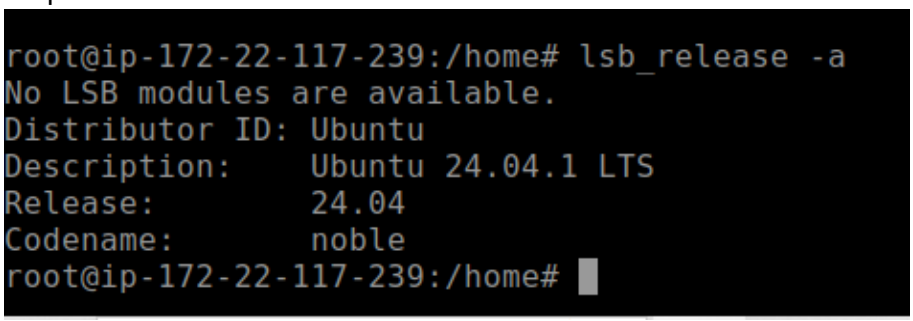
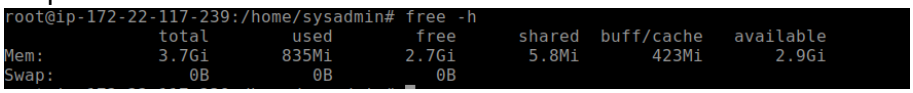
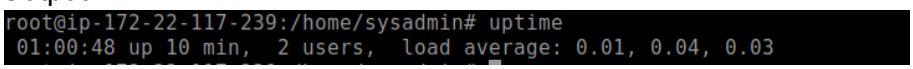
Cybersecurity

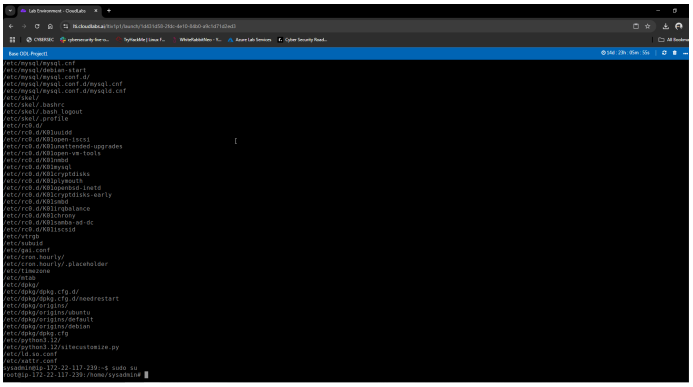
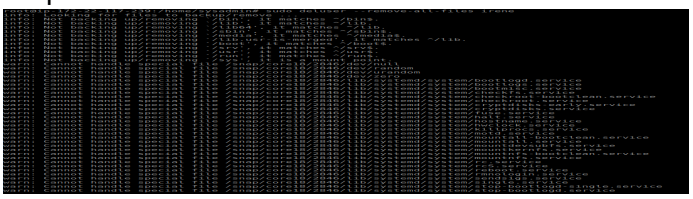
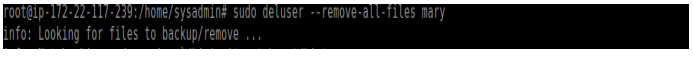
Project 1 Hardening Summary and Checklist

OS Information

Customer	Baker Street Corporation
Hostname	Command used: hostname Output: ip-172-22-117-239
OS Version	Command used: lsb_release -a Output: 
Memory information	Command used: free -h Output: 
Uptime information	Command used: uptime Output: 

Checklist

Completed	Activity	Script(s) used / Tasks completed / Screenshots

☑	OS backup	Command used: 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 / Output:  #sidenote: I ran the code posted in the guide but when i clicked out of the vm, the whole thing refreshed and took me out of root. I had done so before, but the second to last line in the screenshot is me switching back to root.
☑	Auditing users and groups	(deleting irene) Command used:sudo deluser --remove-all-files irene Output:  (deleting mary) Command used: sudo deluser --remove-all-files mary Output:  (deleting gregson) Command used: sudo deluser --remove-all-files gregson Output:

```
root@ip-172-22-117-239:/home/sysadmin# sudo deluser --remove-all-files gregson
info: Looking for files to backup/remove ...
info: Not backing up/removing `/bin', it matches ^/bin$.
info: Not backing up/removing `/lib', it matches ^/lib.
info: Not backing up/removing `/lib64', it matches ^/lib.
info: Not backing up/removing `/sbin', it matches ^/sbin$.
info: Not backing up/removing `/media', it matches ^/media$.
info: Not backing up/removing `/lib.usr-is-merged', it matches ^/lib.
info: Not backing up/removing `/boot', it matches ^/boot$.
info: Not backing up/removing `/srv', it matches ^/srv$.
info: Not backing up/removing `/usr', it matches ^/usr$.
info: Not backing up/removing `/run', it matches ^/run$.
info: Not backing up/removing `/sys', it is a mount point.
warn: Cannot handle special file /snap/core18/2846/dev/null
warn: Cannot handle special file /snap/core18/2846/dev/random
warn: Cannot handle special file /snap/core18/2846/dev/urandom
warn: Cannot handle special file /snap/core18/2846/dev/zero
```

- (locking temporary leave staff)

Command used:
sudo usermod -L moriarty
sudo usermod -L mrs_hudson

output:

```
root@ip-172-22-117-239:/home/sysadmin# sudo usermod -L moriarty
root@ip-172-22-117-239:/home/sysadmin# sudo usermod -L mrs_hudson
```

- (unlocking employed users)

Command used:
sudo passwd -d adler (bypasses “no password” error when using sudo usermod -U adler)

sudo usermod -U adler

Output:

```
root@ip-172-22-117-239:/home/sysadmin# sudo passwd -d adler
passwd: password changed.
root@ip-172-22-117-239:/home/sysadmin# sudo usermod -U adler
```

Command used: sudo passwd -d toby (bypasses “no password” error)

sudo usermod -U toby

Output:

```
root@ip-172-22-117-239:/home/sysadmin# sudo passwd -d toby
passwd: password changed.
root@ip-172-22-117-239:/home/sysadmin# openssl passwd -1 "new_password"
                                       sudo usermod -U toby
```

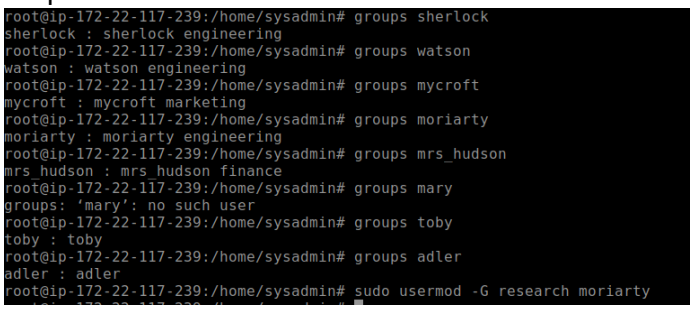
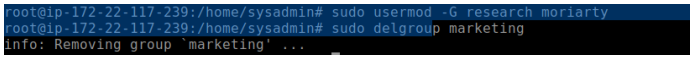
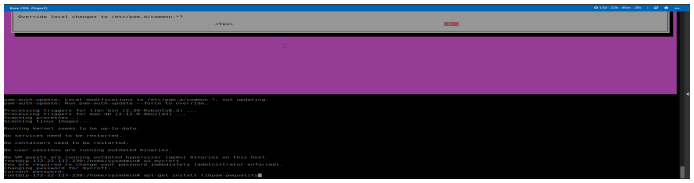
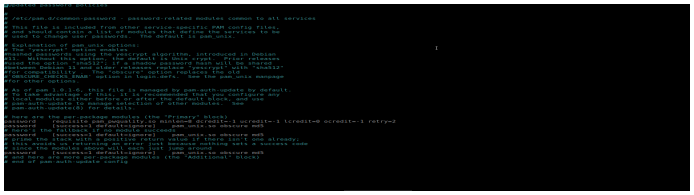
(please ignore the openssl command)

