# Udacity Cybersecurity Course #1 Project

Contents

Student Information 2

Scenario 3

1- Reconnaissance 4

2- Securing the PC 15

3- Securing Access 21

4- Securing Applications 26

5- Securing Files and Folders 33

6- Basic Computer Forensics (Optional) 35

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: Mariam Alabkari

Date of completion: 6/22/2021

## 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.***

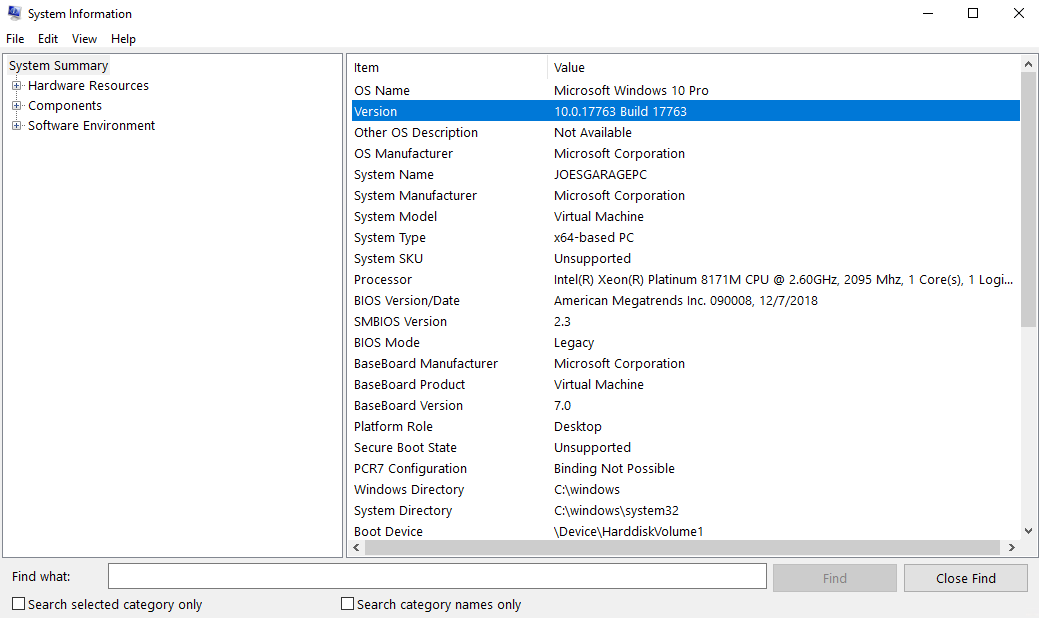
|  |  |
| --- | --- |
| Device Name | JoesGragePC |
| Processor | Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz, 2095 Mhz, 1 Core(s), 1 Logical Processor(s) |
| Install RAM | 1.00 GB |
| System Type | x64-based PC |
| Windows Edition | Microsoft Windows 10 Pro |
| Version | 10.0.17763 N/A Build 17763 |
| Installed on | 5/11/2020, 10:55:54 AM |
| OS build | 17763.1158 |

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

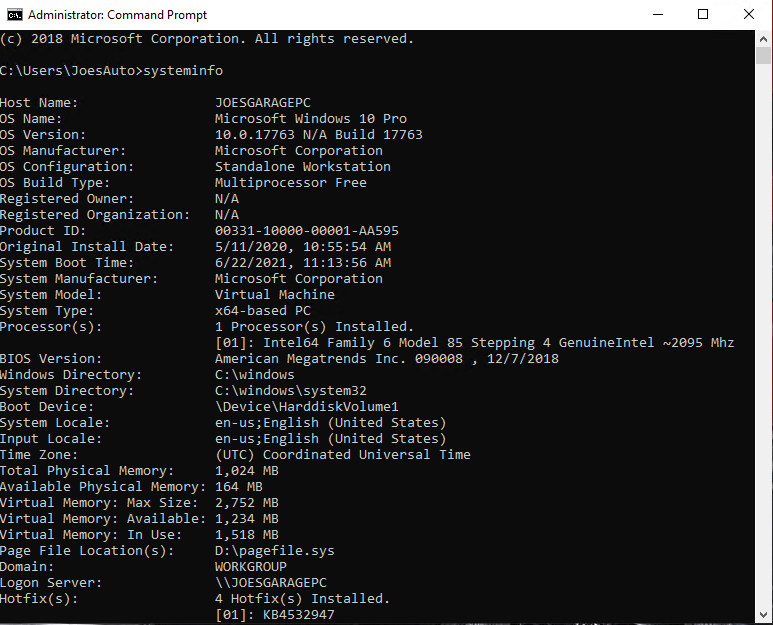
I used the Command Prompt to type Systeminfo command in order to find information about the system. Also, I tried to use different ways such as, open the System Information panel on Windows and from Windows menu go to *Settings > System > About* for more system specifications.

1. ***Provide a screenshot showing this information about Joe’s PC:***

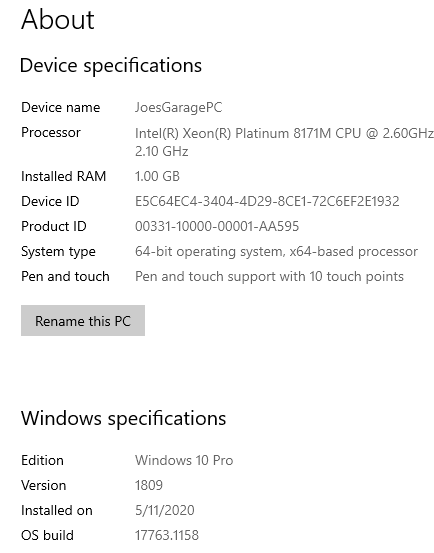
*System Information Panel:*



Command Prompt:



Settings > System > About



***Software***

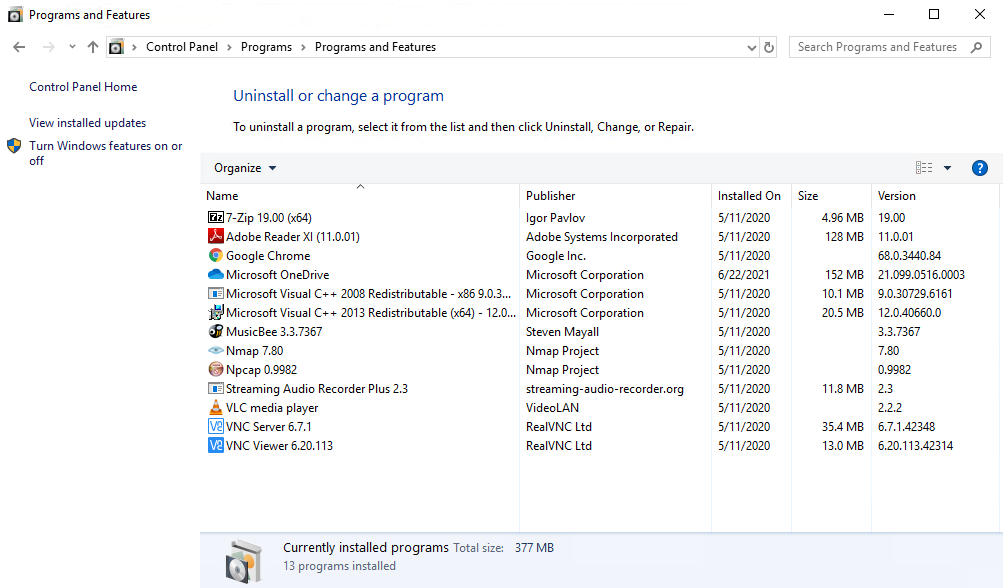
Another common early step in securing is taking an inventory of software or applications installed on a computer system. These are programs outside of the standard operating system.

