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: Hyunbyung, Park

Date of completion: 2021-07-13

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 has 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 is 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 will 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 will also need to explain how you got the answers and provide screenshots showing your work.

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

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

Account Name: JoesAuto
Password: @UdacityLearning#1

1. Reconnaissance

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

Complete each section below.

Hardware

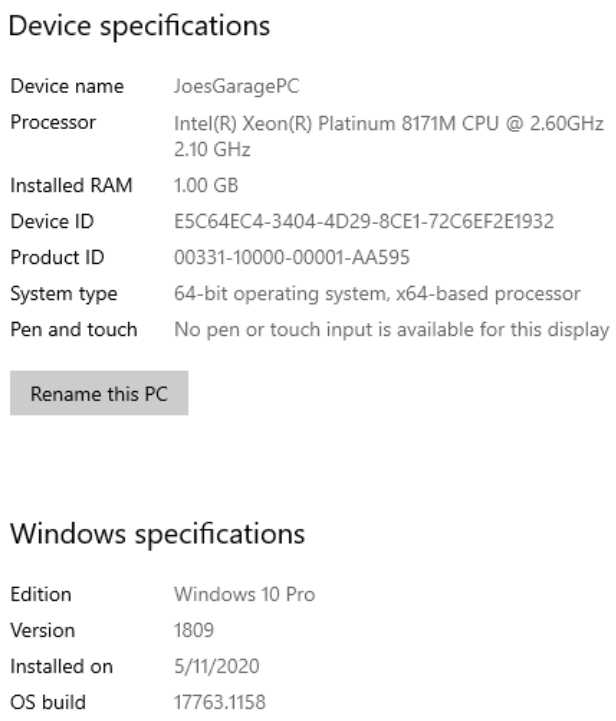
1. *Fill in the following table with system information for Joe's PC.*

Device Name	JoesGaragePC
Processor	Intel® Xeon® Platinum 8171M CPU @ 2.60GHz 2.10GHz
Install RAM	1.00GB
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:*

   After right-clicking on the Windows Start icon, select "System."

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



Software

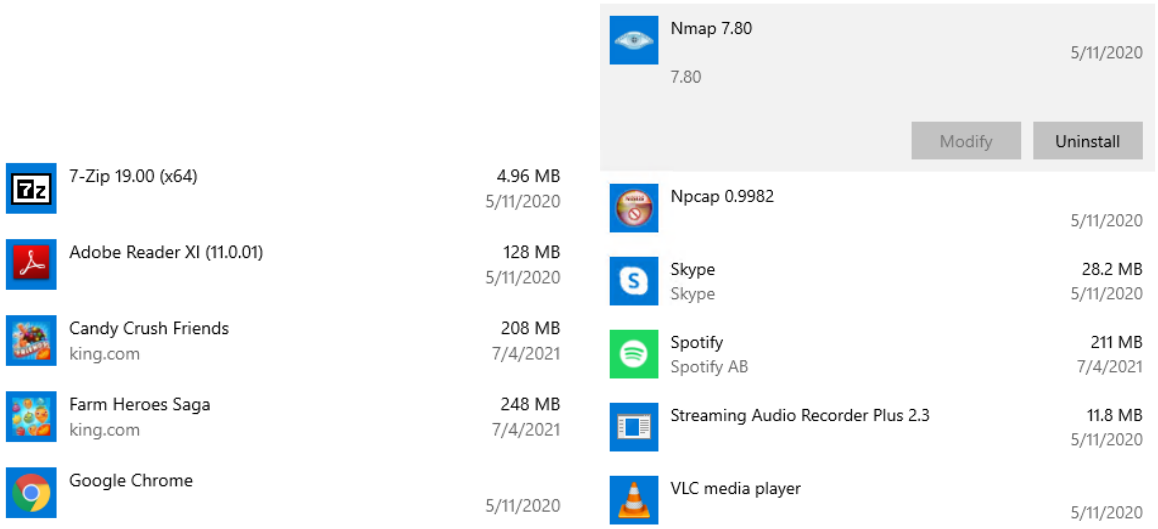
Another common early step in securing is taking an inventory of software or applications installed on a computer system. These are programs outside of the standard operating system.

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

- 7-Zip 19.00 (x64)
- Google Chrome
- Nmap 7.80
- Spotify
- VLC media player

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

   After right-clicking on the windows start icon, select "Apps and Features."



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

   Basic Controls - 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	

Frank	Frank	
Hacker	A Hacker	Administrator
JaneS	Jane Smith	
JoesAuto	Joes Account	Administrator
Notadmin	Do Not Use	

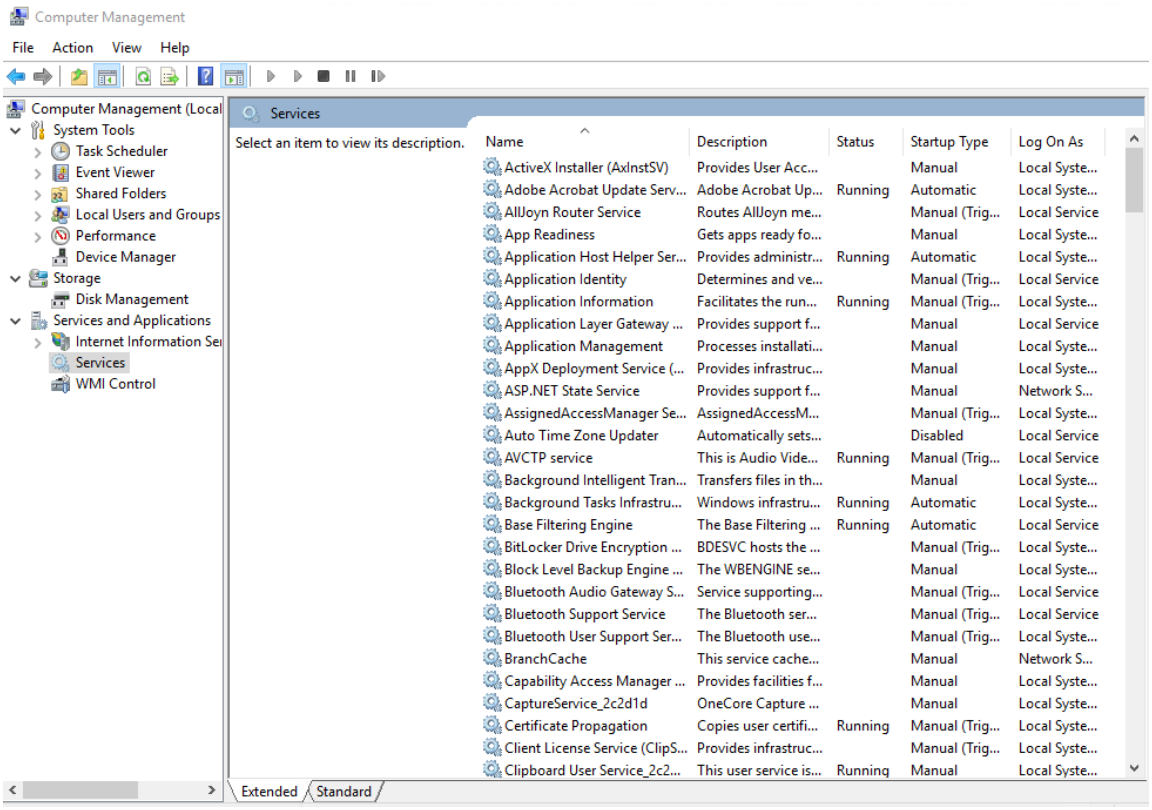
2. *Provide a screenshot of the Local Users.*

Name	Full Name	Description
AUser	A User	Account for Cyber Course 1. Not part of project
DefaultAcco...		A user account managed by the system.
Frank	Frank	Franks account
Guest		Built-in account for guest access to the computer/domain
Hacker	A Hacker	
JaneS	Jane Smith	Jane Smith - IT Mgr
JoesAuto	Joes Account	Built-in account for administering the computer/domain
Notadmin	Do Not Use	
WDAGUtility...		A user account managed and used by the system for Windows Defender Application Guard scenari...

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.

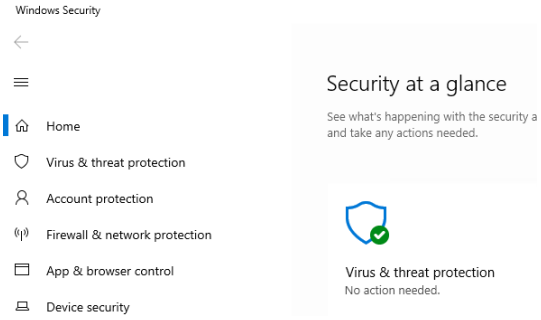
1. *Provide a screenshot of the services running on this PC.*



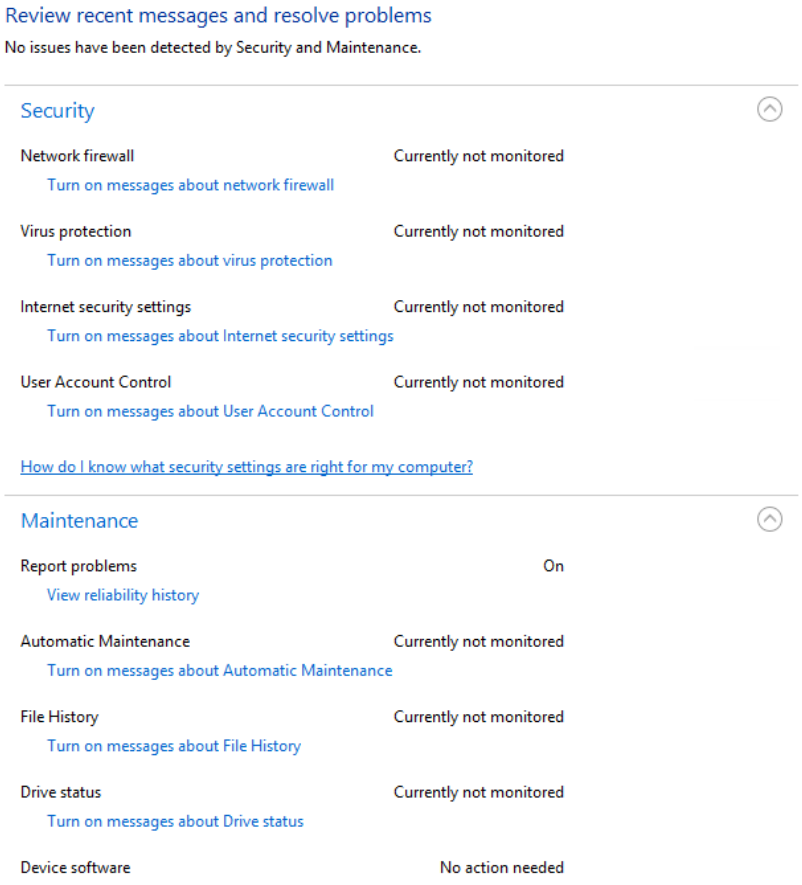
Security Services

Joe wants to ensure that standard security services are running on his PC. He is 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.**

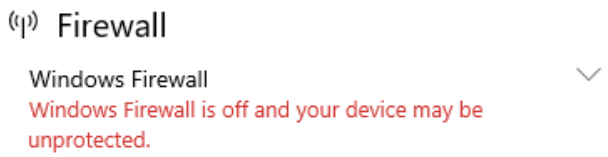
1. *To view a summary of security on Windows 10, start from the **Control Panel**. Use the "Find a setting" bar and search on Windows Defender. You can also search for Windows Defender using the Windows Run bar. Take a screenshot of what you see on the Windows Security screen and include it here:*



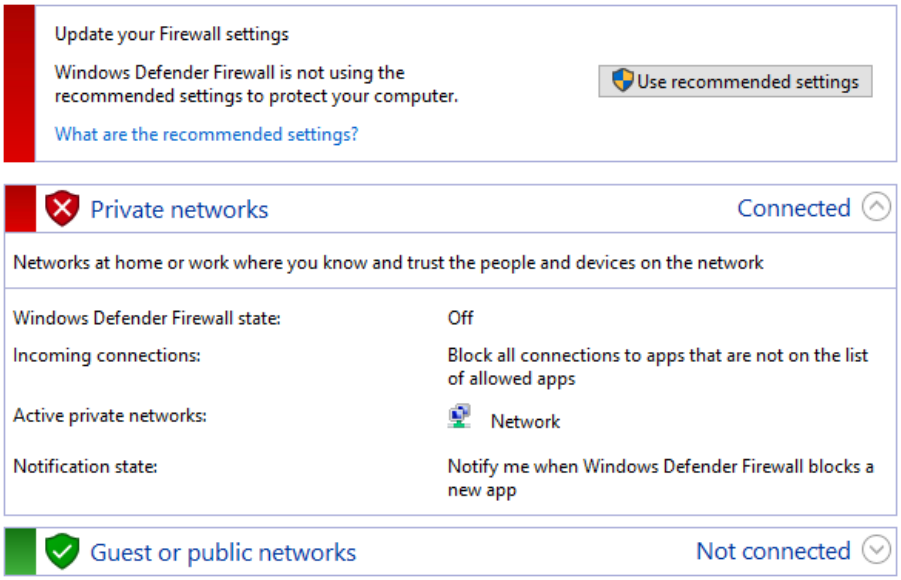
2. *The Windows 10 Security settings are also found from the **Control Panel > System and Security > Security and Maintenance**. Start by viewing **"Review your computer's status and resolve issues."** Provide a screenshot of this below:*



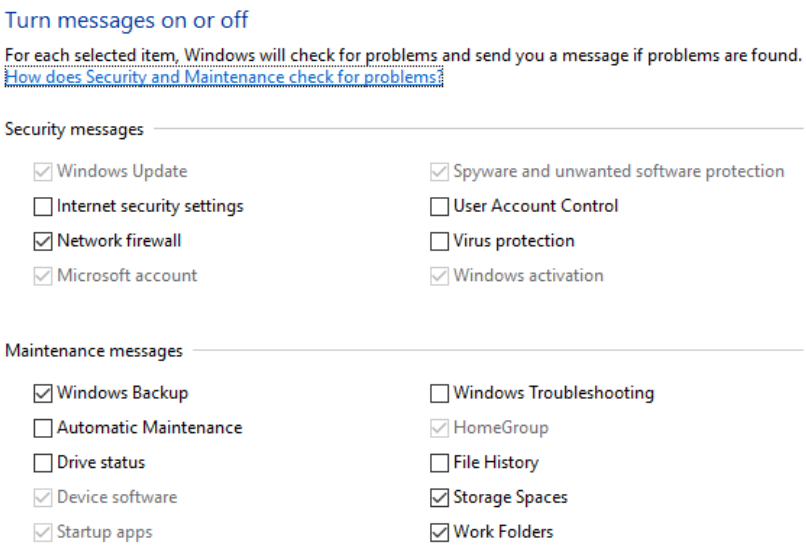
3. *Click on View in Windows Security to see the status there. Provide a screenshot of the* ***Firewall*** *settings.*