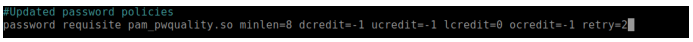
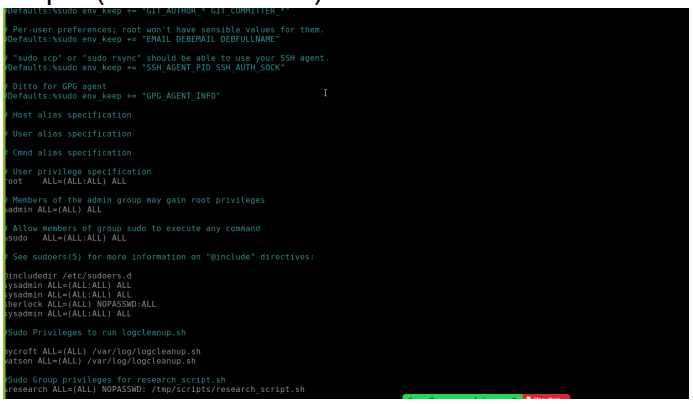
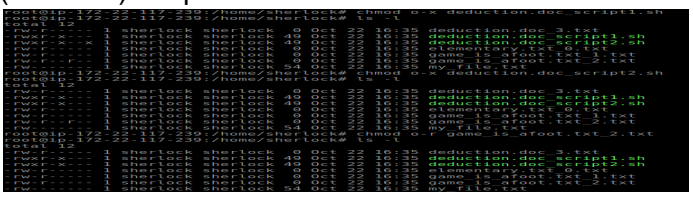
- (creating and moving group users from marketing to research group)

(creating research group) Command used: sudo addgroup research

Output:

```
root@ip-172-22-117-239:/home/sysadmin# sudo addgroup research
info: Selecting GID from range 1000 to 59999 ...
info: Adding group `research' (GID 1009) ...
```

		(checking users) Command used: groups <username> then (moving moriarty) Command used: sudo usermod -G research moriarty Output:  (deleting marketing group) Command used: sudo delgroup marketing Output: 
☑	Updating and enforcing password policies	Command used:apt-get install libpam-pwquality Output:  (bottom of install, way too long to screenshot full install) (Common password file prior to editing password requisites):  (new password policies) command used: minlen=8 dcredit=-1 ucredit=-1 lcredit=0 ocredit=-1 retry=2 Output:

		
☑	Updating and enforcing sudo permissions	• (giving sherlock full sudo privileges) Command used: sudo visudo (opens sudoers file) sherlock ALL=(ALL) NOPASSWD:ALL • (giving sudo privileges to mycroft and watson to run logcleanup.sh) Command used: mycroft ALL=(ALL) /var/log/logcleanup.sh watson ALL=(ALL) /var/log/logcleanup.sh (giving research group privileges to run research_script.sh) Command used: %research ALL=(ALL) NOPASSWD: /tmp/scripts/research_scripts.sh Output (for all the above): 
☑	Validating and updating permissions on files and directories	• (removing world permissions from user's home directories) Command used: chmod o-x <filename>, chmod o-r <filename>, chmod o-w <filename> (sherlock) Output: 

(watson) Output:

```
root@ip-172-22-117-239:/home# cd watson
root@ip-172-22-117-239:/home/watson# ls -l
total 12
-rw-r--r-- 1 watson watson  0 Oct 22 16:35 Finance_script.sh_3.txt
-rwxr-xr-x 1 watson watson 47 Oct 22 16:35 Finance_script.sh_script1.sh
-rwxr-xr-x 1 watson watson 47 Oct 22 16:35 Finance_script.sh_script2.sh
-rw-r--r-- 1 watson watson  0 Oct 22 16:35 deduction.doc_0.txt
-rw-r--r-- 1 watson watson  0 Oct 22 16:35 deduction.doc_1.txt
-rw-r--r-- 1 watson watson  0 Oct 22 16:35 deduction.doc_2.txt
-rw------- 1 watson watson 54 Oct 22 16:35 my_file.txt
root@ip-172-22-117-239:/home/watson# chmod o-r Finance_script.sh_3.txt
root@ip-172-22-117-239:/home/watson# chmod o-rx Finance_script.sh_
Finance_script.sh_3.txt      Finance_script.sh_script1.sh  Finance_script.sh_script2.sh
root@ip-172-22-117-239:/home/watson# chmod o-rx Finance_script.sh_
Finance_script.sh_3.txt      Finance_script.sh_script1.sh  Finance_script.sh_script2.sh
root@ip-172-22-117-239:/home/watson# chmod o-rx Finance_script.sh_script1.sh
root@ip-172-22-117-239:/home/watson# chmod o-rx Finance_script.sh_script2.sh
root@ip-172-22-117-239:/home/watson# chmod o-r deduction.doc_0.txt
root@ip-172-22-117-239:/home/watson# chmod o-r deduction.doc_1.txt
root@ip-172-22-117-239:/home/watson# chmod o-r deduction.doc_2.txt
root@ip-172-22-117-239:/home/watson# ls -l
total 12
-rw-r----- 1 watson watson  0 Oct 22 16:35 Finance_script.sh_3.txt
-rwxr-x--- 1 watson watson 47 Oct 22 16:35 Finance_script.sh_script1.sh
-rwxr-x--- 1 watson watson 47 Oct 22 16:35 Finance_script.sh_script2.sh
-rw-r----- 1 watson watson  0 Oct 22 16:35 deduction.doc_0.txt
-rw-r----- 1 watson watson  0 Oct 22 16:35 deduction.doc_1.txt
-rw-r----- 1 watson watson  0 Oct 22 16:35 deduction.doc_2.txt
-rw------- 1 watson watson 54 Oct 22 16:35 my_file.txt
root@ip-172-22-117-239:/home/watson#
```

(moriarty) Output:

```
root@ip-172-22-117-239:/home/moriarty# chmod o-r Finance_script.sh_0.txt
root@ip-172-22-117-239:/home/moriarty# chmod o-r Finance_script.sh_2.txt
root@ip-172-22-117-239:/home/moriarty# chmod o-r elementary.txt_1.txt
root@ip-172-22-117-239:/home/moriarty# chmod o-r game_is_afoot.txt_3.txt
root@ip-172-22-117-239:/home/moriarty# chmod o-rx game_is_afoot.txt_script1.sh
root@ip-172-22-117-239:/home/moriarty# chmod o-rx game_is_afoot.txt_script2.sh
root@ip-172-22-117-239:/home/moriarty# la -l
total 28
-rw-r--r-- 1 moriarty moriarty  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 moriarty moriarty 8163 Dec  3 22:12 .bashrc
-rw-r--r-- 1 moriarty moriarty  807 Mar 31  2024 .profile
-rw-r----- 1 moriarty moriarty    0 Oct 22 16:35 Finance_script.sh_0.txt
-rw-r----- 1 moriarty moriarty    0 Oct 22 16:35 Finance_script.sh_2.txt
-rw-r----- 1 moriarty moriarty    0 Oct 22 16:35 elementary.txt_1.txt
-rw-r----- 1 moriarty moriarty    0 Oct 22 16:35 game_is_afoot.txt_3.txt
-rwxr-x--- 1 moriarty moriarty   49 Oct 22 16:35 game_is_afoot.txt_script1.sh
-rwxr-x--- 1 moriarty moriarty   49 Oct 22 16:35 game_is_afoot.txt_script2.sh
-rw------- 1 moriarty moriarty   54 Oct 22 16:35 my_file.txt
root@ip-172-22-117-239:/home/moriarty# ls -l
total 12
-rw-r----- 1 moriarty moriarty  0 Oct 22 16:35 Finance_script.sh_0.txt
-rw-r----- 1 moriarty moriarty  0 Oct 22 16:35 Finance_script.sh_2.txt
-rw-r----- 1 moriarty moriarty  0 Oct 22 16:35 elementary.txt_1.txt
-rw-r----- 1 moriarty moriarty  0 Oct 22 16:35 game_is_afoot.txt_3.txt
-rwxr-x--- 1 moriarty moriarty 49 Oct 22 16:35 game_is_afoot.txt_script1.sh
-rwxr-x--- 1 moriarty moriarty 49 Oct 22 16:35 game_is_afoot.txt_script2.sh
-rw------- 1 moriarty moriarty 54 Oct 22 16:35 my_file.txt
root@ip-172-22-117-239:/home/moriarty#
```