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

* Nmap
* Google Ghrome
* 7-Zip
* Adobe Reader
* Npcap
* VNC Server
* VNC Viewer
* VLC media player
* Streaming Audio Recorder
* MusicBee
* Microsoft OneDrive
* Microsoft Visual C++

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

I opened the Window Menu then go to Control Panel > Programs > Programs and Features. I found all the software and applications that Installed on Joes PC which are total of 13 programs.



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

Inventory and control of software assets.

***Accounts***

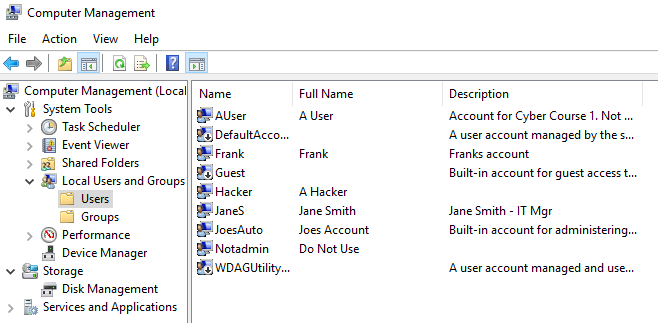
As part of your security assessment, you should know the user accounts that may access the PC.

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

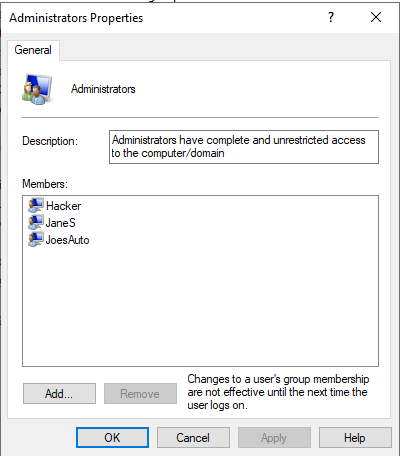
|  |  |  |
| --- | --- | --- |
| **Account Name** | **Full Name** | **Access Level** |
| AUser | A User | Standard |
| DefaultAccount | - | - |
| Frank | Frank | Standard |
| Guest | - | - |
| Hacker | A Hacker | Administrator |
| JaneS | Jane Smith | Administrator |
| JoesAuto | Joes Account | Administrator |
| Notadmin | Do Not Use | Standard |
| WDAGUtilityAccount | - | - |

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

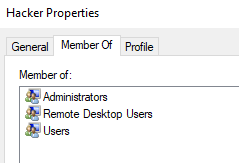
*I opened Computer Management > Local Users and Groups > Users to display the list of users.*



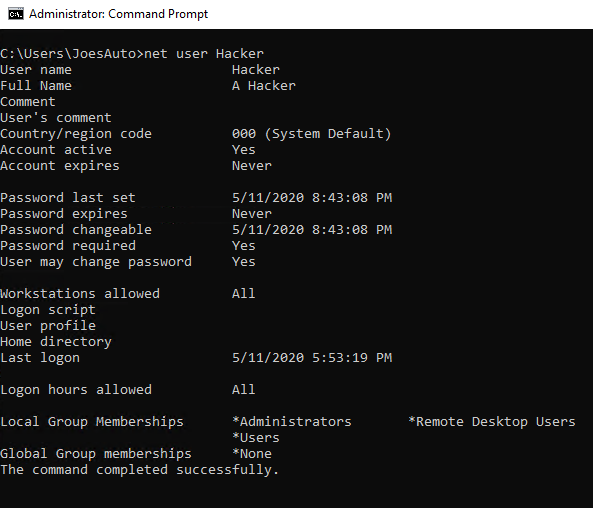
*I checked the Administrators properties to display the admin users.*



*Also, I checked the properties of each user to display the access level. If the user member of Administrators this mean the user has an* administrative privilege, if only member of Users it is just a standard account.

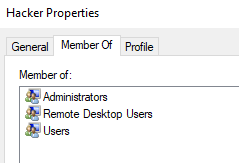


Also, I tried to use type net user command in the Command Prompt to display the access level of each user.



Properties:

Used to check the access level of each user

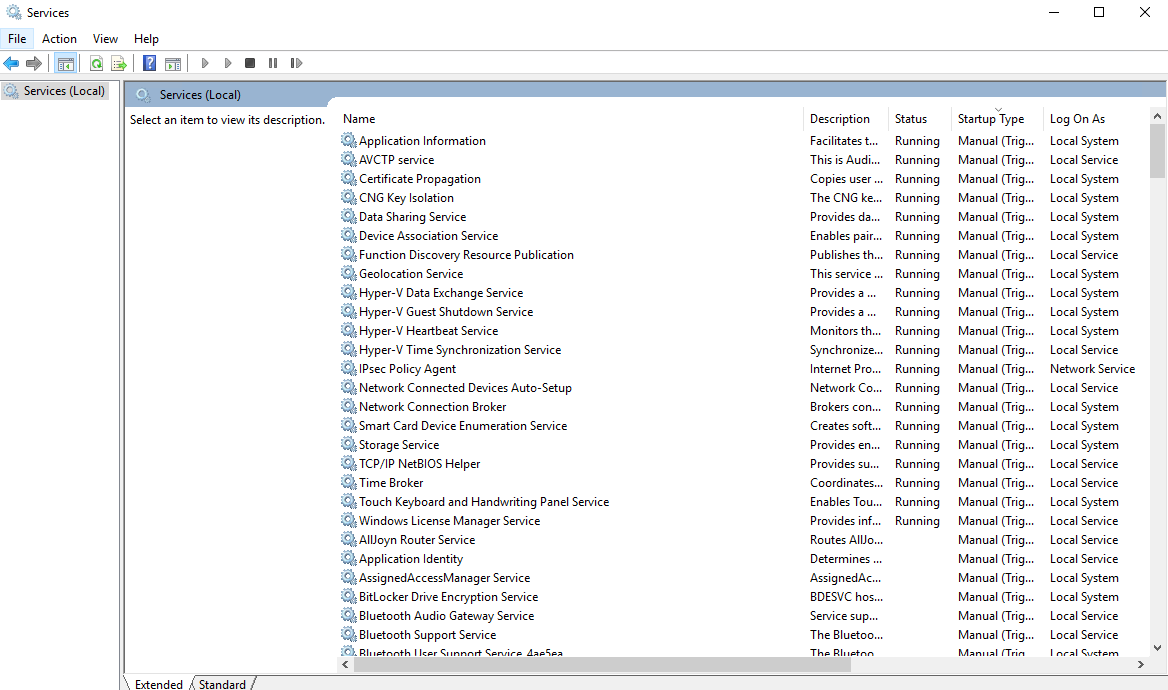


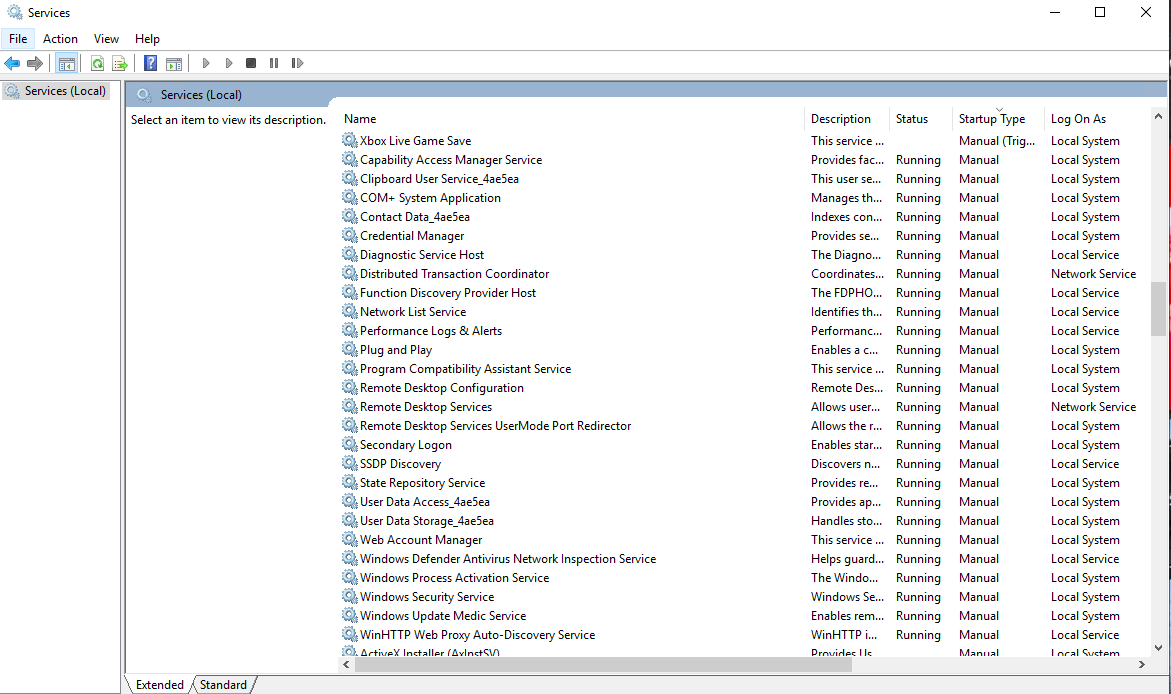
***Services***

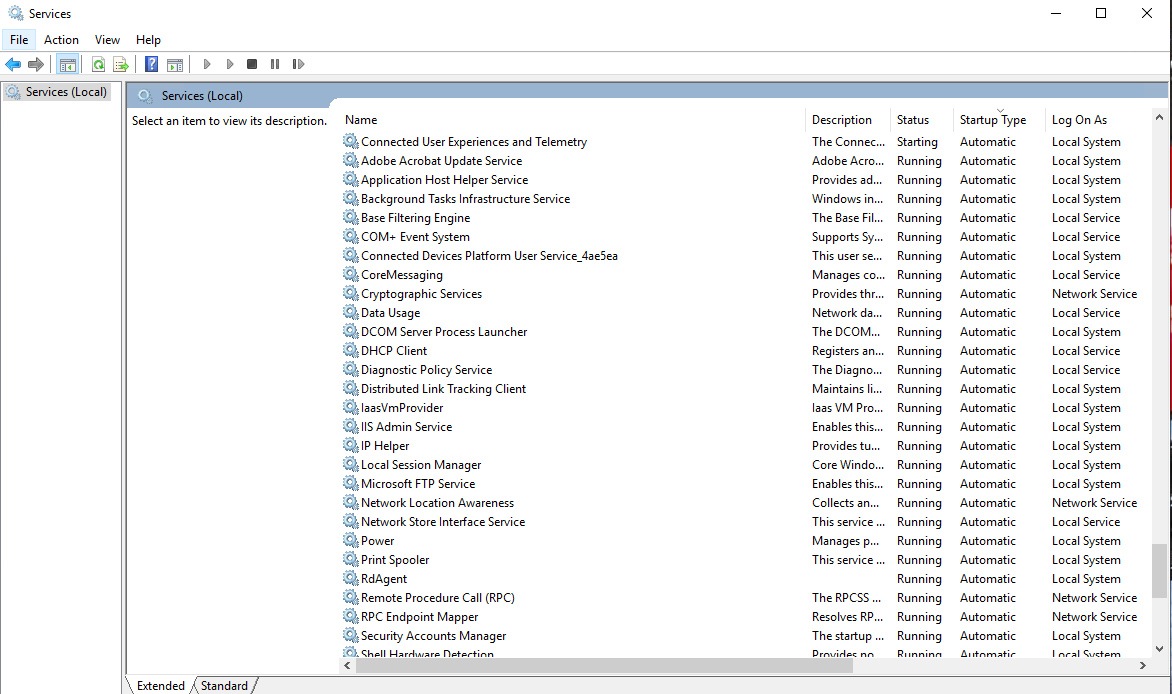
Services are applications often running in the background. Most of them provide needed functionality for the PC. Some may also be used to violate security policies.

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

I opened the Services section which contains a Status column that shows the running programs.







***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.**

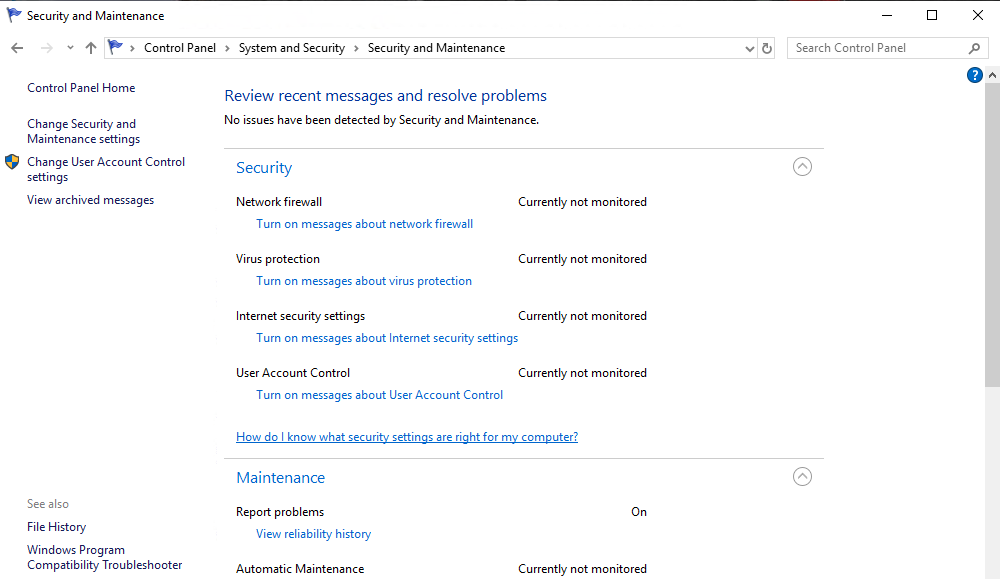
1. *To view a summary of security on Windows 10, start from the* ***Control Panel****. Use the “Find a setting” bar and search on Windows Defender. You can also search for Windows Defender using the Windows Run bar. Take a screenshot of what you see on the Windows Security screen and include it here:*

