Cybersecurity

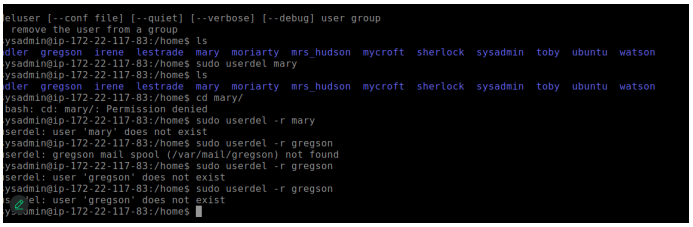
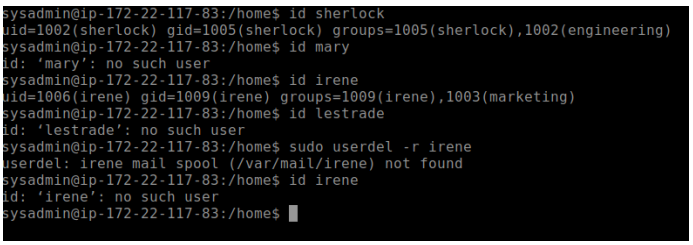
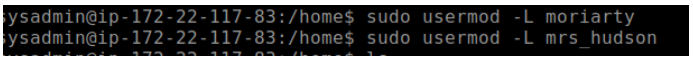
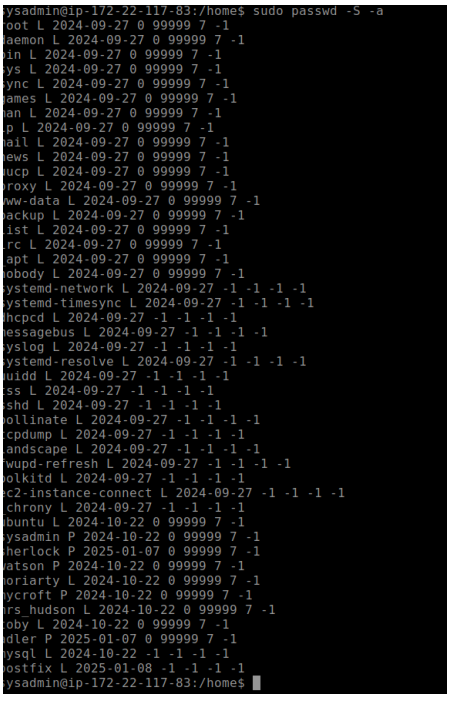
Project 1 Hardening Summary and Checklist

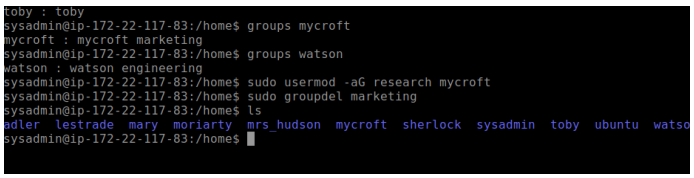
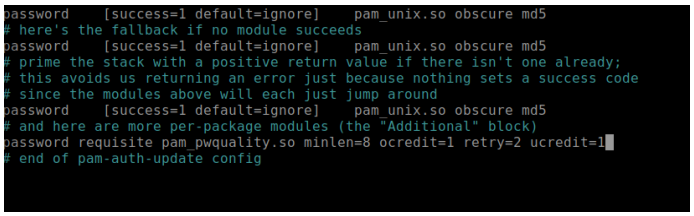
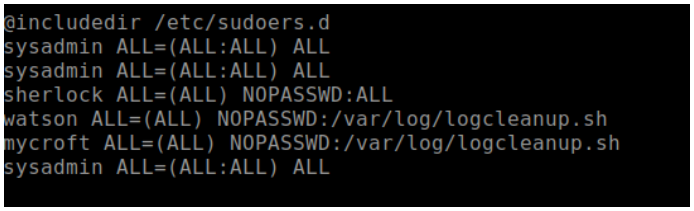
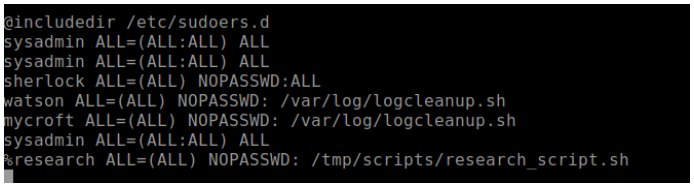
OS Information