(mycroft) Output:

```
root@ip-172-22-117-239:/home# cd mycroft
root@ip-172-22-117-239:/home/mycroft# ls -l
total 8
-rw-r--r-- 1 mycroft mycroft  0 Oct 22 16:35 Engineering_script.sh_0.txt
-rw-r--r-- 1 mycroft mycroft  0 Oct 22 16:35 Finance_script.sh_3.txt
-rwxr-xr-x 1 mycroft mycroft 48 Oct 22 16:35 Finance_script.sh_script1.sh
-rwxr-xr-x 1 mycroft mycroft 48 Oct 22 16:35 Finance_script.sh_script2.sh
-rw-r--r-- 1 mycroft mycroft  0 Oct 22 16:35 deduction.doc_1.txt
-rw-r--r-- 1 mycroft mycroft  0 Oct 22 16:35 deduction.doc_2.txt
root@ip-172-22-117-239:/home/mycroft# chmod o-r Engineering_script.sh_0.txt
root@ip-172-22-117-239:/home/mycroft# chmod o-r Finance_script.sh_3.txt
root@ip-172-22-117-239:/home/mycroft# chmod o-rx Finance_script.sh_script1.sh
root@ip-172-22-117-239:/home/mycroft# chmod o-rx Finance_script.sh_script2.sh
root@ip-172-22-117-239:/home/mycroft# chmod o-r deduction.doc_1.txt
root@ip-172-22-117-239:/home/mycroft# chmod o-r deduction.doc_2.txt
root@ip-172-22-117-239:/home/mycroft# ls -l
total 8
-rw-r----- 1 mycroft mycroft  0 Oct 22 16:35 Engineering_script.sh_0.txt
-rw-r----- 1 mycroft mycroft  0 Oct 22 16:35 Finance_script.sh_3.txt
-rwxr-x--- 1 mycroft mycroft 48 Oct 22 16:35 Finance_script.sh_script1.sh
-rwxr-x--- 1 mycroft mycroft 48 Oct 22 16:35 Finance_script.sh_script2.sh
-rw-r----- 1 mycroft mycroft  0 Oct 22 16:35 deduction.doc_1.txt
-rw-r----- 1 mycroft mycroft  0 Oct 22 16:35 deduction.doc_2.txt
```

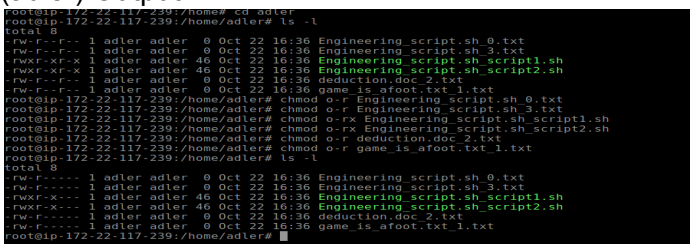
(mrs_hudson) Output:

```
root@ip-172-22-117-239:/home# cd mrs_hudson
root@ip-172-22-117-239:/home/mrs_hudson# ls -l
total 8
-rw-r--r-- 1 mrs_hudson mrs_hudson  0 Oct 22 16:35 Engineering_script.sh_1.txt
-rw-r--r-- 1 mrs_hudson mrs_hudson  0 Oct 22 16:35 deduction.doc_0.txt
-rw-r--r-- 1 mrs_hudson mrs_hudson  0 Oct 22 16:35 deduction.doc_2.txt
-rw-r--r-- 1 mrs_hudson mrs_hudson  0 Oct 22 16:35 elementary.txt_3.txt
-rwxr-xr-x 1 mrs_hudson mrs_hudson 51 Oct 22 16:35 elementary.txt_script1.sh
-rwxr-xr-x 1 mrs_hudson mrs_hudson 51 Oct 22 16:35 elementary.txt_script2.sh
root@ip-172-22-117-239:/home/mrs_hudson# chmod o-r Engineering_script.sh_1.txt
root@ip-172-22-117-239:/home/mrs_hudson# chmod o-r deduction.doc_0.txt
root@ip-172-22-117-239:/home/mrs_hudson# chmod o-r deduction.doc_2.txt
root@ip-172-22-117-239:/home/mrs_hudson# chmod o-r elementary.txt_3.txt
root@ip-172-22-117-239:/home/mrs_hudson# chmod o-rx elementary.txt_script1.sh
root@ip-172-22-117-239:/home/mrs_hudson# chmod o-rx elementary.txt_script2.sh
root@ip-172-22-117-239:/home/mrs_hudson# ls -l
total 8
-rw-r----- 1 mrs_hudson mrs_hudson  0 Oct 22 16:35 Engineering_script.sh_1.txt
-rw-r----- 1 mrs_hudson mrs_hudson  0 Oct 22 16:35 deduction.doc_0.txt
-rw-r----- 1 mrs_hudson mrs_hudson  0 Oct 22 16:35 deduction.doc_2.txt
-rw-r----- 1 mrs_hudson mrs_hudson  0 Oct 22 16:35 elementary.txt_3.txt
-rwxr-x--- 1 mrs_hudson mrs_hudson 51 Oct 22 16:35 elementary.txt_script1.sh
-rwxr-x--- 1 mrs_hudson mrs_hudson 51 Oct 22 16:35 elementary.txt_script2.sh
root@ip-172-22-117-239:/home/mrs_hudson#
```

(toby) Output:

```
root@ip-172-22-117-239:/home# cd toby
root@ip-172-22-117-239:/home/toby# ls -l
total 8
-rw-r--r-- 1 toby toby  0 Oct 22 16:36 Engineering_script.sh_2.txt
-rw-r--r-- 1 toby toby  0 Oct 22 16:36 deduction.doc_1.txt
-rw-r--r-- 1 toby toby  0 Oct 22 16:36 elementary.txt_0.txt
-rw-r--r-- 1 toby toby  0 Oct 22 16:36 elementary.txt_3.txt
-rwxr-xr-x 1 toby toby 45 Oct 22 16:36 elementary.txt_script1.sh
-rwxr-xr-x 1 toby toby 45 Oct 22 16:36 elementary.txt_script2.sh
root@ip-172-22-117-239:/home/toby# chmod o-r Engineering_script.sh_2.txt
root@ip-172-22-117-239:/home/toby# chmod o-r deduction.doc_1.txt
root@ip-172-22-117-239:/home/toby# chmod o-r elementary.txt_0.txt
root@ip-172-22-117-239:/home/toby# chmod o-r elementary.txt_3.txt
root@ip-172-22-117-239:/home/toby# chmod o-rx elementary.txt_script1.sh
root@ip-172-22-117-239:/home/toby# chmod o-rx elementary.txt_script2.sh
root@ip-172-22-117-239:/home/toby# ls -l
total 8
-rw-r----- 1 toby toby  0 Oct 22 16:36 Engineering_script.sh_2.txt
-rw-r----- 1 toby toby  0 Oct 22 16:36 deduction.doc_1.txt
-rw-r----- 1 toby toby  0 Oct 22 16:36 elementary.txt_0.txt
-rw-r----- 1 toby toby  0 Oct 22 16:36 elementary.txt_3.txt
-rwxr-x--- 1 toby toby 45 Oct 22 16:36 elementary.txt_script1.sh
-rwxr-x--- 1 toby toby 45 Oct 22 16:36 elementary.txt_script2.sh
root@ip-172-22-117-239:/home/toby#
```

