Udacity Cybersecurity Course #1 Project

Contents

Learning Objectives:

- Explain security fundamentals including core security principles, critical security controls, and cybersecurity best practices.
- Evaluate specific security techniques used to administer a system that meets industry standards and core controls
- Assess high-level risks, vulnerabilities and attack vectors of a sample system
- Explain methods for establishing and maintaining the security of a network, computing environment, and application.

Student Information

Student Name: 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.***

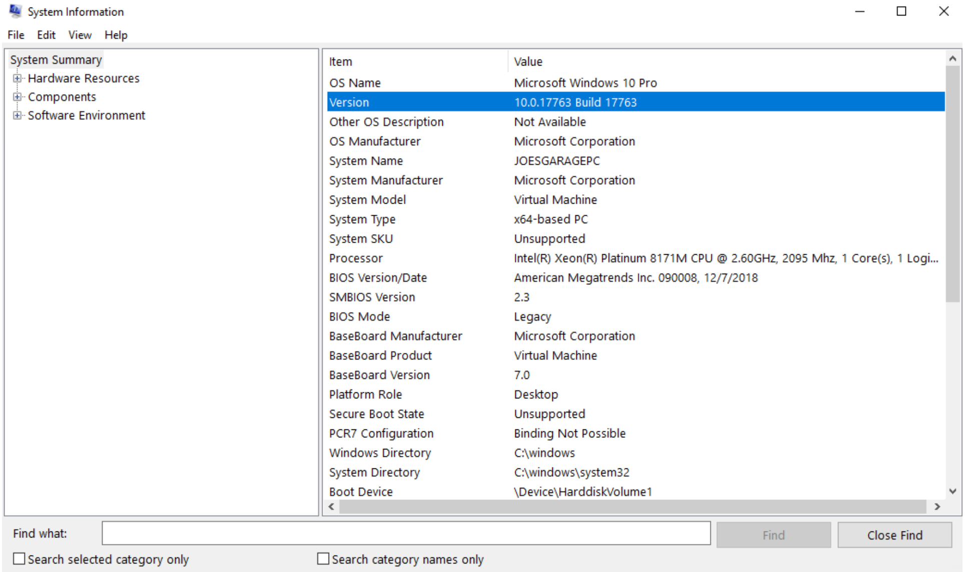
Device Name	JoesGragePC
Processor	Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz, 2095 Mhz, 1 Core(s), 1 Logical Processor(s)
Install RAM	1.00 GB
System Type	x64-based PC
Windows Edition	Microsoft Windows 10 Pro
Version	10.0.17763 N/A Build 17763
Installed on	5/11/2020, 10:55:54 AM
OS build	17763.1158

2. ***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.

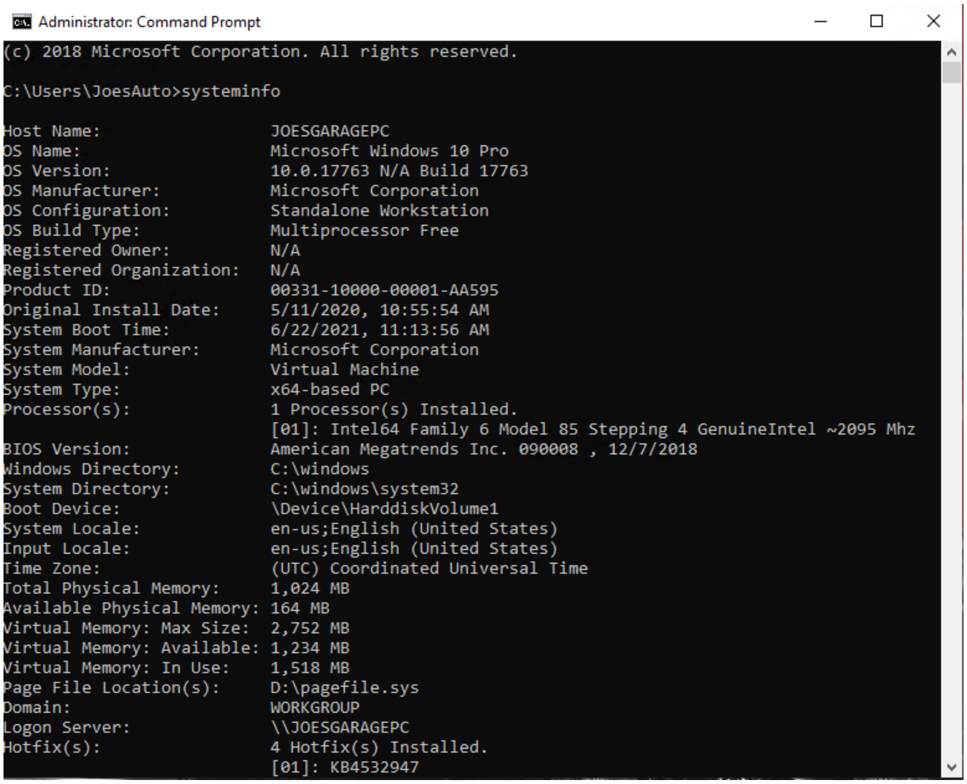
3. ***Provide a screenshot showing this information about Joe's PC:***

System Information Panel:



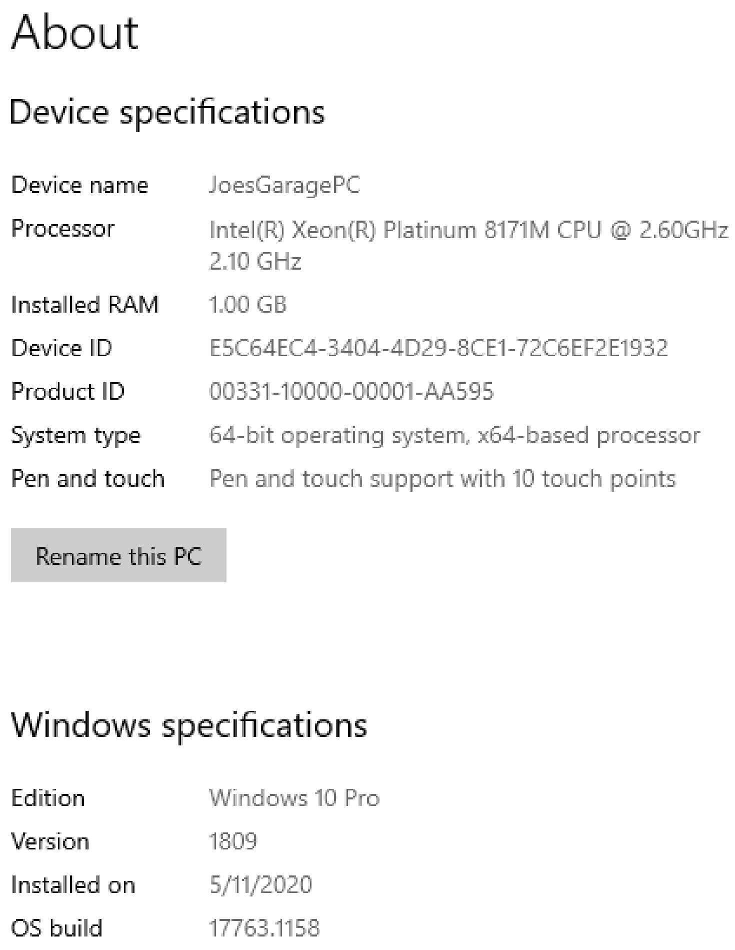
Item	Value
OS Name	Microsoft Windows 10 Pro
Version	10.0.17763 Build 17763
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	JOESGARAGEPC
System Manufacturer	Microsoft Corporation
System Model	Virtual Machine
System Type	x64-based PC
System SKU	Unsupported
Processor	Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz, 2095 Mhz, 1 Core(s), 1 Logi...
BIOS Version/Date	American Megatrends Inc. 090008, 12/7/2018
SMBIOS Version	2.3
BIOS Mode	Legacy
BaseBoard Manufacturer	Microsoft Corporation
BaseBoard Product	Virtual Machine
BaseBoard Version	7.0
Platform Role	Desktop
Secure Boot State	Unsupported
PCR7 Configuration	Binding Not Possible
Windows Directory	C:\windows
System Directory	C:\windows\system32
Boot Device	\Device\HarddiskVolume1

Command Prompt:



```
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\JoesAuto>systeminfo

Host Name:                 JOESGARAGEPC
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          N/A
Registered Organization:   N/A
Product ID:                00331-10000-00001-AA595
Original Install Date:     5/11/2020, 10:55:54 AM
System Boot Time:          6/22/2021, 11:13:56 AM
System Manufacturer:       Microsoft Corporation
System Model:              Virtual Machine
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 4 GenuineIntel ~2095 Mhz
BIOS Version:              American Megatrends Inc. 090008 , 12/7/2018
Windows Directory:         C:\windows
System Directory:          C:\windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC) Coordinated Universal Time
Total Physical Memory:     1,024 MB
Available Physical Memory: 164 MB
Virtual Memory: Max Size:  2,752 MB
Virtual Memory: Available: 1,234 MB
Virtual Memory: In Use:    1,518 MB
Page File Location(s):     D:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\JOESGARAGEPC
Hotfix(s):                 4 Hotfix(s) Installed.
                           [01]: KB4532947
```

Settings > System > About



About

Device specifications

Device name	JoesGaragePC
Processor	Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz 2.10 GHz
Installed RAM	1.00 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	Pen and touch support with 10 touch points

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.

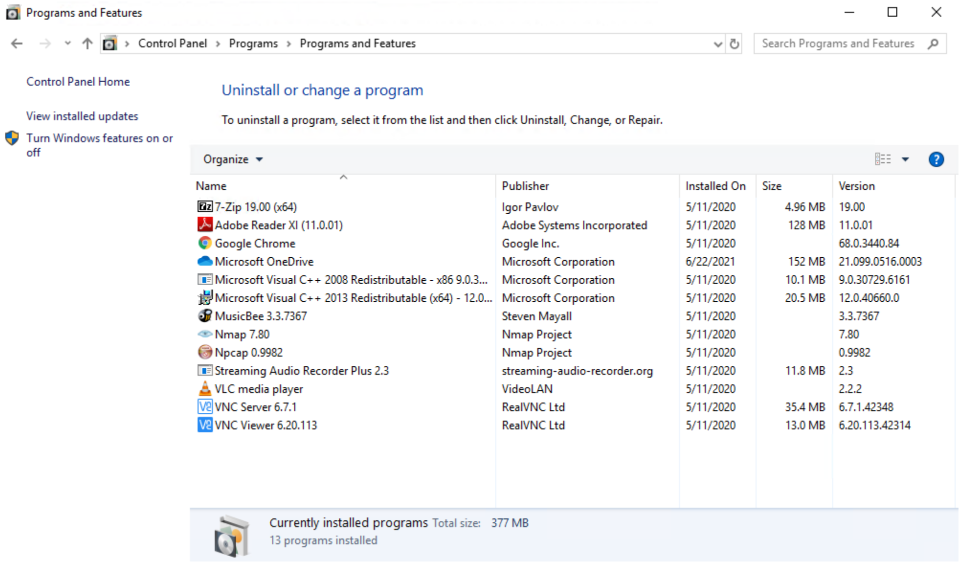
1. ***List at least 5 installed applications on Joe's computer:***

- Nmap
- Google Ghrome
- 7-Zip
- Adobe Reader
- Npcap
- VNC Server
- VNC Viewer
- VLC media player
- Streaming Audio Recorder
- MusicBee

- Microsoft OneDrive
- Microsoft Visual C++

2. ***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.


Programs and Features
Control Panel > Programs > Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
7-Zip 19.00 (x64)	Igor Pavlov	5/11/2020	4.96 MB	19.00
Adobe Reader XI (11.0.01)	Adobe Systems Incorporated	5/11/2020	128 MB	11.0.01
Google Chrome	Google Inc.	5/11/2020		68.0.3440.84
Microsoft OneDrive	Microsoft Corporation	6/22/2021	152 MB	21.099.0516.0003
Microsoft Visual C++ 2008 Redistributable - x86 9.0.3...	Microsoft Corporation	5/11/2020	10.1 MB	9.0.30729.6161
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0...	Microsoft Corporation	5/11/2020	20.5 MB	12.0.40660.0
MusicBee 3.3.7367	Steven Mayall	5/11/2020		3.3.7367
Nmap 7.80	Nmap Project	5/11/2020		7.80
Npcap 0.9982	Nmap Project	5/11/2020		0.9982
Streaming Audio Recorder Plus 2.3	streaming-audio-recorder.org	5/11/2020	11.8 MB	2.3
VLC media player	VideoLAN	5/11/2020		2.2.2
VNC Server 6.7.1	RealVNC Ltd	5/11/2020	35.4 MB	6.7.1.42348
VNC Viewer 6.20.113	RealVNC Ltd	5/11/2020	13.0 MB	6.20.113.42314

Currently installed programs Total size: 377 MB
13 programs installed

3. ***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.

