

Udacity Cybersecurity Course #1 Project

Contents

Student Information	2
Scenario	3
1. Reconnaissance	4
2. Securing the PC	6
3. Securing Access	8
4. Securing Applications	10
5. Securing Files and Folders	13
6. Basic Computer Forensics (Advanced)	14
7. Project Completion	15

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: Senthil Kumar Appadorai

Date of completion: 19/9/2020

Scenario

Congratulations!

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

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

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

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

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

Account Name: JoesAuto

Password: @UdacityLearning#1

1. Reconnaissance

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

Complete each section below.

Hardware

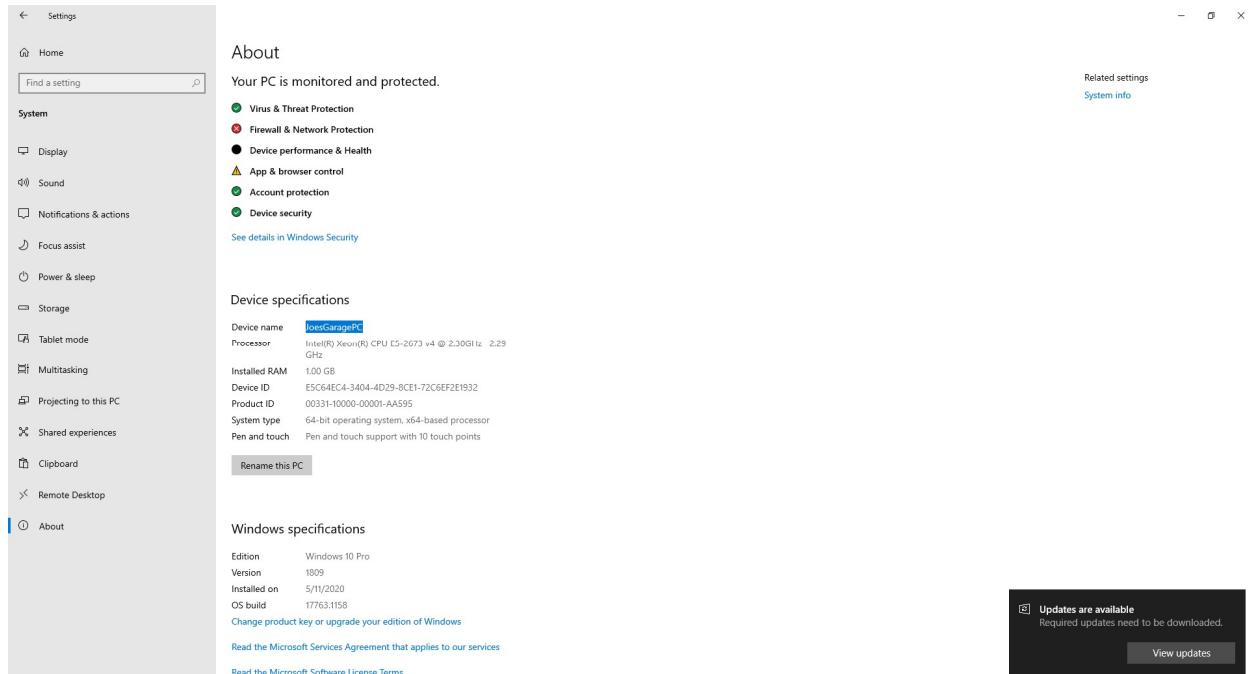
- Fill in the following table with system information for Joe's PC.

Device Name	JoesGaragePC
Processor	Intel® Xeon® CPU E5-2673 v4 @ 2.30GHz 2.29 GHz
Install RAM	1GB
System Type	64 bit operating systems, x64 based processor
Windows Edition	Windows 10 Pro
Version	1809
Installed on	5/11/2020
OS build	17763.1158

- Explain how you found this information:

Start -> Settings -> About - will give all the above details

- Provide a screenshot showing this information about Joe's PC:



Software

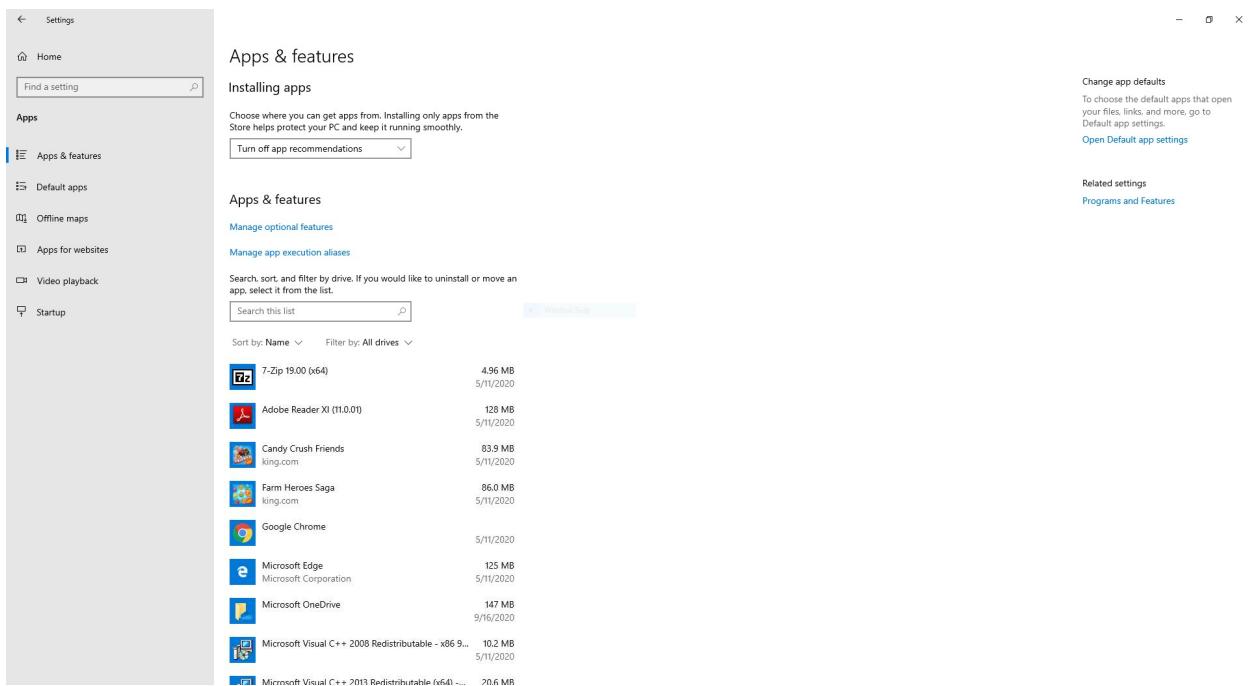
Another common early step in securing is taking an inventory of software or applications installed on a computer system. These are programs outside of the standard operating system.

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

- 7 zip
- Adobe Reader
- Candy Crush Friends
- Farm Heroes Saga
- Google Chrome

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

Start -> Settings -> Apps – Will list all the apps installed in the system



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

Inventory of Authorized and Unauthorized Software

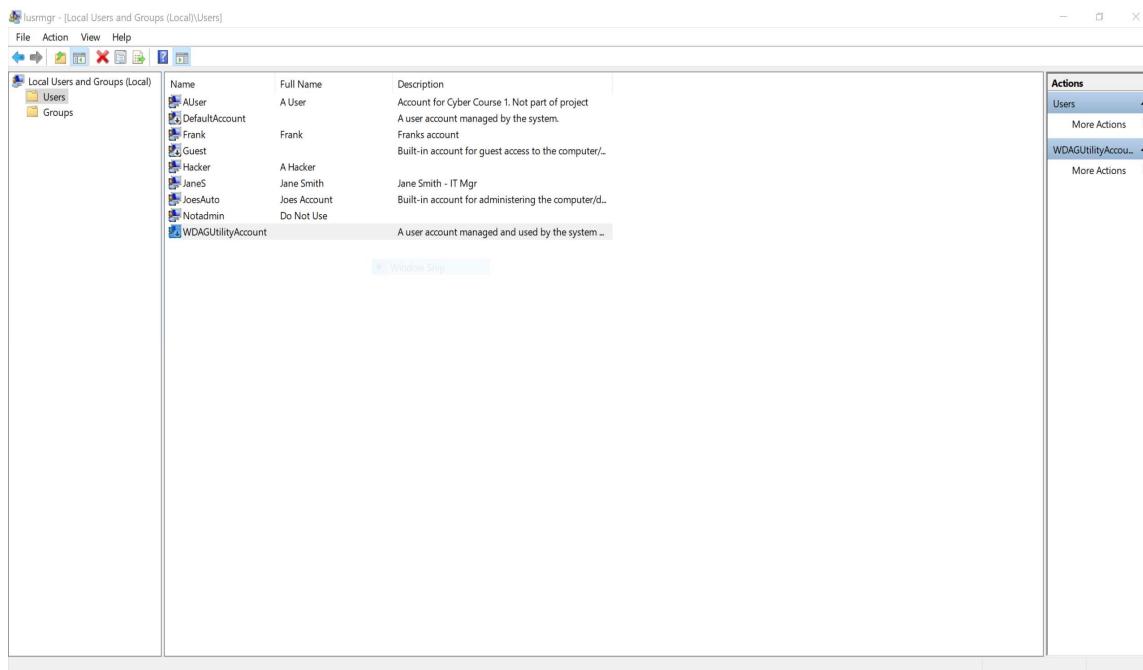
Accounts

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

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

Account Name	Full Name	Access Level
AUser	A User	users
DefaultAccount		Systems Managed accounts group
Frank	Frank	Remote Desktop user, users
Guest		Guests
Hacker	A Hacker	Administrator, Remote Desktop users, Users
JaneS	Jane Smith	Administrator, Remote Desktop users, Users
JoesAuto	Joes Account	Administrator
Notadmin	Do not use	Remote Desktop users, Users
WDAGUtilityAccount		