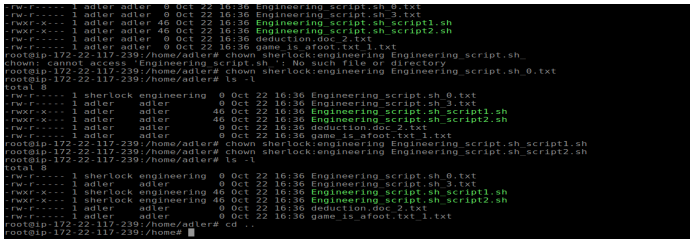
(adler) Output:



- (managing group scripts)

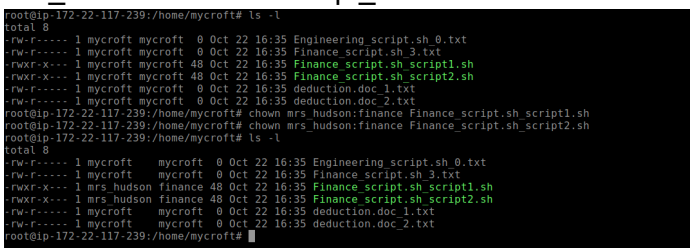
(engineering scripts) Command used:
chown sherlock:engineering <script_name>

Output:



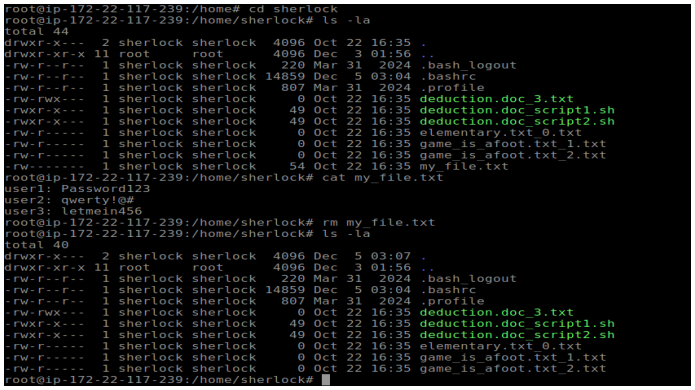
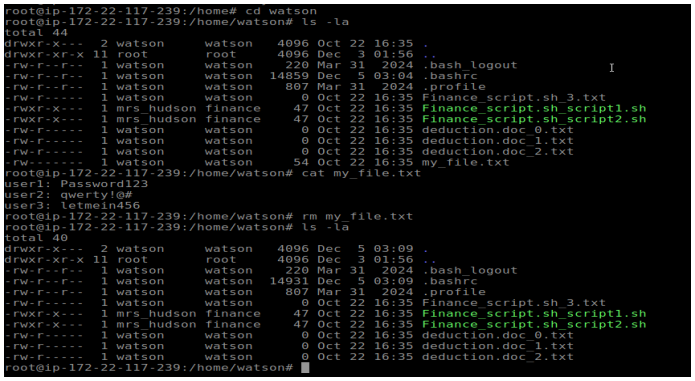
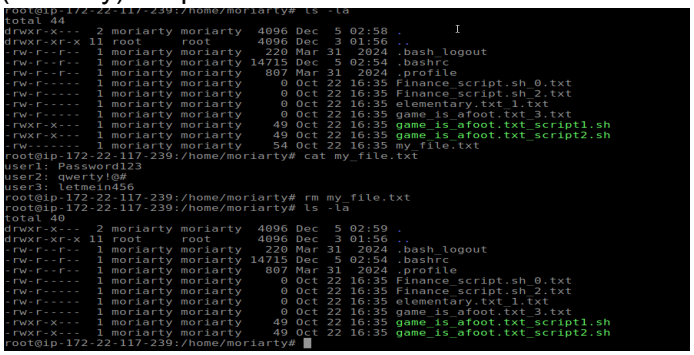
(research scripts) Command used: no research group scripts

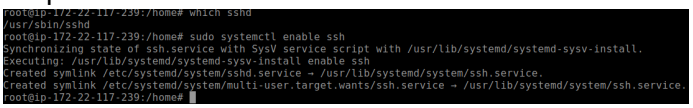
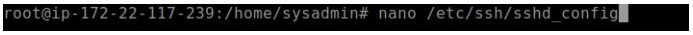
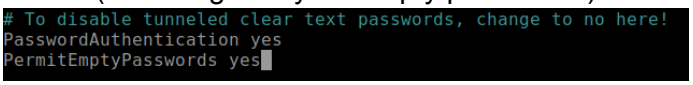
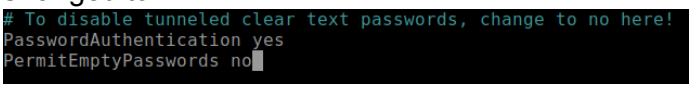
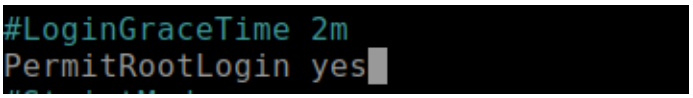
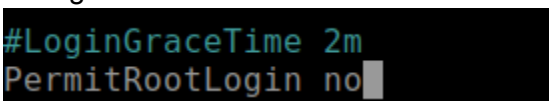
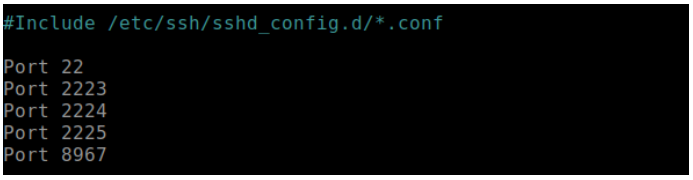
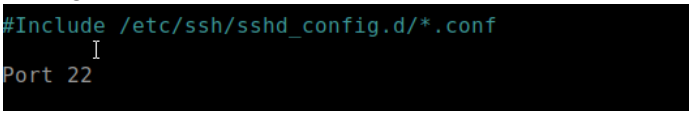
(finance scripts) Command used: chown mrs_hudson:finance <script_name>

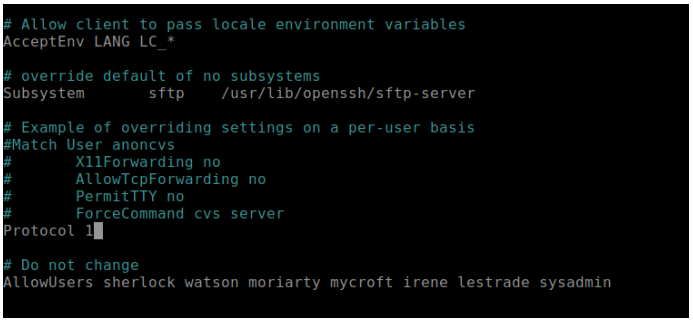
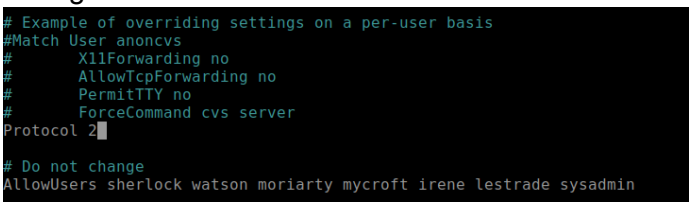
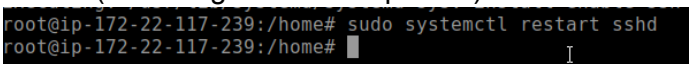
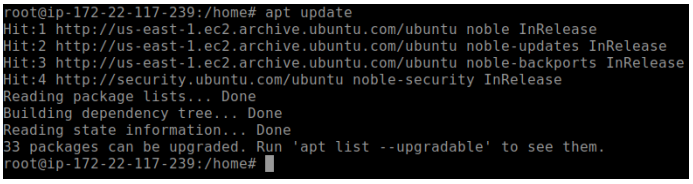
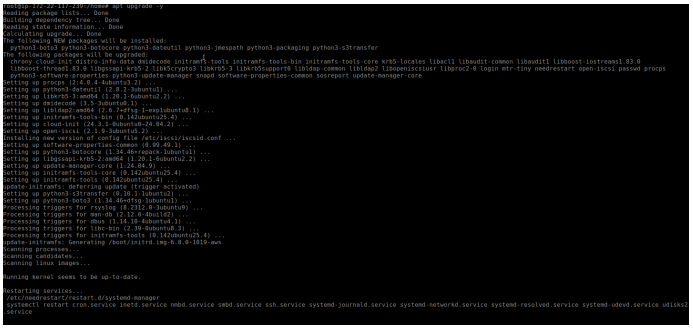