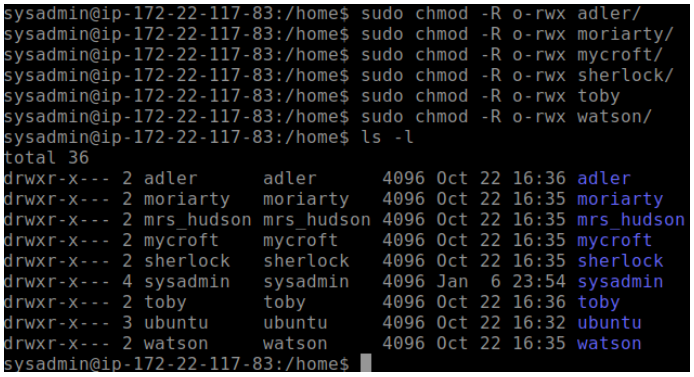
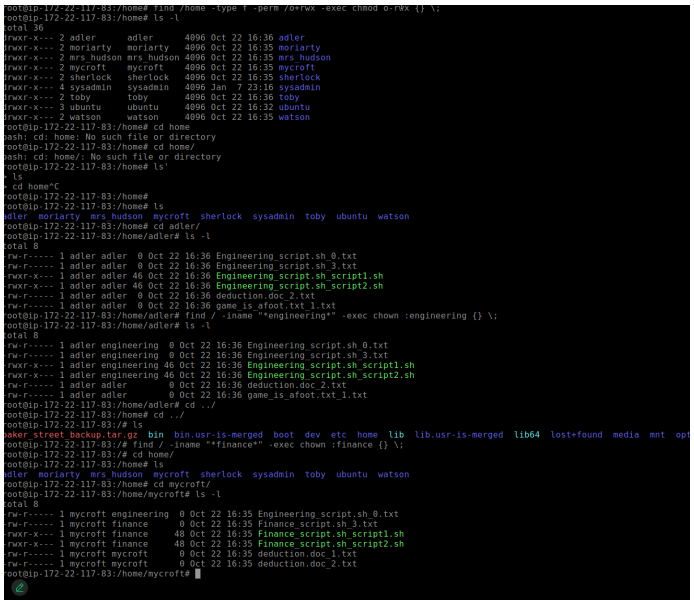
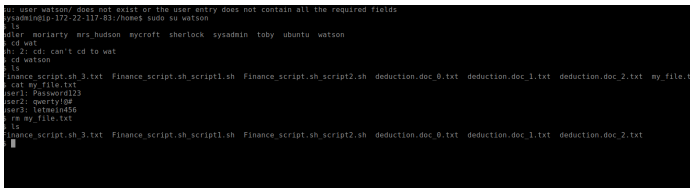
Customer	Baker Street Corporation
Hostname	ip-172-22-117-83
OS Version	6.8.0-1016-aws (**Uname** command was used)
Memory information	3.7Gi (**Free -h** command was used)
Uptime information	36 min (**Uptime** command was used)