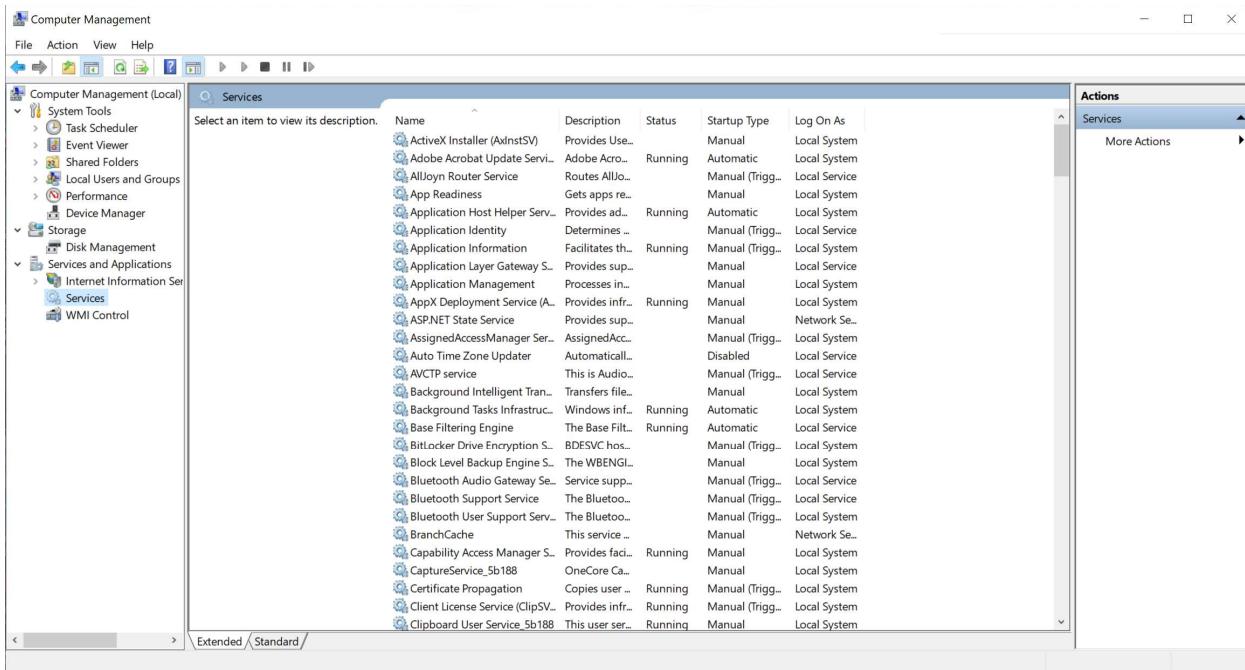
2. Provide a screenshot of the Local Users.



Services

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

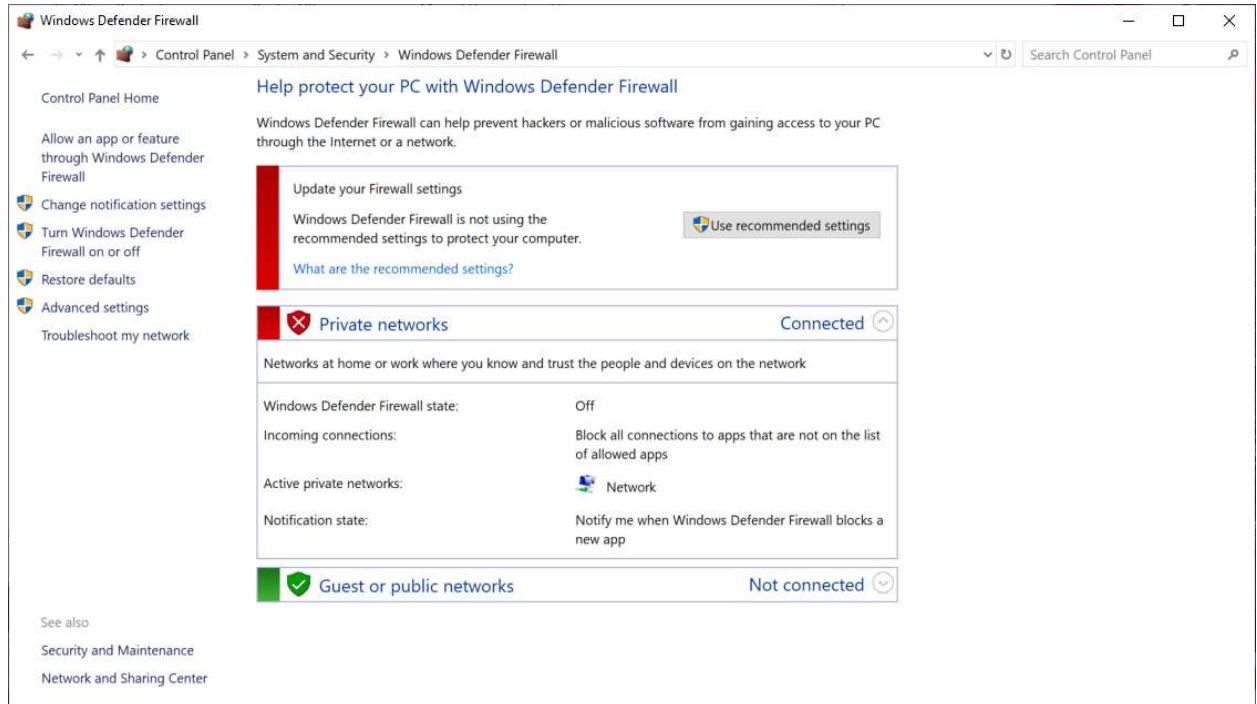
1. Provide a screenshot of the services running on this PC.