- (Removing hidden files from sherlock, moriarty, watson)

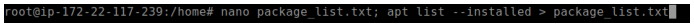
Command used: cd <user>, ls -la (displays all files including hidden files), rm <filename>
(sherlock) Output:

		 (watson) Output:  (moriarty) Output: 
☑	Optional: Updating password hashing configuration	n/a

☑	Auditing and securing SSH	• (enabling ssh) Command used:sudo systemctl enable ssh Output:  • (editing ssh file) Command used: nano /etc/ssh/sshd_config Output:  • (removing ability for empty passwords)  Changed to:  • (removing ability to ssh into root user)  Changed to:  • (removing ability to ssh with any port besides port 22)  Changed to:  • (enabling ssh protocol 2)

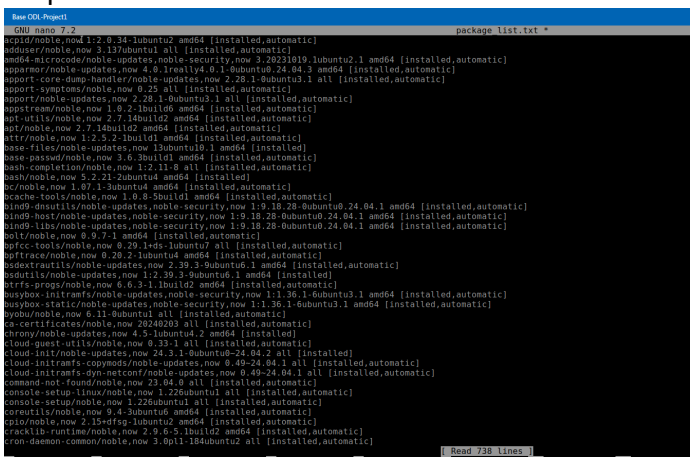
		 Changed to:  • (restarting ssh to set updates) 
☑	Reviewing and updating system packages	• (running apt update) Command used: apt update Output:  • (updating all installed packages) Command used: apt upgrade -y Output:   • (creating package_list.txt by dumping full list into the .txt file)

Command(s) used: nano package_list.txt; apt list --installed > package_list.txt
Output:

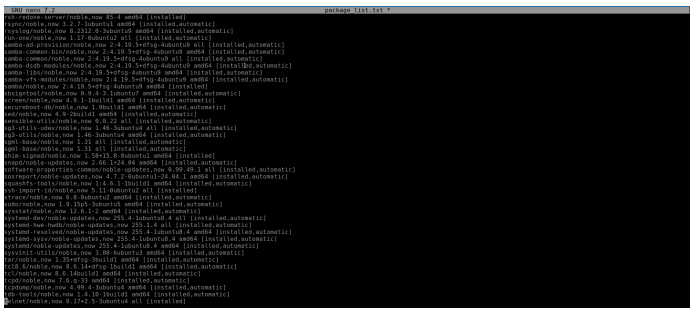


- (showing top and bottom of package_list.txt)

Command used: nano package_list.txt
Output:



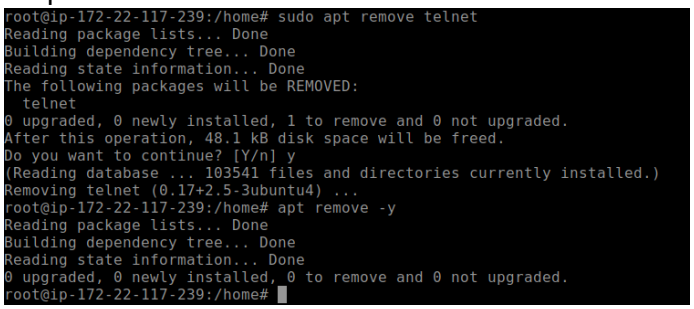
- (identifying telnet and rsh-client)



(rsh shown on top line, telnet shown on bottom line)

- (removing telnet)

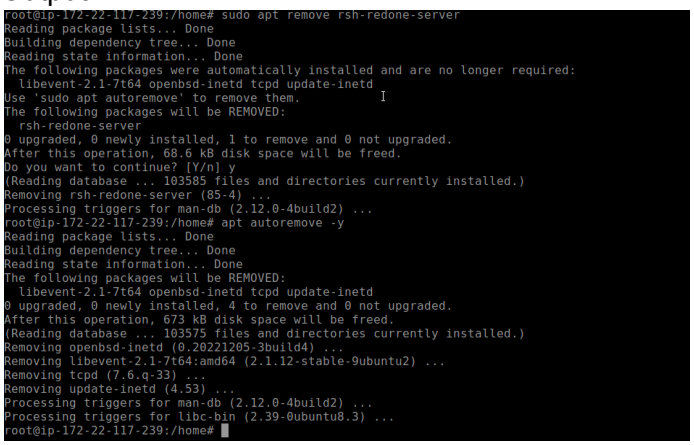
Command used: sudo apt remove telnet
Output:



(after review of the screenshot, i realized that i forgot to use “apt autoremove -y” but instead used “apt remove -y)

- (removing rsh-client and dependencies)

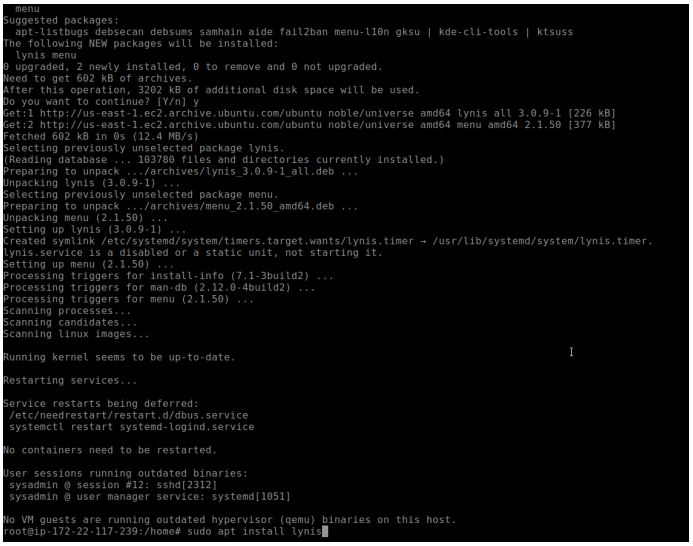
Command used:
sudo apt remove rsh-redone-server
apt auto remove -y
Output:

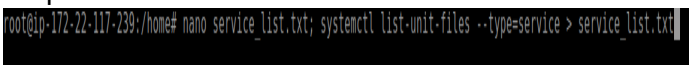


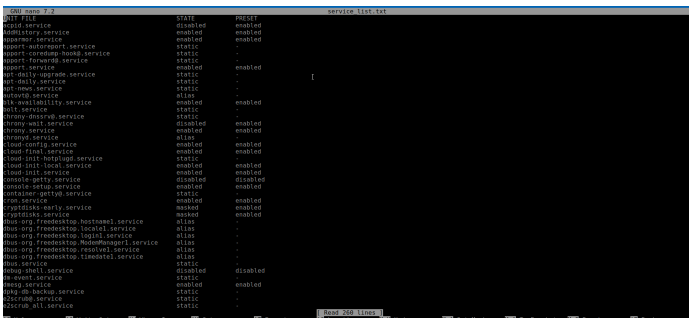
- (listing why “telnet” is a security risk)