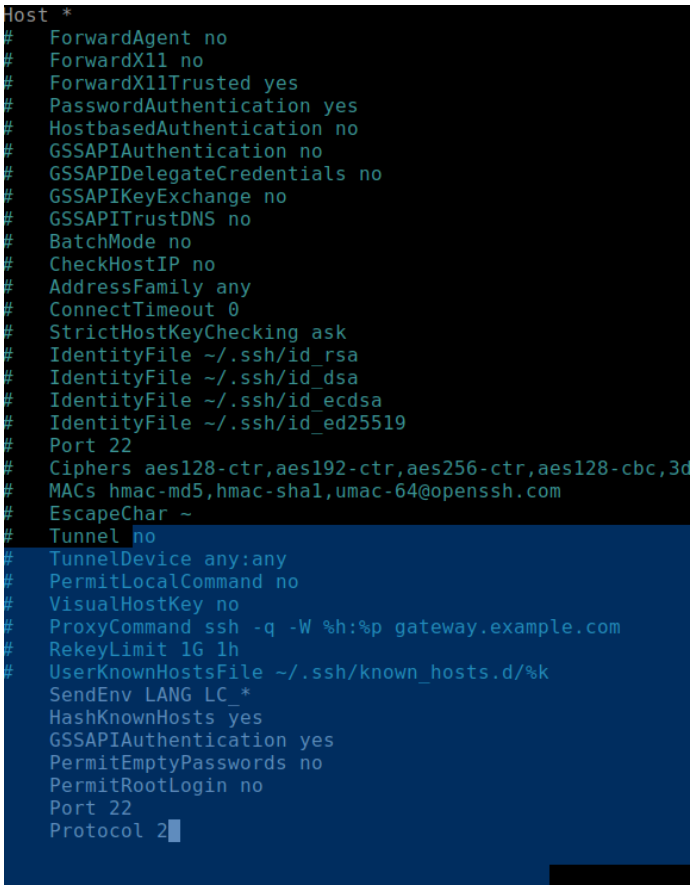
Checklist

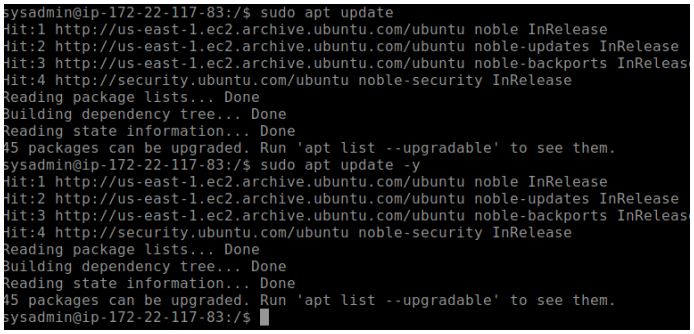
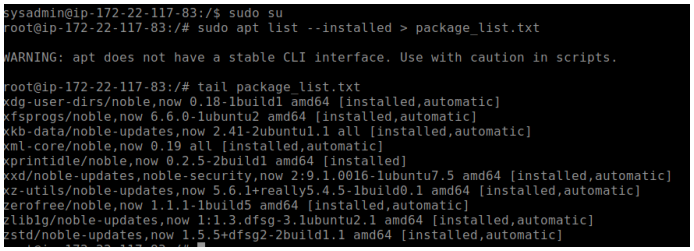
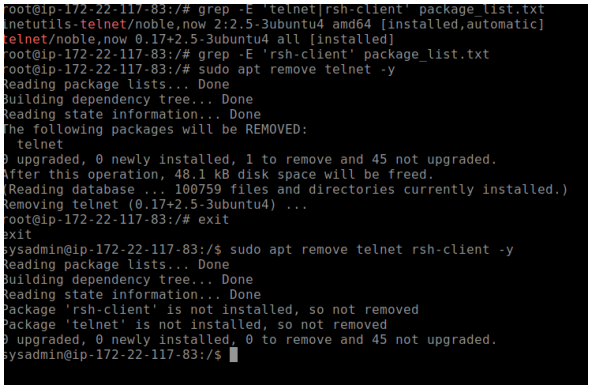
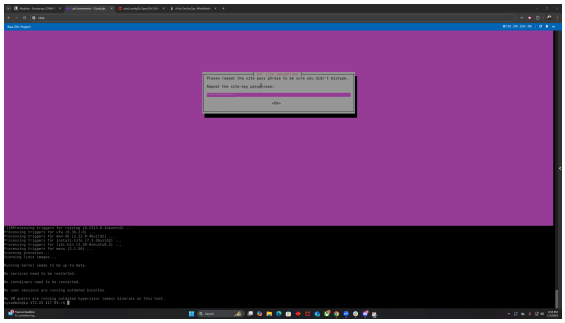
Completed	Activity	Script(s) used / Tasks completed / Screenshots
☑	OS backup	 The command I used was sudo tar -cvpzf /baker_street_backup.tar.gz --exclude=/baker_street_backup.tar.gz --exclude=/proc --exclude=/tmp --exclude=/mnt --exclude=/sys --exclude=/dev --exclude=/run / command creates a compressed archive of the entire file system, excluding the current backup