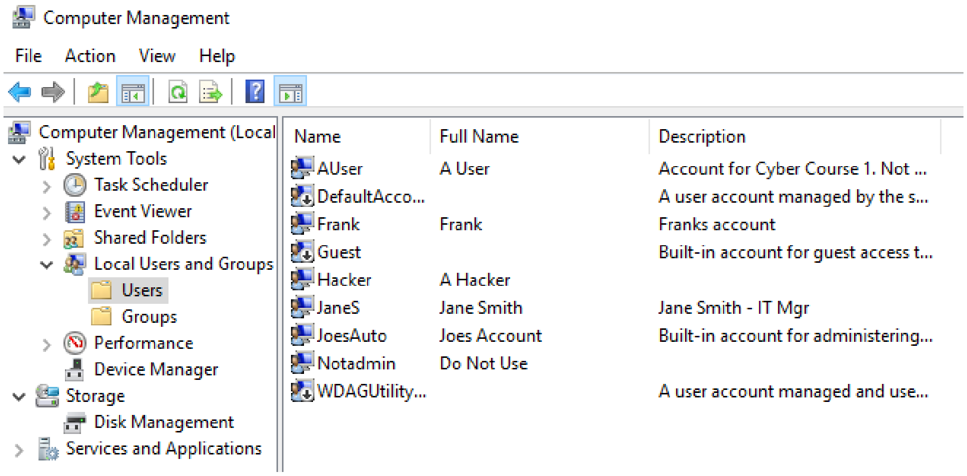
1. ***List the names of the accounts found on Joe's PC and their access level.***

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	-	-

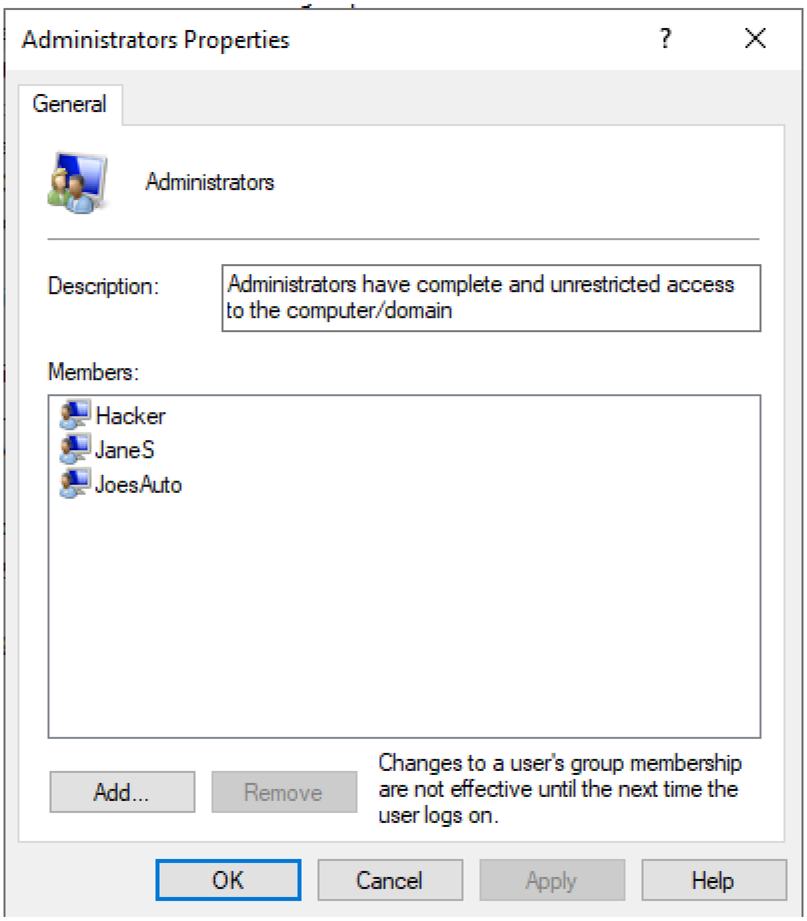
2. ***Provide a screenshot of the Local Users.***

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



Name	Full Name	Description
AUser	A User	Account for Cyber Course 1. Not ...
DefaultAcco...		A user account managed by the s...
Frank	Frank	Franks account
Guest		Built-in account for guest access t...
Hacker	A Hacker	
JaneS	Jane Smith	Jane Smith - IT Mgr
JoesAuto	Joes Account	Built-in account for administering...
Notadmin	Do Not Use	
WDAGUtility...		A user account managed and use...

I checked the Administrators properties to display the admin users.



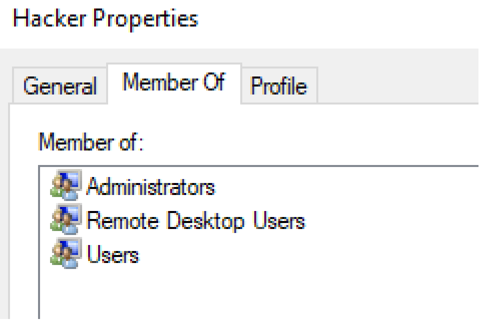
Description: Administrators have complete and unrestricted access to the computer/domain

Members:

Hacker
JaneS
JoesAuto

Changes to a user's group membership are not effective until the next time the user logs on.

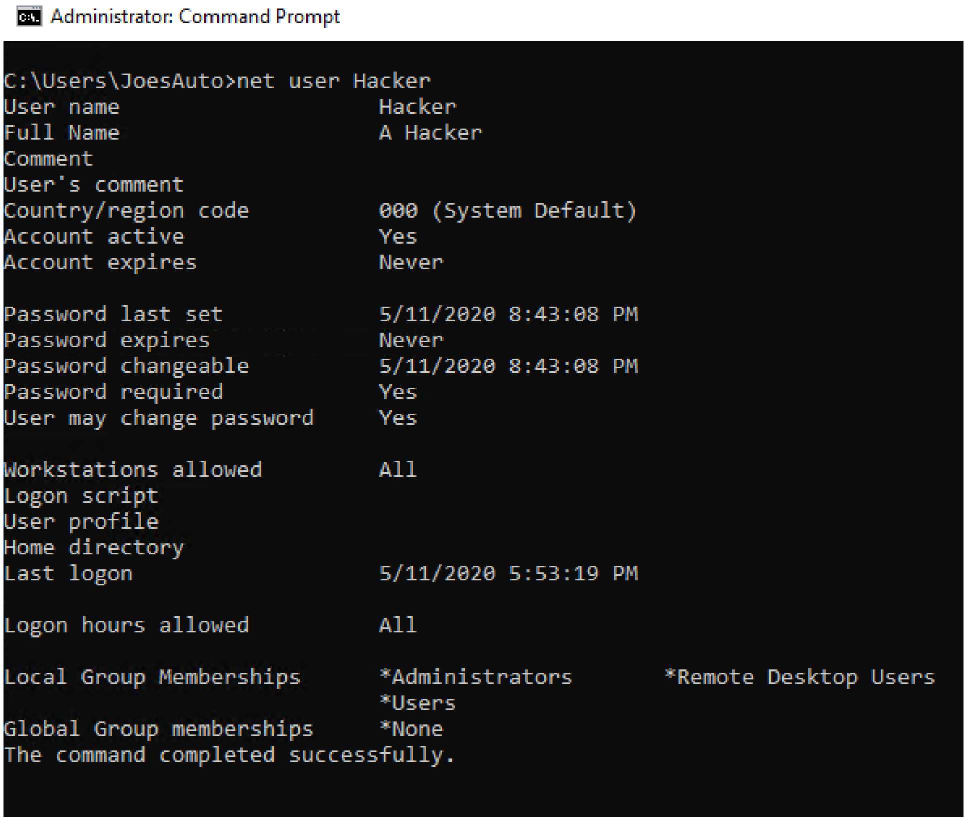
Also, I checked the properties of each user to display the access level. If the user member of Administrators this mean the user has an administrative privilege, if only member of Users it is just a standard account.



Member of:

Administrators
Remote Desktop Users
Users

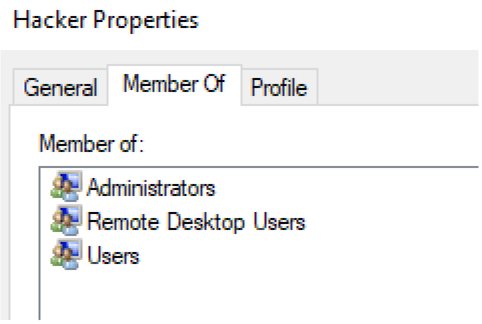
Also, I tried to use type net user command in the Command Prompt to display the access level of each user.



```
C:\Users\JoesAuto>net user Hacker
User name                    Hacker
Full Name                    A Hacker
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/11/2020 8:43:08 PM
Password expires             Never
Password changeable          5/11/2020 8:43:08 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   5/11/2020 5:53:19 PM

Logon hours allowed          All

Local Group Memberships      *Administrators       *Remote Desktop Users
                             *Users
Global Group memberships     *None
The command completed successfully.
```

Properties:

Used to check the access level of each user



Member of:

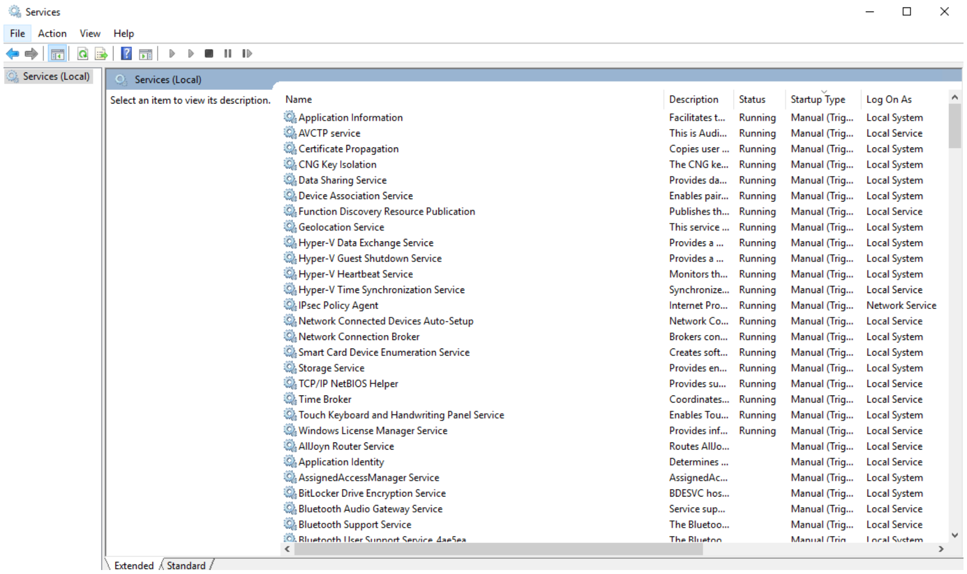
- Administrators
- Remote Desktop Users
- Users

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.

