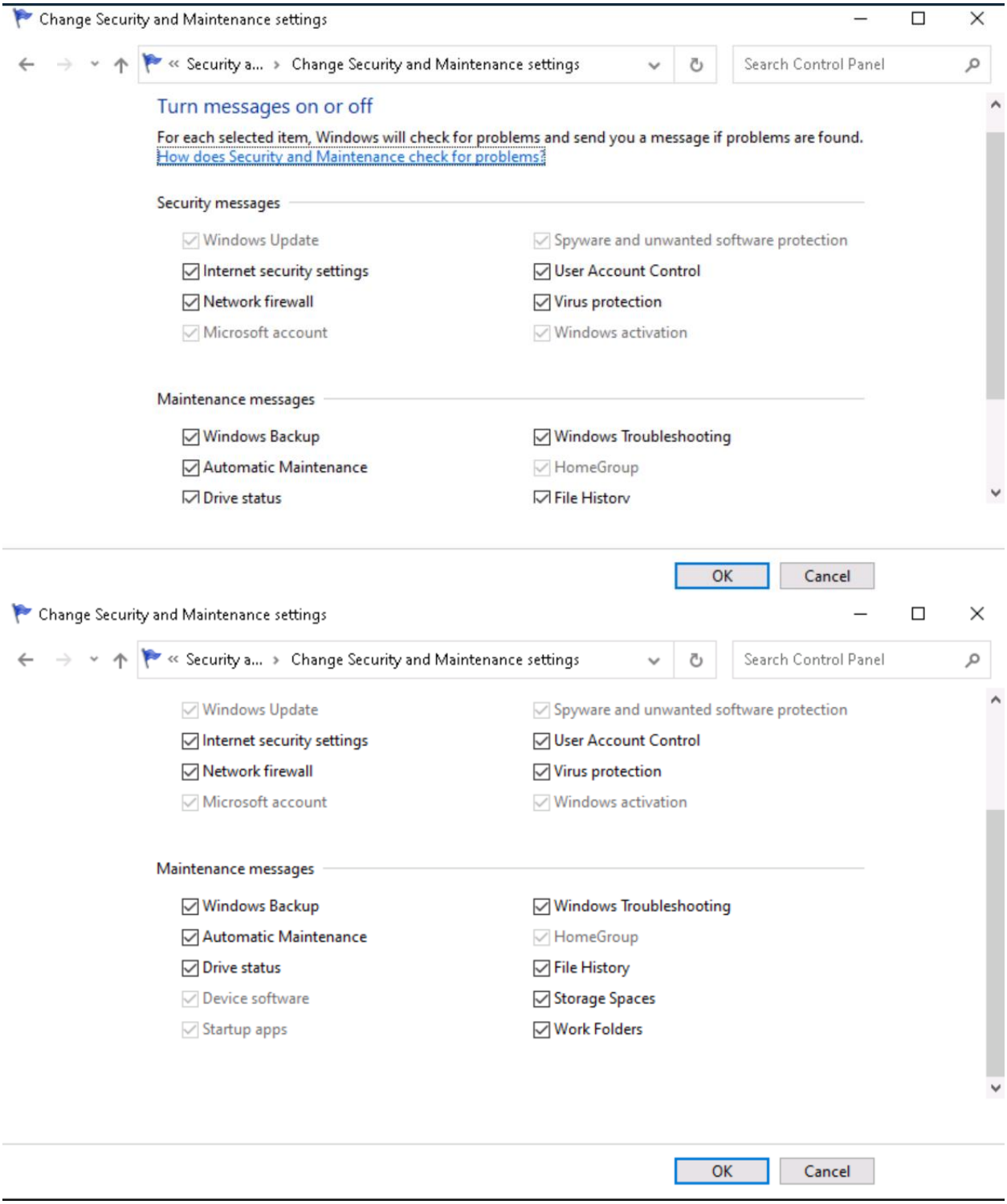


4. *From the **Control Panel**, go to **System and Security**. In that window, select **Windows Defender Firewall**. **Provide a screenshot of it here**:*



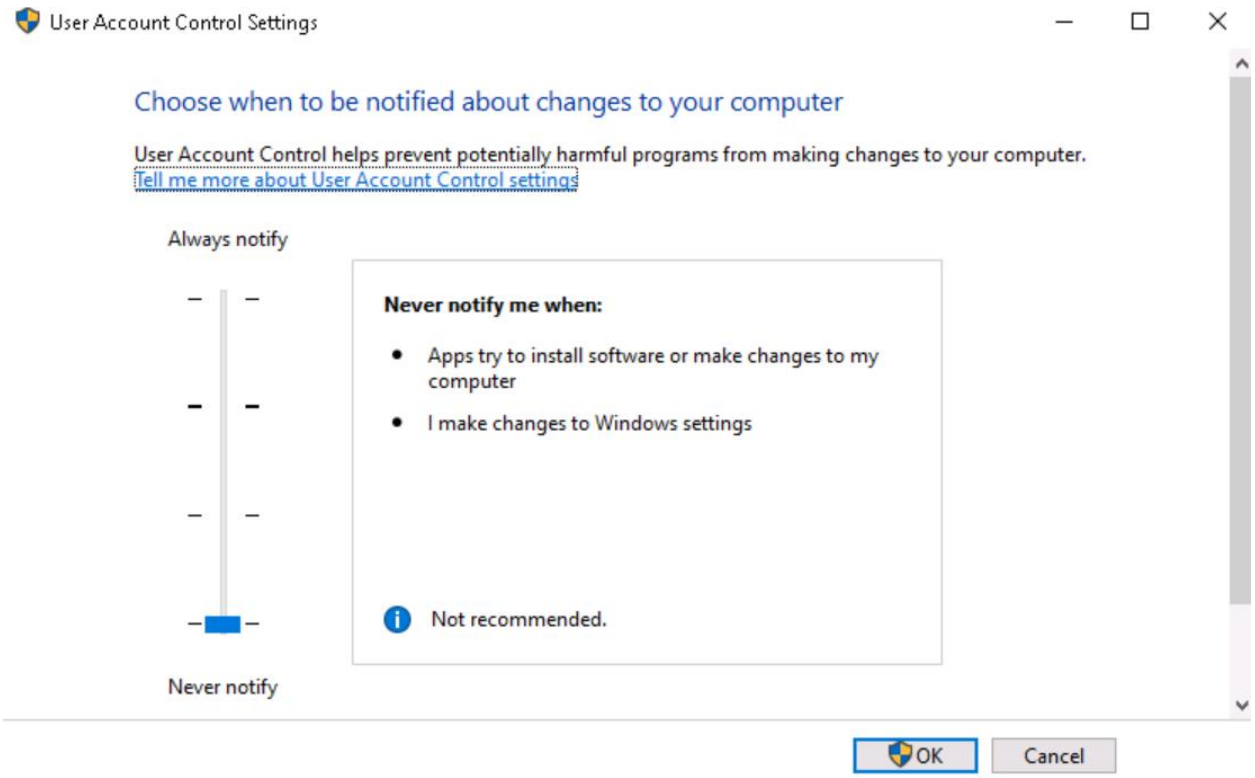


5. *PC users should be notified whenever there is a security or maintenance message**. In the Security & Maintenance window, click on Change Security and Maintenance settings and take a screenshot. Paste it here:***

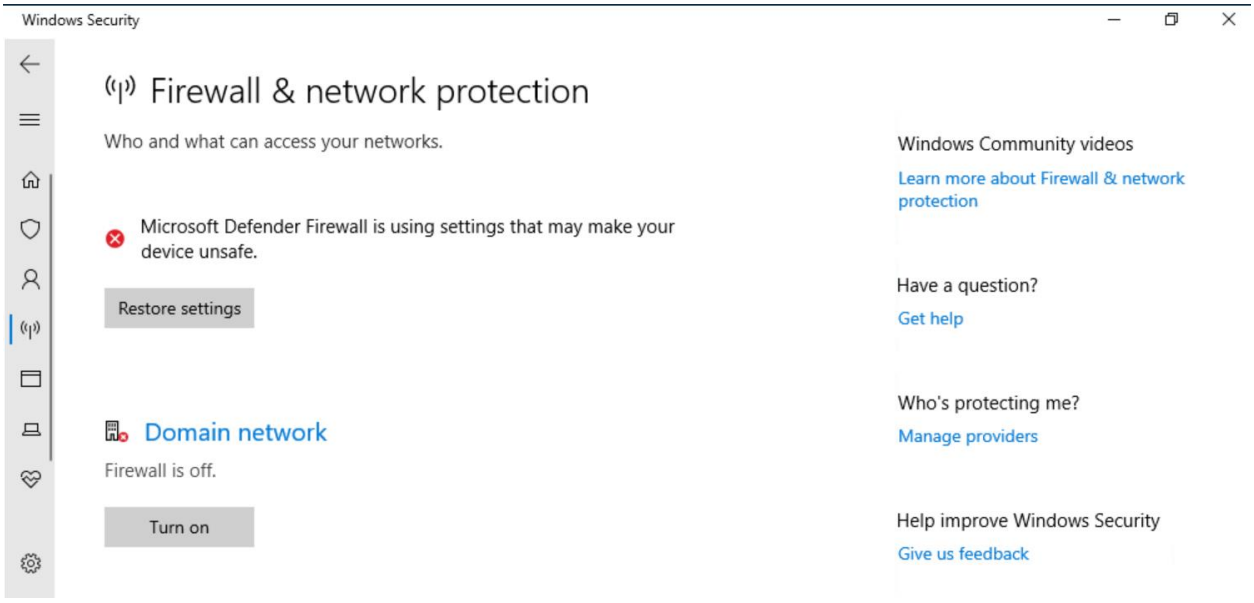


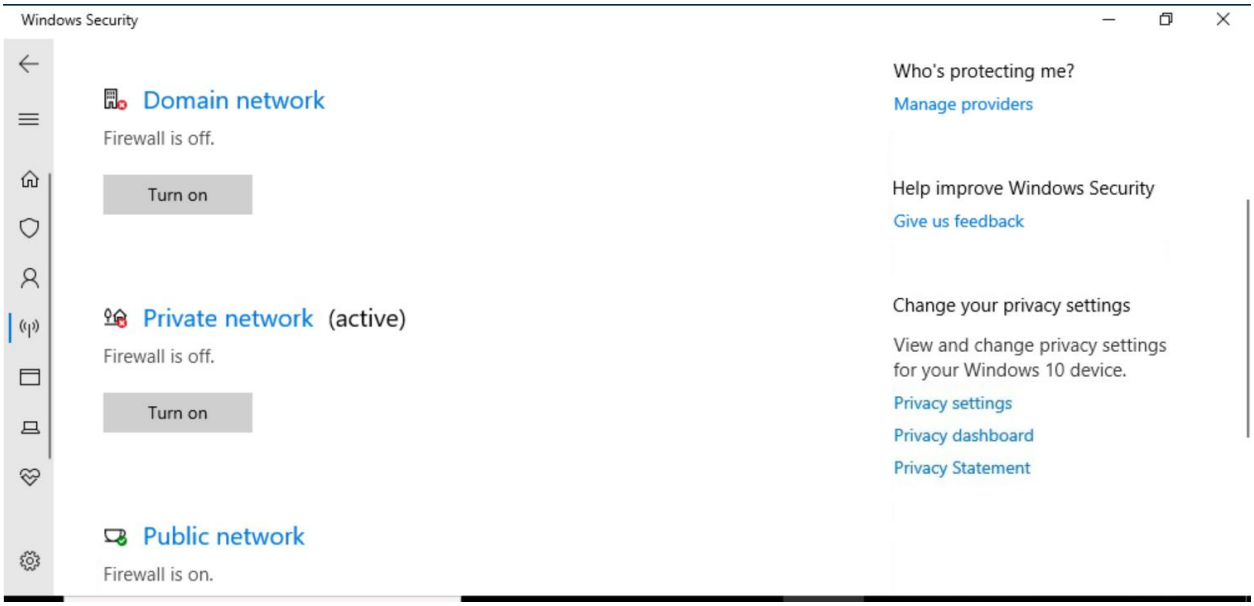
6. ***Document the status of the PC's security settings listed below. Include the process you used to determine this information along with any screenshots. At this point, you are only documenting what you find. Do not make changes (yet).***

   - *For finding the User Account Control Setting, search for 'User Account Control Settings':*

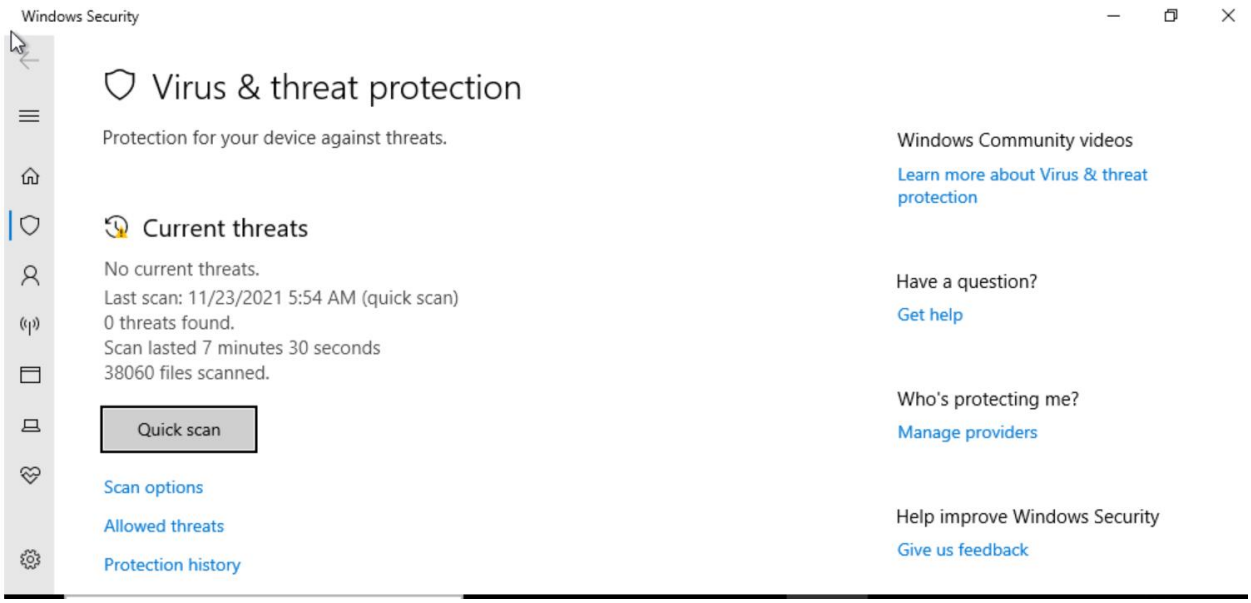


- *For finding the Internet Security message, search for 'Windows Security' then click on 'Firewall & network protection'*





- *For finding the Virus Protection message, search for 'Virus & threat protection'*



Security Feature	Status
Firewall product and status – Private network	Off
Firewall product and status – Public network	On
Virus protection product and status	On – Quick Scan Due
Internet Security messages	Internet Security Settings OK
Network firewall messages	Windows Defender Firewall is not using the recommended settings to protect the computer
Virus protection messages	No current threats – Quick scan due
User Account Control Setting	Status is 'Never notify'

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.]
   - Applications that aren't needed for the business as they may contain malware and they are a distraction for the business.
   - Many users have administration privileges. The risk is that unauthorized software could be installed.
   - Windows Defender Firewall is not using the recommended settings to protect the computer. This may allow unwanted access to the computer.

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?***
    - Choosing the NIST standard will allow us to go through the categories of each function in turn so that the company can move from its current profile to a much more secure profile. By using the NIST Framework we can implement the CIS Benchmarks to ensure the systems are hardened as well as possible.

2. ***What industry baseline do you recommend to Joe?***
   [Hint: Look in the documents folder]
    - *CIS-Controls-Version-7-1*

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.

Assume Joe uses the CIS as his baseline, what controls or steps does this meet?

