

Lab 03 – Potential Hardening Techniques

David Murillo Santiago

Professor Valecha

IS-3423

28 November 2023

INTRODUCTION

In this lab, I aim to enhance the security of my Windows machine by implementing ten distinct host hardening techniques. These measures include incorporating AdBlockers, forcing logoff when inactivity/logon hours expire, enabling Hard Drive Encryption (BitLocker), updating, and patching the operating system, turning off Secondary Logon Services, closing unused ports and services, enabling Windows Notifications for Events, disabling default Windows services, installing, and updating an antivirus, and limiting the physical access of a host.

PROCESS

(Part A) Step 1: 10 Hardening Techniques

I chose to strengthen my device security by implementing the following 10 hardening techniques:

1. Use AdBlockers or Pop-Up Blockers

Ad-blockers are software tools designed to improve the online experience by blocking unwanted ads on web pages. Although they are widely used for this purpose, they also strengthen your computer's security, to the point that the FBI even recommends their use. Ad-blockers reduce the risk of inadvertently clicking on malicious ads, providing an added layer of security against malware and phishing attacks. These extensions also block ads in search results, protecting users from malicious campaigns impersonating legitimate brands. Additionally, they enhance privacy by preventing tracking tools embedded in ads from collecting user data. Because ad-blockers filter all pop-up advertising, websites may require you to disable ad-blocking as they earn money from displaying ads. Therefore, users should consider the impact on content creators and publishers who rely on ad revenue when employing these tools.

2. Force Logoff when Inactivity/Logon Hours Expire

Implementing an automatic logoff after user inactivity feature is a vital security measure. Force logoff reduces the risk of unauthorized access when a system is left unattended. Similarly, auto logoff after specified logon hours reinforces access restrictions, lowering the risk of unauthorized access during restricted time periods and ensuring compliance with company access policies. One downside to this feature is users may become frustrated as they have to login every time after briefly stepping away from the computer.

3. Enable Hard Drive Encryption (BitLocker)

Enabling hard drive encryption strengthens your device security, especially in the case that your device is stolen or has been accessed by malicious actors. The way it works is the contents of the hard drive go through an encryption process where only the users with the right password can access the information. One disadvantage of encrypting your hard drive with a password is if the password is forgotten. Good password management is required as forgetting the password will likely result in the loss of the data.

4. Update and Patch Operating System

Updating your Operating System is an important hardening activity as the system updates include security patches for found vulnerabilities. Checking for updates regularly is an important security measure to protect yourself from vulnerability exploitation. Although updating your devices is important, one disadvantage of frequent updates is it may create application compatibility issues until the application developers too release an update.

5. Turning Off Secondary Logon Services

Disabling the Secondary Logon service is a security move involving the shutdown of a Windows service responsible for running processes with alternative credentials. Because this service allows users to execute programs with different credentials, it poses a security risk if exploited. Turning off Secondary Logon Services mitigates privilege escalation threats and unauthorized access. However, one downside of turning the service off is some applications rely on this service, leading to compatibility issues.

6. Close Unused Ports and Services

Closing unused ports and services is a fundamental step in computer hardening. Ports are communication endpoints that allow data to be transmitted between a computer and external networks. By closing unused ports, you minimize potential points of entry for cyber threats. Closing unused ports is important to limit your attack surface, but one must be careful when closing ports as closing the wrong one may impede network traffic and cause Network issues.

7. Enable Windows Notifications if Events.

Windows notifications offer real-time alerts which encompass software updates, system warnings, and security events. By enabling notifications, users can become immediately informed of new updates that are released. One downside to enabling notifications is information overload. A user may become fatigued from constant alerts and begin to ignore them all together. Therefore, it is important to prioritize the important notifications.

8. Disable Default Windows Services

Windows defaults various services, some of which are nonessential for specific users. By deactivating unnecessary services, users improve system security as the unused services will no longer have access to the machine. One disadvantage of disabling services is if you accidentally disable the wrong service, you may affect the functionality of your device. Therefore, it is important to research the service you are disabling prior to disabling it.

9. Install and Update an Antivirus

Installing anti-virus software helps defend against various threats such as viruses, Trojans, spyware, and ransomware. Anti-virus software offers continuous detection and behavioral analysis and also remove threats. Although anti-virus software can be helpful, some of them are signature based, meaning they rely on known identifiers of specific malware. If the malware is new and its signature has yet to be identified, it is unlikely the anti-virus would detect the malware.

10. Limit the Physical Access of a Host

Limiting the physical access of a host is a fundamental practice in computer security. It involves restricting direct interaction with the actual hardware, such as servers, desktops, or laptops. This prevents unauthorized tampering with the system, stealing sensitive data, or introducing malicious software. While it enhances protection, strict limitations on physical access can create inconvenience for legitimate users who may require direct access for tasks like maintenance, upgrades, or troubleshooting.

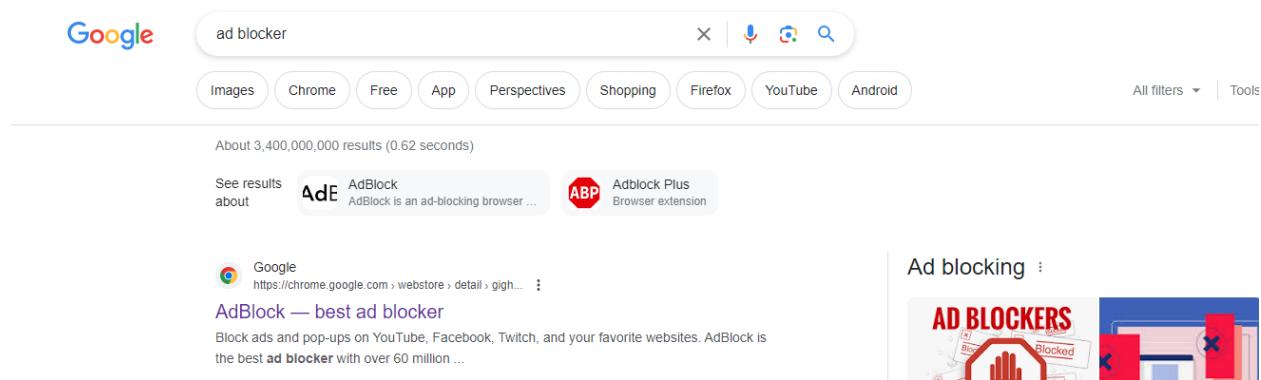
(Part B) Step 2: 10 Hardening Techniques

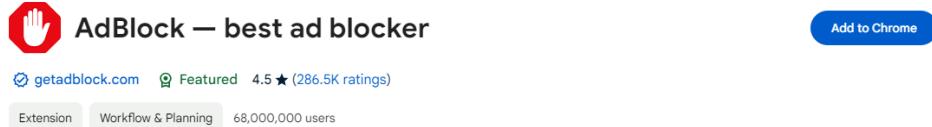
1. Incorporating AdBlockers

I will download Google's ad-blocker to help block pop-up ads and third-party tracking.

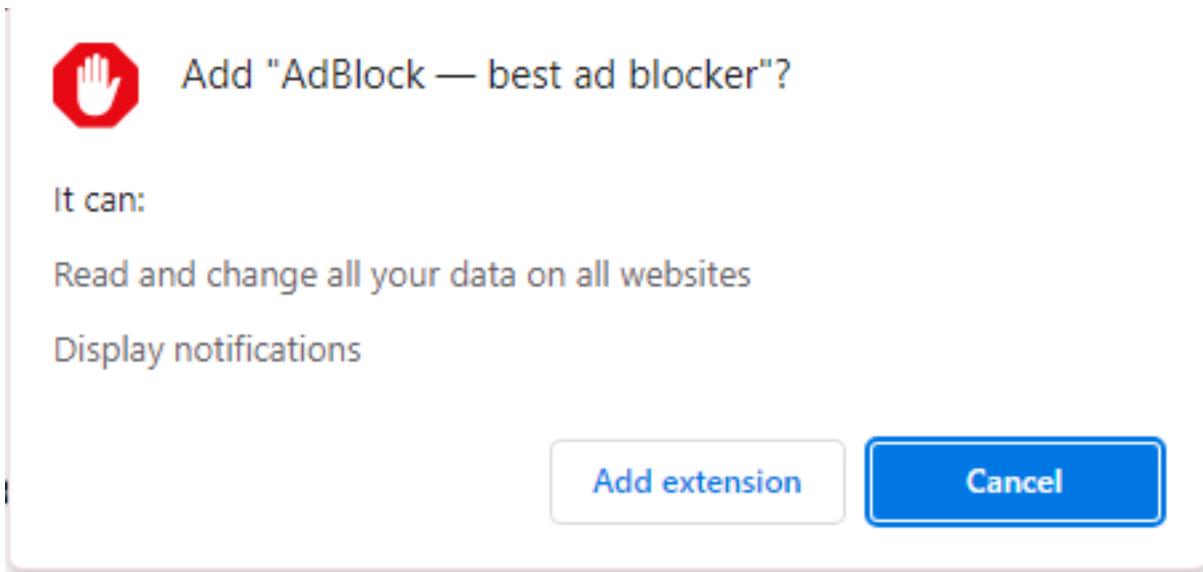
Step 1: *Google AdBlock*

To begin, I searched up AdBlocker on Google, to look for the Chrome extension 'AdBlocker.'

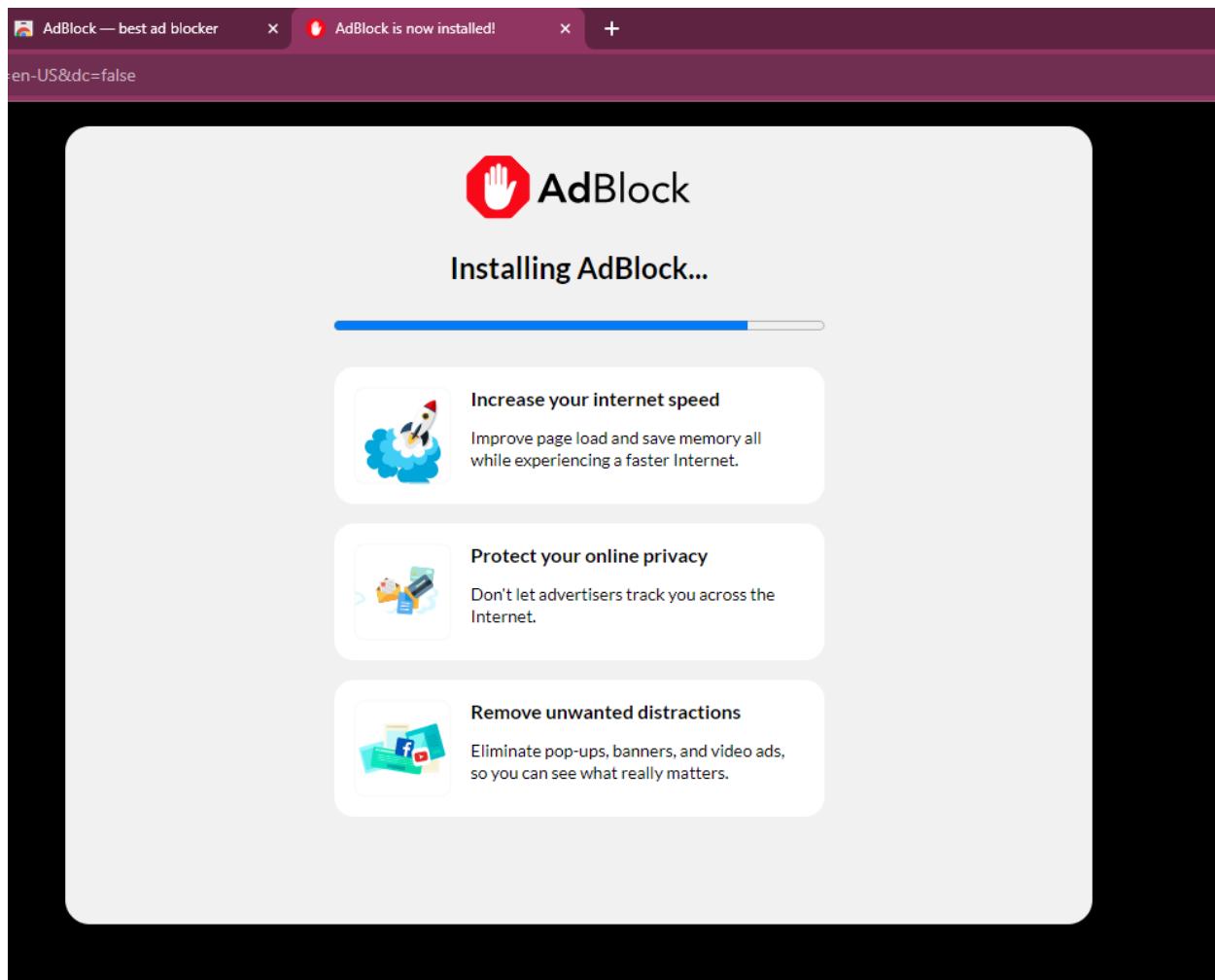




Next, I entered the website and clicked 'Add to Chrome' to download the extension.

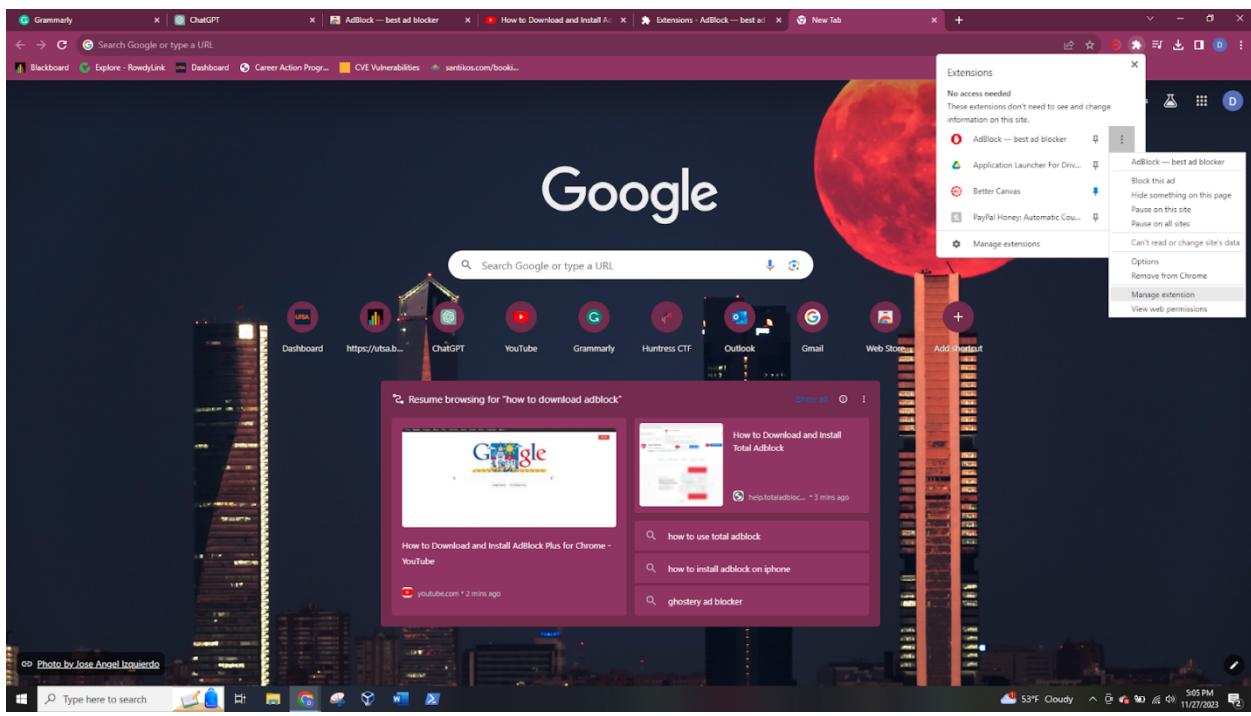


Next, I clicked "Add extension.'



Next, the extension was downloading and when it fully downloaded, it took me to a page which asked me to donate. Once it fully downloaded, I closed the donation page because the extension is free.

Now that the extension is fully downloaded, I wanted to analyze the settings.