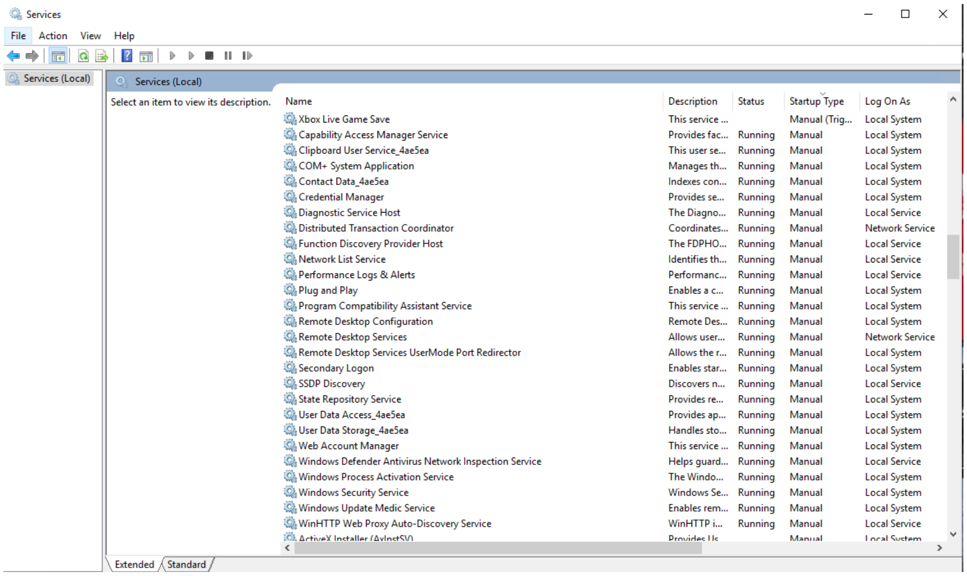
1. ***Provide a screenshot of the services running on this PC.***

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

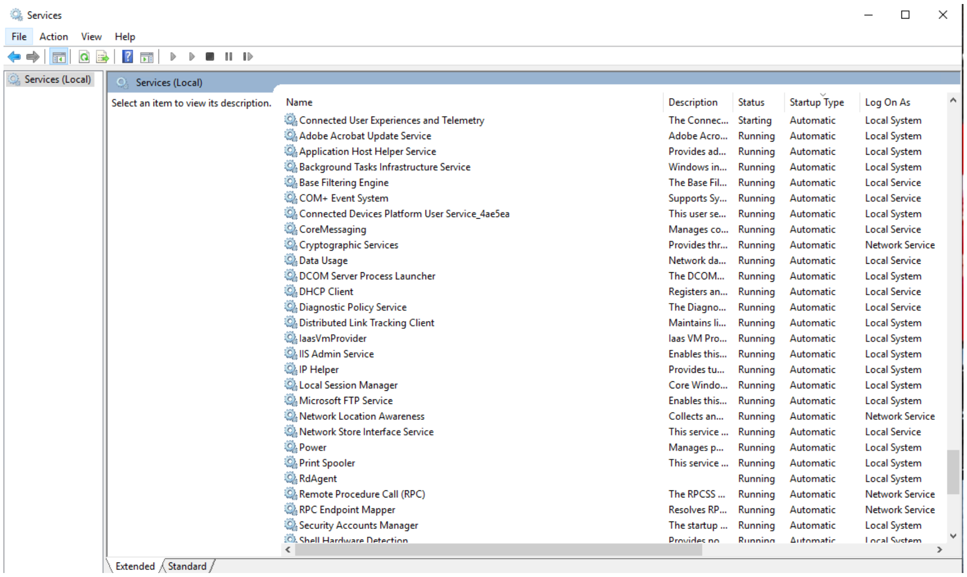


Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
Application Information	Facilitates t...	Running	Manual (Trig...	Local System
AVCTP service	This is Audi...	Running	Manual (Trig...	Local Service
Certificate Propagation	Copies user ...	Running	Manual (Trig...	Local System
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local System
Data Sharing Service	Provides da...	Running	Manual (Trig...	Local System
Device Association Service	Enables pair...	Running	Manual (Trig...	Local System
Function Discovery Resource Publication	Publishes th...	Running	Manual (Trig...	Local Service
Geolocation Service	This service ...	Running	Manual (Trig...	Local System
Hyper-V Data Exchange Service	Provides a ...	Running	Manual (Trig...	Local System
Hyper-V Guest Shutdown Service	Provides a ...	Running	Manual (Trig...	Local System
Hyper-V Heartbeat Service	Monitors th...	Running	Manual (Trig...	Local System
Hyper-V Time Synchronization Service	Synchronize...	Running	Manual (Trig...	Local Service
IPsec Policy Agent	Internet Pro...	Running	Manual (Trig...	Network Service
Network Connected Devices Auto-Setup	Network Co...	Running	Manual (Trig...	Local Service
Network Connection Broker	Brokers con...	Running	Manual (Trig...	Local System
Smart Card Device Enumeration Service	Creates soft...	Running	Manual (Trig...	Local System
Storage Service	Provides en...	Running	Manual (Trig...	Local System
TCP/IP NetBIOS Helper	Provides su...	Running	Manual (Trig...	Local Service
Time Broker	Coordinates...	Running	Manual (Trig...	Local Service
Touch Keyboard and Handwriting Panel Service	Enables Tou...	Running	Manual (Trig...	Local System
Windows License Manager Service	Provides inf...	Running	Manual (Trig...	Local Service
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Local Service
Application Identity	Determines ...		Manual (Trig...	Local Service
AssignedAccessManager Service	AssignedAc...		Manual (Trig...	Local System
BitLocker Drive Encryption Service	BDESVC hos...		Manual (Trig...	Local System
Bluetooth Audio Gateway Service	Service sup...		Manual (Trig...	Local Service
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Local Service
Bluetooth User Support Service 4ae5ea	The Bluetoo		Manual (Trig	Local System



Name	Description	Status	Startup Type	Log On As
Xbox Live Game Save	This service ...		Manual (Trig...	Local System
Capability Access Manager Service	Provides fac...	Running	Manual	Local System
Clipboard User Service_4ae5ea	This user se...	Running	Manual	Local System
COM+ System Application	Manages th...	Running	Manual	Local System
Contact Data_4ae5ea	Indexes con...	Running	Manual	Local System
Credential Manager	Provides se...	Running	Manual	Local System
Diagnostic Service Host	The Diagno...	Running	Manual	Local Service
Distributed Transaction Coordinator	Coordinates...	Running	Manual	Network Service
Function Discovery Provider Host	The FDPHO...	Running	Manual	Local Service
Network List Service	Identifies th...	Running	Manual	Local Service
Performance Logs & Alerts	Performanc...	Running	Manual	Local Service
Plug and Play	Enables a c...	Running	Manual	Local System
Program Compatibility Assistant Service	This service ...	Running	Manual	Local System
Remote Desktop Configuration	Remote Des...	Running	Manual	Local System
Remote Desktop Services	Allows user...	Running	Manual	Network Service
Remote Desktop Services UserMode Port Redirector	Allows the r...	Running	Manual	Local System
Secondary Logon	Enables star...	Running	Manual	Local System
SSDP Discovery	Discovers n...	Running	Manual	Local Service
State Repository Service	Provides re...	Running	Manual	Local System
User Data Access_4ae5ea	Provides ap...	Running	Manual	Local System
User Data Storage_4ae5ea	Handles sto...	Running	Manual	Local System
Web Account Manager	This service ...	Running	Manual	Local System
Windows Defender Antivirus Network Inspection Service	Helps guard...	Running	Manual	Local Service
Windows Process Activation Service	The Windo...	Running	Manual	Local System
Windows Security Service	Windows Se...	Running	Manual	Local System
Windows Update Medic Service	Enables rem...	Running	Manual	Local System
WinHTTP Web Proxy Auto-Discovery Service	WinHTTP i...	Running	Manual	Local Service
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local System



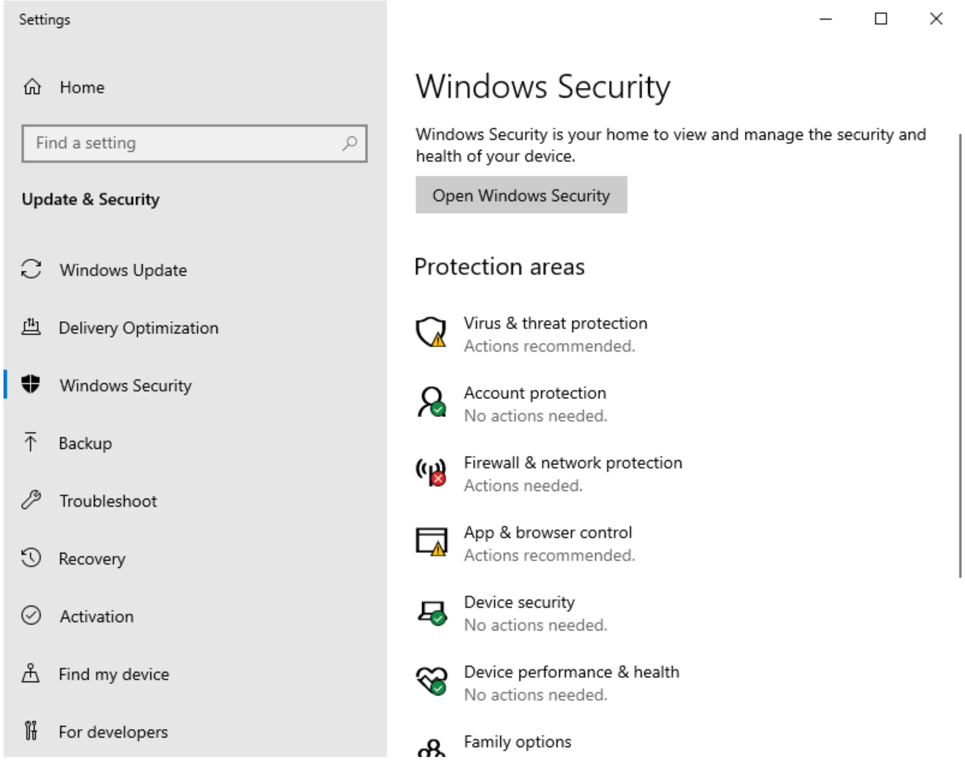
Name	Description	Status	Startup Type	Log On As
Connected User Experiences and Telemetry	The Connec...	Starting	Automatic	Local System
Adobe Acrobat Update Service	Adobe Acro...	Running	Automatic	Local System
Application Host Helper Service	Provides ad...	Running	Automatic	Local System
Background Tasks Infrastructure Service	Windows in...	Running	Automatic	Local System
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
Connected Devices Platform User Service_4ae5ea	This user se...	Running	Automatic	Local System
CoreMessaging	Manages co...	Running	Automatic	Local Service
Cryptographic Services	Provides thr...	Running	Automatic	Network Service
Data Usage	Network da...	Running	Automatic	Local Service
DCOM Server Process Launcher	The DCOM...	Running	Automatic	Local System
DHCP Client	Registers an...	Running	Automatic	Local Service
Diagnostic Policy Service	The Diagno...	Running	Automatic	Local Service
Distributed Link Tracking Client	Maintains li...	Running	Automatic	Local System
IaasVmProvider	Iaas VM Pro...	Running	Automatic	Local System
IIS Admin Service	Enables this...	Running	Automatic	Local System
IP Helper	Provides tu...	Running	Automatic	Local System
Local Session Manager	Core Windo...	Running	Automatic	Local System
Microsoft FTP Service	Enables this...	Running	Automatic	Local System
Network Location Awareness	Collects an...	Running	Automatic	Network Service
Network Store Interface Service	This service ...	Running	Automatic	Local Service
Power	Manages p...	Running	Automatic	Local System
Print Spooler	This service ...	Running	Automatic	Local System
RdAgent		Running	Automatic	Local System
Remote Procedure Call (RPC)	The RPCSS ...	Running	Automatic	Network Service
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network Service
Security Accounts Manager	The startup ...	Running	Automatic	Local System
Shell Hardware Detection	Provides no...	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:*

Settings > Update & Security > Windows Security



Windows Security

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

Protection areas

Virus & threat protection
Actions recommended.

Account protection
No actions needed.

Firewall & network protection
Actions needed.

App & browser control
Actions recommended.

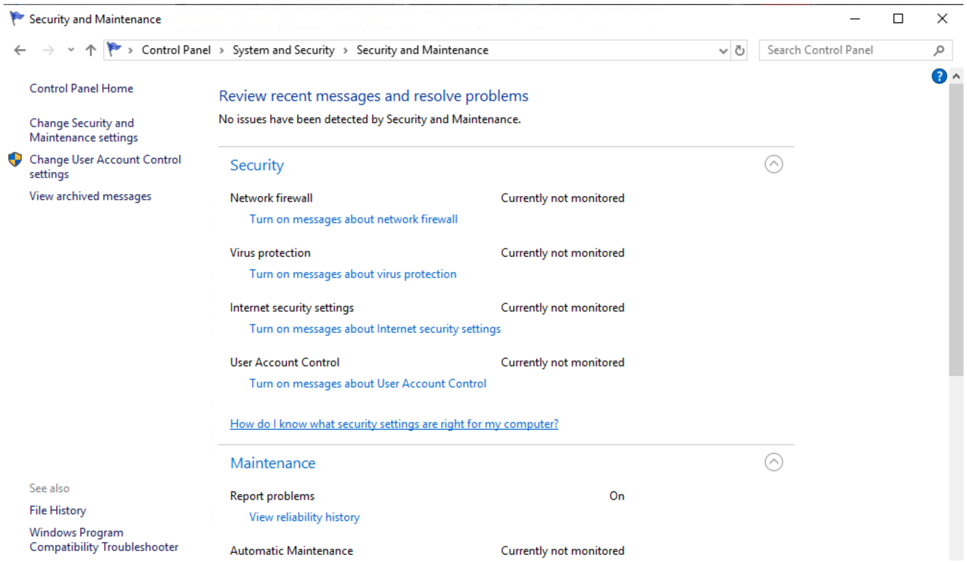
Device security
No actions needed.