- *Step 8: Malware Defenses.*
- *Step 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches.*

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:

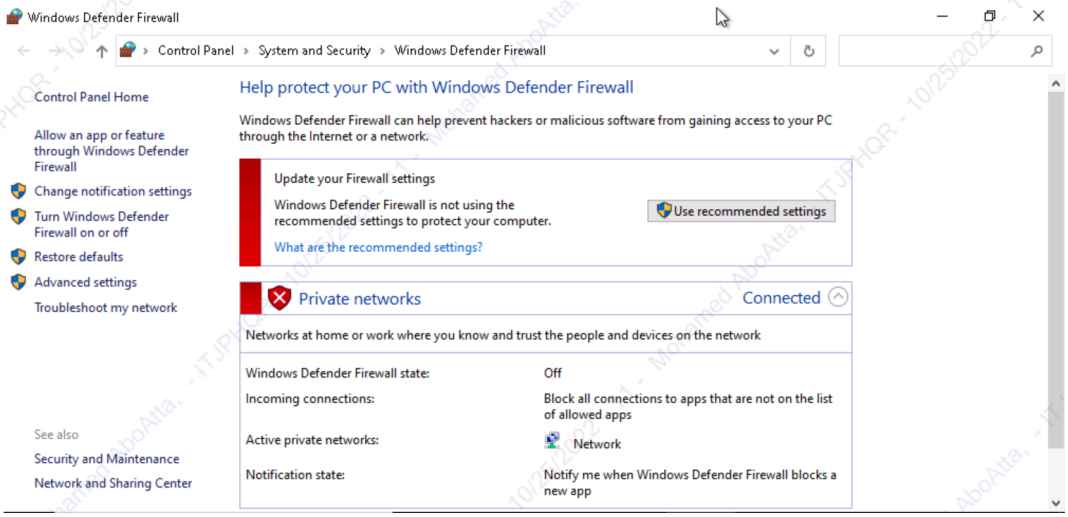
- Firewall
- Virus & Threat Protection
- App & Browser Control
- User Account Control settings
- Securing Removable Media

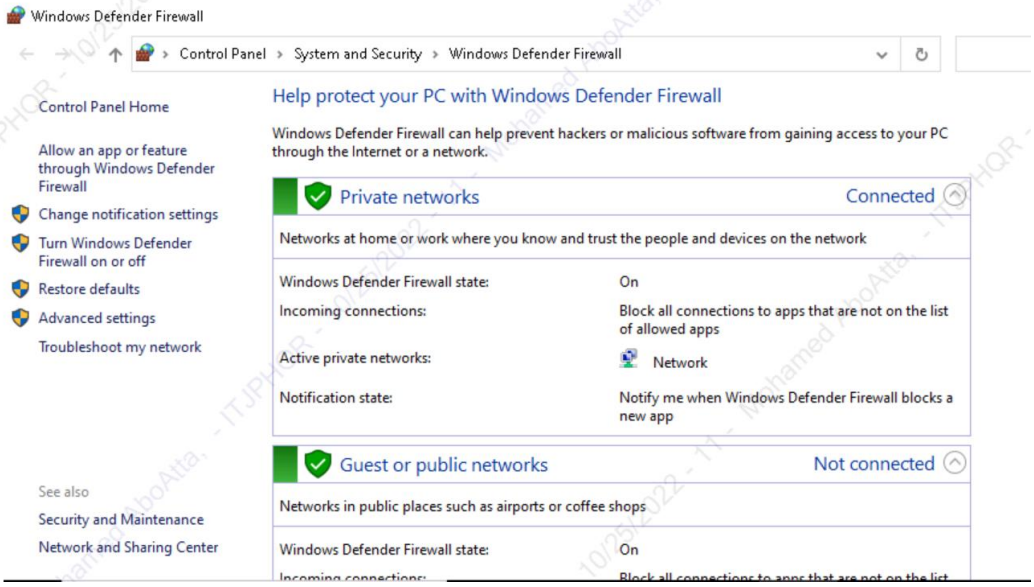
Firewall

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

1. ***Explain the process you take to do this.***
   - *Search for 'firewall' then open 'Windows Defender Firewall'.*
   - *Click on 'Use recommended settings'*

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





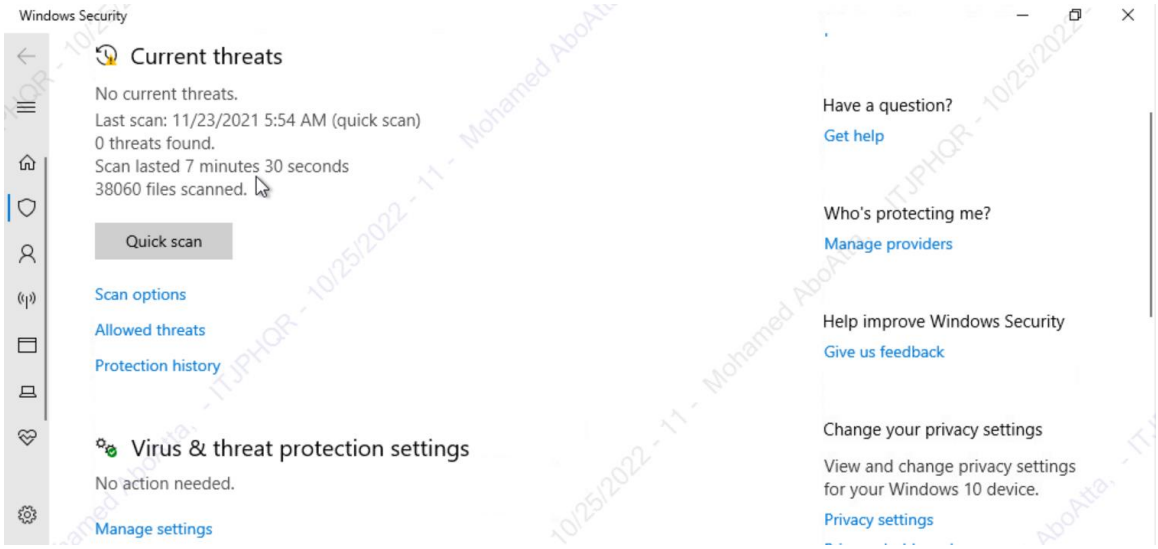
3. ***What protection does this provide?***
   - *The firewall can help prevent hackers or malicious software from gaining access to the PC through the Internet of a network.*

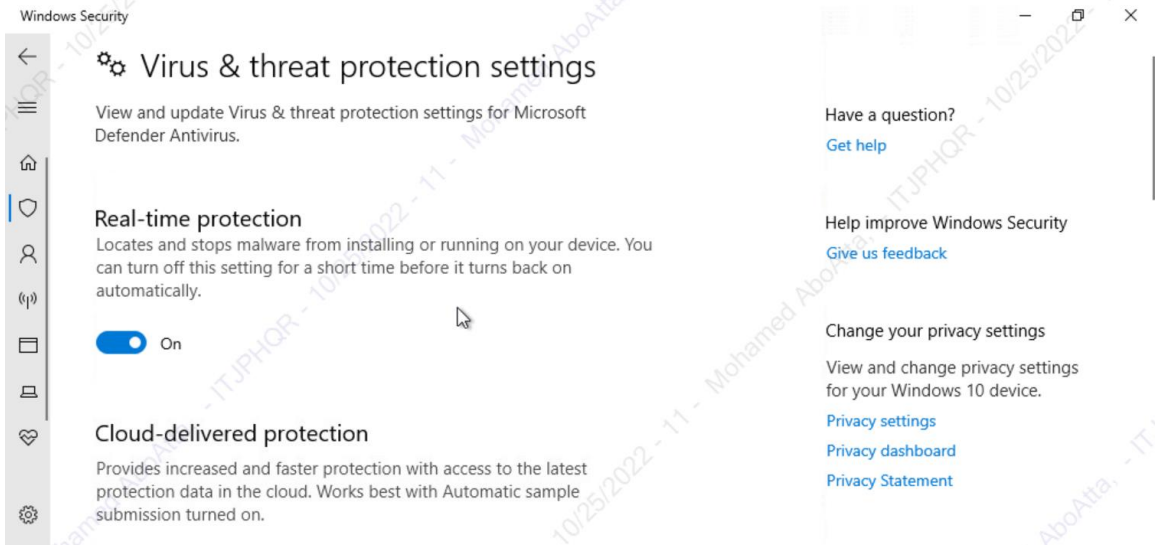
Virus & Threat Protection

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

1. ***Explain the process you take to do this.***
   - Search for 'Virus & threat protection'.
   - Under 'Virus & threat protection settings' click 'Manage settings'.
   - Ensure that 'Real-time protection', 'Cloud-delivered protection', 'Automatic sample submission' and 'Tamper Protection' are all turned on.

2. ***Include screenshots to confirm that anti-virus is enabled.***

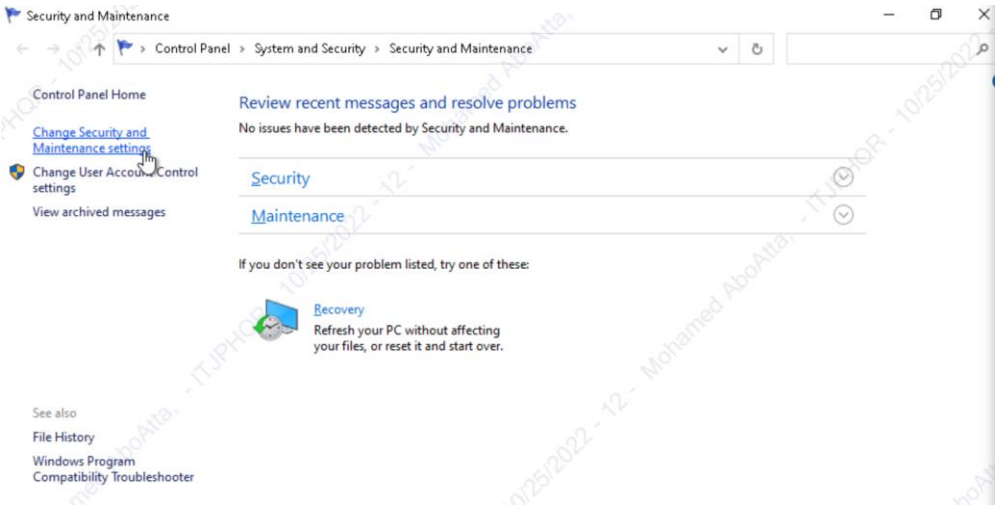


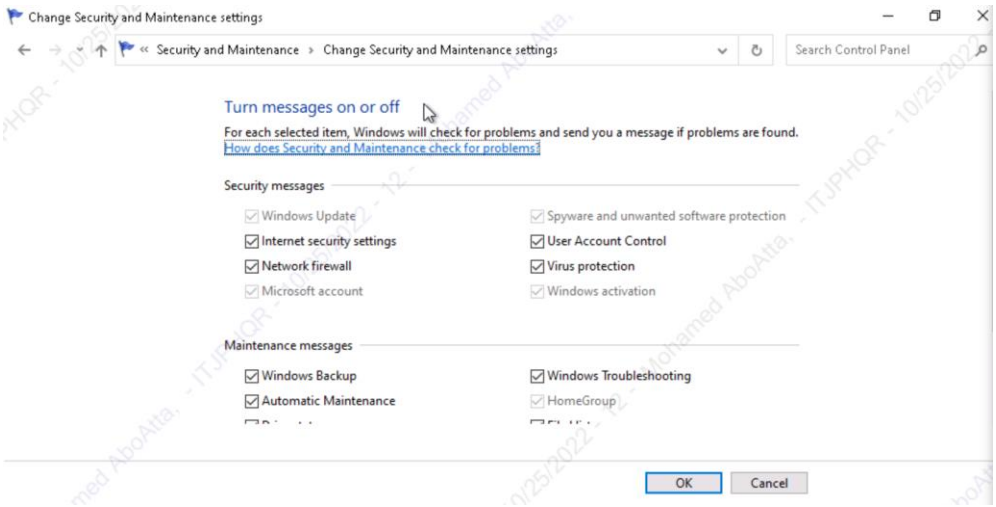


Once you determine that virus & threat protection is on and updated, you need to turn on messages about the Network firewall and Virus protection. Refer to the instructions above for viewing the settings within Security and Maintenance, Review recent messages and resolve problems.

1. ***Turn on the Network firewall and Virus protection messages using Change Security and Maintenance Settings.***
    - Search for 'Security and maintenance'. Then click on 'Change Security and Maintenance Settings' option in the sidebar.

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





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

- Firewalls can help prevent hackers or malicious software from gaining access to the PC through the Internet of a network. By turning on the notification messages of the firewall, we can know if there is any security problem with our firewall to secure it.
- Virus protection defends against various types of viruses and malwares. By turning on the virus protection notification messages, we can know if there is any problem with our virus protection to secure it.

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

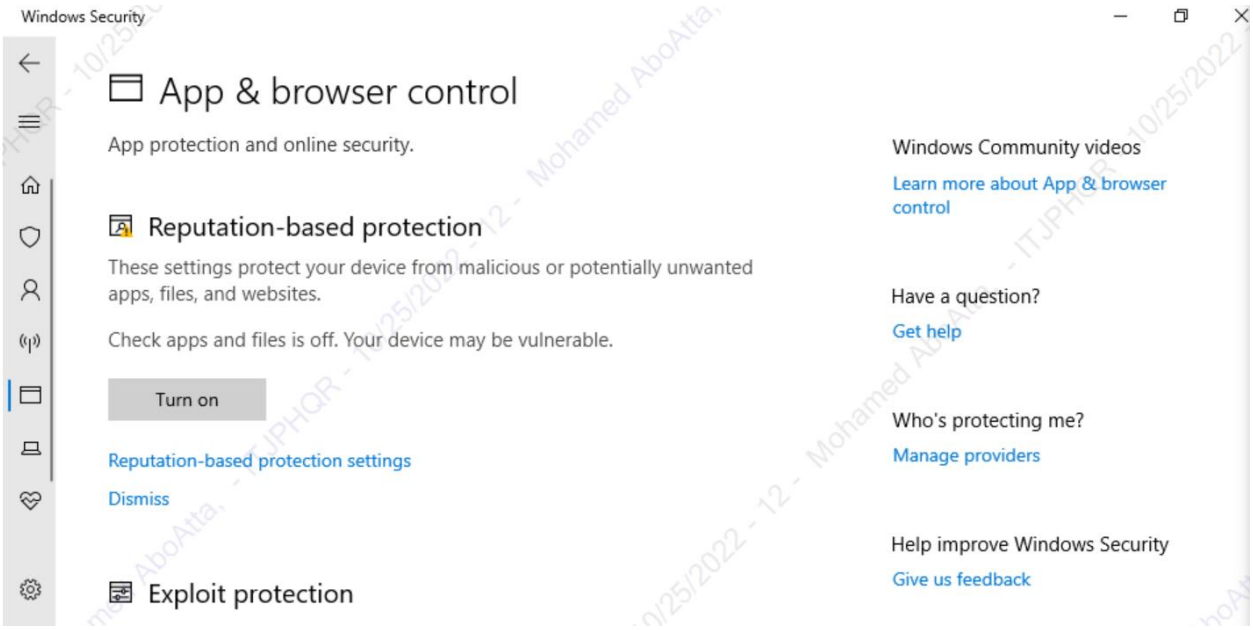
- 8. Malware Defenses
- 11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

App & Browser Control

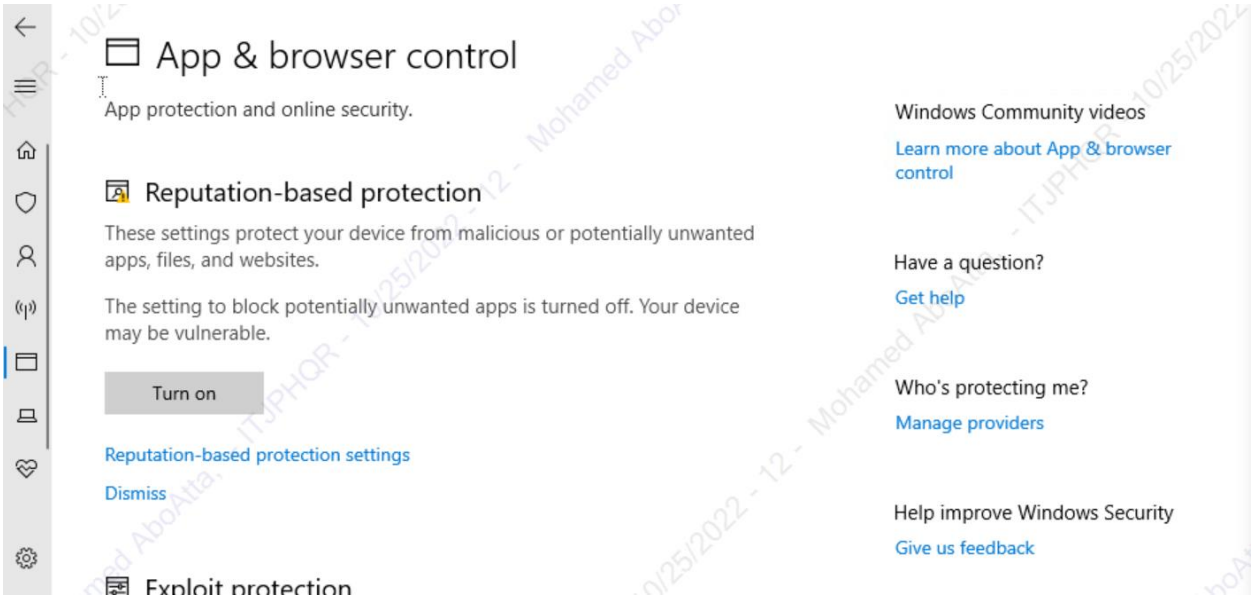
The App protection within Windows Defender helps to protect your device by checking for unrecognized apps and files and from malicious sites and downloads. Review the settings found within the *Account protection window, and App & browser control windows* found on the *Windows Defender Security page*.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

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

   - *Turn on Reputation-based protection*

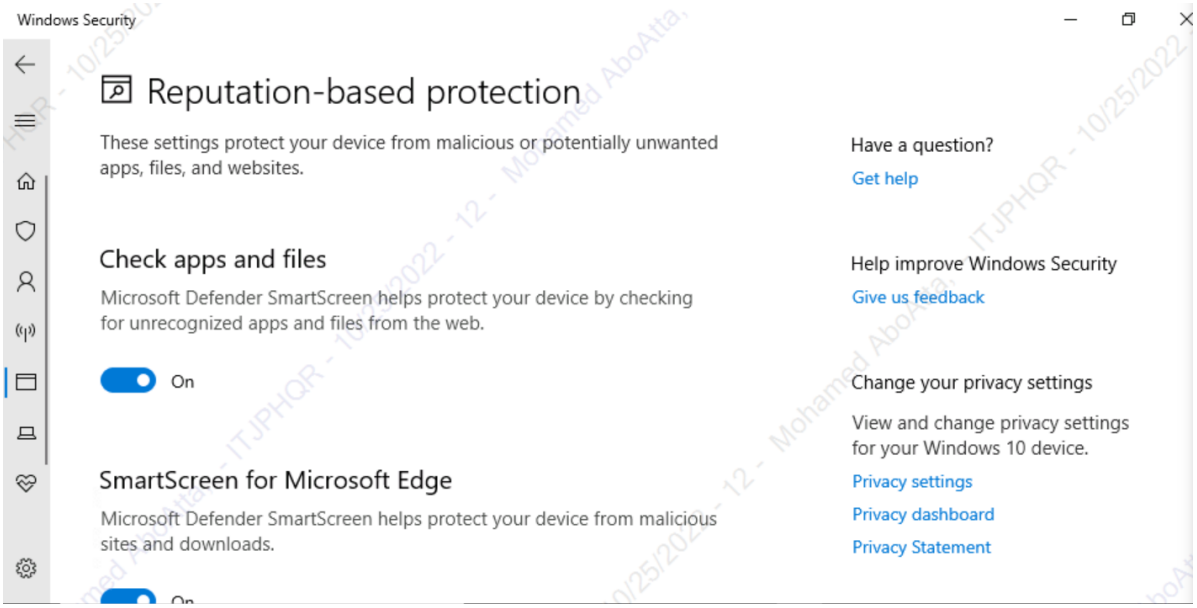


- *After clicking on 'Turn on' a message above it has appeared:*

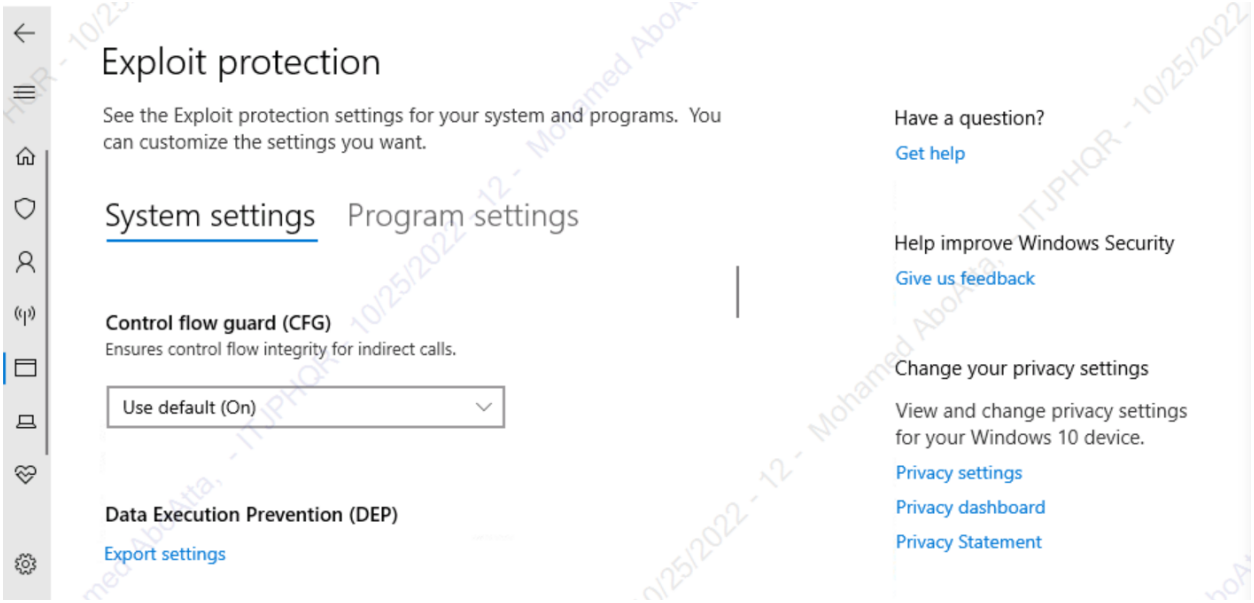


- *By clicking on 'Turn on' again, the reputation-based protection was enabled:*

- *We can review its settings by clicking on 'Reputation-based protection setting' to ensure all security settings are enabled:*



- *From the* 'App & browser control' window, we can click on 'Exploit protection settings' to ensure that correct settings are enable.

