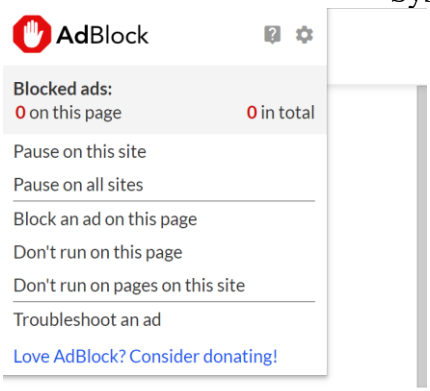
System Hardening Paper

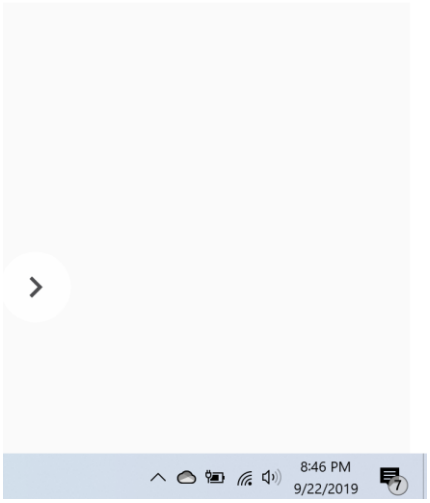
Mohanad Horani

UAT

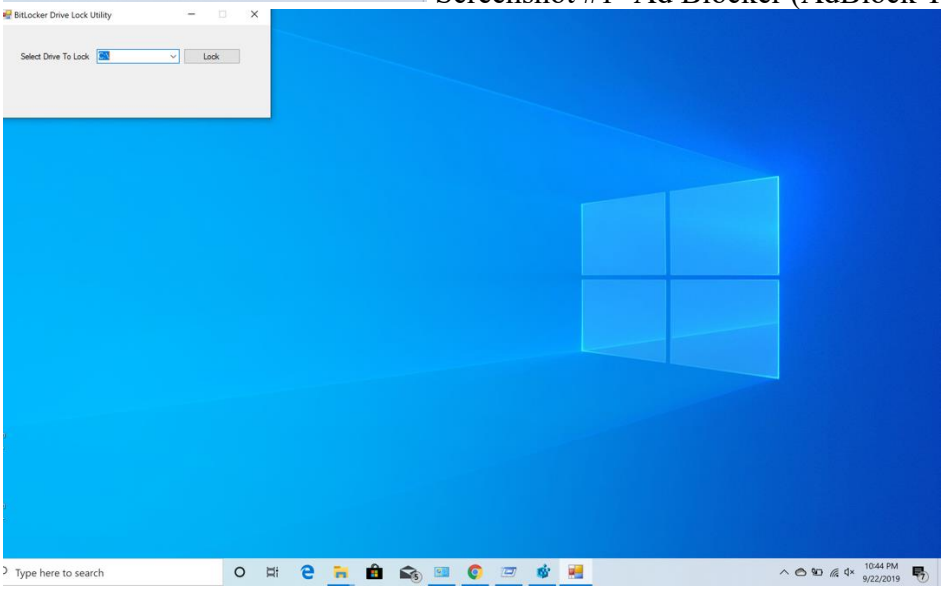
Identity Protection and Personal Security

System Hardening Screenshots #1-2:



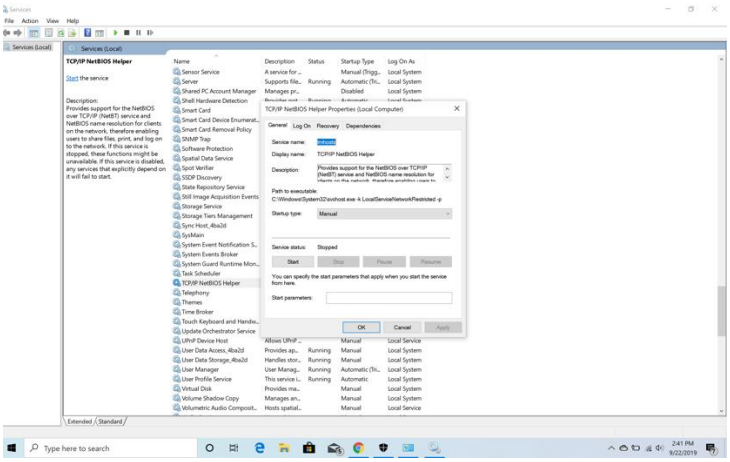


Screenshot #1- Ad Blocker (AdBlock Tool)