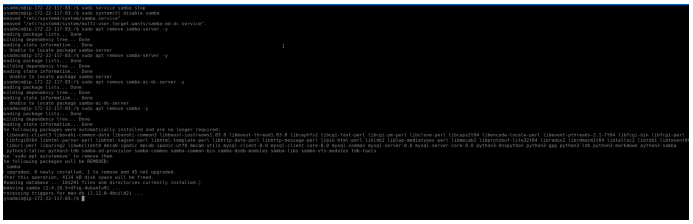
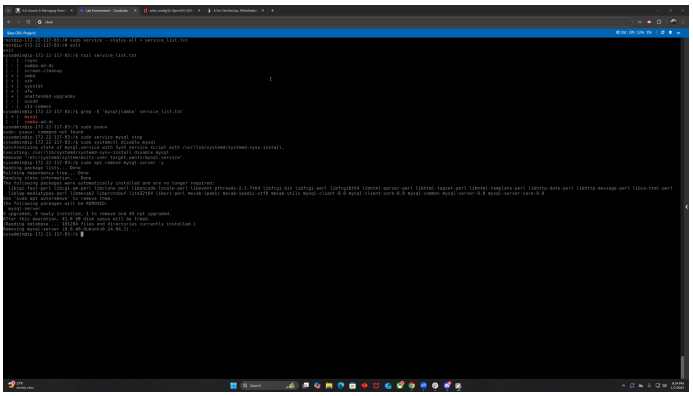
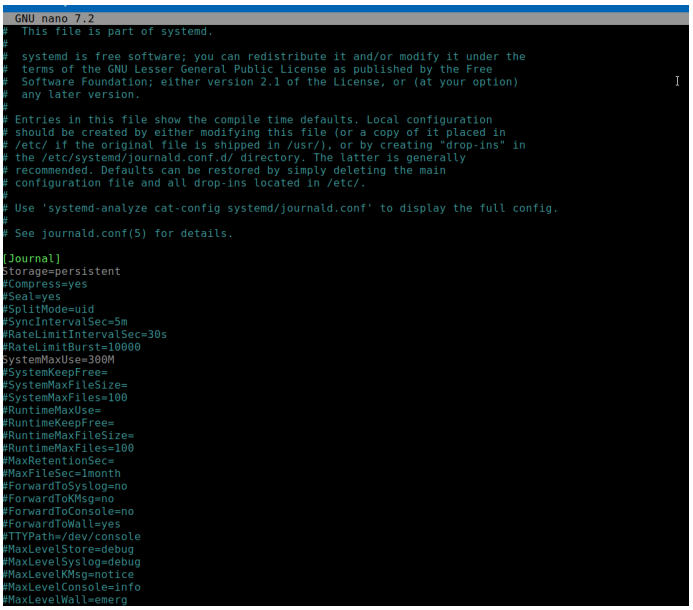
		archive, temporary files, and system directories, which are often unnecessary for backup.
☑	Auditing users and groups	   

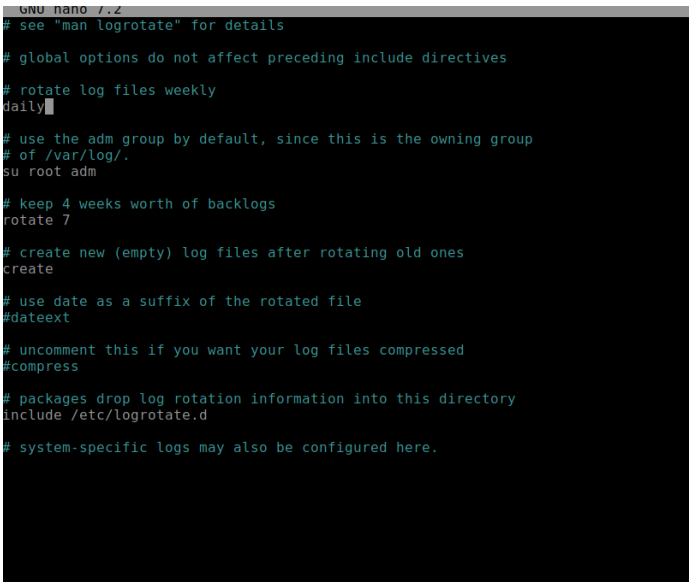
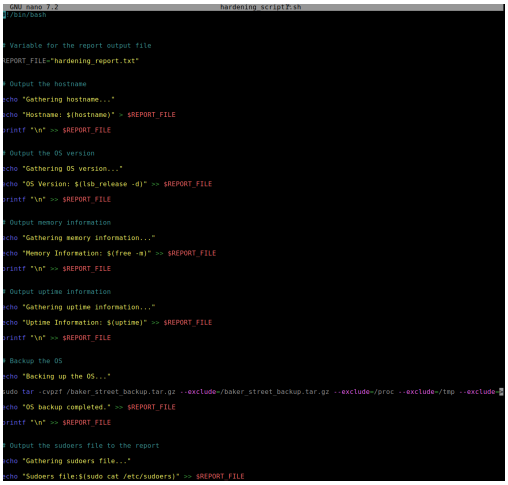
	Auditing users and groups	 to delete a user I used the command (sudo userdel -r *usersname*) and once the user was deleted I would verifty it by using the command (id *username*) Locker a user account I would use the command (sudo usermod -L *username*)
☑	Updating and enforcing password policies	 For password requirement and while using the Day 1 activity template I used/created the line of code as folllows: password prequisite pam_pwquality.so minlen=8 ocredit=1 retry=2 ucredit=1
☑	Updating and enforcing sudo permissions	  - once giving all priv var to both watson and mycroft as well as the research group, I verified it by using ls -l

