NETWORK SECURITY HARDENING TECHNIQUES

DECEMBER 7, 2020

Authors:

MAX VILLARREAL
JESUS SAN DIEGO
JONATHAN LOPEZ

Password Hardening

1. Add a Secure BIOS Password

PART A:

1. How does it harden your host?

This focuses on physical security. Adding a secure BIOS password prevents unauthorized changes to the boot settings of a computing asset. This also prevents firmware attacks on a device where a malicious entity loads compromised firmwares that bypasses operating system security such as weakening encryption, intercepting communication channels, and bypassing endpoint security.

Reference:
Anatomy of a firmware attack. (2019, December 23). Security Boulevard.
https://securityboulevard.com/2019/12/anatomy-of-a-firmware-attack/

2. What are the advantages and disadvantages of it?

Advantage for adding a secure bios password means that only authorized users are allowed to change critical asset settings and prevents accidental device misconfiguration or changing boot order priority.

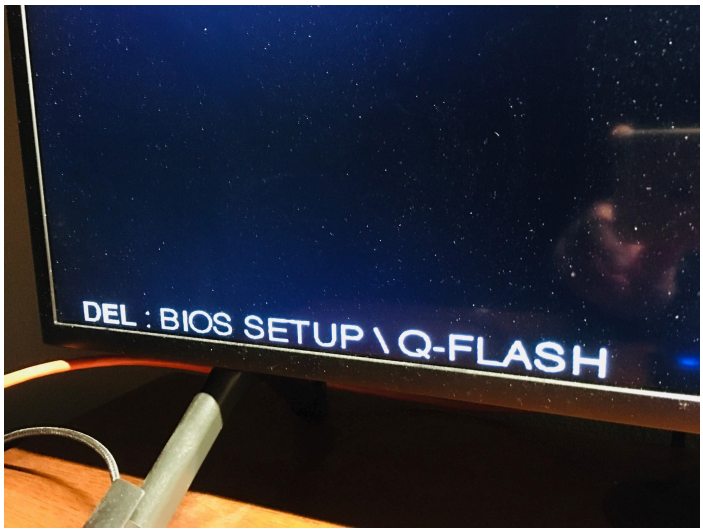
Disadvantage: Passwords can be misplaced or lost. Change management for when new administrators come and the handful who controlled BIOS passwords leave. If there is poor documentation on asset passwords that could slow down organizational changes. Passwords have to be input before changing BIOS settings could be a hindrance when handling 1000+ computing assets.

PART B:

1. Step by Step instruction for executing hardening technique

2. Snapshot of steps

Upon computer start, enter BIOS SETUP (for this computer DELETE Key)



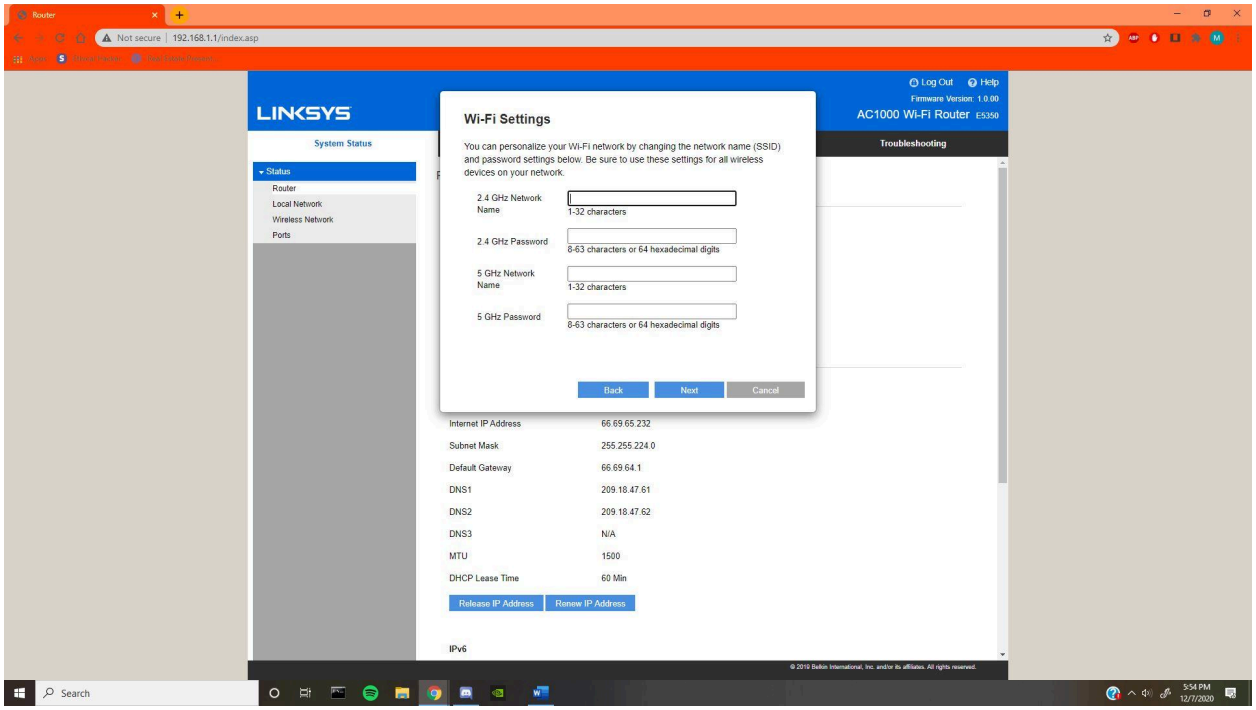
Once inside BIOS, go to preference tab and look for “Administrator Password” setting

System will prompt the user to input Administrator Password. Reboot to accept changes.

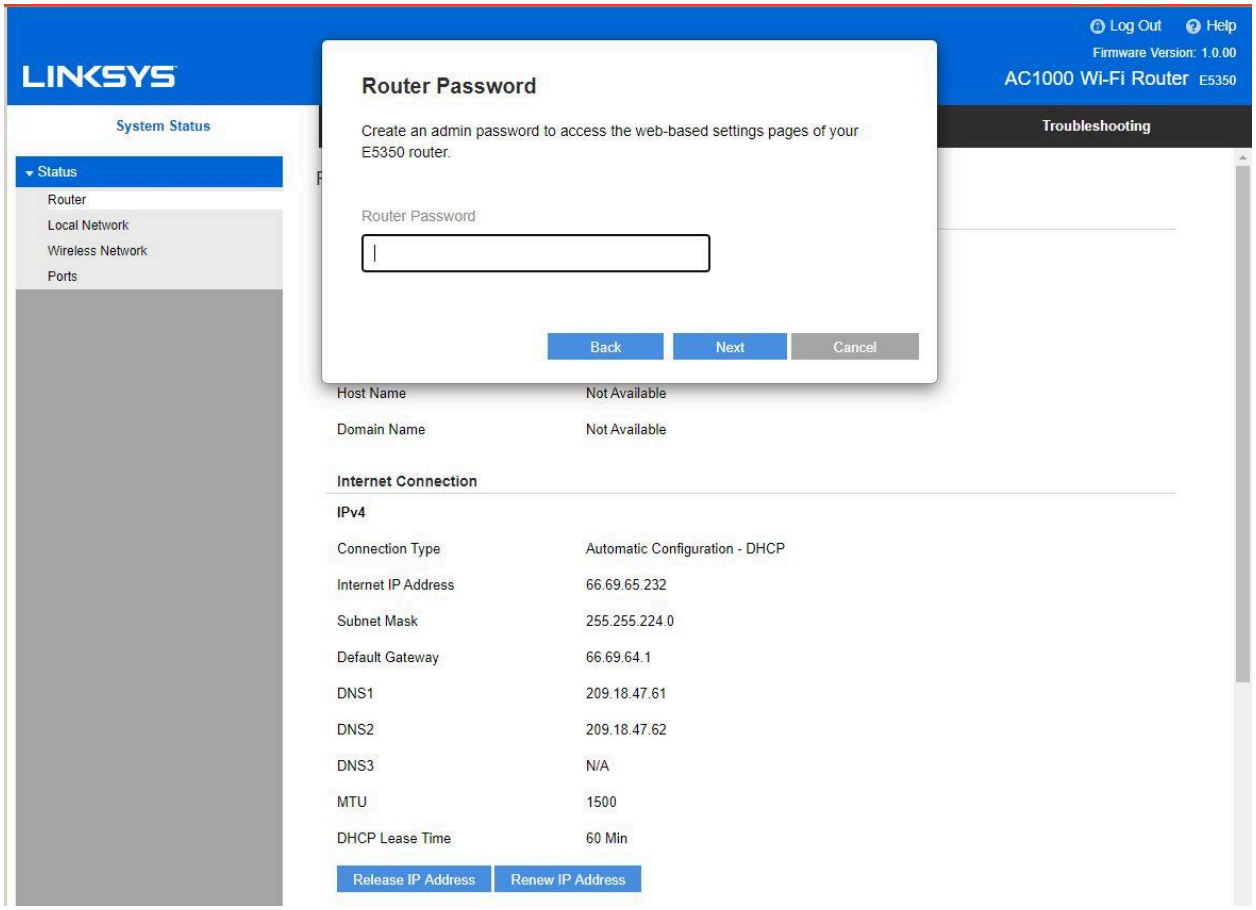
2. Change the Default Password on Routers

Changing the default passwords on routers is important because often these values can be saved as “admin” or “12345” as a filler so that the user can replace them. The advantage of changing these passwords is having a more secure router, and lessening the chance of an effective brute force attack. The disadvantage is that you must store these passwords properly; if lost you will have to perform another factory reset.

1. To start the factory reset I held the reset button on the router for 10 seconds.
2. For a linksys router enter 192.168.1.1 in the address bar of your web browser.



3. First, you accept the terms of use and software agreement. Then you set the SSID's and new wifi passwords. It is important to use good password practices for all passwords created.



4. The next propt is to create a password for accessing your router settings. This password is important, and controls many of your wireless network settings.

Encryption Hardening

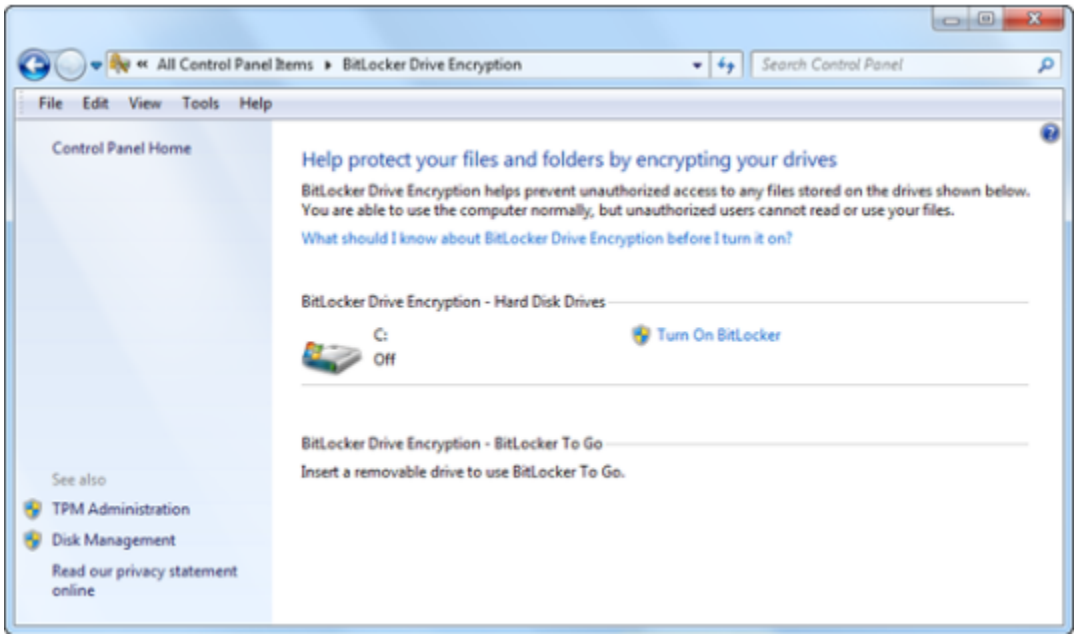
3. Enable Hard Drive Encryption (BitLocker)

Part A:

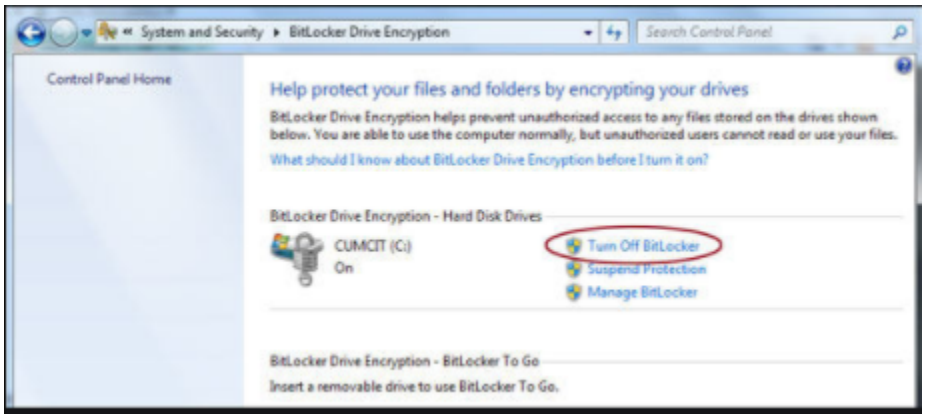
BitLocker secures your data by encrypting it. Encryption secures your data by scrambling it so it can't be read without authenticated decrypting using a recovery key. Bitlocker differs from most other encryption programs because it uses your Windows login to secure your data; no extra passwords needed.