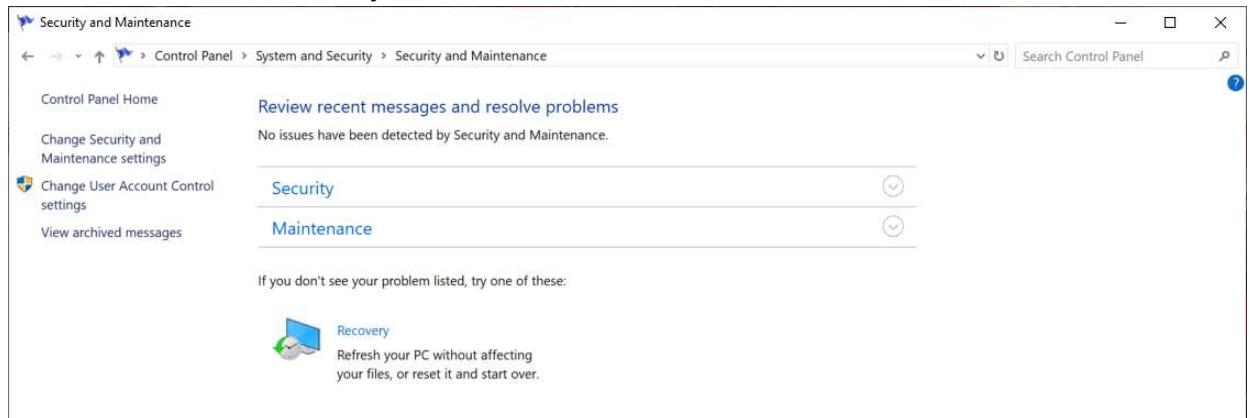
Security Services

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

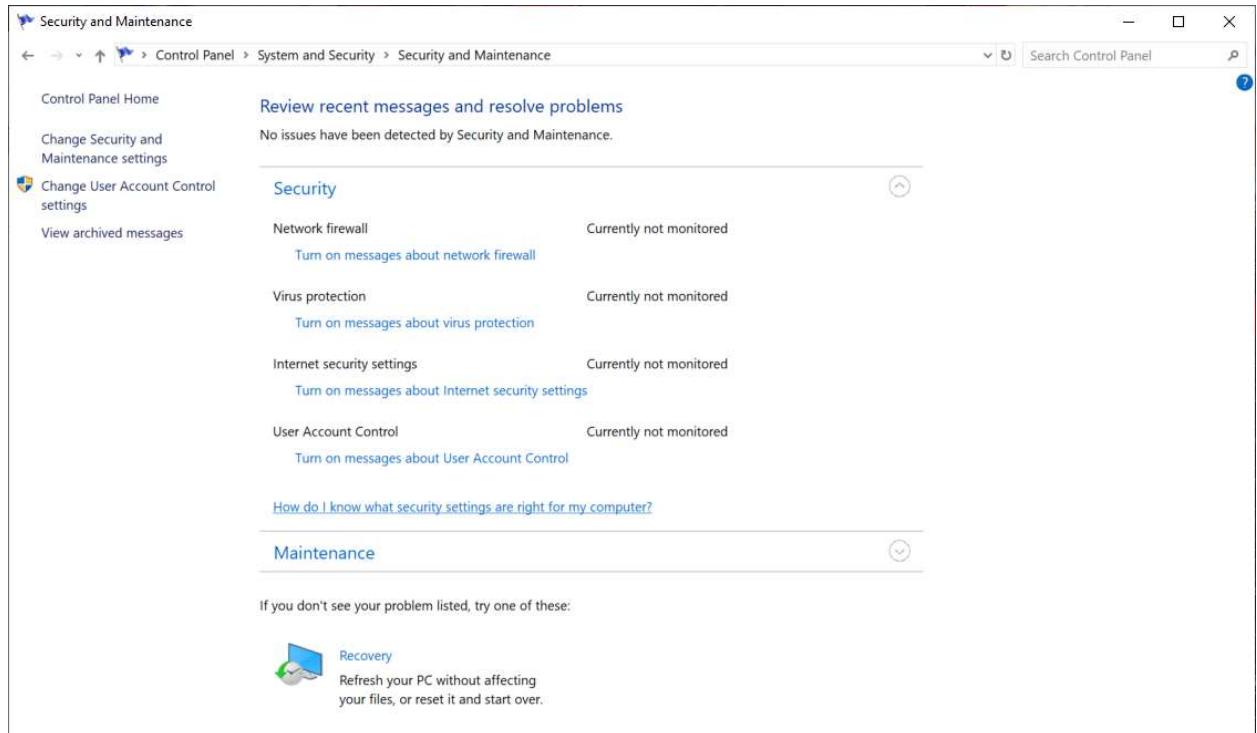
1. To view a summary of security on Windows 10, start from the **Control Panel**. Use the “Find a setting” bar and search on Windows Defender. You can also search for Windows Defender using the Windows Run bar. Take a screenshot of what you see on the Windows Security screen and include it here:



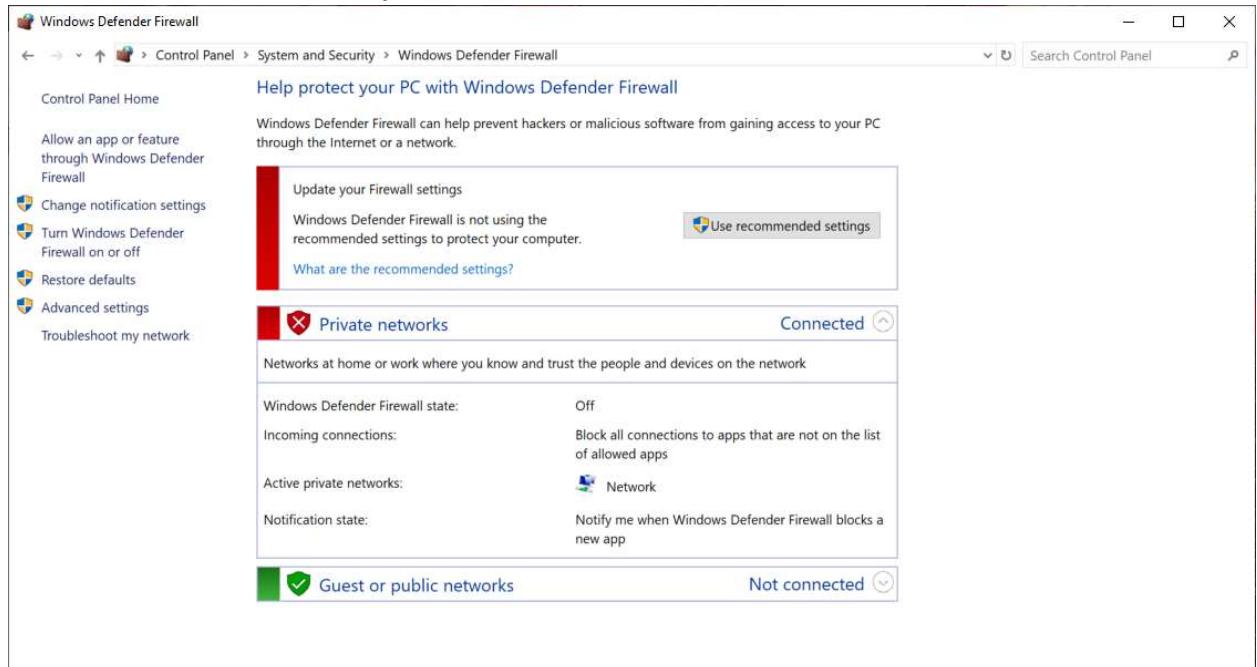
2. The Windows 10 Security settings are also found from the **Control Panel > System and Security > Security and Maintenance**. Start by viewing “**Review your computer’s status and resolve issues.**” Provide a screenshot of this below:



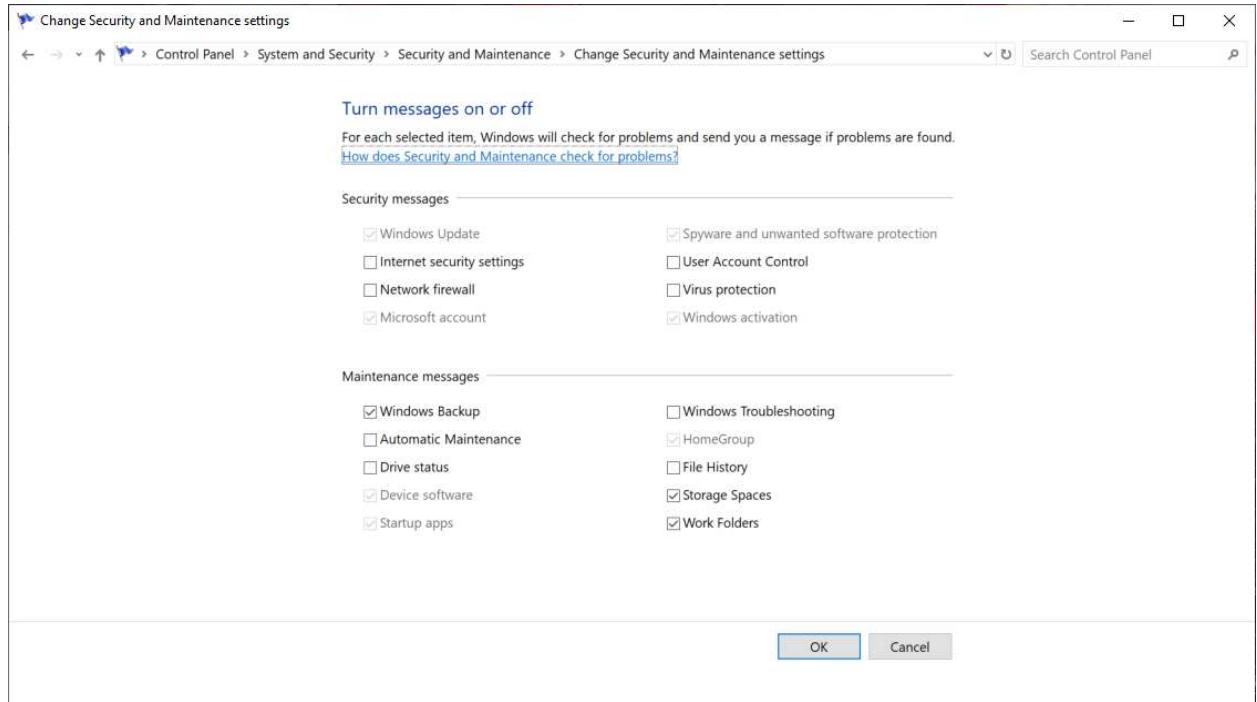
3. Click on View in Windows Security to see the status there. Provide a screenshot of the **Firewall settings**.



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



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



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

Security Feature	Status
Firewall product and status – Private network	Connected. Windows Defender Firewall stats - OFF
Firewall product and status – Public network	Not Connected. Windows Defender Firewall stats - ON
Virus protection product and status	Currently not monitored
Internet Security messages	OFF
Network firewall messages	OFF
Virus protection 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.]

- User account control is OFF – thereby every user has admin rights, which should be avoided.
- No Network Firewall – implies unauthorized access to the system isn't blocked
- Virus Protection is OFF – high risk since viruses or worm could penetrate into the system

2. Securing the PC

Baselines

Joe has asked that you follow industry standards and baselines for security settings on this system.

1. *What industry standard should Joe use for setting security policies at his organization and justify your choice?*

Joe should use the ISO/IEC 27000 series, specifically ISO/IEC 27001:2013 to set his company's security policy.

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

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

[Hint: Look in the documents folder]

Joe should consider the CIS baseline. CIS benchmarks are configuration baselines and best practices for securely configuring a system. Each of the guidance recommendations references one or more CIS controls that were developed to help organizations improve their cyberdefense capabilities. CIS controls map to many established standards and regulatory frameworks, including the NIST Cybersecurity Framework (CSF) and NIST SP 800-53, the ISO 27000 series of standards, PCI DSS, HIPAA, and others.

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?

This relates to the Basic controls where in the hardware inventory is assessed.