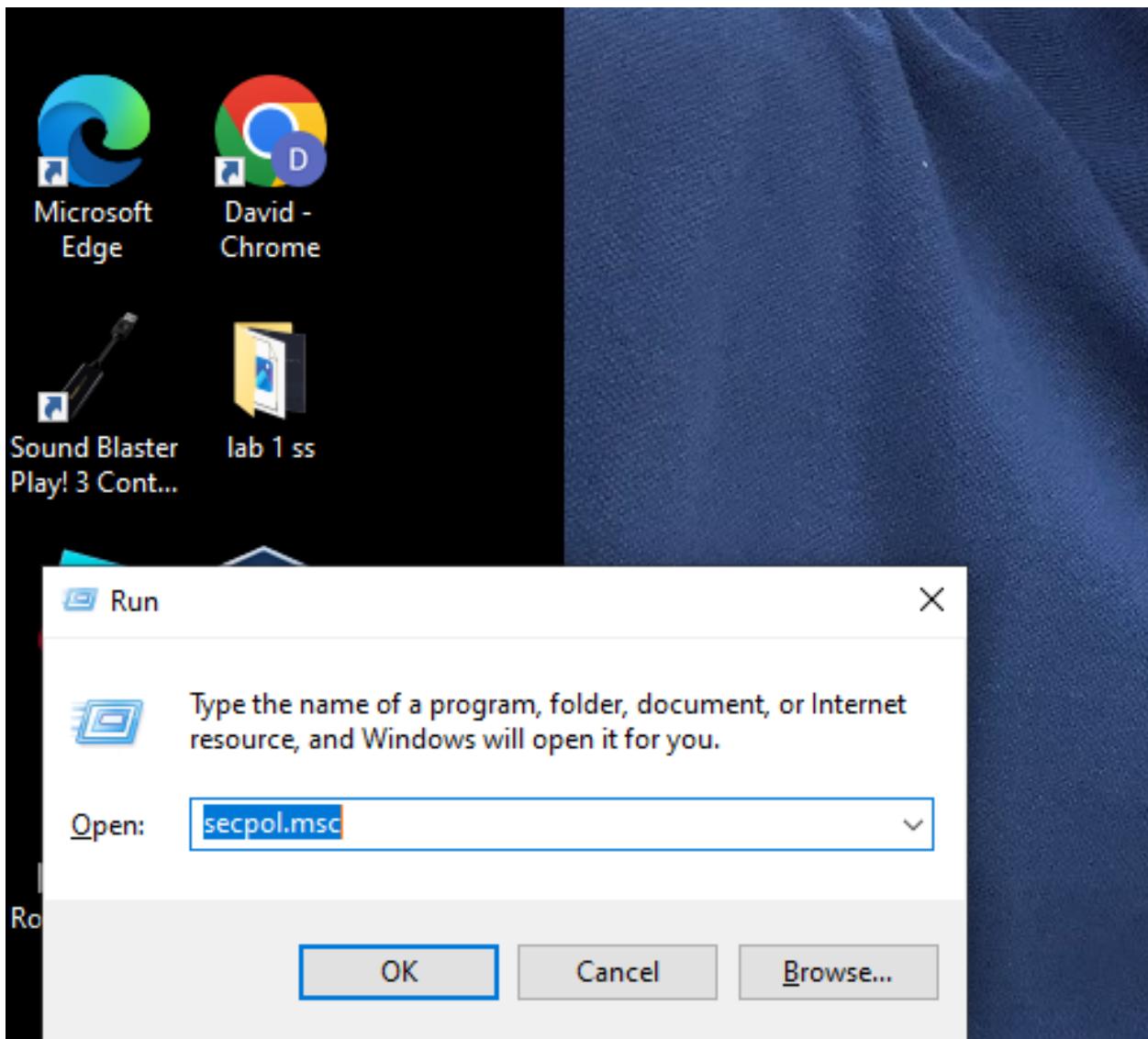


To analyze the settings, you click on the ‘puzzle’ icon and then the 3 dots besides ‘Ad Block.’ Next, you click on ‘Manage Extension.’

Version	5.15.0
Size	14.1 MB
Permissions	<ul style="list-style-type: none">• Read and change all your data on all websites• Display notifications
Site access	<p>Allow this extension to read and change all your data on websites you visit: ?</p> <p>On all sites </p>
Site settings	
Pin to toolbar	
Allow in Incognito	
Warning: Google Chrome cannot prevent extensions from recording your browsing history. To disable this extension in Incognito mode, unselect this option.	
Allow access to file URLs	
Extension options	
View in Chrome Web Store	
Source	Chrome Web Store
Remove extension	

In the settings you could choose whether you want the AdBlocker to work on all sites, specific sites, or whether you want it to continue working on Incognito mode.

2. Forcing logoff when inactivity/logon hours expire



First I used the window key + r shortcut to bring up the run line. Once the run line comes up, I entered 'secpol.msc' to bring the security policies for my local machine.

Local Security Policy

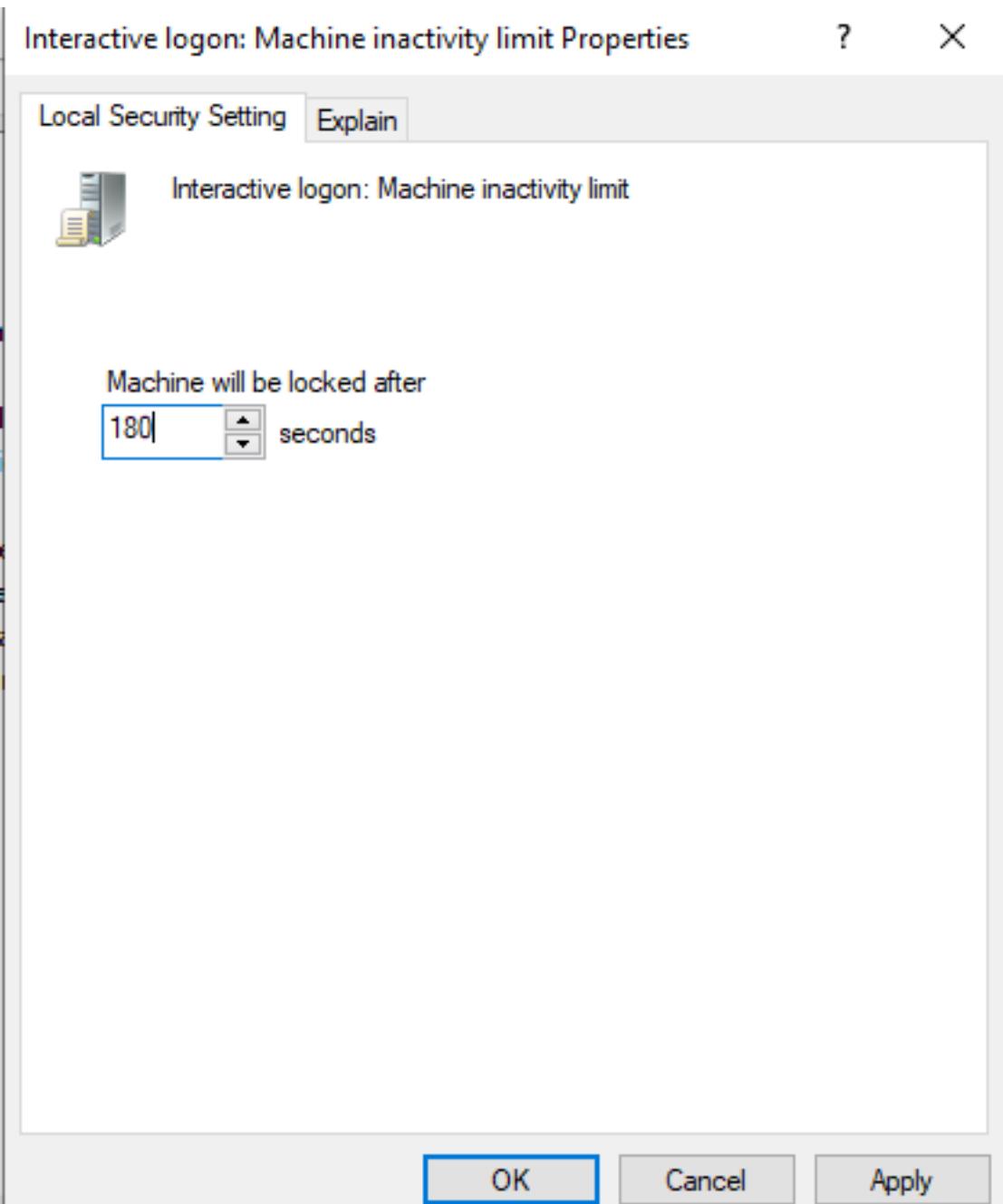
File Action View Help

Security Settings

- > Account Policies
- > Local Policies
 - > Audit Policy
 - > User Rights Assignment
 - Security Options**
- > Windows Defender Firewall with Adv...
- > 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
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Don't display last signed-in	Disabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...)	10 logons
Interactive logon: Prompt user to change password before e...	5 days
Interactive logon: Require Domain Controller authentication...	Disabled
Interactive logon: Require Windows Hello for Business or sm...	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (al...	Disabled
Microsoft network client: Digitally sign communications (if ...	Enabled
Microsoft network client: Send unencrypted password to thi...	Disabled
Microsoft network server: Amount of idle time required bef...	Not Defined
Microsoft network server: Attempt S4U2Self to obtain claim ...	Not Defined
Microsoft network server: Digitally sign communications (al...	Disabled
Microsoft network server: Digitally sign communications (if ...	Disabled
Microsoft network server: Disconnect clients when logon ho...	Enabled
Microsoft network server: Server SPN target name validation...	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of S...	Enabled

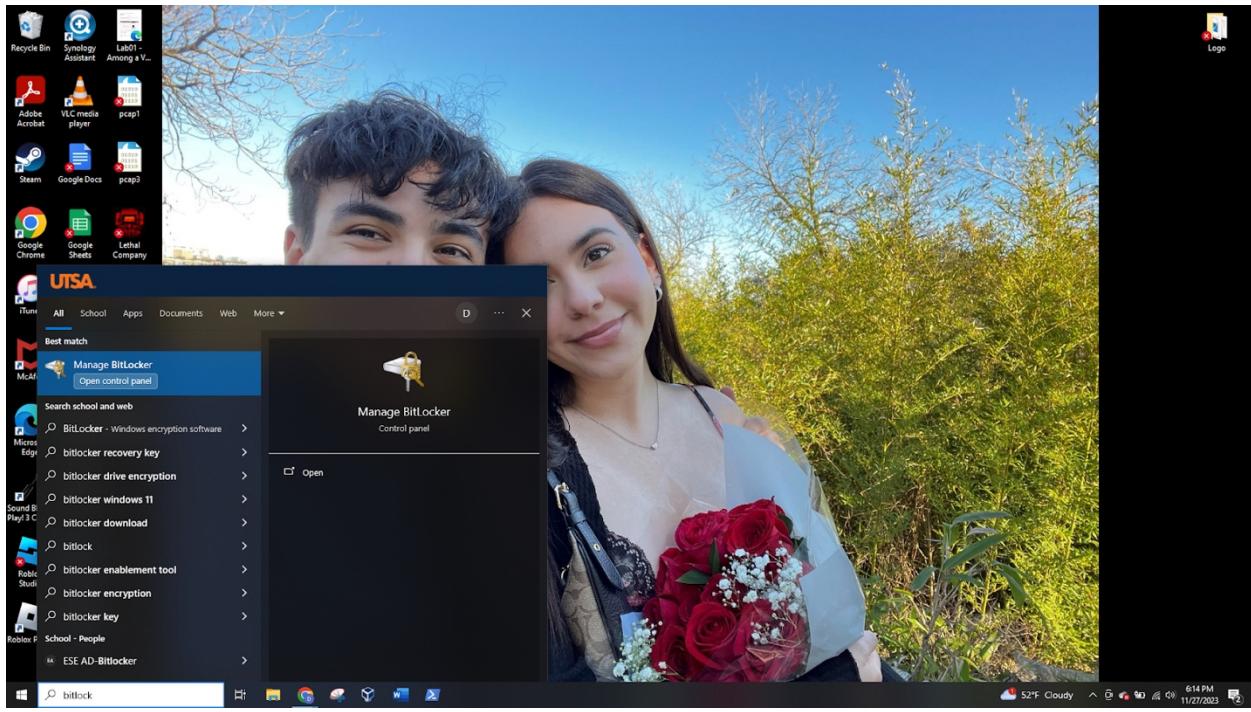
Next, I expanded the 'Local Policies' and clicked 'Security Options' and I looked for 'Interactive logon: Machine inactivity limit.'



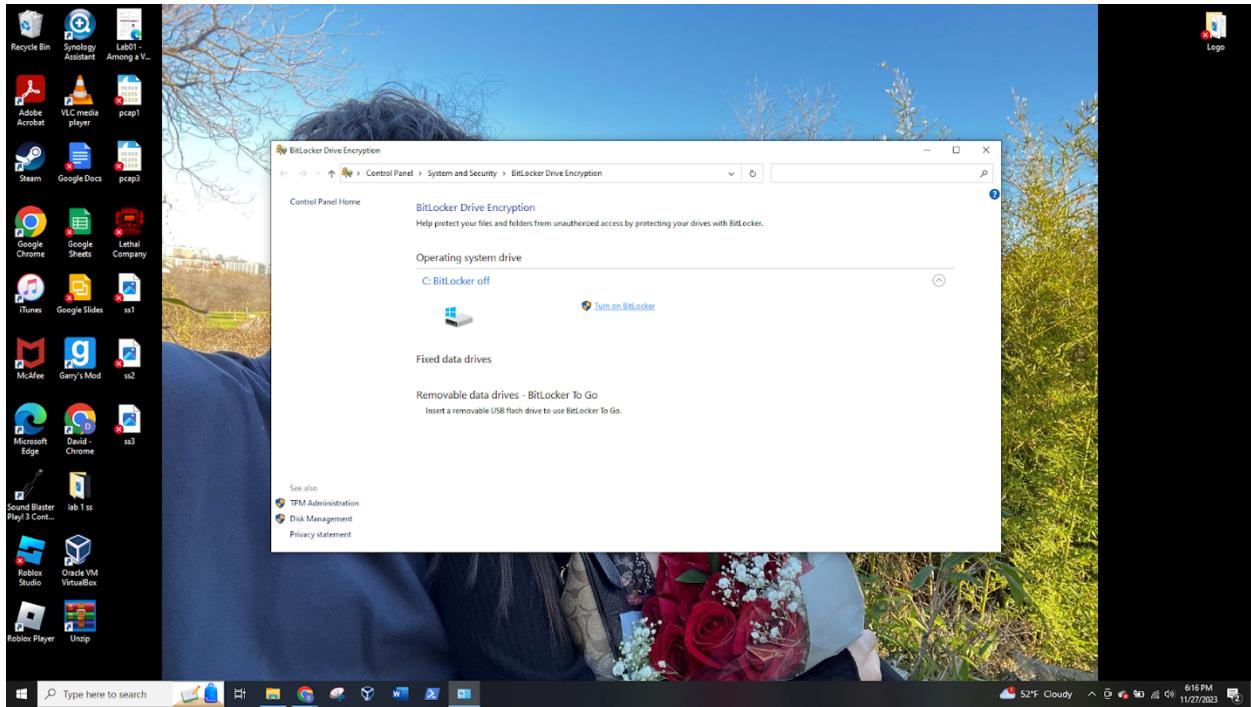
Next, I set the machine to lock after 180 seconds in order to ensure the machine is locked after being inactive for 3 minutes.

Next, I clicked and apply in order to apply the security changes.

3. Enabling Hard Drive Encryption (BitLocker)



First, I searched for BitLocker on the Windows search bar and I clicked on “Manage BitLocker.”



Next, I clicked on the shield that says “Turn on BitLocker.”

X

← BitLocker Drive Encryption (C:)

Starting BitLocker

- ✖ This device can't use a Trusted Platform Module. Your administrator must set the "Allow BitLocker without a compatible TPM" option in the "Require additional authentication at startup" policy for OS volumes.

.....
[What are BitLocker's system requirements?](#)

Cancel

Next, I got this error which stated that I need to have the administrative account enable BitLocker without a compatible TPM option.