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

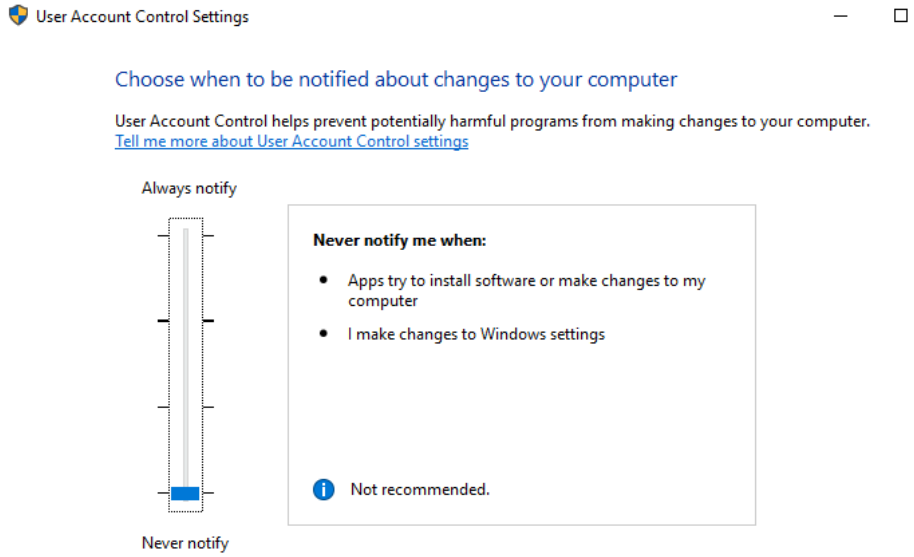


5. *PC users should be notified whenever there is a security or maintenance message. In the Security & Maintenance window, click on Change Security and Maintenance settings and take a screenshot. Paste it here:*



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).*

   I used the screenshots included on above steps.
   - Window Defender Firewall for "Firewall product and status"
   - Window Security for "Virus protection product and status"
   - Security & Maintenance window for "messages"
   - User Account Control for "User Account Control setting"



Security Feature	Status
Firewall product and status – Private network	Off
Firewall product and status – Public network	On
Virus protection product and status	Windows Defender Antivirus On
Internet Security messages	Off
Network firewall messages	On
Virus protection messages	Off
User Account Control messages	Off
User Account Control Setting	Off

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.]

- Networking Monitoring and Defense is not working so user might not notify when hacker is attacking, and private firewall is down so if someone attack with private route it will be easily penetrated.
- Network Infrastructure Management is also could be considered as failure.

- Currently virus protection message is off, so Malware Defense is not done properly. Window defender might block some virus, but user will not know it is protecting well or not.
- User Account Control Setting message is off so if someone fix this setting nobody will know. This means Account Management will not be done properly. Because even someone add administrator account nobody will know about it. Hacker might make an account secretly.
- No message about important security message means fails of Continuous Vulnerability Management.

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?*
   NIST Cybersecurity Framework (CSF)
   This standard includes five level functions for organization. Identity, Protect, Detect, Respond, Recover. It is intuitive and logical. Also, this standard helps organization to mature their level of security by Tier system. Lastly, it helps organization to profile itself by comparing the current organization profile with a target profile. So, the company can identify the are to improve the cybersecurity.
2. *What industry baseline do you recommend to Joe?*
   [Hint: Look in the documents folder]

   Center for Internet Security Controls (CIS)

   This includes the top 20 steps for organizational security with detailed guideline. It helps to secure or lockdown operating systems, software, applications, and networks. Its goal is to establish a form of a checklist of activities as organizations mature their cybersecurity programs from basic to foundation to organization. So, this is great fit for the baseline.

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?

   Synopsis of the Windows 10 security settings includes protecting the computer itself including hardware and software by notification. From endpoint to the computer inside.

CIS Controls – Basic Controls - Step 5 – Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers.

CIS Controls – Foundational Controls – Step 8 – Malware Defenses

System and Security

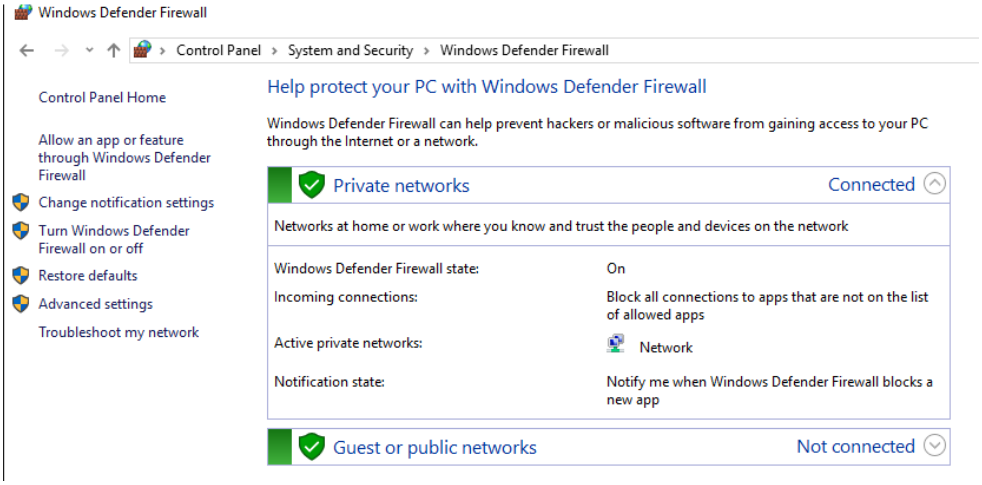
At this point, you need to enable security services for this PC. Pick at least 3 of the following 5 areas to secure in order to satisfactorily meeting the project requirements:

- 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.*
   From the control panel, go to System and Security. And select Windows defender Firewall. And Click Use recommended Settings button.
2. *Include screenshots showing the firewall is turned on.*



3. *What protection does this provide?*

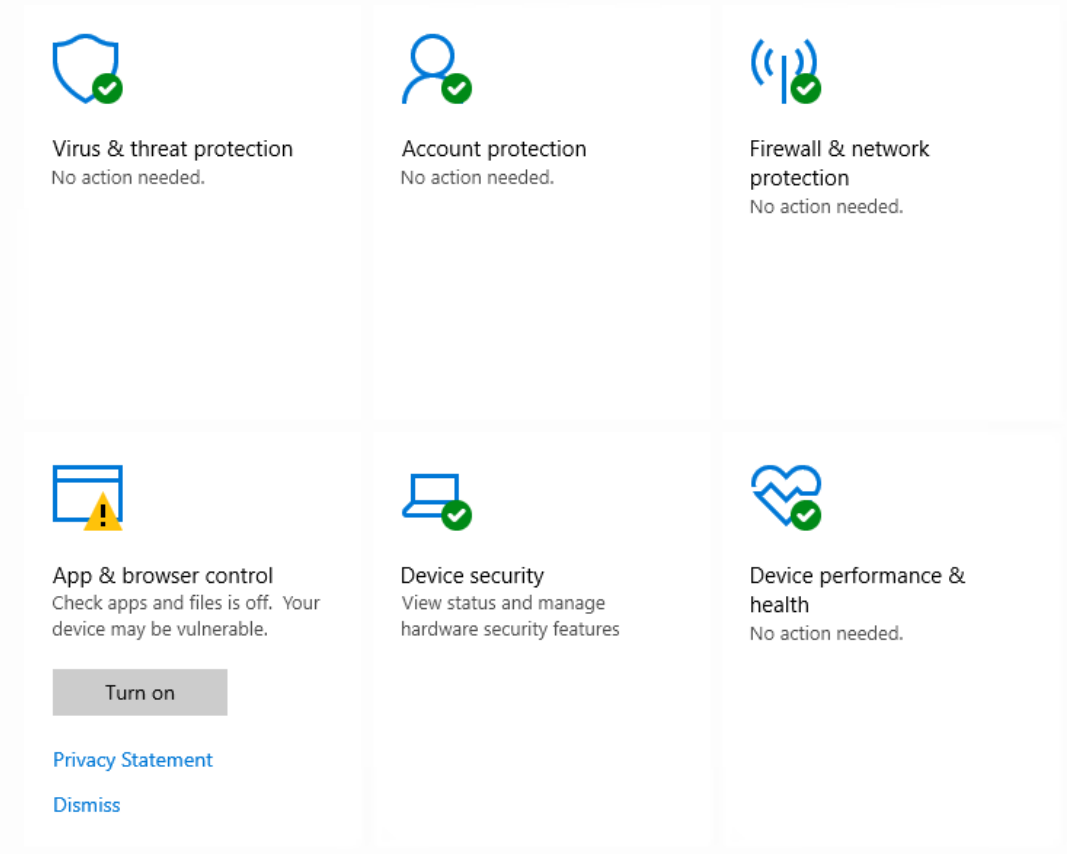
   Firewall refers to a network device which blocks certain kinds of network traffic, forming a barrier between a trusted and an untrusted network.

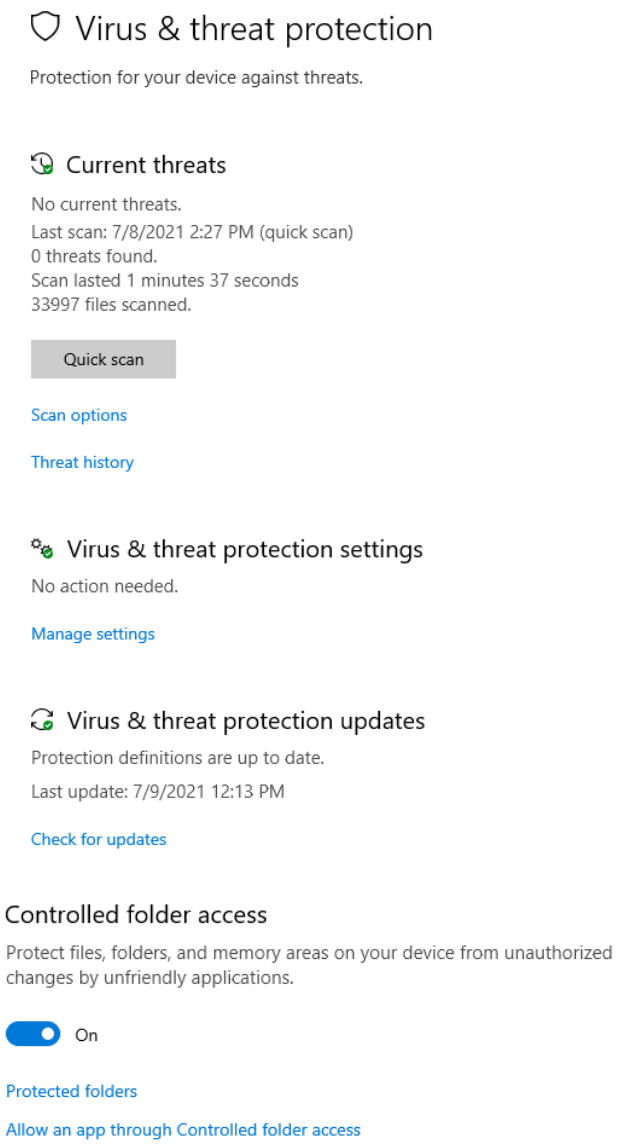
Virus & Threat Protection

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.*
   From the control panel, go to System and Security. Then click Security and Maintenance. In the window click the toggle button at Security Section. There is Virus protection. Click the View in the Windows Security. The protection was already turned on and updates were automatically done.

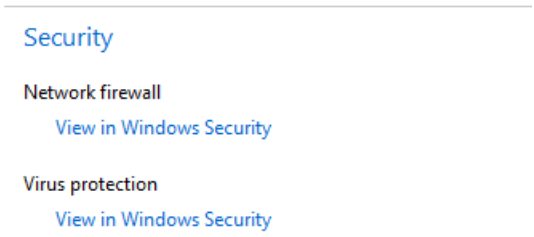
2. *Include screenshots to confirm that anti-virus is enabled.*





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:*

- Hacker secretly log in to the computer and nobody knows.
- Hacker could install all kind of malwares and virus and there is no way to block it. Worst case user might not even recognize there is such a bad program running.

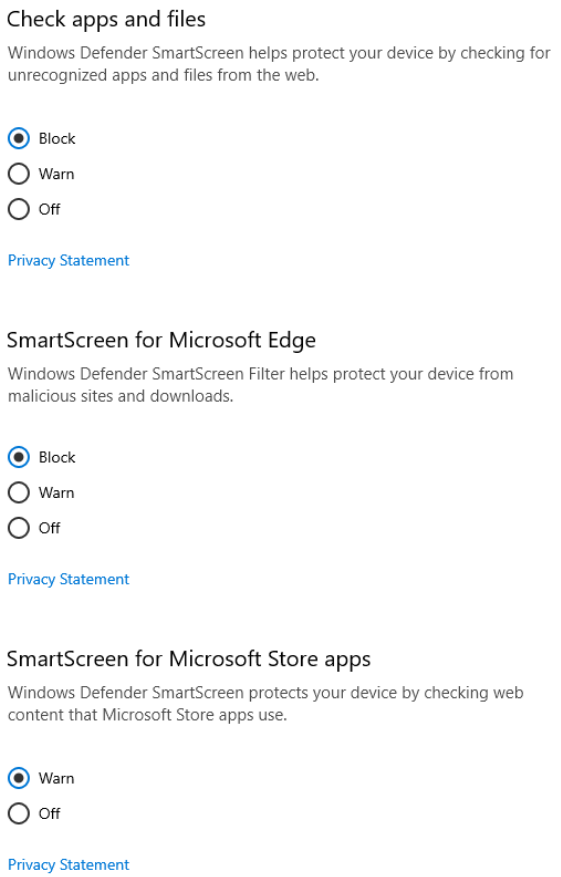
4. *From the CIS baseline controls, provide the controls satisfied by completing this.*