*Settings > Update & Security > Windows Security*



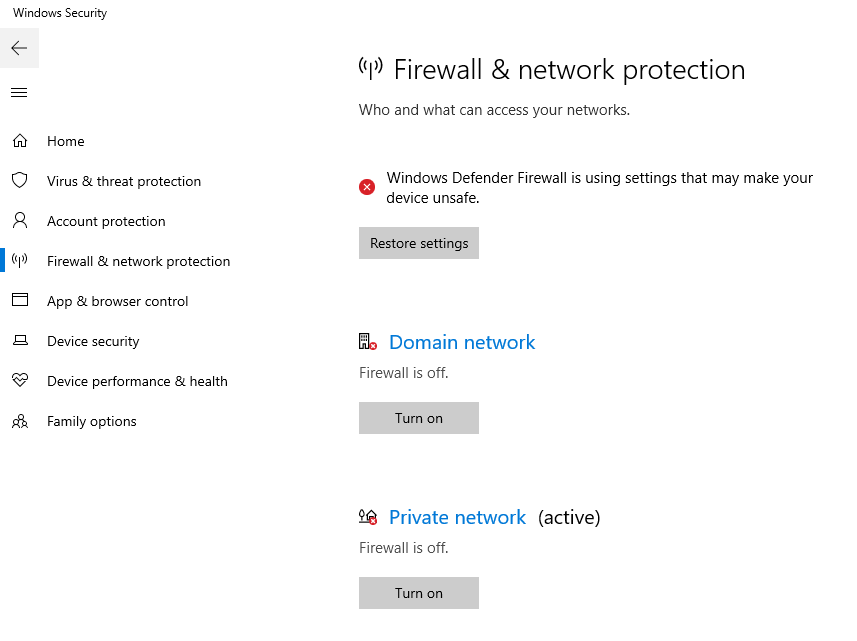
1. *The Windows 10 Security settings are also found from the* ***Control Panel > System and Security > Security and Maintenance****. Start by viewing* ***“Review your computer’s status and resolve issues.”*** *Provide a screenshot of this below:*

*Control Panel > System and Security > Security and Maintenance*



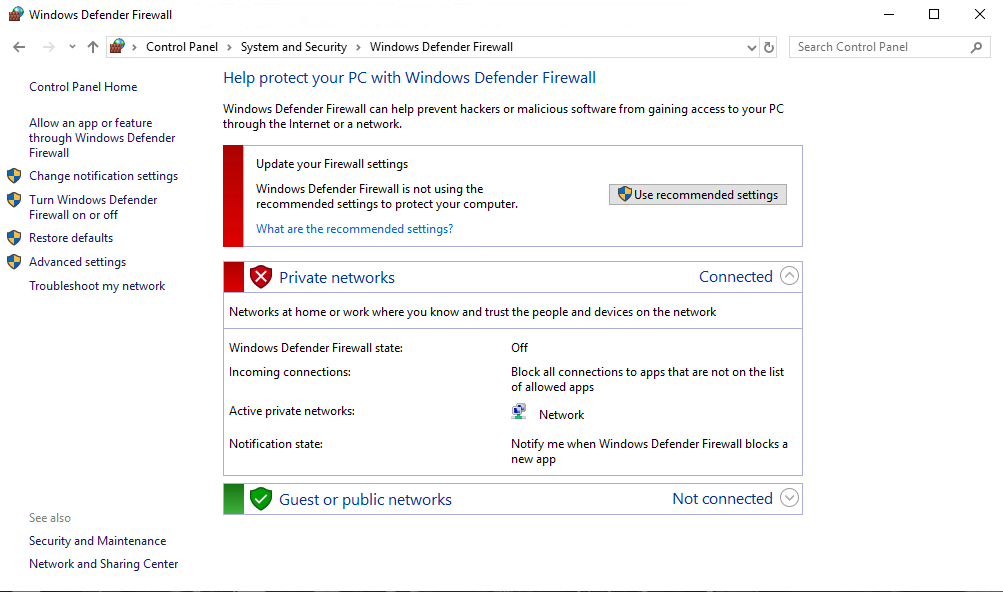
1. *Click on View in Windows Security to see the status there. Provide a screenshot of the* ***Firewall*** *settings.*

*Windows Security > Firewall & Network Protection*



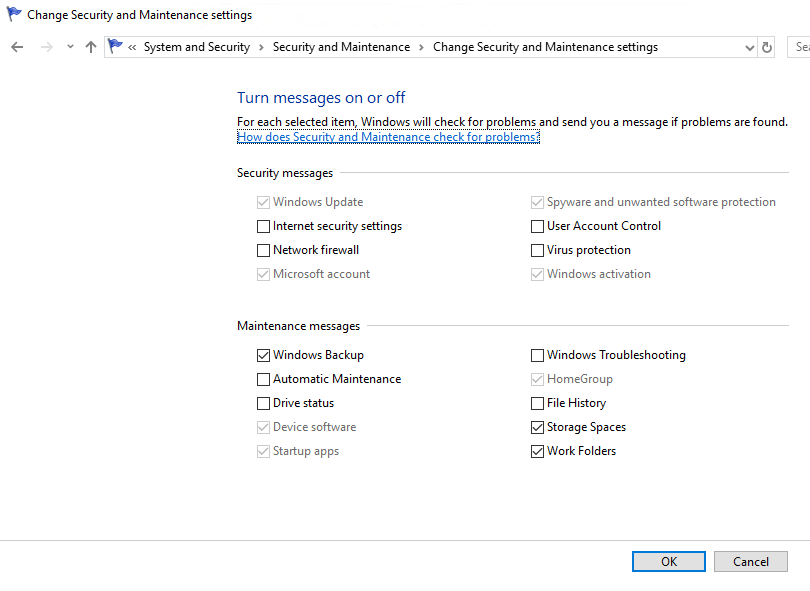
1. *From the* ***Control Panel****, go to* ***System and Security****. In that window, select* ***Windows Defender Firewall****. Provide a screenshot of it here:*

*Control Panel > System and Security > Windows Defender Firewall*



1. *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:*

*Control Panel > System and Security > Security and Maintenance > Change Security and Maintenance settings*



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

|  |  |  |
| --- | --- | --- |
| **Security Feature** | **Status** | **Process Used** |
| Firewall product and status – Private network | Off | Windows Security > Firewall & Network Protection |
| Firewall product and status – Public network | On | Windows Security > Firewall & Network Protection |
| Virus protection product and status | On | Windows Security > Virus & Threat Protection |
| Internet Security messages | Currently not monitored | Control Panel > System and Security > Security and Maintenance |
| Network firewall messages | Currently not monitored | Control Panel > System and Security > Security and Maintenance |
| Virus protection messages | Currently not monitored | Control Panel > System and Security > Security and Maintenance |
| User Account Control Setting | Currently not monitored | Control Panel > System and Security > Security and Maintenance |

1. ***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.]***

* The private network's firewall is turned off, which could allow unauthorized access to the network.
* The settings for User Account Control set as never notify me, which means it will not notify the user if the applications try to install software or make changes to the computer or the settings.
* Windows Defender SmartScreen is off, which means it can't safeguard the device by checking apps and data downloaded from the internet.
* The Virus Protection Messages feature is disabled, therefore the user will not be warned if something goes wrong.