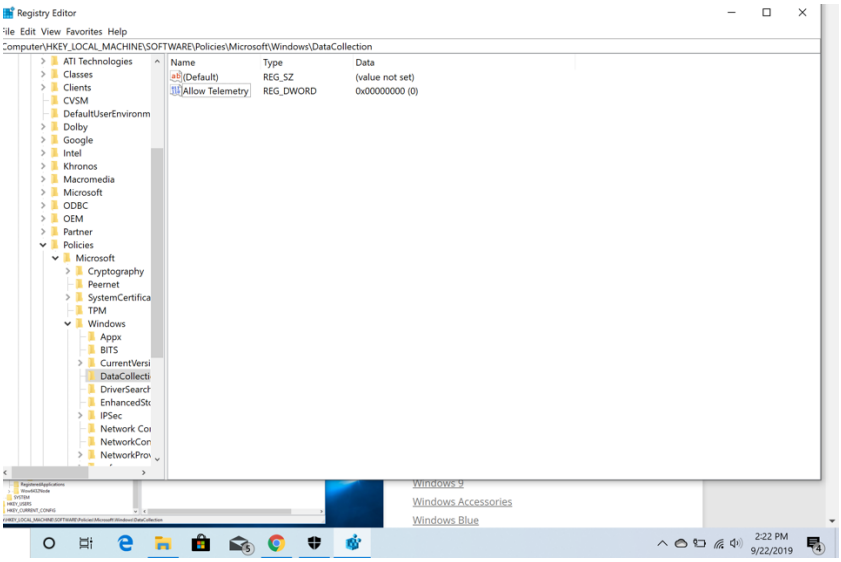


Screenshot #2- BitLocker Tool

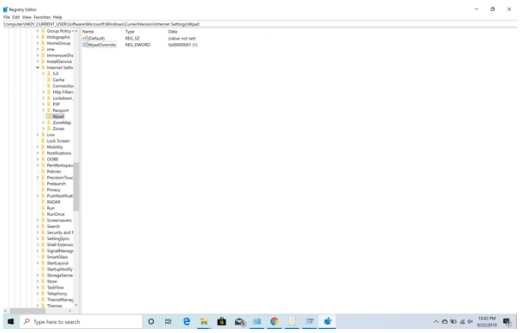
System Hardening Screenshots #3-5:



Screenshot #3- TCP/IP NetBIOS Helper Disabled

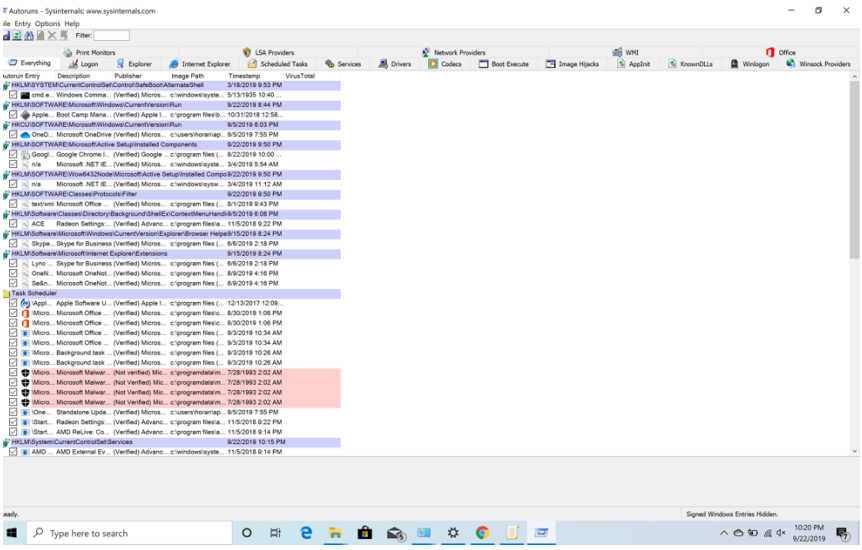


Screenshot #4- Disabling Telemetry

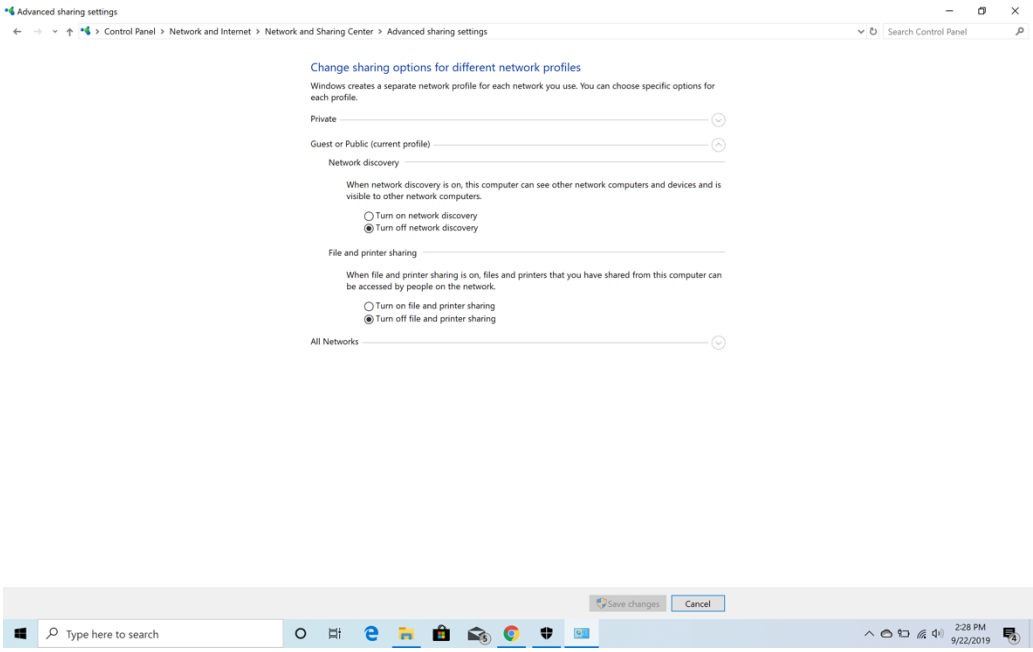


Screenshot #5- Disable WPAD

System Hardening Screenshots #6-7

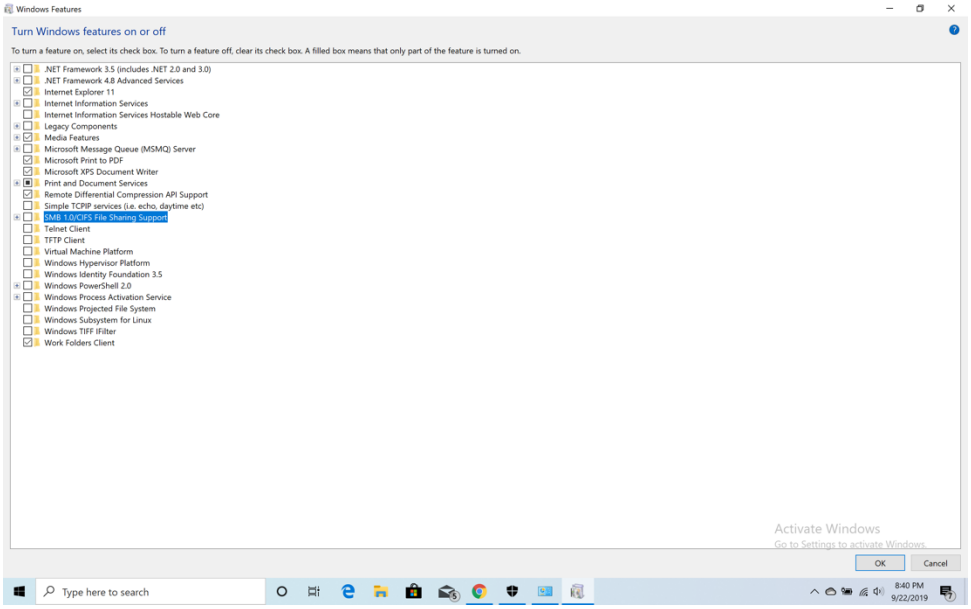


Screenshot #6- SysInternals

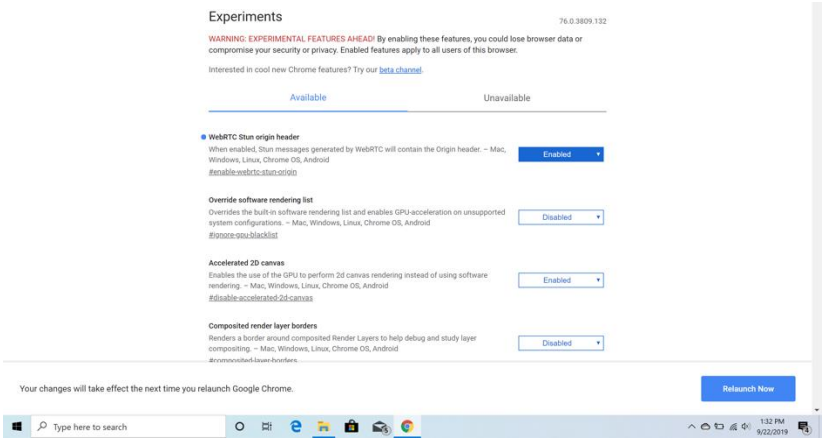


Screenshot #7- Disabling Network Discovery and Disabling File Sharing/Printer Sharing

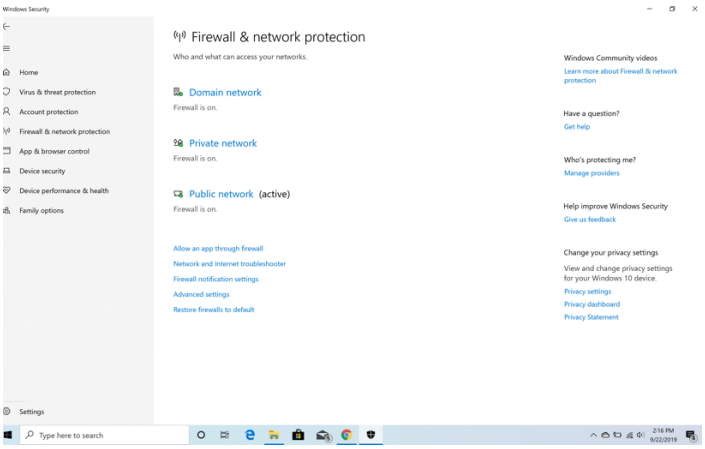
System Hardening Screenshots #8-10



Screenshot #8- Turning off unused Windows 10 features.



Screenshot #9- Disabling WebRTC in Chrome



Screenshot #10- Enabling Firewall

System Hardening Screenshot Descriptions:

Screenshot #1- In the first screenshot, I installed an Ad Blocker for Chrome which is called "Adblock." I simply installed it by searching the main website of the ad blocker called "getadblock.com" and then installed it onto Google Chrome while making sure it was running. The main objective of an ad blocker like the one mentioned above is to prevent advertisements from running on websites that users browse online.

Screenshot #2- In the second screenshot, I utilized BitLocker. BitLocker is accessible from Windows 10 Settings, although there are other methods in accessing it such as searching it in the Windows 10 search bar. The purpose of an application such as BitLocker is to protect your files by utilizing drive encryption while setting a password to access the hard drive.

Screenshot #3- In the third screenshot, I disabled TCP/IP NetBIOS settings and prevented TCP/IP NetBIOS from running on my Windows 10 machine. I found these settings under Control Panel under administrative settings. The purpose of this disabling these settings includes improving performance while the purpose of these setting in general is to allow for communication services on local networks.