Device performance & health
No actions needed.

Family options

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:*

Control Panel > System and Security > Security and Maintenance


Security and Maintenance
Control Panel › System and Security › Security and Maintenance
Search Control Panel
Control Panel Home
Change Security and Maintenance settings
Change User Account Control settings
View archived messages
See also
File History
Windows Program Compatibility Troubleshooter

Review recent messages and resolve problems

No issues have been detected by Security and Maintenance.

Security

Network firewall	Currently not monitored
Turn on messages about network firewall	
Virus protection	Currently not monitored
Turn on messages about virus protection	
Internet security settings	Currently not monitored
Turn on messages about Internet security settings	
User Account Control	Currently not monitored
Turn on messages about User Account Control	

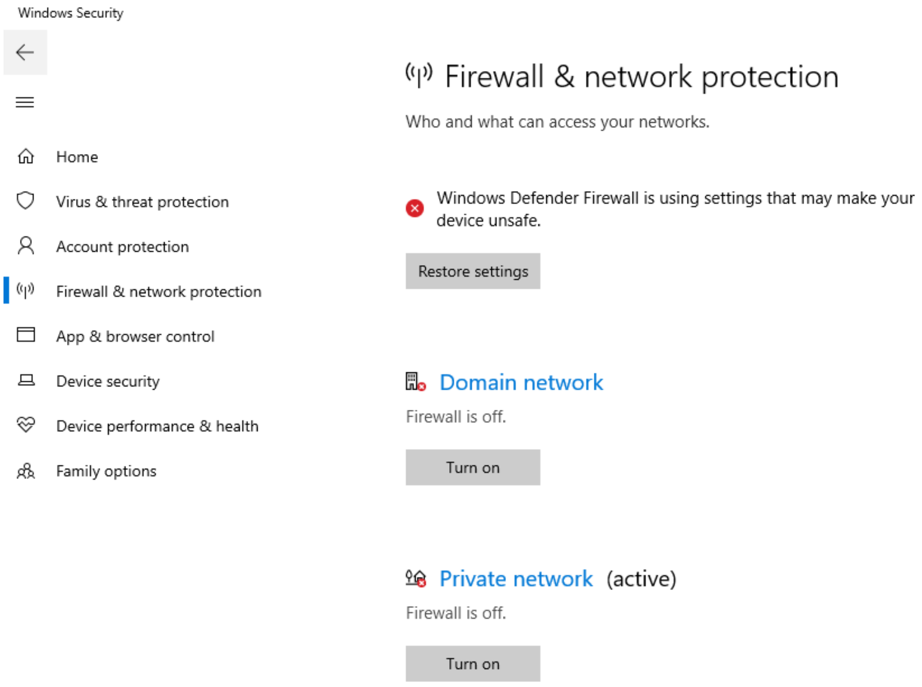
How do I know what security settings are right for my computer?

Maintenance

Report problems	On
View reliability history	
Automatic Maintenance	Currently not monitored

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

Windows Security > Firewall & Network Protection



Firewall & network protection

Who and what can access your networks.

Windows Defender Firewall is using settings that may make your device unsafe.

Domain network

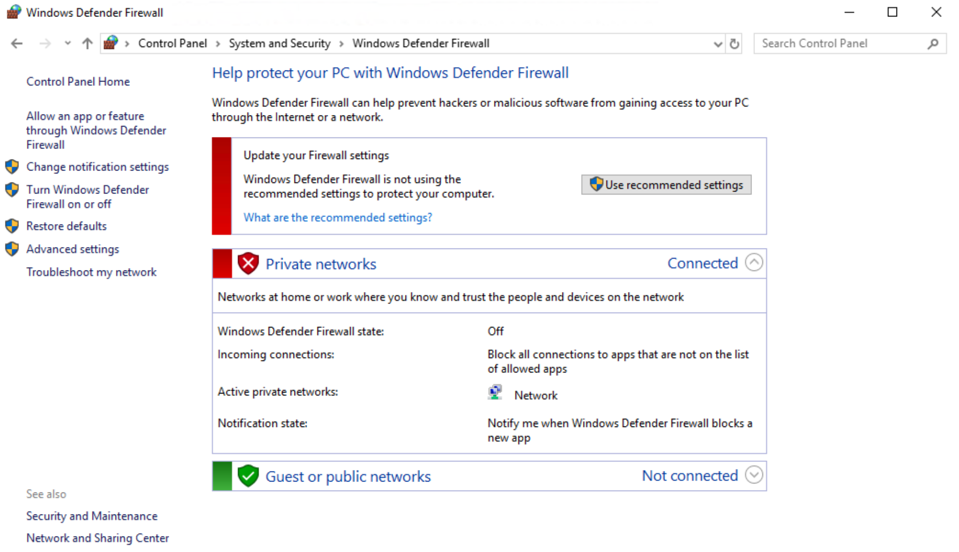
Firewall is off.

Private network (active)

Firewall is off.

4. *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



Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Defender Firewall

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

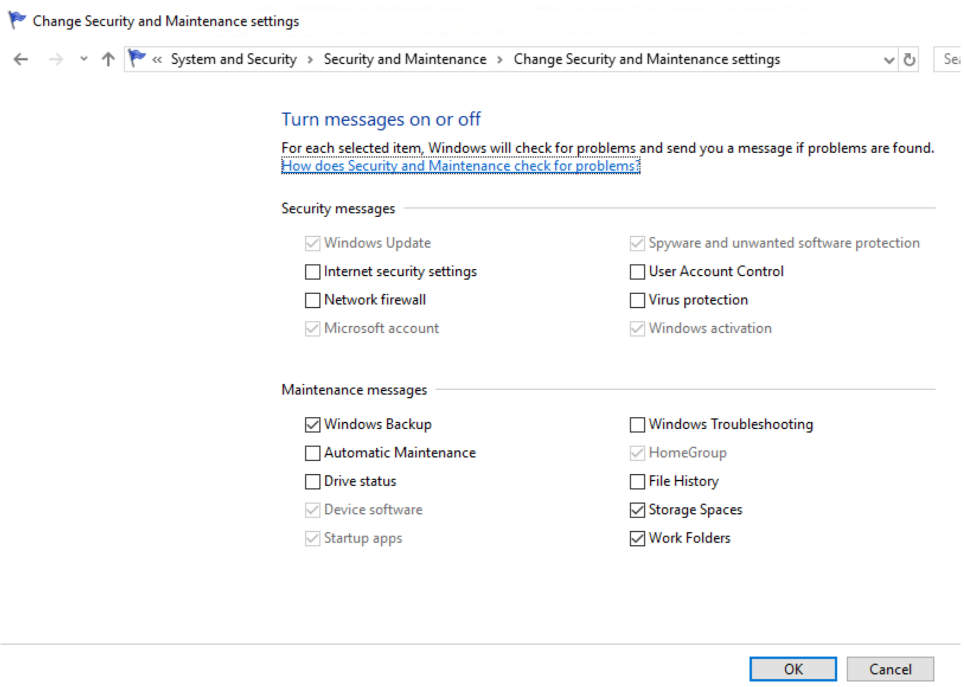
Networks at home or work where you know and trust the people and devices on the network

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:*

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


Change Security and Maintenance settings
« System and Security › Security and Maintenance › Change Security and Maintenance settings
Sea
OK
Cancel

Turn messages on or off

For each selected item, Windows will check for problems and send you a message if problems are found.
How does Security and Maintenance check for problems?

Security messages

☑ Windows Update
☑ Spyware and unwanted software protection
□ Internet security settings
□ User Account Control
□ Network firewall
□ Virus protection
☑ Microsoft account
☑ Windows activation

Maintenance messages

☑ Windows Backup
□ Windows Troubleshooting
□ Automatic Maintenance
☑ HomeGroup
□ Drive status
□ File History
☑ Device software
☑ Storage Spaces
☑ Startup apps
☑ Work Folders

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**	**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

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.]

- 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.

2. ***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.

3. **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

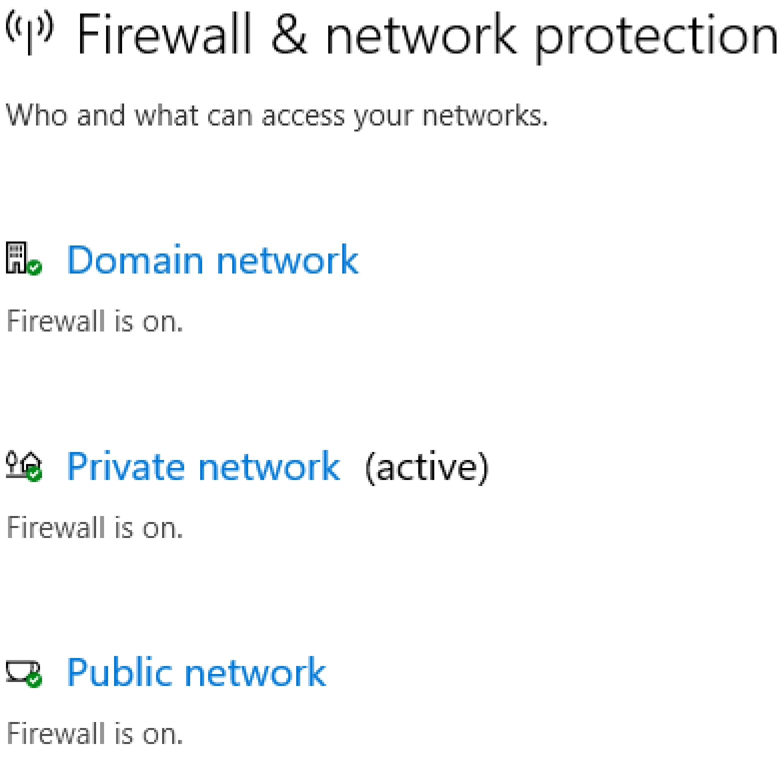
Firewall

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.

2. ***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.

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

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

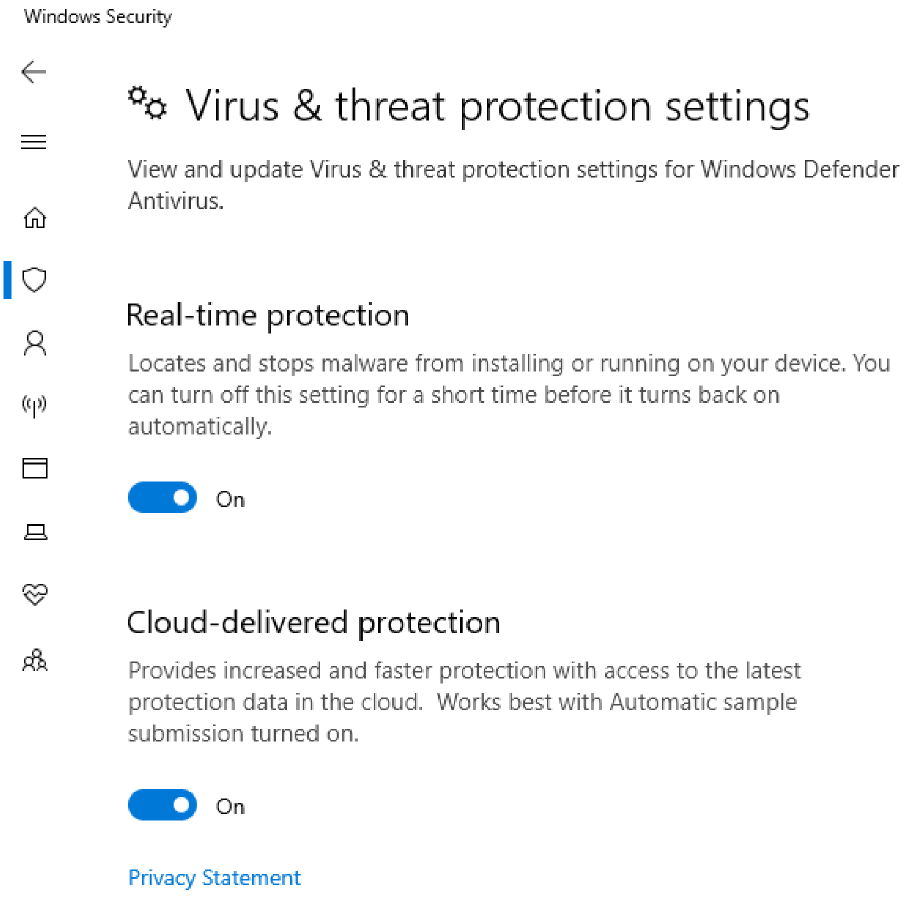
Virus & Threat Protection

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.