## 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?***

*He should follow the NIST security policies, because it is responsible for establishing information security standards and guidelines.*

1. ***What industry baseline do you recommend to Joe?*** ***[Hint: Look in the documents folder]***

*I highly recommend the CIS controls document, because it outlines in depth what an organization should do to protect itself against cyber-threats.*

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.

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

* Inventory and Control of Software Assets
* Inventory and Control of Hardware Assets
* Controlled Use of Administrative Privileges
* Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
* 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

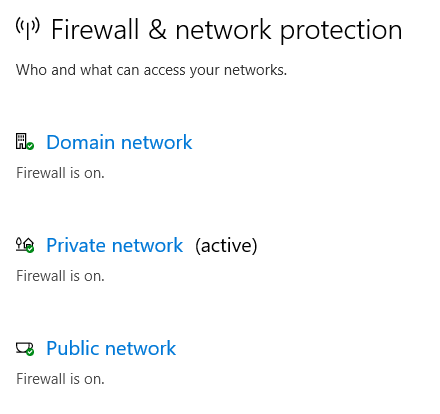
**Firewall**

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

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

*I opened Windows Security > Firewall & Network Protection then I turned on the firewalls.*

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



1. ***What protection does this provide?***

This will ensure that there will be no unauthorized access to the network.

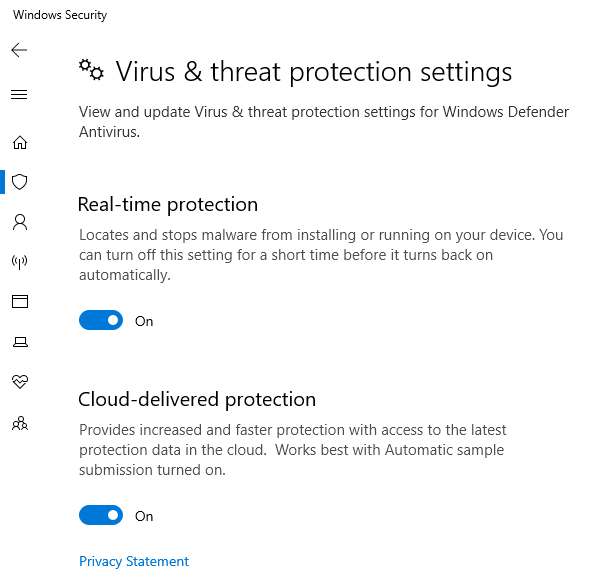
**Virus & Threat Protection**

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.***

*I opened the Settings > Update & Security > Windows Security > Virus & Threat Protection Settings and turned the antivirus on.*

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

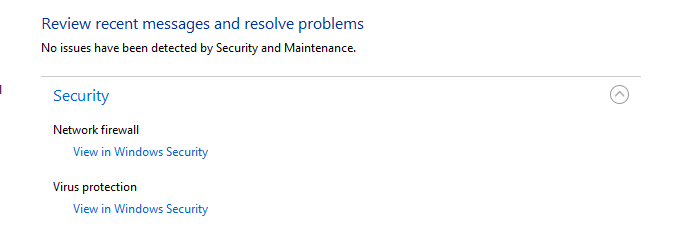


Once you determine that virus & threat protection is on and updated, you need to turn on messages about the Network firewall and Virus protection. Refer to the instructions above for viewing the settings within Security and Maintenance, Review recent messages and resolve problems.

1. ***Turn on the Network firewall and Virus protection messages using Change Security and Maintenance Settings.***

*Control Panel > System and Security > Security and Maintenance*

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

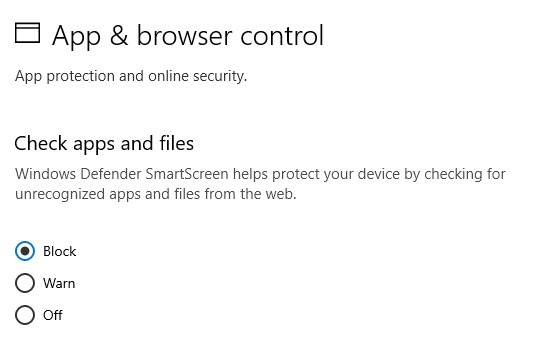


1. ***Provide at least two risks mitigated by enabling these security settings:*** 
   * Enabling network firewall messages will assist in notifying the user if there is any unauthorized network access.
   * Enabling virus protection messages will assist in notifying the user if a virus is present or if something goes wrong.
2. ***From the CIS baseline controls, provide the controls satisfied by completing this.*** 
   * Malware Defenses
   * Secure Configuration for Network Devices, such as Firewalls
   * Boundary Defense

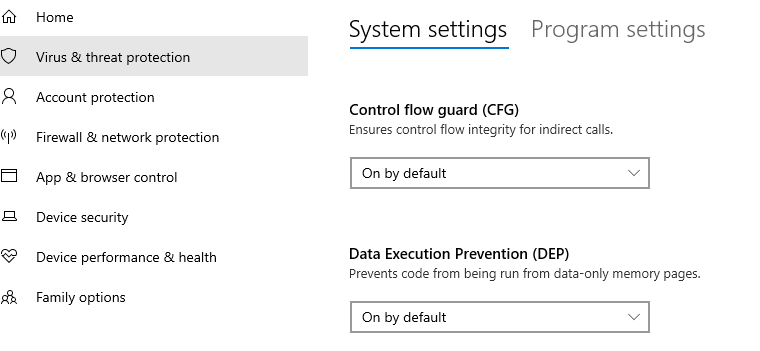
**App & Browser Control**

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.*



Exploit protection



**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.

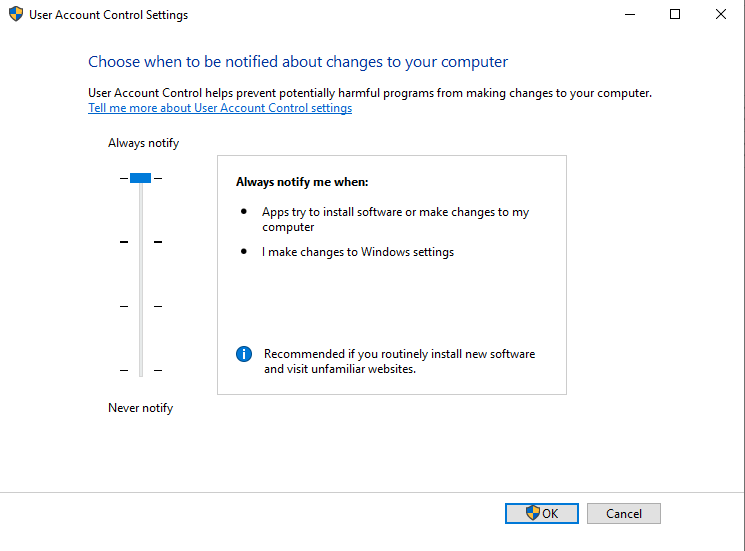
1. ***What is the current UAC setting on Joe’s computer?***

**This is available from the above security settings.**

Never notify whenever apps try install or make changes.

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

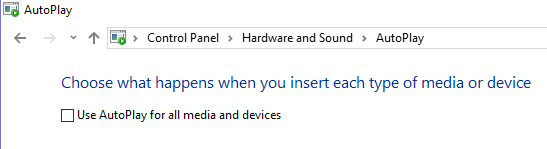
*It should set to always notify*



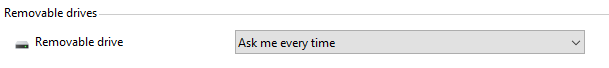
**Securing Removable Media**

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.”***



1. ***For the Removable Drive, make the default, “Ask me every time.” Include a screenshot of your results.***

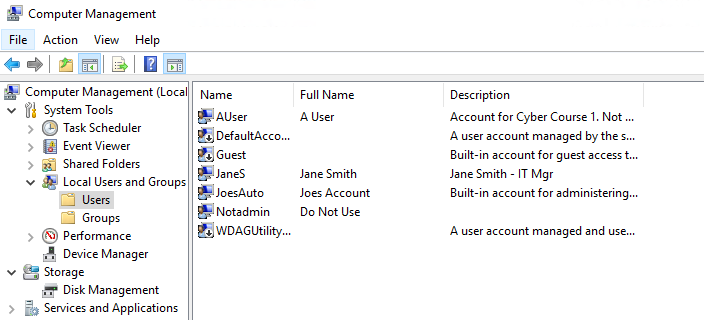


## 3. Securing Access

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 & Hacker*

1. ***Bonus questions: What is Hacker’s password?***
2. ***Explain the steps you take to disable or remove unwanted accounts.***

*I opened the Computer Management > Local Users and Groups > Users then I deleted Frank and Hacker.*

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

Unneeded accounts should be disabled or removed to avoid unauthorized access and protect the device and data from inside attacks.

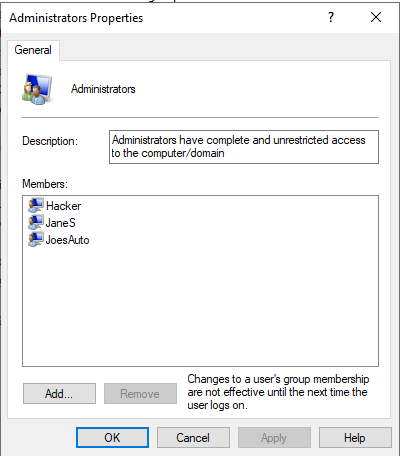
Only specific accounts should have administrator privileges. This reduces the ability for unwanted applications to be installed including malware.

1. **Which account(s) have administrator rights that shouldn’t?**

Hacker & JaneS

1. **Explain how you determined this. Provide screenshots as needed.**

*I checked the Administrators properties to display the admin users.*



Administrator privileges for too many users are another security challenge.

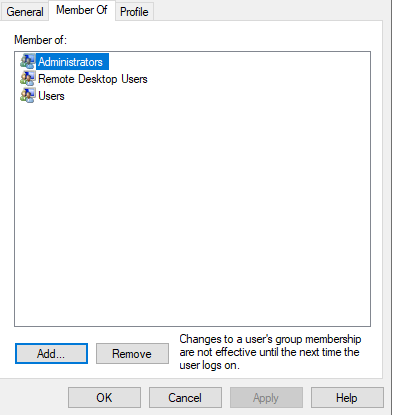
1. **Provide at least three risks associated with users having administrator rights on a PC.**

* Install software and applications that contains malware
* Make unwanted changes in the system
* Delete or access to important files

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

1. ***Explain the process for doing this. Include screenshots to show your work.***

Go to properties then member of, then choose administrators and finally click at delete.



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

*Least-privilege*

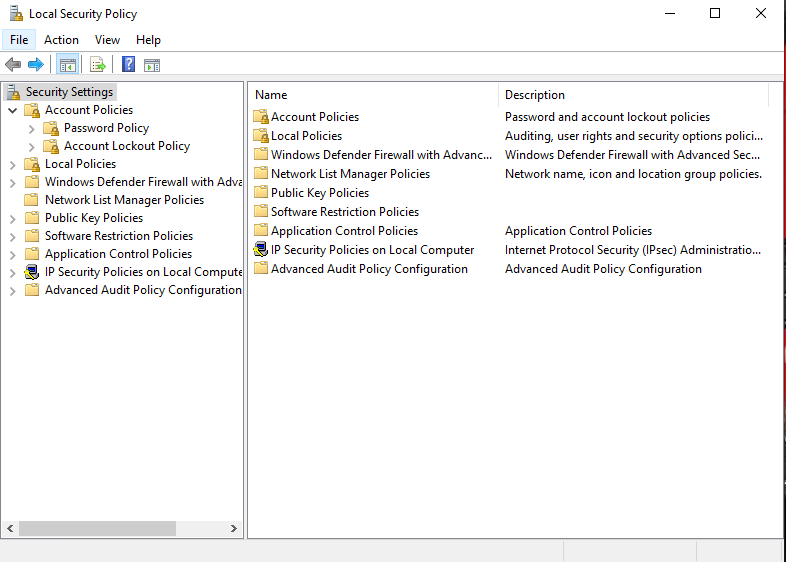
1. **The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?**

Control use of administrative privileges

***Setting Access and Authentication Policies***

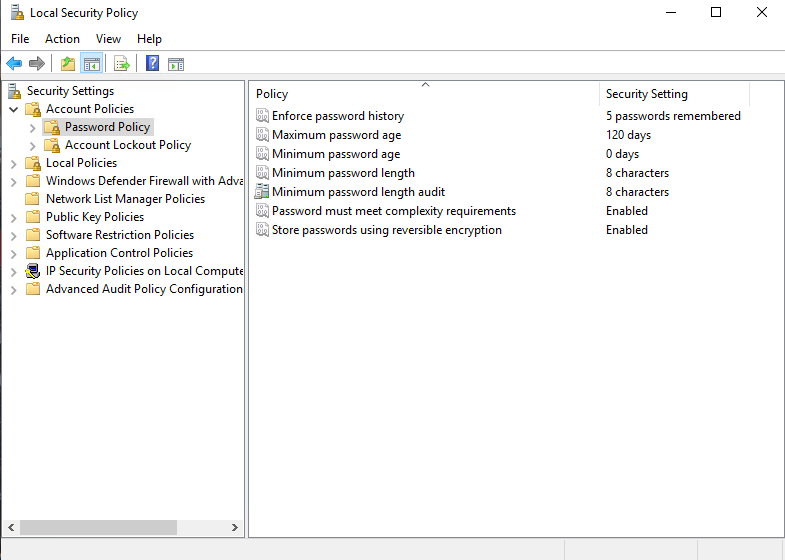
After you talked with Joe about security, he has asked that the access rules outlined above be in place on his PC. These are set using the Local Security Policy function in Windows 10. On the Windows search bar, type “*Local Security Policy*” to access it. Click the > arrow next to both “*Account Policies*”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



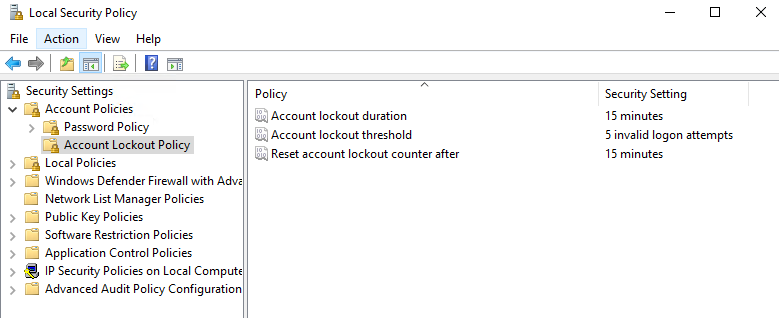
1. Explain the process for setting the password and access control policies locally on a Windows 10 PC. Provide screenshots showing how you set the rules on the PC.
   * **Setting the Password Policy:**

From the Local Security Policy, I chose Password Policy and I made all the changes that mentioned earlier.



* + **Setting the Account Lockout Policy:**

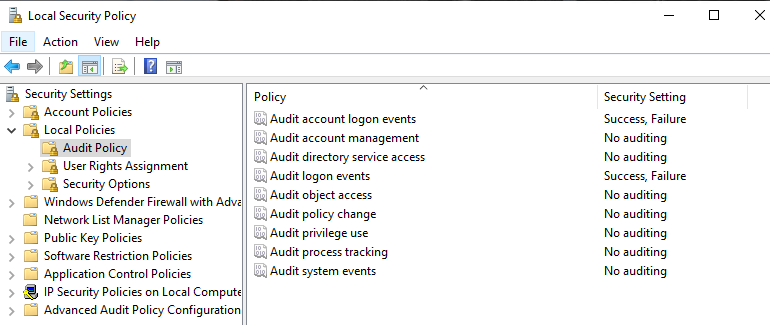
From the Local Security Policy, I chose Account Lockout Policy and I made all the changes that mentioned earlier.



***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.***

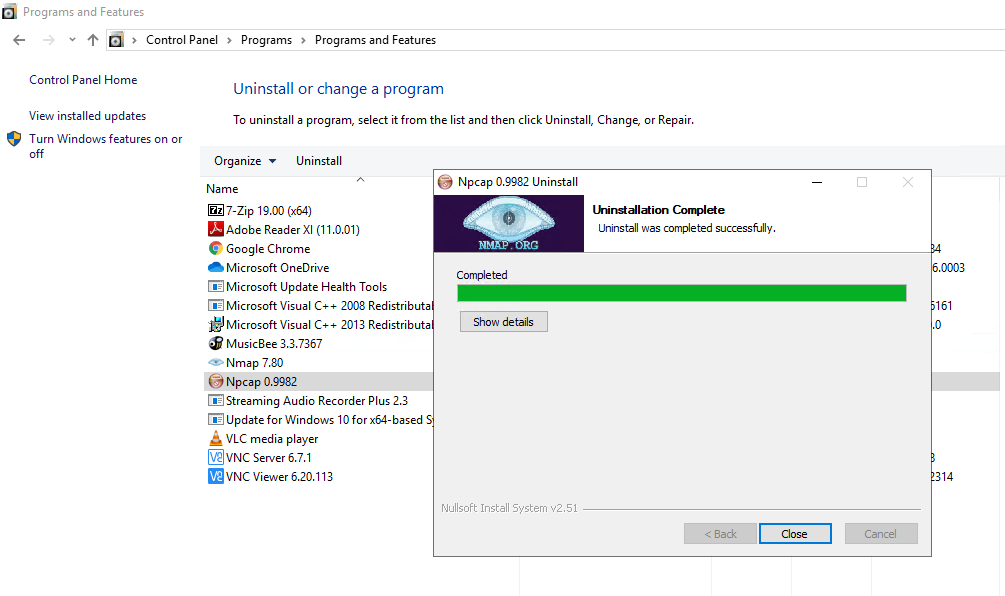
* *7-zip*
* *Npcap*
* *Candy Crush Friends*
* *MusicBee*
* *Microsoft OneDrive*

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

* Allow unauthorized and illegal access to the computer
* Display inappropriate ads or windows such as fake antivirus notifications.
* Consume system resources and violate licensing agreements
* Cause the computer to slow down or crash
* Modify the security settings, which greatly increasing the risk of malwares.

1. ***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.***

From the Window Menu I opened Control Panel > Programs > Programs and Features. Then I click at the unwanted programs and I uninstalled them.

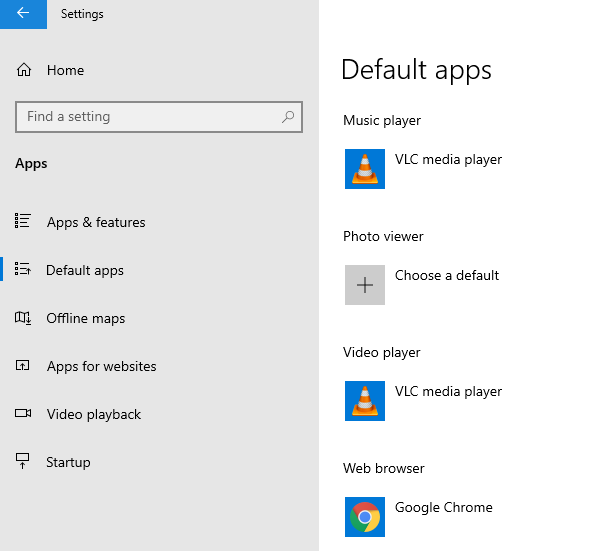


***Default Browser***

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.***

I opened Settings > Default apps. Then I changed the default web browser to Google Chrome.

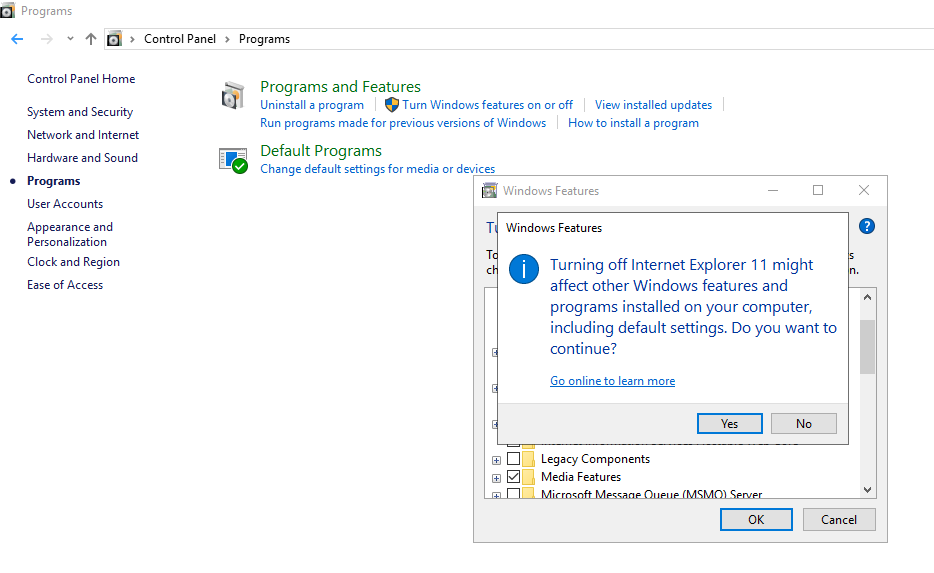


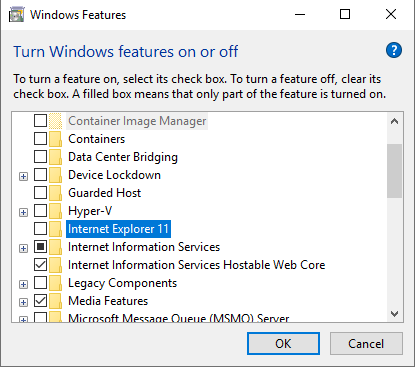
1. ***Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.***

* Lack of Support
* Frequent Vulnerabilities.
* Unsafe

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**.”