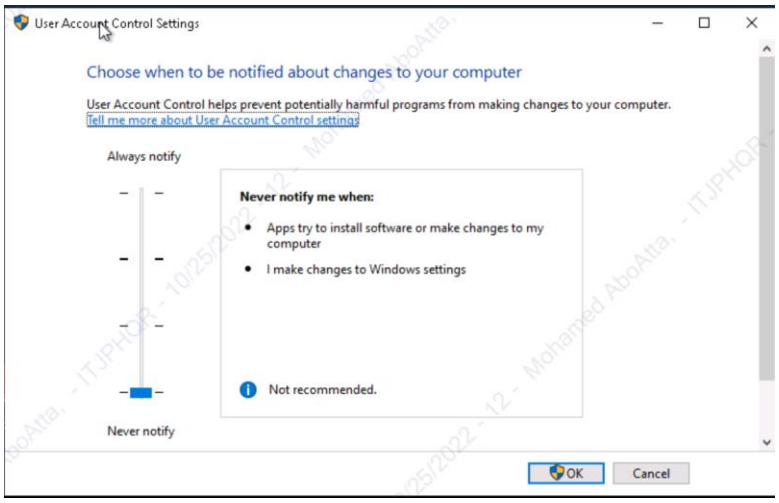


User Account Control Settings

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

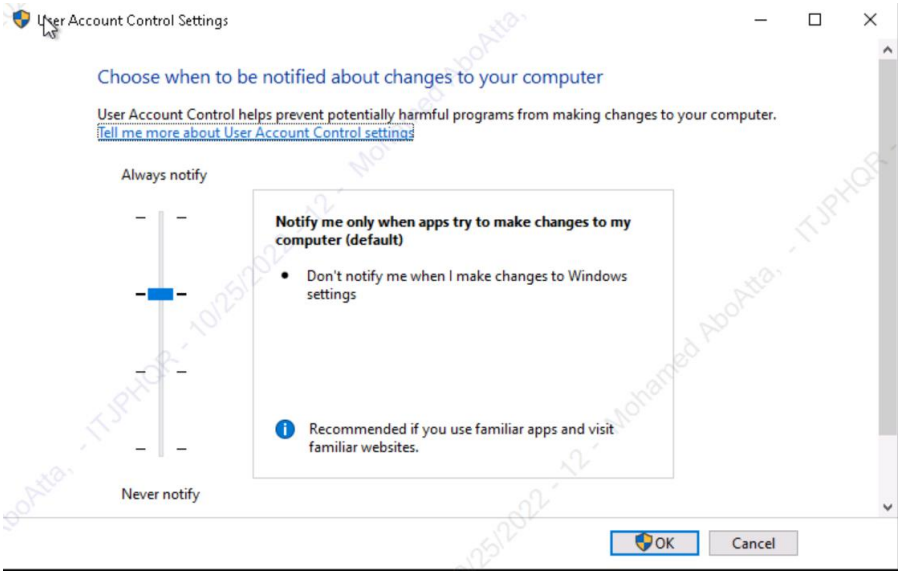
1. ***What is the current UAC setting on Joe's computer?***

   - This is available from the above security settings.
   - The current UAC setting is to never notify if apps try to install software or make changes to the computer.



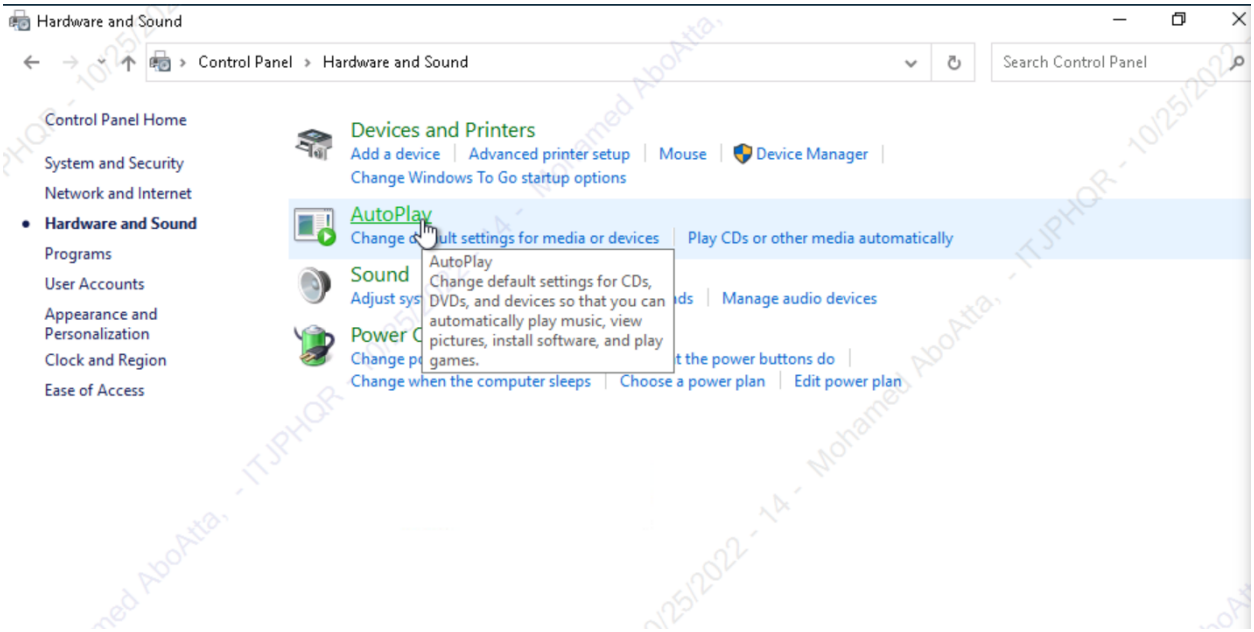
2. ***What should it be set to? Include a screenshot of the new setting.***

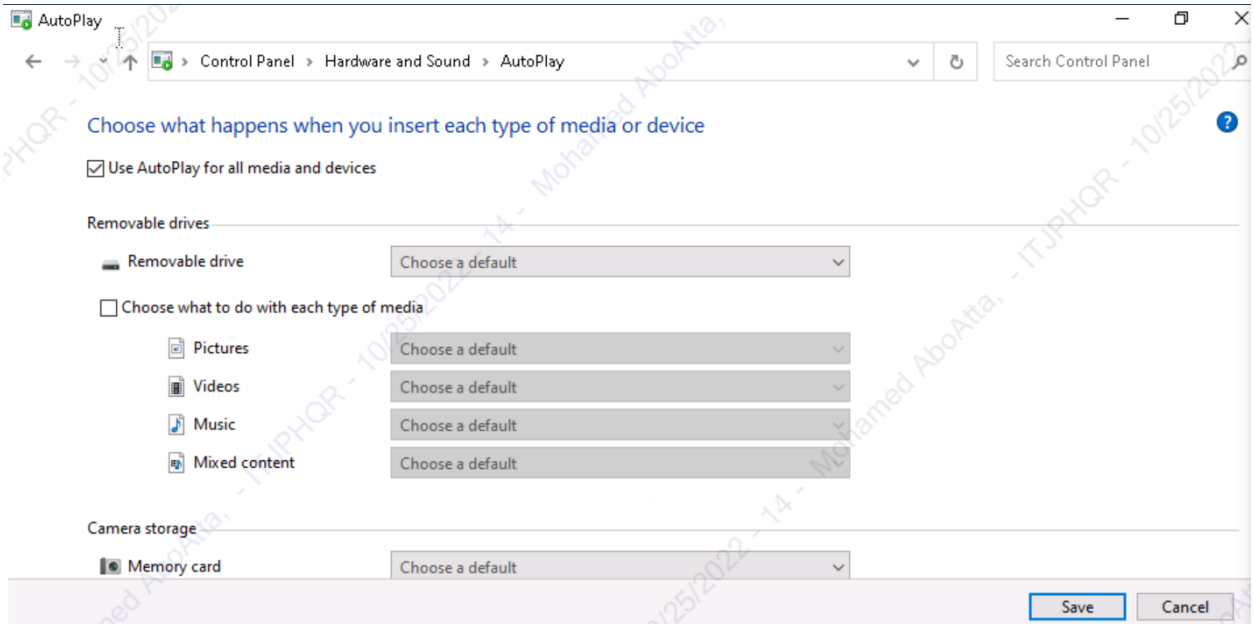
   - *The recommended settings are to notify when apps try to make changes to the computer*



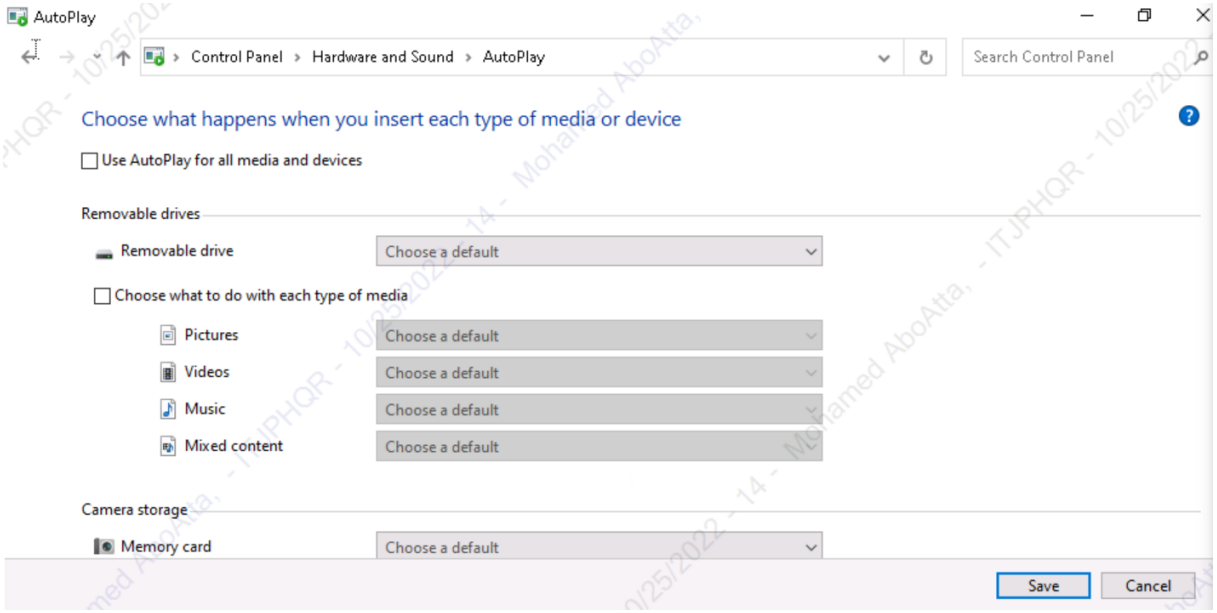
Securing Removable Media

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.

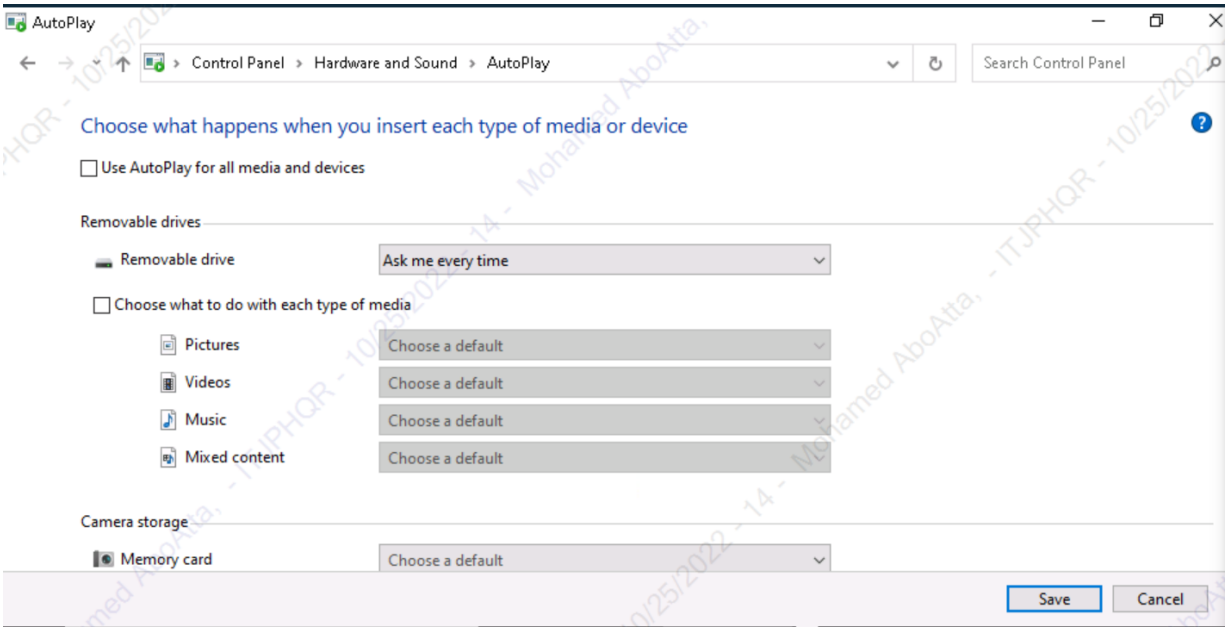




1. ***On Joe's computer, go to that function and deselect "Use AutoPlay for all media and devices."***



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.

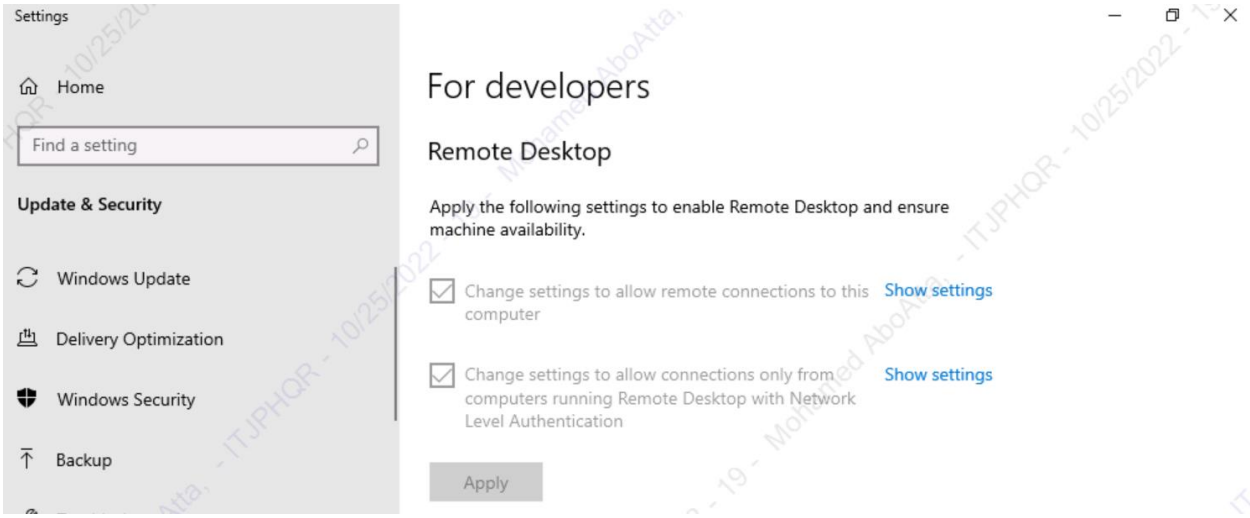
On Joe's computer, only the following accounts should be in use:

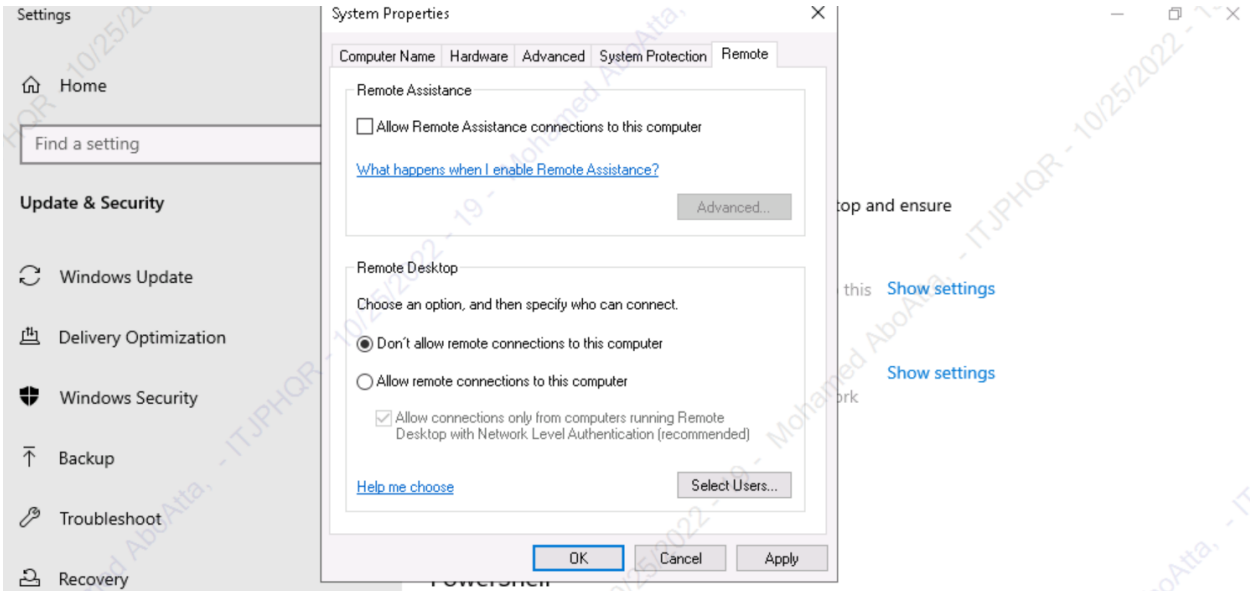
- JoesAuto
- Jane Smith (Joe's assistant)
- A User - Used for exercises (Not used in this project)
- Notadmin - Built-in administrator account (Not used for this project)
- Windows built-in accounts: Guest, DefaultAccount, and WDAGUtility (Not used for this project)

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.**
    - ➢ Search for ‘Allow remote connections to this computer’. Under the ‘Remote Desktop’ section, click on ‘Show settings’. Choose ‘Don’t allow remote connections to this computer’. You may also disable ‘Allow Remote Assistance connections to this computer’.