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



Windows Security

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

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

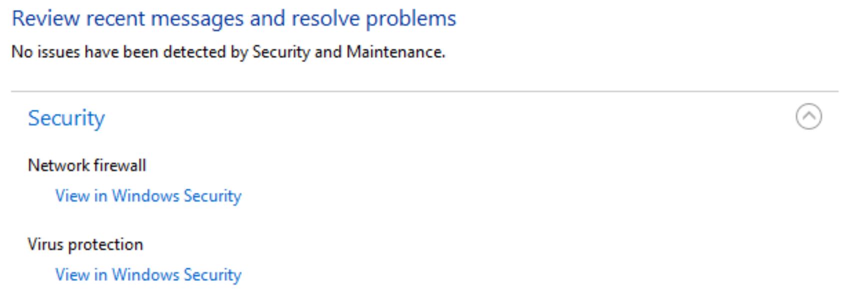
Privacy Statement

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

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



Review recent messages and resolve problems

No issues have been detected by Security and Maintenance.

Security

Network firewall

View in Windows Security

Virus protection

View in Windows Security

3. ***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.

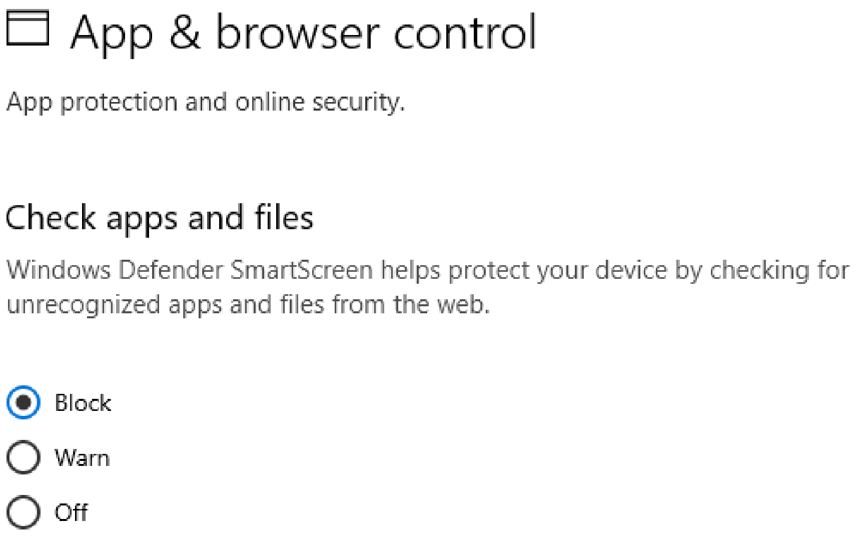
4. ***From the CIS baseline controls, provide the controls satisfied by completing this.***

- 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.*



App & browser control

App protection and online security.

Check apps and files

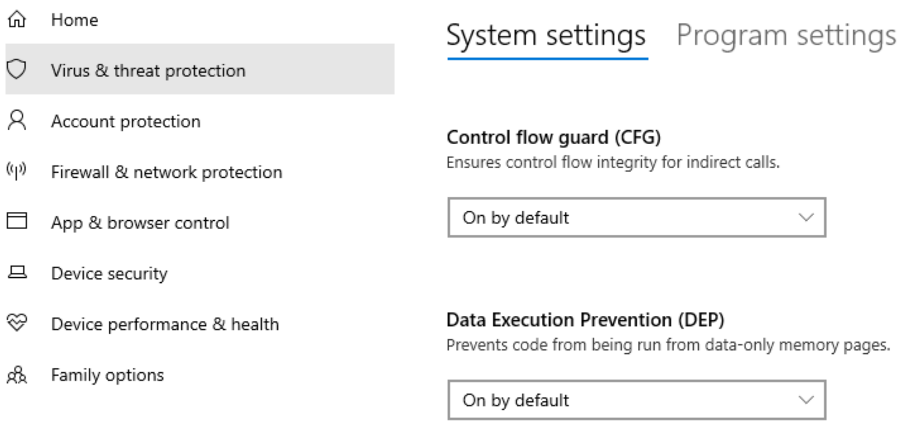
Windows Defender SmartScreen helps protect your device by checking for unrecognized apps and files from the web.

● Block

○ Warn

○ Off

Exploit protection



Control flow guard (CFG)

Ensures control flow integrity for indirect calls.

On by default

Data Execution Prevention (DEP)

Prevents code from being run from data-only memory pages.

On by default

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.

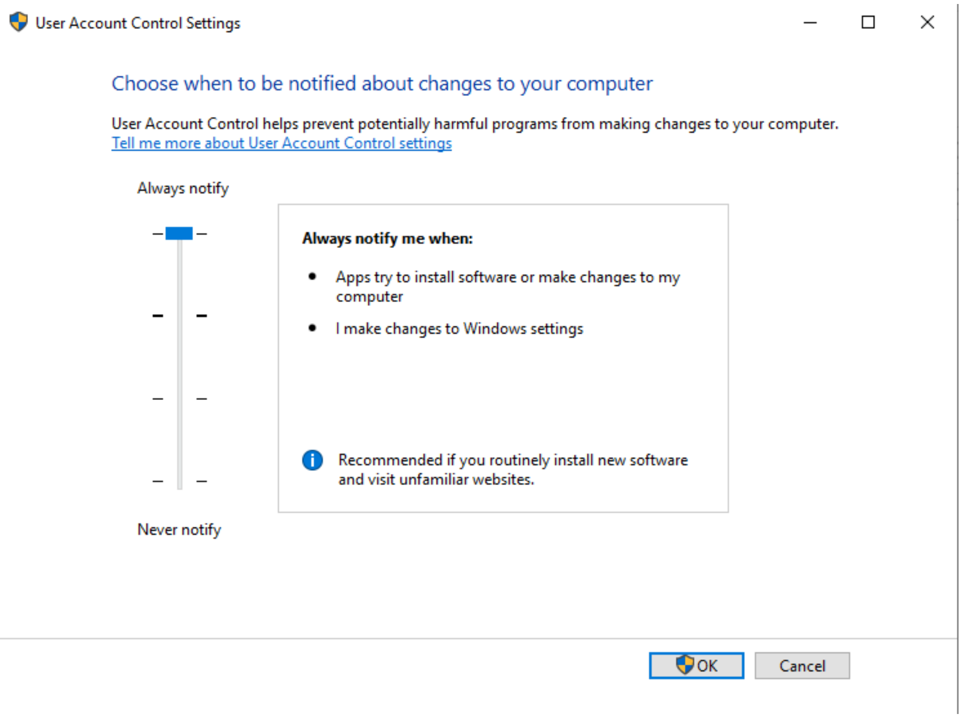
1. ***What is the current UAC setting on Joe's computer?***

   This is available from the above security settings.

   Never notify whenever apps try install or make changes.

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

It should set to always notify



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 computer.
Tell me more about User Account Control settings

Always notify

Always notify me when:

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

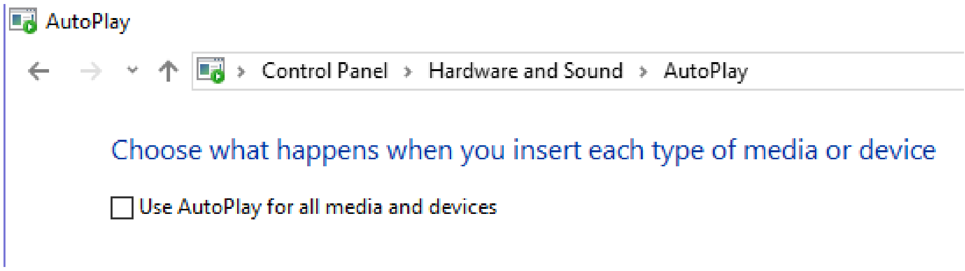
Recommended if you routinely install new software and visit unfamiliar websites.

Never 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."***



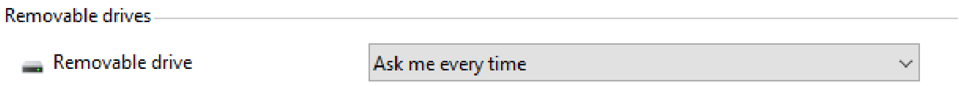
AutoPlay

Control Panel > Hardware and Sound > AutoPlay

Choose what happens when you insert each type of media or device

□ 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.***



Removable drives

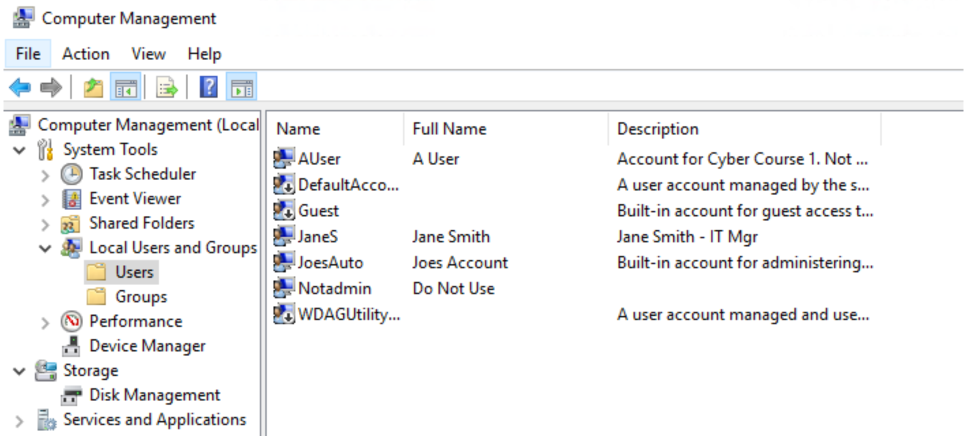
Removable drive: Ask me every time

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)



Name	Full Name	Description
AUser	A User	Account for Cyber Course 1. Not ...
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...
JaneS	Jane Smith	Jane Smith - IT Mgr
JoesAuto	Joes Account	Built-in account for administering...
Notadmin	Do Not Use	
WDAGUtility...		A user account managed and use...

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?***
3. ***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.

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

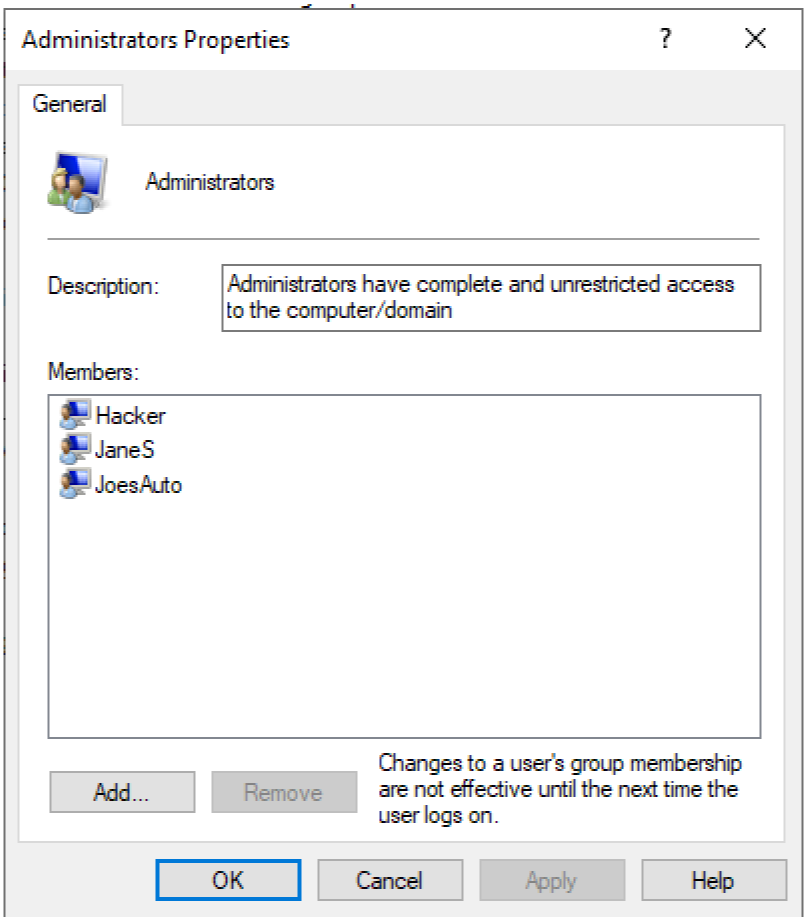
Only specific accounts should have administrator privileges. This reduces the ability for unwanted applications to be installed including malware.

5. **Which account(s) have administrator rights that shouldn't?**

Hacker & JaneS

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

I checked the Administrators properties to display the admin users.



Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

Hacker
JaneS
JoesAuto

Changes to a user's group membership are not effective until the next time the user logs on.

Administrator privileges for too many users are another security challenge.

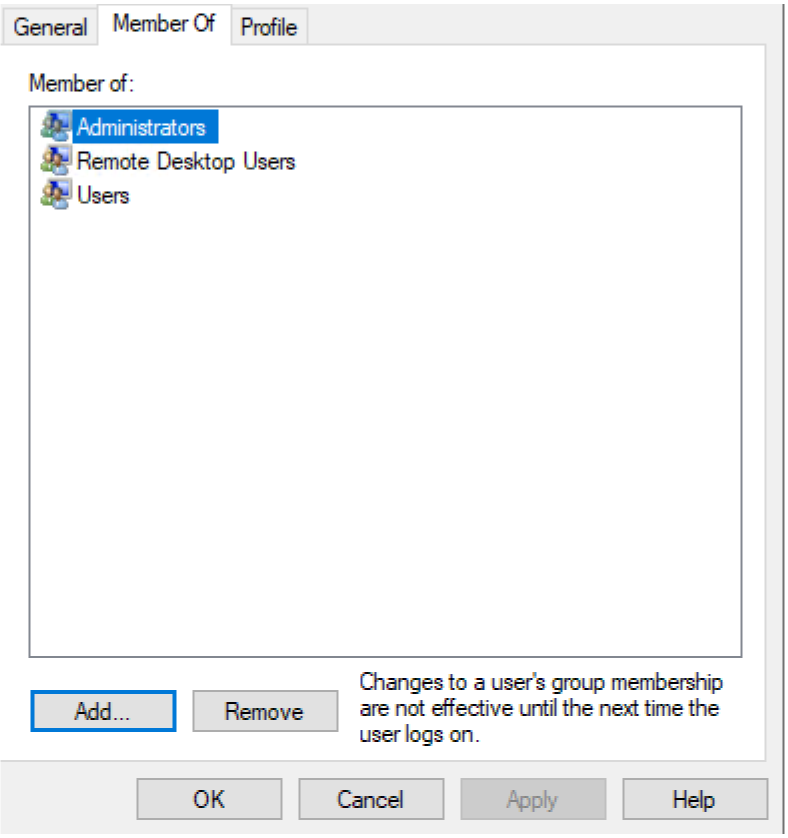
7. **Provide at least three risks associated with users having administrator rights on a PC.**

- 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.

8. ***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.



Member of:

Administrators
Remote Desktop Users
Users

Changes to a user's group membership are not effective until the next time the user logs on.

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

Least-privilege

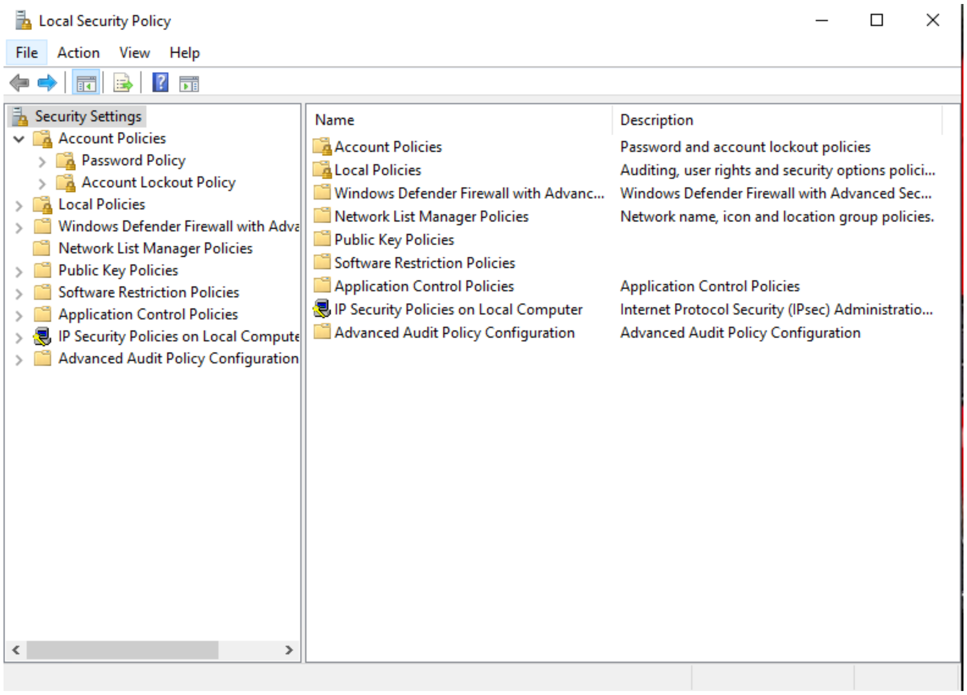
10. **The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?**

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.

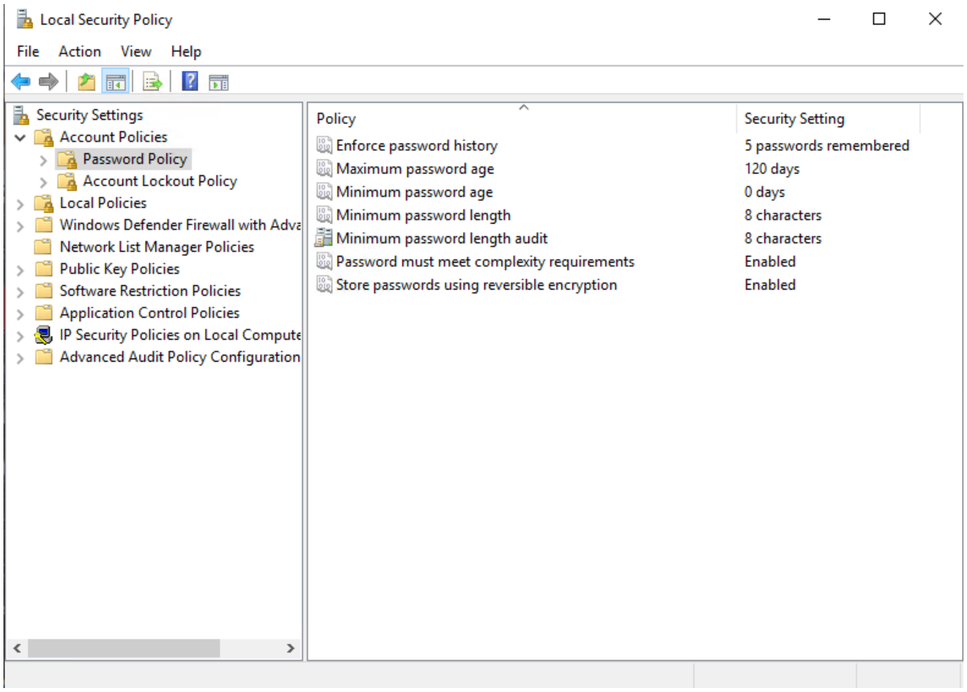
1. ***Provide a screenshot of the Local Security Policy window here.***
   [Note: Local Security Policy is not available on Windows 10 Home edition.]


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Defender Firewall with Advanc...	Windows Defender Firewall with Advanced Sec...
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

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:**

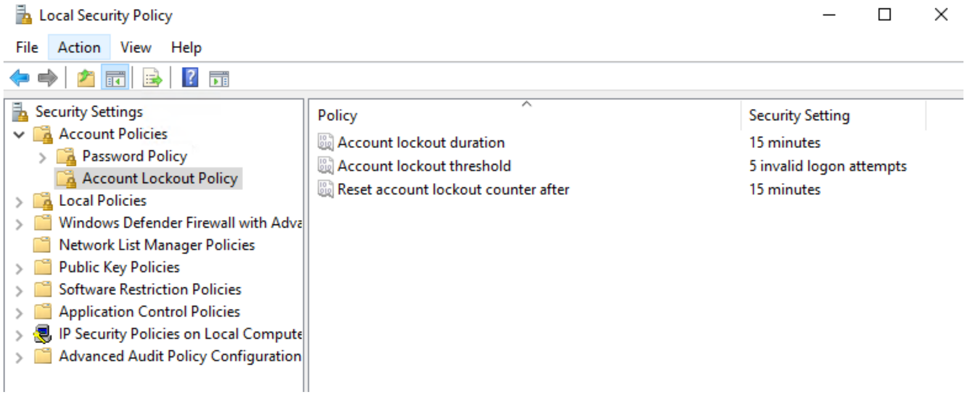
   From the Local Security Policy, I chose Password Policy and I made all the changes that mentioned earlier.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

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

- **Setting the Account Lockout Policy:**

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

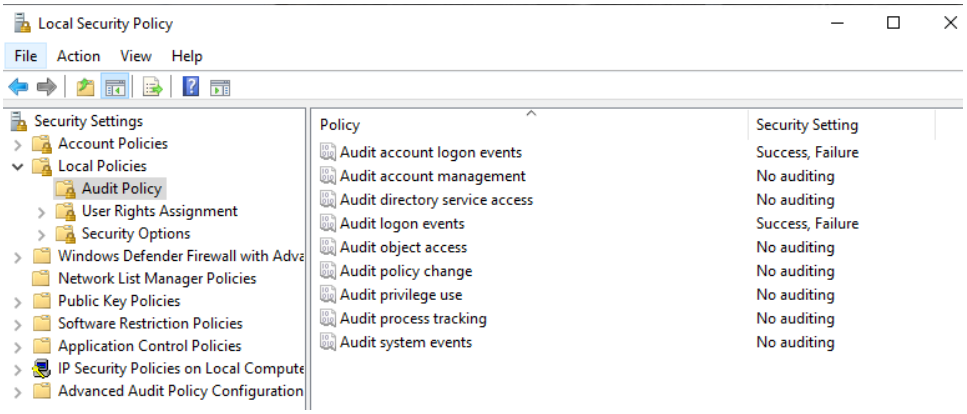

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	15 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	15 minutes

Auditing and Logging

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

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


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

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

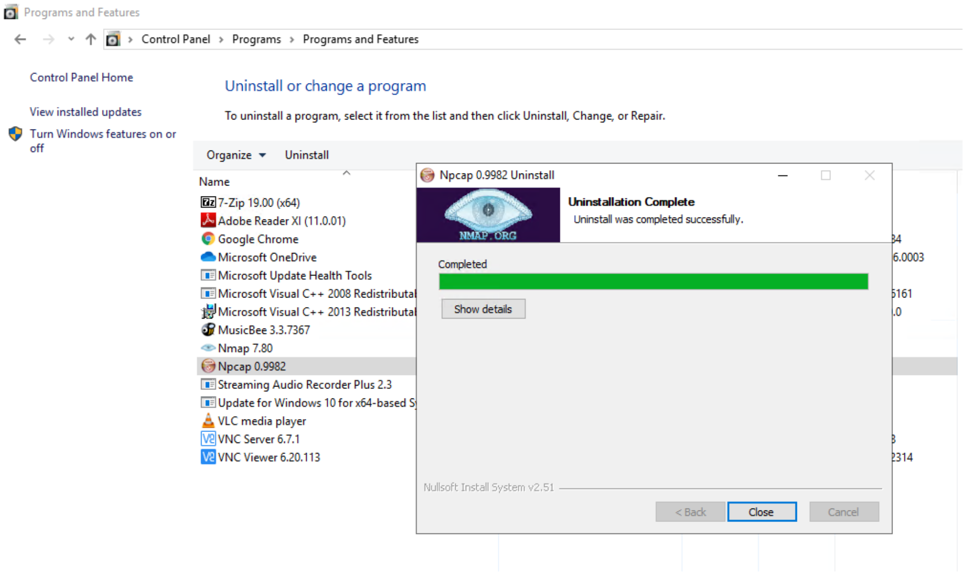
- *7-zip*
- *Npcap*
- *Candy Crush Friends*
- *MusicBee*
- *Microsoft OneDrive*

2. ***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.