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

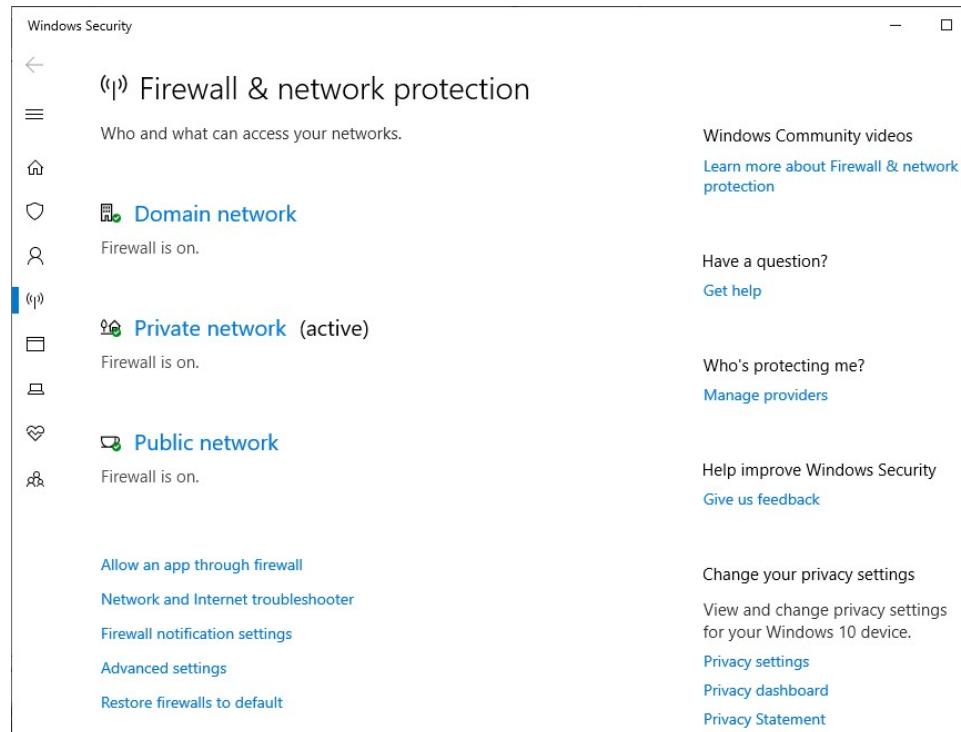
You need to ensure the Windows Firewall is enabled for all network access.

1. Explain the process you take to do this.

I will enable the default firewall defender system shipped with Windows 10.

Currently the recommended settings are not used.

2. Include screenshots showing the firewall is turned on.



3. What protection does this provide?

This will block all connections to apps that are not on the list of allowed apps.

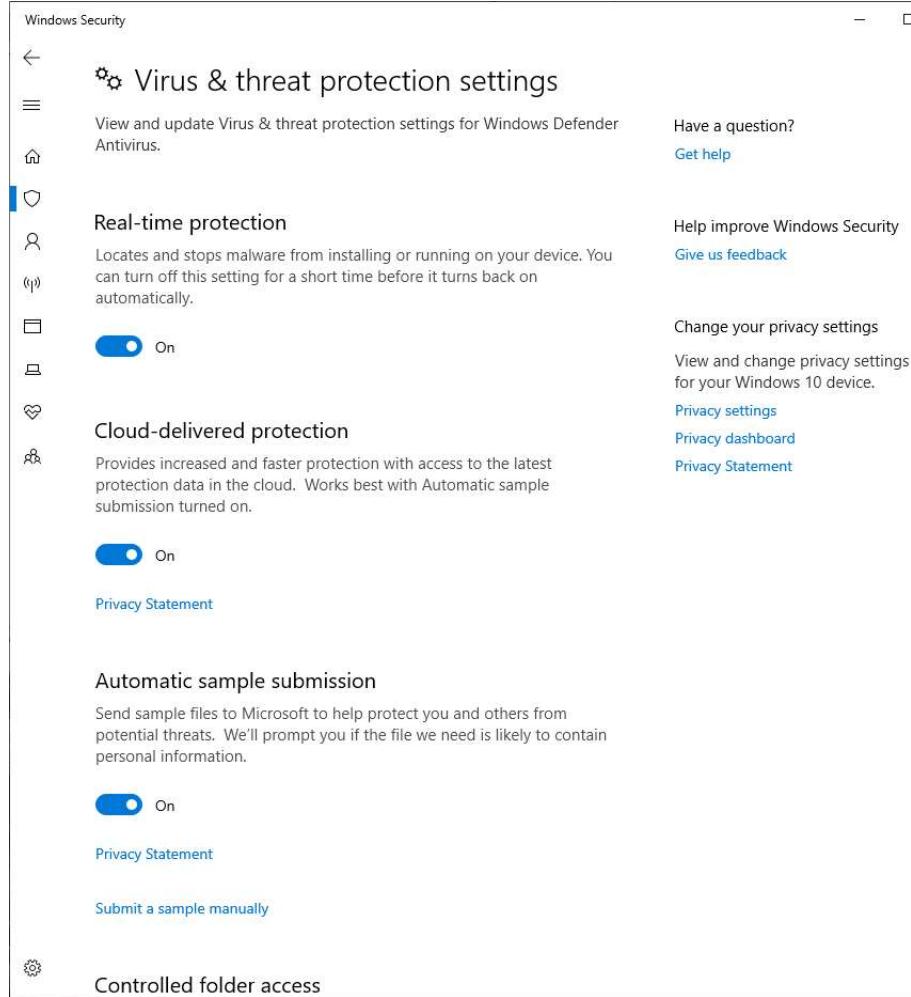
Virus & Threat Protection

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.*

We can turn on the Virus protection by navigating to Windows Security->Virus & Threat Protection and turning ON the virus protection

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



The screenshot shows the Windows Security interface. The main title is "Virus & threat protection". Below it, a sub-section titled "Current threats" indicates "No current threats" with a scan history from 9/16/2020 at 4:36 AM (quick scan). A "Quick scan" button is highlighted. Other options include "Scan options" and "Threat history". To the right, there are links for "Windows Community videos", "Learn more about Virus & threat protection", "Have a question?", "Get help", "Who's protecting me?", "Manage providers", "Help improve Windows Security", and "Give us feedback".

Virus & threat protection settings
No action needed.
[Manage settings](#)

Virus & threat protection updates
Protection definitions are up to date.
Last update: 9/16/2020 8:51 PM
[Check for updates](#)

Ransomware protection
Set up OneDrive for file recovery options in case of a ransomware attack.
[Set up OneDrive](#)

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:*
 - By turning on firewall any unauthorized external apps will be blocked from accessing the system

- By turning ON the Virus protection, any virus infection could be found out by running periodic scan and eliminate those viruses.
4. *From the CIS baseline controls, provide the controls satisfied by completing this.*

Following Basic controls are satisfied

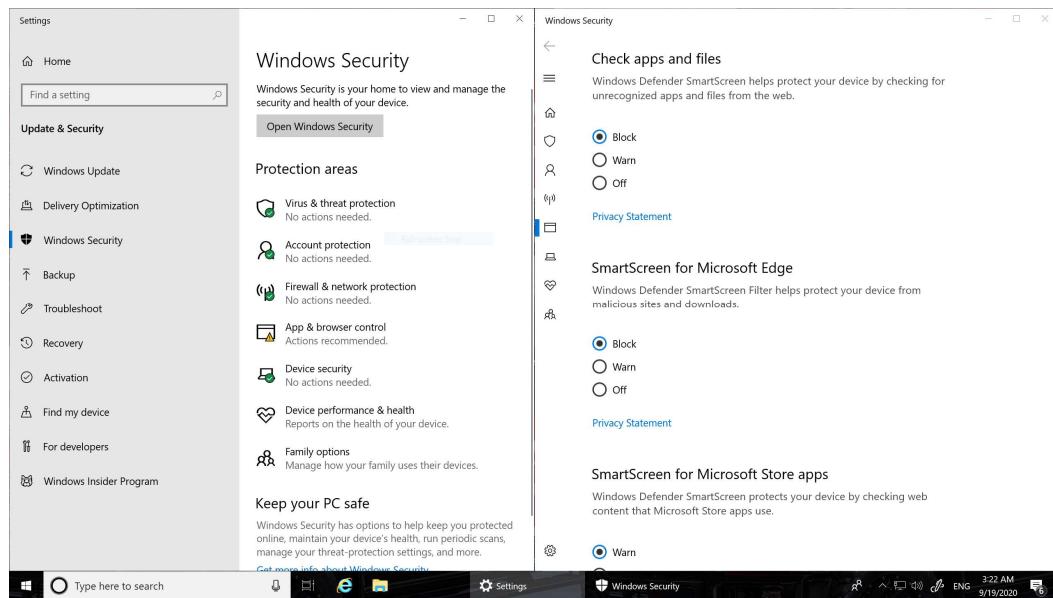
- Inventory and Control of Hardware Assets
- Inventory and Control of Software Assets
- Continuous Vulnerability Management

App & Browser Control

The App protection within Windows Defender helps to protect your device by checking for unrecognized apps and files and from malicious sites and downloads. Review the settings found within the *Account protection window, and App & browser control windows* found on the *Windows Defender Security page*.