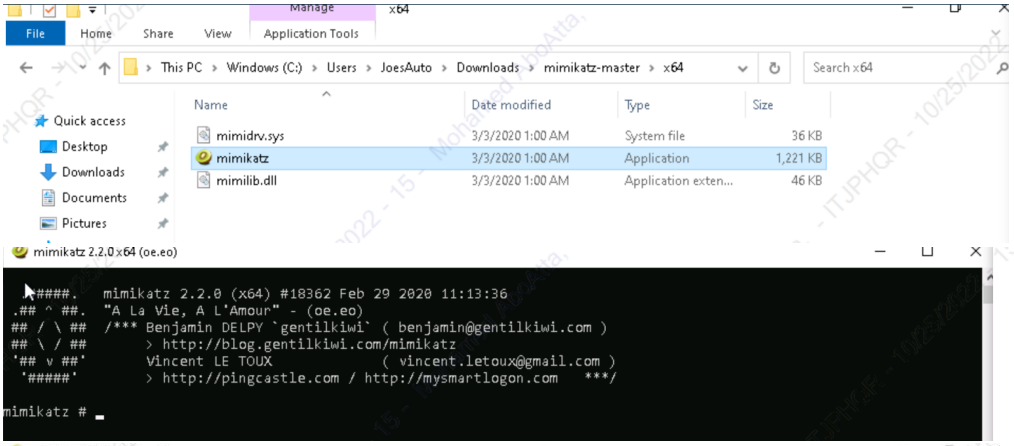


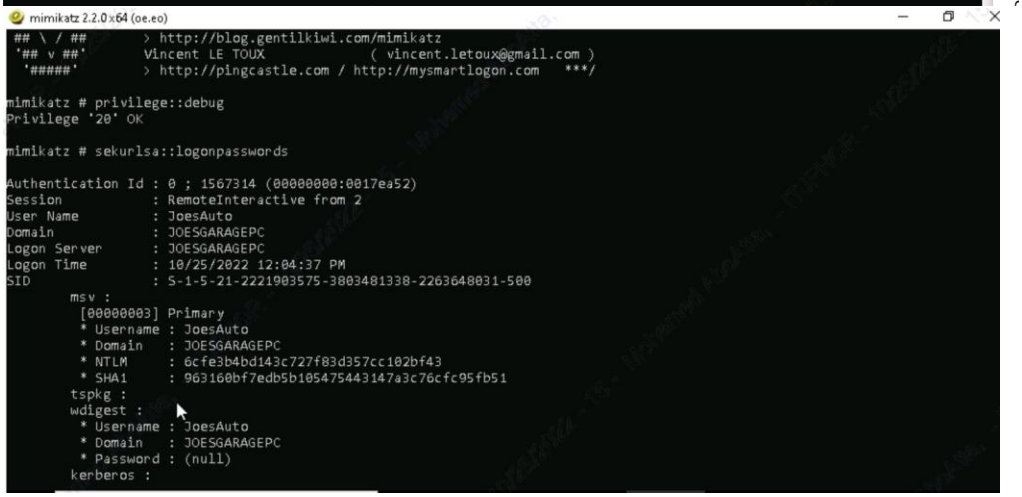
User Accounts

1. ***What user accounts should not be there?***
    - *Frank*
    - *Hacker*

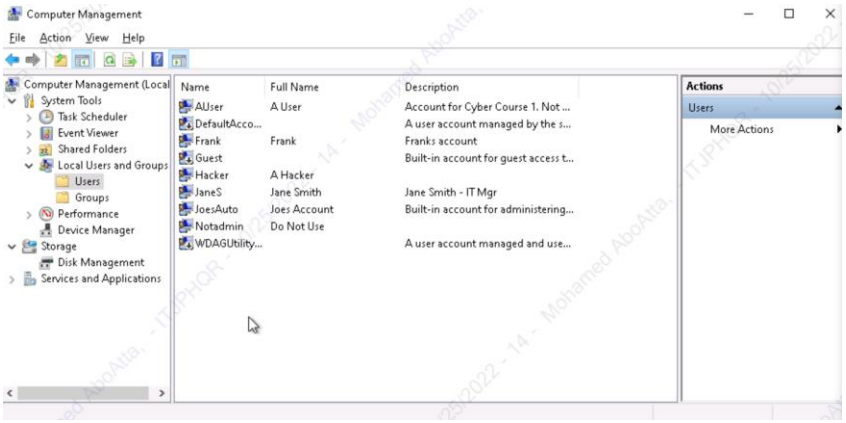
2. ***Bonus questions: What is Hacker's password?***

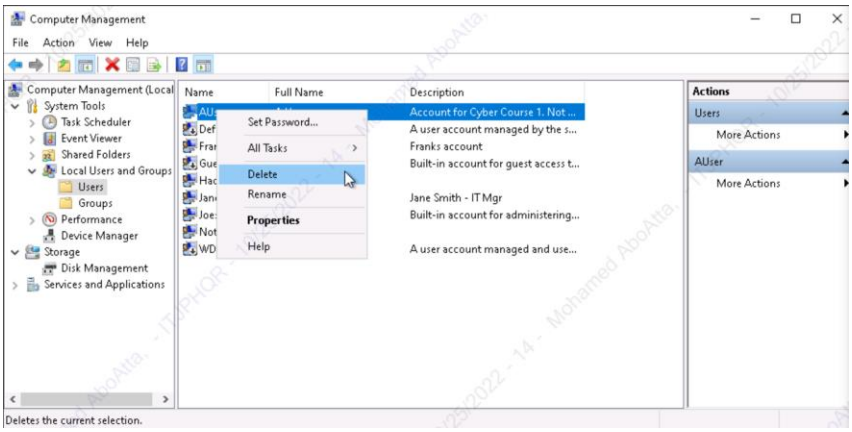
I've disabled the anti-virus protection and downloaded 'Mimikatz' from Github. After extracting the repo, I entered 'x64' folder, and opened 'mimikatz.exe' as administrator.

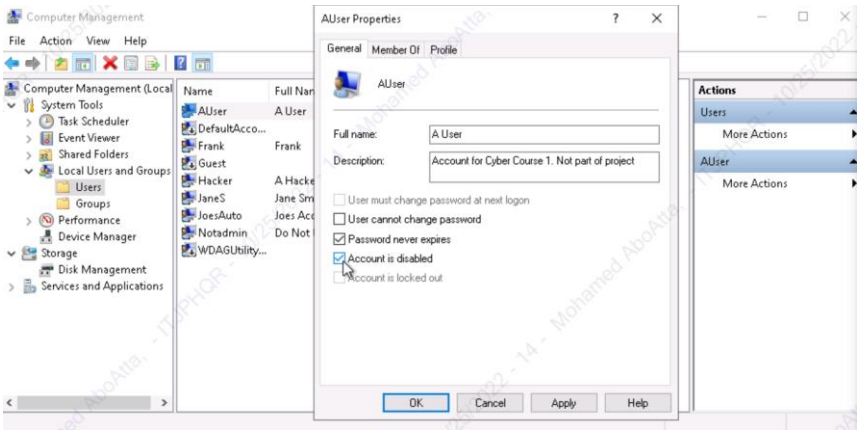




3. ***Explain the steps you take to disable or remove unwanted accounts.***
    - *Search for 'Computer Management', then click on 'Local users and groups'.*
    - *Then click on 'Users'. Right click on username.*
    - *If we want to delete the user account, we choose 'delete'.*
    - *If we want to disable the account, we click on 'Properties', then choose 'Account is disabled'*







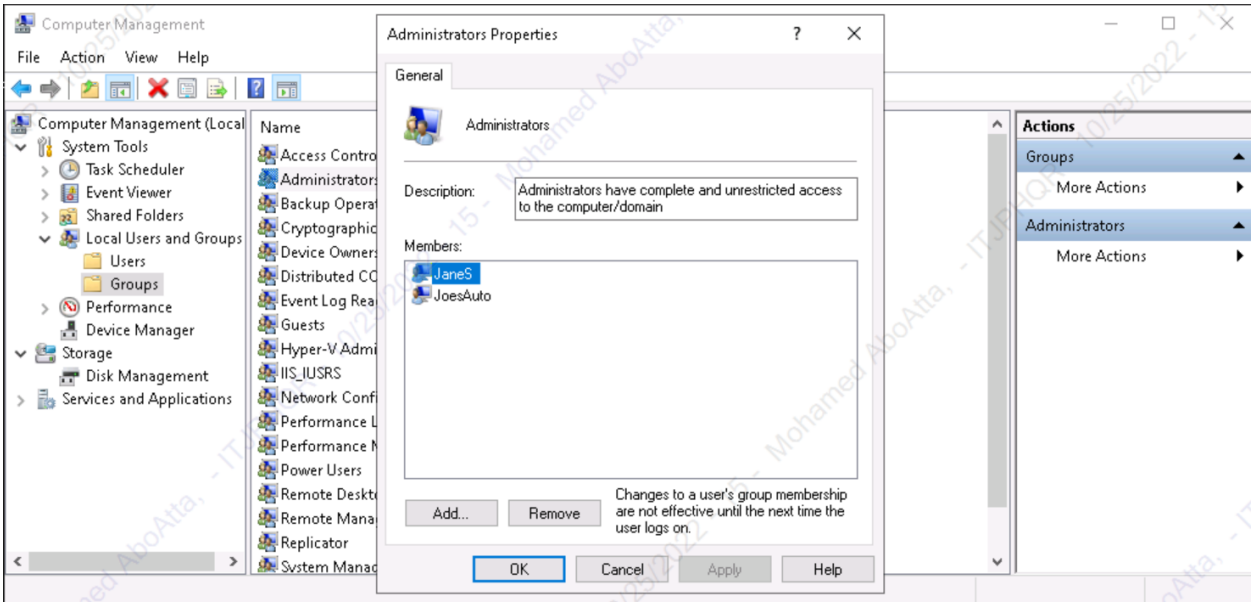
4. ***Why is it important to disable or remove unneeded accounts from a PC or application? Include potential vulnerabilities and risks.***

    - *This helps to keep Active Directory safe and secure from insider and outsider attacks.*

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?**
    - JaneS

6. **Explain how you determined this. Provide screenshots as needed.**
    - By viewing the administrator's group in 'Computer Management' window

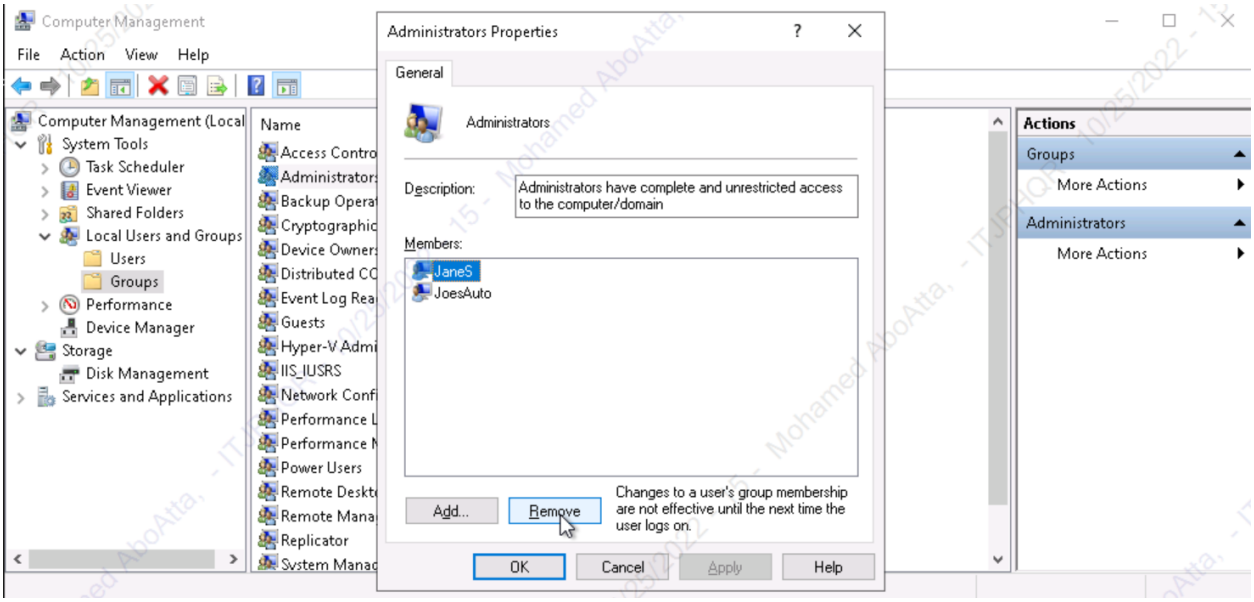


Administrator privileges for too many users are another security challenge.

7. **Provide at least three risks associated with users having administrator rights on a PC.**
    - Higher Risk of Virus/Malware Infections
    - Allowing Hackers to Create New User Accounts
    - Attacking Other Devices on Your Network

Now, you need to remove administrator privileges for any user(s) that should not have it.

8. ***Explain the process for doing this. Include screenshots to show your work.***
   - *By choosing the user account we want to remove from the administrator group, then click 'Remove'*



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

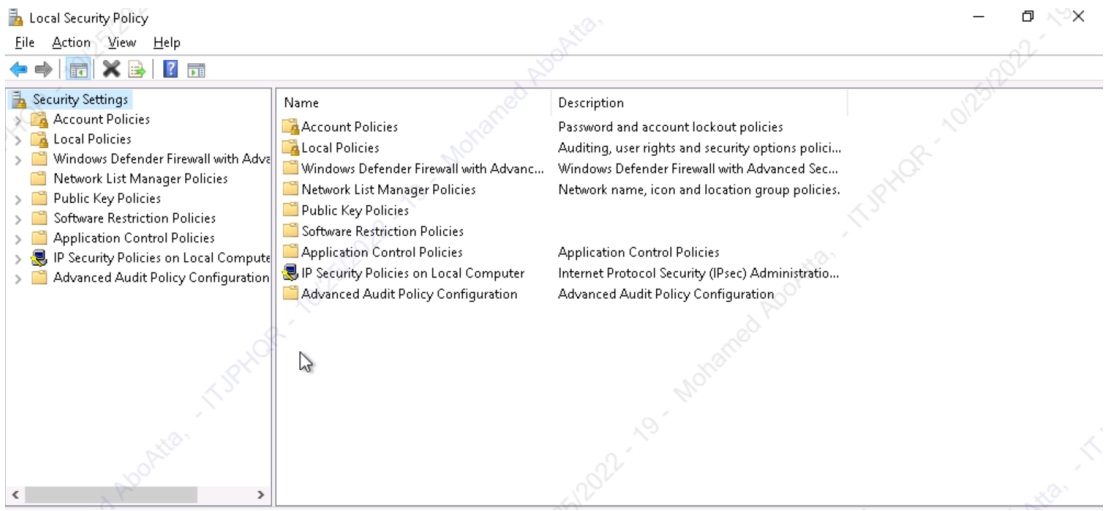
10. **The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?**
    - Step 4: *Controlled Use of Administrative Privileges*

Setting Access and Authentication Policies

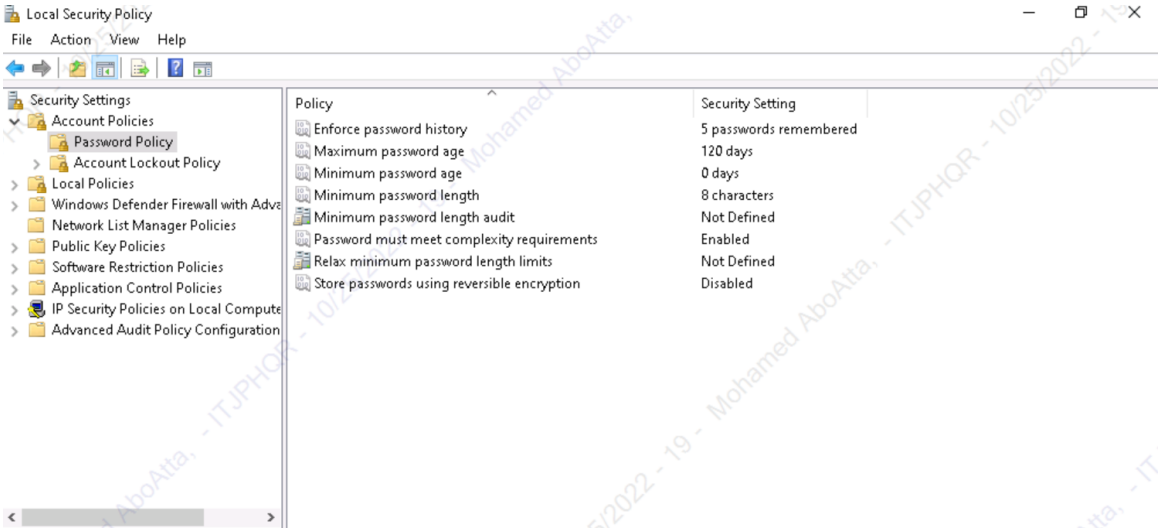
After you talked with Joe about security, he has asked that the access rules outlined above be in place on his PC.