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.***

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



Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

- 7-Zip 19.00 (x64)
- Adobe Reader XI (11.0.01)
- Google Chrome
- Microsoft OneDrive
- Microsoft Update Health Tools
- Microsoft Visual C++ 2008 Redistributal
- Microsoft Visual C++ 2013 Redistributal
- MusicBee 3.3.7367
- Nmap 7.80
- Npcap 0.9982
- Streaming Audio Recorder Plus 2.3
- Update for Windows 10 for x64-based S
- VLC media player
- VNC Server 6.7.1
- VNC Viewer 6.20.113

Uninstallation Complete

Uninstall was completed successfully.

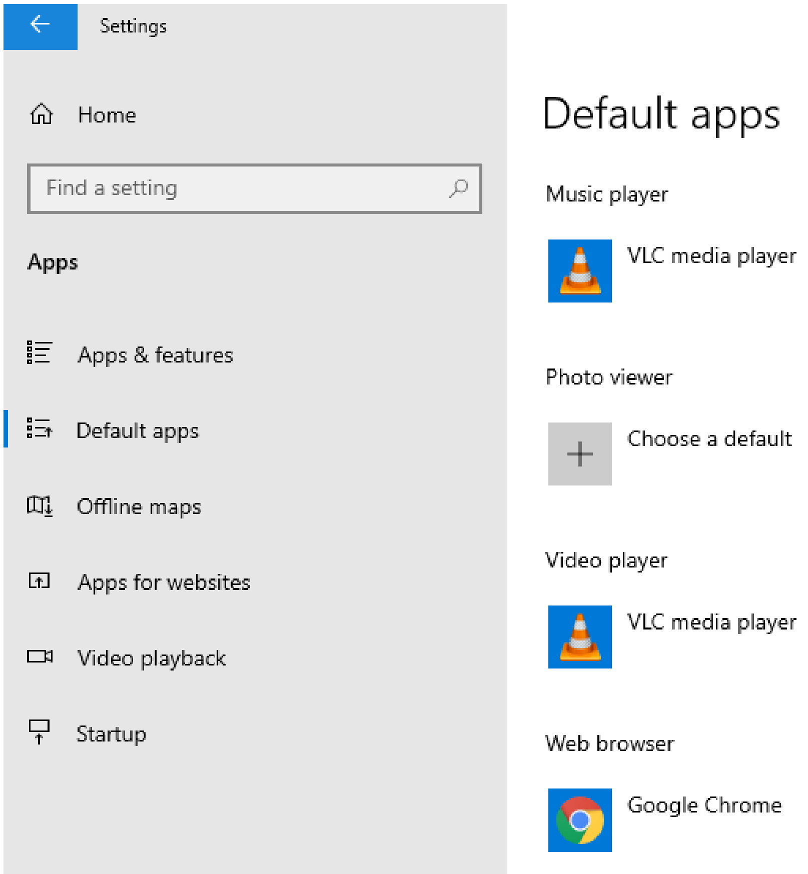
Nullsoft Install System v2.51

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.



Default apps

Music player: VLC media player

Photo viewer: Choose a default

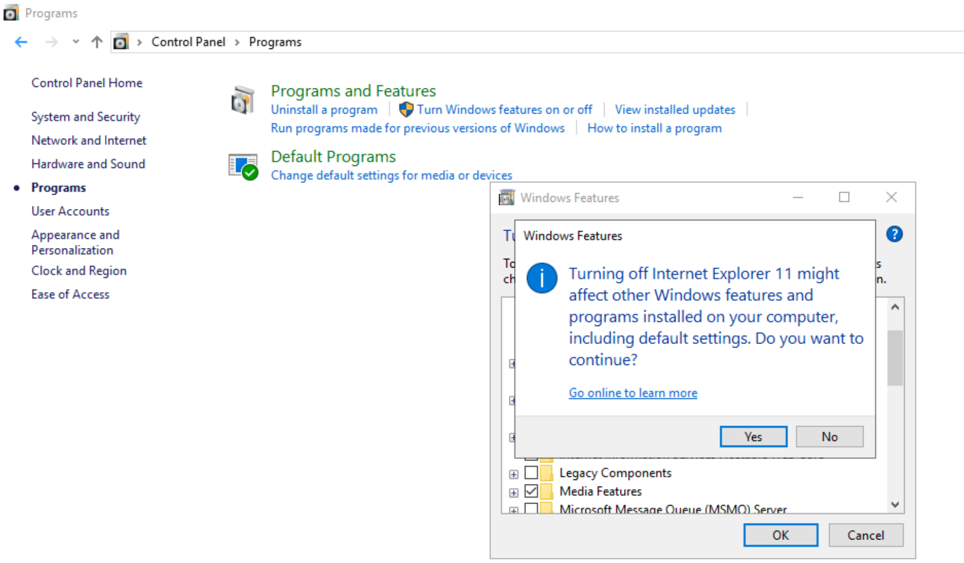
Video player: VLC media player

Web browser: Google Chrome

2. ***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**.”

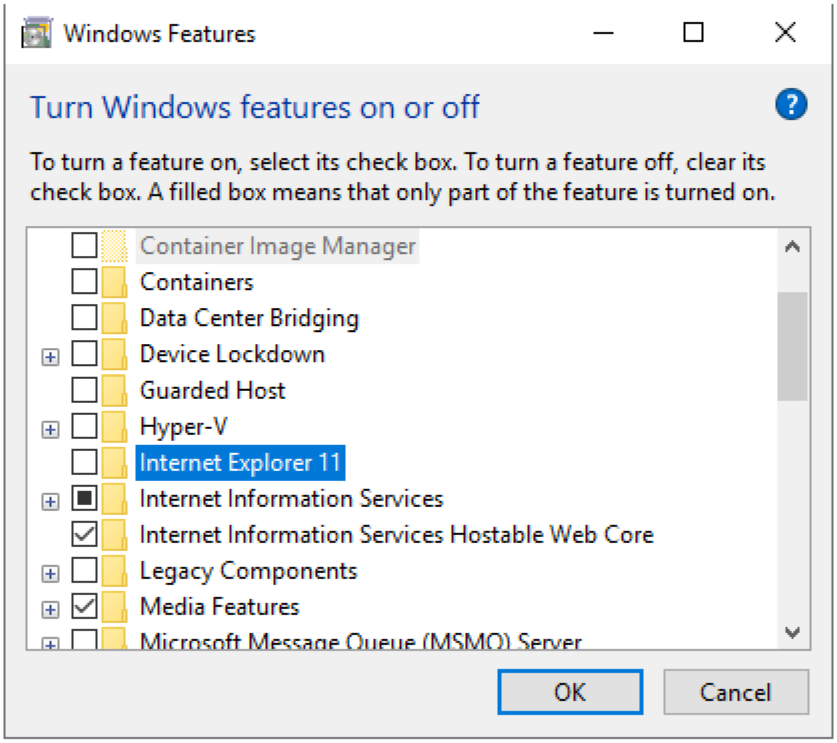
3. *Provide a screenshot showing Internet Explorer 11 is off.*


Programs
Control Panel › Programs
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Programs and Features
Uninstall a program | Turn Windows features on or off | View installed updates
Run programs made for previous versions of Windows | How to install a program
Default Programs
Change default settings for media or devices
Windows Features
Legacy Components
Media Features
Microsoft Message Queue (MSMQ) Server
OK
Cancel

Windows Features

Turning off Internet Explorer 11 might affect other Windows features and programs installed on your computer, including default settings. Do you want to continue?

Go online to learn more



Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

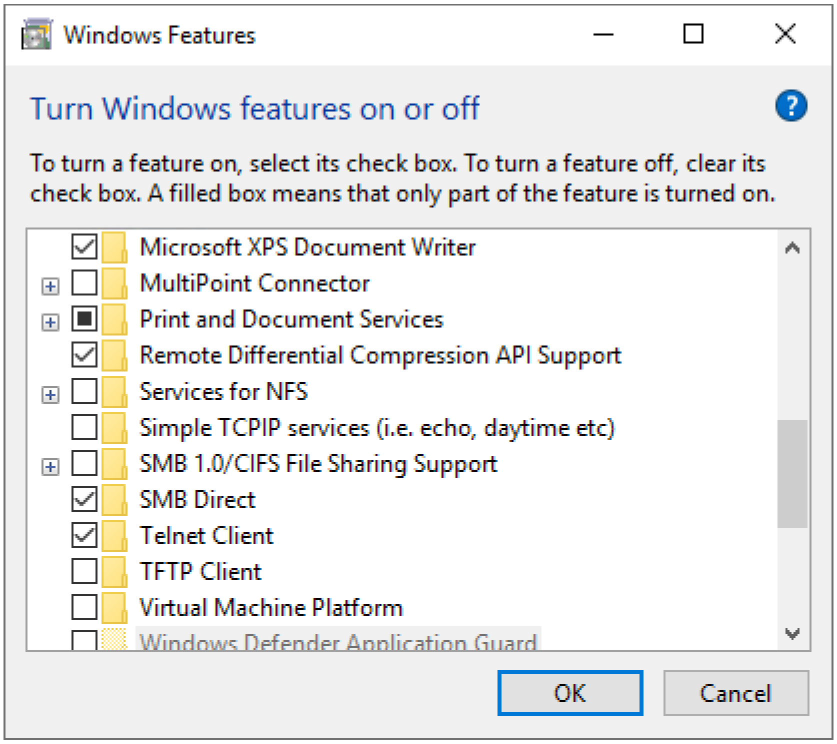
- □ Container Image Manager
- □ Containers
- □ Data Center Bridging
- □ Device Lockdown
- □ Guarded Host
- □ Hyper-V
- □ Internet Explorer 11
- ■ Internet Information Services
- ☑ Internet Information Services Hostable Web Core
- □ Legacy Components
- ☑ Media Features
- □ Microsoft Message Queue (MSMQ) Server

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.



Windows Features

Turn Windows features on or off

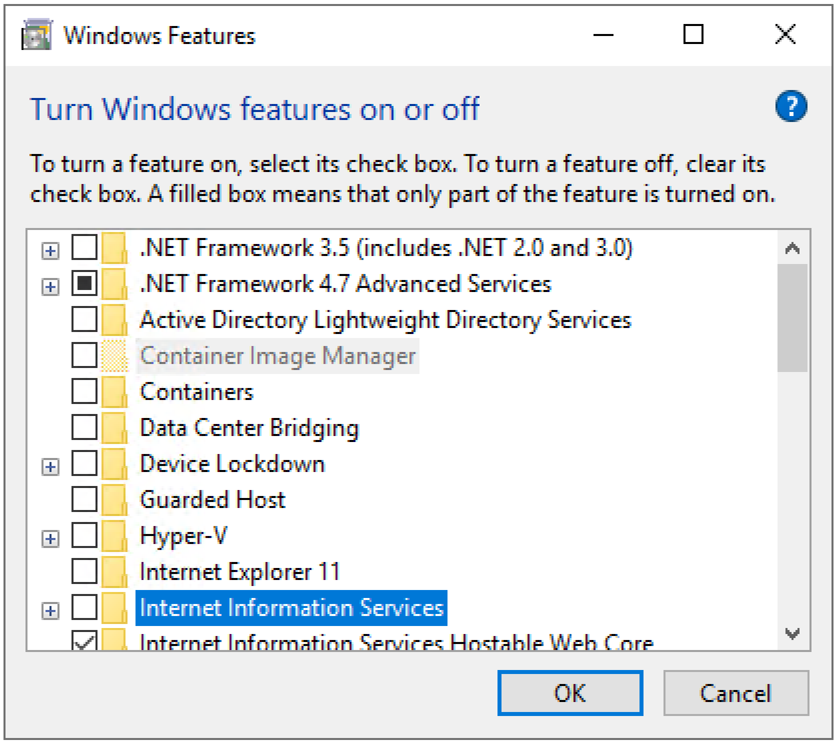
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☑ Microsoft XPS Document Writer
- □ MultiPoint Connector
- ■ Print and Document Services
- ☑ Remote Differential Compression API Support
- □ Services for NFS
- □ Simple TCPIP services (i.e. echo, daytime etc)
- □ SMB 1.0/CIFS File Sharing Support
- ☑ SMB Direct
- ☑ Telnet Client
- □ TFTP Client
- □ Virtual Machine Platform
- □ Windows Defender Application Guard

2. **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.