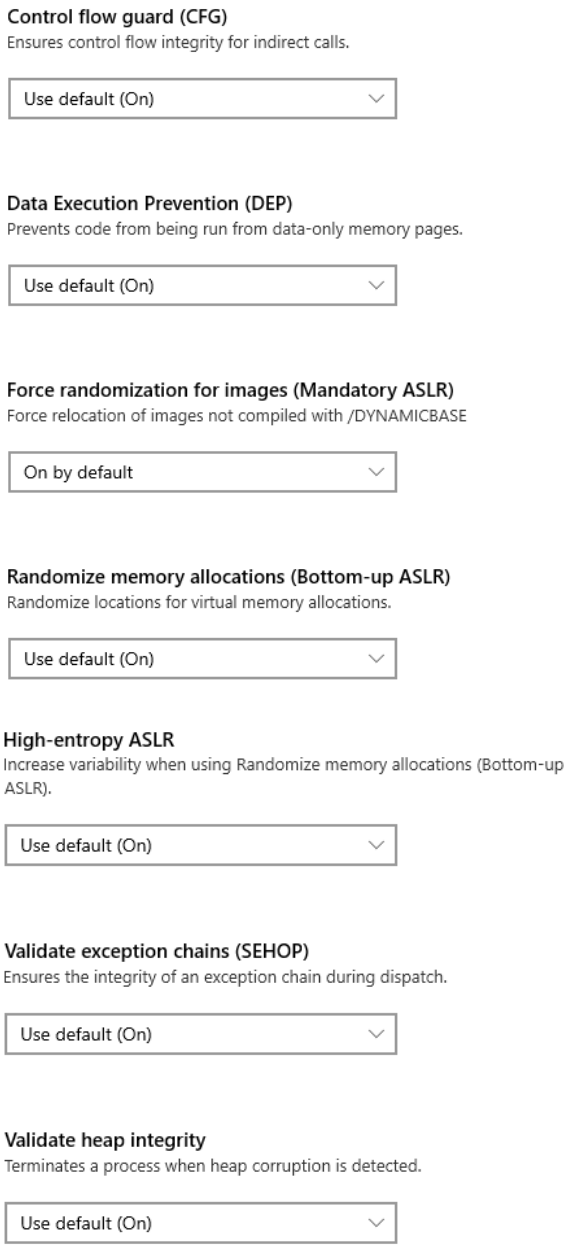
   CIS Controls – Foundational Controls – Step 3 – Data Protection
   CIS Controls – Foundational Controls – Step 13 – Network Monitoring and Defense

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

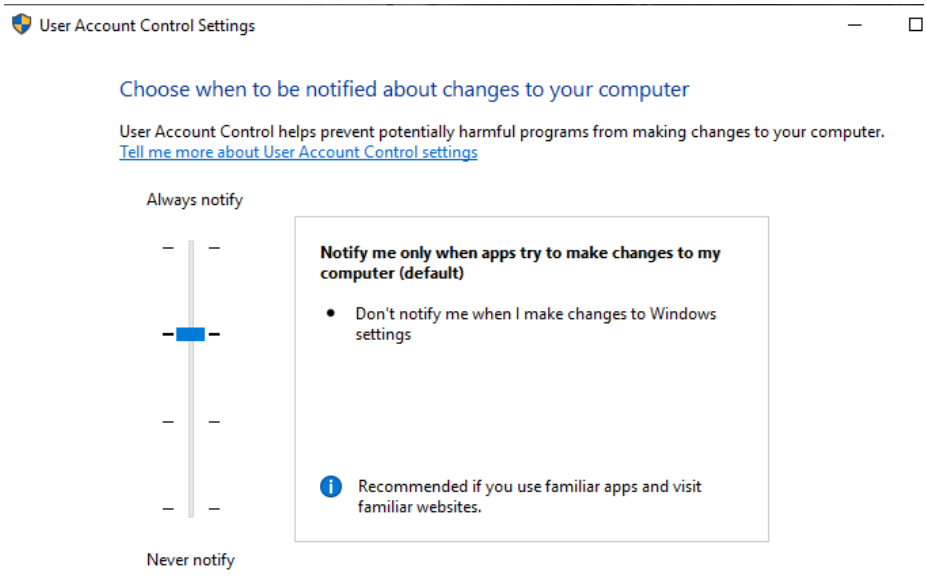
Joe wants to prevent potentially harmful programs from making changes and wants to be notified whenever apps try to make changes to his computer. This is done through the User Account Control Setting.

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

   It is set to "Never notify me no matter what"

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

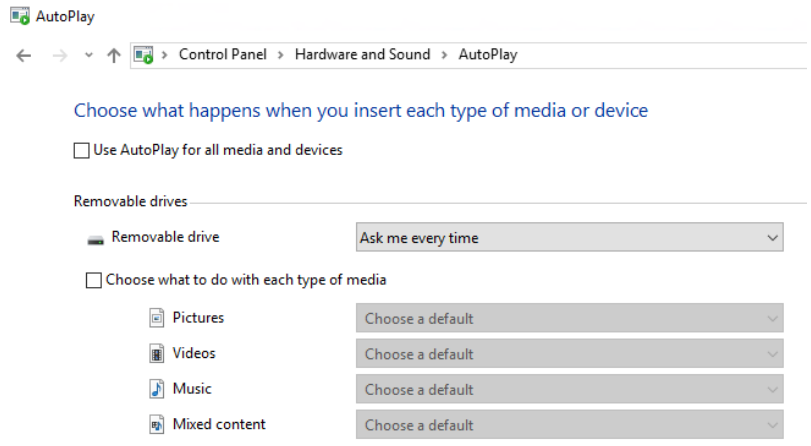
   It should be notifying! Also, it should be set by dim available so user could know when they are trying to make some changes on their desktop. This also might help to spot the malicious program working underneath and trying to harm the computer.



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 do not automatically start when the media is inserted, and the user is asked what should happen. This is set from the Control Panel > Hardware and Sound > Autoplay menu.

1. *On Joe's computer, go to that function and deselect "Use AutoPlay for all media and devices."*
2. *For the Removable Drive, make the default, "Ask me every time." Include a screenshot of your results.*



3. Securing Access

Ensuring only specific people have access on a computer system is a common step in information security. It starts by understanding who should have access and the rules or policies that need to be followed.

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

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

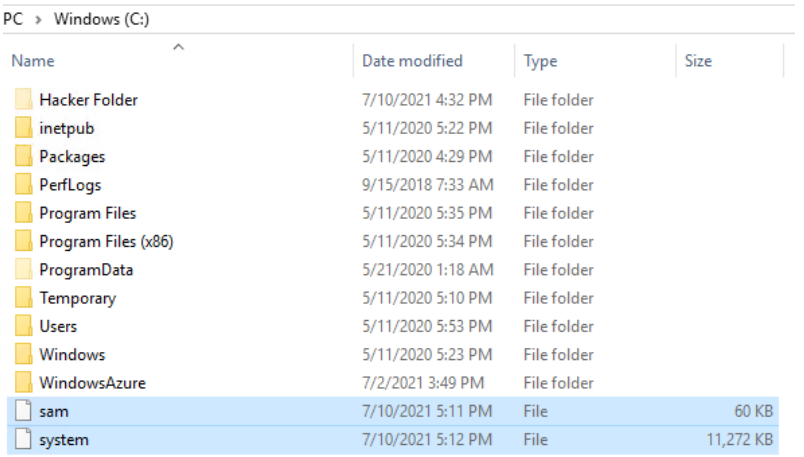
Joe's Auto Access Rules:

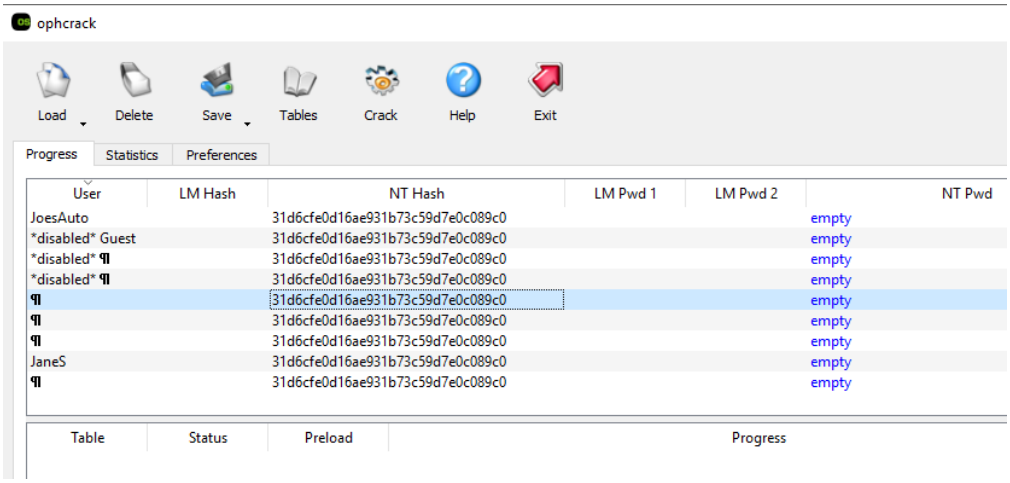
- Only JoesAuto and A User should have administrative privileges on this PC.
- Joe wants to prevent potentially harmful programs from making changes and wants to be notified whenever apps try to make changes to his computer.
- All valid users should have a password following Joe's password policy below.
    - At least 8 characters
    - Complexity enabled.
    - Changed every 120 days.
    - Cannot be the same as the previous 5 passwords.
- Account should be automatically disabled after 5 unsuccessful login attempts. The account should be locked for 15 minutes and then should automatically unlock.
- Upon first logging into the PC, Joe wants a warning banner letting anyone using to know that this is to only be used for work at Joe's Auto Body shop by authorized people.
- There is to be no remote access to this computer.

User Accounts

1. *What user accounts should not be there?*
    - *Frank*
    - *A Hacker*
2. *Bonus questions: What is Hacker's password?*

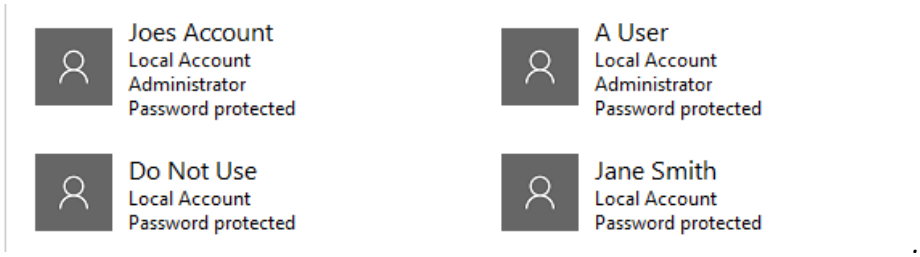
```
c:\Windows\System32>reg save hklm\sam c:\sam
The operation completed successfully.

c:\Windows\System32>reg save hklm\system c:\system
The operation completed successfully.
```





I gave up ☹

3. *Explain the steps you take to disable or remove unwanted accounts.*
   Control panel – User Account – User Account – Manage another Accounts.
   I clicked on the User I want to modify and click Delete the account.



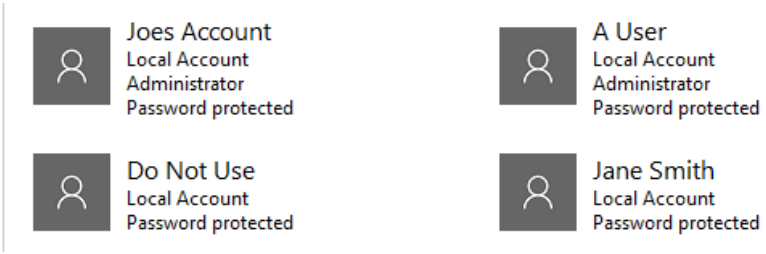
4. *Why is it important to disable or remove unneeded accounts from a PC or application? Include potential vulnerabilities and risks.*

Because the unneeded accounts could be used by hacker to harm the system. Once hacker got the administrator account then the computer is already not safe. We can experience all kind of bad events as far as hacker wants. For example, they could steel all our password and use it. Even hacker does not have administrator account the meaning they have one is that they could sneak into the vulnerabilities and attempt to do bad things. It is like gave them a chance to try such a thing.

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 should not?
   A Hacker which is removed now, and Jane Smith.
6. Explain how you determined this. Provide screenshots as needed.

   Control panel – User Account – User Account – Manage another Accounts.
   We can check who is Administrator and who is not easily. I already modify all the settings, so the screenshot shows after fixed.



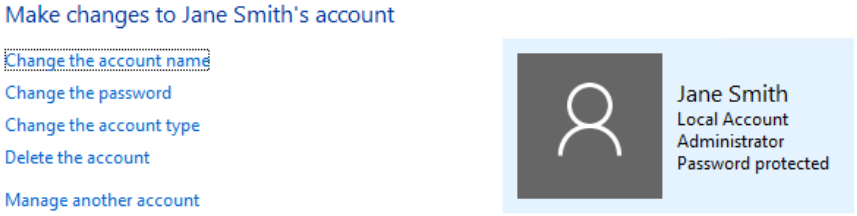
Administrator privileges for too many users are another security challenge.

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

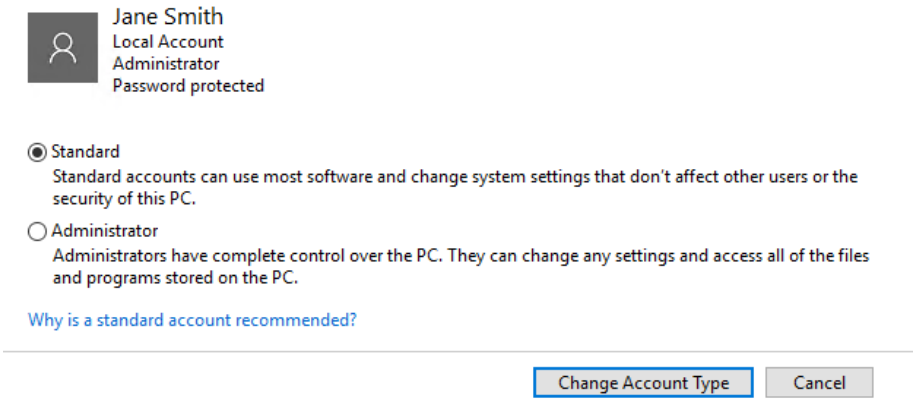
- User could install program that has virus inside
- User could accidently delete all the accounts and all the important files.
- User could modify important files for window system without knowing what they are doing.

Now you need to remove administrator privileges for any user(s) that should have it.

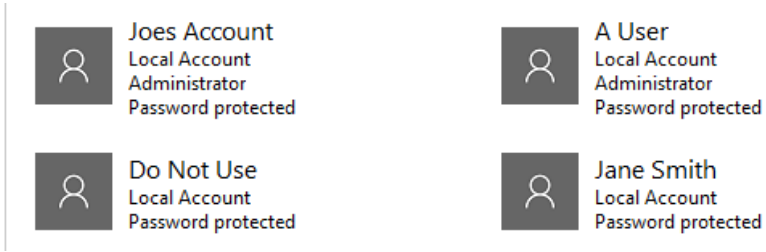
8. *Explain the process for doing this. Include screenshots to show your work.*
   Control panel – User Account – User Account – Manage another Accounts.
   Click the user I want to modify and click "Change the account type".



After that click Standard radio button and click "Change Account Type"



Done!



9. What is the security principle behind this?

   It is Least Privilege.