Run

X



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open:

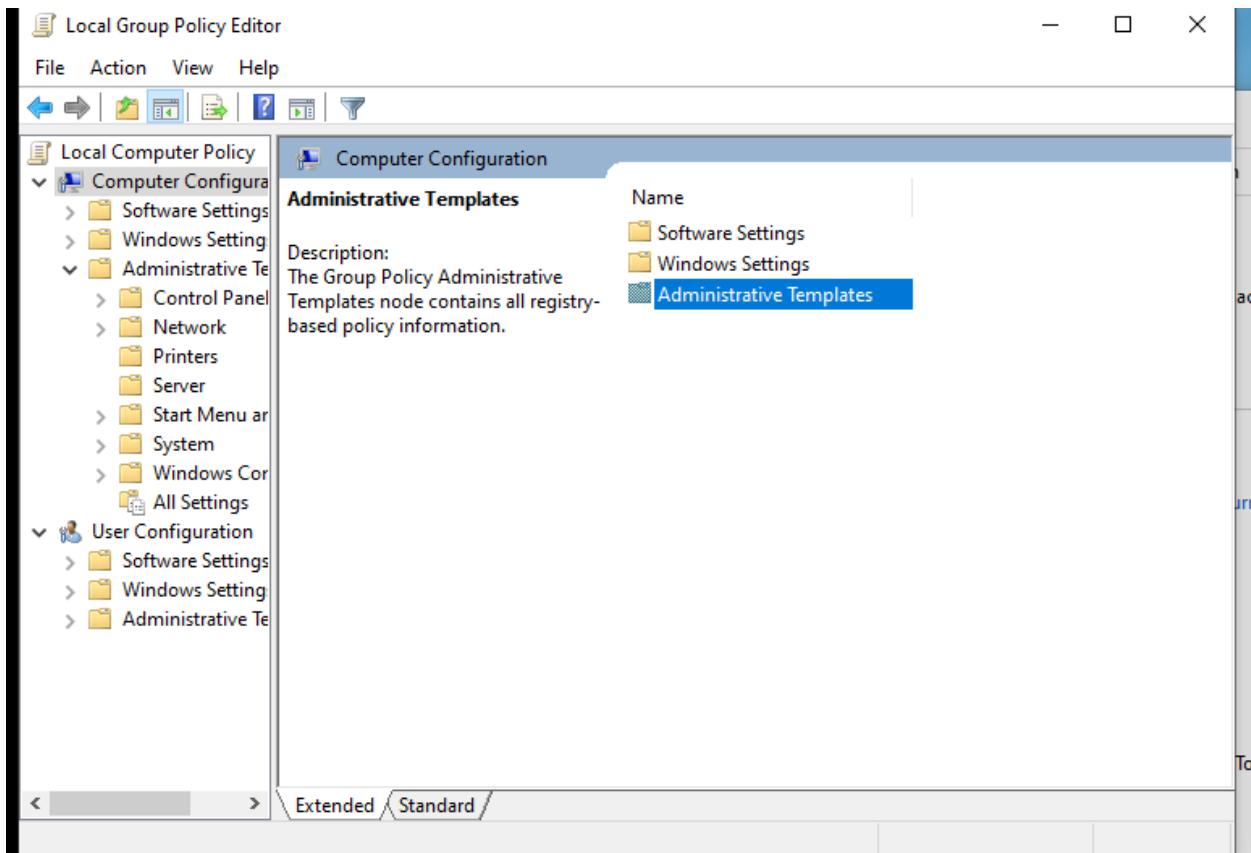
gpedit.msc

OK

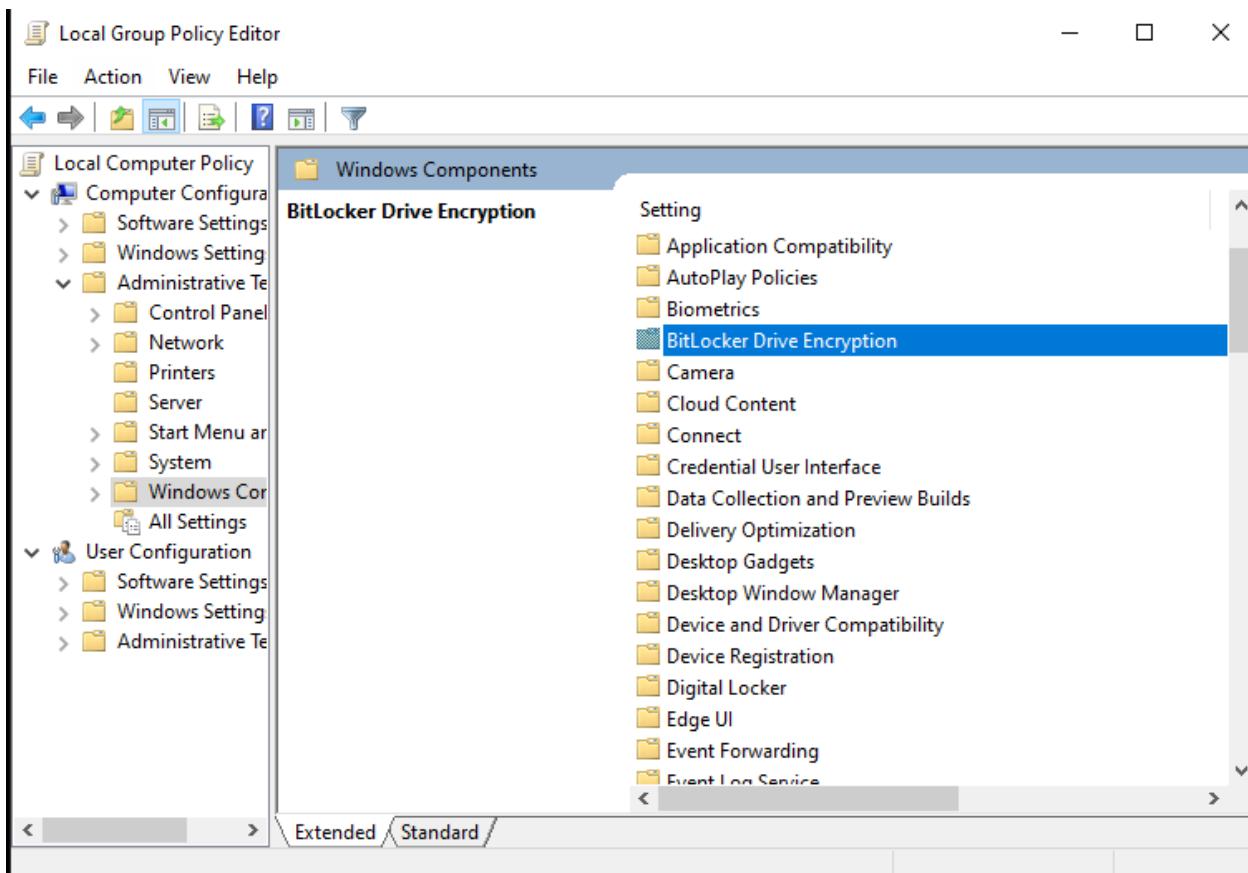
Cancel

Browse...

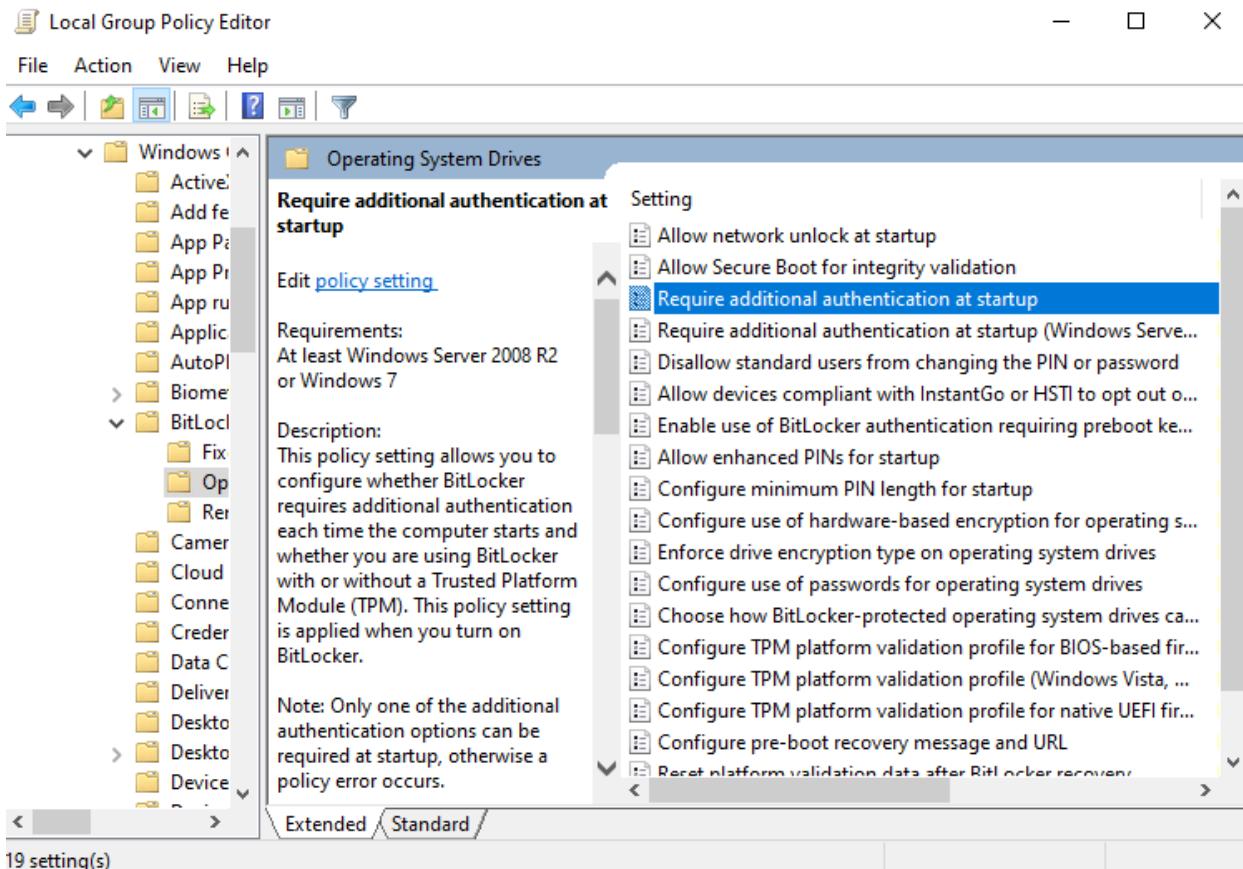
To fix this error, I opened the run line and searched 'gpedit.msc' to open the Local Group Policy Editor.



Next, I clicked on "Computer Configuration" and "Administrative Templates."

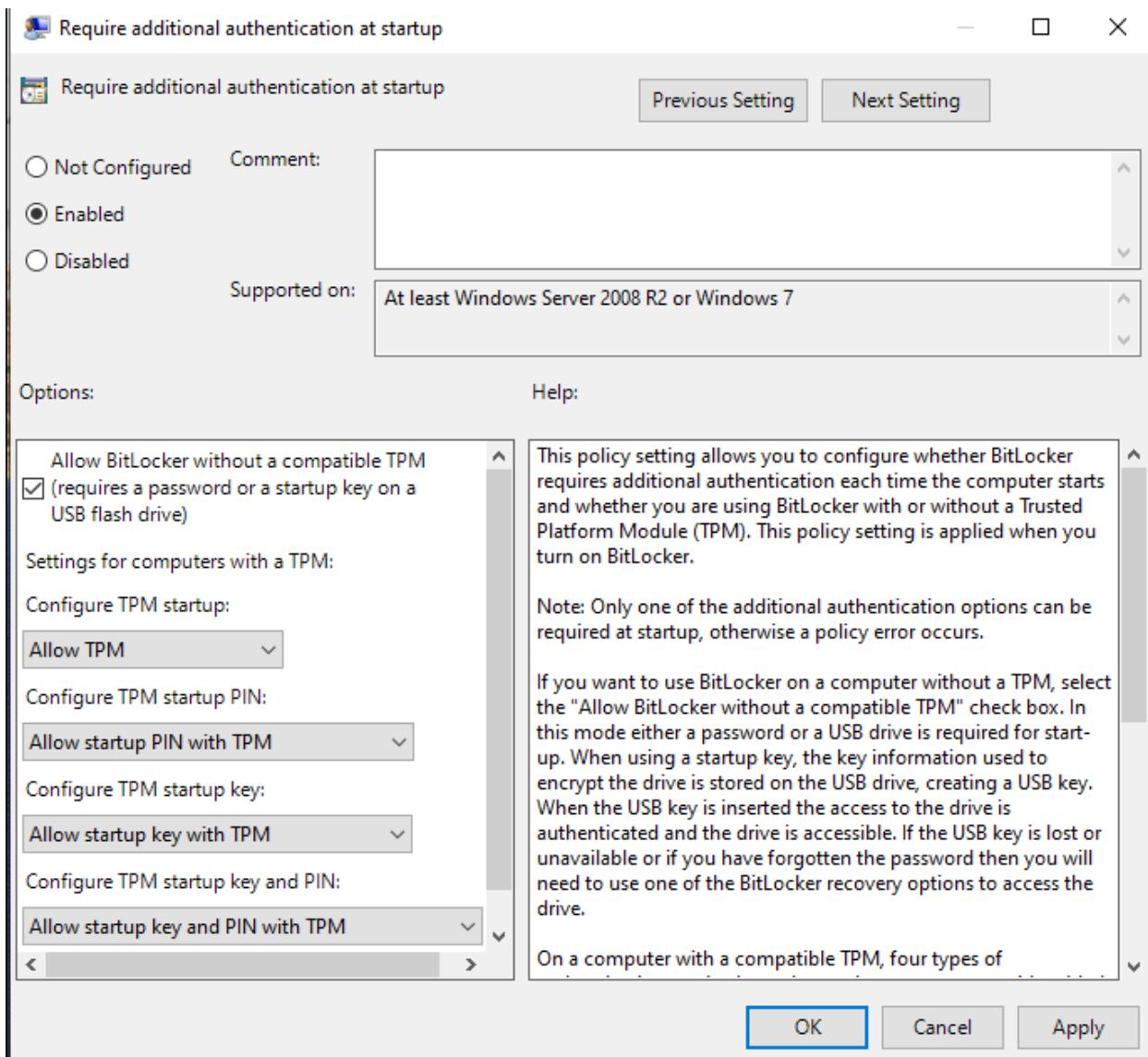


Next, I clicked on Windows Components and BitLocker Drive Encryption.



19 setting(s)

Next, I clicked on "Operating System Drives" and then I clicked on "Require additional authentication at startup."



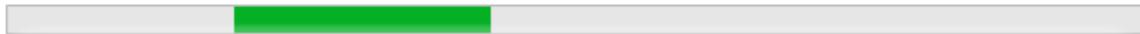
Once on “Require additional authentication at startup,” I clicked ‘enable’ and then applied my changes.

X

← BitLocker Drive Encryption (C:)

Checking your PC's configuration

BitLocker is verifying that your PC meets its system requirements. This might take a few minutes.



[What are BitLocker's system requirements?](#)

Cancel

Next, I went back to turn on “BitLocker” by clicking on the shield icon.

X

← BitLocker Drive Encryption (C:)

Drive preparation is complete

BitLocker must restart your computer to finish preparing your system drive for encryption.

[Restart now](#)

Next, BitLocker asked me to restart my device.

X

← BitLocker Drive Encryption (C:)

BitLocker Drive Encryption setup

When you turn on BitLocker, your computer performs the following steps:

- ✓ Prepare your drive for BitLocker
Encrypt the drive

[What are BitLocker's system requirements?](#)

Next **Cancel**

Once I restarted my computer, this screen popped up and I clicked next to encrypt the drive.

X

← BitLocker Drive Encryption (C:)

Choose how to unlock your drive at startup

- i** Some settings are managed by your system administrator.

To help keep your data more secure, you can have BitLocker prompt you to enter a password or insert a USB flash drive each time you start your PC.

→ Insert a USB flash drive

→ Enter a password

I chose to encrypt the drive with a password.

Cancel

X

← BitLocker Drive Encryption (C:)

Create a password to unlock this drive

You should create a strong password that uses uppercase and lowercase letters, numbers, symbols, and spaces.

Enter your password

 ······

Reenter your password

 ······

[Tips for creating a strong password.](#)

Next

Cancel

I chose a safe password that used a combination of capital letters and numbers and special characters.

X

← BitLocker Drive Encryption (C:)

How do you want to back up your recovery key?

 Some settings are managed by your system administrator.

A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC.

→ Save to your Azure AD account

→ Save to a USB flash drive

→ Save to a file

→ Print the recovery key

[How can I find my recovery key later?](#)

Next

Cancel

Next, I chose to print recovery key so I could keep a copy saved in my lockbox in case I forget the password.

X

← BitLocker Drive Encryption (C:)

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected—even data that you deleted but that might still contain retrievable info.