Telnet: According to ssh.com, a telnet session

		between a server and client is not encrypted. With this, anyone with access to the TCP/IP packet flow between both endpoints can reconstruct the data to read plaintext messages along with the usernames and passwords that were used to log into the session. Along with this, the tools used for this network attack are readily available. (**Source:** https://www.ssh.com/academy/ssh/telnet#:~:text=The%20Telnet%20session%20between%20the,in%20to%20the%20remote%20machine.) ● (listing why rsh-client is a security risk) **RSH-Client**: According to ssh.com, the method of authentication used with RSH-client (dependent on .rhosts files and /etc/hosts.equiv) relied on IP addresses and DNS. With this release coming out during the 1980s, IP spoofing was easy if the attacker was on the local network and could even be done remotely. Ssh.com recommends to immediately disable RSH-Client. (**Source**: https://www.ssh.com/academy/ssh/rsh#:~:text=Security%20Issues%20in%20rsh,-rsh%20used%20.&text=rhosts%20files%20and%20%2Fetc%2Fhosts,could%20even%20be%20done%20remotely.) ● (installing ufw, lynis, tripwire) (ufw) Command used: sudo apt install ufw Output:  (lynis) Command used: sudo apt install lynis Output:

		 (sidenote: with how much was displayed during the installation, i was unable to show a full image of the command prior to the install as it was cut and I was unable to scroll to it. The command is shown at the bottom line.) (tripwire) Command used: sudo apt install tripwire Output:  (sidenote: similar with the lynis install, so much was shown that it cut out the portion where I can the command as well and the bottom. The popup that has you set a passphrase might have been the culprit.)  • (listing why tripwire, lynis, and ufw are beneficial to linux hardening) **Tripwire**: According to eaglepubs.erau.edu, Tripwire is a Host-based Intrusion Detection System that can monitor for unauthorized file and directory modification on local systems. It does so by recording aspects of a file such as its hash, timestamp of last modification, and permissions. These records are put into an encrypted database created by the Tripwire program and is used as a reference when cross-checking files for changes.

		(**Source**: https://eaglepubs.erau.edu/mastering-enterprise-networks-labs/chapter/intrusion-detection-tripwire/#:~:text=Tripwire%20is%20a%20Host%2Dbased%20Intrusion%20Detection%20System,baseline%20reference%20when%20cross%2Dchecking%20files%20for%20changes.) • (listing why Lynis is beneficial to linux hardening) **Lynis:** Directly from cisofy.com: Lynis is a battle-tested security tool for systems running Linux, macOS, or Unix-based operating system. It performs an extensive health scan of your systems to support system hardening and compliance testing. (**Source**: https://cisofy.com/lynis/#:~:text=Lynis%20is%20a%20battle%2Dtested,system%20hardening%20and%20compliance%20testing.) • (Listing why UFW is beneficial to linux hardening) **UFW**: According to swhosting.com: UFW allows users to configure firewall rules using simple terminal commands. This allows for easy implementation of basic security policies like allowing or denying traffic on specific ports or IP addresses. (**Source**: https://www.swhosting.com/en/blog/ufw-an-in-depth-look-at-linux-security#:~:text=UFW%20allows%20users%20to%20configure,certain%20ports%20or%20IP%20addresses.)
☑	Disabling unnecessary services	• (Command to list all services then dump its output into service_list.txt) Command used: nano service_list.txt; systemctl list-unit-files - -type=service > service_list.txt Output: 

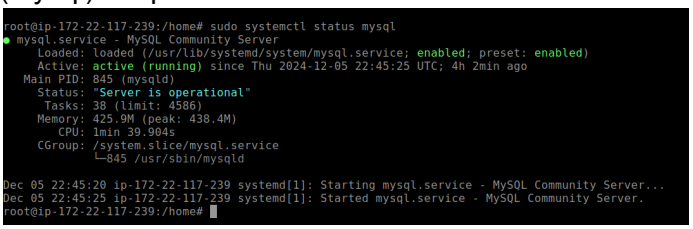


(this is just a portion of the service list, the list was extensive, so I am posting just one screenshot in an effort to reduce space)

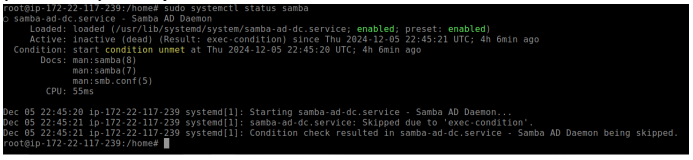
- (Identifying mysql and samba)

Command(s) used:
sudo systemctl status mysql
sudo systemctl status samba

(mysql) Output:



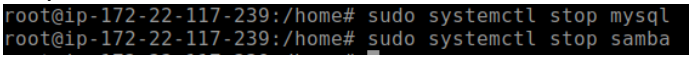
(samba) Output:



- (Stopping, Disabling, Removing mysql and samba)

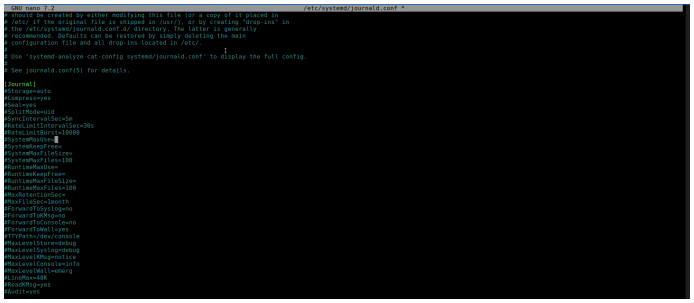
(Stopping) Commands used:
sudo systemctl stop mysql
sudo systemctl stop samba

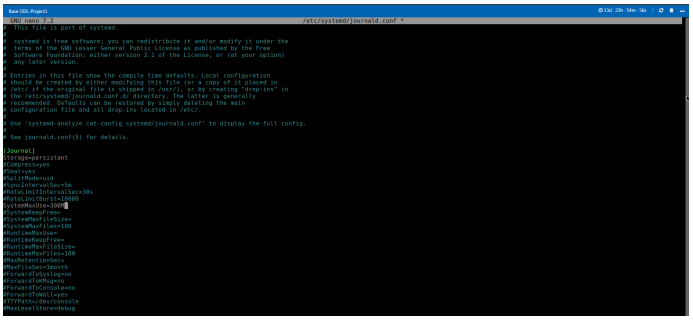
Output:



(Disabling) Commands used:
sudo systemctl disable mysql
sudo systemctl disable samba

		(samba) Output:
		`root@ip-172-22-117-239:/home# sudo systemctl disable samba`
		`Removed "/etc/systemd/system/samba.service".`
		`Removed "/etc/systemd/system/multi-user.target.wants/samba-ad-dc.service".`
		`root@ip-172-22-117-239:/home#`
		
		(mysql) Output:
		`root@ip-172-22-117-239:/home# sudo systemctl disable mysql`
		`mysql.service is not a native service, redirecting to systemd-sysv-install.`
		`Executing: /usr/lib/systemd/systemd-sysv-install disable mysql`
		
		(Removal) Commands used:
		sudo rm /lib/systemd/system/mysql.service
		sudo rm /lib/systemd/system/smbd.service
		
		Output:
		`root@ip-172-22-117-239:/home# sudo rm /lib/systemd/system/mysql.service`
		`root@ip-172-22-117-239:/home# sudo rm /lib/systemd/system/smbd.service`
		`root@ip-172-22-117-239:/home#`

☑	Enabling and configuring logging	• (displaying journald.conf) Command used: nano /etc/systemd/journald.conf Output:  • (making edits to journald.conf) Uncomment: #Storage=auto and #SystemMaxUse= Command(s) used: Storage=persistent SystemMaxUse=300M Output:

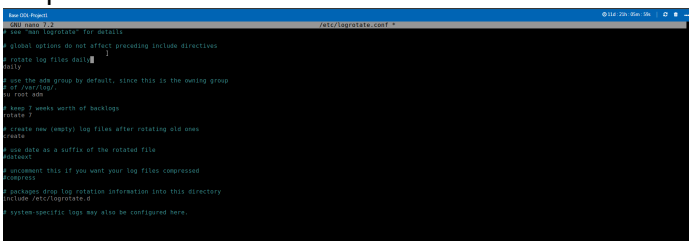


- (installing logrotate)

Command used: sudo apt install logrotate
Output:

- (displaying logrotate.conf)

Command used: nano /etc/logrotate.conf
Output:

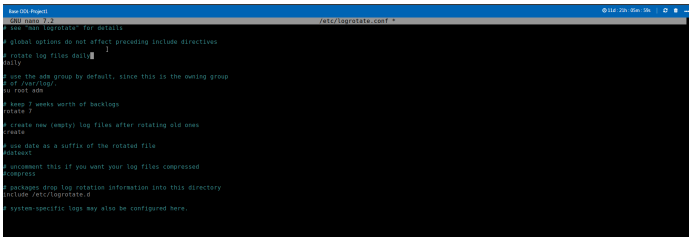


- (making edits to /etc/logrotate.conf)

Changed:
rotate log files daily from: daily
To: weekly

#keep 7 weeks worth of backlogs from: rotate 7
To: rotate 4

Output:



- (restarting journald)

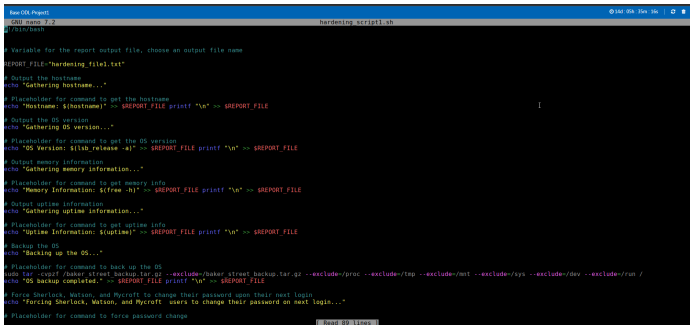
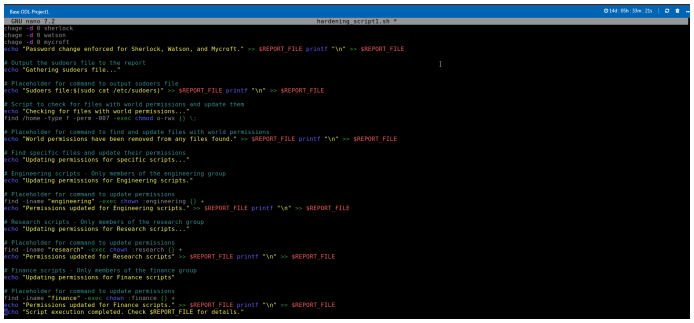
Command used: systemctl restart systemd-journald

		Output: `root@ip-172-22-117-239:/home# systemctl restart systemd-journald`

☑	Scripts created	• (hardening_script1.sh)
		
		Command used: nano hardening_script1.sh
		`root@ip-172-22-117-196:/home/sysadmin# nano hardening_script1.sh`
		
		Script:
		
		#!/bin/bash
		
		# Variable for the report output file, choose an output file name
		REPORT_FILE="hardening_file1.txt"
		
		# Output the hostname
		echo "Gathering hostname..."
		# Placeholder for command to get the hostname
		echo "Hostname: $(hostname)" >> $REPORT_FILE
		printf "\n" >> $REPORT_FILE
		
		# Output the OS version
		echo "Gathering OS version..."
		# Placeholder for command to get the OS version
		echo "OS Version: $(lsb_release -a)" >> $REPORT_FILE
		printf "\n" >> $REPORT_FILE
		
		# Output memory information
		echo "Gathering memory information..."
		# Placeholder for command to get memory info
		echo "Memory Information: $(free -h)" >> $REPORT_FILE
		printf "\n" >> $REPORT_FILE
		
		# Output uptime information
		echo "Gathering uptime information..."
		# Placeholder for command to get uptime info

		echo "Uptime Information: $(uptime)" >> $REPORT_FILE printf "\n" >> $REPORT_FILE # Backup the OS echo "Backing up the OS..." # Placeholder for command to back up the OS 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 / echo "OS backup completed." >> $REPORT_FILE printf "\n" >> $REPORT_FILE # Force Sherlock, Watson, and Mycroft to change their password upon their next login echo "Forcing Sherlock, Watson, and Mycroft users to change their password on next login..." # Placeholder for command to force password change chage -d 0 sherlock chage -d 0 watson chage -d 0 mycroft echo "Password change enforced for Sherlock, Watson, and Mycroft." >> $REPORT_FILE printf "\n" >> $REPORT_FILE # Output the sudoers file to the report echo "Gathering sudoers file..." # Placeholder for command to output sudoers file echo "Sudoers file:$(sudo cat /etc/sudoers)" >> $REPORT_FILE printf "\n" >> $REPORT_FILE

		# Script to check for files with world permissions and update them echo "Checking for files with world permissions..." find /home -type f -perm -007 -exec chmod o-rwx {} \; # Placeholder for command to find and update files with world permissions echo "World permissions have been removed from any files found." >> $REPORT_FILE printf "\n" >> $REPORT_FILE # Find specific files and update their permissions echo "Updating permissions for specific scripts..." # Engineering scripts - Only members of the engineering group echo "Updating permissions for Engineering scripts." # Placeholder for command to update permissions find -iname '*engineering*' -exec chown :engineering {} + echo "Permissions updated for Engineering scripts." >> $REPORT_FILE printf "\n" >> $REPORT_FILE # Research scripts - Only members of the research group echo "Updating permissions for Research scripts..." # Placeholder for command to update permissions find -iname “research” -exec chown :research {} + echo "Permissions updated for Research scripts" >> $REPORT_FILE

		printf "\n" >> $REPORT_FILE # Finance scripts - Only members of the finance group echo "Updating permissions for Finance scripts" # Placeholder for command to update permissions find -iname “finance” -exec chown :finance {} + echo "Permissions updated for Finance scripts." >> $REPORT_FILE printf "\n" >> $REPORT_FILE echo "Script execution completed. Check $REPORT_FILE for details." ● (end of hardening_script1.sh) Output:   ● (enabling execute on hardening_script1.sh) Command used: chmod +x hardening_script1.sh Output:

```
root@ip-172-22-117-196:/home/sysadmin# chmod +x hardening_script1.sh
root@ip-172-22-117-196:/home/sysadmin# ls -l
total 112
-rw-r--r-- 1 root root   2799 Dec 19 04:07 hardening_file1.txt
-rw-r--r-- 1 root root 100014 Dec 19 21:57 hardening_file2.txt
-rwxr-xr-x 1 root root   3253 Dec 19 22:02 hardening_script1.sh
-rwxr-xr-x 1 root root   1252 Dec 19 21:54 hardening_script2.sh
```

- (running hardening_script1.sh)

Command used: ./hardening_script1.sh
Output:

```
root@ip-172-22-117-196:/home/sysadmin# ./hardening_script1.sh
```