These are set using the Local Security Policy function in Windows 10. On the Windows search bar, type "*Local Security Policy*" to access it. Click the > arrow next to both "*Account Policies*" and "*Local Policies*" and review their contents.

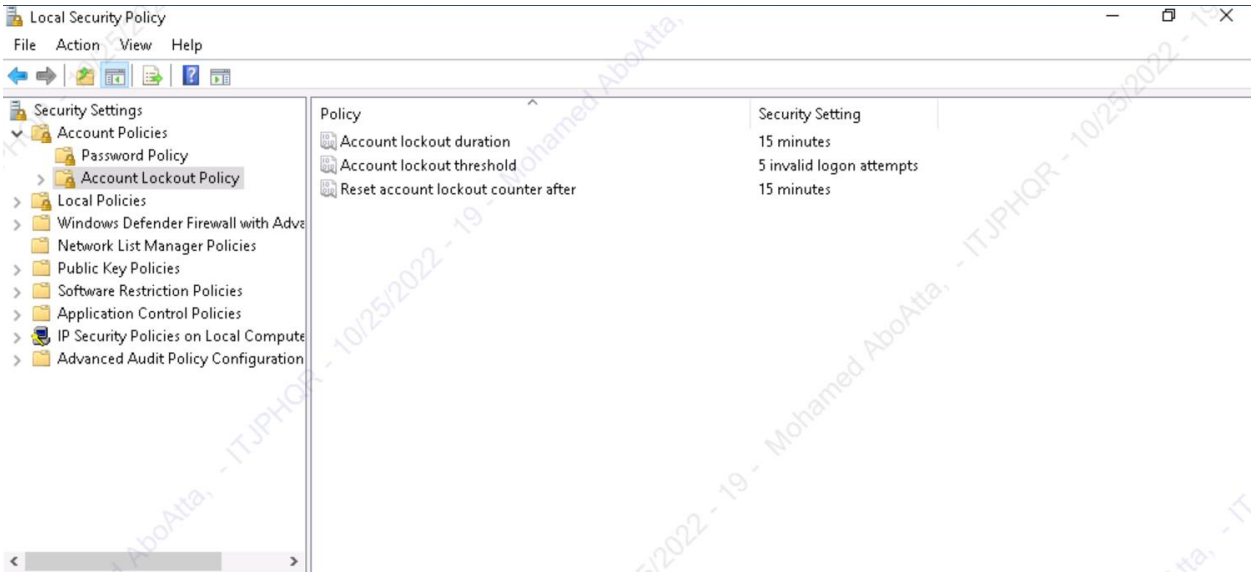
1. ***Provide a screenshot of the Local Security Policy window here.***
   [Note: Local Security Policy is not available on Windows 10 Home edition.]



2. **Explain the process for setting the password and access control policies locally on a Windows 10 PC. Provide screenshots showing how you set the rules on the PC.**
    - Setting the Password Policy:
    - Click on 'Account Policies' then click on 'Password Policy'. Double click any settings to edit it. Screenshot after setting the Password Policy:



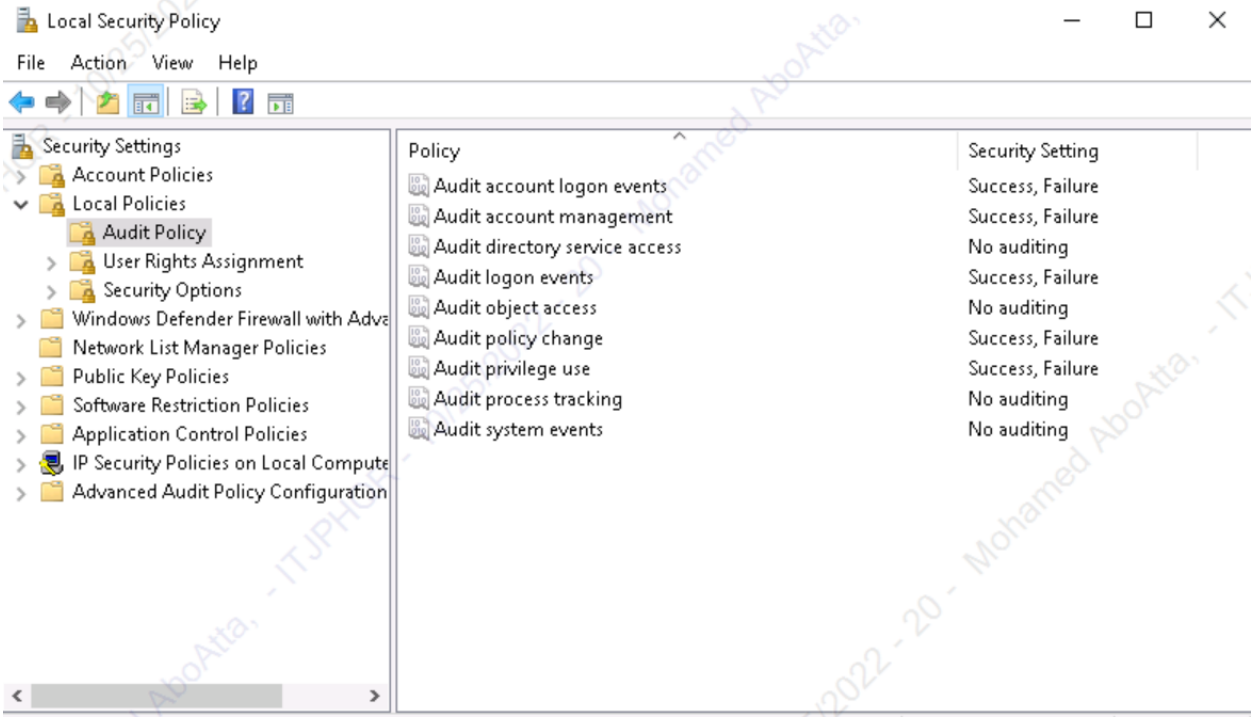
- Setting the Account Lockout Policy:
- Click on 'Account Policies' then click on 'Account Lockout Policy'. Double click any settings to edit it. Screenshot after setting the Account Lockout Policy:



Auditing and Logging

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

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



4. Securing Applications

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

Joe has established the following rules regarding PC applications:

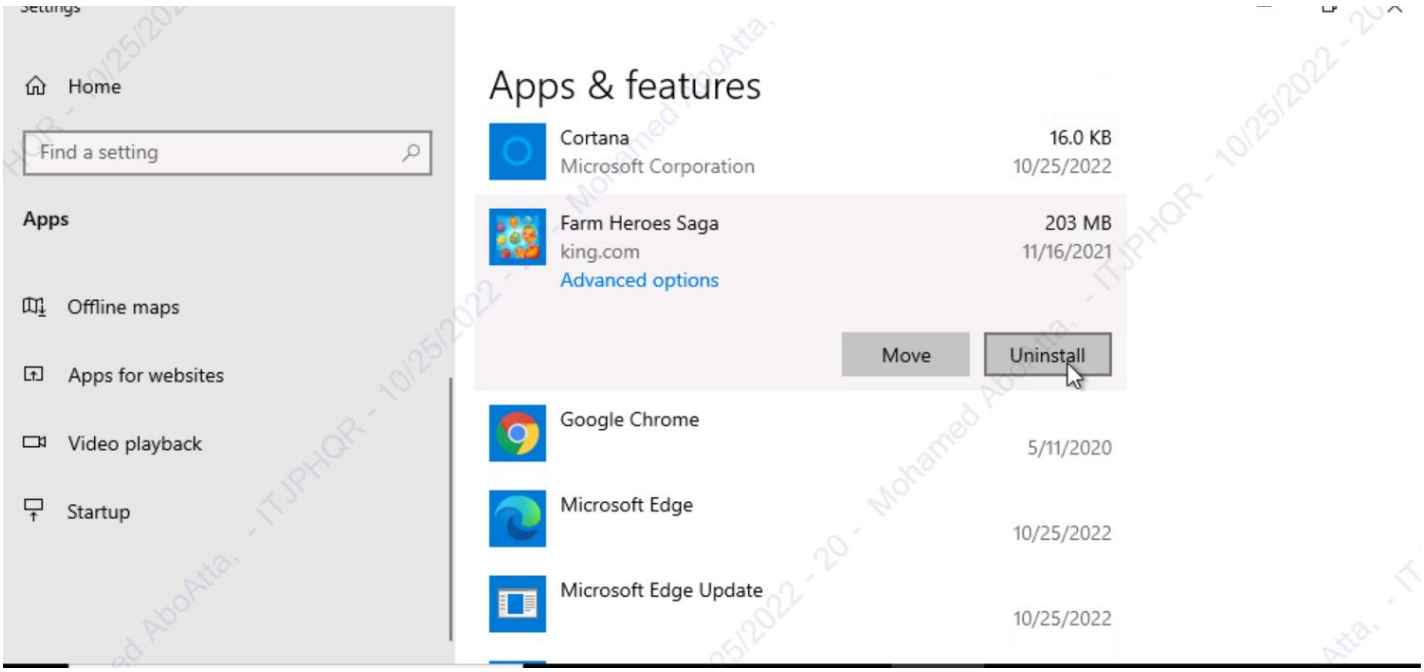
- Joe wants everyone to use the latest version of the Chrome browser by default.
- There should be no games or non-work-related applications installed or downloaded.
- Joe is also concerned that there are “hacking” programs downloaded or installed on the PC that should be removed.
- This PC is used for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

Remove unneeded or unwanted applications

1. ***List at least three application(s) that violate this policy.***
   - *Candy Crush Friends*
   - *Farm Heroes Saga*
   - *Spotify Music*

2. ***Name at least three vulnerabilities, threats or risks with having unnecessary applications:***
   - *Unneeded programs could be vulnerable to attacks*
   - *Unneeded programs can* allow unauthorized access into the computer
   - *Unneeded programs* consume system resources
   - *Unneeded programs* could also violate licensing agreements

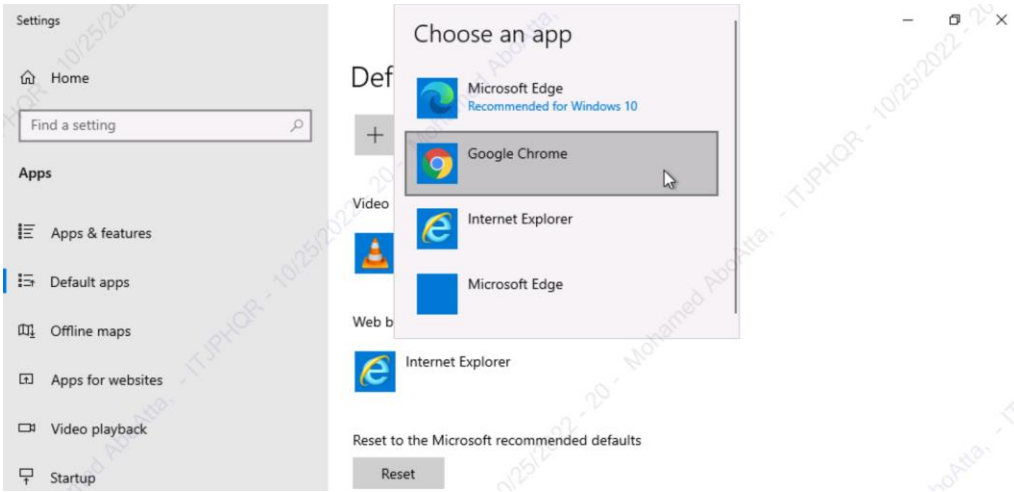
3. ***Joe wants you to make sure unneeded applications or programs are no longer on the PC. Explain the steps you take to disable or remove them. Include screenshots to show your work.***
   - *Search for 'Apps & features'. Click on any app name. Click 'Uninstall'.*



Default Browser

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

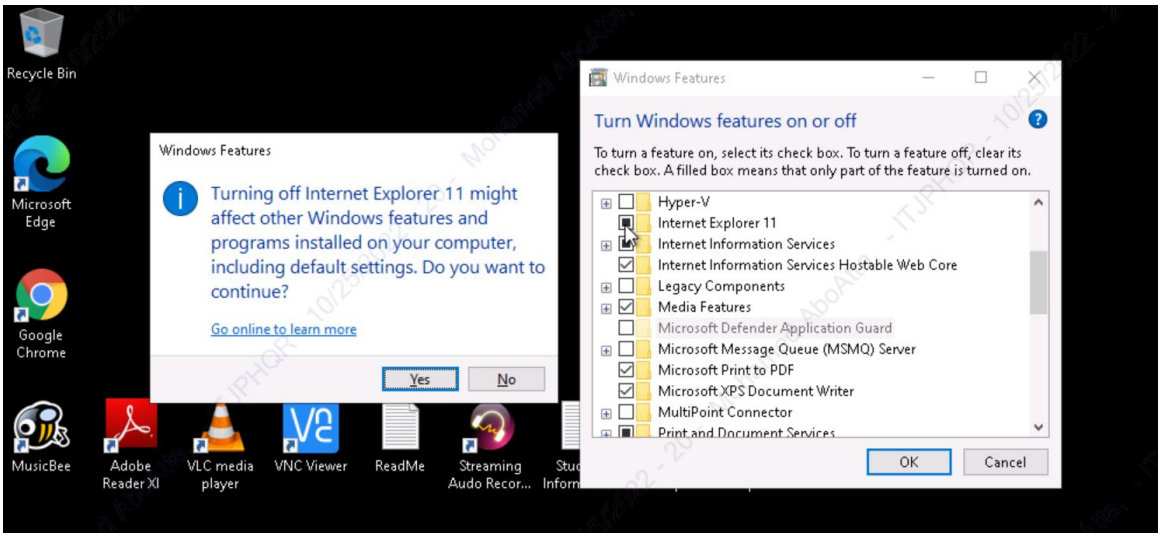
1. ***Explain how you set default applications within the Windows 10 operating system. Include screenshots as necessary.***
    - *Search for 'Default apps'. Under 'Web browser', choose 'Google Chrome'*



2. ***Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.***
    - Several zero-day vulnerabilities have exploited issues within Internet Explorer.
    - Lack of Support

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**."

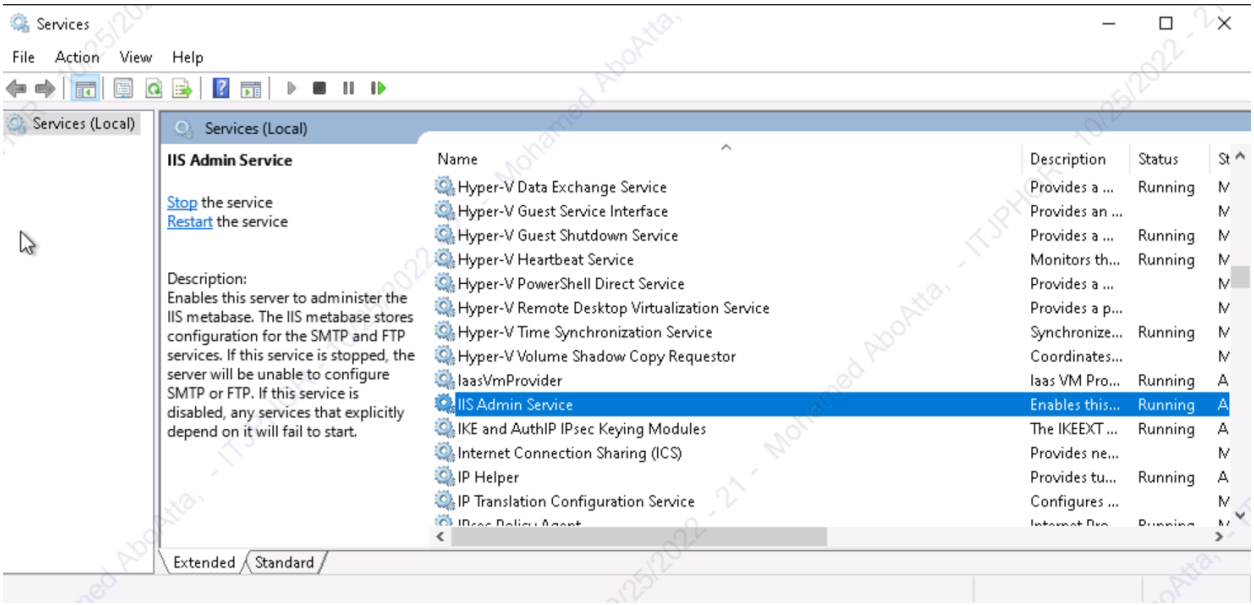
3. ***Provide a screenshot showing Internet Explorer 11 is off.***



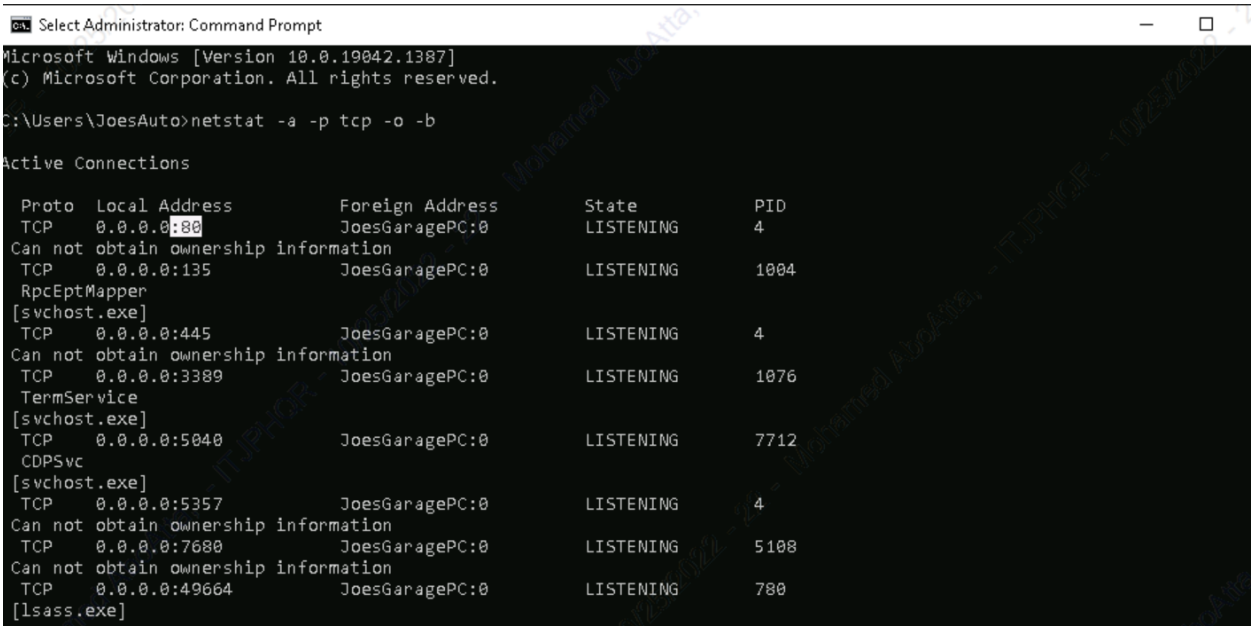
Windows Services

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.