- Encrypt used disk space only (faster and best for new PCs and drives)
- Encrypt entire drive (slower but best for PCs and drives already in use)

Next

Cancel

Next, I chose to encrypt the entire drive because this PC is already in use.

X

← BitLocker Drive Encryption (C:)

Choose which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

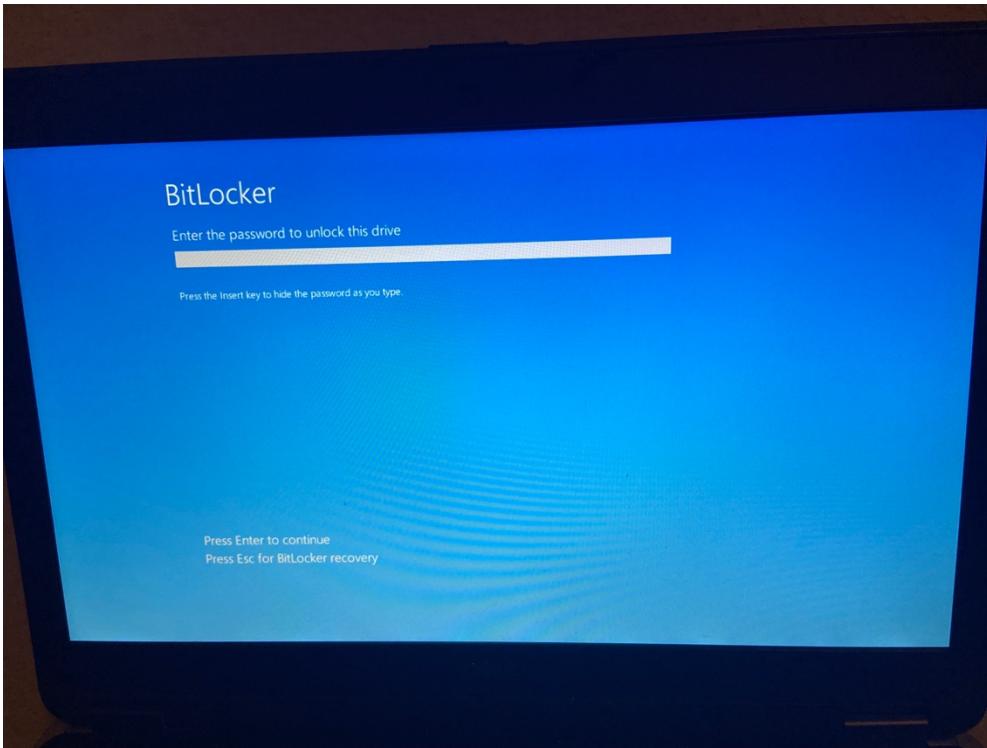
If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

- New encryption mode (best for fixed drives on this device)
 Compatible mode (best for drives that can be moved from this device)

Next

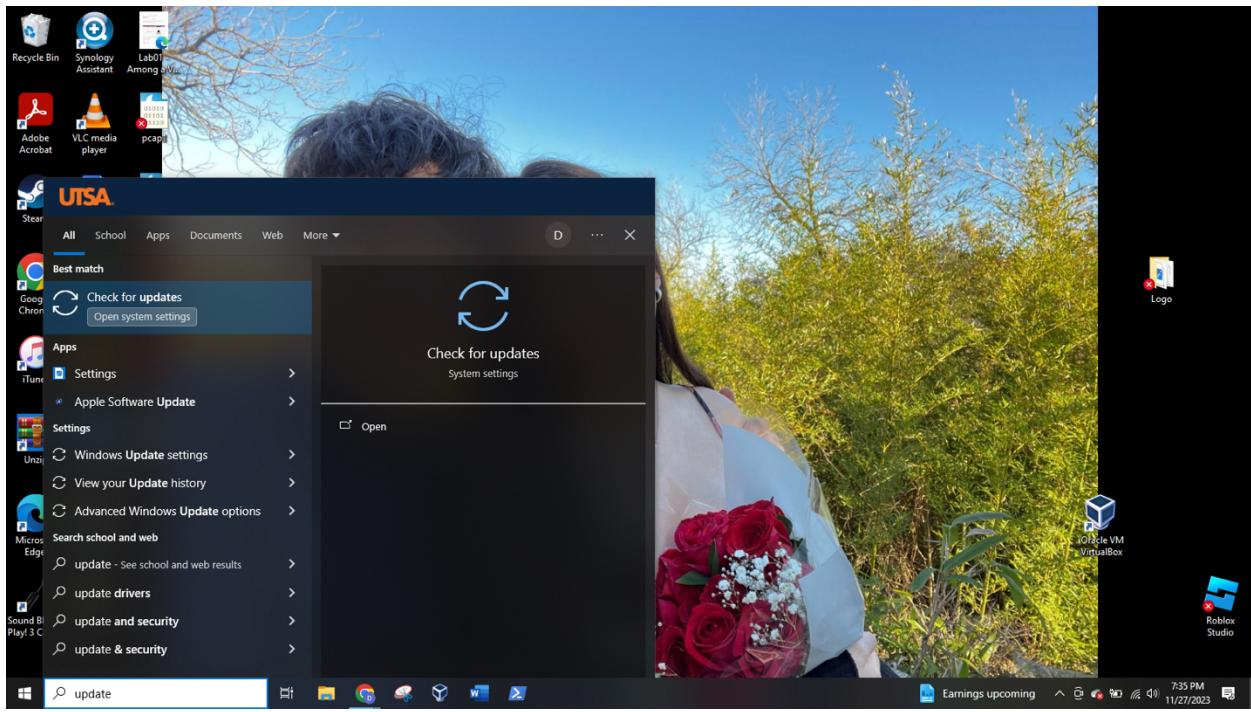
Cancel

Next, I used the 'New encryption mode' because my drive is fixed to my device.



Finally, I restarted my computer to finalize the set-up of BitLocker. Once the device rebooted, I was able to verify that BitLocker was turned on as I was prompted to enter the BitLocker password to access the hard drive.

4. Updating and patching the operating system



To update the OS, search 'update' on the Windows search bar and select 'Check for updates.'



Windows Update



You're up to date

Last checked: Today, 6:14 PM

[Check for updates](#)

[View optional updates](#)



Pause updates for 7 days

Visit Advanced options to change the pause period



Change active hours

Currently 3:00 AM to 2:00 PM



View update history

See updates installed on your device

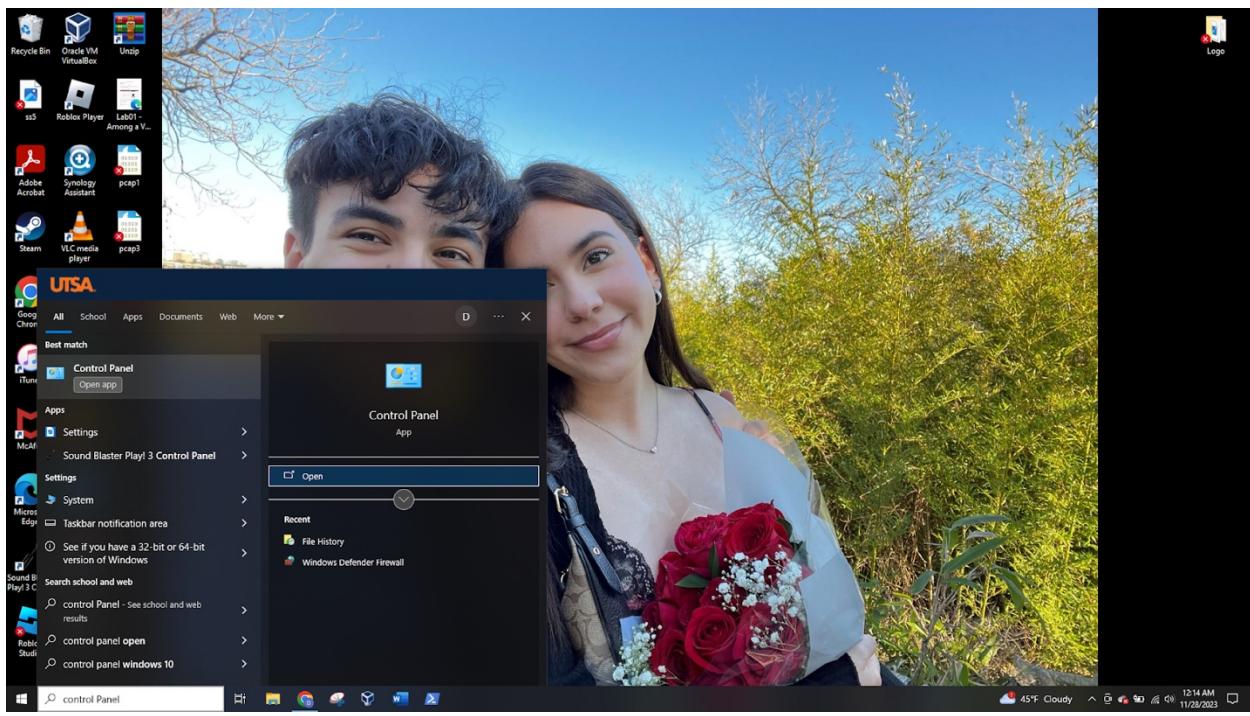


Advanced options

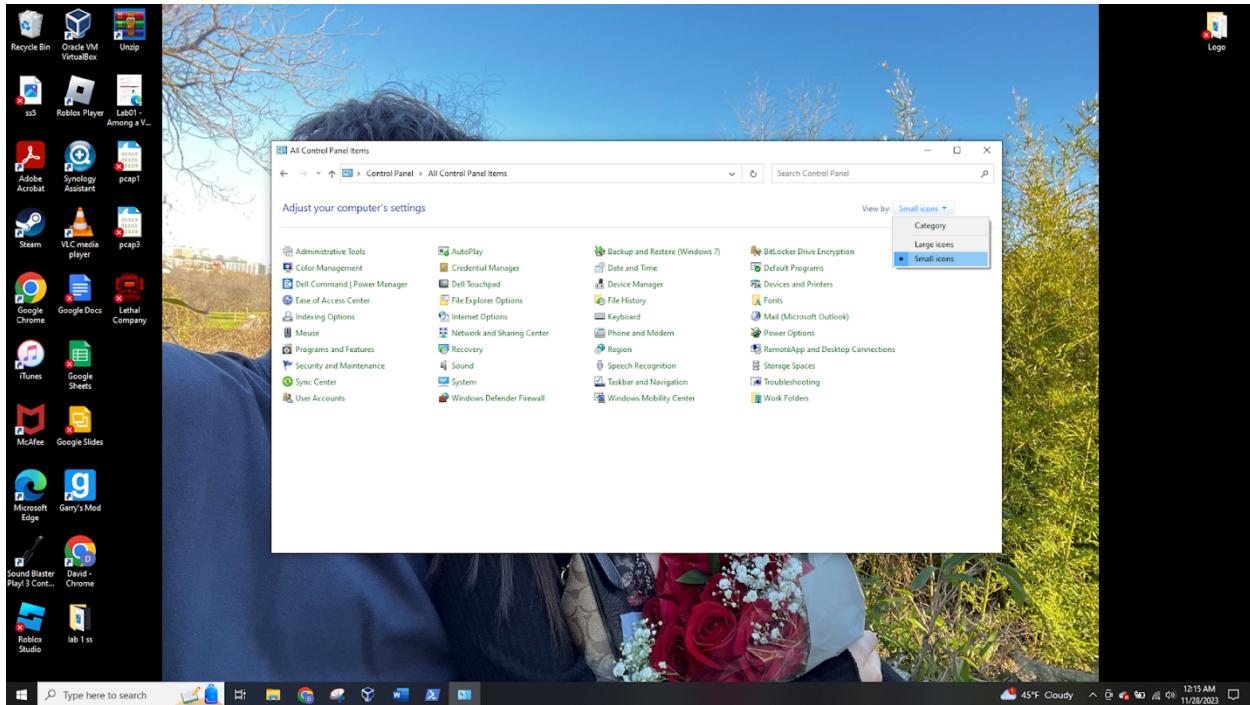
Additional update controls and settings

Once here, you can view if an update is available or if your device is up to date. You could also select 'View optional updates' if you'd like. My device is already up to date so there are no more patches or updates I could download.

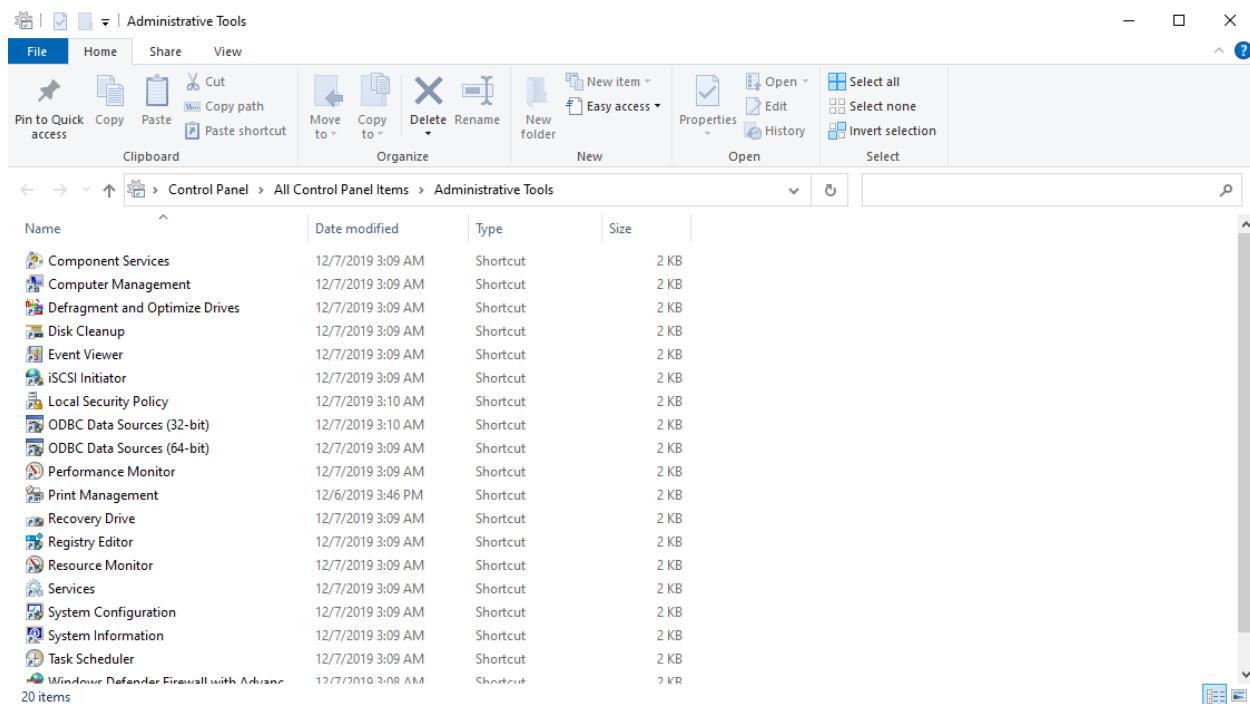
5. Turning off Secondary Logon Services



To begin, I searched for and opened the 'Control Panel.'



Next, I filtered the panel by 'small icons.'



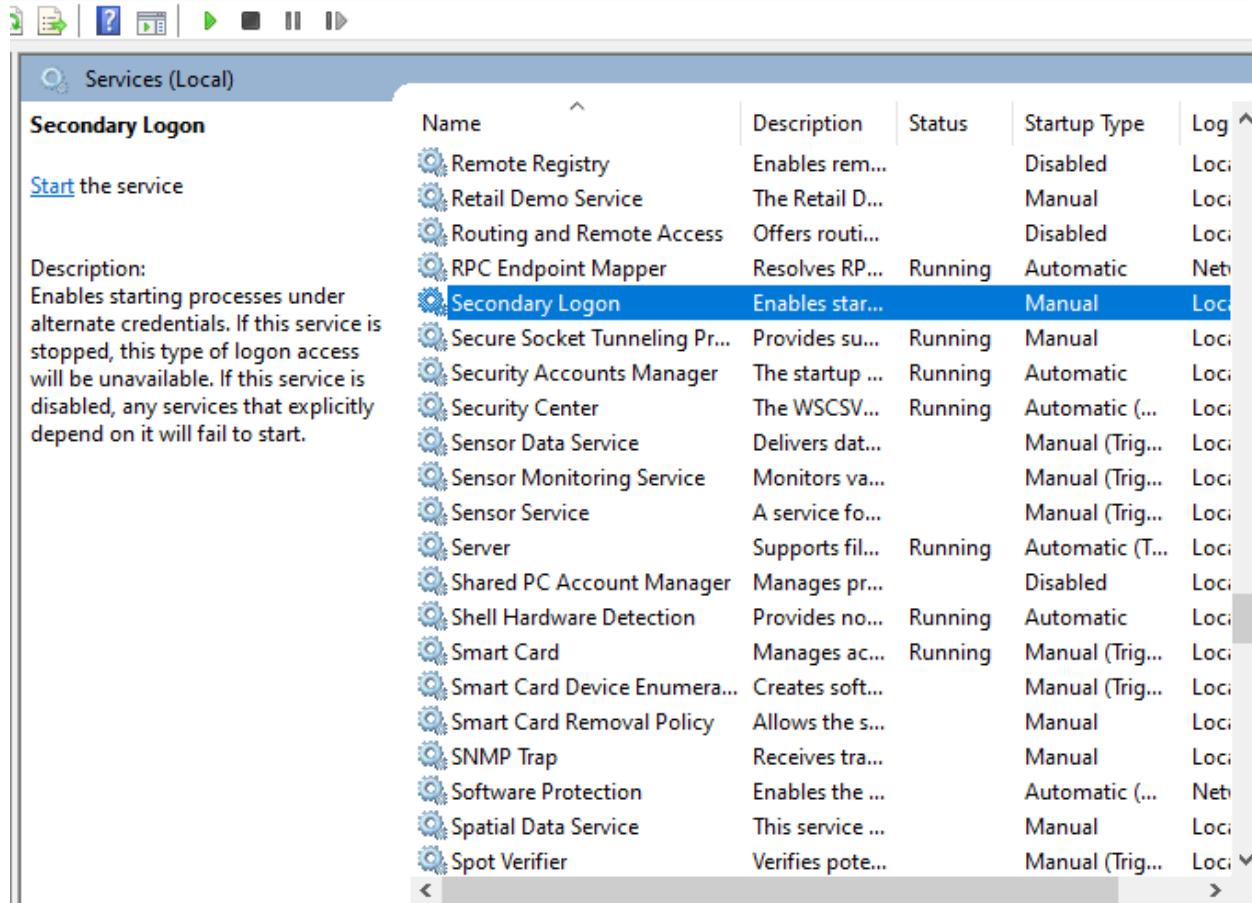
Next, I selected 'administrative tools.'

Name	Date modified	Type	Size
Component Services	12/7/2019 3:09 AM	Shortcut	2 KB
Computer Management	12/7/2019 3:09 AM	Shortcut	2 KB
Defragment and Optimize Drives	12/7/2019 3:09 AM	Shortcut	2 KB
Disk Cleanup	12/7/2019 3:09 AM	Shortcut	2 KB
Event Viewer	12/7/2019 3:09 AM	Shortcut	2 KB
iSCSI Initiator	12/7/2019 3:09 AM	Shortcut	2 KB
Local Security Policy	12/7/2019 3:10 AM	Shortcut	2 KB
ODBC Data Sources (32-bit)	12/7/2019 3:10 AM	Shortcut	2 KB
ODBC Data Sources (64-bit)	12/7/2019 3:09 AM	Shortcut	2 KB
Performance Monitor	12/7/2019 3:09 AM	Shortcut	2 KB
Print Management	12/6/2019 3:46 PM	Shortcut	2 KB
Recovery Drive	12/7/2019 3:09 AM	Shortcut	2 KB
Registry Editor	12/7/2019 3:09 AM	Shortcut	2 KB
Resource Monitor	12/7/2019 3:09 AM	Shortcut	2 KB
Services	12/7/2019 3:09 AM	Shortcut	2 KB
System Configuration	12/7/2019 3:09 AM	Shortcut	2 KB
System Information	12/7/2019 3:09 AM	Shortcut	2 KB
Task Scheduler	12/7/2019 3:09 AM	Shortcut	2 KB
Windows Defender Firewall with Advance	12/7/2010 3:08 AM	Shortcut	2 KB

20 items | 1 item selected 1.13 KB

I then selected services.

Help

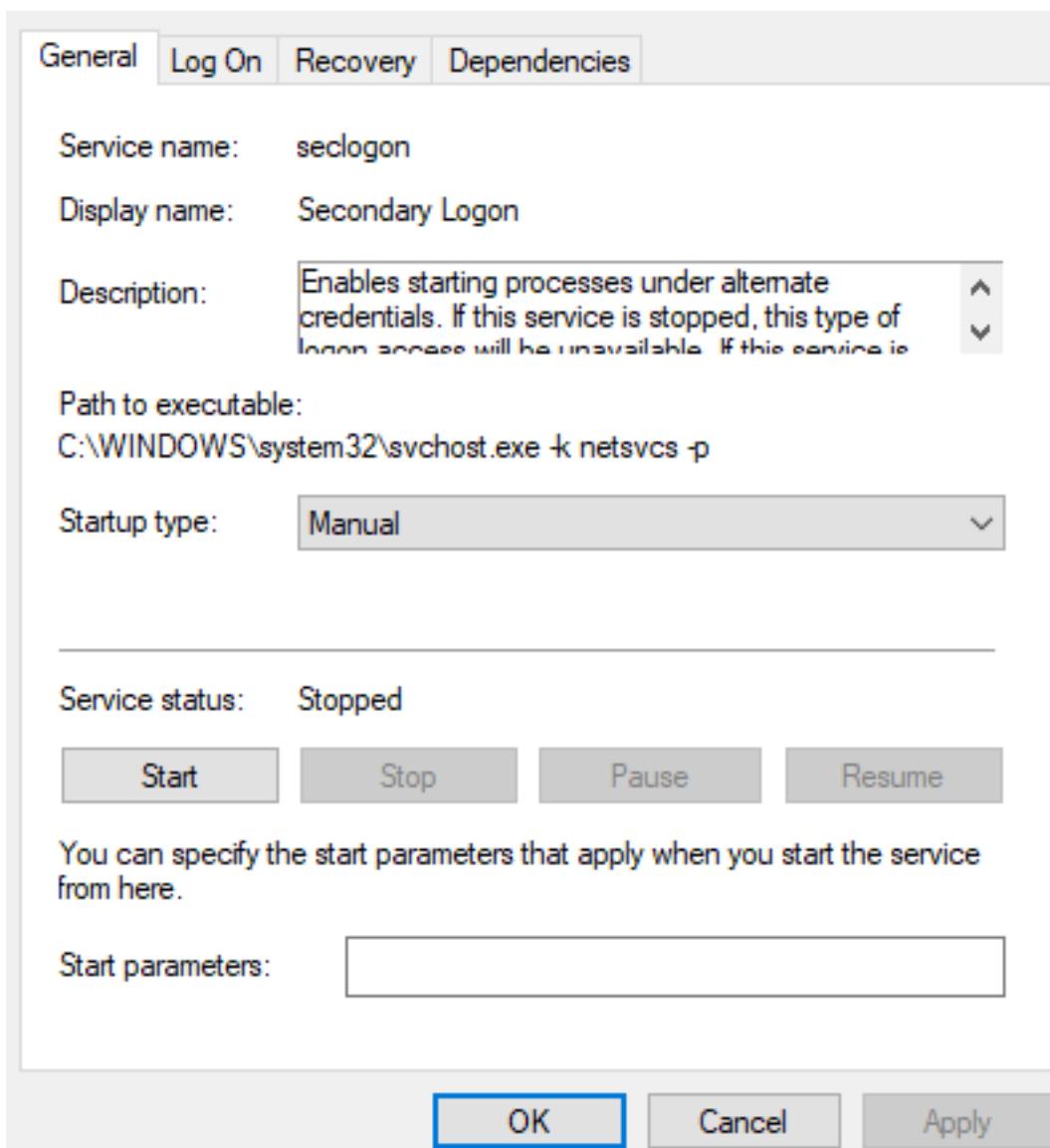
A screenshot of the Windows Services Local window. The title bar says "Services (Local)". The left pane shows a section titled "Secondary Logon" with a link to "Start the service". Below it is a "Description:" block stating: "Enables starting processes under alternate credentials. If this service is stopped, this type of logon access will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start." The right pane is a table with columns: Name, Description, Status, Startup Type, and Log. The "Secondary Logon" service is highlighted in blue. The table data is as follows:

Name	Description	Status	Startup Type	Log
Remote Registry	Enables rem...	Disabled	Locally	
Retail Demo Service	The Retail D...	Manual	Locally	
Routing and Remote Access	Offers routi...	Disabled	Locally	
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network
Secondary Logon	Enables star...	Manual	Locally	
Secure Socket Tunneling Pr...	Provides su...	Running	Manual	Locally
Security Accounts Manager	The startup ...	Running	Automatic	Locally
Security Center	The WSCSV...	Running	Automatic (...)	Locally
Sensor Data Service	Delivers dat...		Manual (Trig...	Locally
Sensor Monitoring Service	Monitors va...		Manual (Trig...	Locally
Sensor Service	A service fo...		Manual (Trig...	Locally
Server	Supports fil...	Running	Automatic (T...	Locally
Shared PC Account Manager	Manages pr...		Disabled	Locally
Shell Hardware Detection	Provides no...	Running	Automatic	Locally
Smart Card	Manages ac...	Running	Manual (Trig...	Locally
Smart Card Device Enumera...	Creates soft...		Manual (Trig...	Locally
Smart Card Removal Policy	Allows the s...		Manual	Locally
SNMP Trap	Receives tra...		Manual	Locally
Software Protection	Enables the ...		Automatic (...)	Network
Spatial Data Service	This service ...		Manual	Locally
Spot Verifier	Verifies pote...		Manual (Trig...	Locally

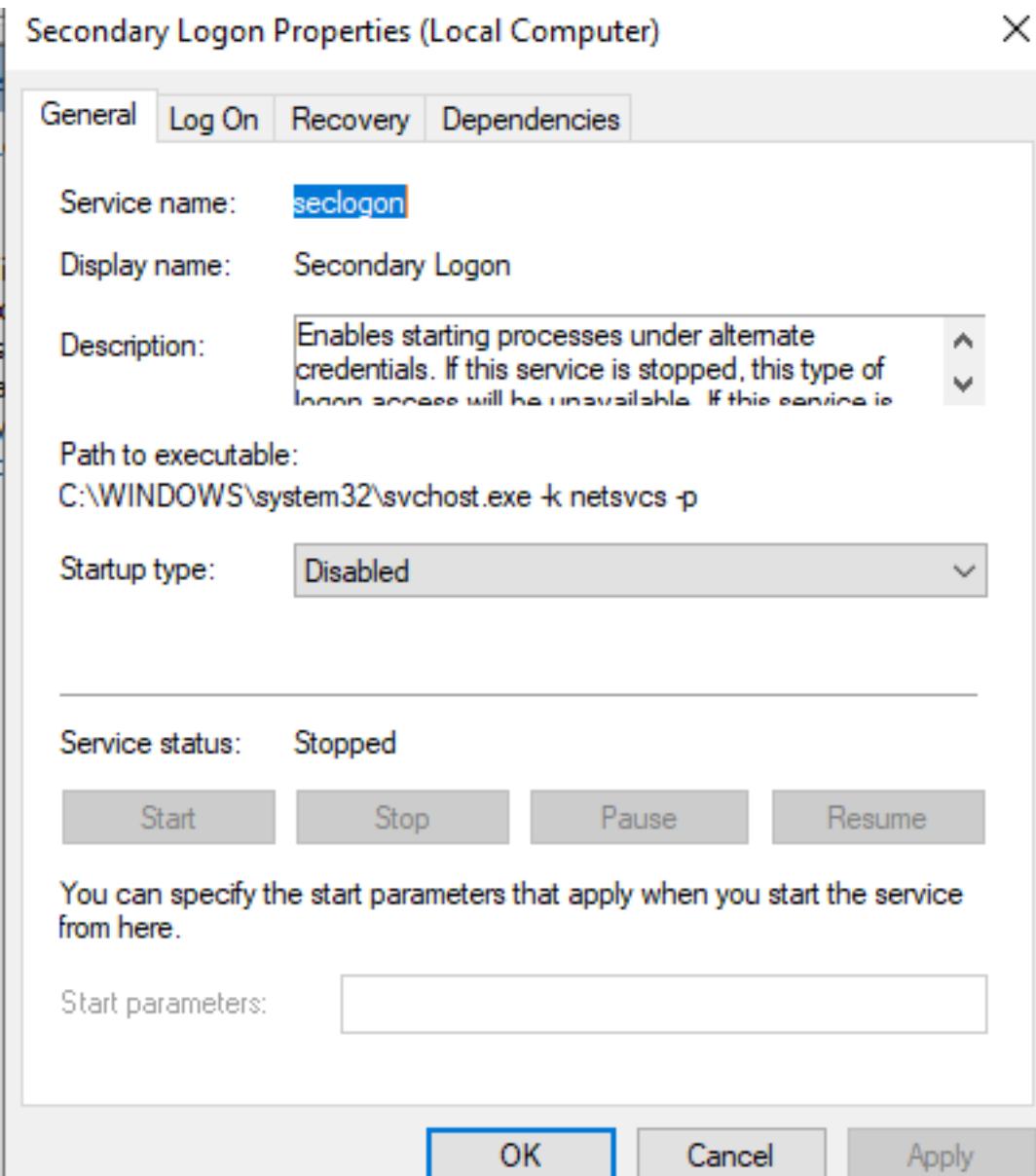
Next, I looked for "Secondary Logon."

Secondary Logon Properties (Local Computer)

X



Next, I right clicked on "Secondary Logon" and selected "Properties." After, I selected where it says "Manual" next to "Startup type" and I changed it to disabled.



Once Secondary Logon was disabled, I clicked apply and then OK.

Services (Local)					
Secondary Logon	Name	Description	Status	Startup Type	Log On
Description: Enables starting processes under alternate credentials. If this service is stopped, this type of logon access will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.	Remote Registry	Enables rem...	Disabled	Local S...	
	Retail Demo Service	The Retail D...	Manual	Local S...	
	Routing and Remote Access	Offers routi...	Disabled	Local S...	
	RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Netwo...
	Secondary Logon	Enables star...	Disabled	Local S...	
	Secure Socket Tunneling Pr...	Provides su...	Running	Manual	Local S...
	Security Accounts Manager	The startup ...	Running	Automatic	Local S...
	Security Center	The WSCSV...	Running	Automatic (...)	Local S...
	Sensor Data Service	Delivers dat...		Manual (Trig...)	Local S...
	Sensor Monitoring Service	Monitors va...		Manual (Trig...)	Local S...
	Sensor Service	A service fo...		Manual (Trig...)	Local S...
	Server	Supports fil...	Running	Automatic (T...	Local S...
	Shared PC Account Manager	Manages sh...	Disabled	Local S...	

After selecting apply, you could see under "Startup Type" that "Secondary Logon" was successfully disabled.

6. Closing unused ports and services

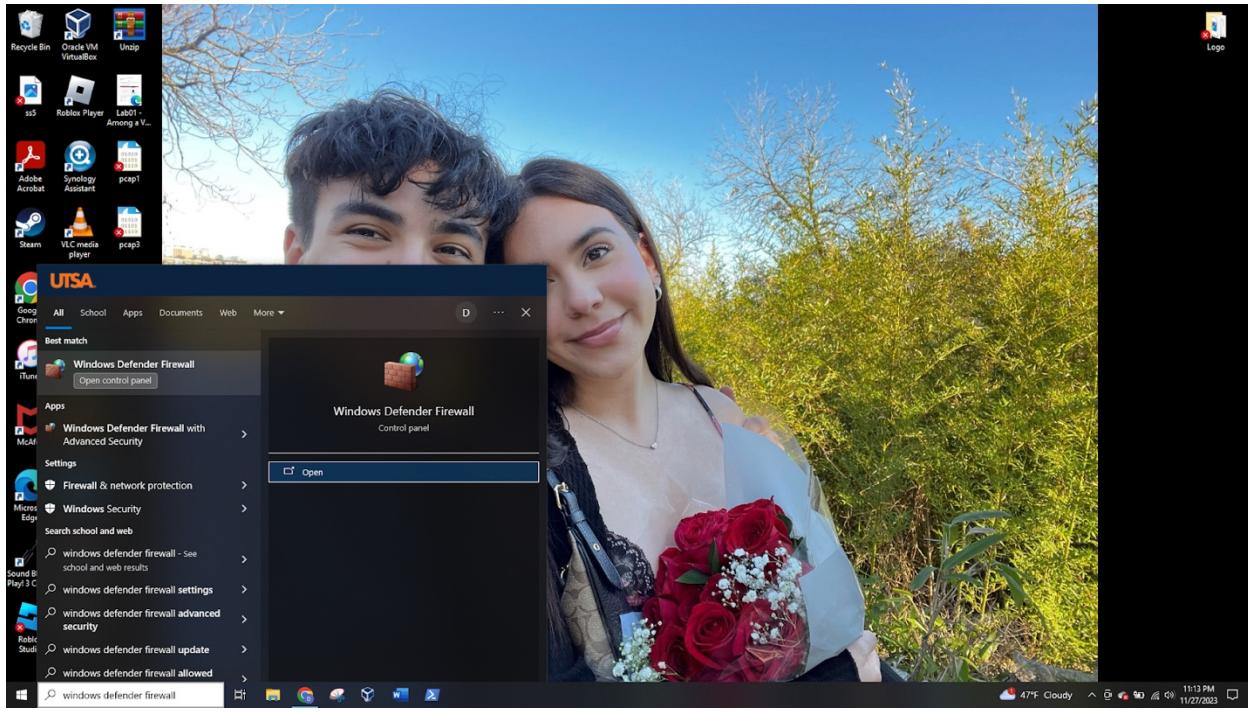
In order to reduce your attack surface, you should close unused ports. One feature that I never use is RDP, a protocol which allows for remote access of your machine. This feature has been exploited repeatedly over the years; therefore, I will close the port associated with this feature. According to CIS's article, RDP uses port 3389; therefore, I will close port 3389.

```
Microsoft Windows [Version 10.0.19045.3693]
(c) Microsoft Corporation. All rights reserved.

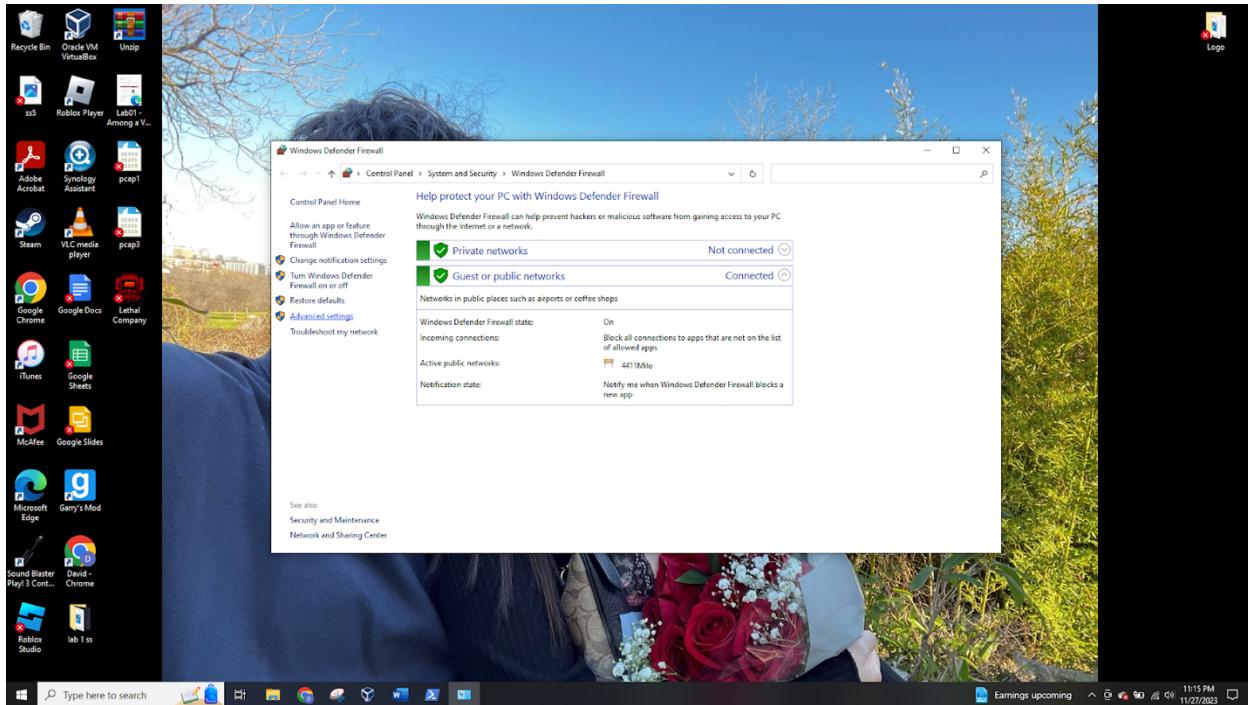
C:\Users\spygu>netstat -tao
```

Active Connections						
Proto	Local Address	Foreign Address	State	PID	Offload	State
TCP	0.0.0.0:135	LT-Dell-E6440:0	LISTENING	916		InHost
TCP	0.0.0.0:445	LT-Dell-E6440:0	LISTENING	4		InHost
TCP	0.0.0.0:623	LT-Dell-E6440:0	LISTENING	2308		InHost
TCP	0.0.0.0:5040	LT-Dell-E6440:0	LISTENING	7288		InHost
TCP	0.0.0.0:7680	LT-Dell-E6440:0	LISTENING	4200		InHost
TCP	0.0.0.0:16992	LT-Dell-E6440:0	LISTENING	2308		InHost
TCP	0.0.0.0:49664	LT-Dell-E6440:0	LISTENING	656		InHost
TCP	0.0.0.0:49665	LT-Dell-E6440:0	LISTENING	576		InHost
TCP	0.0.0.0:49666	LT-Dell-E6440:0	LISTENING	1688		InHost
TCP	0.0.0.0:49667	LT-Dell-E6440:0	LISTENING	1468		InHost
TCP	0.0.0.0:49670	LT-Dell-E6440:0	LISTENING	5148		InHost
TCP	0.0.0.0:49673	LT-Dell-E6440:0	LISTENING	648		InHost
TCP	127.0.0.1:5354	LT-Dell-E6440:0	LISTENING	6300		InHost
TCP	127.0.0.1:5354	LT-Dell-E6440:49671	ESTABLISHED	6300		InHost
TCP	127.0.0.1:5354	LT-Dell-E6440:49672	ESTABLISHED	6300		InHost
TCP	127.0.0.1:8884	LT-Dell-E6440:0	LISTENING	4		InHost
TCP	127.0.0.1:27015	LT-Dell-E6440:0	LISTENING	6328		InHost
TCP	127.0.0.1:49671	LT-Dell-E6440:5354	ESTABLISHED	6328		InHost
TCP	127.0.0.1:49672	LT-Dell-E6440:5354	ESTABLISHED	6328		InHost
TCP	127.0.0.1:49880	LT-Dell-E6440:0	LISTENING	2308		InHost
TCP	192.168.1.102:139	LT-Dell-E6440:0	LISTENING	4		InHost

To view both the open and ports in use, I entered 'netstat -tao' in the terminal. By viewing your machine's port activity, you will be able to better understand which ports you need and which you could turn off without issue.



Next, I searched for and opened 'Windows Defender.'



Next, I selected 'Advanced settings' on the left side of the 'Windows Defender Firewall.'

The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left navigation pane includes 'Inbound Rules', 'Outbound Rules', 'Connection Security Rules', and 'Monitoring'. The main area displays a table titled 'Inbound Rules' with columns for 'Name', 'Group', and 'Profile'. The table lists various entries such as 'Among Us', 'Apple Push Service', 'Bonjour Service', 'CefSharp.BrowserSubprocess.exe', 'Garry's Mod', 'iTunes.MSI', 'Lethal Company', and others. The right side features an 'Actions' pane with options like 'New Rule...', 'Filter by Profile', 'Filter by State', 'Filter by Group', 'View', 'Refresh', 'Export List...', and 'Help'.

Next, I selected 'Inbound Rules' and 'New Rule.'

The screenshot shows the 'New Inbound Rule Wizard' with the 'Rule Type' step selected. On the left, a 'Steps:' list shows 'Rule Type' as the current step, followed by 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The main area asks 'What type of rule would you like to create?'. It offers four options: 'Program' (radio button), 'Port' (radio button selected), 'Predefined:' (radio button), and 'Custom' (radio button). The 'Port' option is described as 'Rule that controls connections for a TCP or UDP port.' The 'Predefined:' option has a dropdown menu showing '@FirewallAPI.dll,-80200'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

I created a new rule, and I selected "Port" to ensure the firewall rule I create disables the RDP port.



New Inbound Rule Wizard



Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

TCP

UDP

Does this rule apply to all local ports or specific local ports?

All local ports

Specific local ports:

3389

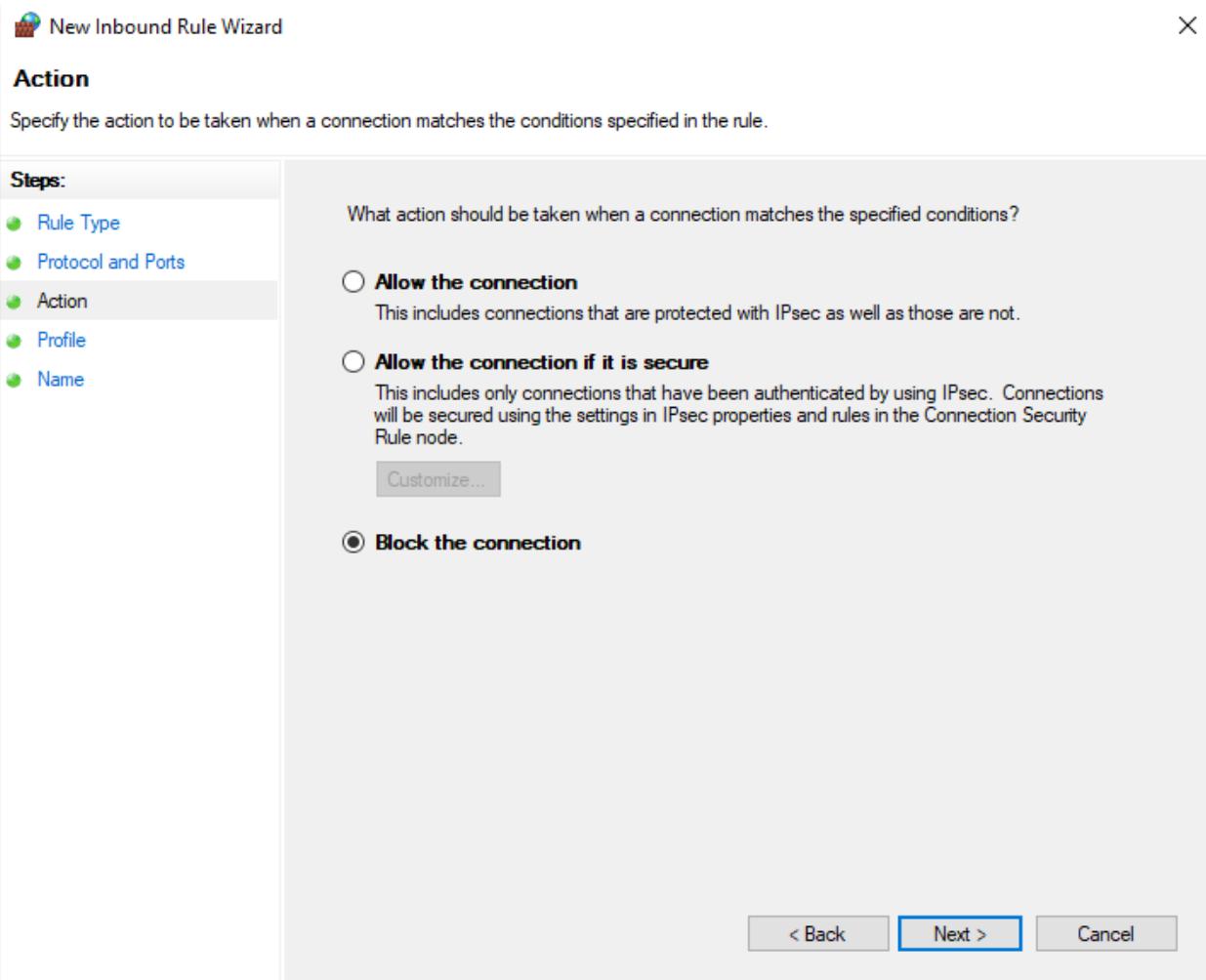
Example: 80, 443, 5000-5010

< Back

Next >

Cancel

RDP uses TCP port 3389.



Next, I selected 'Block the connection.'

 New Inbound Rule Wizard

X

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

 Domain

Applies when a computer is connected to its corporate domain.

 Private

Applies when a computer is connected to a private network location, such as a home or work place.

 Public

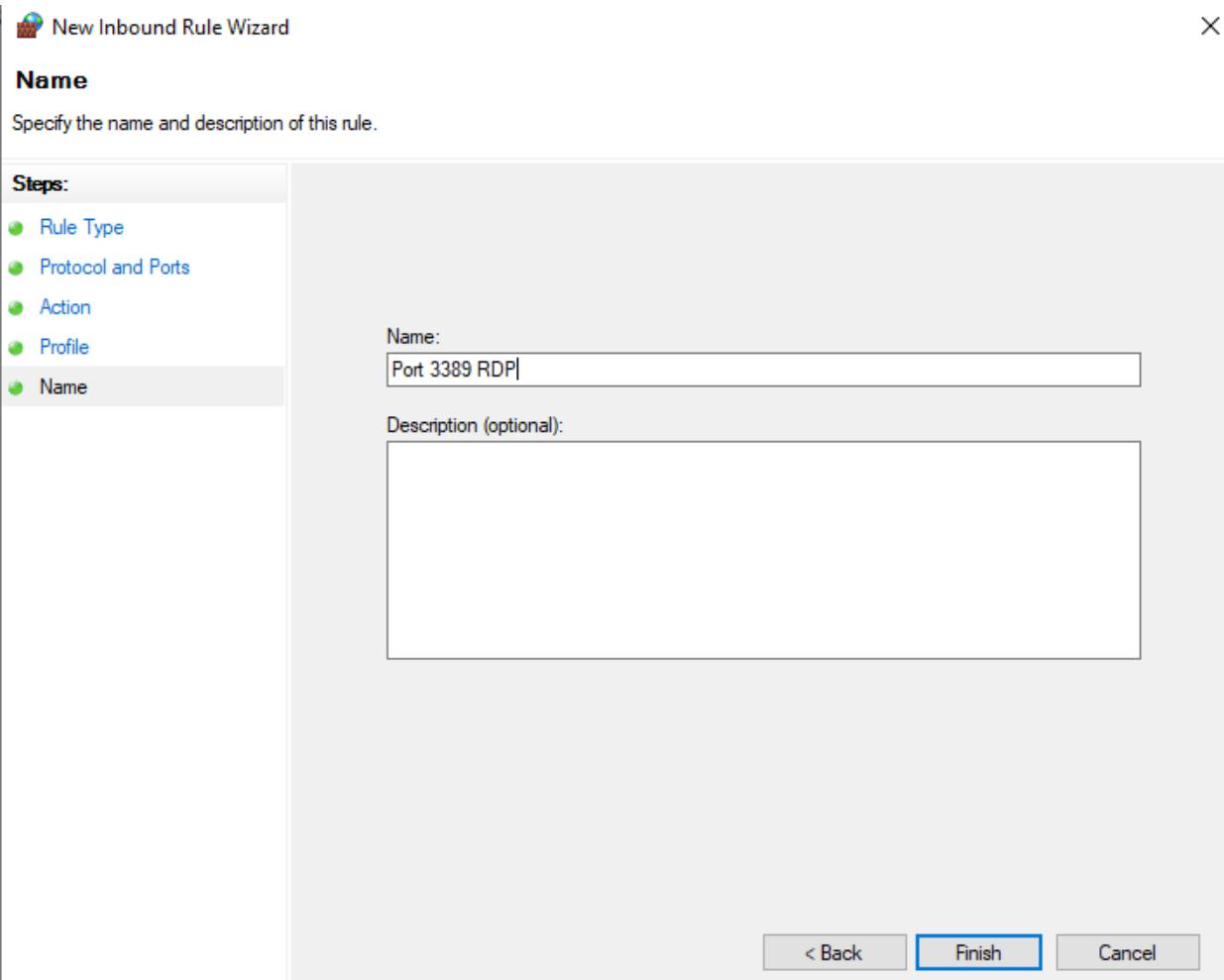
Applies when a computer is connected to a public network location.