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



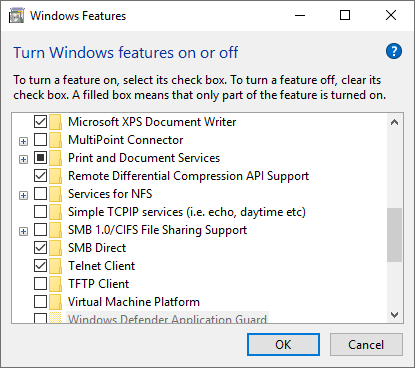


***Windows Services***

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.**

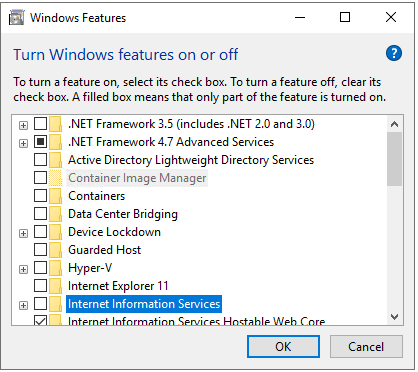
I used the Windows Features section which determined the services that on or off.



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

Control Panel > Programs > Programs and Features > Windows Features.

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



1. **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.**

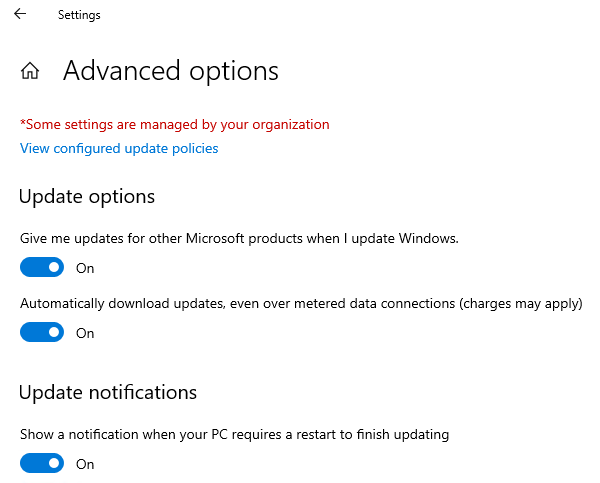
Not available

***Patching and Updates***

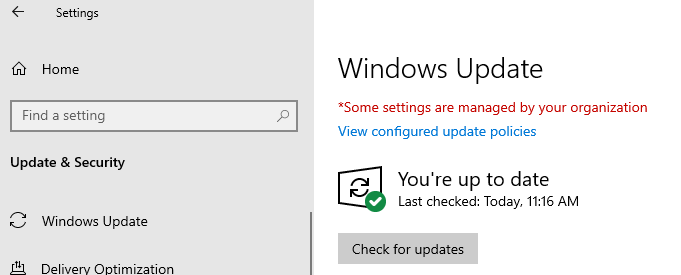
Keeping the operating system current on patches and fixes is a critical part of security. Joe wants his PC to be on the latest version of Windows 10. He also wants you to set it up for automated updates.

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

*From settings I opened the Advanced options then allow the automatically updates.*



1. *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.

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

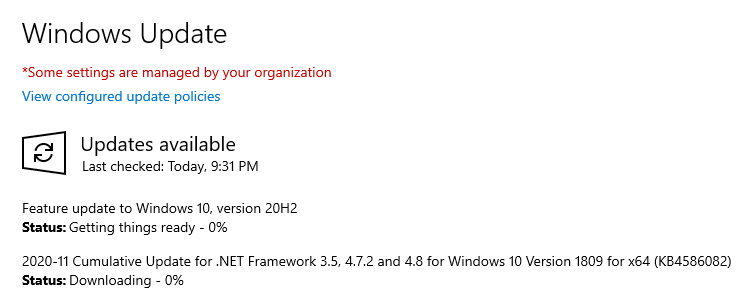
* .NET Framework
* Google Chrome
* Microsoft OneDrive

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

*From settings I opened the Windows Updates then I clicked at check for updates. In addition, I looked for new versions of the applications in their websites.*

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

*I began to upgrade the new versions after checking for new updates.*



## 5. Securing Files and Folders

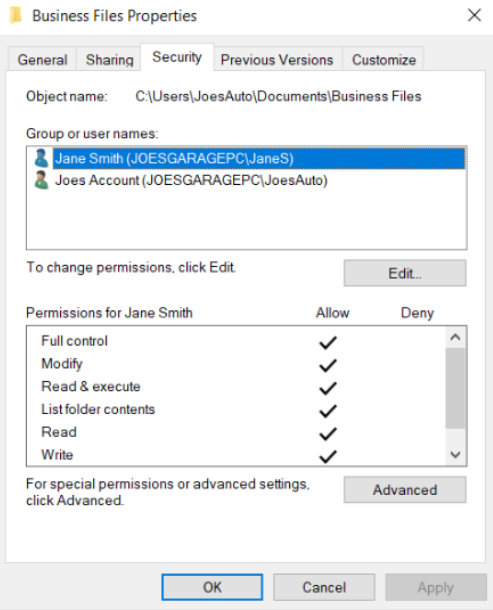
Joe has some work files in his Business folder that he wants to secure since they contain his customer information. They are labeled “JoesWork.”

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.]***

*I opened the business file properties, then I clicked at edit and I removed all the users excepts Joe and Jane.*



1. ***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.***

* *I right click on the file and select 7-zip*
* *Add it to the archive*
* *Select file type and enter the password as SU37\*$xv3p1*
* *Select desired encryption and choose the AES algorithm*

1. ***What security fundamental does this provide?***

*Confidentiality*

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

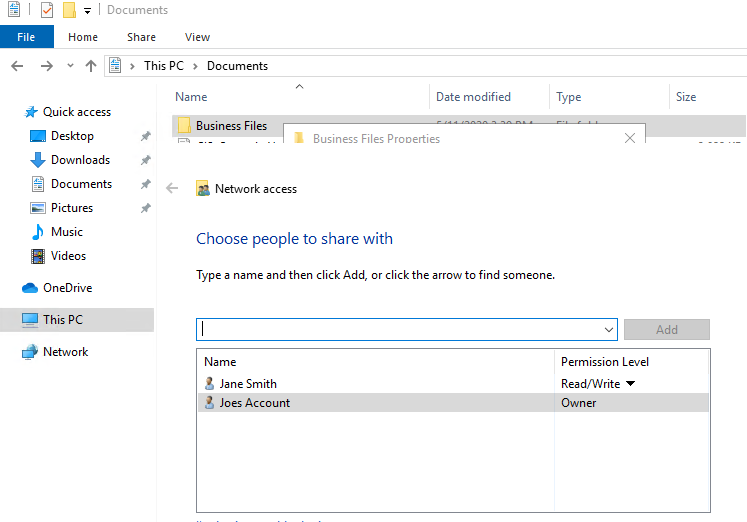
Data protection

***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.***

*From the property of the folder, then click at sharing. Choose share option then pick the users.*



1. ***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.***

*From Computer Management > Shared Folders we could find list of the file that shared*

## 

## 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]

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.