Advanced students: You should also review the settings on the Exploit protection page.

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

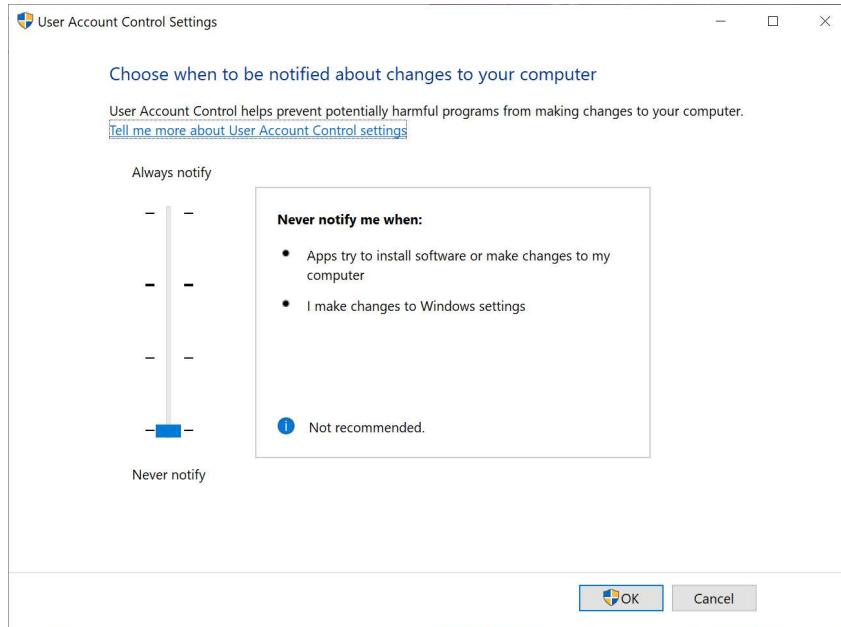


User Account Control Settings

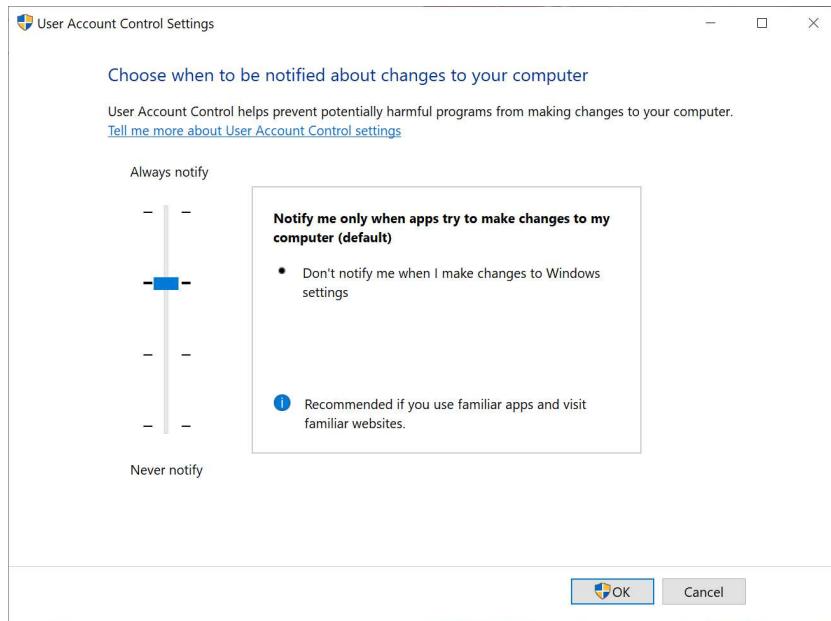
Joe wants to prevent potentially harmful programs from making changes and wants to be notified whenever apps try to make changes to his computer. This is done through the User Account Control Setting.

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

This is available from the above security settings.



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

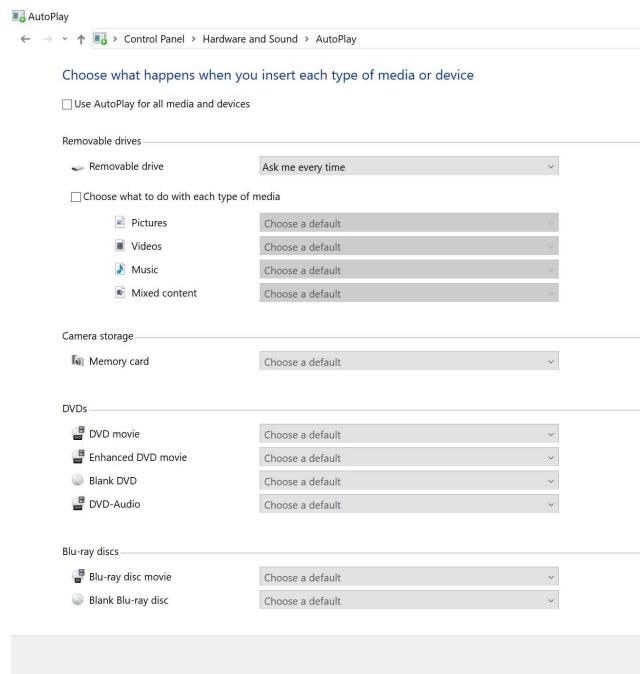


Securing Removable Media

A security best practice is to not allow the use of removable hard drives (USB sticks, Memory Cards, and DVDs). They are needed as part of Joe's backup policy. The next best thing is to make

sure that any applications don't automatically start when the media is inserted and the user is asked what should happen. This is set from the Control Panel > Hardware and Sound > Autoplay menu.

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



3. Securing Access

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

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

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

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.

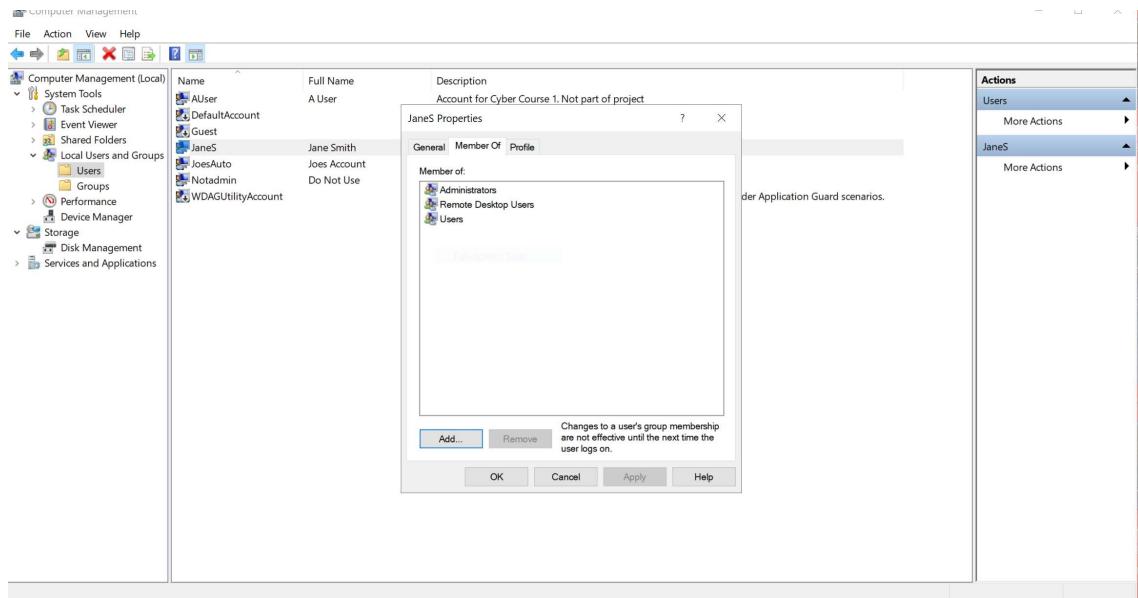
User Accounts

1. *What user accounts should not be there?*
Frank,
Hacker
2. *Bonus questions: What is Hacker's password?*
Nothing - empty
3. *Explain the steps you take to disable or remove unwanted accounts.*
Right click on the user account and delete it.
4. *Why is it important to disable or remove unneeded accounts from a PC or application? Include potential vulnerabilities and risks.*
 - *Unneeded accounts should be deleted*
 - *to prevent remote access (if that account had remote access capability)*
 - *to prevent abuse of data/information in the system by someone who has the credentials of the unneeded account*
 - *Invalid auditing logs – if someone access the system using unneeded account's credentials then it's not easy to track who actually accessed the system*

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

5. Which account(s) have administrator rights that shouldn't?
Jane Smith has admin access
6. Explain how you determined this. Provide screenshots as needed.

We could read the properties of the user account and check the 'Member of' tab to see if the user is part of the admin group.



Administrator privileges for too many users are another security challenge.

7. Provide at least three risks associated with users having administrator rights on a PC.
 - If an admin account is compromised, then the entire system's security is jeopardized. Given that, too many admin users increase the system's security risk exponentially.
 - Usually admin rights come with added responsibility – one should be mindful of the software being installed, avoid surfing the internet and use the system for personal uses that could jeopardize the system's security. They know to investigate and report possibly compromised computers. However, not everybody tends to be clued into this mindset. Application users who have admin rights tend not to be as responsible as a system admin needs to be.
 - The scope of virus infection is minimal if the infection occurred through a user account without admin access - it generally only affects that users' account on that system

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.*
Simply remove the Administrator group from the member of tab for those users who have admin access but shouldn't have them in the first place.
9. *What is the security principle behind this?*
10. The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?
This comes under 'Detect' in CIS's Basic controls list – **Controlled use of Administrative Privileges**.