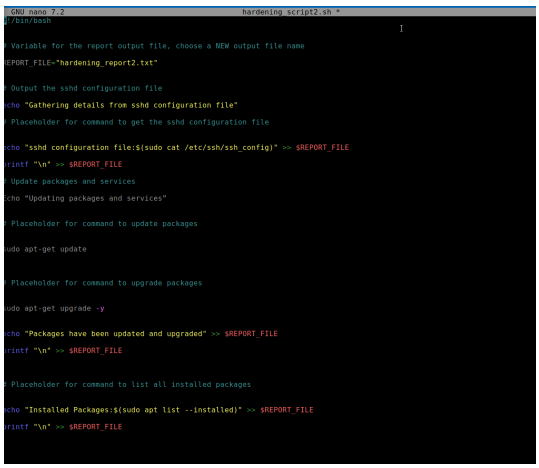
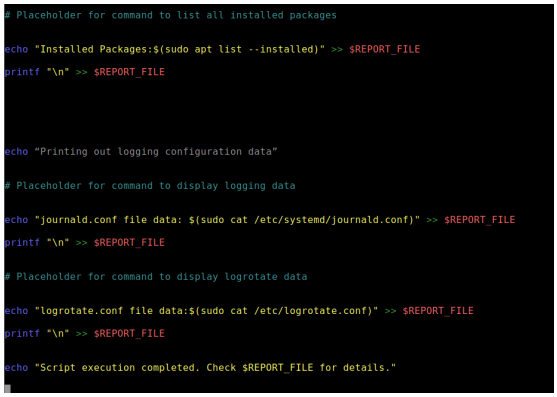
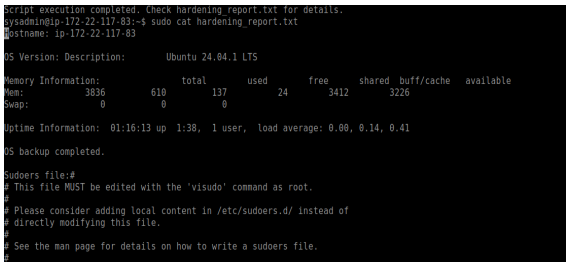
☑	Validating and updating permissions on files and directories	   -by using the sudo chmod I was able to remove world permissionsfrom all users as well using the chown command to change persmissions from files to only specific memebrs in designated groups. - to remove unwanted files from users I switched users to other users using (sudo su) and removing the my_file.txt from them.

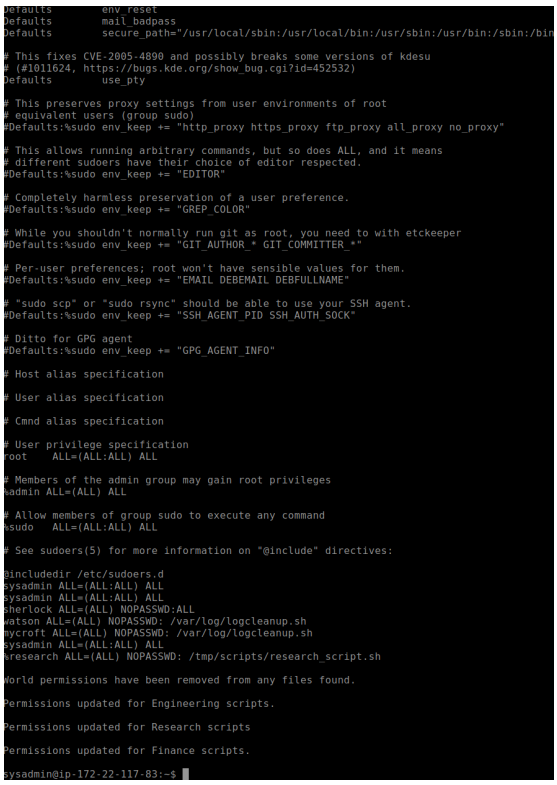
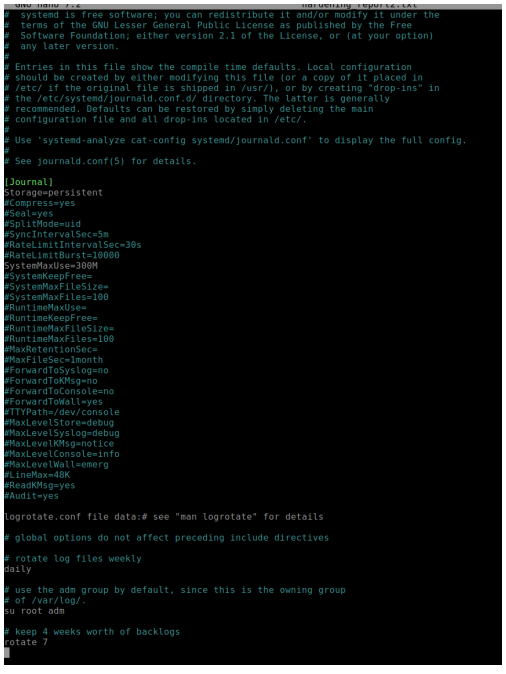
☐	Optional: Updating password hashing configuration	
☑	Auditing and securing SSH	 -using the daemon config file that was in thea activity file I was able to determine what to add and remove from the bash file for auditing and securing the SSH. - as well to restart the server i used the command (sudo service ssh restart) which allowd all the SSH updates to save