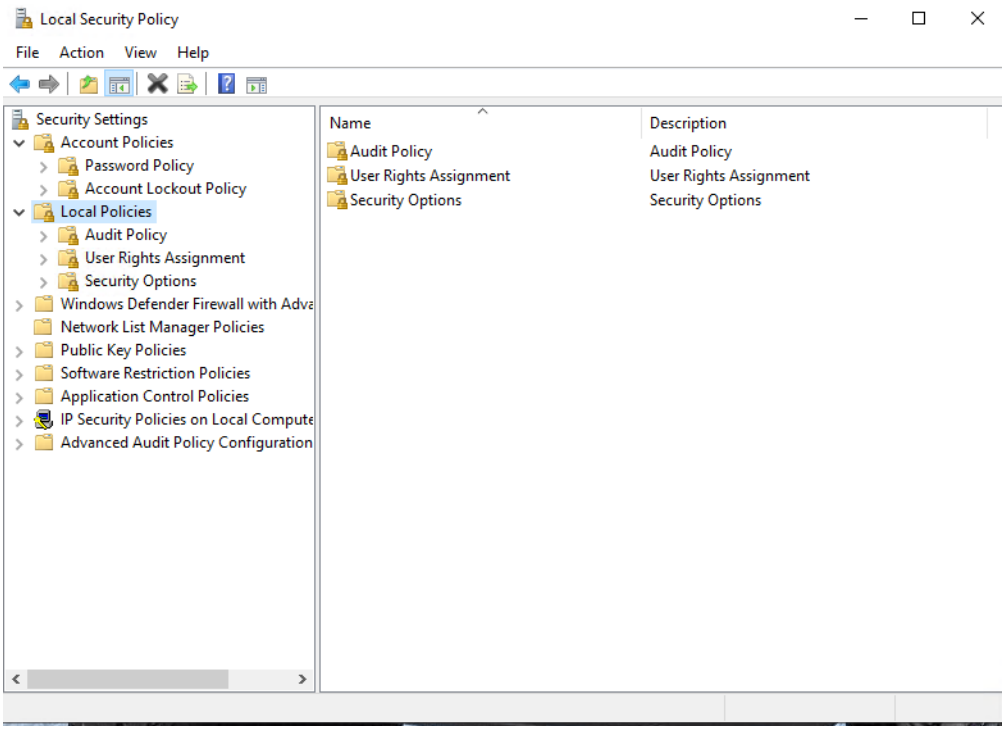
10. The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?

    CIS Controls – Basic Controls - Step 4 – Controlled Use of Administrative Privileges

Setting Access and Authentication Policies

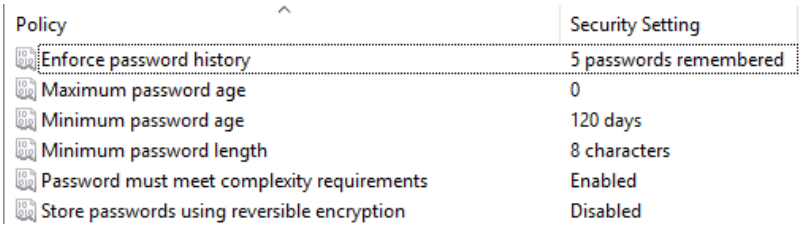
After you talked with Joe about security, he has asked that the access rules outlined above be in place on his PC. These are set using the Local Security Policy function in Windows 10. On the Windows search bar, type "*Local Security Policy*" to access it. Click the > arrow next to both "*Account Policies*"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



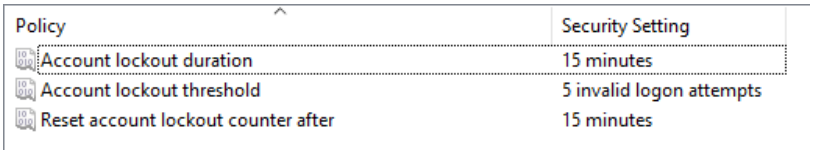
2. Explain the process for setting the password and access control policies locally on a Windows 10 PC. Provide screenshots showing how you set the rules on the PC.

- Setting the Password Policy:
  Go to Account policies – Password Policy.
  1. Minimum password length: 8 characters
  2. Password must meet complexity requirements: Enabled
  3. Minimum password age: 120 days
  4. Enforce password history: 5 passwords remembered.



- Setting the Account Lockout Policy:

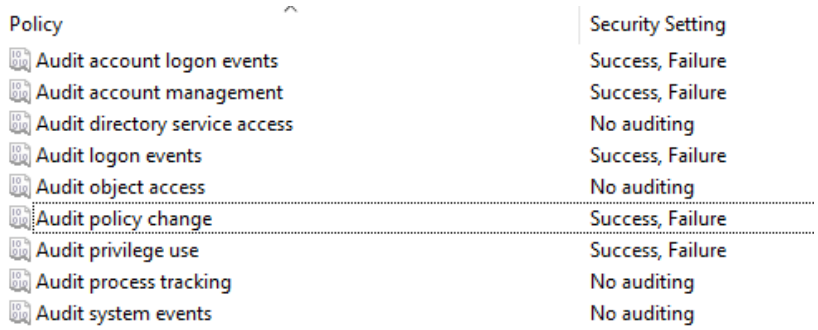
  5. Account lockout threshold: 5 invalid logon attempts
  6. Account lockout duration: 15 minutes
  7. Reset account lockout counter after 15 minutes



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.



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	No auditing

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.*

- *ophcrack*
- *Nmap*
- *Candy Crush Friends*

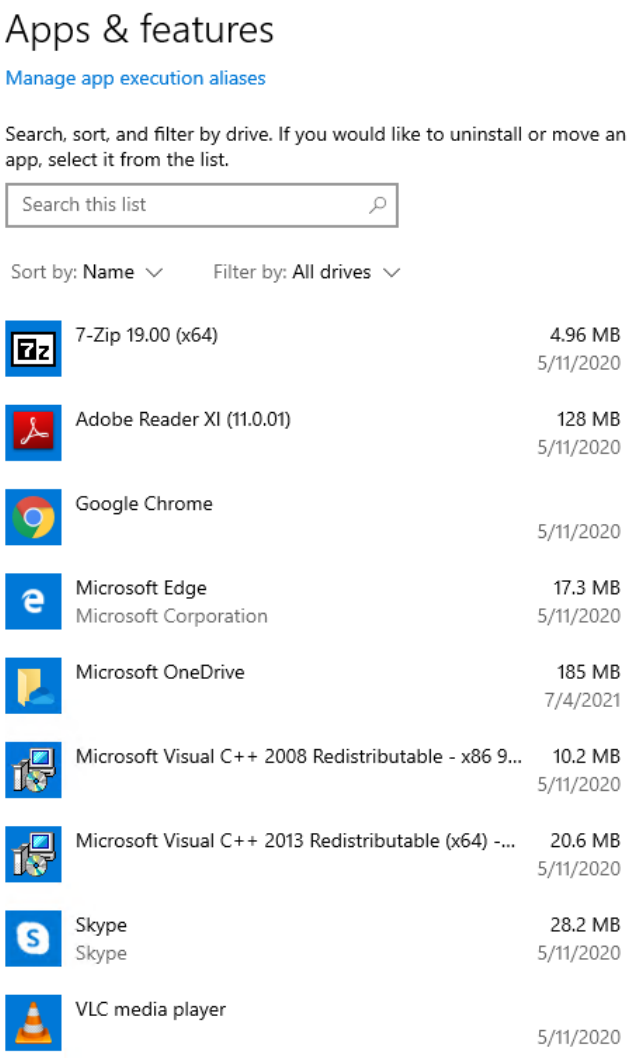
2. *Name at least three vulnerabilities, threats, or risks with having unnecessary applications:*

- *The application might be a hacking tool* used *by hacker to break the system down.*
- *The application itself might have vulnerabilities that allow hacker to break in the system.*
- *The application is disguising as normal but malware.*

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.*
After right-clicking on the Windows Start icon, select "App and Features". Click the App that I want to remove and click Uninstall button.

Removed App

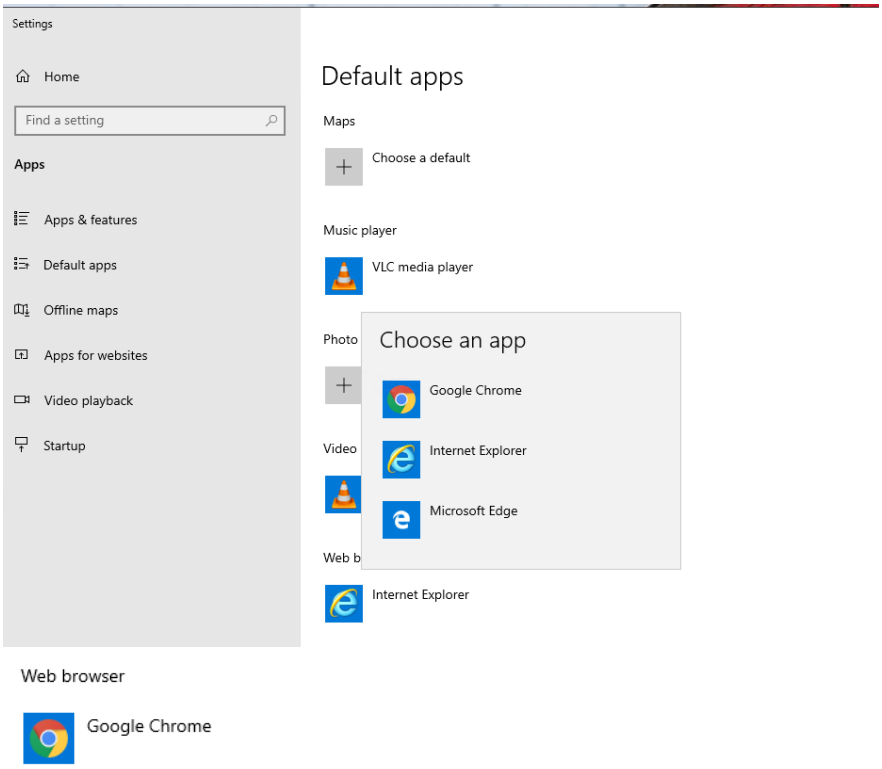
- *Candy Crush Friends*
- *Farm Heroes Saga*
- *Ophcrack*
- *Npcap*
- *Nmap*
- *Spotify*
- *MusicBee*
- *Streaming Audio Recorder Plus*
- *VNC Server*
- *VNC Viewer*



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.*
   Window Start menu – Settings – Apps – Default apps
   We can set what application to use by clicking the respecting section (Maps, Music player, etc.)

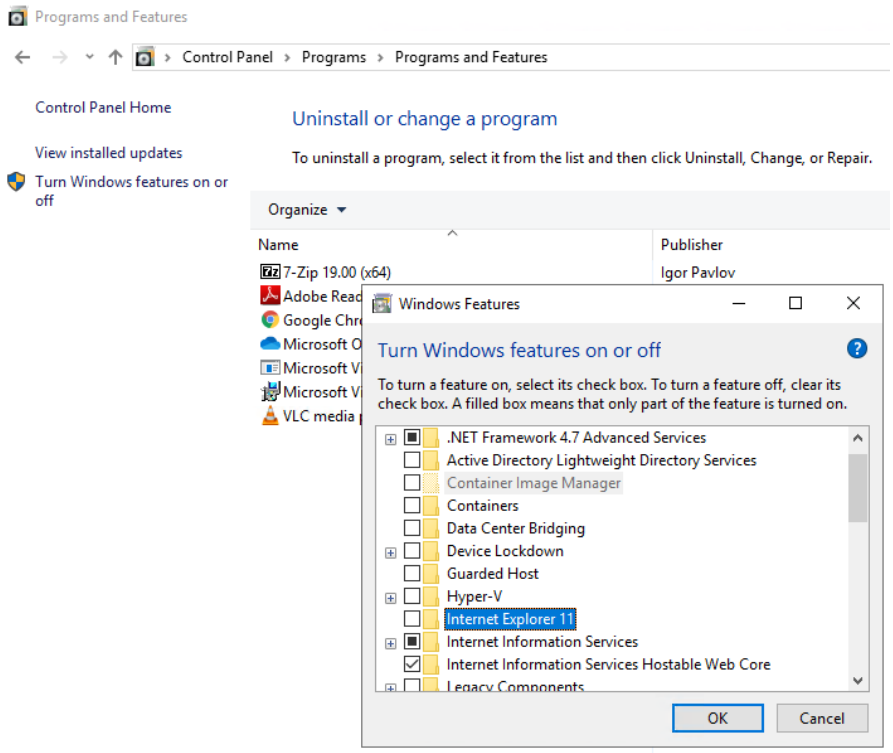


2. *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
   - **Internet Explorer Memory Corruption Vulnerability**
     It could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.
   - **Internet Explorer Remote Code Execution Vulnerability**
     A remote code execution (RCE) bug resides in the scripting engine's library jscript9.dll, which is used by default by all versions of Internet Explorer since IE9. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website.

     The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. They could embed an ActiveX control marked "safe for initialization" in an application of Microsoft office documentation that hosts the IE rendering engine.

Because of the reasons you give above, Internet Explorer should be removed. To do that, go to the **Control Panel**, select **Programs**. On the **Programs and Features** window, select "**Turn Windows features on or off**."