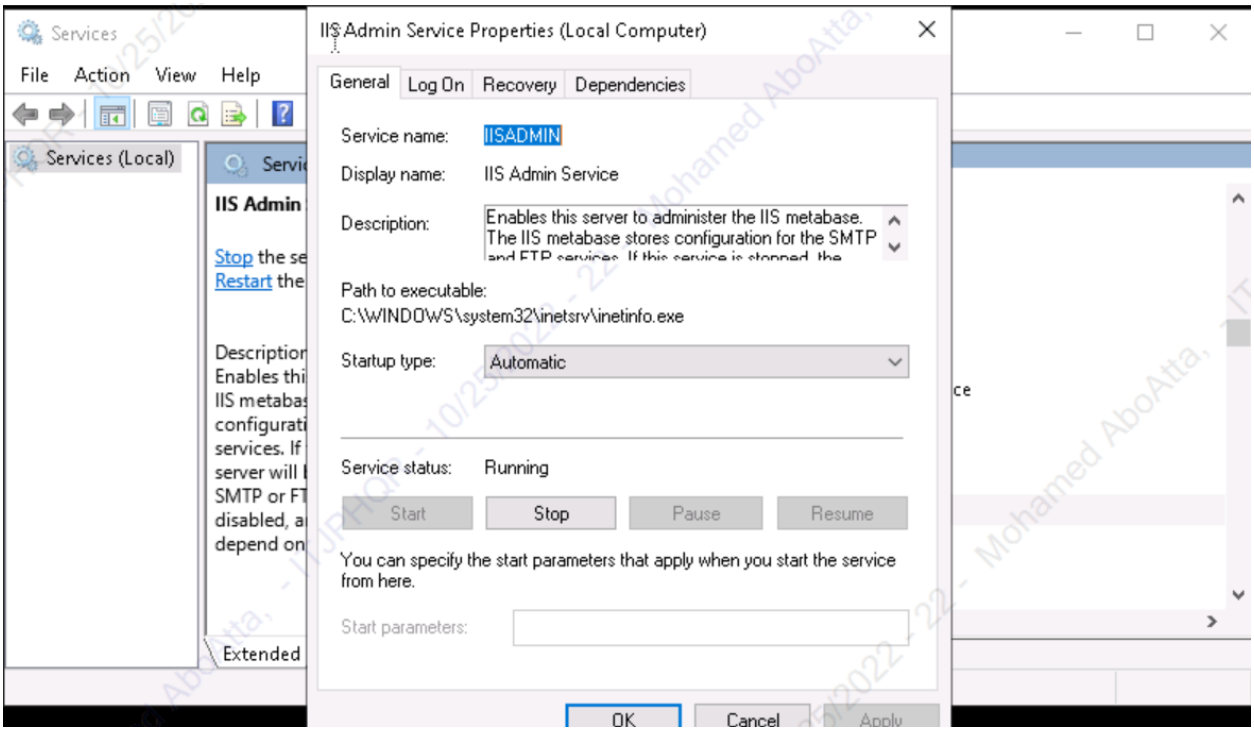
1. **How did you determine these services were running? Include screenshots to show how you found them.**
    - Search for 'Services' and check services list



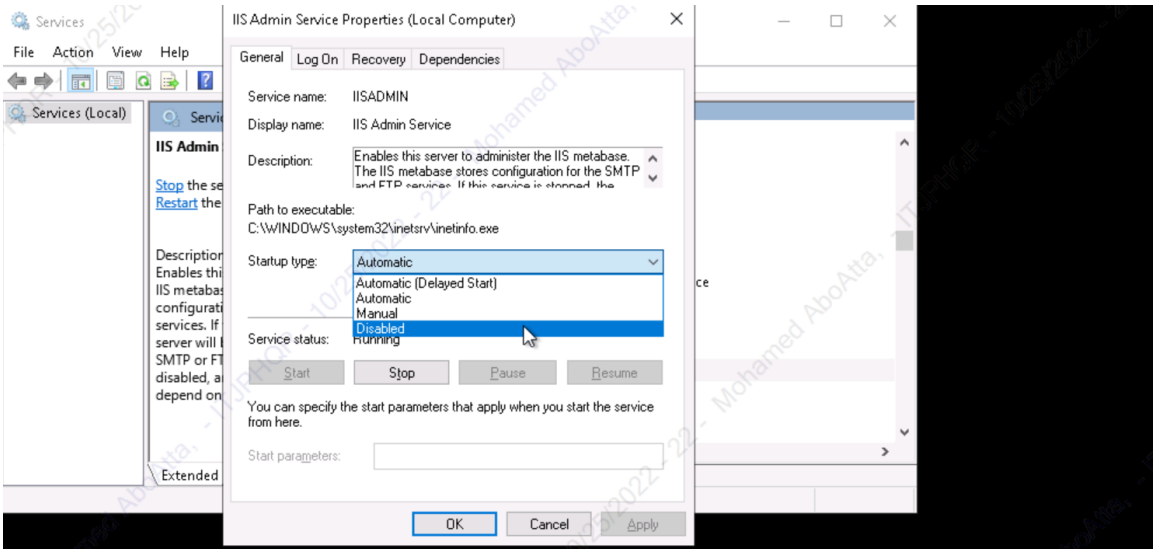
2. **Advanced users should provide at least two methods for determining a web server is running on a host**
    - By running the following command in cmd ‘netstat -a -p tcp -o -b’. Then check if there is any listening connection at port 80 or 443.



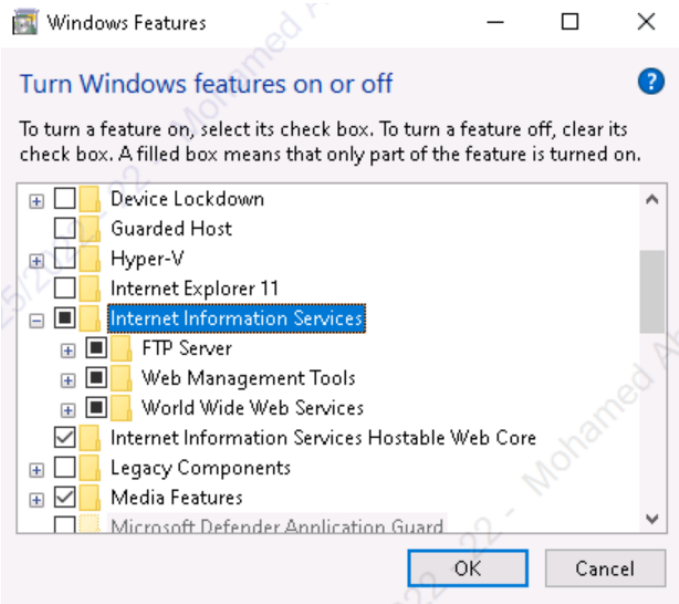
    - From ‘services’ window, check any service that is related to ‘IIS’ (Internet Information Services’ is running.



3. **How do you disable them and make sure they are not restarted?**
    - We can disable any service by right click on it. Then choose 'Properties'. From 'Startup type', choose 'Disabled'. Then finally we can stop the service immediately by clicking on 'Stop'.



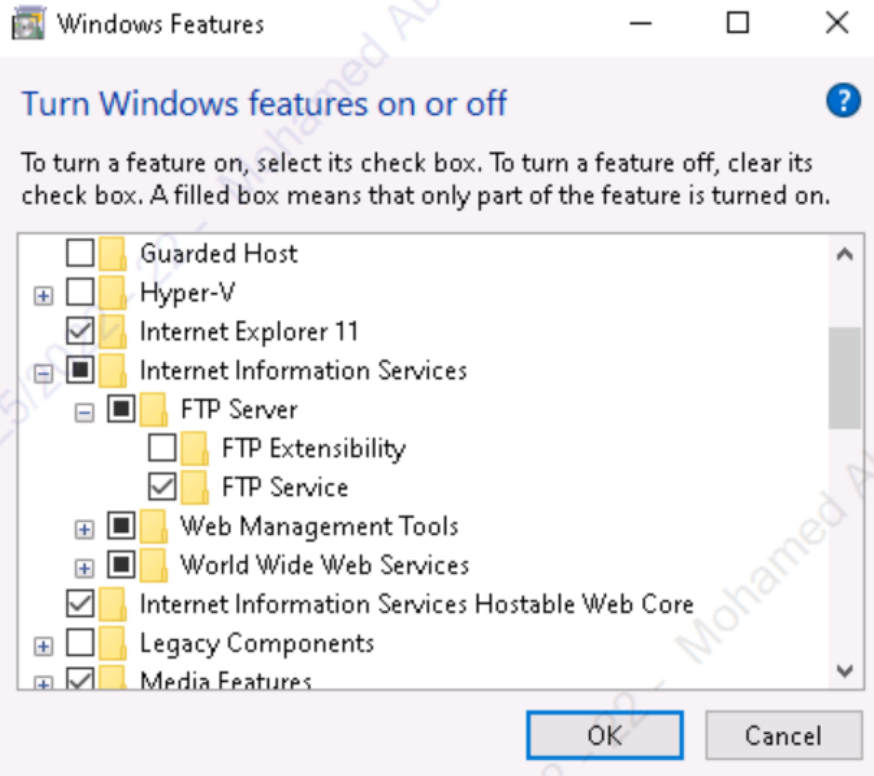
    - We can also disable the IIS service through the windows features window



    - It's also advised to disable the services in the following resources:
        - https://www.pcerror-fix.com/windows-10-services-to-disable-for-gaming
        - https://windowsreport.com/disable-windows-services/
        - List of all Windows 10 Services: https://ss64.com/nt/syntax-services.html

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.**

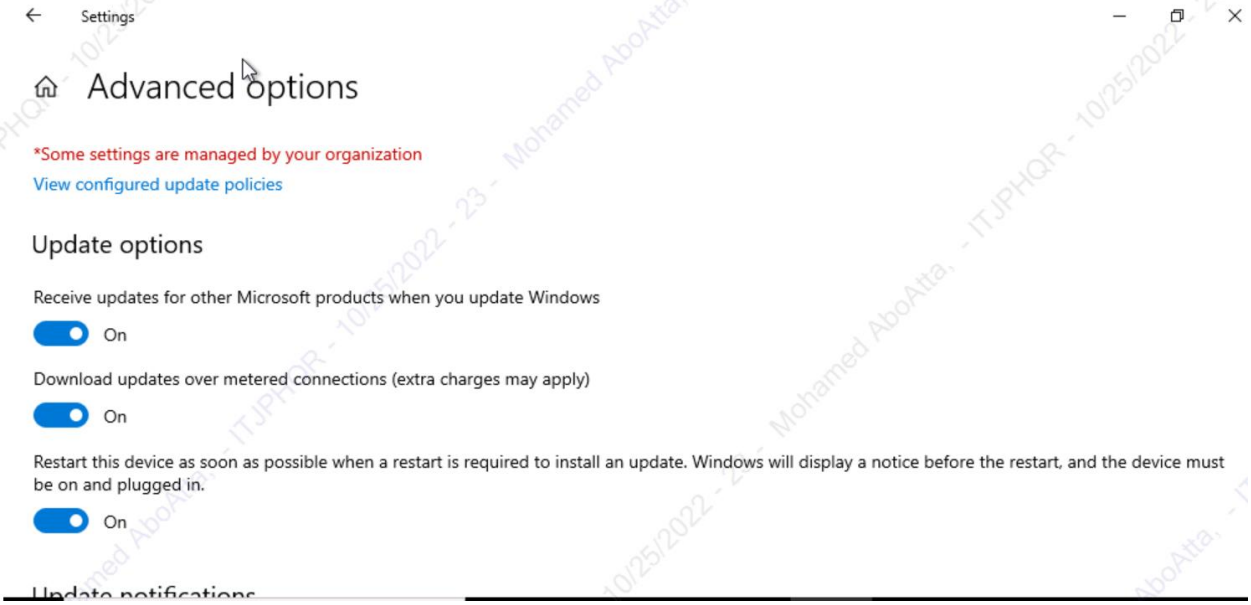
   - We can disable the FTP by searching for 'Turn Windows features on or off'. Then expand 'Internet Information Services' options. Also, expand 'FTP Server' options. We can see that the 'FTP Service' is enabled, so we should disable it.



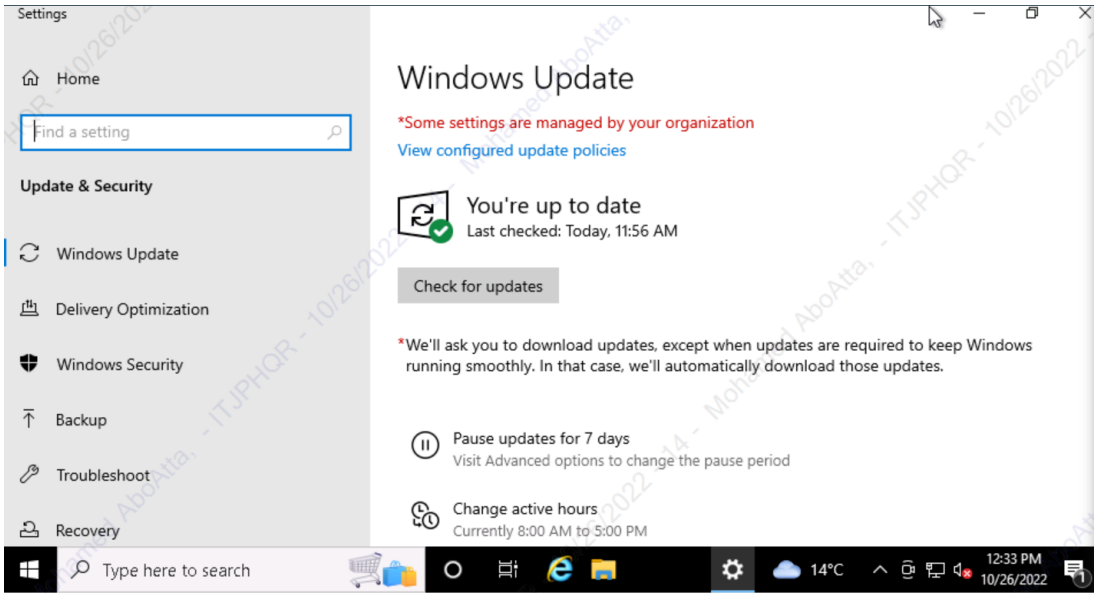
Patching and Updates

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.***
    - *Search for 'Windows Update'. Then click on 'Advanced options'. Turn on all needed options*

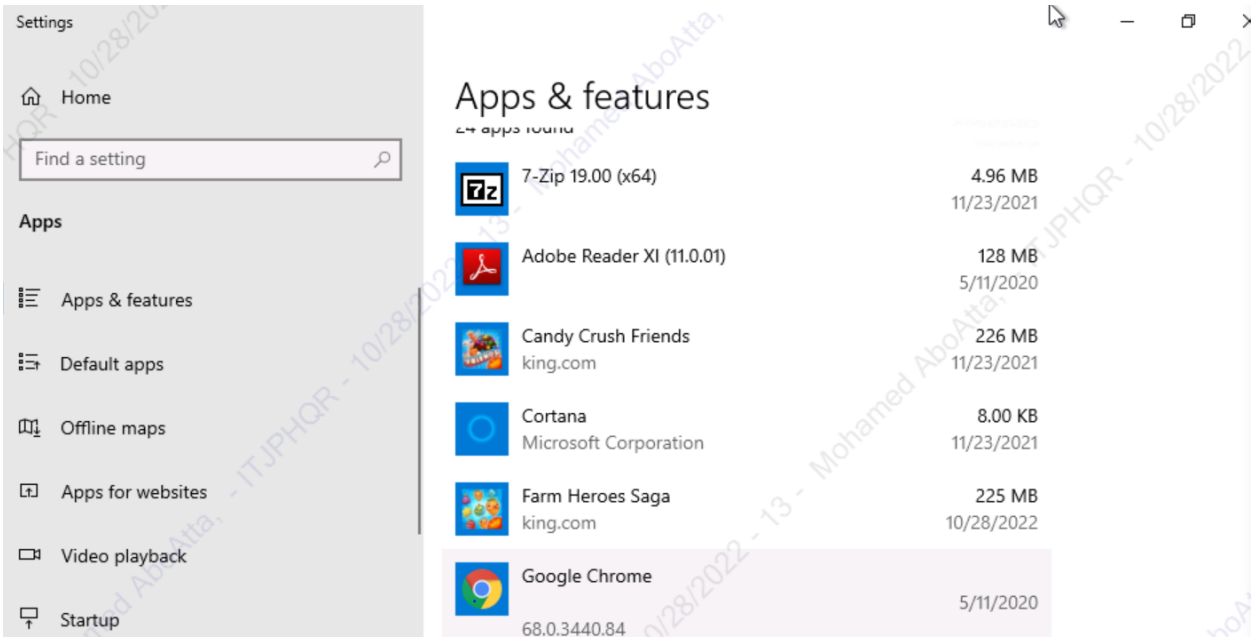


2. *Go ahead and update this PC to the latest version. Warning this may take a while and require numerous restarts. When it is complete, provide a screenshot showing the PC is on the latest version.*



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

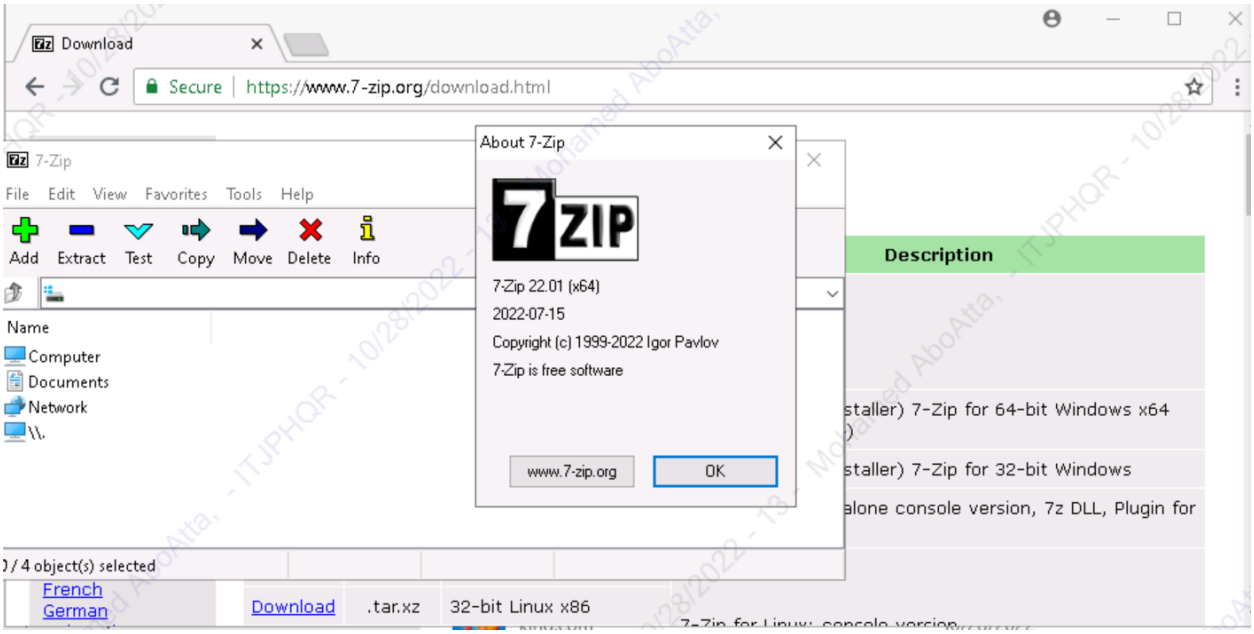
3. ***List at least two applications on Joe's PC that are out of date. List them below:***
   - 7-Zip v19.00(x64)
   - Google Chrome v68.0.3440.84



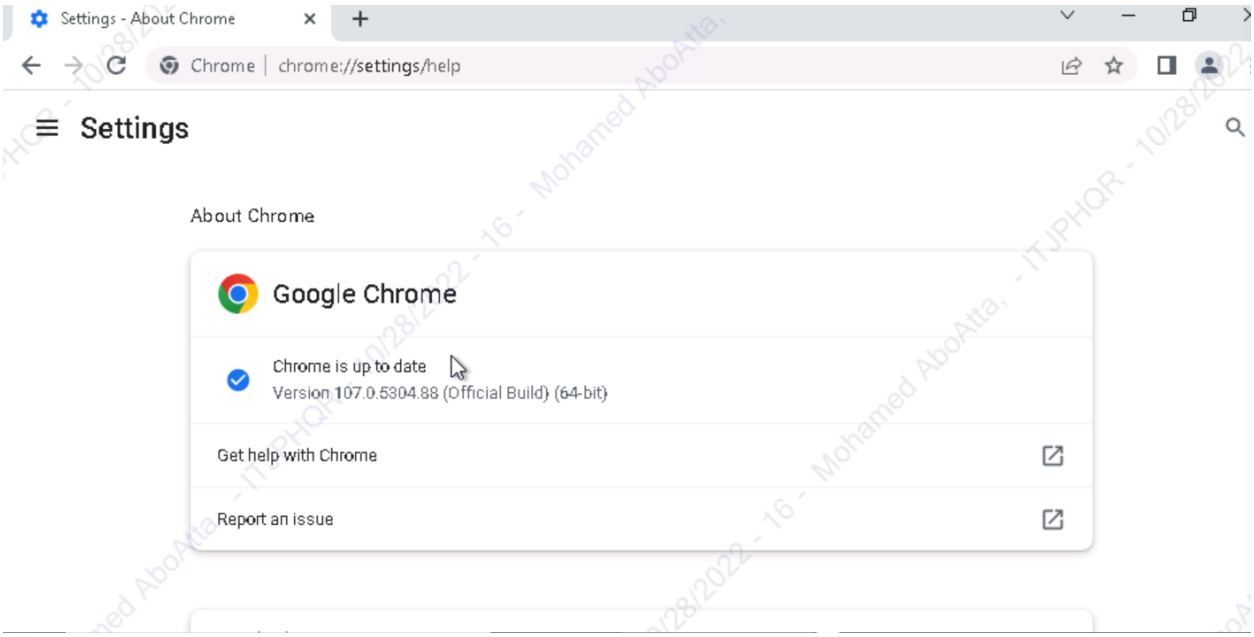
4. ***Explain the steps you took to determine this information.***
   - *By checking application versions and comparing them against vendors changelogs.*
   - *We can check application version by searching for 'Apps & features'*

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

- **7-Zip:** Downloaded and installed the latest version from vendor's website.



- Chrome: Downloaded and installed the latest version from vendor's website.



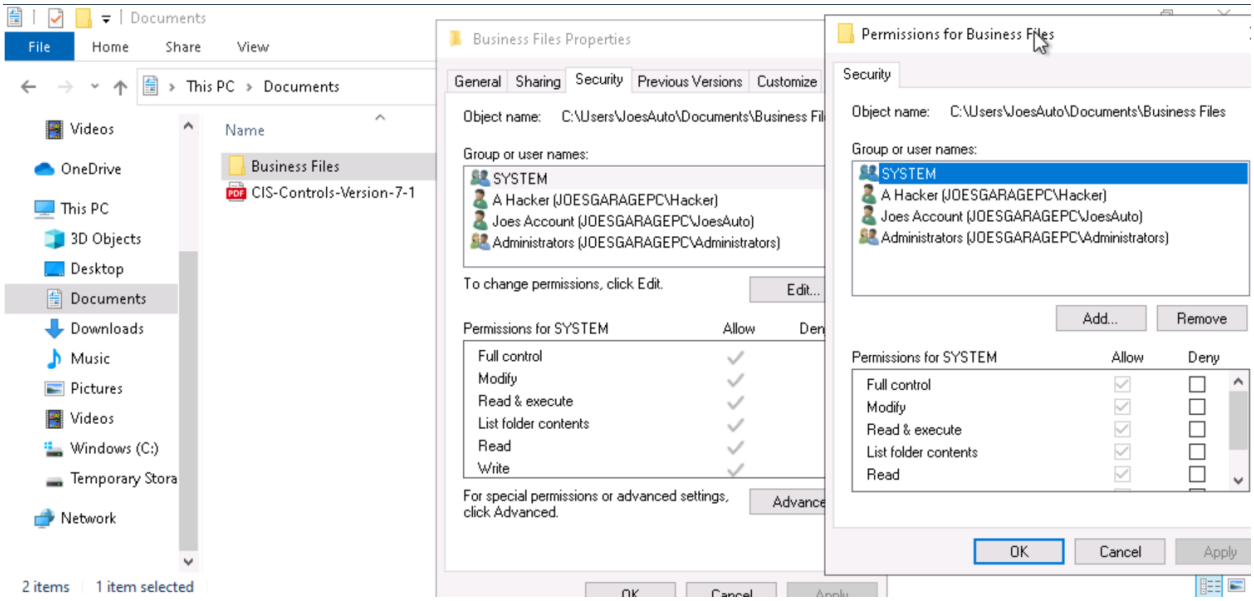
5. Securing Files and Folders

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

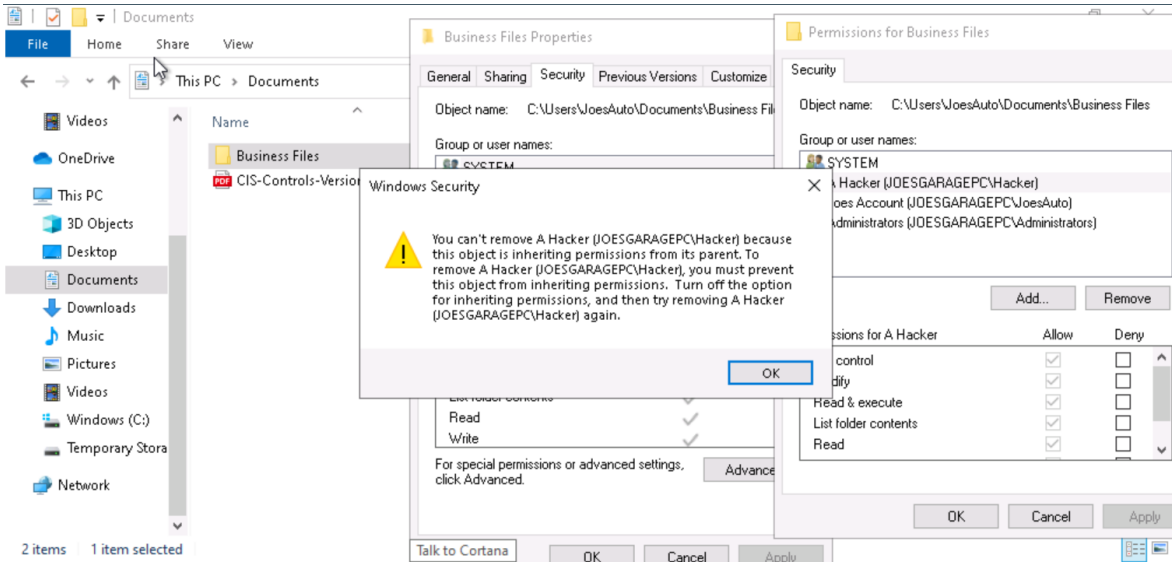
Joe suspects that other users on this computer beside him and Jane can see and change his business files. He wants you to check to make sure that only those two users have privileges to view or change the files.

Encrypting files and folders

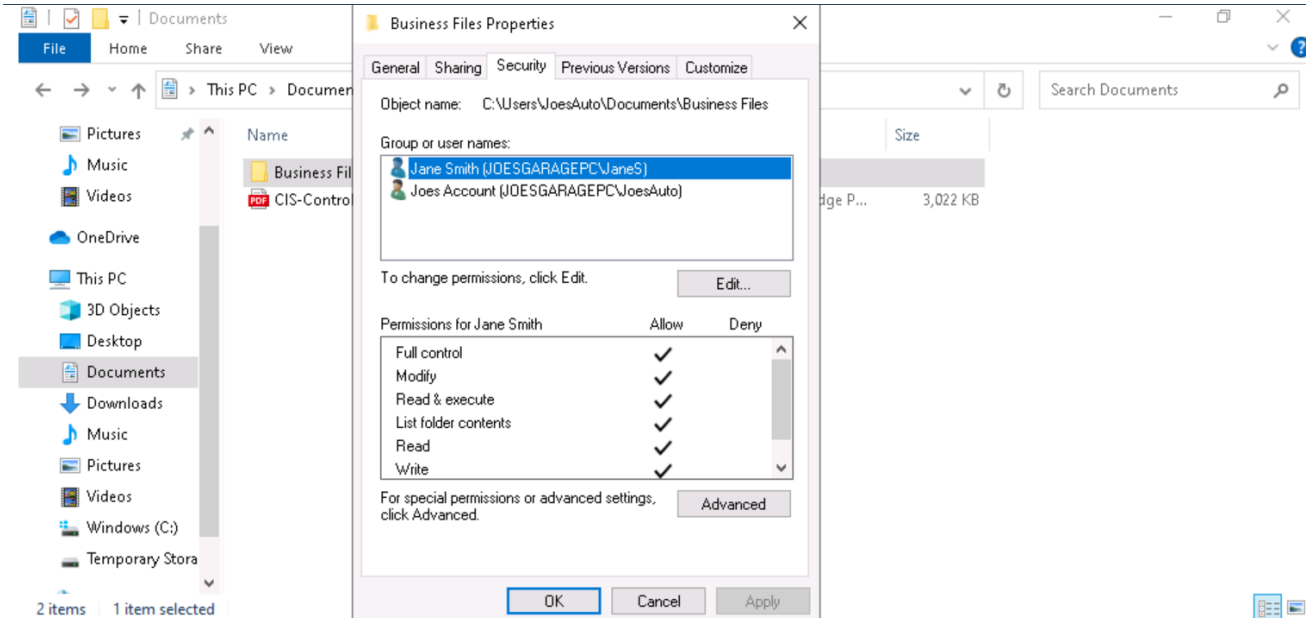
1. ***Explain the process for checking this and changing any necessary settings on the file. Include screenshots showing that ONLY Joe and Jane have permissions to change Joes work files. [Hint: Right-click the folder and select Properties.]***
    - *Navigate to folder path. Right click on the folder and choose 'Properties'.*
    - *Click on 'Security' tab. Under 'Group or usernames' you can see all users and groups who can access the folder. Click on any group or username, and you will see under 'Permissions for' section, all the permissions of that user/group on that folder.*



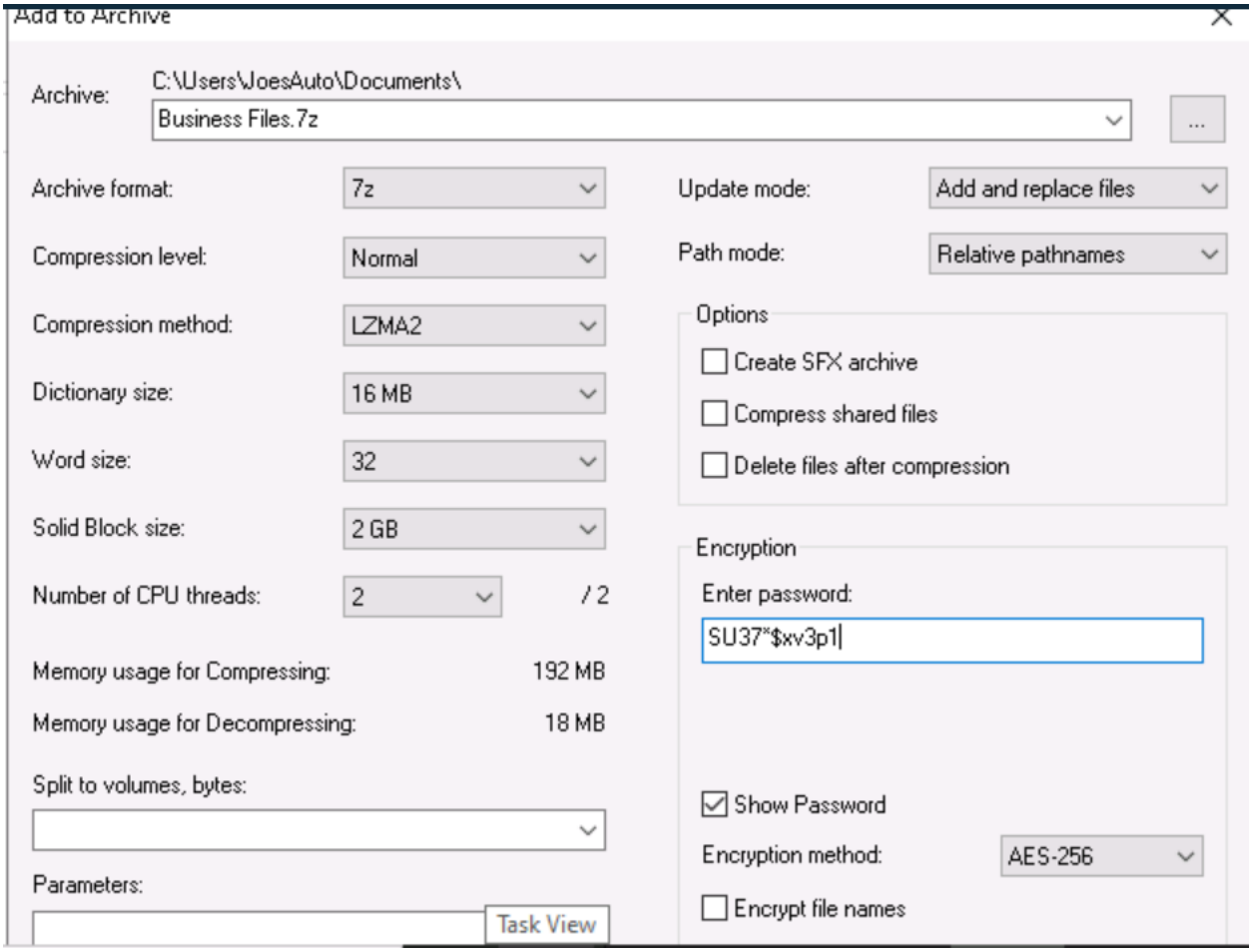
- *WE can add and remove any users/groups by clicking 'Add' and 'Remove'.*
- *We can choose permissions rights by selecting the user/group and selecting the permissions rights under 'Permissions for' section.*
- *If we try to remove a user or a group, the following error appears.*



- *We should disable inheritance of that folder first. We go back to the security tab then click 'Advanced'. Then we click 'Disable Inheritance'.*
- *Then we can remove or add any users/groups without any issues.*



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.***
    - *Archive format = 7z (ZIP is a much less secure encryption method). Encryption method = AES-256 (Advanced Encryption Standard is the strongest and most secure encryption method)*



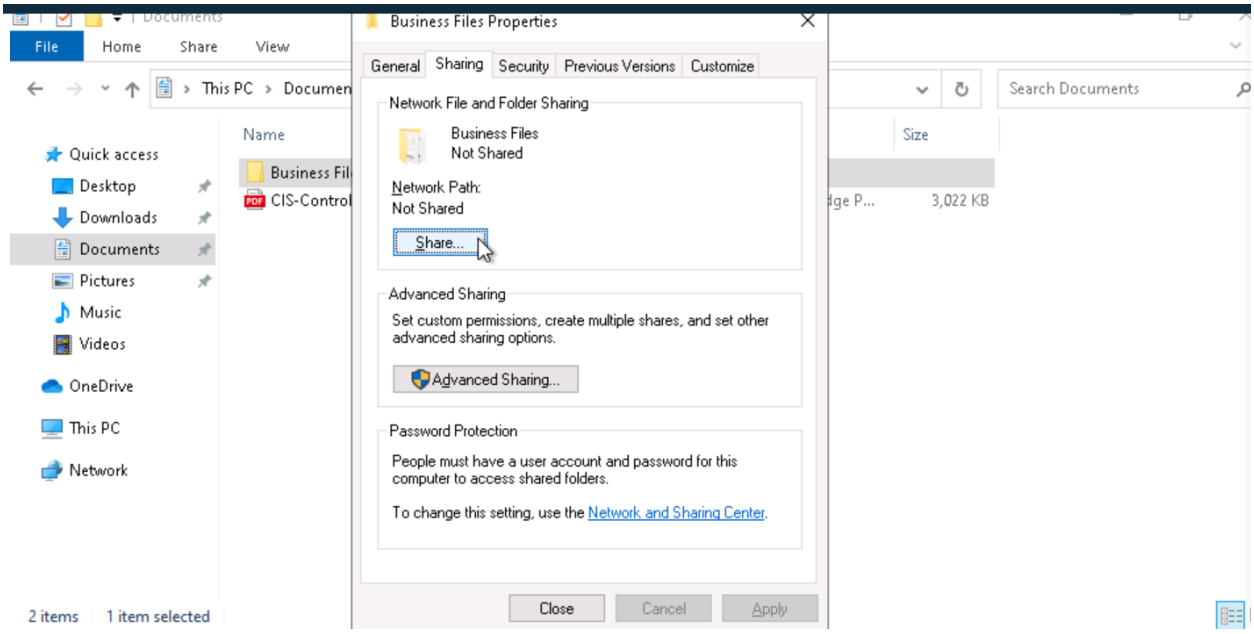
3. ***What security fundamental does this provide?***
    - *Confidentiality*

4. ***The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?***
    - Step13: Data Protection

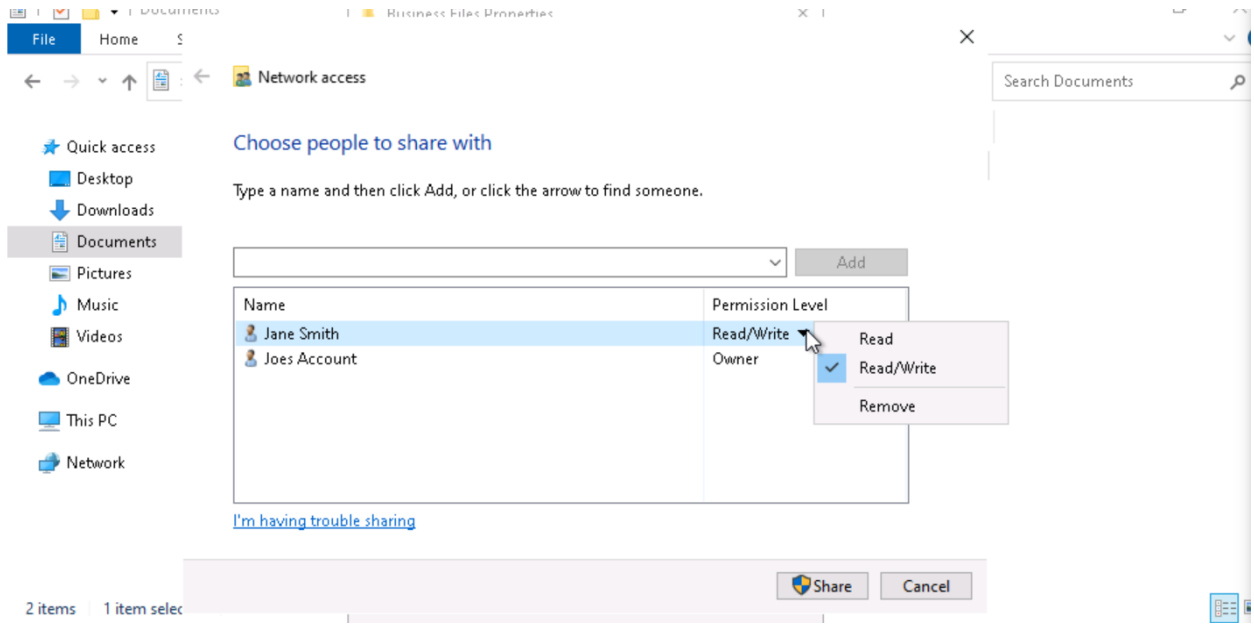
Shared Folders

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.

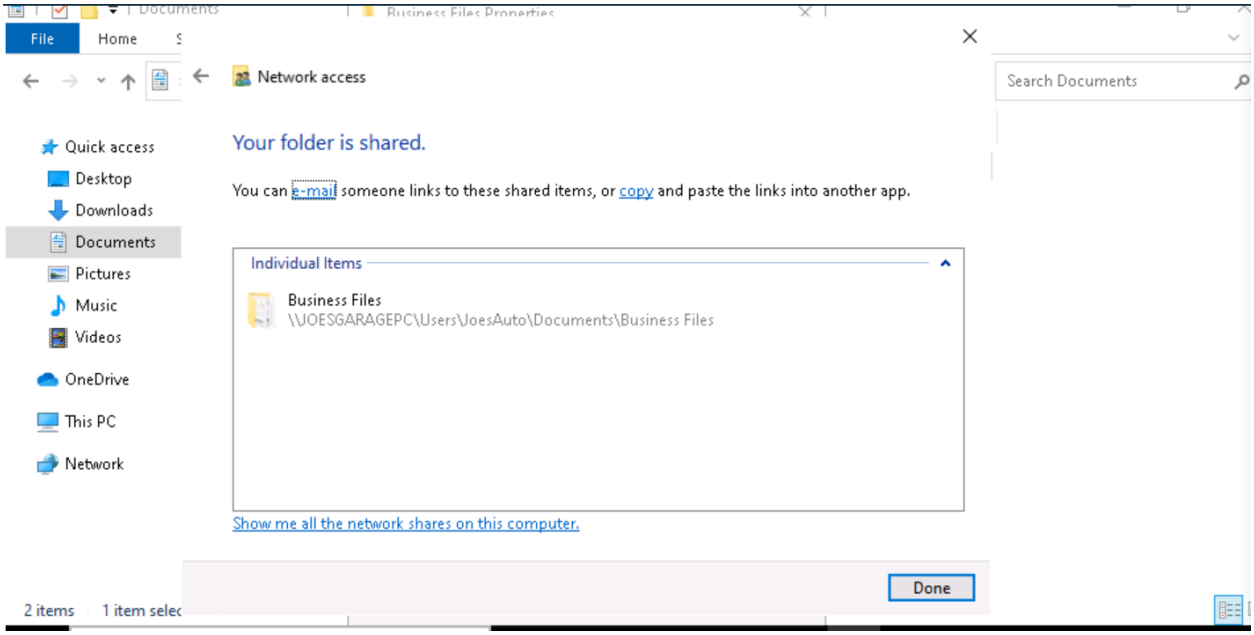
1. ***Explain how you would do that and provide a screenshot showing how you can do it. Make sure it's only shared between Joe and Jane.***
    - *Right click on the folder, then choose 'Properties'. Go to the 'Sharing' tab.*



    - *Click on 'Share'. Remove any unwanted user. Add any wanted user. Set the permission to the users with either 'Read' or 'Read/Write'.*

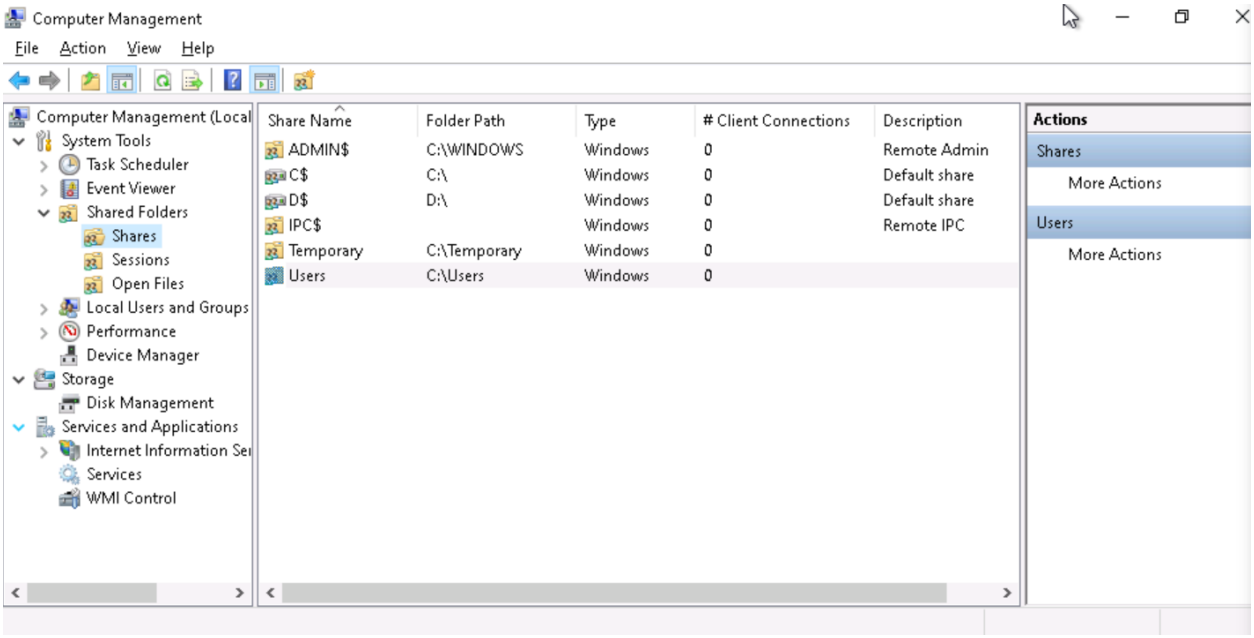


- *A confirmation windows will show with that the folder is now shared. It will display also the folder path in the network where authorized users can access the shared folder.*



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

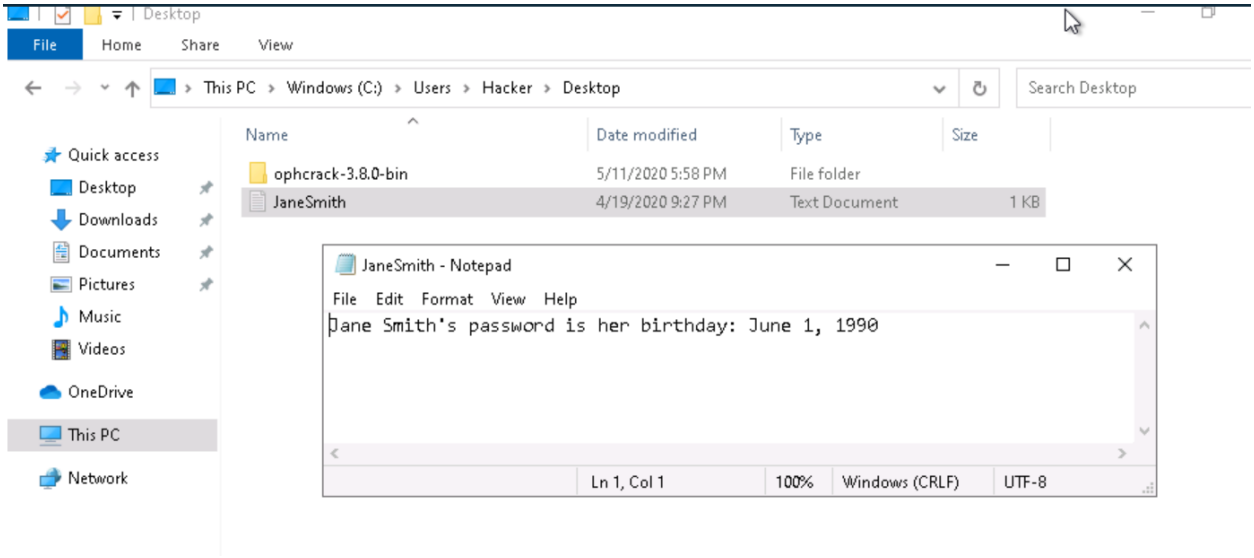
    - *Search for 'Computer Management'. Under 'Shared Folders' tab, click on 'Shares'. A list of all shared folders and files will show.*
    - *Other shared items are there too, such as C$, D$, IPC$ and ADMIN$. These are administrative (hidden) shares that Windows 10 enables by default and are not visible unless someone uses the specific path and proper credentials.*
    - *Although this method can help see all the folders currently shared on the network, note that if you share a folder inside your profile folder, it will appear as the Users folder being shared in the network.*



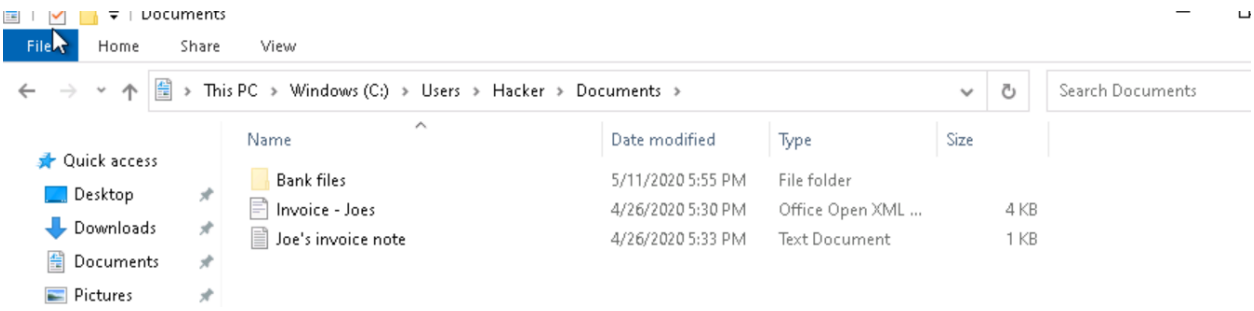
6. Basic Computer Forensics (Optional)

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]

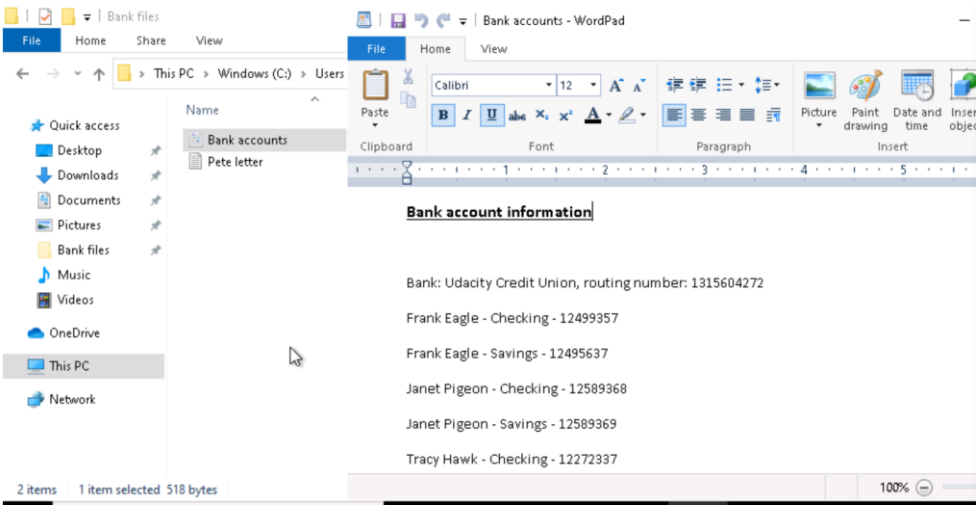
- There were two unwanted user accounts on the PC: **Frank** and **Hacker.**
- Under the user **Hacker**, there are several suspicious files.
- There is a file which contains Jane's password. Risk: it may leads to stealing data or doing suspicious actions under Jane's username.



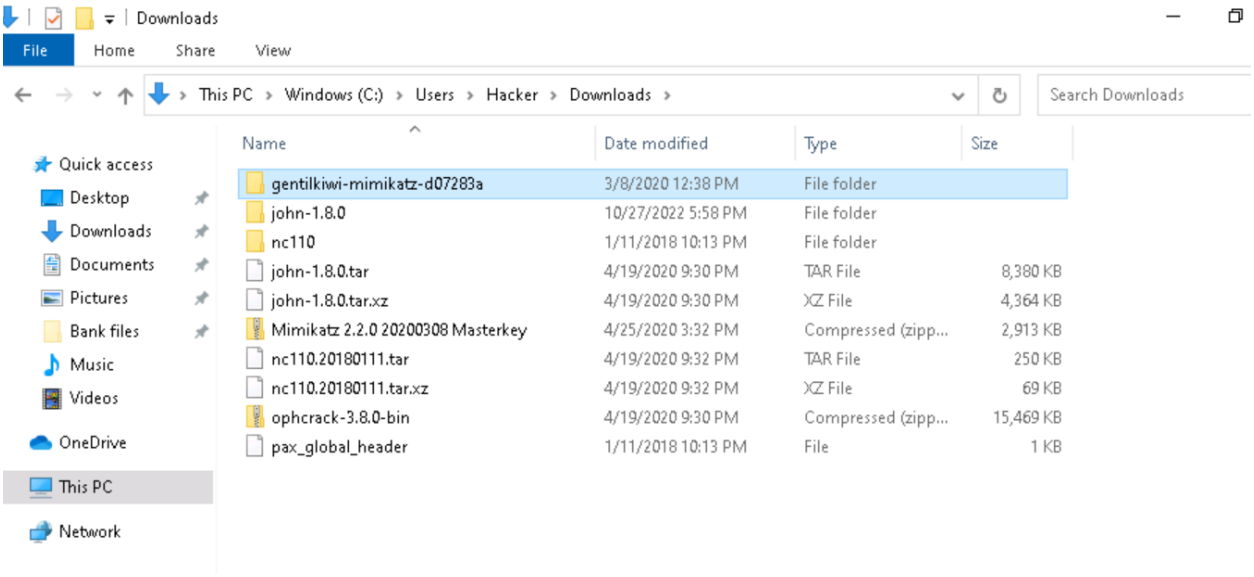
- There is also a suspicious program in the same folder "OphCrack". It is a free Windows password cracker based on rainbow tables. It is a very efficient implementation of rainbow tables done by the inventors of the method. It comes with a Graphical User Interface and runs on multiple platforms. Risk: It may lead to crack users' passwords and steal their data or do suspicious actions under their usernames.
- Fake invoice that was sent to Joe from Jane email to make him make an online payment while thinking he is doing a legitimate business transaction.



- Some of Joe's customers got their bank details stolen by the hacker:



- Under the downloads folder in the hacker user, there are several suspicious programs.
- **Mimikatz** is a leading post-exploitation tool that dumps passwords from memory. It can lead to steal passwords of other logged in users on the PC.
- **John the Ripper** is a popular open-source password cracking tool that combines several different cracking programs and runs in both brute force and dictionary attack modes. It leads also to steal users' passwords.
- **Netcat** or **NC** is a utility tool that uses TCP and UDP connections to read and write in a network. It can be used for both attacking and security. In the case of attacking. It helps us to debug the network along with investing it. It runs on all operating systems.
- **Ophcrack** is a free open-source (GPL licensed) program that cracks Windows log-in passwords by using LM hashes through rainbow tables. The program includes the ability to import the hashes from a variety of formats, including dumping directly from the SAM files of Windows.



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.