Part B:

1. Click Start, click Control panel, click system and security and then click BitLocker Drive Encryption

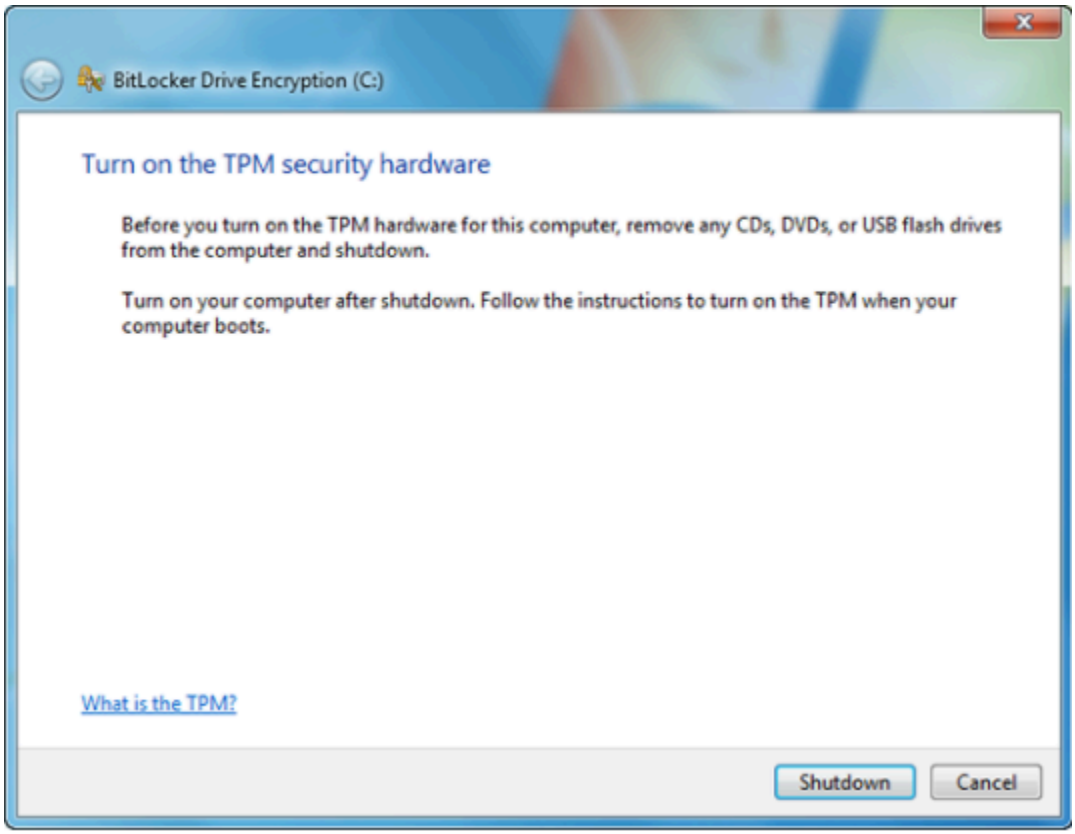


2. Click Turn on BitLocker

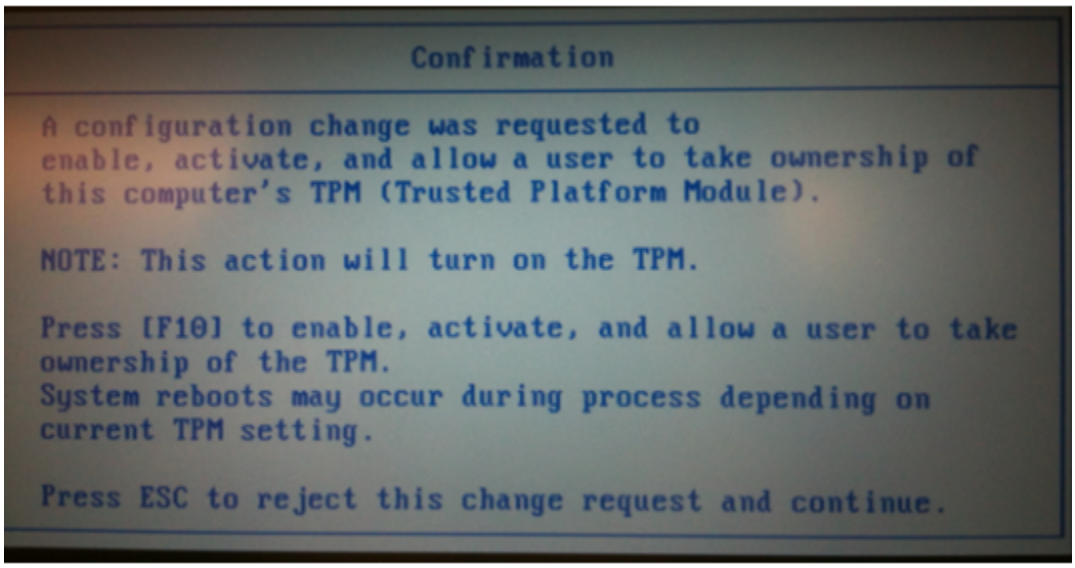


3. Bitlocker scans your computer to verify that it meets the system requirements.

4. If prompted to do so, remove any CDs, DVD's and USB Flash drives from your computer and then click Shutdown



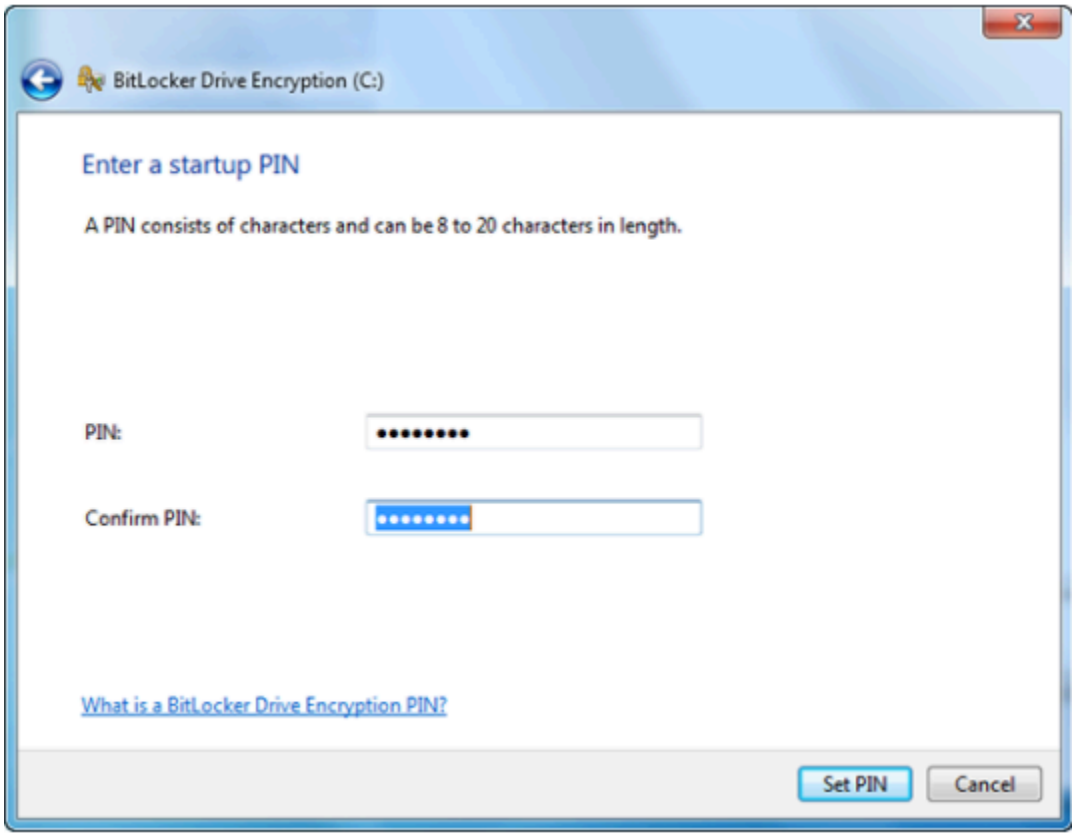
5. Turn your computer back on after shutdown and depending on the Model on the computer repeatedly press the F# ket to enter the BIOS and enable TPM.



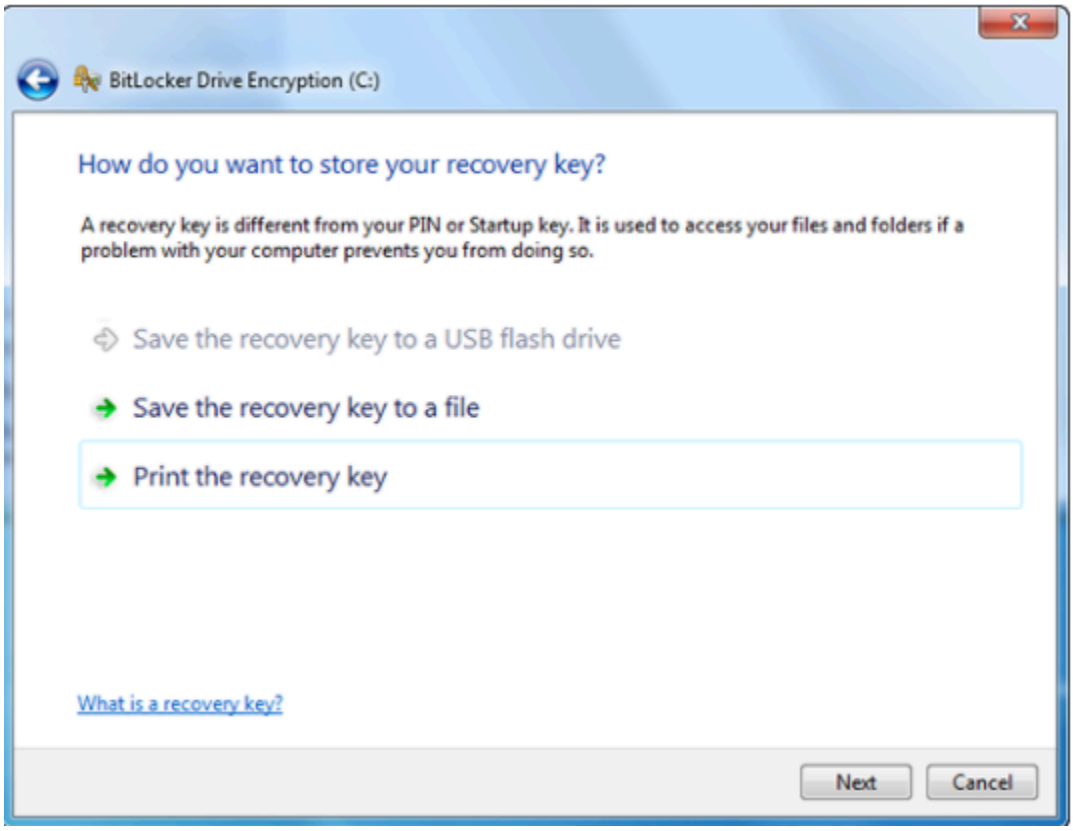
6. Computer will shutdown and turn back on and Botlocker setup Wizard will resume automatically, Click Next.


BitLocker Drive Encryption (C:)
BitLocker Drive Encryption setup
The following preparations will be made on this computer to enable BitLocker.
Turn on the TPM security hardware
Encrypt the drive
What are BitLocker's system requirements?
Cancel

7. When Bitlocker startup page is displayed click Require a PIN at every startup and enter a 8 to 20 character PIN and confirm PIN.



8. Store your recovery Key and click Print the recovery Key and click next. You will be prompted to restart your computer to start the encryption process.



4. macOS File Vault

PART A:

1. How does it harden your host?

File Vault is a macOS file encryption scheme. This prevents unauthorized users from accessing user data without the proper password to the machine.

Reference:

Use FileVault to encrypt the startup disk on your Mac. (2018, November 30). Apple Support. https://support.apple.com/en-us/HT204837

2. What are the advantages and disadvantages of it?

Advantage: This is a full-disk encryption that protects the startup disk of the machine and ensures that sensitive data is protected from unauthorized access.

Disadvantage: On older apple devices, this adds seconds to the delay of the startup process depending on the speed of the hardware. On modern devices the start up delay is negligible, but adds a delay nonetheless. Lost passwords means that it would be more difficult to recover user data in the event of an emergency.