Screenshot #4- In the fourth screenshot, I disabled Telemetry on my Windows 10 machine. I accomplished this by searching for the Registry Editor and then utilizing it to add a value called "Allow Telemetry" while setting its value to 0 in the same Registry Editor. The purpose of disabling Telemetry includes limiting the amount of data that is collected by Windows as well as improving the privacy on the user's Windows machine.

System Hardening Screenshot Descriptions Continued:

Screenshot #5- In the fifth screenshot, I disabled WPAD (Web Proxy Auto-Discovery). I accomplished this by creating a value in the registry editor called “WpadOverride” while setting its value to one. The purpose of performing these steps includes not allowing organizations or computers to discover the web proxy that the user is utilizing for privacy reasons.

Screenshot #6- In the sixth screenshot, I accessed SysInternals on my Windows 10 device. I accomplished this by downloading the software from the Windows website. The purpose of accessing SysInternals on any Windows device is to monitor, manage, and troubleshoot the Windows device that the user is utilizing.

Screenshot #7- In the seventh screenshot, I disabled file/printer sharing, and network sharing. I easily accomplished this by clicking on Control Panel and then under “Network and Sharing Center” under the “Network and Internet Settings,” I clicked on the “Advanced Sharing Settings.” The purpose of disabling file sharing/printer sharing/network sharing is to prevent unauthorized access to the user’s network, files, and printer.

Screenshot #8- In the eighth screenshot, I disabled Windows settings that were considered unnecessary such as .net 3.5, SMB v1, and Powershell 2. I disabled these settings by accessing Control Panel and then accessing the settings “Turn Windows Features on or off.” The purpose of this is to protect the user’s device as well as not allowing for vulnerabilities.

Screenshot #9- In the ninth screenshot, I disabled WebRTC in the Google Chrome on my Windows device. I accomplished this by typing "chrome://flags/#disable-webrtc" in the search box of the device. The purpose of disabling WebRTC is primarily to not let the browser determine the user's IP address as well as to not decrease the effectiveness of the proxy server.

Screenshot #10- In the tenth screenshot, I enabled Windows Firewall for all three networks (Domain, Private, and Public). I simply accessed the Windows 10 settings and then searched Firewall where the settings were displayed. The purpose of enabling the firewall for all three types of networks is to prevent unauthorized access to the network while connected and to not allow malware on the network as well.

References

Cawley, C. (2016, July 22). 5 Reasons Why You Should Use a Firewall. Retrieved from https://www.makeuseof.com/tag/5-reasons-use-firewall/

Chu, W. (2019, March 1). Should You Disable Windows 10 Telemetry? Retrieved from https://www.neweggbusiness.com/smartbuyer/windows/should-you-disable-windows-10-telemetry/

Disable File and Printer Sharing for Additional Security. (n.d.). Retrieved from https://support.microsoft.com/en-us/help/199346/disable-file-and-printer-sharing-for-additional-security

Exabytes.my (Malaysia) Support Portal. (n.d.). Retrieved from https://support.exabytes.com.my/en/support/solutions/articles/14000060758-disable-netbios-over-tcp-ip-support

Hoffman, C. (2017, March 14). Disable WPAD in Windows to Stay Safe on Public Wi-Fi Networks. Retrieved from https://www.howtogeek.com/298460/disable-wpad-in-windows-to-stay-safe-on-public-wi-fi-networks/

How to disable WebRTC in various browsers. (n.d.). Retrieved from https://whoer.net/blog/article/how-to-disable-webrtc-in-various-browsers/

Huculak, M. (2016, July 5). Setting up BitLocker Drive Encryption on Windows 10. Retrieved from https://www.windowscentral.com/how-use-bitlocker-encryption-windows-10

What is Windows Sysinternals? - Definition from WhatIs.com. (n.d.). Retrieved from https://searchwindowsserver.techtarget.com/definition/Windows-Sysinternals

Why and how to disable SMB1 on Windows 10/8/7. (2017, June 28). Retrieved from https://www.thewindowsclub.com/disable-smb1-windows