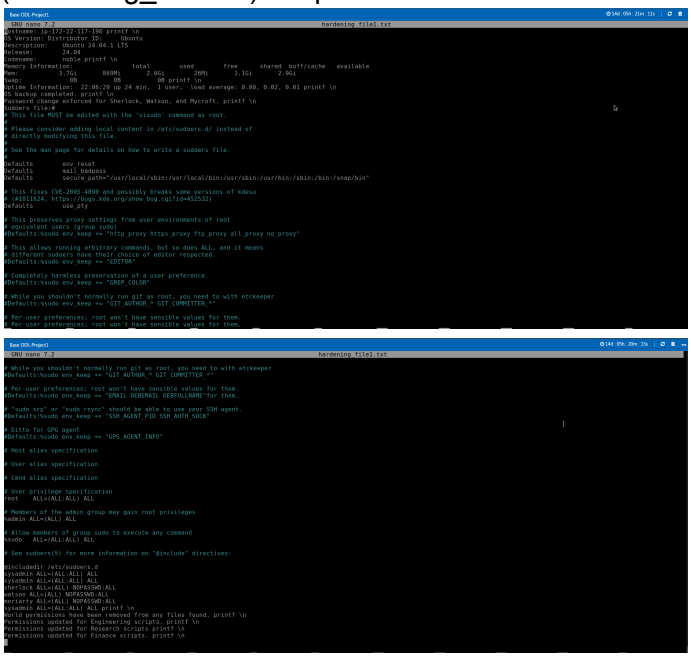
- (completion of hardening_script1.sh)

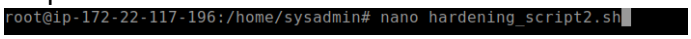
- (hardening_script1.sh output file -> hardening_file1.txt)

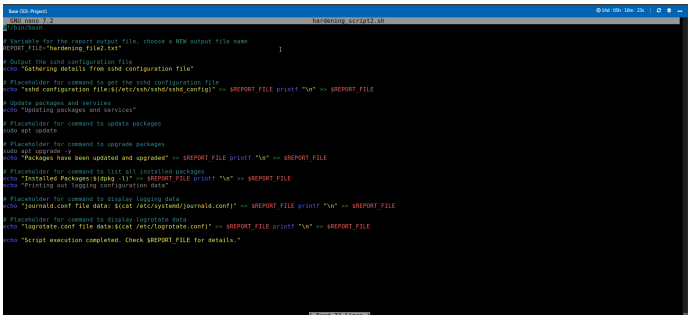
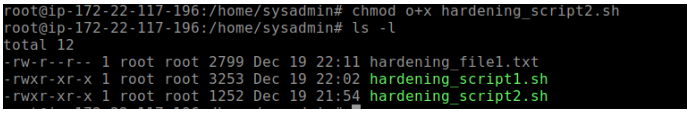
Command used:

```
root@ip-172-22-117-196:/home/sysadmin# ls -l
total 112
-rw-r--r-- 1 root root   2799 Dec 19 22:11 hardening_file1.txt
```

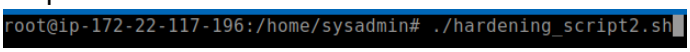
(hardening_file1.txt) Output:



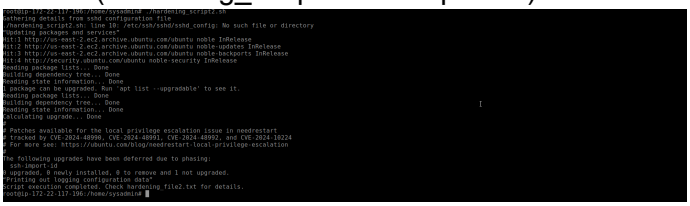
		• (hardening_script2.sh)
		
		Command used: nano hardening_script2.sh
		Output:
		 
		
		Script:
		
		#!/bin/bash
		
		# Variable for the report output file, choose a NEW output file name
		REPORT_FILE="hardening_file2.txt"
		
		# Output the sshd configuration file
		echo "Gathering details from sshd configuration file"
		# Placeholder for command to get the sshd configuration file
		
		echo "sshd configuration file:$(/etc/ssh/sshd/sshd_config)" >> $REPORT_FILE
		printf "\n" >> $REPORT_FILE
		
		# Update packages and services
		Echo “Updating packages and services”
		
		# Placeholder for command to update packages
		
		sudo apt update
		
		# Placeholder for command to upgrade packages
		
		sudo apt upgrade -y
		
		echo "Packages have been updated and upgraded" >> $REPORT_FILE printf "\n" >> $REPORT_FILE
		
		# Placeholder for command to list all installed packages

		echo "Installed Packages:$(dpkg -l)" >> $REPORT_FILE printf "\n" >> $REPORT_FILE echo “Printing out logging configuration data” # Placeholder for command to display logging data echo "journald.conf file data: $(cat /etc/systemd/journald.conf)" >> $REPORT_FILE printf "\n" >> $REPORT_FILE # Placeholder for command to display logrotate data echo "logrotate.conf file data:$(cat /etc/systemd/logrotate.conf)" >> $REPORT_FILE printf "\n" >> $REPORT_FILE echo "Script execution completed. Check $REPORT_FILE for details." (in nano) Output:  ● (enabling execute on hardening_script2.sh) Command used: chmod o+x hardening_script2.sh Output:  ● (running hardening_script2.sh)

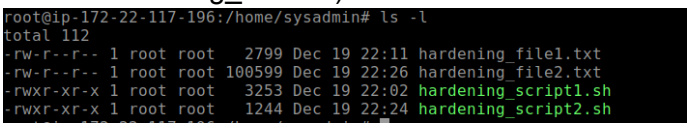
Command used: ./hardening_script2.sh
Output:



- (hardening_script2.sh completion)

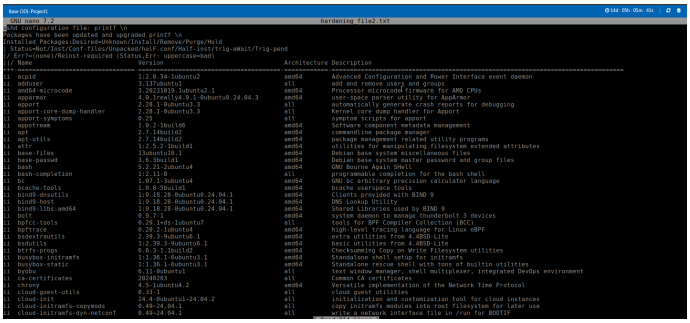


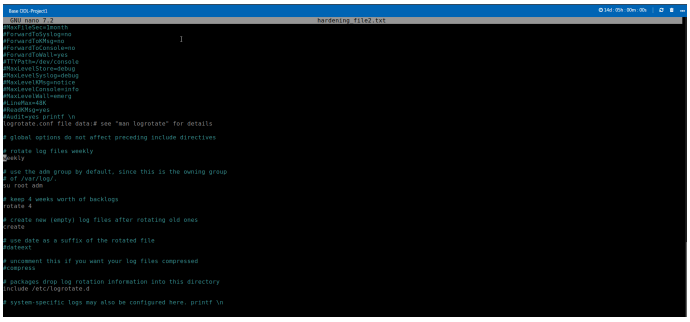
- (hardening_script2.sh output file -> hardening_file2.txt)



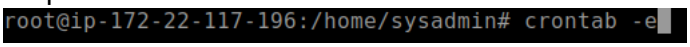
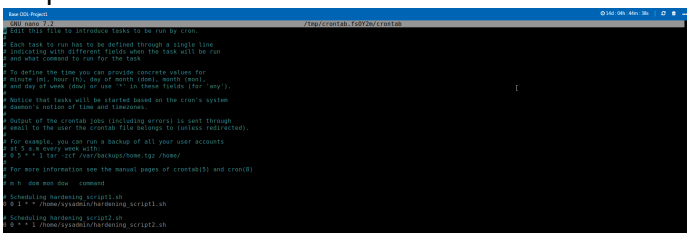
- (hardening_file2.txt)

Command used: nano hardening_file2.txt
Output:





(again, in an effort to save space, the screenshots above are the top and bottom screen of the output file)

☑	Scripts scheduled with cron	• (cron file) Command used: crontab -e Output:  • (editing cron file) Lines added: 0 0 1 * * /home/sysadmin/hardening_script1.sh 0 0 * * 1 /home/sysadmin/hardening_script2.sh Output:  • (veryfing cron schedule) Command used: crontab -l Output: