

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: **Simone Canty**

Date of completion: **Oct 10,2021**

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	JoesGaragePC
Processor	Intel®Xeon®Platinum 8272CL CPU @ 2.60GHz 2.59 GHz
Install RAM	4.00GB
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:

1. I went to Microsoft flag and right-clicked
2. Went to System

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

Device specifications

Device name	JoesGaragePC
Processor	Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz 2.59 GHz
Installed RAM	4.00 GB
Device ID	E5C64EC4-3404-4D29-8CE1-72C6EF2E1932
Product ID	00331-10000-00001-AA595
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Rename this PC

Windows specifications

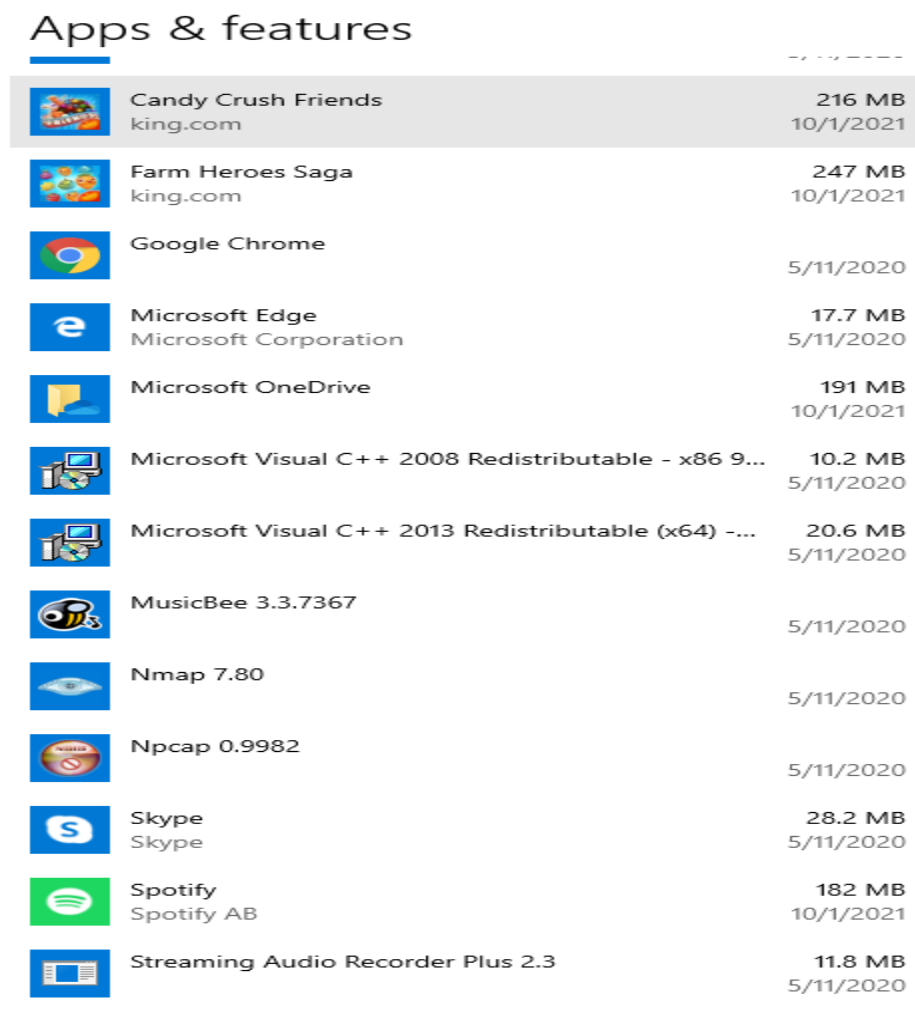
Edition	Windows 10 Pro
Version	1809
Installed on	5/11/2020
OS build	17763.1158

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:
 - Google Chrome
 - Adobe Reader XI
 - MusicBee
 - Skype
 - Spotify
2. Explain how you found this information. Provide screenshots showing this information.

1. Went to Settings-->Apps



The screenshot shows the 'Apps & features' section of the Windows Settings application. It displays a list of installed applications with their icons, names, publishers, sizes, and installation dates. The applications listed are: Candy Crush Friends, Farm Heroes Saga, Google Chrome, Microsoft Edge, Microsoft OneDrive, Microsoft Visual C++ 2008 Redistributable, Microsoft Visual C++ 2013 Redistributable, MusicBee, Nmap, Npcap, Skype, Spotify, and Streaming Audio Recorder Plus.

App Icon	App Name	Publisher	Size	Installation Date
	Candy Crush Friends	king.com	216 MB	10/1/2021
	Farm Heroes Saga	king.com	247 MB	10/1/2021
	Google Chrome			5/11/2020
	Microsoft Edge	Microsoft Corporation	17.7 MB	5/11/2020
	Microsoft OneDrive		191 MB	10/1/2021
	Microsoft Visual C++ 2008 Redistributable - x86 9...		10.2 MB	5/11/2020
	Microsoft Visual C++ 2013 Redistributable (x64) -...		20.6 MB	5/11/2020
	MusicBee 3.3.7367			5/11/2020
	Nmap 7.80			5/11/2020
	Npcap 0.9982			5/11/2020
	Skype	Skype	28.2 MB	5/11/2020
	Spotify	Spotify AB	182 MB	10/1/2021
	Streaming Audio Recorder Plus 2.3		11.8 MB	5/11/2020

3. *The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill? CIS Control 2: Inventory and Control of Software Assets*

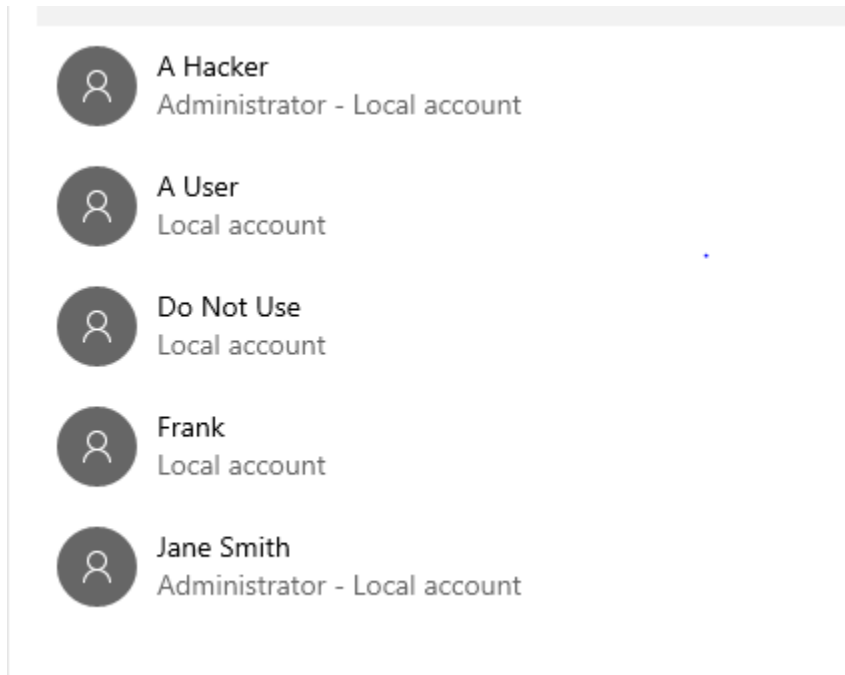
Accounts

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
Administrator	A Hacker	Administrator
Local Account	Frank	Standard User
Local Account	Jane Smith	Administrator
Local Account	A User	Standard User
Local Account	Do Not Use	Standard User
Administrator	Joe	Administrator

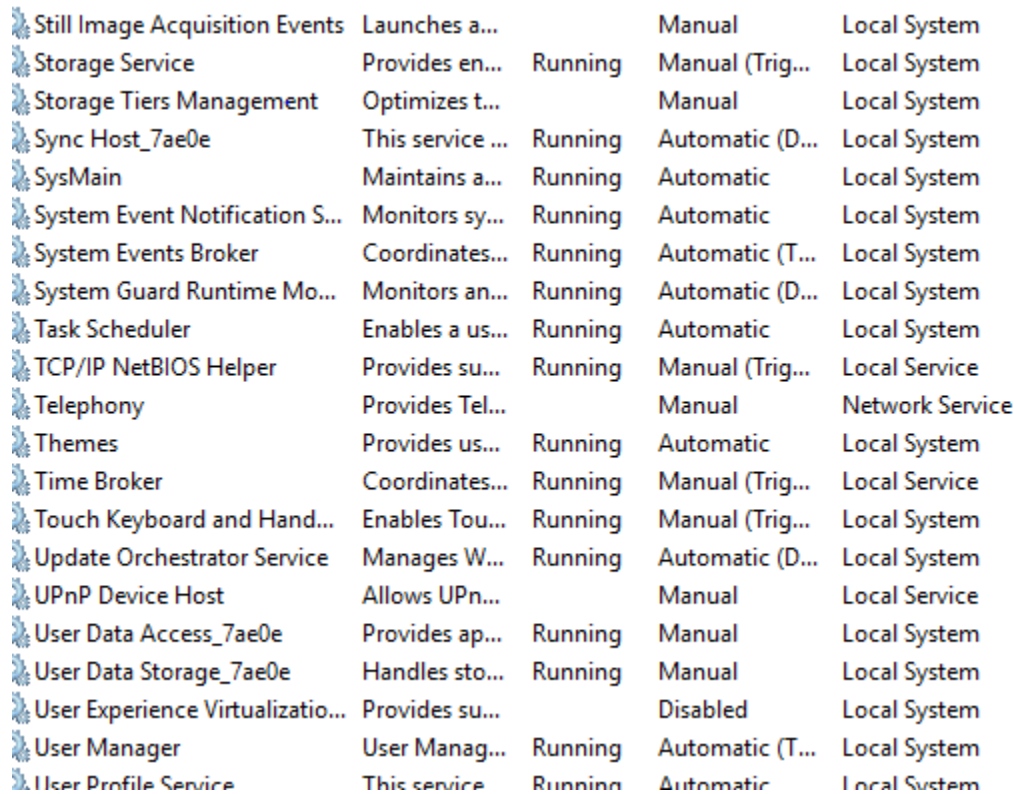
2. *Provide a screenshot of the Local Users.*



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.



Still Image Acquisition Events	Launches a...		Manual	Local System
Storage Service	Provides en...	Running	Manual (Trig...	Local System
Storage Tiers Management	Optimizes t...		Manual	Local System
Sync Host_7ae0e	This service ...	Running	Automatic (D...	Local System
SysMain	Maintains a...	Running	Automatic	Local System
System Event Notification S...	Monitors sy...	Running	Automatic	Local System
System Events Broker	Coordinates...	Running	Automatic (T...	Local System
System Guard Runtime Mo...	Monitors an...	Running	Automatic (D...	Local System
Task Scheduler	Enables a us...	Running	Automatic	Local System
TCP/IP NetBIOS Helper	Provides su...	Running	Manual (Trig...	Local Service
Telephony	Provides Tel...		Manual	Network Service
Themes	Provides us...	Running	Automatic	Local System
Time Broker	Coordinates...	Running	Manual (Trig...	Local Service
Touch Keyboard and Hand...	Enables Tou...	Running	Manual (Trig...	Local System
Update Orchestrator Service	Manages W...	Running	Automatic (D...	Local System
UPnP Device Host	Allows UPn...		Manual	Local Service
User Data Access_7ae0e	Provides ap...	Running	Manual	Local System
User Data Storage_7ae0e	Handles sto...	Running	Manual	Local System
User Experience Virtualizatio...	Provides su...		Disabled	Local System
User Manager	User Manag...	Running	Automatic (T...	Local System
User Profile Service	This service	Running	Automatic	Local System

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:


Windows Security


Windows Security is your home to view and manage the health of your device.


Open Windows Security


Protection areas


 Virus & threat protection
Actions recommended.

 Account protection
No actions needed.

 Firewall & network protection
Actions needed.

 App & browser control
Actions recommended.

 Device security
No actions needed.

 Device performance & health
No actions needed.

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:

[Review recent messages and resolve problems](#)

No issues have been detected by Security and Maintenance.

[Security](#)



[Maintenance](#)




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:

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

 Use recommended settings

[What are the recommended settings?](#)



Private networks

Connected 

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state: Off

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active private networks:  Network

Notification state: Notify me when Windows Defender Firewall blocks a new app



Guest or public networks

Not connected 

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:

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings



☐ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Defender Firewall blocks a new app



☒ Turn off Windows Defender Firewall (not recommended)

Public network settings



☒ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Defender Firewall blocks a new app

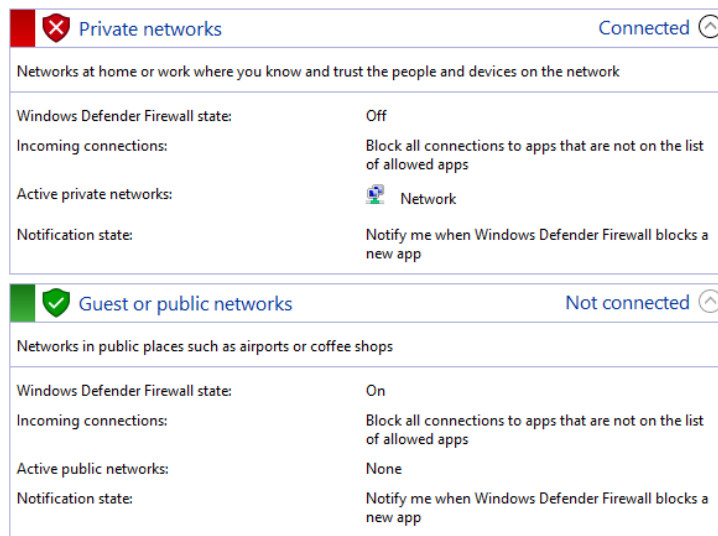


☐ Turn off Windows Defender Firewall (not recommended)

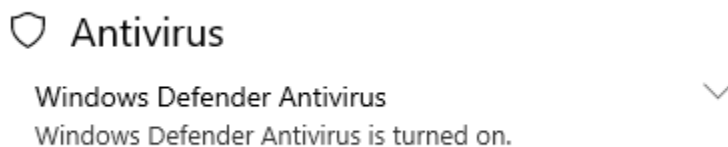
6. Document the status of the PC's security settings listed below. Include the process you used to determine this information along with any screenshots. At this point, you are only documenting what you find. Do not make changes (yet).

Security Feature	Status
Firewall product and status – Private network	Connected; Windows Defender Firewall State: Off
Firewall product and status – Public network	Not Connected; Windows Defender Firewall State: On
Virus protection product and status	Windows Defender Antivirus is turned on.
Internet Security messages	All internet security settings are set to their recommended levels
Network firewall messages	Is on
Virus protection messages	Is on
User Account Control Setting	Is off

Firewall Product and status for Private Network and Public Network: went to Control Panel >System and Security > Windows Defender Firewall



Virus Protection and Status: Setting > Windows Security> Firewall and Network Protection



Internet Security Messages: control panel >System and Security>Security and Maintenance>Security

Internet security settings

OK

All Internet security settings are set to their recommended levels.

Network Firewall Messages: Settings>Windows Security>Firewall and Network Protection>Firewall
>Open App>Firewall Notifications Settings

Firewall & network protection notifications

Notify me when Windows Defender Firewall blocks a new app

☒ On

☒ Domain firewall

☒ Private firewall

☒ Public firewall

Virus Protection Messages: Settings>Windows Security>Virus & Threat Protections>Virus & Threat
Protection Settings>Manage Settings>Notifications>Change Notification settings>Manage
Notifications

Virus & threat protection notifications

Get informational notifications

☒ On

☒ Recent activity and scan results

☒ Threats found, but no immediate action is needed

☒ Files or activities are blocked

UAC Settings: Control Panel>User Accounts>Change User Account Control Settings:

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your

[Tell me more about User Account Control settings](#)


Always notify



Never notify

Never notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

 Not recommended.

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.]

- Increase risk for virus and malware to invade systems and networks.
- Attackers have access to the same information and can take advantage of gaps between the appearance of new knowledge and remediation. This can cause an attacker to "weaponize", deploy an attack, exploit.
- There could be malicious software that an attack your systems, devices, and data.

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 use the CIS Controls. The reason is CIS controls set the standards on how organizations should set up their security operations.

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

- **CIS Controls**

[Hint: Look in the documents folder]

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?

- **CIS Controls: 5 and 15**

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.

- *Explain the process you take to do this.*
Settings>Window Security>Firewall and Network Protection
- *Include screenshots showing the firewall is turned on.*

🔒 Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

Private network (active)

Firewall is on.

Public network

Firewall is on.

- *What protection does this provide?*

This provides protection from hackers or malicious software from gaining access to your PC via internet or 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.*
Settings>Windows Security>Virus and Threat Protection>
2. *Include screenshots to confirm that anti-virus is enabled.*

Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

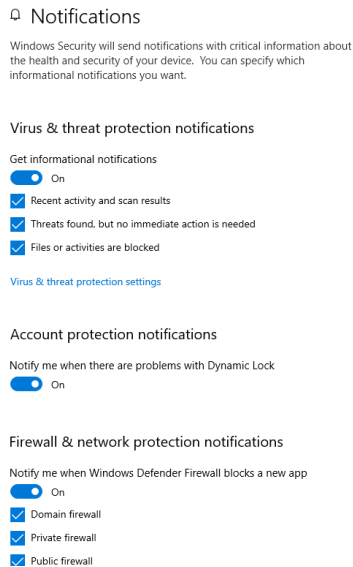
Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

 On

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:*
 - Notifies of any malicious threats/attacks on your system and will block them from further actions
 - Automatically run assessments daily to monitor systems for threats
4. *From the CIS baseline controls, provide the controls satisfied by completing this.*
 - CIS Control 8: Malware Defenses
 - CIS Control 3: 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.

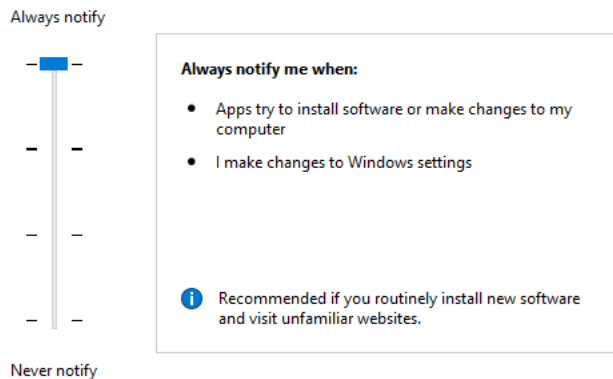
- **The current setting is Never Notify.**

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

3. **Always notify**

[Choose when to be notified about changes to your computer](#)

User Account Control helps prevent potentially harmful programs from making changes to your computer.
[Tell me more about User Account Control settings](#)



Securing Removable Media

A security best practice is to not allow the use of removable hard drives (USB sticks, Memory Cards, and DVDs). They are needed as part of Joe's backup policy. The next best thing is to make sure that any applications don't automatically start when the media is inserted and the user is asked what should happen. This is set from the Control Panel > Hardware and Sound > Autoplay menu.

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

3. Securing Access

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

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

- JoesAuto
- Jane Smith (Joe's assistant)

- A User - Used for exercises (Not used in this project)
- Notadmin - Built-in administrator account (Not used for this project)
- Windows built-in accounts: Guest, DefaultAccount, and WDAGUtility (Not used for this project)

Joe's Auto Access Rules:

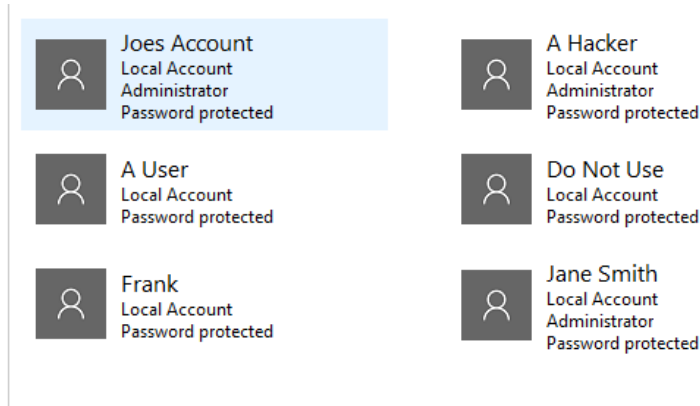
- Only JoesAuto and A User should have administrative privileges on this PC.
- Joe wants to prevent potentially harmful programs from making changes and wants to be notified whenever apps try to make changes to his computer.
- All valid users should have a password following Joe's password policy below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

User Accounts

1. *What user accounts should not be there?*
 - **A Hacker**
 - **Frank**
2. *Bonus questions: What is Hacker's password?*
 - **It is password protected**
3. *Explain the steps you take to disable or remove unwanted accounts.*
Control panel > User Accounts>User Accounts> Manage accounts
4. *Why is it important to disable or remove unneeded accounts from a PC or application? Include potential vulnerabilities and risks.*
 - **Former employees or a malicious insider can use these inactive accounts for malicious purposes, obtain sensitive information, and access to an organization's computing system.**
 - **Attackers can use inactive user accounts to become legitimate users, therefore, resulting access to potential sensitive data or implementing malicious attacks that can affect the organization's system/network.**

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?
 - A Hacker
6. Explain how you determined this. Provide screenshots as needed.
 - Control Panel>User Accounts>User Accounts>Manage Accounts



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 a user's account has administrative privileges, an attacker can take over the user's account and install malicious software to obtain administrative passwords and/or sensitive data.**
 - **If a user is using the administrative privileges and they open a malicious email attachment or download a file from a malicious website, the attachment or file may have a exploitable code/virus that can automatically run on the organization's network causing harm.**
 - **If administrative privileges are used loosely, attackers can easily gain full total of an organization's 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.*
 - Control Panel>User Accounts>User Accounts>Manage Accounts>Change an Account > Change the Account Type

Choose a new account type for A Hacker



A Hacker
Local Account
Administrator
Password protected

☒ **Standard**

Standard accounts can use most software and change system settings that don't affect other users or the security of this PC.

☐ **Administrator**

Administrators have complete control over the PC. They can change any settings and access all of the files and programs stored on the PC.

9. What is the security principle behind this?

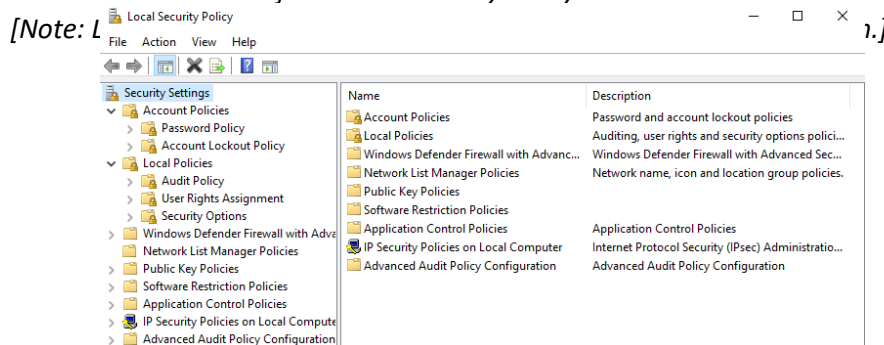
- To give user the least privilege/access necessary.

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






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:
 - Local Security Policy>Account Policies>Password Policy>Password must meet complexity requirements>change to Enable
 - Local Security Policy>Account Policies>Password Policy>Minimum password length>8 characters
 - Local Security Policy>Account Policies>Password Policy>Minimum password age>120 days

- **Local Security Policy>Account Policies>Password Policy>Enforce password history>change to 5 passwords remembered.**

Policy	Security Setting
 Enforce password history	5 passwords remembered
 Maximum password age	0
 Minimum password age	120 days
 Minimum password length	8 characters
 Password must meet complexity requirements	Enabled
 Store passwords using reversible encryption	Disabled










- Setting the Account Lockout Policy:
 - **Local Security Policy>Account Policies>Account Lockout Policy>Account Lockout Threshold>change to 5 invalid logon attempts**

Policy	Security Setting
 Account lockout duration	30 minutes
 Account lockout threshold	5 invalid logon attempts
 Reset account lockout counter after	30 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
 Audit account management	Success
 Audit directory service access	No auditing
 Audit logon events	Success
 Audit object access	No auditing
 Audit policy change	Success
 Audit privilege use	Success
 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.*
 - **MusicBee**
 - **Spotify**
 - **Candy Crush Friends**
2. *Name at least three vulnerabilities, threats or risks with having unnecessary applications:*
 - **Attackers can take advantage of vulnerabilities found in application software**
 - **There can be vulnerabilities such as coding mistakes/errors, logic errors or failure to test for unusual conditions, which can increase the risk of an attacker to use these vulnerabilities for exploitation**
 - **There is the potential for unnecessary applications not being updated with the necessary security patches to prevent vulnerabilities from affecting the organization’s system and network.**
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.*
 - Settings>Apps>Click on the App you want to uninstall/remove>Click on the Uninstall button

	Adobe Reader XI (11.0.01)	128 MB 5/11/2020
	Google Chrome	5/11/2020
	Microsoft Edge Microsoft Corporation	17.3 MB 5/11/2020
	Microsoft OneDrive	191 MB 10/8/2021
	Microsoft Visual C++ 2008 Redistributable - x86 9...	10.2 MB 5/11/2020
	Microsoft Visual C++ 2013 Redistributable (x64) -...	20.6 MB 5/11/2020
	Nmap 7.80	5/11/2020
	Npcap 0.9982	5/11/2020

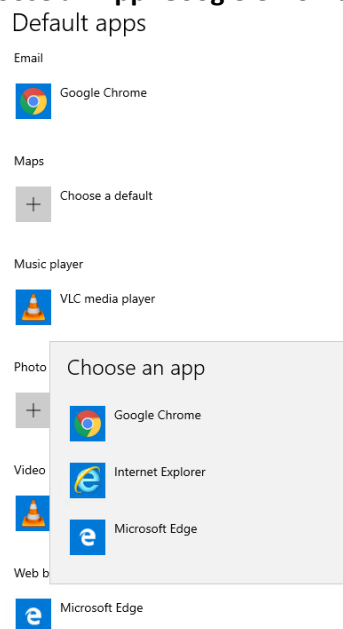
Cybersecurity ND #:

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.*

- **Settings>Apps>Select Default Apps>Web Browser>click on the Web Browser in use>Choose an App>Google Chrome**

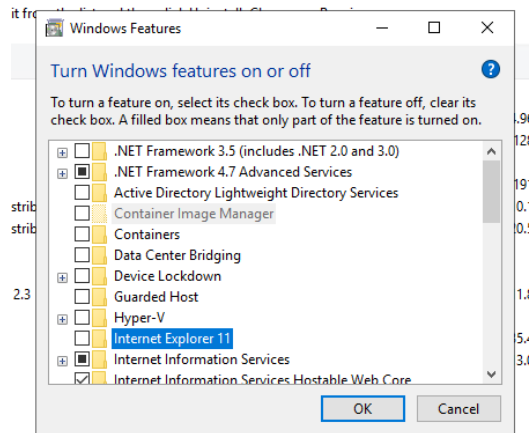


2. *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
 - It is a web browser application that is not going to be used and therefore, it may not receive any updates including security updates/patches and this may increase an attacker's chance of exploiting a vulnerability on your system

- Web Browsers can be targets for social engineering and malicious code exploitation due to users using untrusted websites increasing the risk of vulnerabilities and attacks to a system and/or network. Therefore, you don't want to have several web browsers being used on your system.

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.*

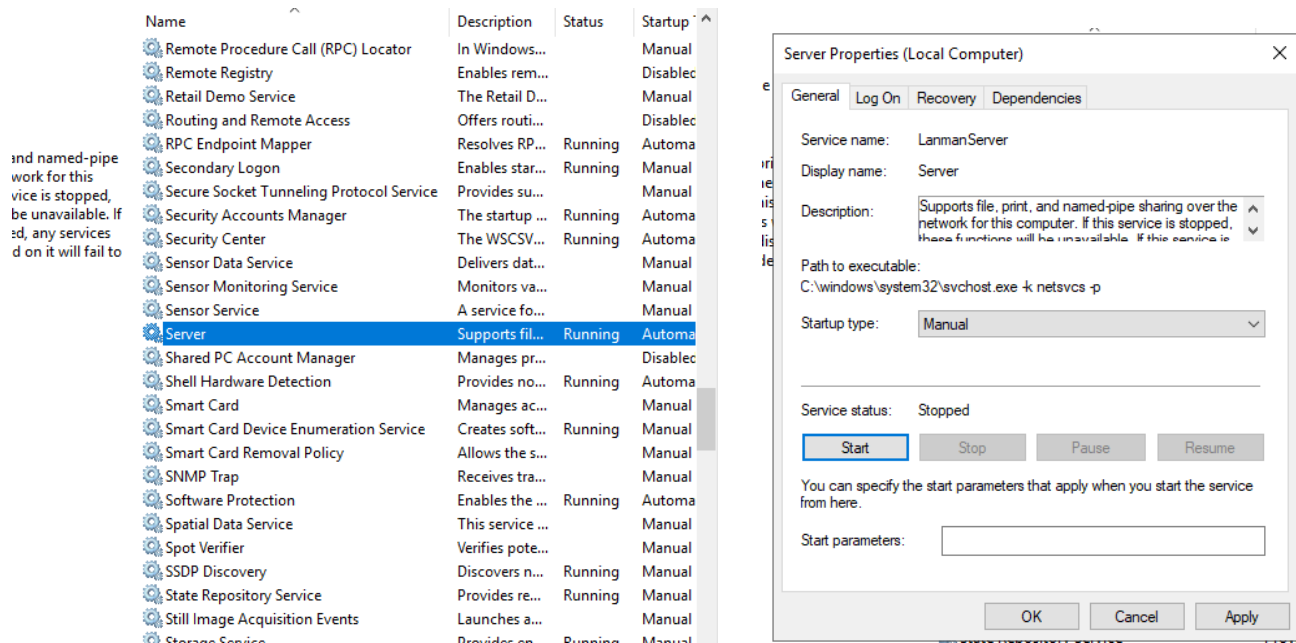


Windows Services

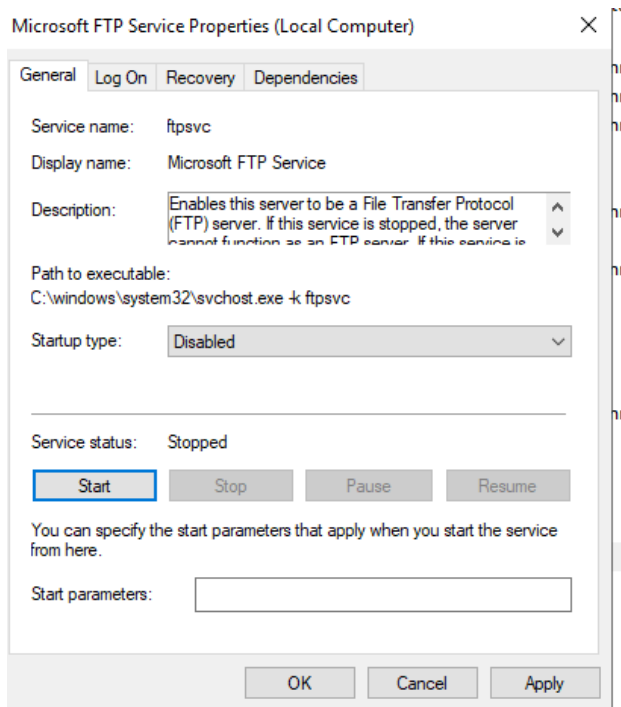
There are Windows features running on Joe's computer that could allow unwanted activity or files. He suspects that someone may have used the PC as a web server in the past. Joe wants you to confirm if web services are turned on, stop it if it is and make sure it is not running whenever the computer restarts.

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

Computer Management>Services and Application>Services>Server



2. Advanced users should provide at least two methods for determining a web server is running on a host
 - **Computer Management>Services and Applications**
 - **Windows (C) >search Windows (c)**
3. How do you disable them and make sure they are not restarted?
 - **Change to the Startup type: Disabled or Manual;**
 - **Change the Service Status to Stopped**
4. Advanced Users: The File Transfer Protocol FTP service is also running on this PC and shouldn't. Explain the process for disabling it and ensuring it is not automatically restarted.
 - **Computer Management>Services>Microsoft FTP Service>Change Startup Type to Disabled >Change Service Status to Stop> Apply>Ok**

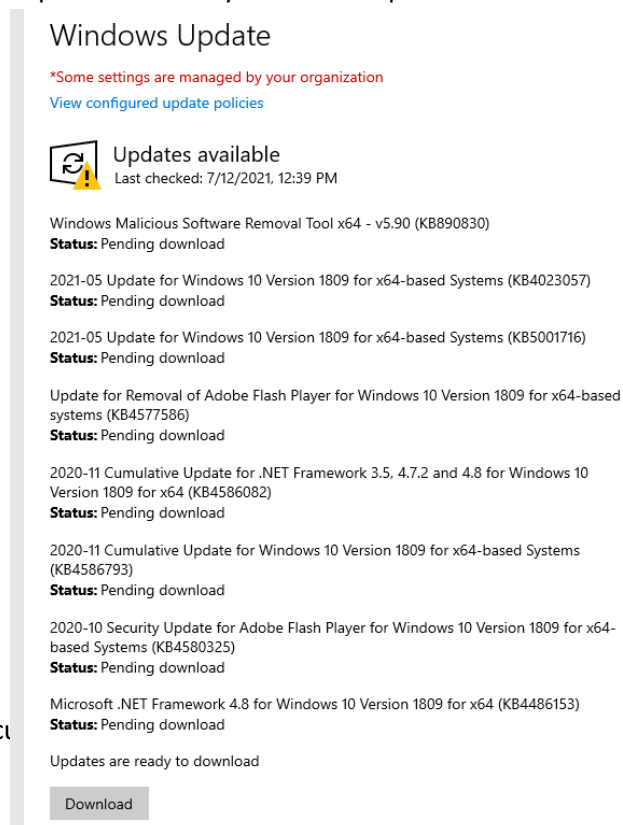


Patching and Updates

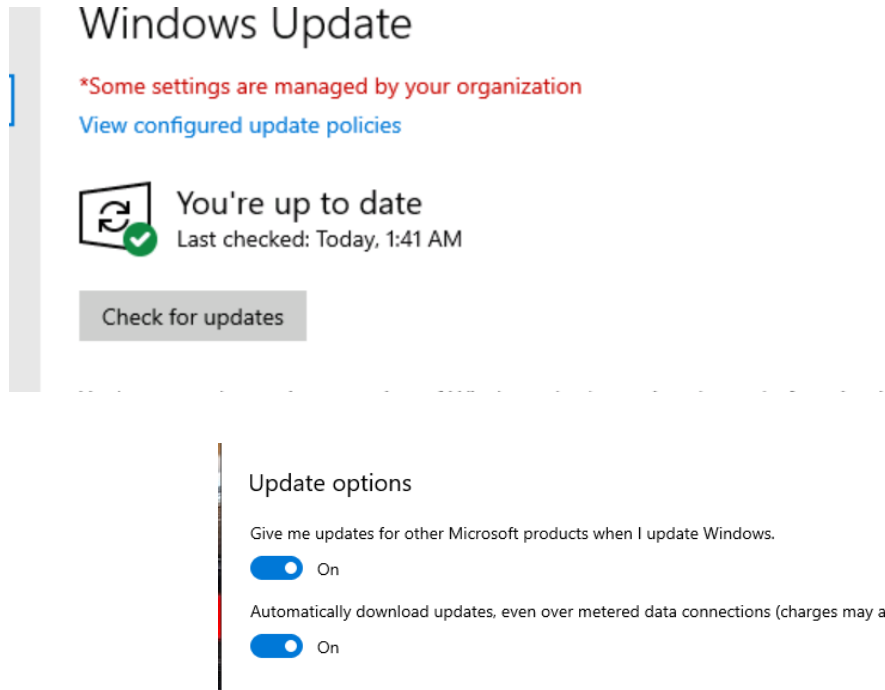
Keeping the operating system current on patches and fixes is a critical part of security. Joe wants his PC to be on the latest version of Windows 10. He also wants you to set it up for automated updates.

- Explain the process for doing this. Include screenshots as needed.

Settings > Update & Security > Windows Updates



- 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.

- List at least two applications on Joe's PC that are out of date. List them below:
 - **VLC Player on the PC version 2.2.2...Vendor website Version 3.0.16**



VLC media player

VideoLAN

5/11/2020

2.2.2

VLC media player

VLC is a free and open source cross-platform multimedia player and framework that plays most multimedia files as well as DVDs, Audio CDs, VCDs, and various streaming protocols.

Download VLC

Version 3.0.16 • Windows 64bit • 40 MB
74,553,401 downloads so far

- **Adobe Reader on the PC version 11.0.01...Vendor website 11.0.023**



Adobe Reader XI (11.0.01)

Adobe Systems Incorporated

5/11/2020

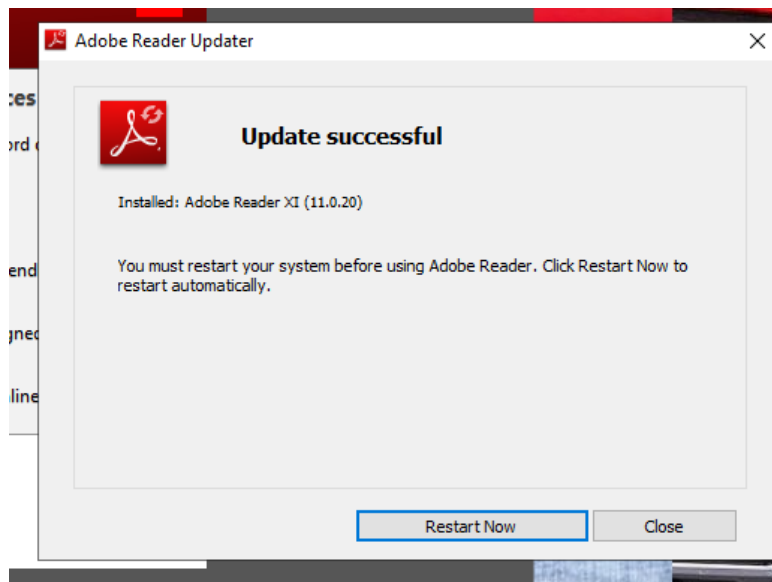
128 MB

11.0.01

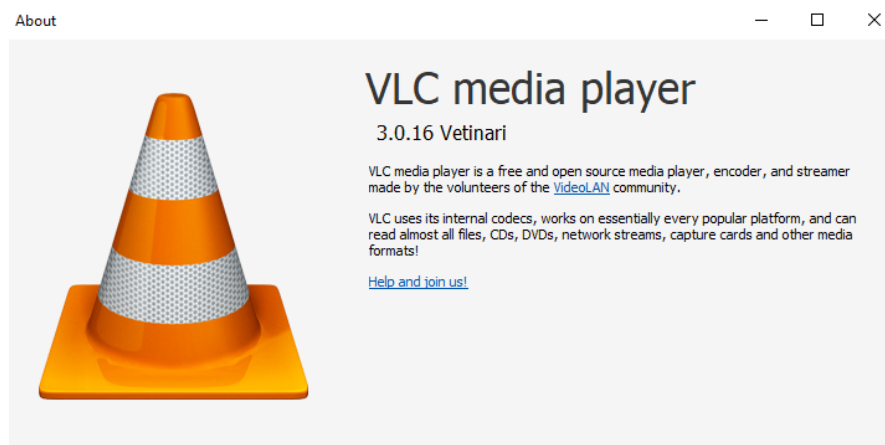
Adobe Reader XI 11.0.23 on 32-bit and 64-bit PCs

- *Explain the steps you took to determine this information.*
 - **Control Panel>Programs >Programs and Features>Look at the version>go the Vendors website to see the latest downloadable version**
- *Explain the steps for updating each of these applications. Include screenshots as needed.*

Adobe XI: Open application>Help>Check for Updates>Install update



VLC Player: Open Application>Help>Check for Updates>Install Update



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.]

- **File Explorer>This PC>documents>Business Files folder>Joes Work files>right clicked>Properties>Sharing>Share>Choose people to share with**

Name	Date modified	Type	Size
Joes Work File April 2020	4/25/2020 9:44 PM	Office Open XML ...	13 KB
Joes Work File March 2020	4/25/2020 9:46 PM	Office Open XML ...	13 KB
Joes Work File May 2020			

← Network access

Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

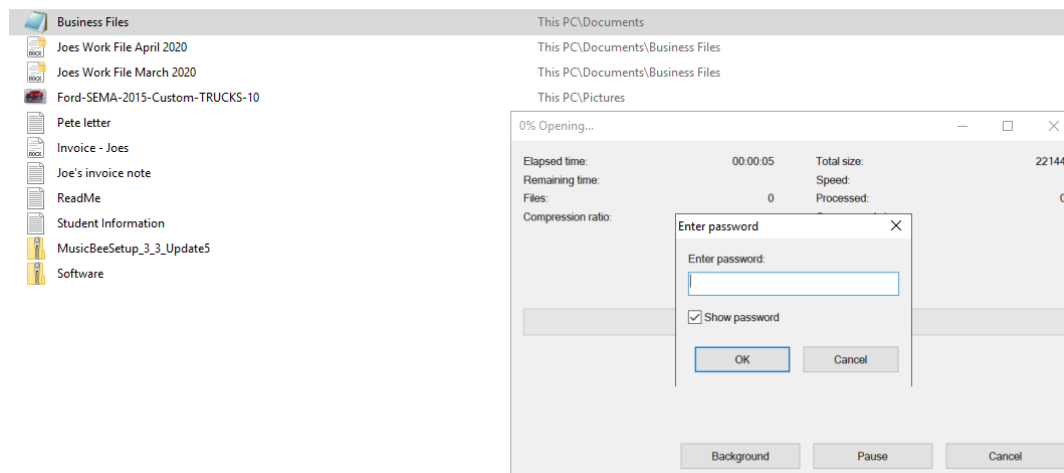
Name	Permission Level
Jane Smith	Read/Write
Joes Account	Owner

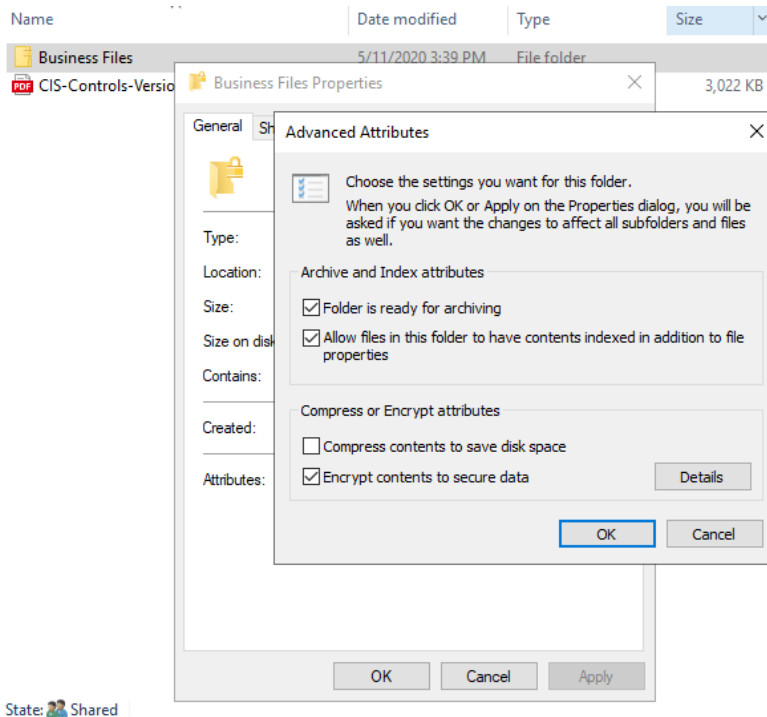
[I'm having trouble sharing](#)

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.

- Highlight folder>right-click>properties>Advanced>Check Encrypt contents to secure data>ok>Apply>Ok

Recent files (11)





3. *What security fundamental does this provide?*

- **Confidentiality**

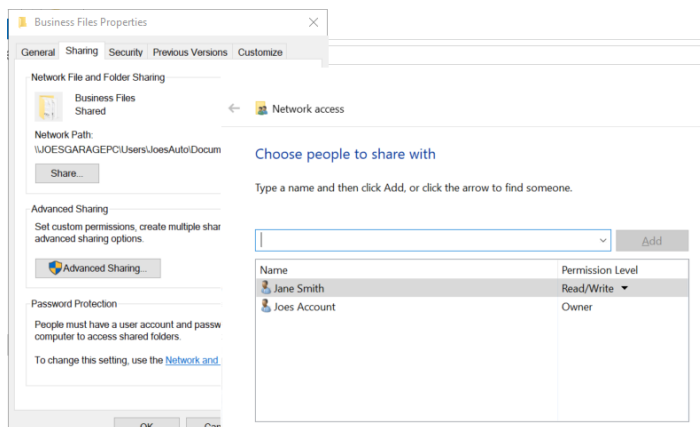
4. *The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill? **CIS Control 13: Data Protection***

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.

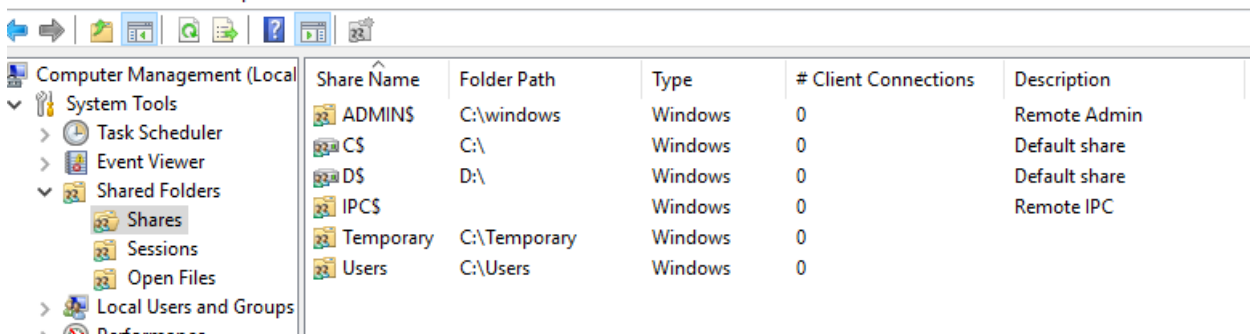
1. *Explain how you would do that and provide a screenshot showing how you can do it. Make sure it's only shared between Joe and Jane.*

- **File Explorer>This PC>documents>Business Files folder> >right clicked>Properties>Sharing>Share>Choose people to share with**



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



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.