< Back

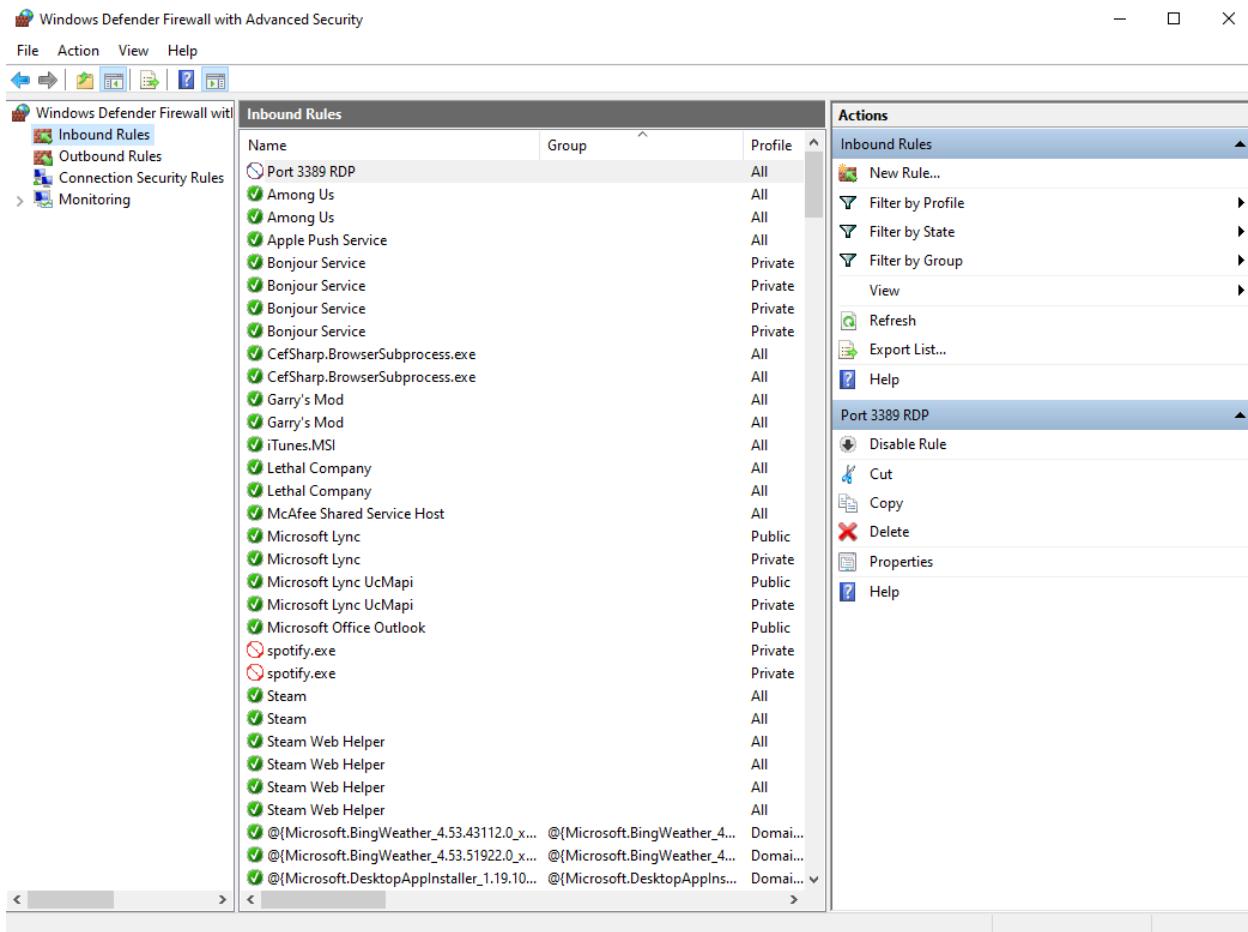
Next >

Cancel

Next, I made sure this rule applied to all domain, private, and public networks.



Next, I named the rule “Port 3389 RDP” and clicked “Finish” to complete the process of blocking the port.

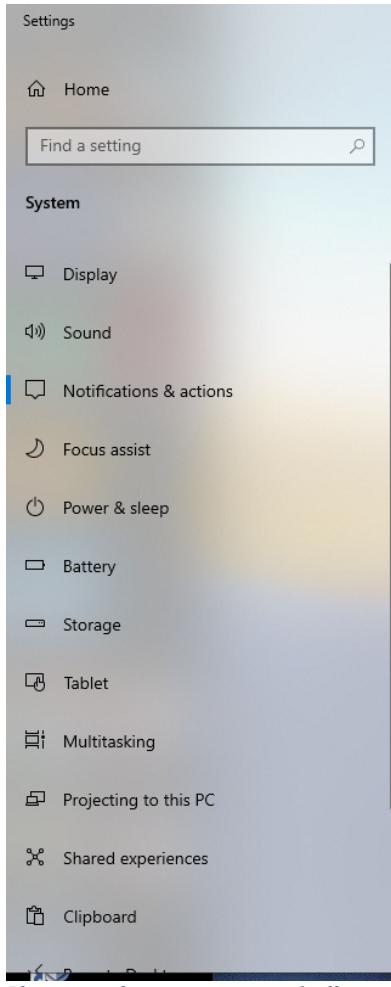


Once I selected “Finish,” I was able to view my new rule at top of the ‘Inbound Rules.’

7. Enabling Windows Notifications for Events



To check Windows event notifications, select the message icon at the bottom right of the screen and, on the right, all the notifications will appear.



Notifications & actions

Quick actions

You can add, remove, or rearrange your quick actions directly in action center.

[Edit your quick actions](#)

Notifications

Get notifications from apps and other senders

On

To control times when you do or don't get notifications, try Focus assist.

[Focus assist settings](#)

- Show notifications on the lock screen
- Show reminders and incoming VoIP calls on the lock screen
- Allow notifications to play sounds
- Show me the Windows welcome experience after updates and occasionally when I sign in to highlight what's new and suggested
- Suggest ways I can finish setting up my device to get the most out of Windows
- Get tips, tricks, and suggestions as you use Windows

Get notifications from these senders

Select a sender to see more settings. Some senders might also have their own notification settings. If so, open the sender to change them.

If your notifications are turned off, you can turn them on by going on system settings and then selecting 'Notifications & actions.'

Notifications

Get notifications from apps and other senders



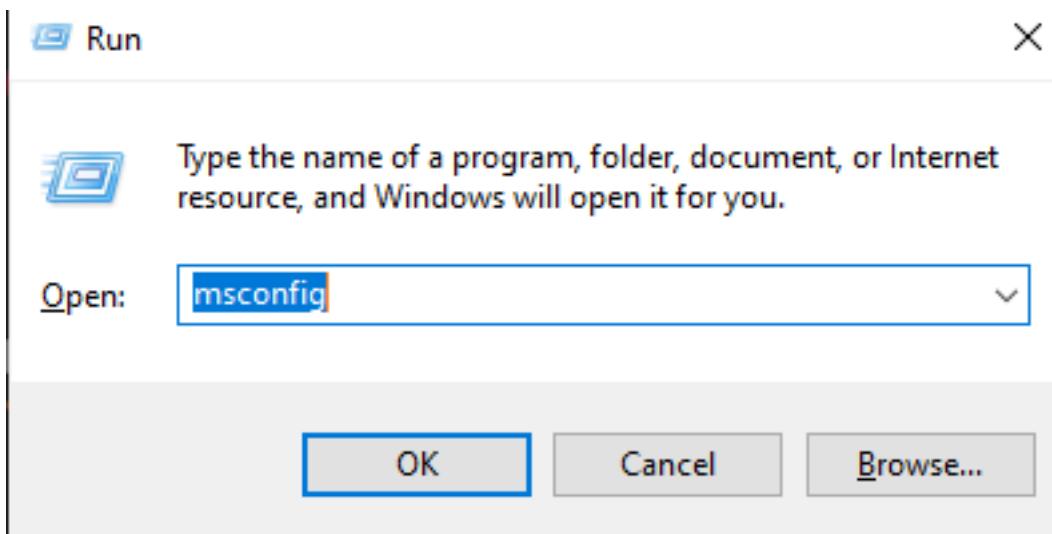
To control times when you do or don't get notifications, try Focus assist.

[Focus assist settings](#)

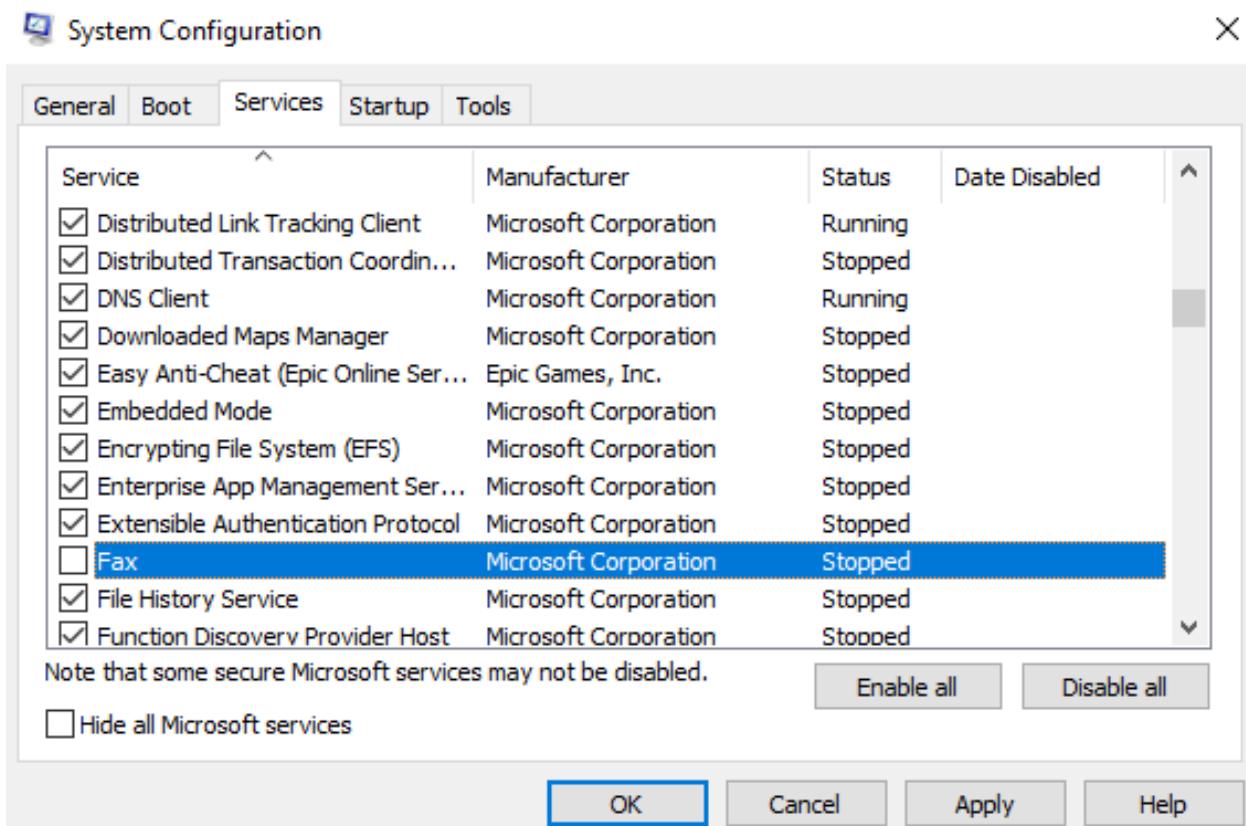
- Show notifications on the lock screen
- Show reminders and incoming VoIP calls on the lock screen
- Allow notifications to play sounds
- Show me the Windows welcome experience after updates and occasionally when I sign in to highlight what's new and suggested
- Suggest ways I can finish setting up my device to get the most out of Windows
- Get tips, tricks, and suggestions as you use Windows

Once here, you can alter your notifications settings based on what you would like to receive notifications over. More specifically, you could choose which apps you would like to receive notifications from or where you would like to display notifications.

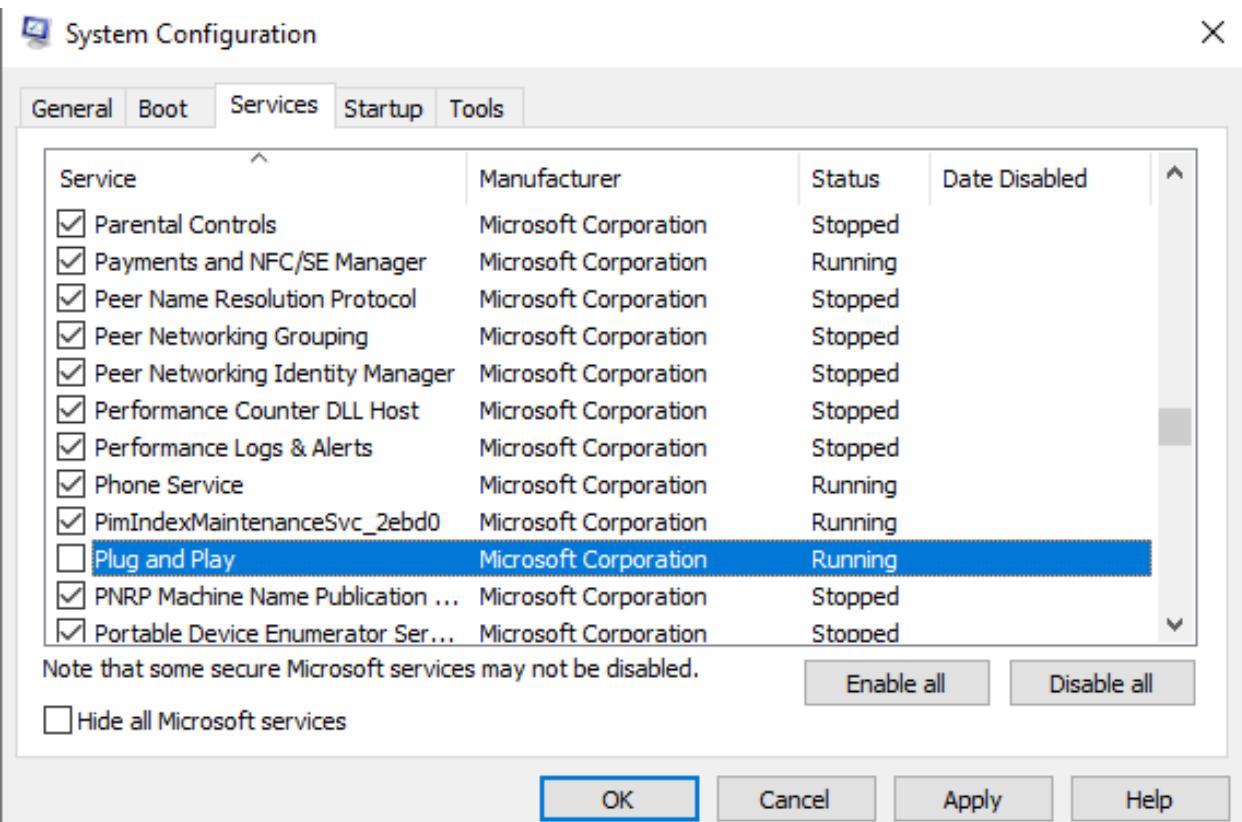
8. Disabling default Windows services



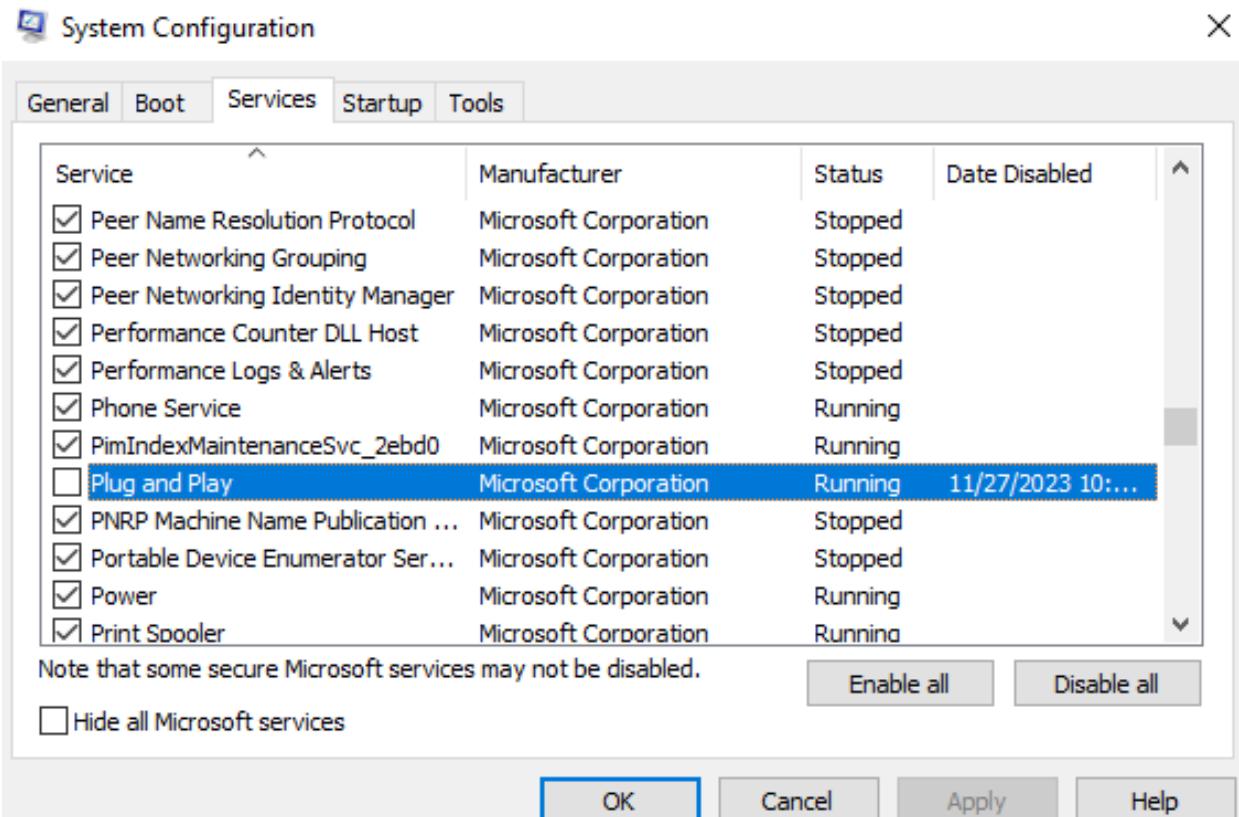
To disable default windows services, I first opened the run line by using the win + r shortcut, and I entered 'msconfig.'



Next, I selected services and began unchecking all the services I wanted to disable.



I also disabled Plug and Play as this service is an immense security risk. If left enabled, if you were to plug in a malicious USB, the services would automatically execute its contents on your computer.



Finally, I clicked apply and you could see that the service was successfully disabled as there is now a date beside the service under 'Date Disabled.'

9. Installing and updating an antivirus

download mcafee - Google Search

← → C 🔒 google.com/search?q=download+mcafee&rlz=1C1ZCEB_enUS1020US1021&oq=download+mca&gs_l

Google

download mcafee

X | Microphone | Camera | Search icon

Free Login For Android For Windows 10 Videos Images Perspectives Installer

About 37,400,000 results (0.41 seconds)

 McAfee
<https://www.mcafee.com> › antivirus › downloads

Download and Install our Award Winning Products

Download our products and discover the latest versions of our installers to purchase or obtain a free trial. Fast, simple, easy to install. Try it today!

 McAfee
<https://www.mcafee.com> › en-us › antivirus › free

Free Antivirus Download | 100% Free and Easy Install

McAfee Free Antivirus and Threat Protection [Download](#). Try our Award-Winning antivirus for today's security and privacy threats. 100% Free [Download](#) Try it ...

People also ask :

How do I download McAfee? ▾

Is McAfee free to download? ▾

Why can I not download McAfee on my computer? ▾

Should I download McAfee protection? ▾

I chose to download McAfee as I am already paying for a McAfee subscription. To begin, I searched up 'download McAfee' and I selected the first search result.



Products ▾ Features ▾ About Us ▾ Resources ▾ Why McAfee

Support ▾



Sign in

Download and install our award-winning products

Discover the latest versions of our products to purchase or obtain a free trial.

[Download now](#)

Feedback

Security

Next, I clicked on "Sign in" to sign into my account.

View Account Info

You're covered with:
McAfee® AntiVirus

McAfee protection and improve your security online.

Protection Center

My McAfee

Purchase history →
See and manage all your subscriptions.

Subscriptions →
Manage your renewal preferences.

Downloads & devices →
Add / remove devices and add extra protection.

My account info

Once signed in, I selected "Downloads and devices."

Welcome McAfee

My Account



My Apps



LT-DELL...

Select subscription

McAfee® AntiVirus



Protect your device

Install McAfee® AntiVirus on this device and enjoy peace of mind whenever you go online.



DOWNLOAD

Once on 'Downloads and devices,' I clicked Download.



Welcome! Let's start installing

You're minutes away from protecting what matters most to you.

Install

Next, the anti-virus began installing.



! Info-check

Downloading

Installing

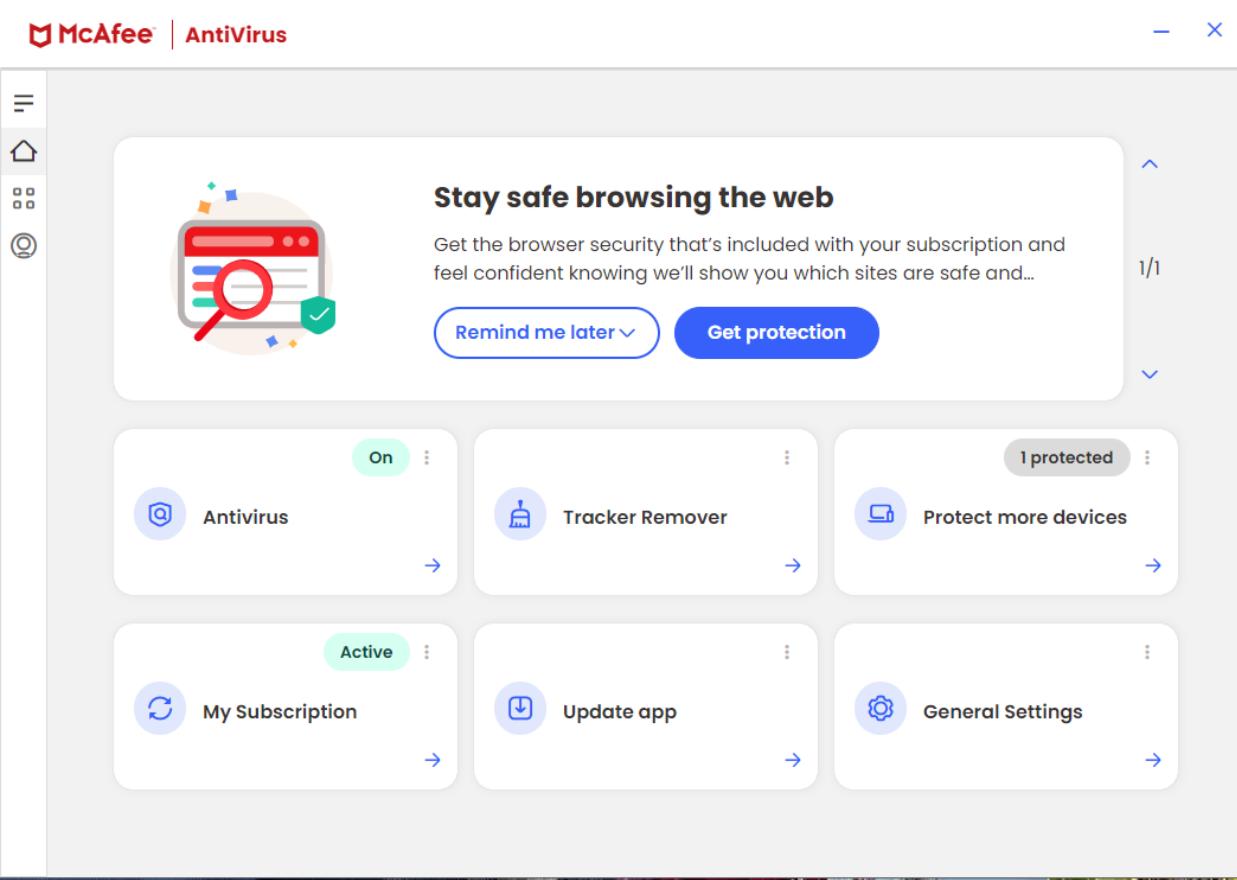
Getting ready to install...

We're checking you have the right operating system.

! Good news, you already have the latest McAfee app installed. Have questions? [Learn more](#)

Open app

Screenshot of McAfee installing onto my Desktop.



Finally, I installed McAfee and I successfully have an antivirus on my device.

10. Limiting the physical access of a host

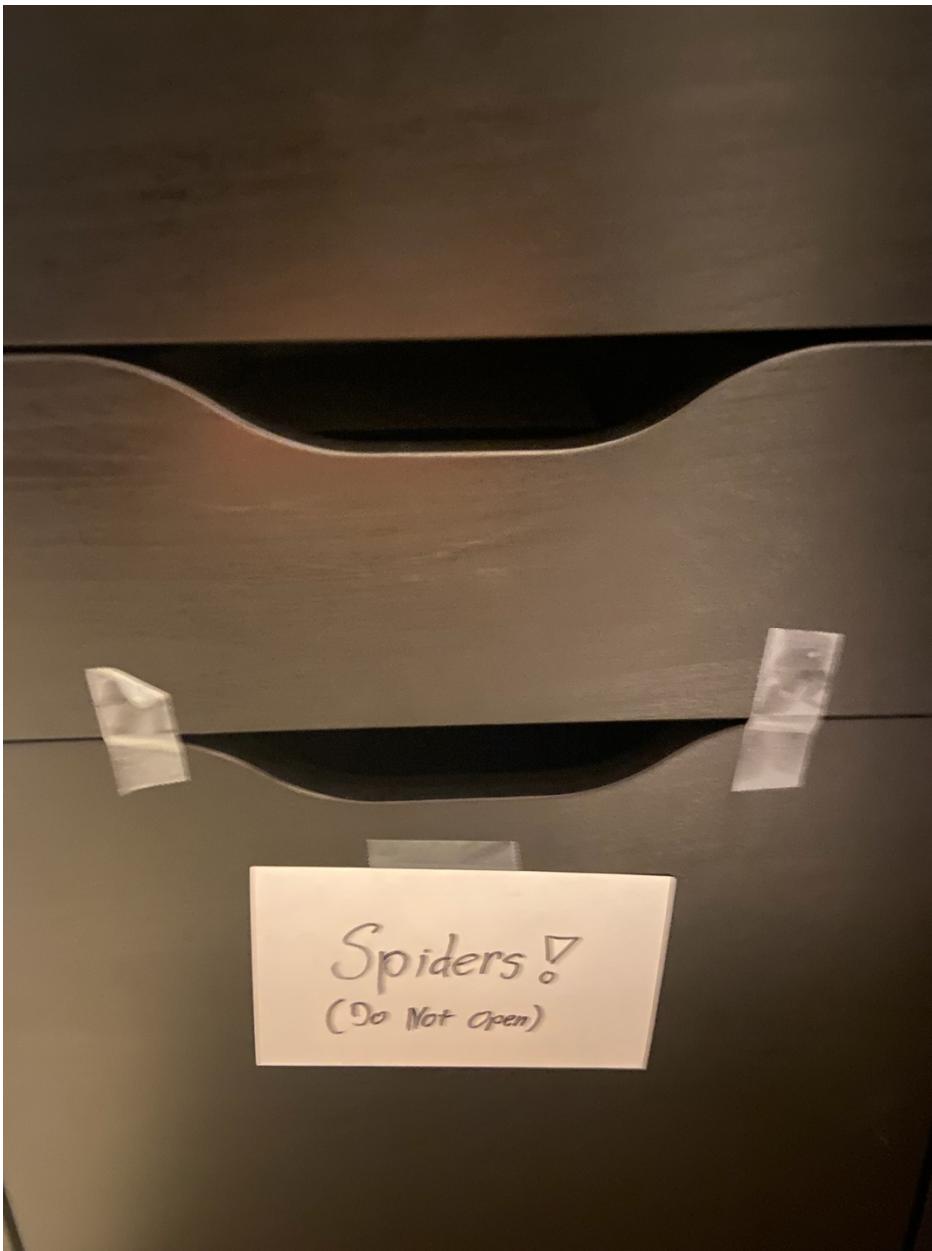
I've already limited physical access to my device as I have both a BIOS password and a profile password. I will further limit physical access to my machine by hiding my device while the computer is inactive.



Normally I keep my device sitting on my table even when inactive.



To limit physical, I will place my laptop inside my cabinet while it is inactive.



Once inside a safe place, one could use a lock or other deterrent to safeguard your device.

LIMITATIONS/CONCLUSION

In this lab, I adeptly implemented 10 hardening techniques that bolstered my computer's security. The hardening techniques I implemented included incorporating AdBlockers, enforcing logoff upon inactivity or when logon hours expire, enabling Hard Drive Encryption (BitLocker), updating and patching the operating system, deactivating Secondary Logon Services, closing unused ports and services, enabling Windows Notifications for Events, deactivating default Windows services, installing and updating an antivirus, and restricting the physical access of a

host.

REFERENCES

TechCrunch: ‘Even the FBU says you should use an ad blocker’

<https://techcrunch.com/2022/12/22/fbi-ad-blocker/#:~:text=This%20holiday%20season%2C%20consider%20giving,or%20extorting%20money%20from%20victims>.

I used this website to become more knowledgeable on ad-blockers and how they could be used to harden your machine.

4Sysops: ‘Automatically log off idle users in Windows.’

<https://4sysops.com/archives/automatically-log-off-idle-users-in-windows/>

I used this website to learn more about Force log off and how I could add that feature onto my computer.

Professor K: ‘Disable Windows 10 Automatic Logoff for Inactivity’

https://www.youtube.com/watch?v=eDuGWGiawfQ&ab_channel=ProfessorK

I used this website to find the Automatic Logoff for Inactivity.

Microsoft: ‘Turn on device encryption.’ <https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838#:~:text=Turn%20on%20standard%20BitLocker%20encryption,->

<https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838#:~:text=Sign%20in%20to&text=In%20the%20search%20box%20on,is%20available%20for%20your%20device.>

I used this webpage to learn more about BitLocker and how to use it on my device.

LinkedIn: ‘What are the benefits and risks of updating to the latest OS version?’

<https://www.linkedin.com/advice/1/what-benefits-risks-updating-latest-os-version>

I used this article to learn a little more on the risks of updating to the latest OS.

Tech Wonders: ‘Disable the Secondary Logon Service to Prevent Starting Processes Under Alternate Credentials.’ <https://www.tech-wonders.com/2009/08/disable-secondary-logon-service-to.html>

I used this article to learn more about Secondary Logon and how to disable it.

SuperUser: ‘How do I close ports that I don’t need in Windows 10?’

<https://superuser.com/questions/1686740/how-do-i-close-ports-that-i-dont-need-in-windows-10>

I used this webpage to understand how to close unused ports on Windows.

Microsoft: ‘Change notification settings in Windows.’ <https://support.microsoft.com/en-us/windows/change-notification-settings-in-windows-8942c744-6198-fe56-4639-34320cf9444e>

I used this webpage to learn how to change my notification settings on Windows.

Windows Report: ‘Windows 10 Services You Can Safely Disable & How to Guide.’

<https://windowsreport.com/disable-windows-services/>

I used this website to research default services, which ones I could disable, and how to disable them.

FTC: ‘Physical Security.’ <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/physical-security>

I used this web page to learn about the importance of physical security.

Chrome Web Store: ‘AdBlock’ <https://chromewebstore.google.com/detail/adblock-%E2%80%94-best-ad-blocker/gighmmpioblkfepjocnamgkkbiglidom?pli=1>

I downloaded this ad-blocker.

JR Tech & Software: ‘What Happens When You Disable All Windows Services?’

<https://www.youtube.com/watch?v=J5o7IZGh9I8>

I used this video to learn how to disable default enabled services.

NordVPN: ‘Should UPnP be enabled or disabled?’

<https://nordvpn.com/cybersecurity/glossary/upnp/#:~:text=Enable%20UPnP%2DUP%20to%20require,at%20the%20cost%20of%20convenience>.

I used this website to determine whether I should disable plug n play on my device.

CIS: ‘Security Primer – Remote Desktop Protocol’ <https://www.cisecurity.org/insights/white-papers/security-primer-remote-desktop-protocol>

I used this website to learn about the security risk posed by RDP and which port I could disable to mitigate the risk.

Win10User: ‘Windows 10: How to Start or Stop Secondary Logon Service.’

<https://www.youtube.com/watch?v=ho3p75xGtJ8>

I used this website to learn how to stop secondary logon on Windows 10.