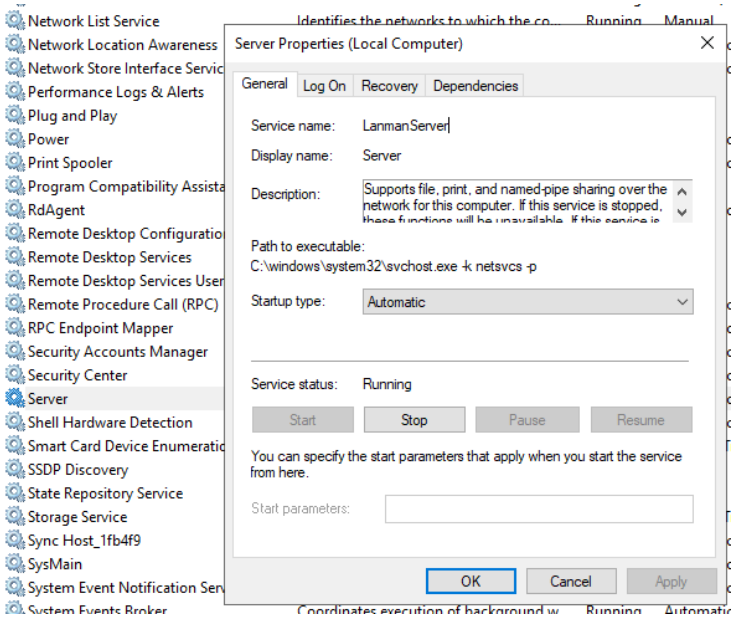
3. *Provide a screenshot showing Internet Explorer 11 is off.*

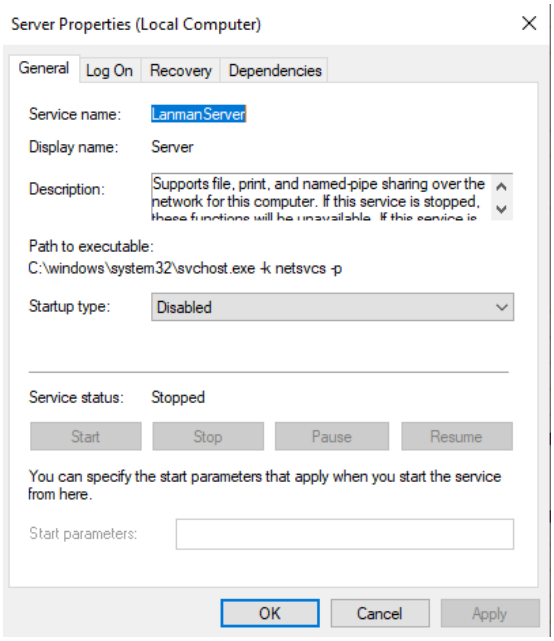


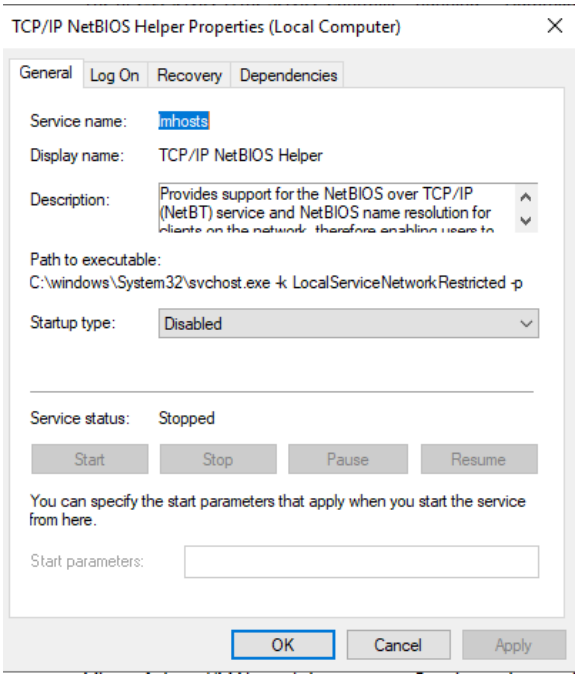
Windows Services

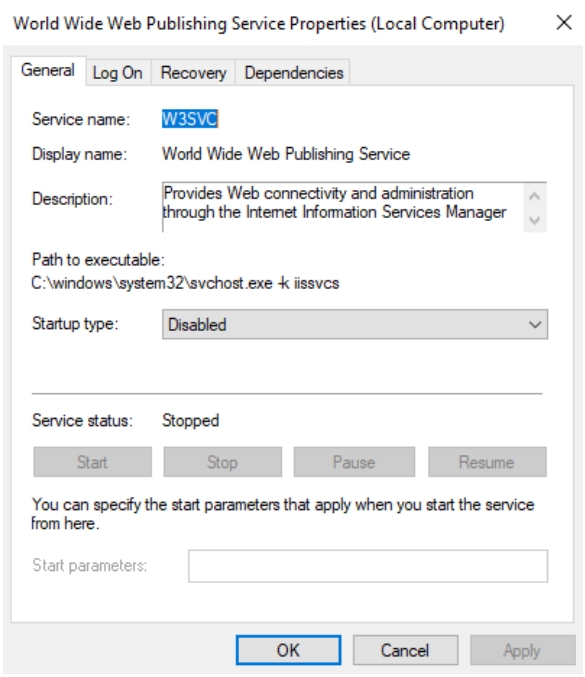
There are Windows features running on Joe's computer that could allow unwanted activity or files. He suspects that someone may have used the PC as a web server in the past. Joe wants you to confirm if web services are turned on, stop it if it is and make sure it is not running whenever the computer restarts.

1. How did you determine these services were running? Include screenshots to show how you found them.
   In the computer management window, click on the > symbol next to "Services and Applications". Select "Services" to see the services available on this PC.
   Look through the Name and Description of services and find which one is related to server.


Network List Service
Network Location Awareness
Network Store Interface Servic
Performance Logs & Alerts
Plug and Play
Power
Print Spooler
Program Compatibility Assista
RdAgent
Remote Desktop Configuratio
Remote Desktop Services
Remote Desktop Services User
Remote Procedure Call (RPC)
RPC Endpoint Mapper
Security Accounts Manager
Security Center
Server
Shell Hardware Detection
Smart Card Device Enumeratic
SSDP Discovery
State Repository Service
Storage Service
Sync Host_1fb4f9
SysMain
System Event Notification Ser
Server Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name: LanmanServer
Display name: Server
Description: Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped,
Path to executable:
C:\windows\system32\svchost.exe -k netsvcs -p
Startup type: Automatic
Service status: Running
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply


Server Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name: LanmanServer
Display name: Server
Description: Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped,
Path to executable:
C:\windows\system32\svchost.exe -k netsvcs -p
Startup type: Disabled
Service status: Stopped
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply

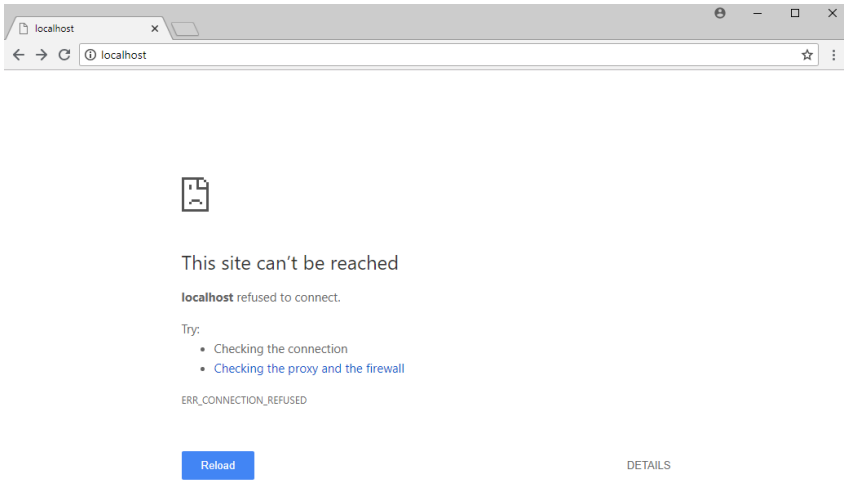




I found 3 services that are related to web server.

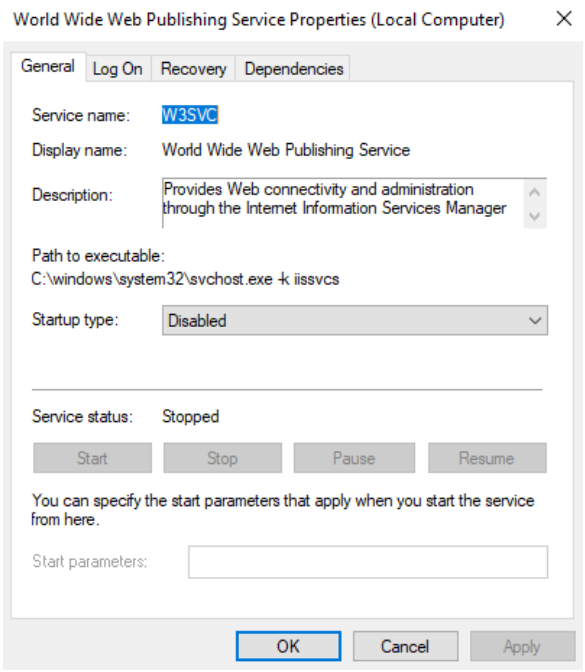
- Server
- TCP/IP NetBIOS Helper Properties
- World Wide Web Publishing Service Properties

2. Advanced users should provide at least two methods for determining a web server is running on a host.
    - Type http://localhost/ and check it works.
    - Use Nmap and type NMAP -p80 <IP address>

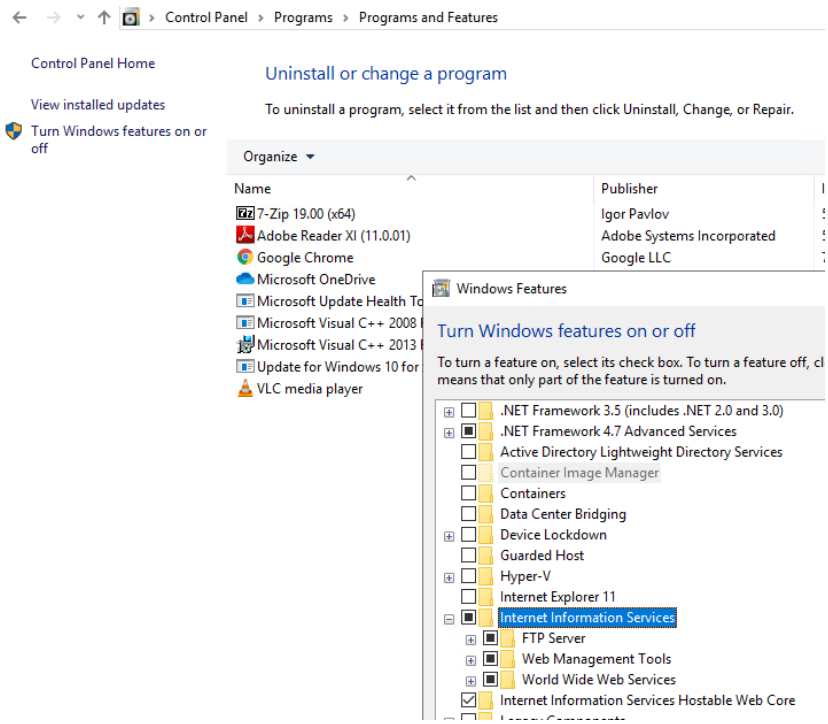


3. How do you disable them and make sure they are not restarted?
   Click on the service that we want to modify.
   - Click Stop button
   - Set the Startup type to Disabled.

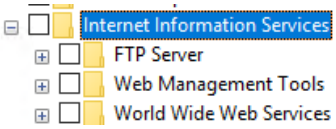
4. Advanced Users: The File Transfer Protocol FTP service is also running on this PC and should not. Explain the process for disabling it and ensuring it is not automatically restarted.



Stop and set startup type disabled of Word Wide Web Publishing Service Properties!



Go to Control Panel > Programs > Programs and Features.
And click “Turn Windows feature on or off”.
Find Internet Information Services and Turn it off!



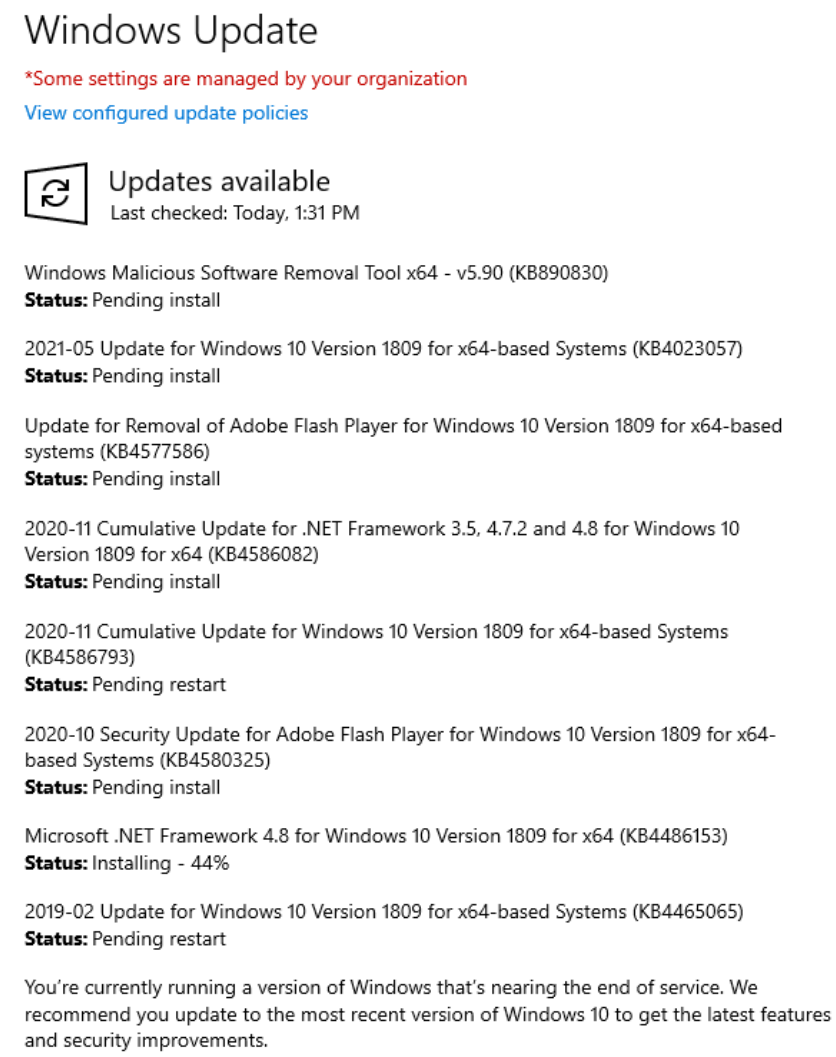
Now FTP is stopped. To check this open Internet Information Services (IIS) Manager

Click > symbol of JOESGARAGEPC – Sites – Default Web Site. When we hover our mouse pointer over “Default Web Site” we can check it is stopped!

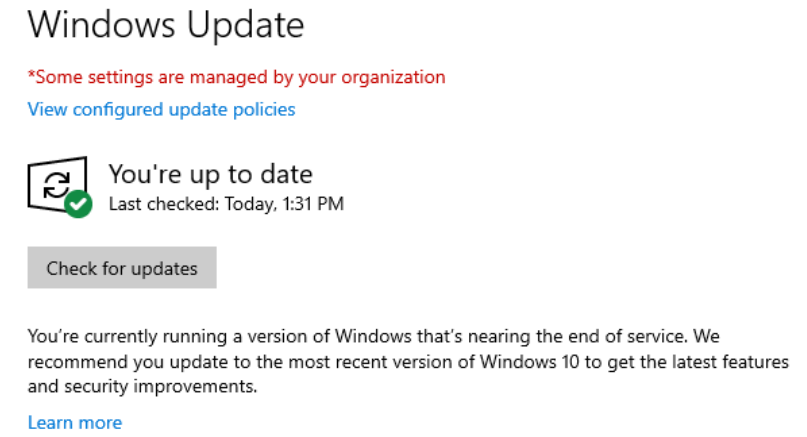
Patching and Updates

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.

