# CSIS 151- Windows OS Hardening

Hardening operating systems is an important part of a layered defense strategy. In this lab, you will take a comprehensive look at the Windows Desktop OS and follow best practices to harden the system to prepare it for deployment.

For each of the following items, provide screenshots as necessary to demonstrate your completion of the task. Paste and type directly into the gray boxes only. The boxes will expand as the paragraph grows.

User ConfigurationDescribe the current configuration along with the steps taken to harden the system based on best practices. Describe how the hardening techniques improve the security of the system.

**Your Response:**

|  |
| --- |
| If I had another user in the system, I would set up their account settings page under accounts and could choose to make them other or family. For the new user, I would not give them admin permission because I do not want to allow them to add whatever they would like to the system that would require the Admin username and password for downloading programs or accessing certain files.  Currently, as Admin I have set as notify when the app tries to make a change to the system, for the new user it would be set to Always notify that way would require them to use Admin username and password to access anything that they were not allowed to.  On my laptop, I currently do not have any other users that have access to or will be using my laptop. For adding a new user I would need to go to the account settings page under accounts and choose to make them other or family. If I did need to add another user I would create a new account and give that user the least privilege. With the current setup I have going on I have the notice if the app attempts to make a change to the system, with new users I would set up to always notify the reason being is that I do not want them to make any unwanted changes to the system or download anything that should not be added, requiring them to enter the admin user and password for downloading anything. Verify guest accounts are disabled as needed. Use password protection methods as well such as complexity and length requirements, setting password expiration, password history not allowing the user to use the same password x amount of days, and account lockout which if the user fails to enter correct password x amount of times they are locked of the account until admin unlocks or they time frame for them to enter passwords is available. |

Network ConfigurationDescribe the current configuration along with the steps taken to harden the system based on best practices. Describe how the hardening techniques improve the security of the system**Your Response**:

|  |
| --- |
| When it comes to my Network configuration, I’m always running off Wi-Fi and never hardwired into the router at all. So when I am on Wi-Fi if it is not my home network I set it to the public so that my computer is unable to be discovered on the network and that no one can access any files or programs I do not want them to have access to at all. I also disabled the option for ethernet port access so random users can not just hardwire into the laptop. My laptop is currently set up to auto DHCP so I do not have to worry about using a static IP address at all. |

Features and RolesDescribe the current configuration along with the steps taken to harden the system based on best practices. Describe how the hardening techniques improve the security of the system  
  
Your Response:

|  |
| --- |
| On my system, I have SMB 1.0/CIFS File Sharing support disabled, because I have no need to be sharing any files with anybody from my system. Also, where Admin has full control and just about every privilege that would be needed to carry out any task except special permissions. Other users who are non-admins only have the ability to read and execute content, read and write. This on my C drive is how it is currently set up. If there are certain files and programs, I do not want the end-user to access I can go to that specific file and make it so that they are unable to have any access to it at all. As it is currently set up the users who are not admins are unable to do anything that could harm files or programs. I could go deeper into the hardening which would make it so that non admin can do less but would come at the cost of them being able to actually use the laptop for their needs. |



patch management configurationDescribe the current configuration along with the steps taken to harden the system based on best practices. Describe how the hardening techniques improve the security of the system

**Your Response:**

|  |
| --- |
| When it comes to patch management, every week there will be a new update that you will need to download on your OS, the patches are used to fix any known zero-day attacks that may have been found that the operating system may be open the same with any malware where attacks that can come up. Keeping up on the updates on your system can be a pain because I like to wait around for the system to update. |

Firewall ConfigurationDescribe the current configuration along with the steps taken to harden the system based on best practices. Describe how the hardening techniques improve the security of the system

**Your Response:**

|  |
| --- |
| My current configuration when it comes to the firewall is that it is on for Domain, Public, and Private. As for techniques for improving my firewall hardening, making sure that firewalls are updated on the system, configuring strong passwords and no default passwords leading back to user configuration, setting up rules for remote accessing in with my current version of windows I do not have the ability to do remote access unless I upgrade, using rules-based such as admins are able to implement this rule other users need admin to username and password to be able to go about accessing the rule, housekeeping the rule base clearing out rules that no longer apply or not need updating rules that do apply and are needed. |

Remote access ConfigurationDescribe the current configuration along with the steps taken to harden the system based on best practices. Describe how the hardening techniques improve the security of the system

**Your Response:**

|  |
| --- |
| When it comes to remote access configuration due to the version of Windows 11 I do not have the ability to set up remote access configuration on my system. There are several ways to harden the system so that it can use remote access configuration with less worries about bad actors taking over. Those steps are the use of network authentication, higher-level encryption, disabling LTP redirections, disabling clipboard redirections, disabling network printer redirections, and restricting admins to one session. |

Service ConfigurationDescribe the current configuration along with the steps taken to harden the system based on best practices. Describe how the hardening techniques improve the security of the system

**Your Response:**

|  |
| --- |
| These are programs that I currently have running in the background of my system and the app I have open at this moment time running I have configured to make it so that when I boot up the programs do not open up at the start due to effecting the time for it to finish its boot-up process. |

Logging and monitoringDescribe the current configuration along with the steps taken to harden the system based on best practices. Describe how the hardening techniques improve the security of the system

**Your Response:**

|  |
| --- |
| So to free up some speed I can out-close programs that I have opened still, like chrome that is running background, closing out the extra apps that I don't need running. Currently, there is not a lot of CPU at this moment, if you pull up blizzard battle.net and then open up a game where a lot of CPU goes mainly. When I play games because of the amount of CPU that it takes up I go and make sure to close out any programs that I do not need running at all, otherwise I notice when I'm playing that speeds are going slower and will cause me latency issues as well. So with start-up, I have just about everything stopped to make it so that the bootup process goes faster. |