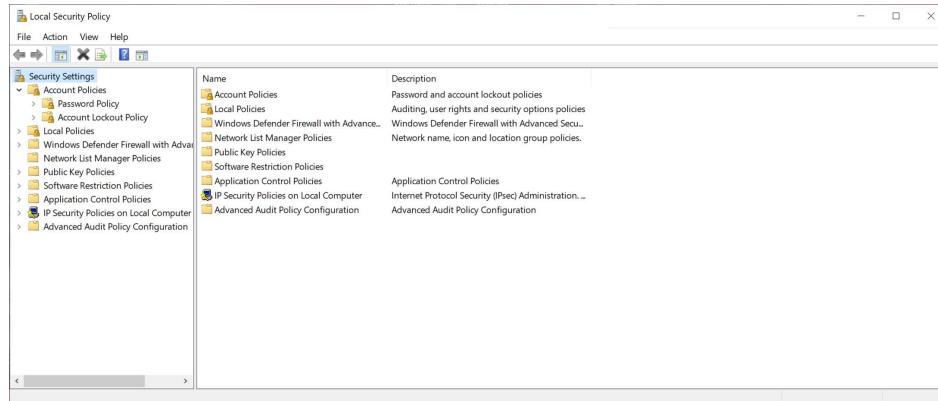
Setting Access and Authentication Policies

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.

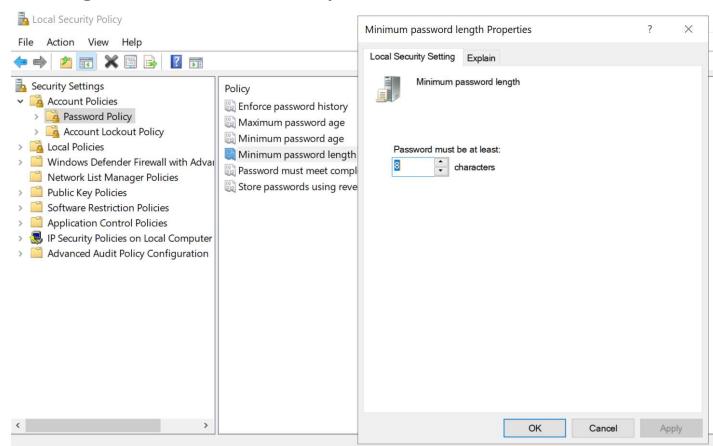
1. Provide a screenshot of the Local Security Policy window here.

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

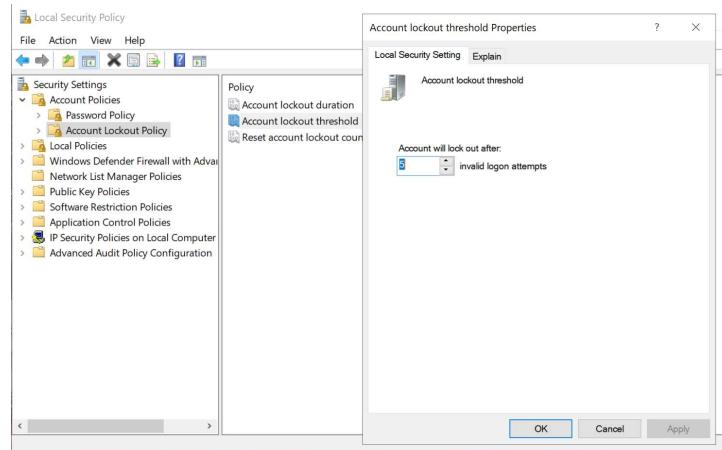


2. Explain the process for setting the password and access control policies locally on a Windows 10 PC. Provide screenshots showing how you set the rules on the PC.

- Setting the Password Policy:



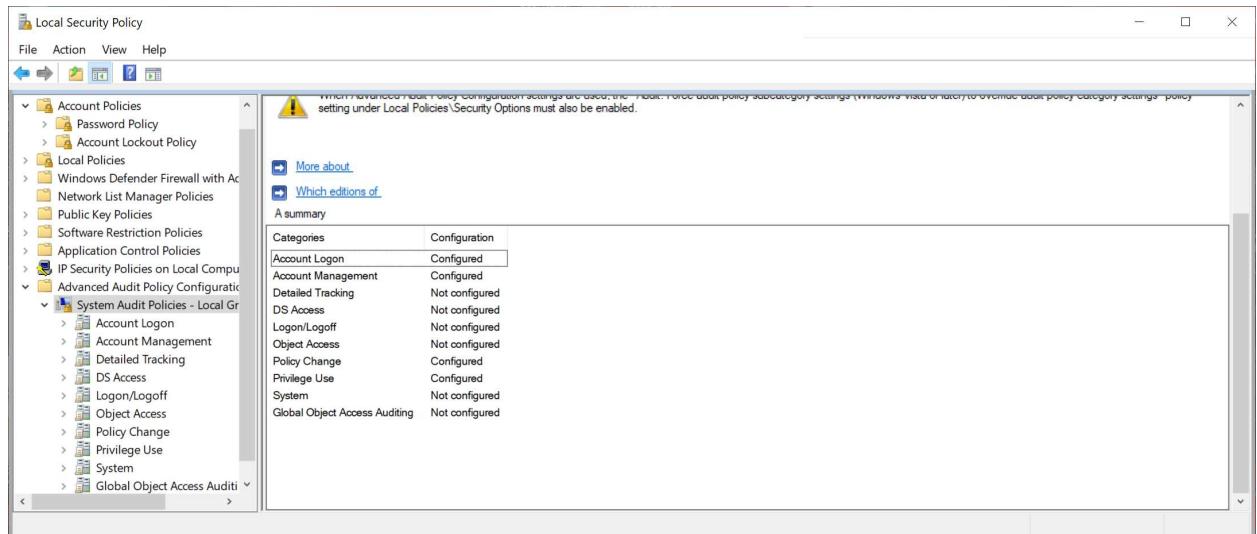
- Setting the Account Lockout Policy:



Auditing and Logging

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

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



4. Securing Applications

As part of the inventory process, you determined computer programs or applications on the PC. The next step is to decide which ones are needed for business and which ones should be removed.

Unneeded programs could be vulnerable to attacks and allow unauthorized access into the computer. They also consume system resources and could also violate licensing agreements.

Joe has established the following rules regarding PC applications:

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

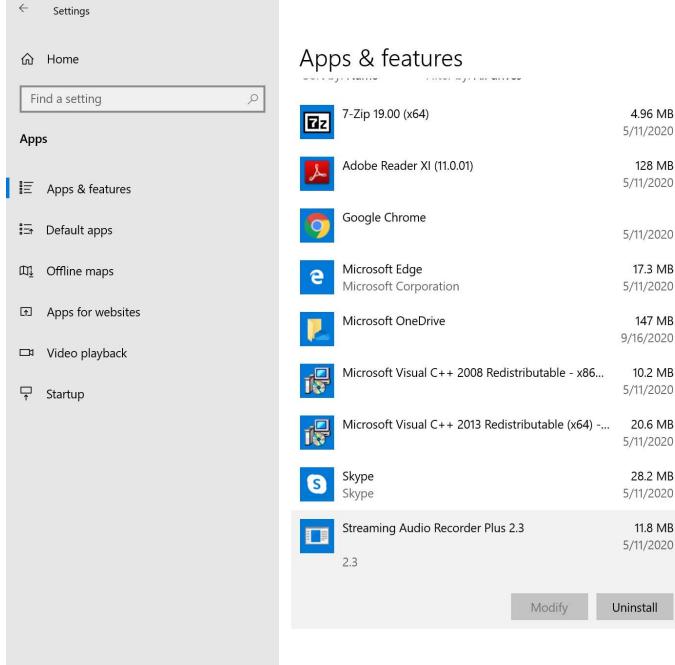
Remove unneeded or unwanted applications

1. List at least three application(s) that violate this policy.
 - Candy Crush friends
 - NMap
 - VNC server

2. *Name at least three vulnerabilities, threats or risks with having unnecessary applications:*
 - Risk = Probability of Attack x Impact of Attack and probability for attackers to gain access to your devices grows with the number of applications installed.
 - Typically, when those unnecessary applications aren't regularly updated, they expose security holes which the hackers could exploit.
 - Unnecessary apps hog valuable system resources, thereby reducing the speed of the system. It's better to remove them to increase the performance of the system.

3. *Joe wants you to make sure unneeded applications or programs are no longer on the PC. Explain the steps you take to disable or remove them. Include screenshots to show your work.*

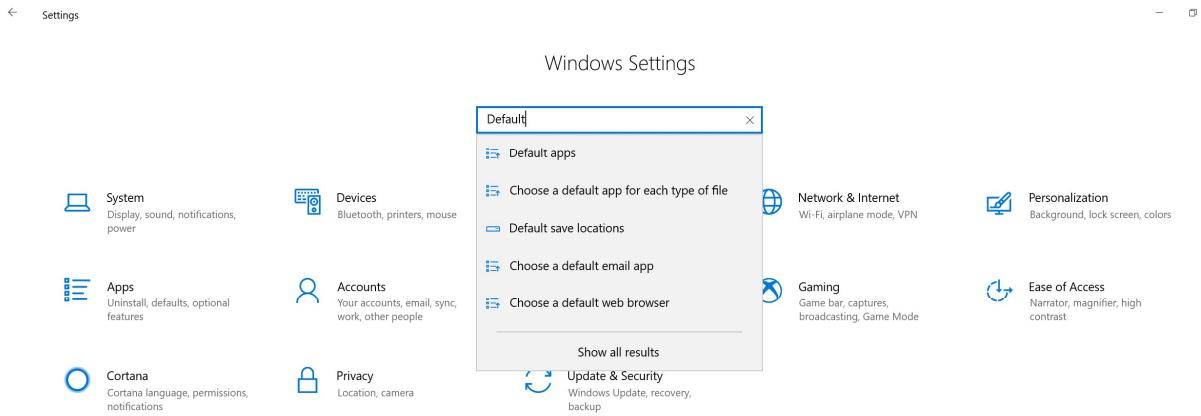
Unwanted apps could be uninstalled through the App & Features menu under Settings. Select those apps that aren't needed and simply uninstall them.



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.*
Search for 'Default' under Settings and choose the Default Apps options.



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

Reason why IE should be disabled

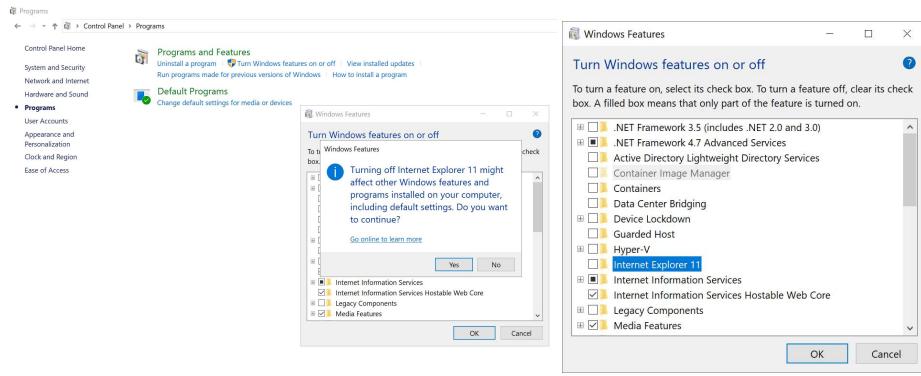
- Browser extensions are not available
- Often has issues with Google Web Apps
- Slow and crashes often

IE Vulnerabilities

- A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user (CVE-2020-1567)
- 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. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability (CVE-2016-0002)

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.

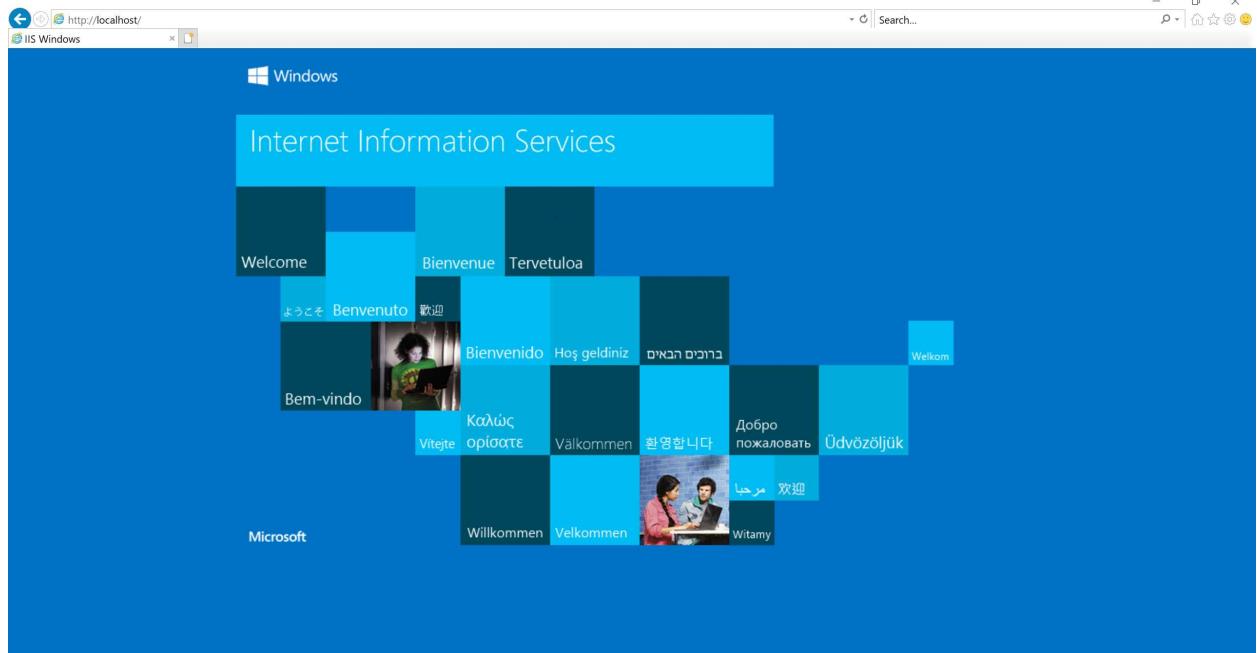


Windows Services

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.

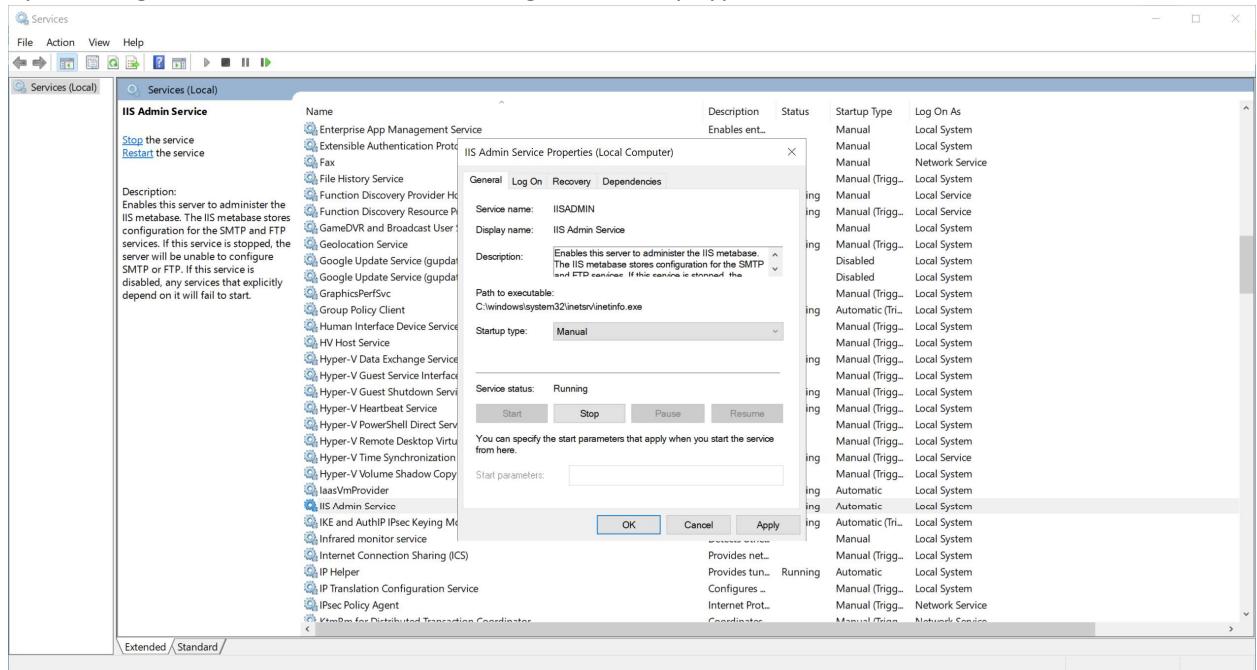
- How did you determine these services were running? Include screenshots to show how you found them.

Why I try to access 'local host' through the browser, I could access the IIS page.