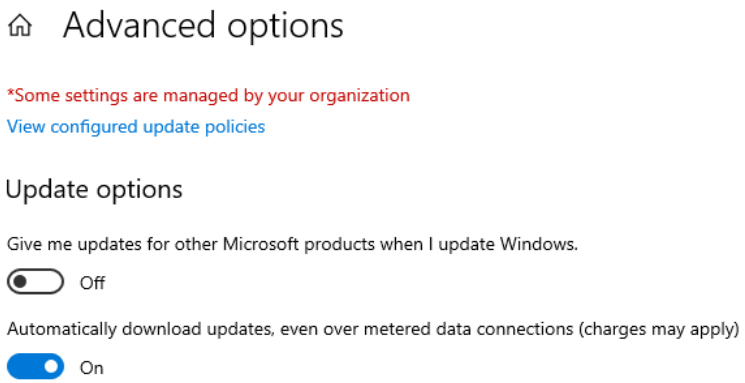
1. *Explain the process for doing this. Include screenshots as needed.*
   Search for “Windows Update settings” and click download. It will automatically install the required updates. This takes a while so need patient.



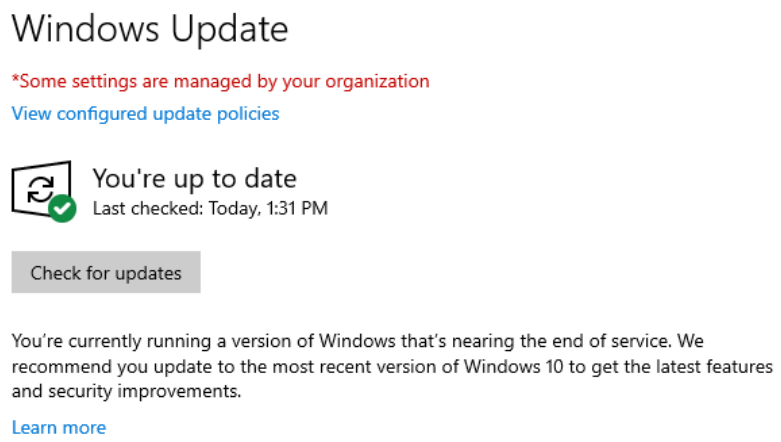
Restart your computer!



Go to Advanced options and turn the automatic download to update window!



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.*

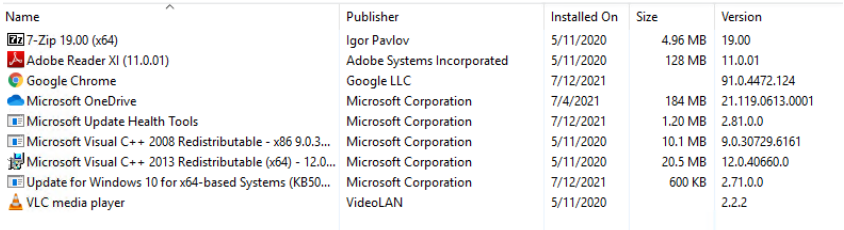


All applications should also be up to date on patches or fixes provided by the manufacturer. Any old versions of software should be uninstalled.

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

- VLC media player
- Adobe Reader XI

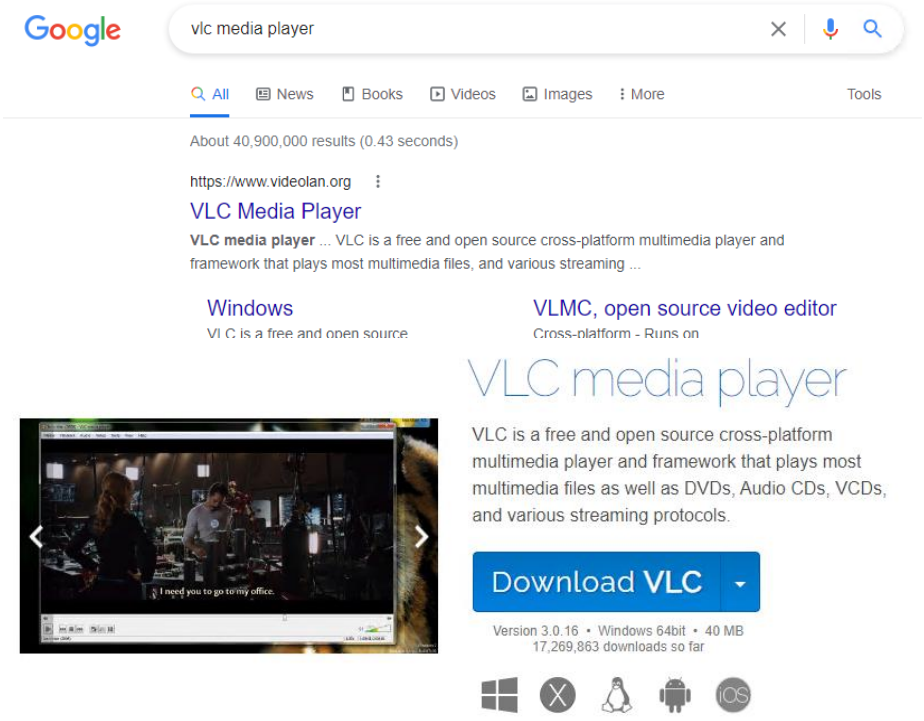
4. *Explain the steps you took to determine this information.*
   Go to Control Panel > Programs > Programs and Features.
   Check the Installed date and search internet for the recent version and check is it up-to-date or out-of-date.



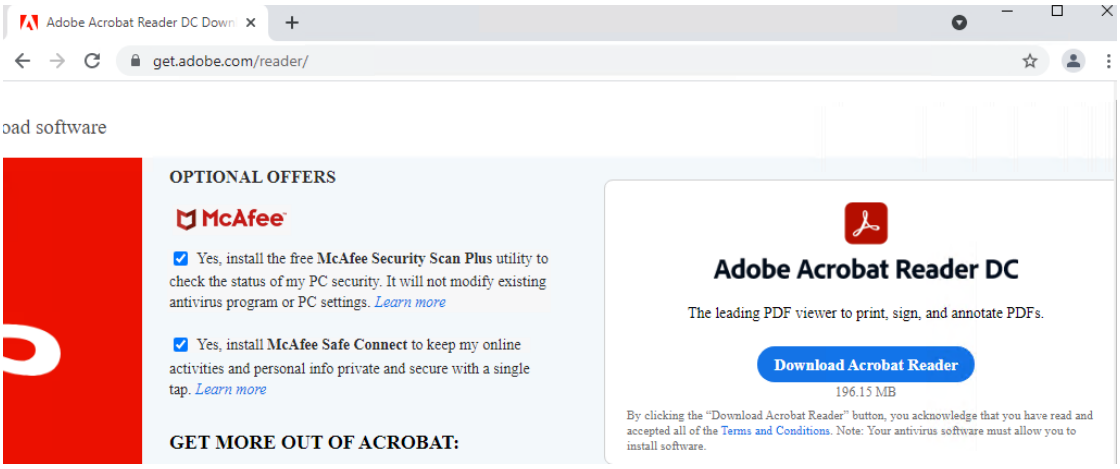
Name	Publisher	Installed On	Size	Version
7-Zip 19.00 (x64)	Igor Pavlov	5/11/2020	4.96 MB	19.00
Adobe Reader XI (11.0.01)	Adobe Systems Incorporated	5/11/2020	128 MB	11.0.01
Google Chrome	Google LLC	7/12/2021		91.0.4472.124
Microsoft OneDrive	Microsoft Corporation	7/4/2021	184 MB	21.119.0613.0001
Microsoft Update Health Tools	Microsoft Corporation	7/12/2021	1.20 MB	2.81.0.0
Microsoft Visual C++ 2008 Redistributable - x86 9.0.3...	Microsoft Corporation	5/11/2020	10.1 MB	9.0.30729.6161
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0...	Microsoft Corporation	5/11/2020	20.5 MB	12.0.40660.0
Update for Windows 10 for x64-based Systems (KB50...	Microsoft Corporation	7/12/2021	600 KB	2.71.0.0
VLC media player	VideoLAN	5/11/2020		2.2.2

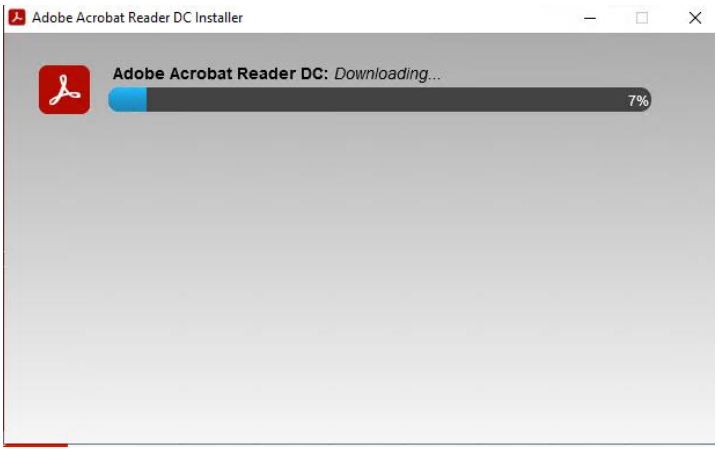
5. *Explain the steps for updating each of these applications. Include screenshots as needed.*

Google it!



Download and install!





Name	Publisher	Installed On	Size	Version
7-Zip 19.00 (x64)	Igor Pavlov	5/11/2020	4.96 MB	19.00
Adobe Acrobat Reader DC	Adobe Systems Incorporated	7/12/2021	349 MB	21.005.20048
Google Chrome	Google LLC	7/12/2021		91.0.4472.124
Microsoft OneDrive	Microsoft Corporation	7/4/2021	184 MB	21.119.0613.0001
Microsoft Update Health Tools	Microsoft Corporation	7/12/2021	1.20 MB	2.81.0.0
Microsoft Visual C++ 2008 Redistributable - x86 9.0.3...	Microsoft Corporation	5/11/2020	10.1 MB	9.0.30729.6161
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0...	Microsoft Corporation	5/11/2020	20.5 MB	12.0.40660.0
Update for Windows 10 for x64-based Systems (KB50...	Microsoft Corporation	7/12/2021	600 KB	2.71.0.0
VLC media player	VideoLAN	7/12/2021		3.0.16

The Application is now Up to date!

- Adobe Acrobat Reader DC
- VLC media player

5. Securing Files and Folders

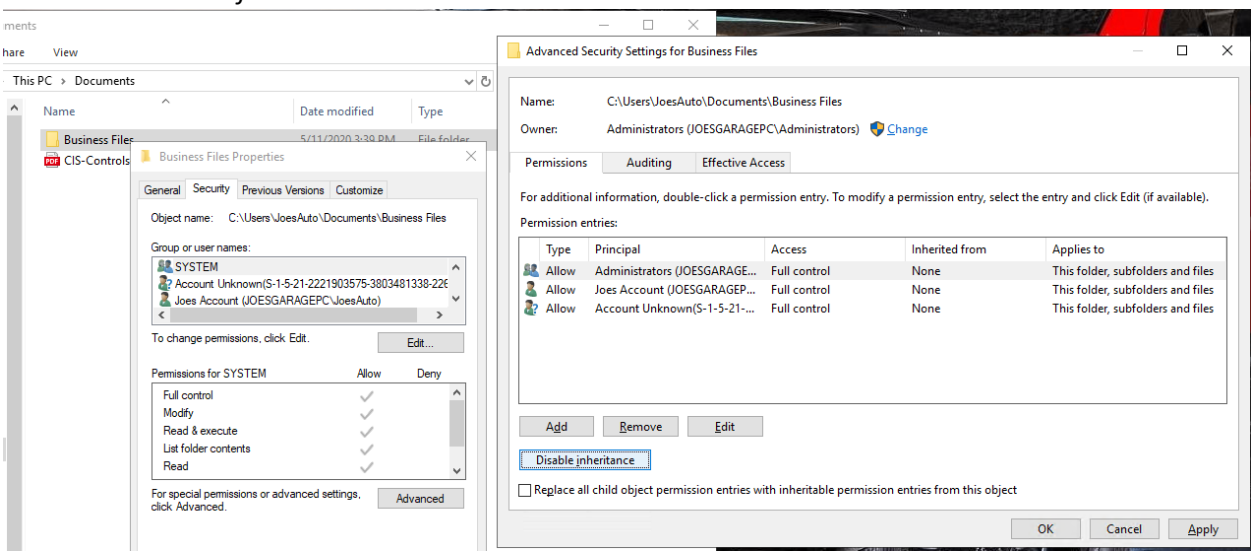
Joe has some work files in his business folder that he wants to secure since they contain his customer information. They are labeled “JoesWork.”

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.

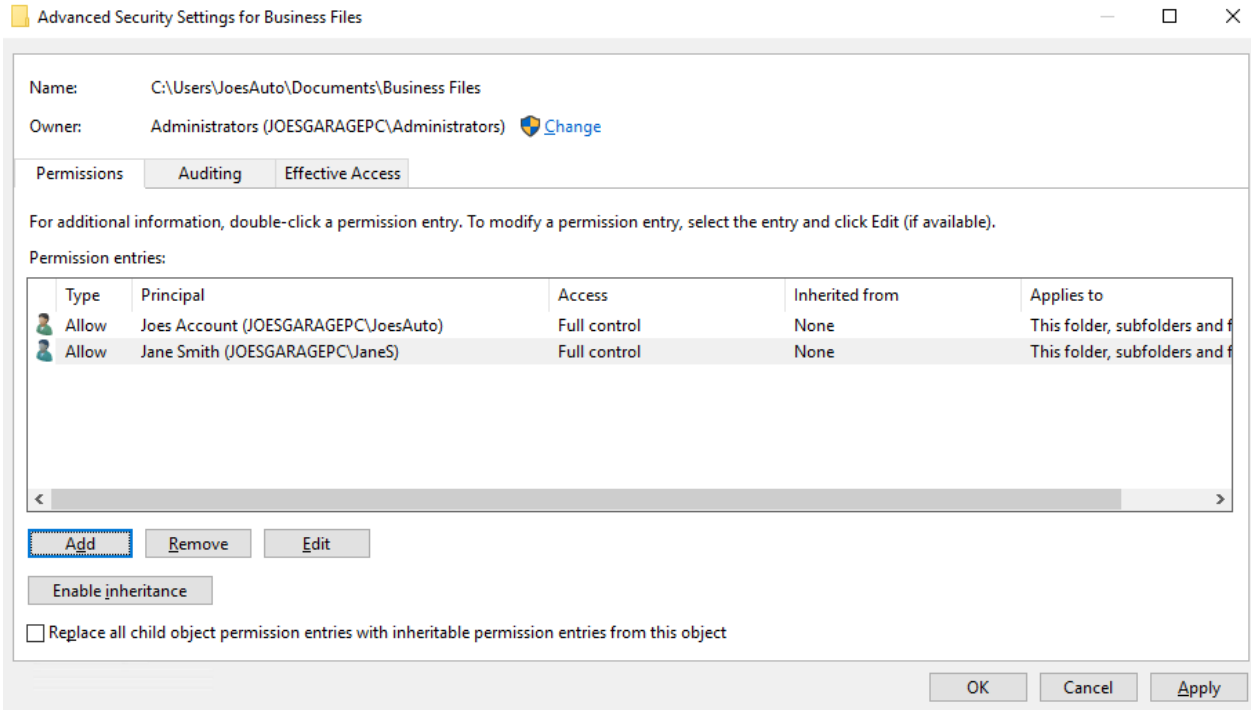
Encrypting files and folders

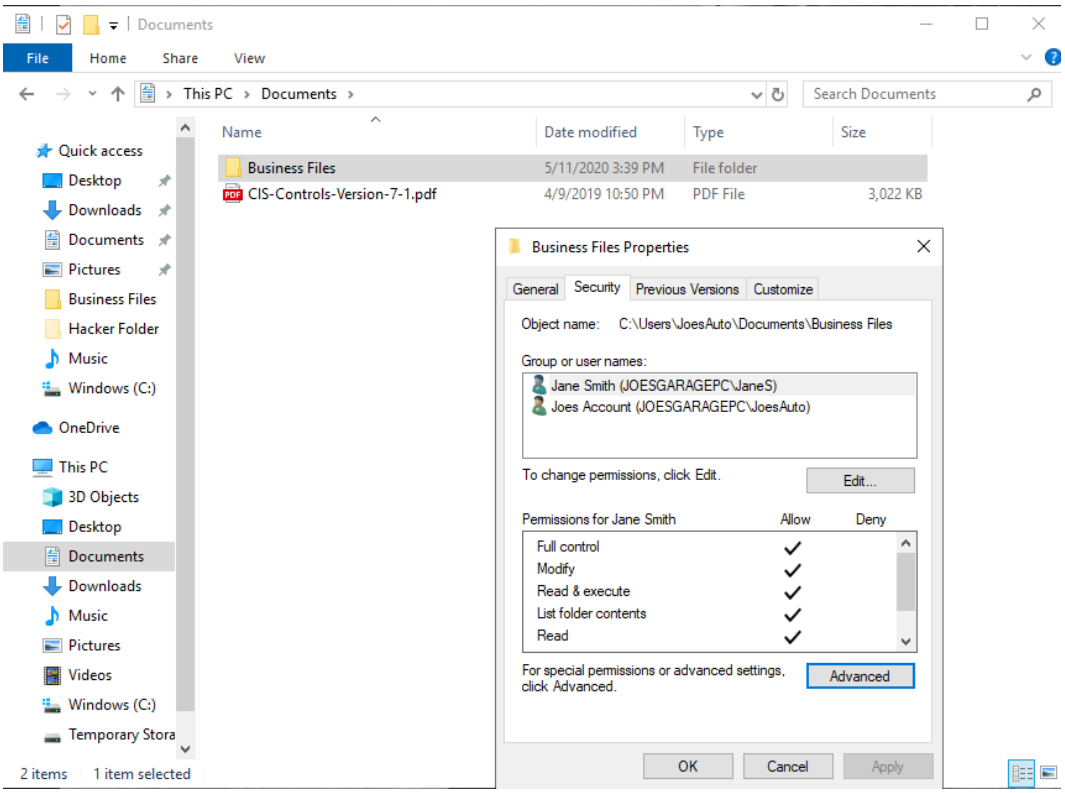
1. *Explain the process for checking this and changing any necessary settings on the file. Include screenshots showing that ONLY Joe and Jane have permissions to change Joes work files. [Hint: Right-click the folder and select Properties.]*

Disable Inheritance first!!!



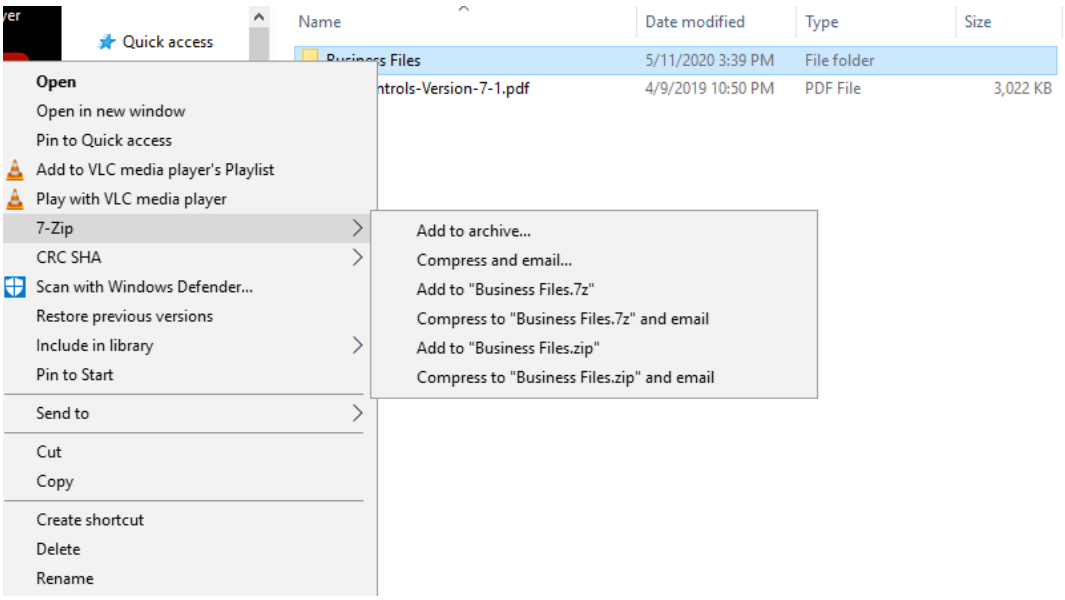
*Remove all unnecessary users, and add **"JaneS"***

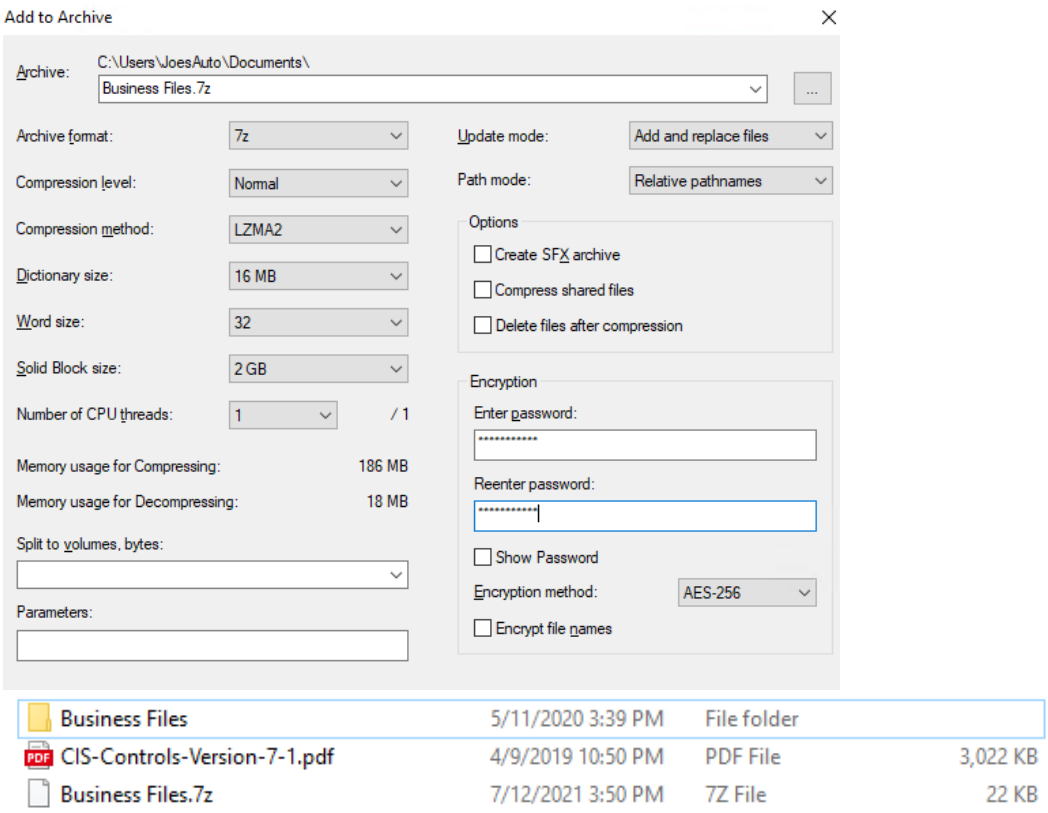




Now only 2 people can access the file!

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.*
   Use 7-zip and add to archive. Then add password with AES-256 encryption. AES-256 is very strong modern encryption algorithm so its strongly recommended.





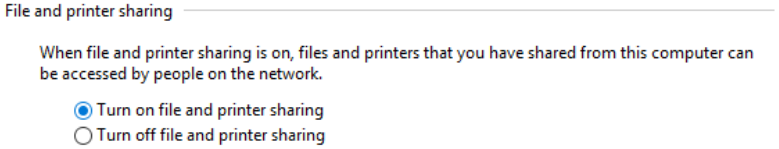
3. *What security fundamental does this provide?*
    - *Confidentiality*
    - *Privacy*
4. *The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?*

    CIS Controls – Foundational Controls - Step 13 – Data Protection

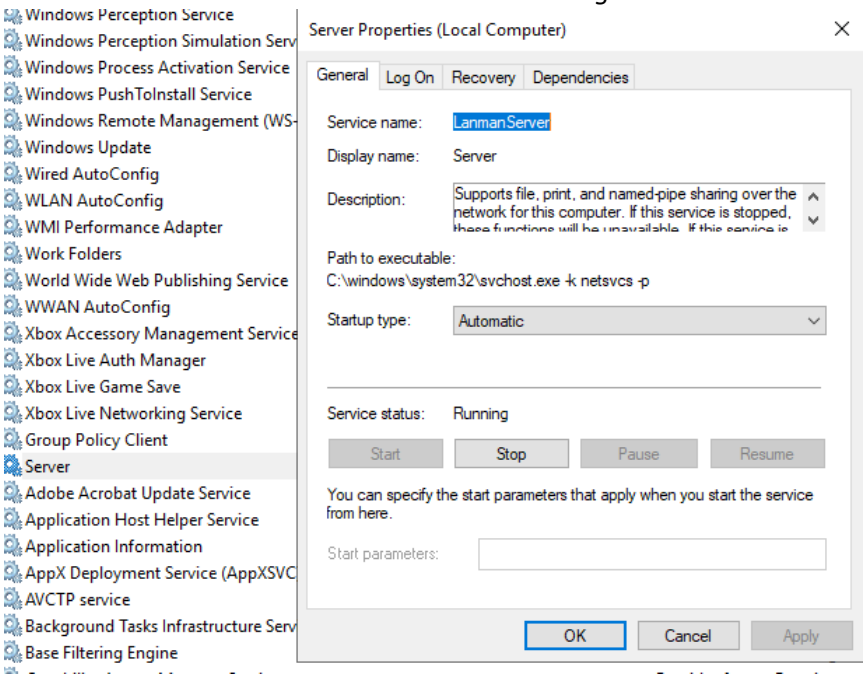
Shared Folders

Shared folders are a common way to make files available to multiple users. There is 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 is only shared between Joe and Jane.*
   First, we need to turn on the sharing available!
    - *Go to "Manage advanced sharing settings"*
    - *Change File and printer setting to **ON***



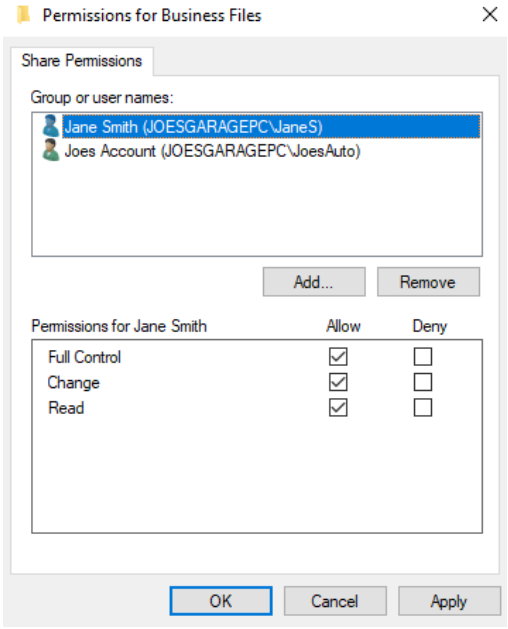
- *Service "Server" should be turned on to use sharing!*

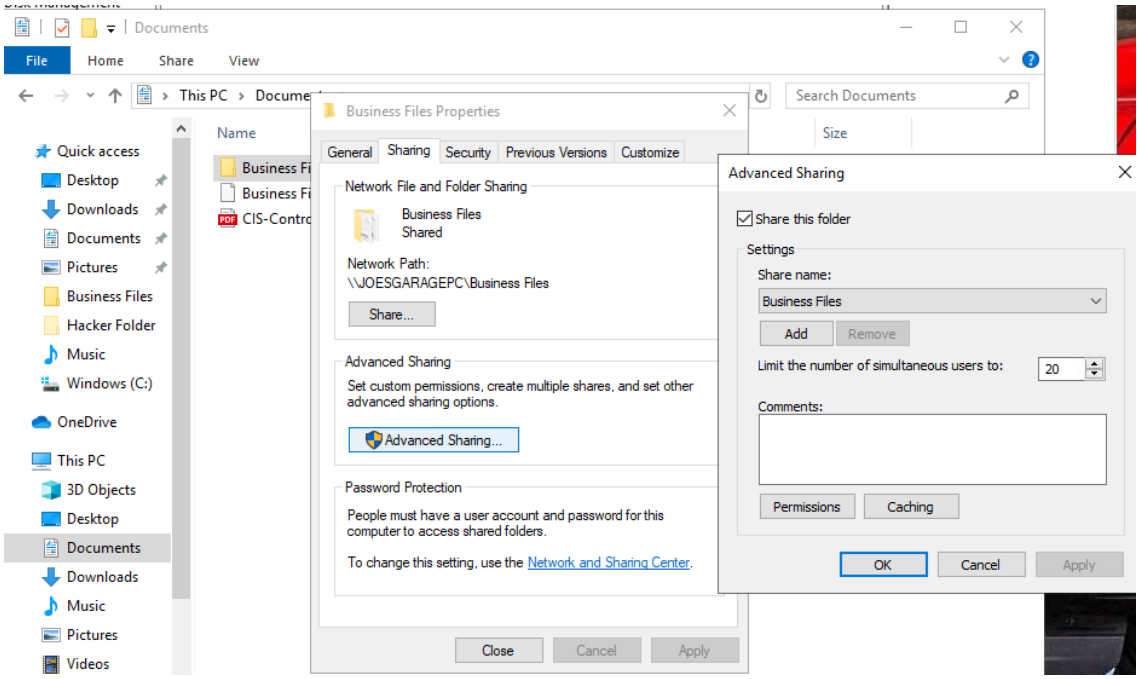


- *Business Files Properties*

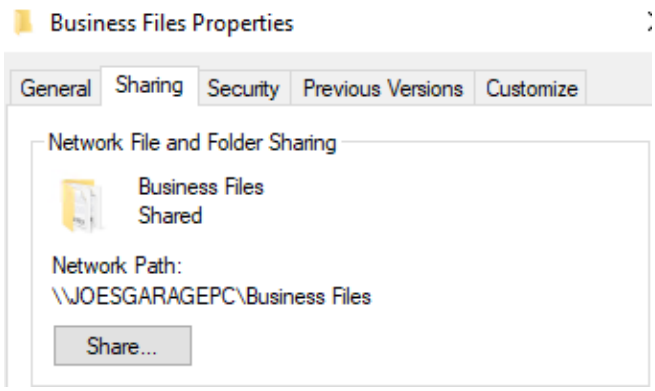
  Make the folder to share folder by following steps.

  Sharing – Advanced Sharing – Set Permission (Add Users) - **OK** *button*





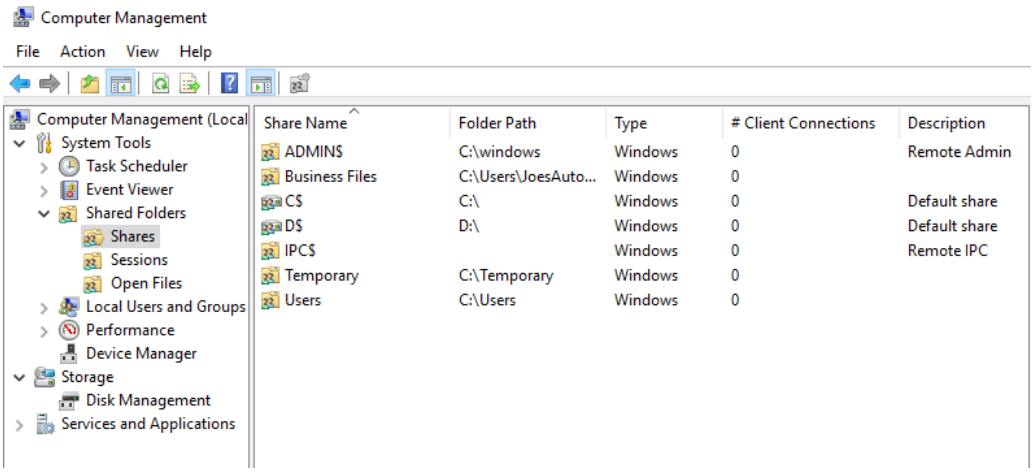
Sharing Done!



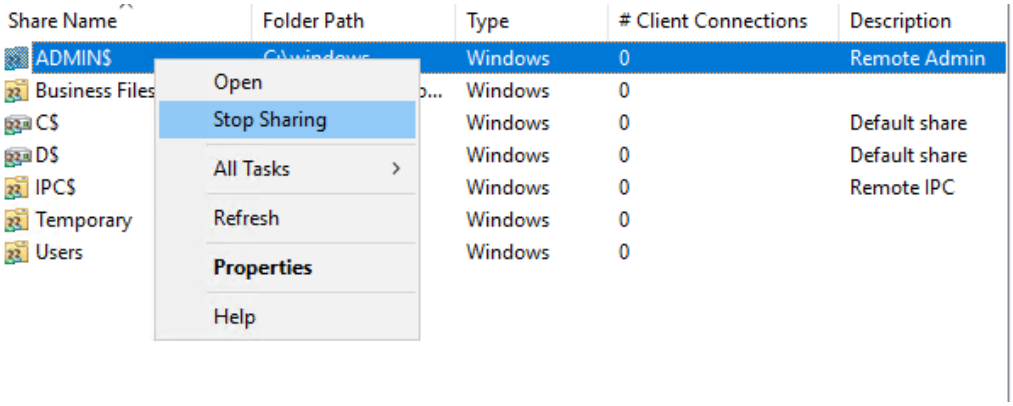
2. *For advanced students: Joe wants to make sure there are no other folders shared on the PC. Explain how you view all shared files and folders on a Windows 10 PC. Include a screenshot as proof.*

   Computer Management - Shared Folders – Shares

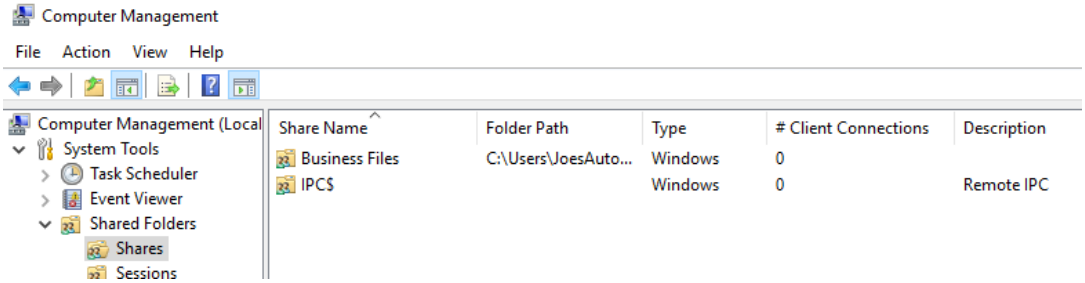
   We can check all the sharing files here!



We can use "Stop Sharing" to remove other sharing folders



Except IPC other shared folders are removed

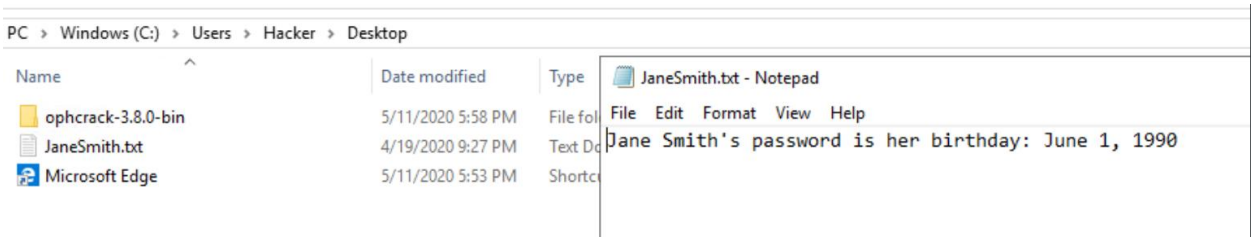


6. Basic Computer Forensics (Optional)

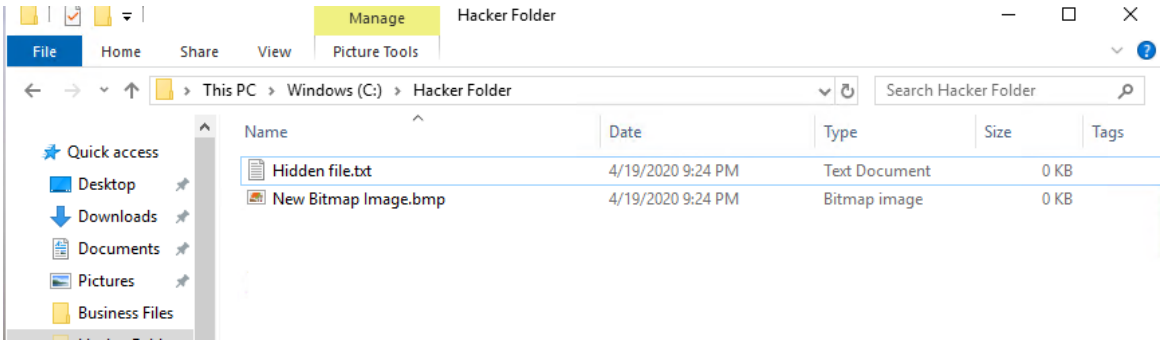
Joe has asked that you investigate his PC to see if there are any other files left behind by previous unwanted users that may show they wanted to harm Joe's business. Look through the unwanted users' folders and list suspicious files. General students should document three issues and advanced students

at least five issues. Include a brief explanation of their contents and their risks. [Hint: there is a “Hacker” in the PC]

- Hackers – Desktop folder

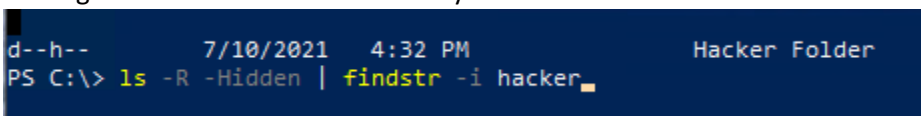


  - Ophcrack – password recovery tool could be used local users to break into other accounts
  - JaneSmith – Jane account password is exposed ☹ hacker could use this account and investigate the important business files or modify or delete it!
- Hacker Folder



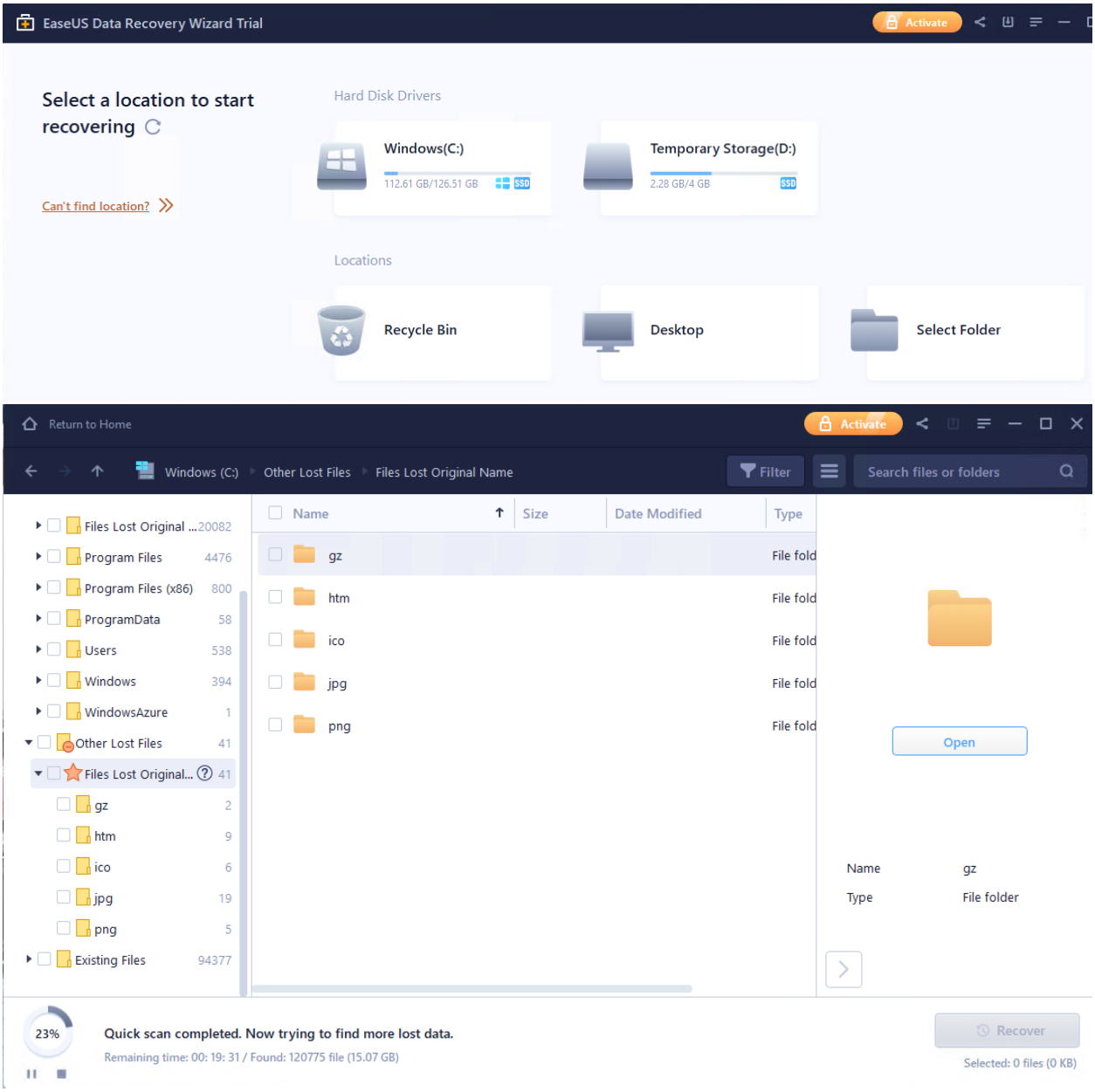
Cannot find out what usage is this hidden folder is for but there might be some risk leaving this folder. Because the folder looks suspicious.

Tried ls on C:\ using PowerShell with administrator privilege but only “Hacker Folder” came out and that is all I got. I think it is because I already removed user “HACKER”

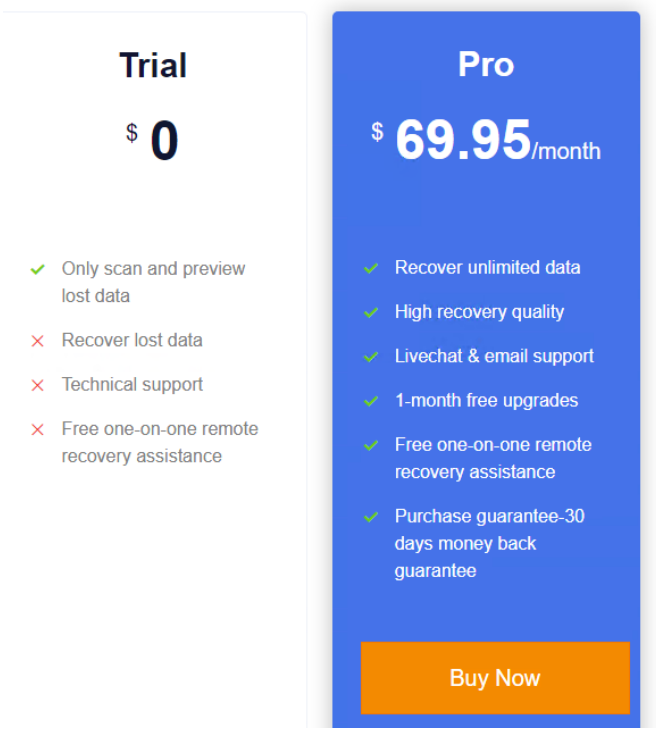


So, I tried to recover the “HACKER” account.

https://www.easeus.com/file-recovery/recover-deleted-user-profile-and-files-in-windows-10.html



I was excited at this moment..



But to recover the data it requires money to recover the lost data, so I gave up ☹

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.