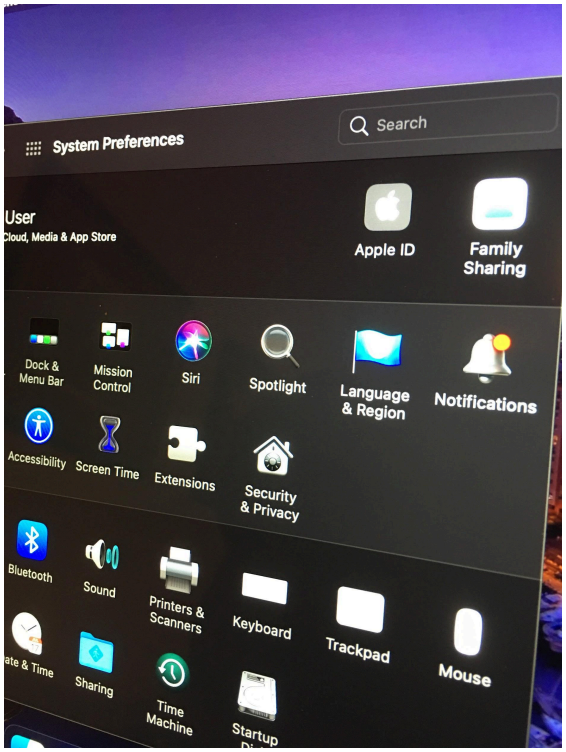
PART B:

1. Step by Step instruction for executing hardening technique

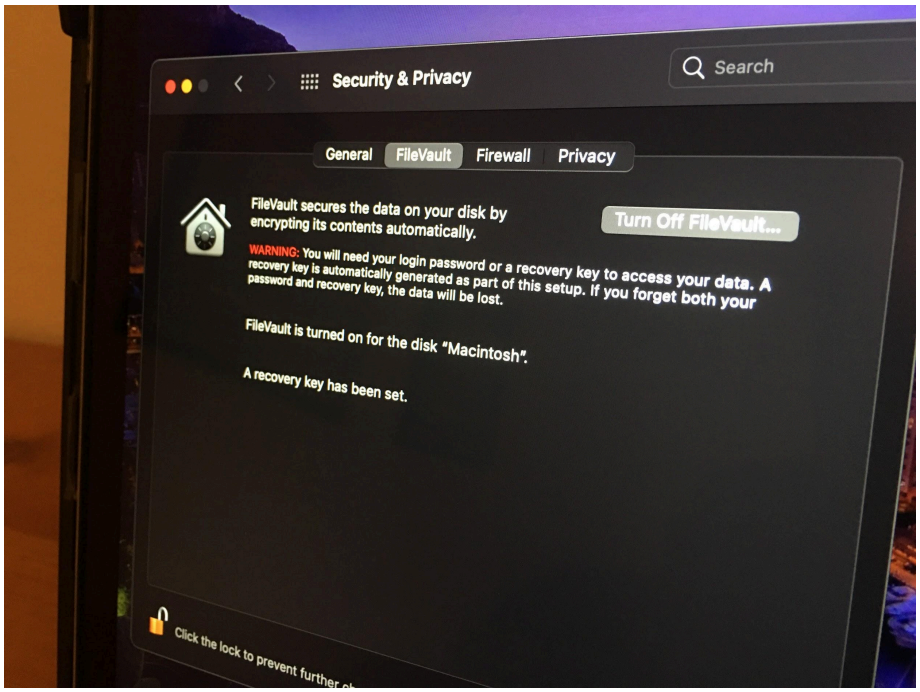
2. Snapshot of steps

Filevault is available on apple computing devices. Power on the device

Go to “System Preferences” and on the second row click the “Security & Privacy” icon



On the “FileVault” tab click “Turn On FileVault” to encrypt the startup disk. Encryption process takes roughly 10-15 minutes on modern Apple devices.



Registry Hardening

5.Secure Registry (Guest and User Account) Privileges

PART A
The Accounts Guest account status policy setting determines whether the Guest account is enabled or Disabled. This account allows unauthenticated network user to gain access by loggin on as a Guest with no Password. This means that any network shared folders with permission that allow access to the Guest Account, the guest group or the Everyone Group will be accessible over the network.

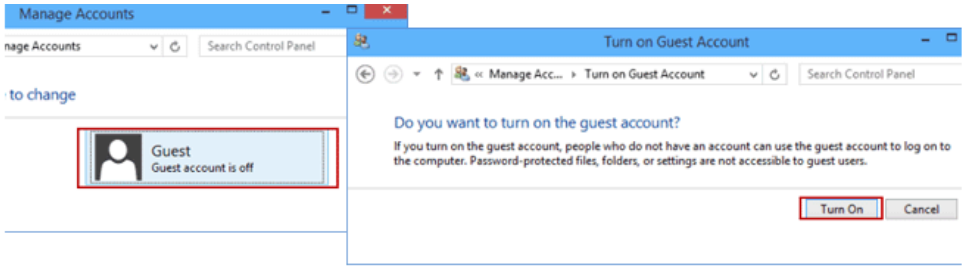
Step 1: Open Control Panel in Windows 10.

Step 2: Go to User Accounts > Manage another account.

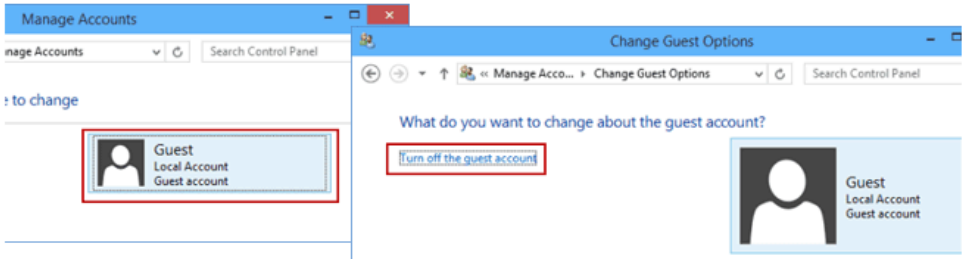
Step 3: Then you can see all the listed accounts including the Guest on your Windows 10.

Step 4: Turn on/off the guest account.

s1. If the guest account is off, click on the Guest and then click Turn On button to turn it on.



2. If the guest account is on, click on **Guest** and then click **Turn off the guest account** link so that you can



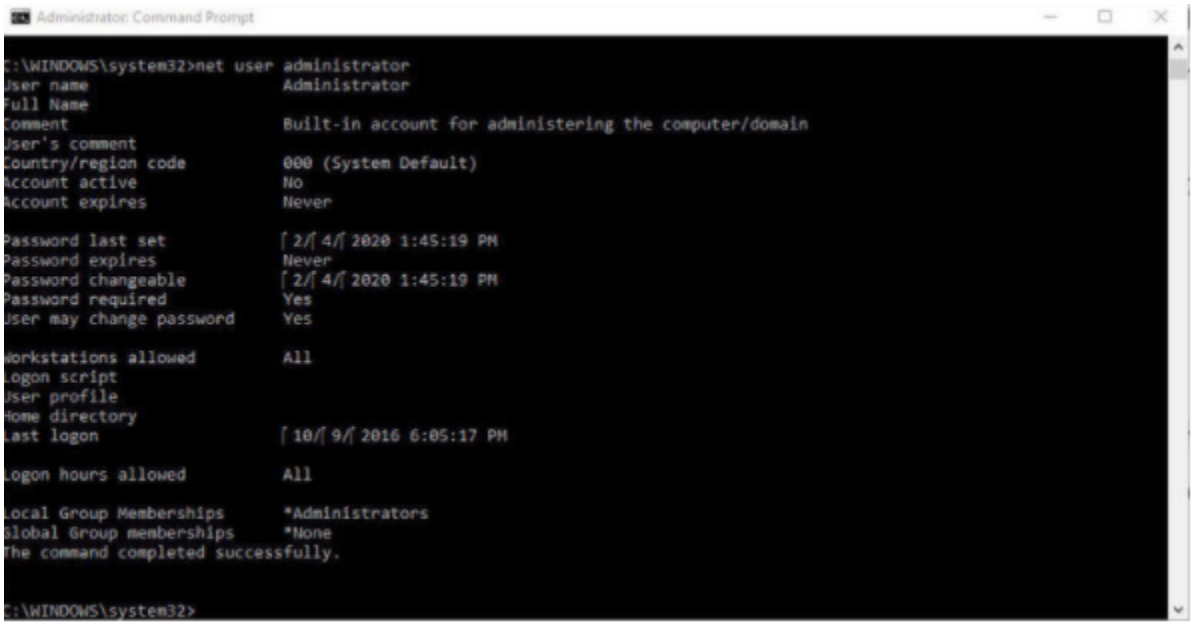
6.Disable Default Windows 10 Administrator Accounts

Similar to the Guest account disabling the default Administrator account in Windows 10. Since this is the default one that is targeted by hackers to gain access and control of your computer. To avoid any issues caused by a hacker this account should be deleted.

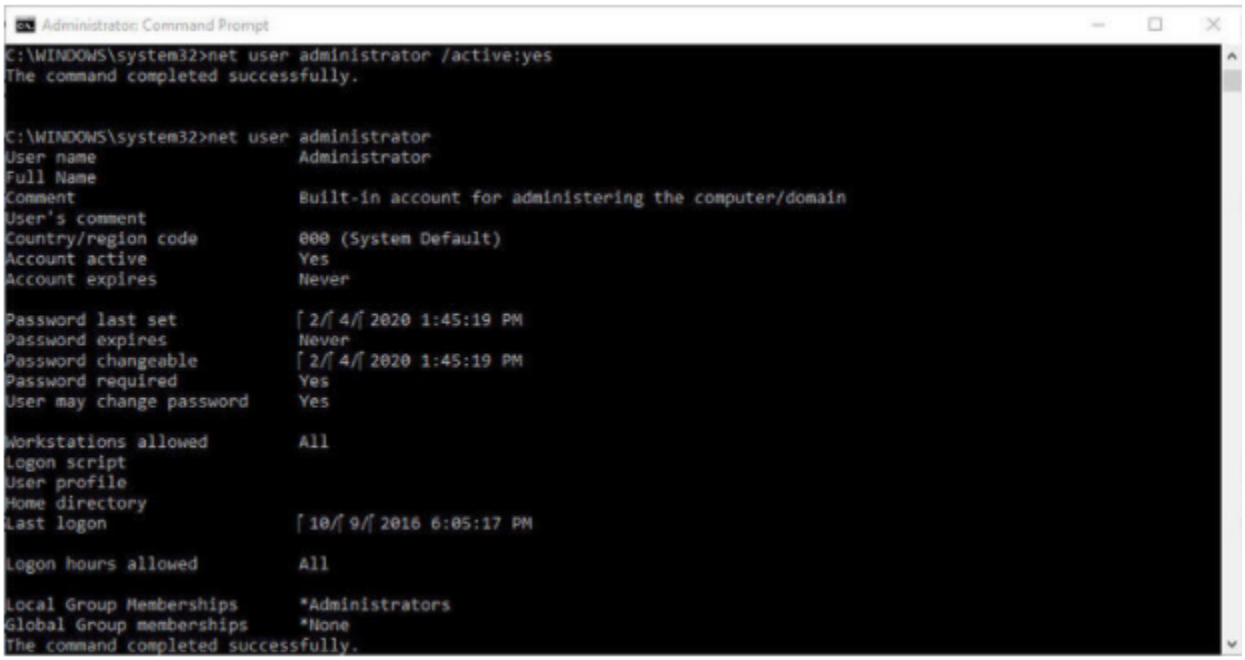
1. Open a command prompt as an administrator by typing cmd in the search field.

From the results, right-click the entry for Command Prompt, and select Run as Administrator.

At the command prompt, type net user administrator. The value for Account Active should say No



2. Type net user administrator /active:yes. You should receive a response that the command completed successfully.
3. Type net user administrator. The value for Account Active should now say Yes



Network Hardening

7. Disable Remote Access to a Computer (RDP)

PART A:

1. How does it harden your host?

Disabling Remote Access to a computer hardens the host from unauthorized access. There are exploits that take advantage of RDP such as “BlueKeep” that quietly enable remote access on target computers and steal sensitive information or conduct malicious actions/scripts.

References:
Locklear, G. (2020, November 24). *RDP vulnerability: Avoid RDP exploits*. Remote Support Blog | Netop. https://blog.netop.com/avoid-rdp-vulnerabilities-with-a-secure-remote-desktop

RDP security explained. (2020, May 5). McAfee Blogs. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rdp-security-explained/

2. What are the advantages and disadvantages of it?

Advantage: Disabling remote access closes potential backdoor on assets and hardens the machine from compromise.

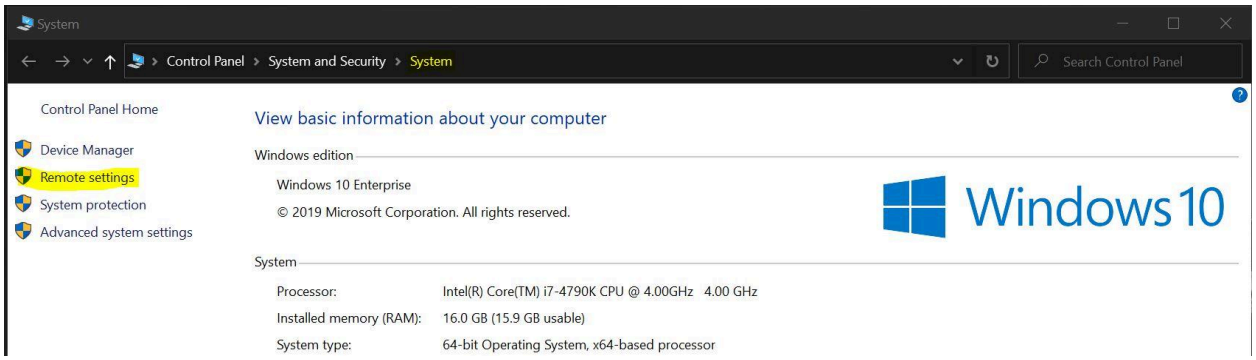
Disadvantage: This removes the ability for legitimate remote access from being used and the functionality is essentially locked away.

PART B:

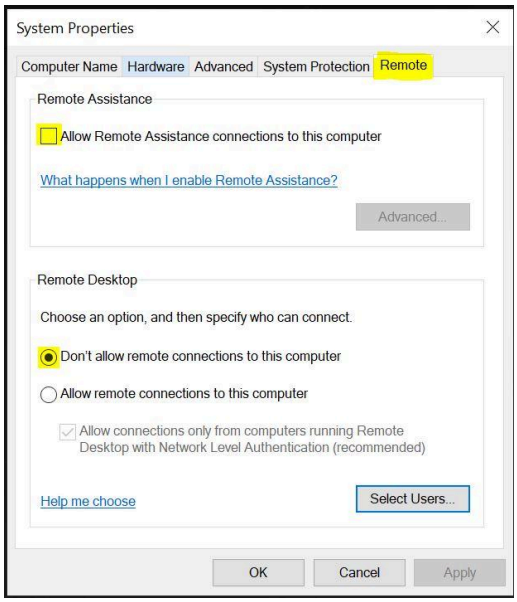
1. Step by Step instruction for executing hardening technique

2. Snapshot of steps

On windows machine navigate to Control Panel > System and Security > System
and on the left side links provided choose “Remote Settings”



A popup window will appear and navigate to “Remote” tab



Make sure “allow Remote Assistance connections to this computer” is unchecked and “Do not allow remote connections to this computer” is selected

8. Close Unused Ports and Services

PART A:

1. How does it harden your host?

Closing unused ports and services hardens computing assets by removing potential vectors for malicious actors. As new zero-day attacks are introduced that take advantage of ports and services, disabling them minimizes the attack surface of a device.

Reference:

How to close unused open ports: TCP and UDP Port scan. (2014, June 19). Acunetix. https://www.acunetix.com/blog/articles/close-unused-open-ports/

2. What are the advantages and disadvantages of it?

Advantage: Closing unused ports and services potentially reduces operating system memory usage and speeds up user interactions with the machine. This also reduces the attack surface of a device for future attacks that take advantage of built-in services or default enabled ports.

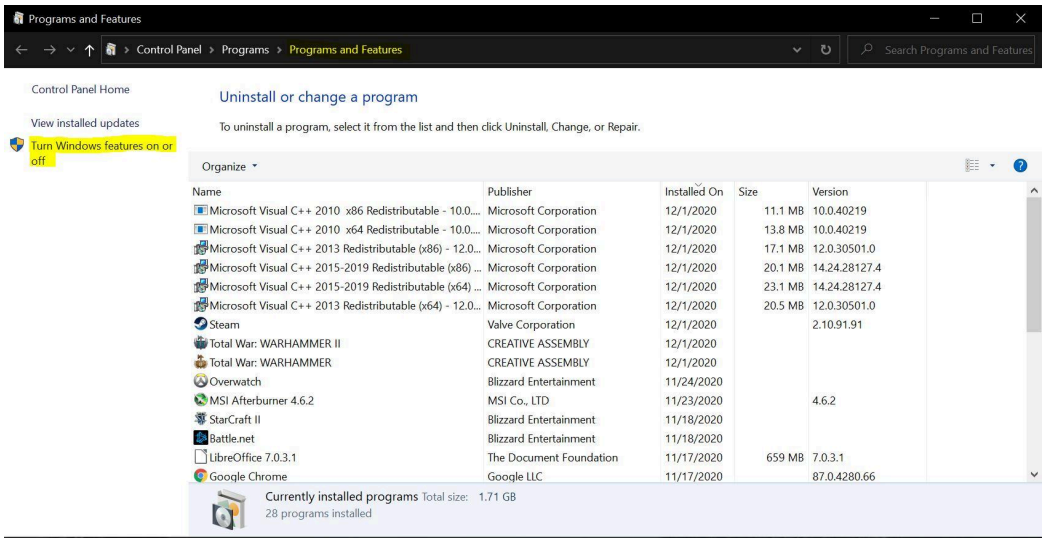
Disadvantage: Functionality will be reduced and in larger organizations that utilize services, compatibility will be impacted if these ports or services are disabled.

PART B:

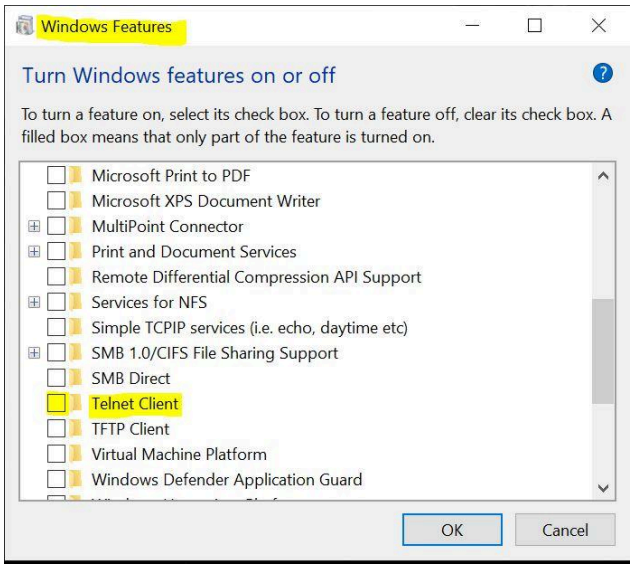
1. Step by Step instruction for executing hardening technique

2. Snapshot of steps

Navigate to Control Panel > Programs > Programs and features.
On left side links, select “Turn Windows features on or off”



New window will open labeled “Windows Features”
Uncheck unused services and ports.
For this example “Telnet Client” which is largely unused legacy feature utilizing port 23



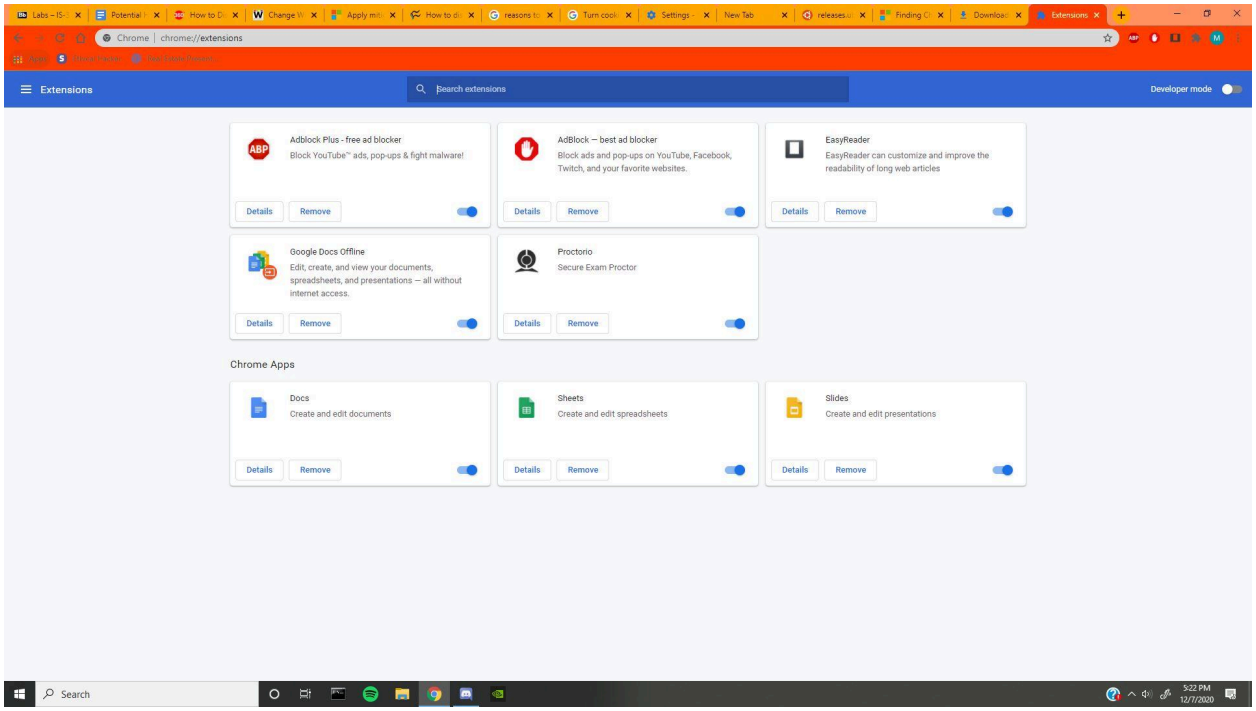
Reference:
Gibson, S., & CORPORATION, G. R. (n.d.). *GRC | Port authority, for internet Port 23*. Home of Gibson Research Corporation . https://www.grc.com/port_23.htm

Web Browser Hardening

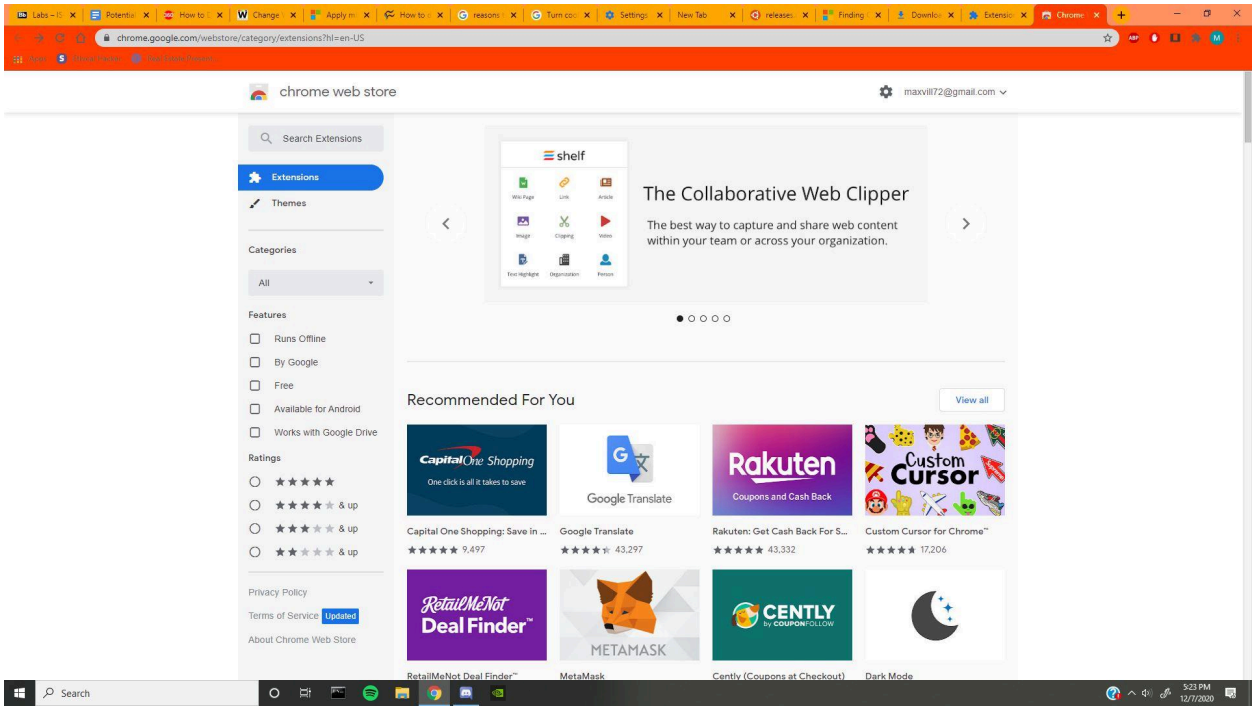
9. Use AdBlockers or Pop-Up Blockers

Ad Blocking software has become quite popular. This software disables or hides advertisements on many websites. Enabling Adblock is quite advantageous for many reasons. It reduces the amount of filler on the screen around articles, and can stop videos from autoplaying on webpages. The disadvantage is that many websites can detect when you are blocking their advertisements, and will not display their content until the ad block is disabled.

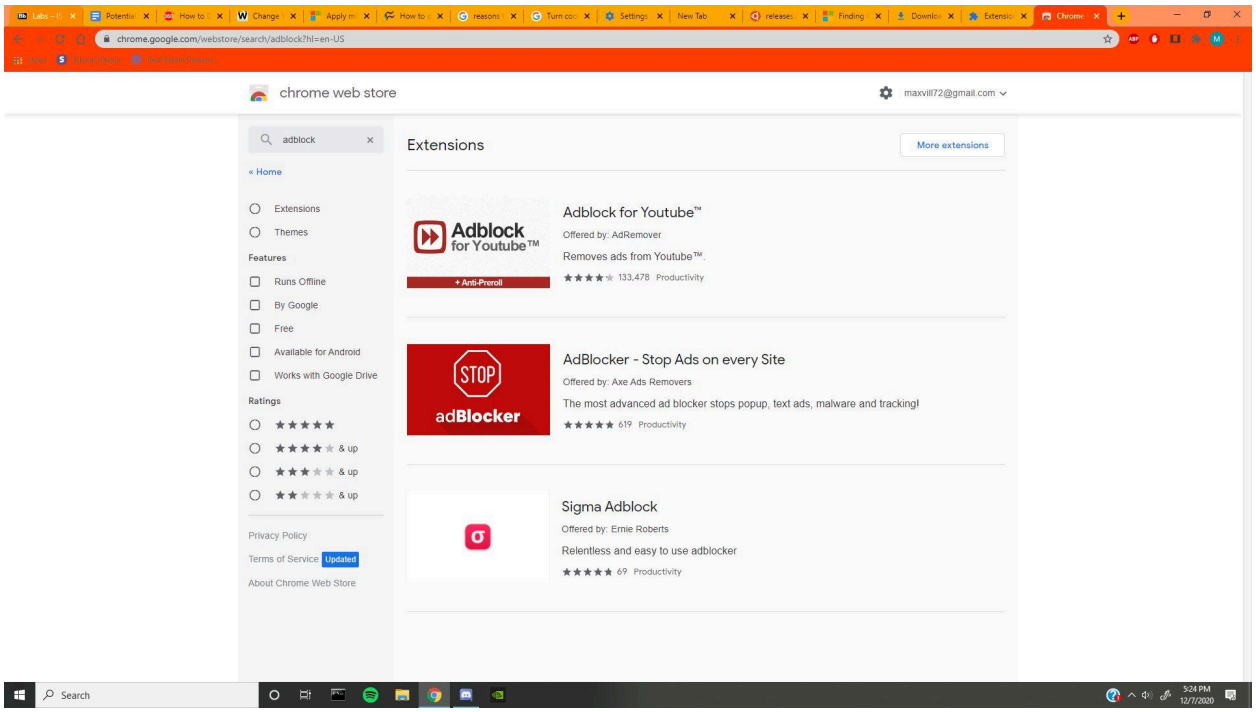
1. Extensions are added through the google store. The way I get to the google store is through the google chrome extensions page



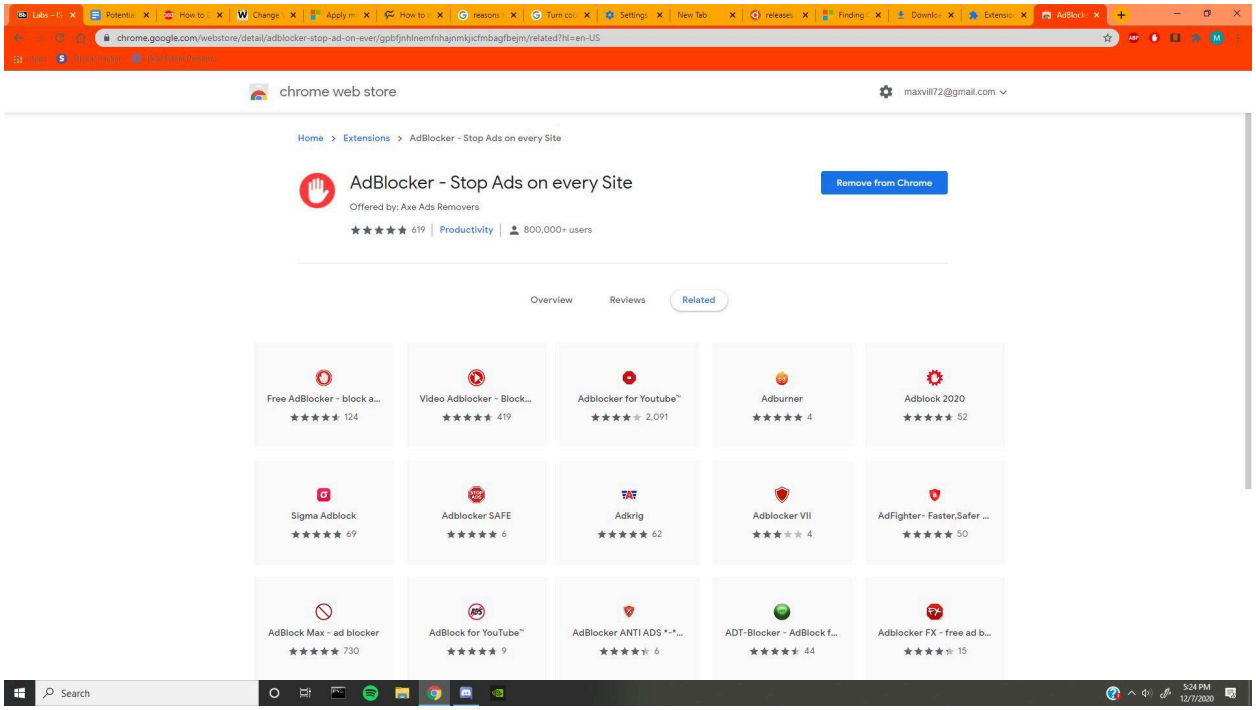
2. Clicking the three bars on the top left of the screen will open a sidebar. At the bottom of this bar will be “open chrome web store”.



3. From the Chrome Store, use the search bar to find an adblock program that suits your needs. Consider the reviews of the software.



4. I select AdBlocker - Stops Ads on every Site.

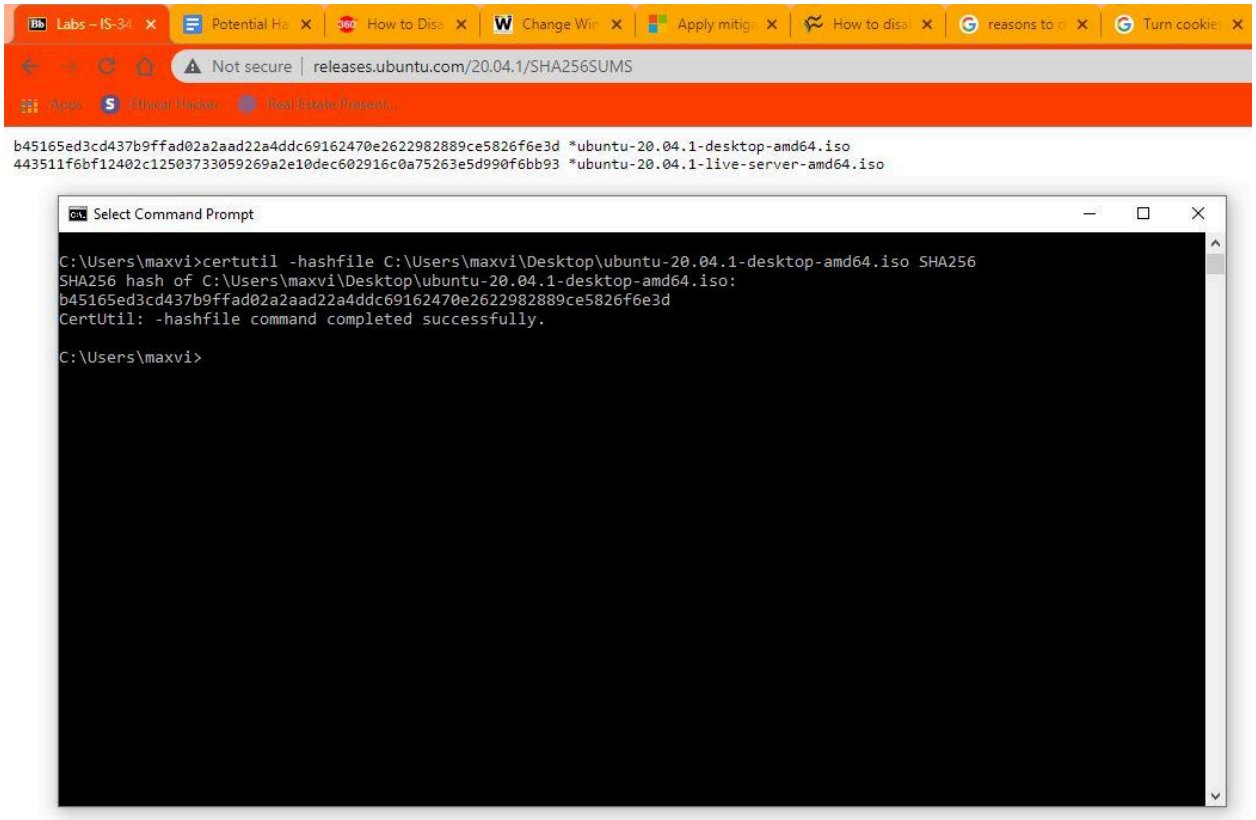


5. Select Add to chrome, and verify in the popup you would like to download the extension. It will install itself as soon as it is finished downloading.

10. Use Reputable Downloads for Software Applications (Verify Integrity with Hashes)

Verifying with hashes is an easy way to see if files downloaded are corrupt/edited. Windows has a hash generator usable in cmd line. To verify a file, you compare the hash generated by the file on your computer to the hashes posted by the creator of the software. The advantage to verifying your files is the knowledge the file you will be executing has not been edited. The disadvantage is these file hashes can sometimes be difficult to find for older software.

1. To generate a hash using the windows command line, type cmd into the search bar and press enter.
2. In the new terminal, type certutil -hashfile (followed by the path of the file you wish to generate a hash from) (then the type of hash you would like generated.)
3. This will display the hash in the terminal, You need to compare the generated hash to one found online for the same file. It is important to be cautious of version and file type when verifying, even small changes completely change the hash generated.

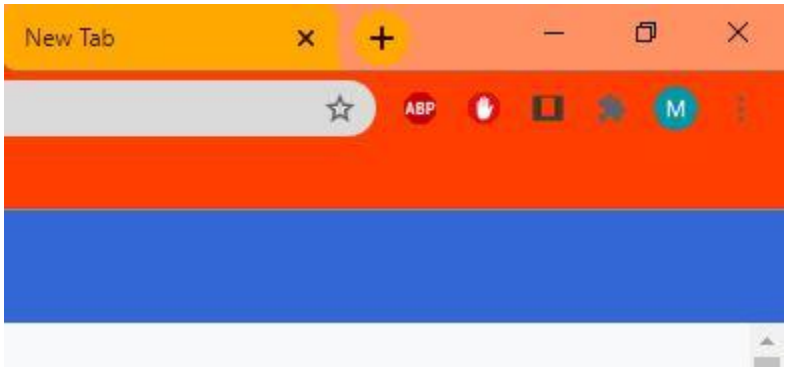


4. In this example I verified my Ubuntu.iso with the SHA256 hash posted online.

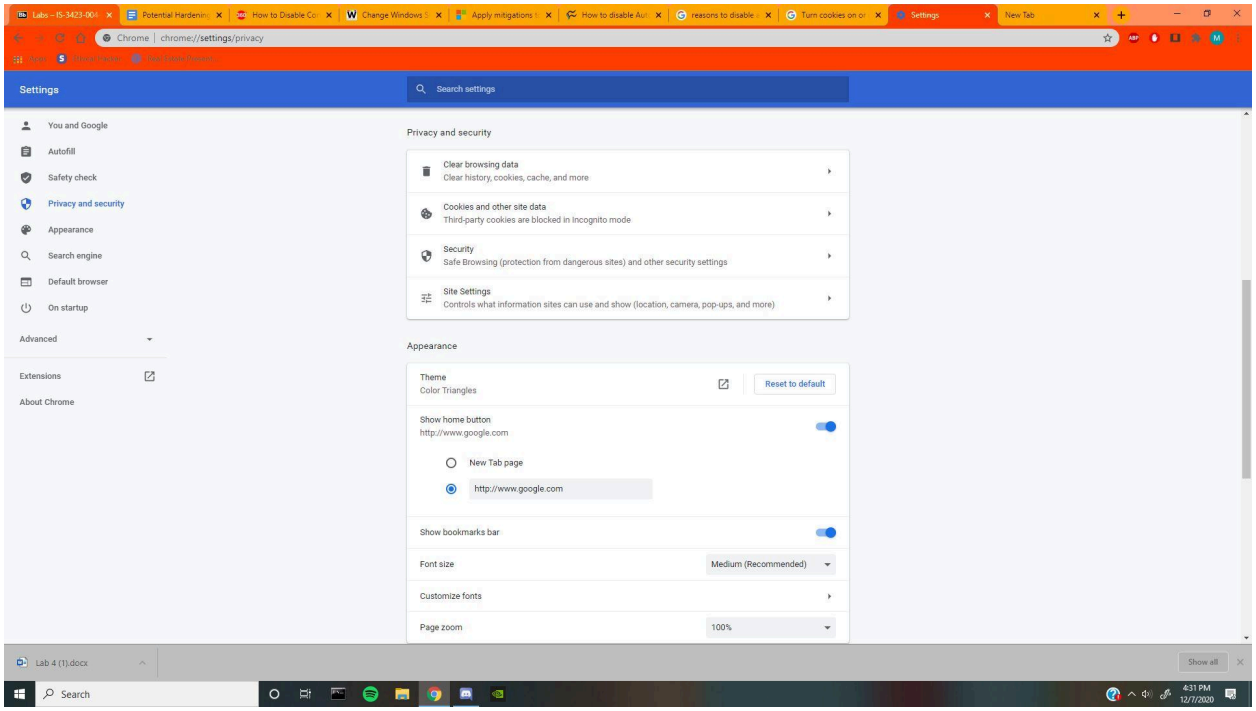
11. Managing/Disable Cookies

Cookies are used to monitor and track data through the internet. Although some cookies can improve user experience, many can track information about the user unknowingly. The advantage to disabling cookies is fewer targeted ads and websites not tracking how much you have visited their site. The disadvantage is your recommendations may not be as accurate compared to cookies enabled.

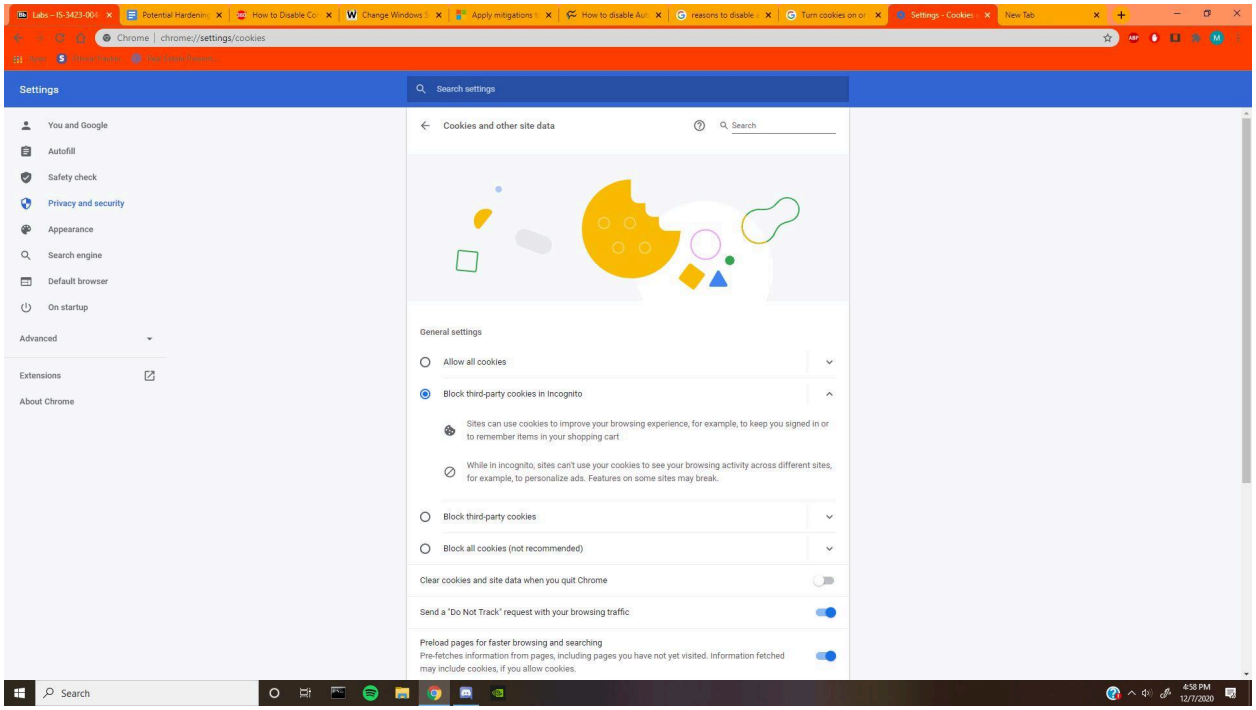
1. To manage your cookie settings on Google Chrome, open your settings by clicking the three dots on the top right corner.



2. From within your settings window, select Privacy and Security, on the left hand side.



3. Within Privacy and Security, select Site settings.

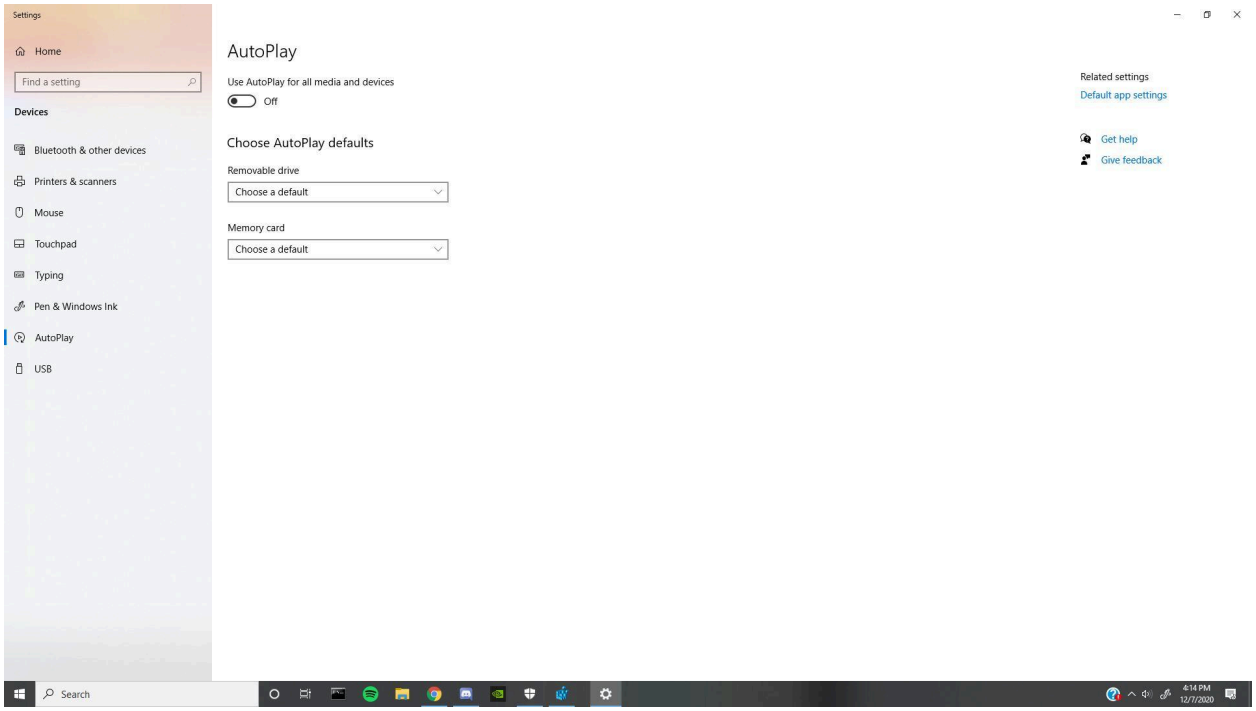


4. From this window you can scroll down to select Cookies and Site data. Here you can manage your settings, and set chrome to delete your cookies when it is closed. You can also totally disable cookies, but this is not recommended.

12. Turn off Autoplay

Autoplay is windows autostarting inserted media and certain file formats. The advantages of disabling autoplay is reduced bandwidth usage, and preventing unwanted media from autoplaying. The disadvantage is connected media will not play automatically.

1. To disable autoplay, search for autoplay in the windows search bar, and open this portion of your settings.



2. You will see an on/off switch for autoplay. Select off.

Operating System Hardening

13. Update and Patch Operating System

PART A:

1. How does it harden your host?

Updating and Patching Operating systems hardens a host device by updating critical software as determined by Microsoft. Microsoft regularly sends out patches to fix exploits, improve system stability, and improve functionality of the operating system.

Reference:

Information technology services. (n.d.). Information Technology Services | Connecting Campus. https://its.uiowa.edu/support/article/1418

2. What are the advantages and disadvantages of it?

Advantage: Having an up to date patched and updated OS means that critical fixes are applied and software has improved stability and security fixes. This minimizes attack surfaces and secures any vulnerabilities.

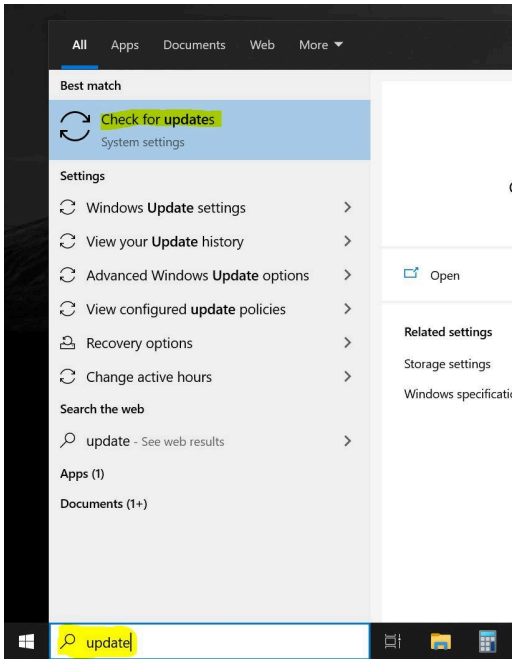
Disadvantage: Some patches might break functionality on existing software. Compatibility might be an issue for large organizations that rely on legacy software on older versions.

PART B:

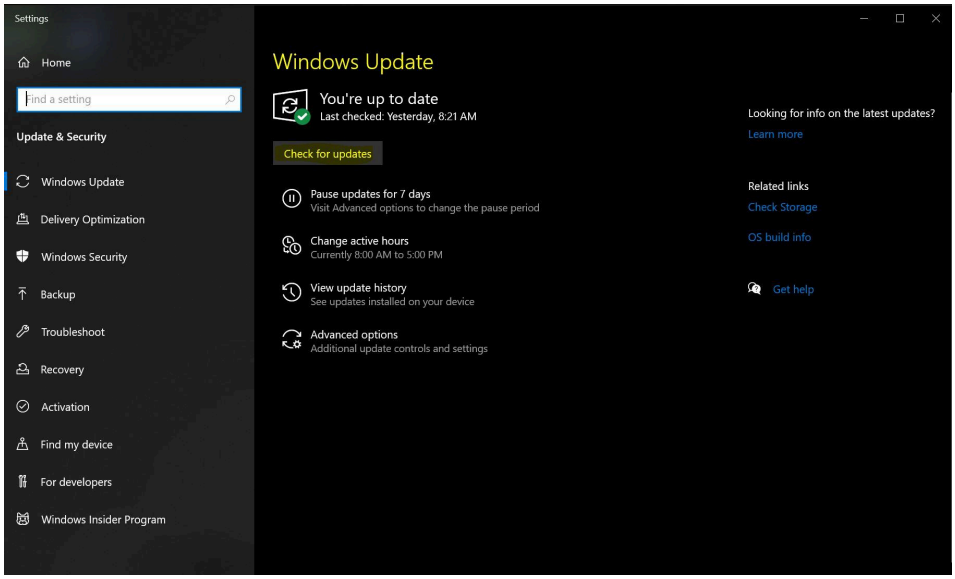
1. Step by Step instruction for executing hardening technique

2. Snapshot of steps

On windows search box search for “Update” and select “Check for updates”



New windows update window will appear.



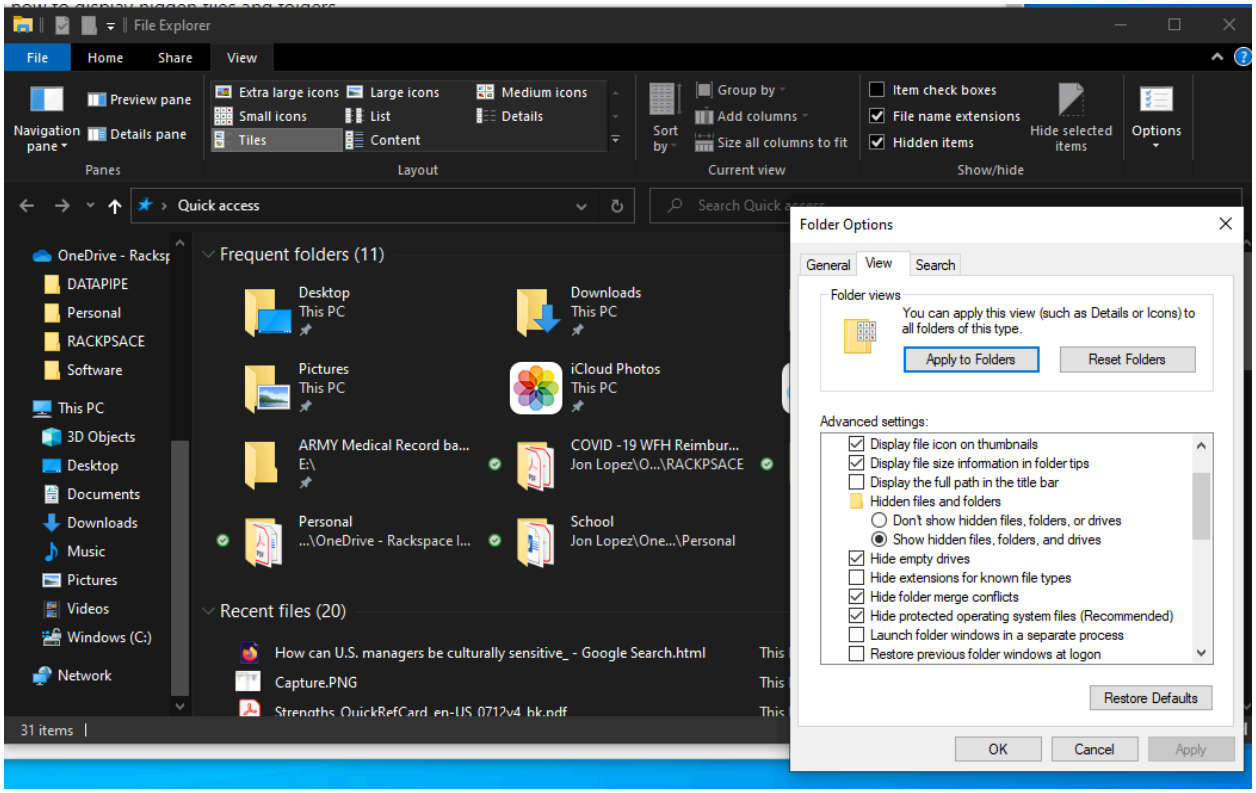
Press “Check for Updates” button to allow machines to contact Microsoft update servers for available patches.

14. Enable Visibility on Hidden Windows Files

This is a precaution that does not really contribute to hardening a server OS. Enabling visibility simply allows Administrators to see all the files. folders on a drive on a computer or server. I would caution against enabling this if normal users have access to the device since they may delete something that could cause functionality issues on the device.

1. Open File explorer, change tab to View and on the top right corner select Options(Change folder and search permissions)

2. Folder options - View and select show hidden files, folder and drives

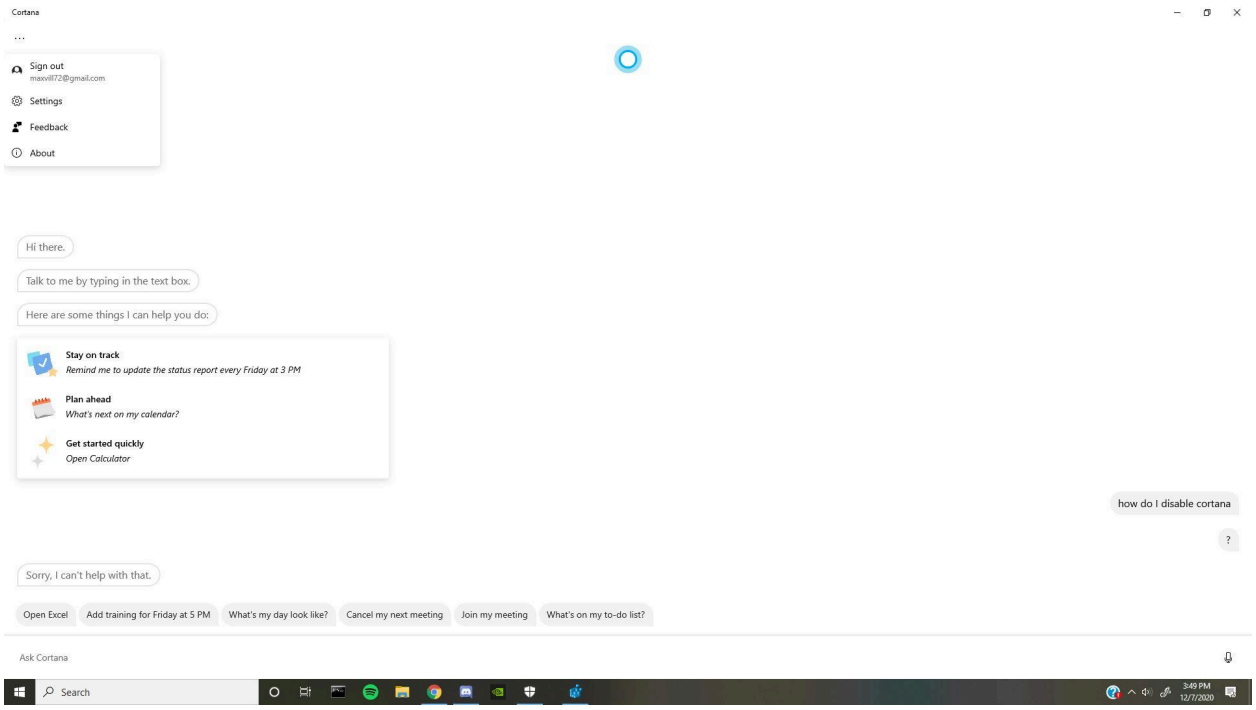


15. Disable Cortana

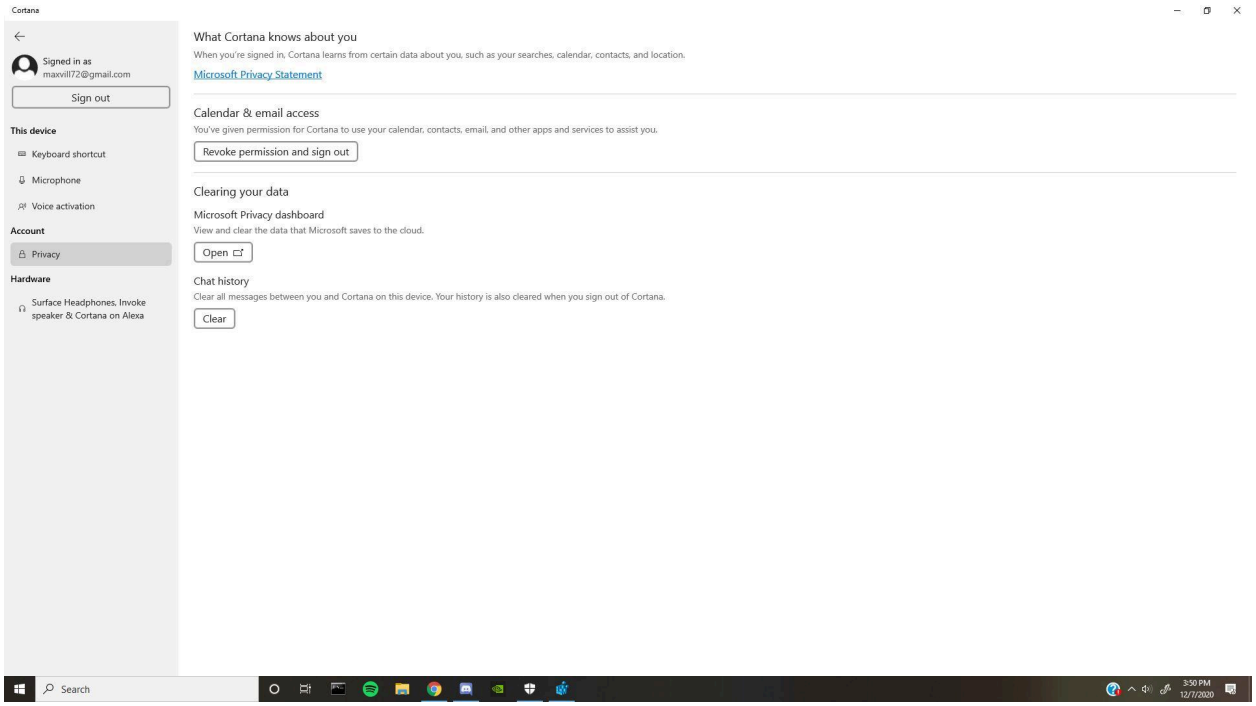
Cortana has been integrated more and more into the windows OS by the update. Cortana is a virtual assistant who learns about the user. This can be a security risk if you do not want your data collected or to be shared with cortana. The disadvantages to disabling Cortana would be a lessened learning about the user's routine, and the lack of the voice virtual assistant.

Disabling Cortana is quite simple.

Search for Cortana using the search bar by the bottom left of the screen and start the cortana program.



Once the cortana app has opened, click the three dots in the top left corner, and select settings.

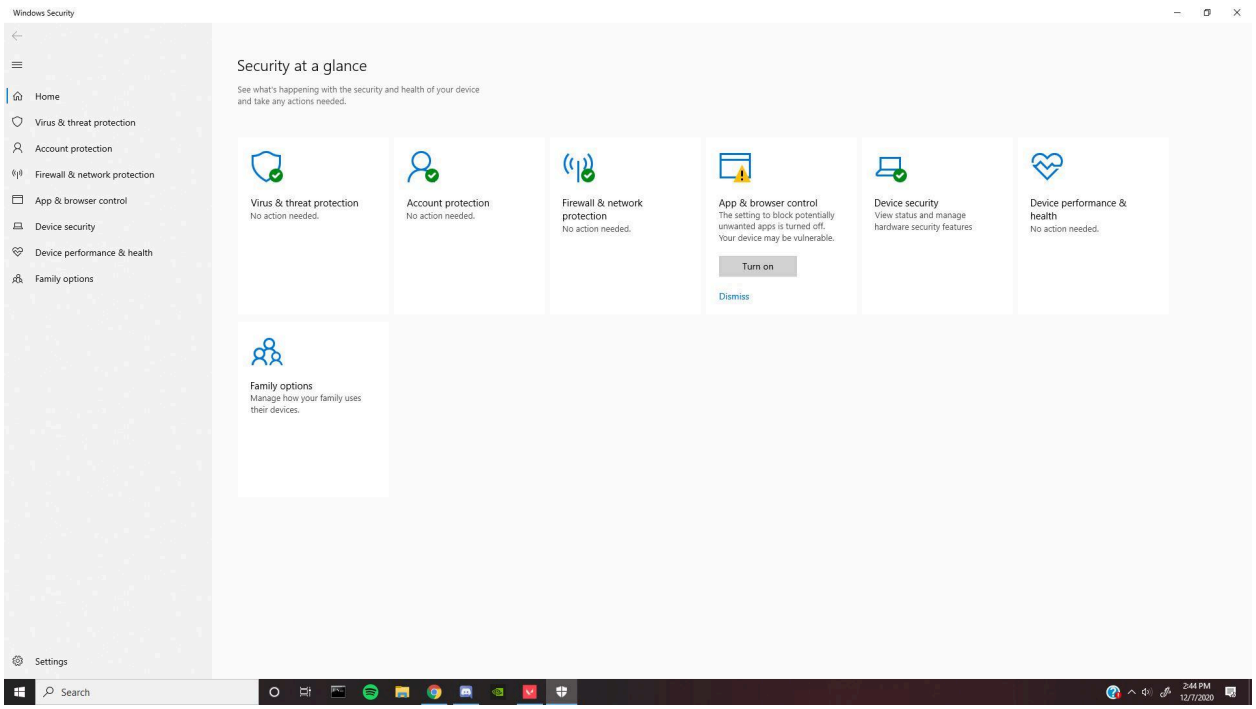


Choose the Revoke permissions and sign out button and you will no longer be using cortana.

16. Turn on Smartscreen filter

Smartscreen filter is a component of App & Browser control in the Windows Security application. The advantages to having it on are warnings when you are running downloaded or online applications. The disadvantage is these warnings may come for applications that the user intends to use.

1.First open the Windows Security application by searching for it using the search bar.



2.Select turn on under app & browser control.
(For more advanced setting you can adjust these settings in the Registry Editor.)

Application Hardening

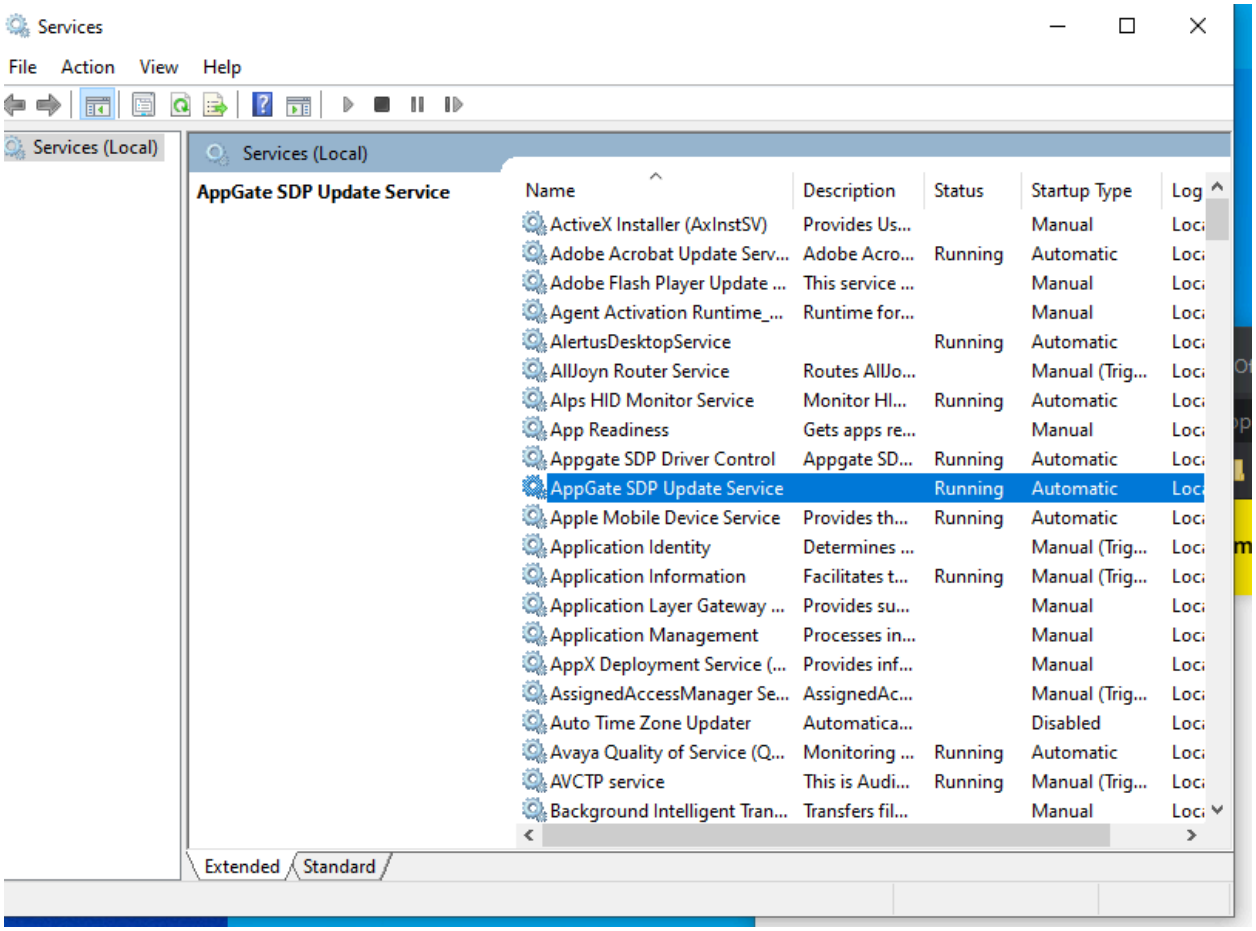
17. Disable Unneeded Services

PART A

Many computer break-ins are a result of people taking advantage of security holes or problems with these programs.

The more services that are running on your computer, the more opportunities there are for others to use them, break into or take control of your computer through them.

1. Open the Services and Locate a service to disable
2. Double-click the service to open its Properties dialog box and Choose Disabled as the Startup type.



3.

AntiVirus Hardening

18. Install and Updating an Antivirus

PART A:

1. How does it harden your host?

Antivirus is software that is purposely built to detect and remediate malicious activity from malware and viruses. Microsoft has built in antivirus functionality called “Windows Defender” which can prevent malicious software from compromising a computing asset. An active antivirus scanning a host system will protect it like a guard dog protecting a house.

Microsoft Corporation. (n.d.). *Latest security intelligence updates for Microsoft defender antivirus and other Microsoft antimalware - Microsoft security intelligence*. Microsoft. https://www.microsoft.com/en-us/wdsi/defenderupdates

2. What are the advantages and disadvantages of it?

Advantages: Active protection from Windows Defender can defend against viruses from establishing a foothold on a host machine. Scanning from antiviruses can validate that a system is clean and free from malware.

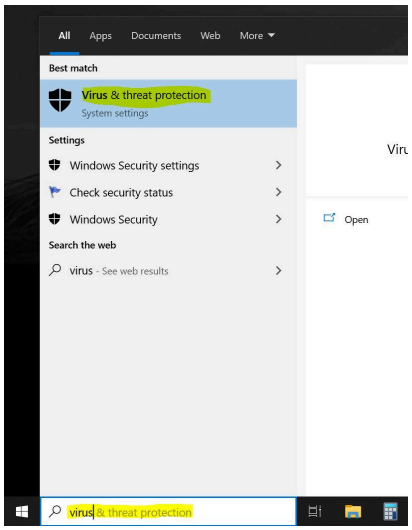
Disadvantages: Windows Defender is signature based antivirus. Signature based means that it will actively look for malware provided from Microsoft’s library of actively malicious software. More advanced zero-day threats might not be detected. Active scanning of a host device can take up computing resources from the CPU and RAM.

PART B:

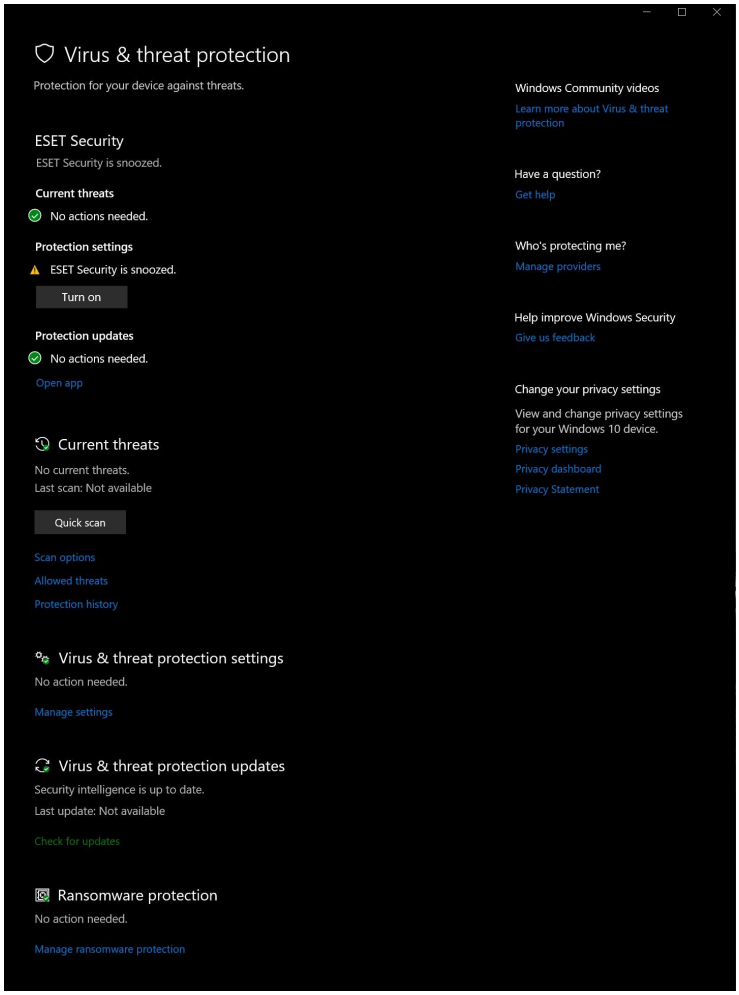
1. Step by Step instruction for executing hardening technique

2. Snapshot of steps

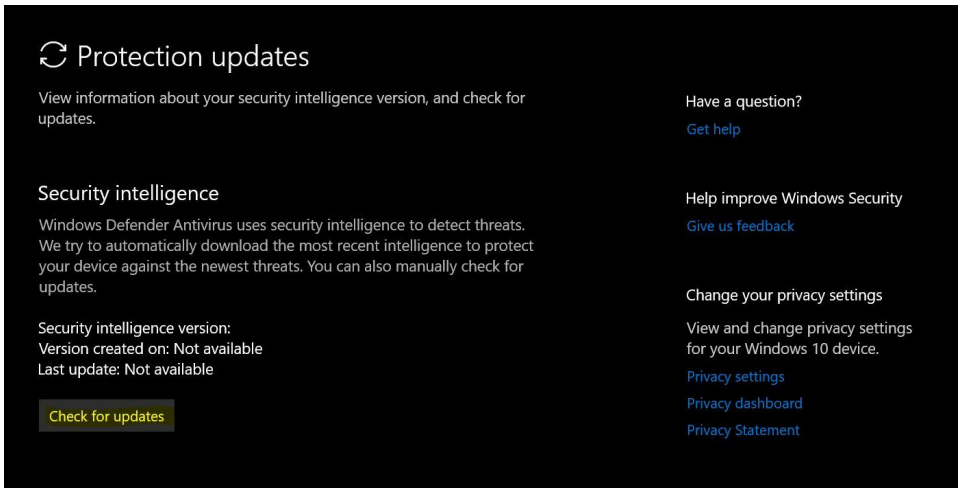
In windows search box, search for “Virus & Threat Protection”



Once Virus & Threat Protection window opens, select option to enable threat scanning



Select Protection Update click “Check for Updates” to check for latest antivirus definitions



Physical Hardening

19. Limit the Physical Access of a Host

PART A:

1. How does it harden your host?

Limiting physical access of the host computer minimizes attack surface. This protects the USB ports and from physically damaging the computer rendering it unusable. USB devices that have built-in keyloggers and other malicious payloads can be plugged in.

Information Security Training | SANS Cyber Security Certifications & Research. https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120

2. What are the advantages and disadvantages of it?

Advantage: This protects a computing device from unauthorized access and minimizes the attack surface from malicious entities. This provides a certain level of protection if only authorized users can open a computer case or change peripheral devices plugged into it.

Disadvantage: Some locations might have bad airflow which could raise operating temperatures for the computing device. Hard to reach locations could potentially make upgrading or using peripheral devices difficult. If a location/cabinet uses locks, maintaining keys and ensuring keys are not lost increases overhead for an organization.

PART B:

1. Step by Step instruction for executing hardening technique

2. Snapshot of steps

Locate a computing asset and find a suitable location where peripheral devices can reach

Place computer inside cabinet and secure door to protect from unauthorized access

20. Create Physical Backups

PART A:

1. How does it harden your host?

Separate physical backups is good policy towards disaster recovery. This hardens a host machine's data from untimely events such as corrupted data, ransomware and other malware infection, and accidental deletions of files. It's always good to be able to roll back from unfortunate events especially if this data is critical such as photos, tax documents, etc.

Got backups? (n.d.). SANS Security Awareness.
https://www.sans.org/security-awareness-training/resources/got-backups

2. What are the advantages and disadvantages of it?

Advantage: This allows users to be able to deflect unfortunate events and be able to continue moving forward. Data can be pulled from external physical sources to quickly recover from these events. Data can be transferred without going through the cloud. This can be useful for data security or where internet connection is not available or reliable.

Disadvantage: It requires time to backup and recover data from physical sources. This requires physical access to the host machine to be inserted into USB ports. There are certain cases where machines are locked away behind cabinets and USB ports are difficult to reach. Physical Backups can also be stolen, lost/misplaced. It is important to maintain encryption on this data during storage.

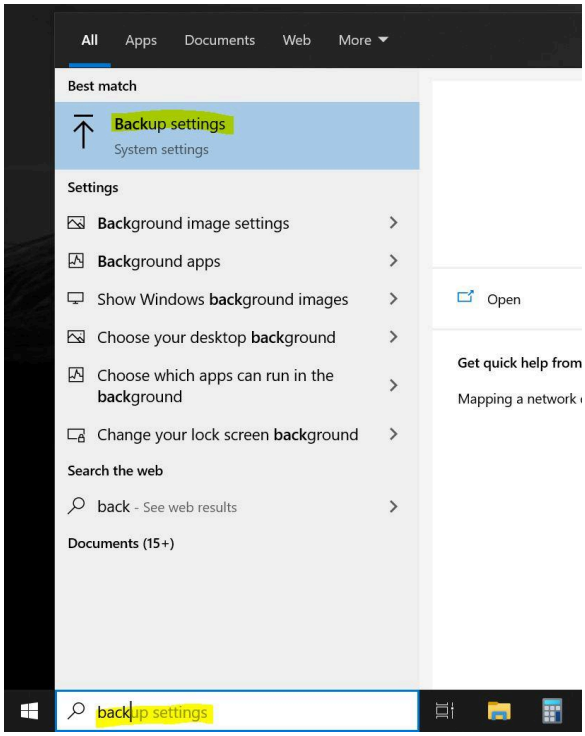
PART B:

1. Step by Step instruction for executing hardening technique

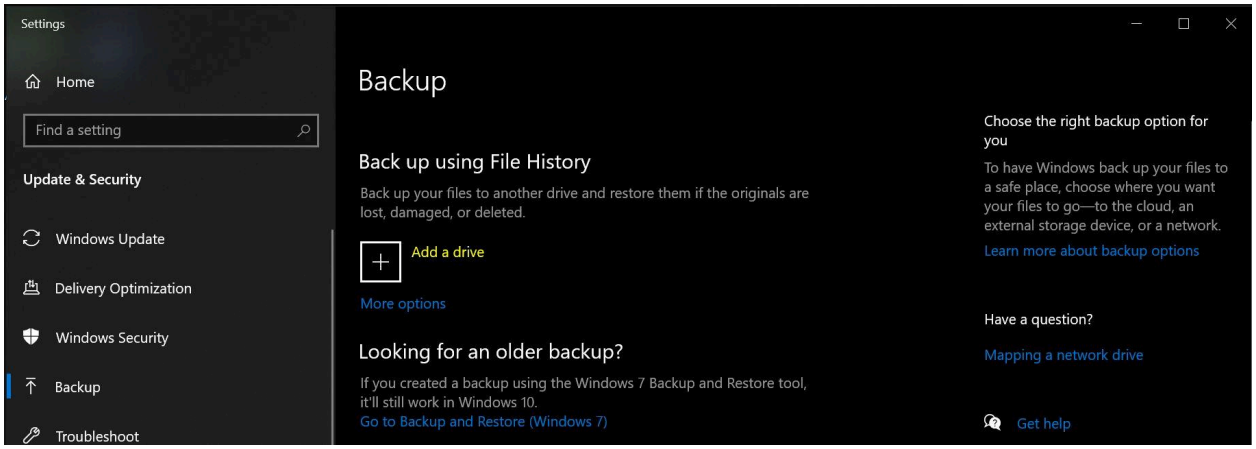
2. Snapshot of steps

Plug in an external hard drive to be used for backup purposes into the host machine USB port.

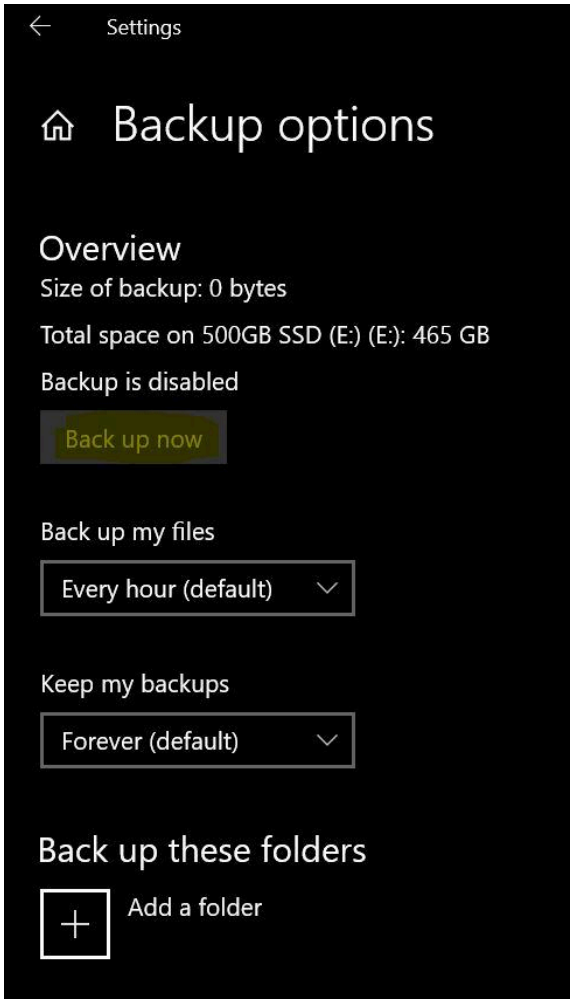
Go to windows search box and look for "Backup Settings"



Back up Window will open, select “Add a Drive” option to choose your external drive



New window showing “Backup Options” opens and select “Back up Now”



Once backup is completed, place the external drive in safe location

Works Cited:

Anatomy of a firmware attack. (2019, December 23). Security Boulevard. https://securityboulevard.com/2019/12/anatomy-of-a-firmware-attack/

Change Windows SmartScreen settings in Windows 10. (2018, August 24). Winaero - At the edge of tweaking. https://winaero.com/change-windows-smartscreen-settings-windows-10/

Changing your router's Wi-Fi password. (n.d.). Linksys. https://www.linksys.com/ca/support-article?articleNum=135554

Denisebmsft. (n.d.). *Apply mitigations to help prevent attacks through vulnerabilities - Windows security*. Developer tools, technical documentation and coding examples | Microsoft Docs. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/exploit-protection

Finding checksum values in Windows 10. (n.d.). Microsoft Community. https://answers.microsoft.com/en-us/windows/forum/windows_10-security/finding-checksum-values-in-windows-10/dbc3c569-4b5a-4967-8810-c25255cdc1fd

Gibson, S., & CORPORATION, G. R. (n.d.). *GRC | Port authority, for internet Port 23*. Home of Gibson Research Corporation . https://www.grc.com/port_23.htm

Got backups? (n.d.). SANS Security Awareness. https://www.sans.org/security-awareness-training/resources/got-backups

How to close unused open ports: TCP and UDP Port scan. (2014, June 19). Acunetix. https://www.acunetix.com/blog/articles/close-unused-open-ports/

How to disable AutoPlay and AutoRun in Windows 10. (2018, May 7). TechRepublic. https://www.techrepublic.com/article/how-to-disable-autoplay-and-autorun-in-windows-10/

Information Security Training | SANS Cyber Security Certifications & Research. https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120

Information Technology Services. (n.d.). Information Technology Services | Connecting Campus. https://its.uiowa.edu/support/article/1418

Locklear, G. (2020, November 24). *RDP vulnerability: Avoid RDP exploits*. Remote Support Blog | Netop. https://blog.netop.com/avoid-rdp-vulnerabilities-with-a-secure-remote-desktop

Microsoft Corporation. (n.d.). *Latest security intelligence updates for Microsoft defender antivirus and other Microsoft antimalware - Microsoft security intelligence*. Microsoft. https://www.microsoft.com/en-us/wdsi/defenderupdates

RDP security explained. (2020, May 5). McAfee Blogs. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rdp-security-explained/

Staff, G. 3. (2017, April 19). *How to disable Cortana on Windows 10*. NDTV Gadgets 360. https://gadgets.ndtv.com/laptops/features/how-to-disable-cortana-on-windows-10-1683223

Use FileVault to encrypt the startup disk on your Mac. (2018, November 30). Apple Support. https://support.apple.com/en-us/HT204837

(n.d.). Ubuntu Releases. https://releases.ubuntu.com/20.04.1/SHA256SUMS