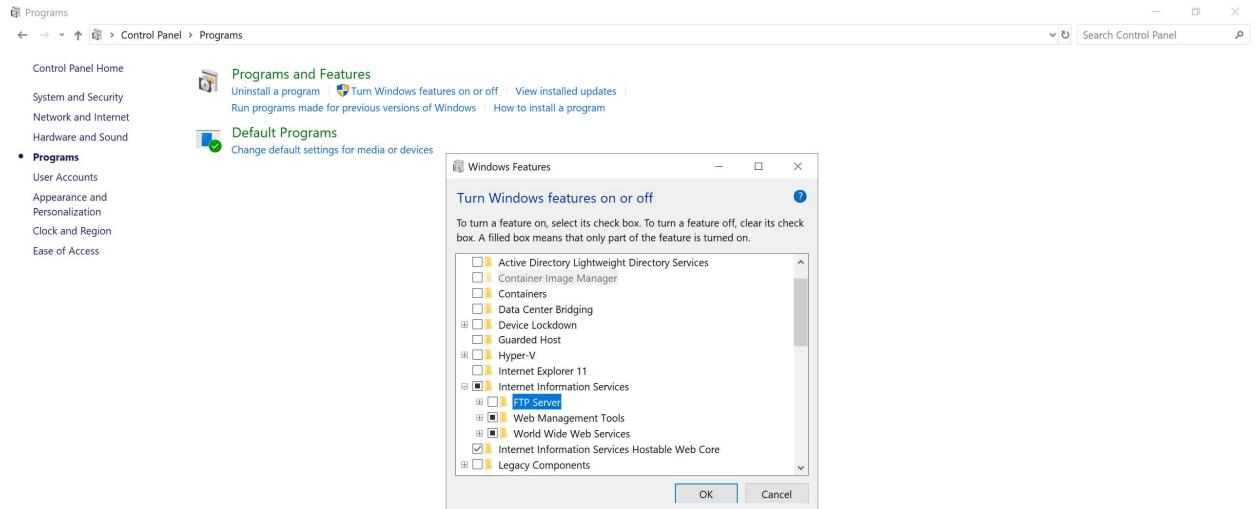
- Advanced users should provide at least two methods for determining a web server is running on a host
 - By accessing the localhost through browser
 - By checking the IIS service under the Services and Applications tab in Computer Management window
- How do you disable them and make sure they are not restarted?

by disabling the IIS from Services and setting the ‘start up type’ to manual – to avoid auto restart



- 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.

FTP service could be disabled from Windows Features as shown below

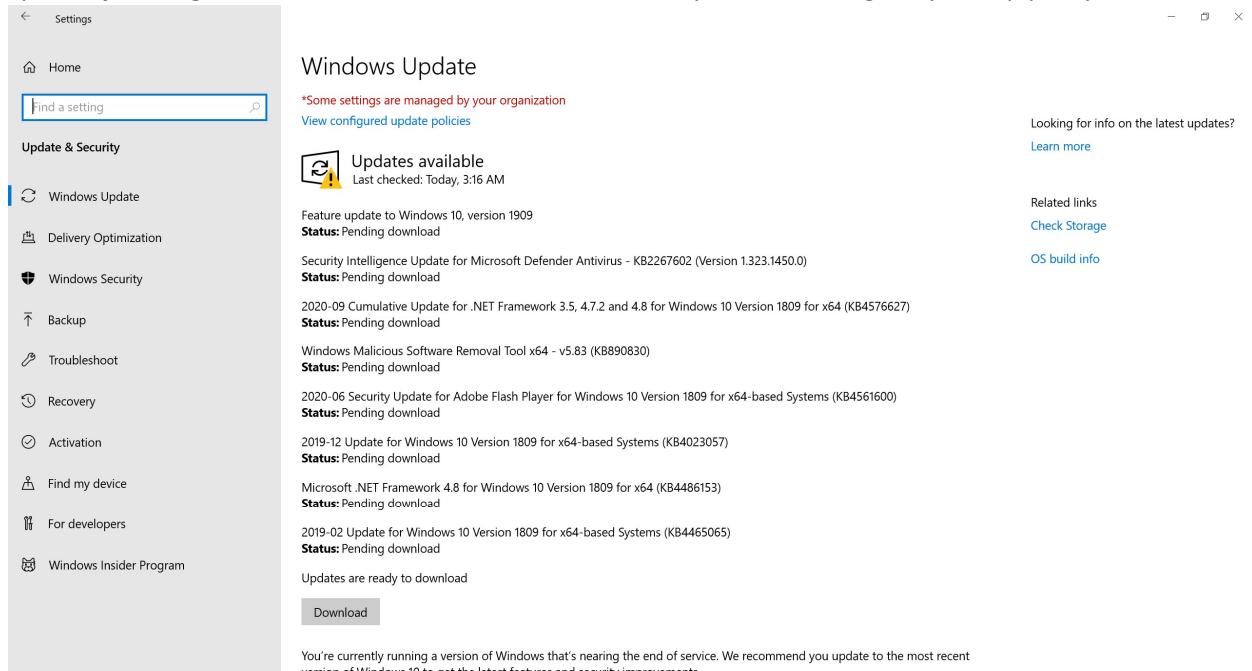


Patching and Updates

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.

Usually we set the Auto Update through Windows Update option under Update & Security option of Settings. In Joe's case it mentions the windows update is managed by Group policy.



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

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

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

- Google Chrome – 68.0.3440.84
- Adobe Reader – 11.0.01

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

Open up the applications and check their ver under 'Help -> About' menu

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

Every application provides an option to check for updates under their 'Help' menu

5. Securing Files and Folders

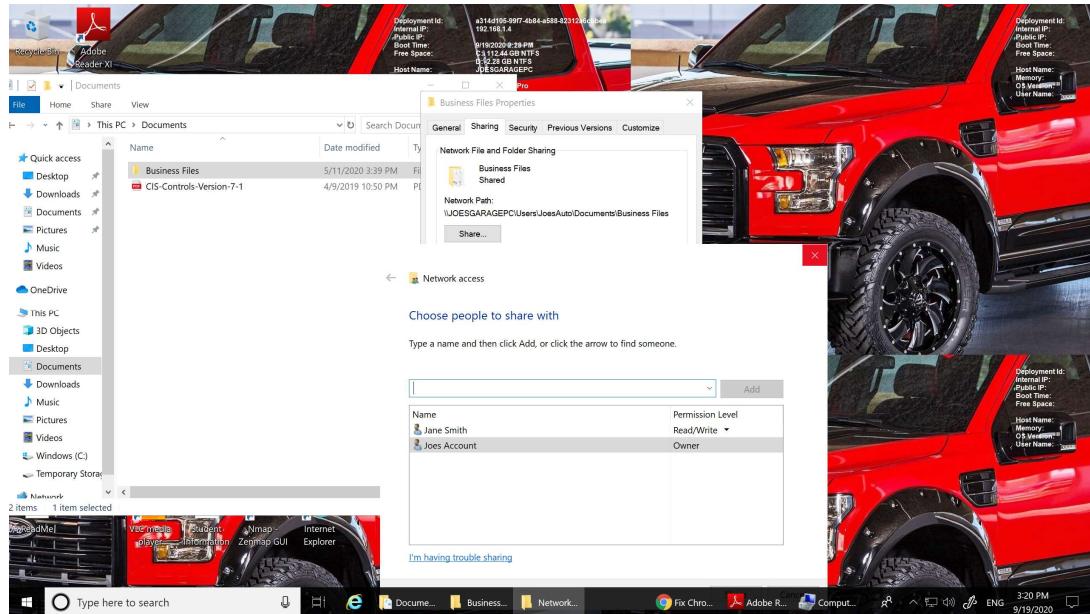
Joe has some work files in his Business folder that he wants to secure since they contain his customer information. They are labeled "JoesWork."

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.]



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.

We can encrypt the files by zipping all of them into a single compressed file secured through a password.

3. What security fundamental does this provide?

Analyze vulnerabilities and threats

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

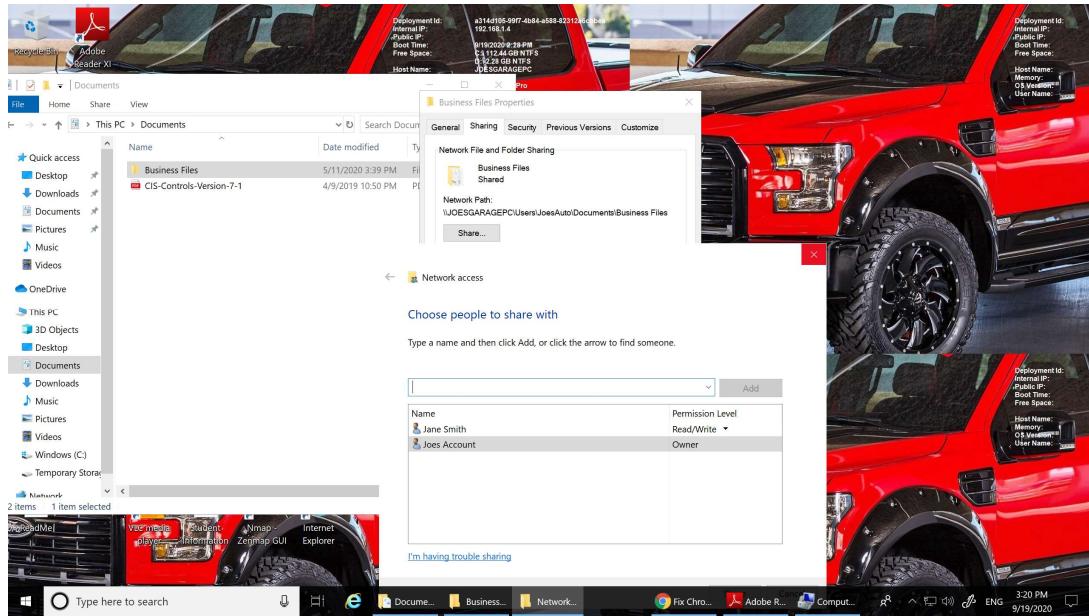
Account monitoring and control

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.

Folder sharing could be managed through the properties settings of that folder



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

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.