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



Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ⊞ □ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- ⊞ ■ .NET Framework 4.7 Advanced Services
- □ Active Directory Lightweight Directory Services
- □ Container Image Manager
- □ Containers
- □ Data Center Bridging
- ⊞ □ Device Lockdown
- □ Guarded Host
- ⊞ □ Hyper-V
- □ Internet Explorer 11
- ⊞ □ Internet Information Services
- ☑ Internet Information Services Hostable Web Core

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.**

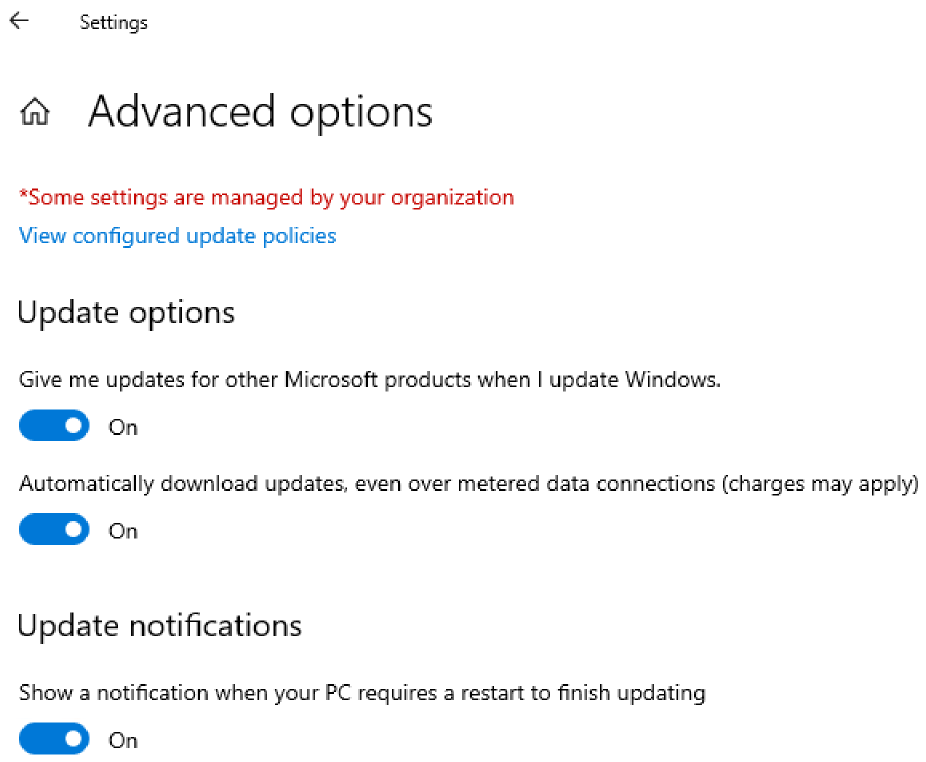
Not available

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.



Advanced options

*Some settings are managed by your organization

View configured update policies

Update options

Give me updates for other Microsoft products when I update Windows.

On

Automatically download updates, even over metered data connections (charges may apply)

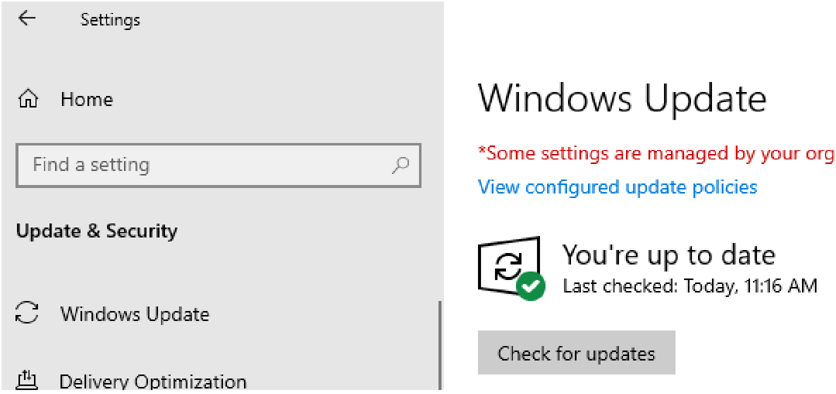
On

Update notifications

Show a notification when your PC requires a restart to finish updating

On

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.*



Windows Update

*Some settings are managed by your organization

View configured update policies

You're up to date

Last checked: Today, 11:16 AM

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:***

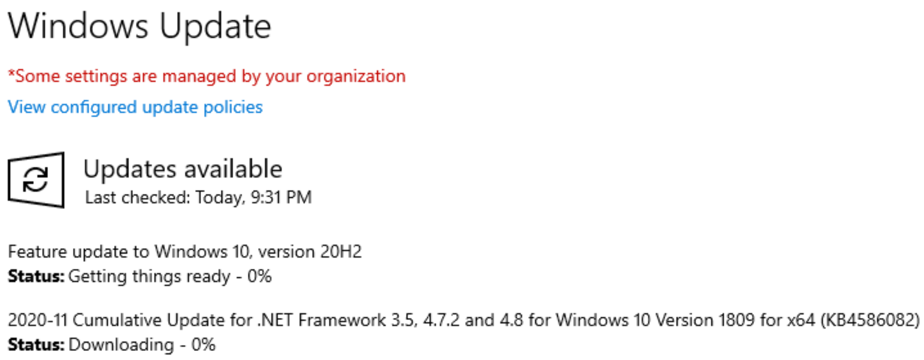
- .NET Framework
- Google Chrome
- Microsoft OneDrive

4. ***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.

5. ***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.



Windows Update

*Some settings are managed by your organization

View configured update policies

Updates available
Last checked: Today, 9:31 PM

Feature update to Windows 10, version 20H2
Status: Getting things ready - 0%

2020-11 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64 (KB4586082)
Status: Downloading - 0%

5. Securing Files and Folders

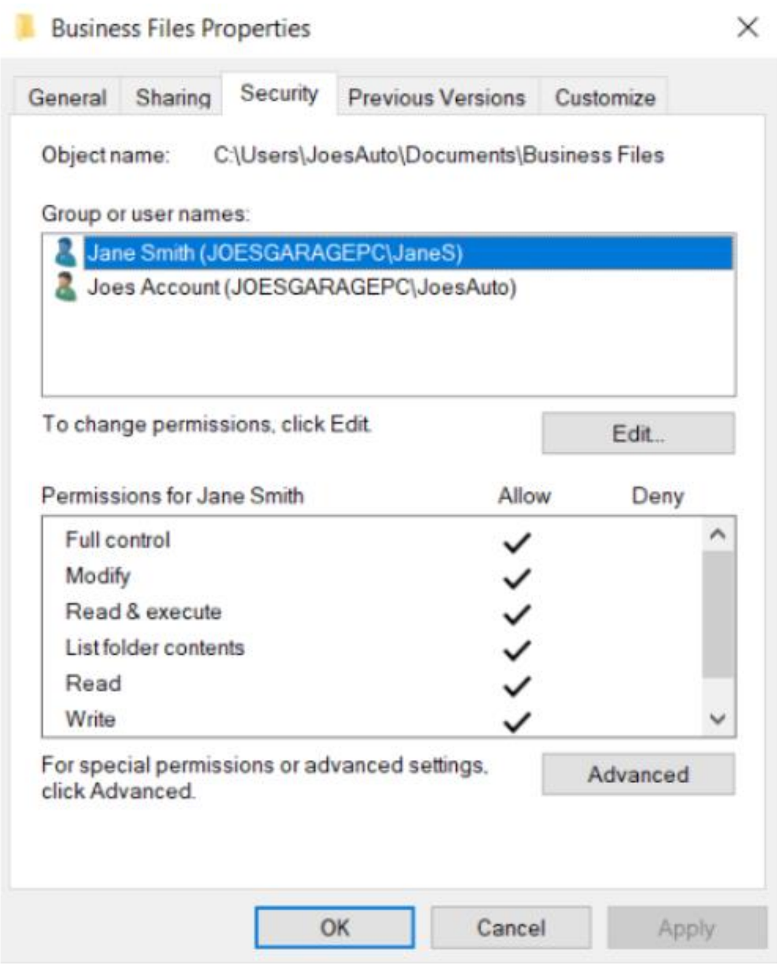
Joe has some work files in his Business folder that he wants to secure since they contain his customer information. They are labeled "JoesWork."

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.



Object name: C:\Users\JoesAuto\Documents\Business Files

Group or user names:

- Jane Smith (JOESGARAGEPC\JaneS)
- Joes Account (JOESGARAGEPC\JoesAuto)

To change permissions, click Edit.

Permissions for Jane Smith	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

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.***

- *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*

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?***

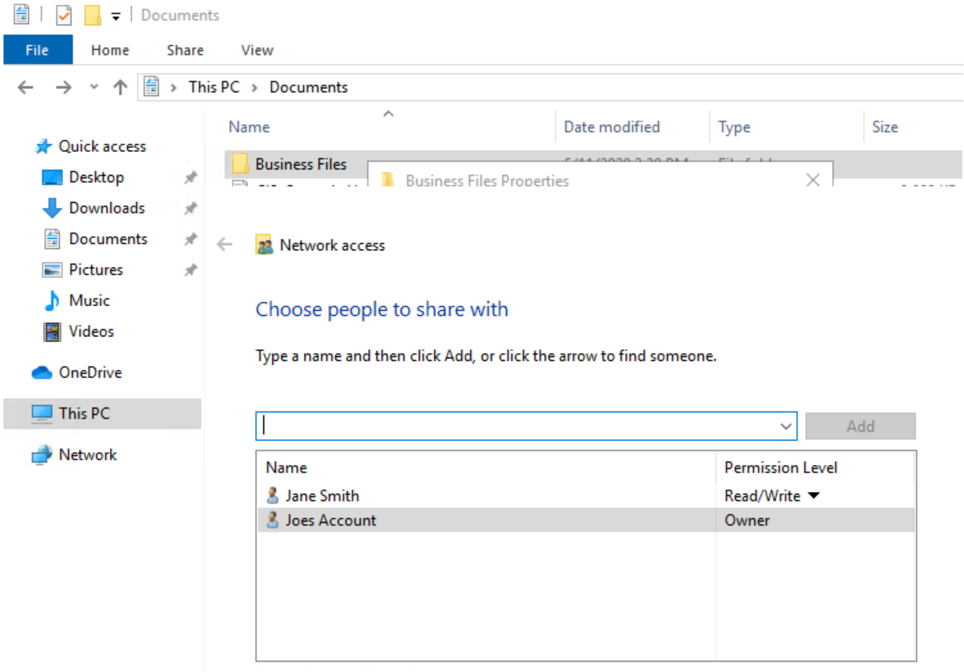
Data protection

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.



Network access

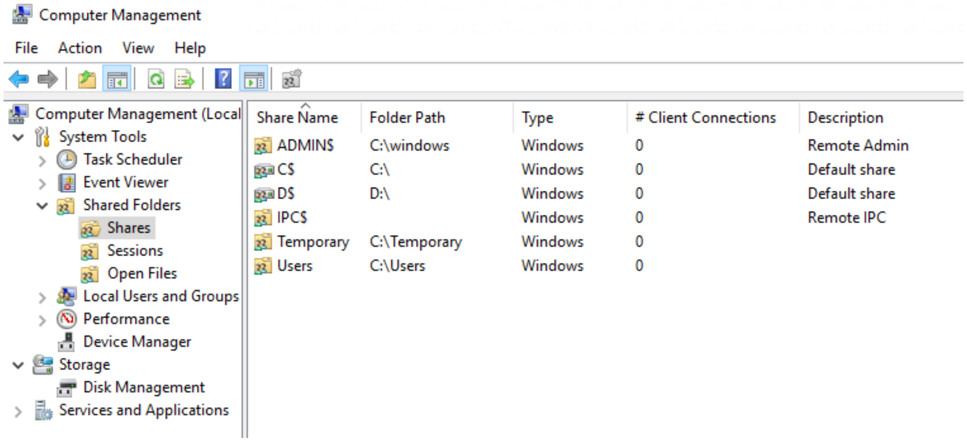
Choose people to share with

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

Name	Permission Level
Jane Smith	Read/Write
Joes Account	Owner

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.***

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



Share Name	Folder Path	Type	# Client Connections	Description
ADMIN$	C:\windows	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
D$	D:\	Windows	0	Default share
IPC$		Windows	0	Remote IPC
Temporary	C:\Temporary	Windows	0	
Users	C:\Users	Windows	0	

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.