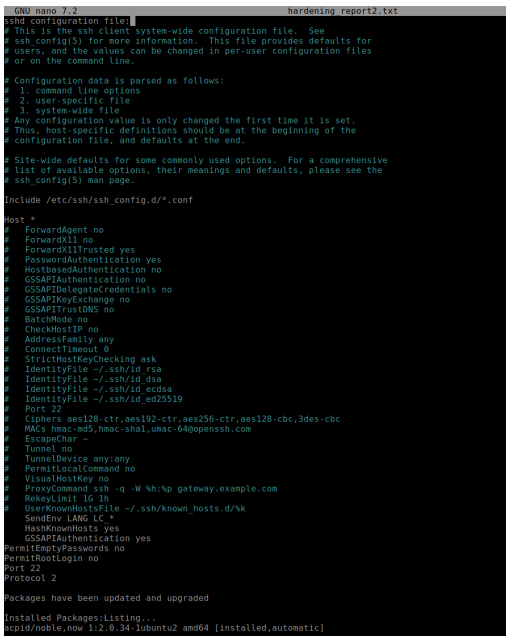
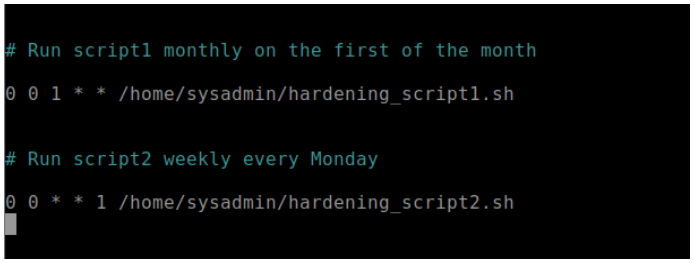
☑	Reviewing and updating system packages	    - for apt update and upgrade I used (sudo apt update / and / apt update -y) - while creating a package list while using (sudo apt lit --installed > package_list.txt) - Next I used the grep command to find any telnet or rsh-client that was need removal and then using the (apt remove) command to remove telnet and rsh-client -finally I installed the following (apt install ufw lynis tripwire)

☑	Disabling unnecessary services	  -First using the grep command i was able to find the existence of both mysql and samba server - then using the service stop /systemctl disable and apt remove for both servers samba and mysql I was able to erase them from my lab.
☑	Enabling and configuring logging	

	Enabling and configuring logging	 -using the Day 2 activity file as instructed I was able to open and edit the journald file and set both storage and systemmaxuse to thier required settings. - using the same strategy and methods of using the activity file i was able to do the same with logrotate file
☑	Scripts created	

	Scripts created	   

	Scripts created	 

	Scripts created	 -using the template file for day 3 I was able to harden the script for both 1 & 2 while updating the permissions to be able to check for any errors.
☑	Scripts scheduled with cron	 - by using the cron command I was able to create and set the times that is asked in the activity file. By making script 1 run on the first of the month and script 2 to be run weekly on every monday

Read Me: During the project my group and I used many resources to complete this project such as going back to old lectures and notes some of us have taken during the course. As well some of us used AI assistance to both understand how the command is working and what is the proper method and order to use the code.