Cybersecurity

Project 1 Hardening Summary and Checklist

OS Information

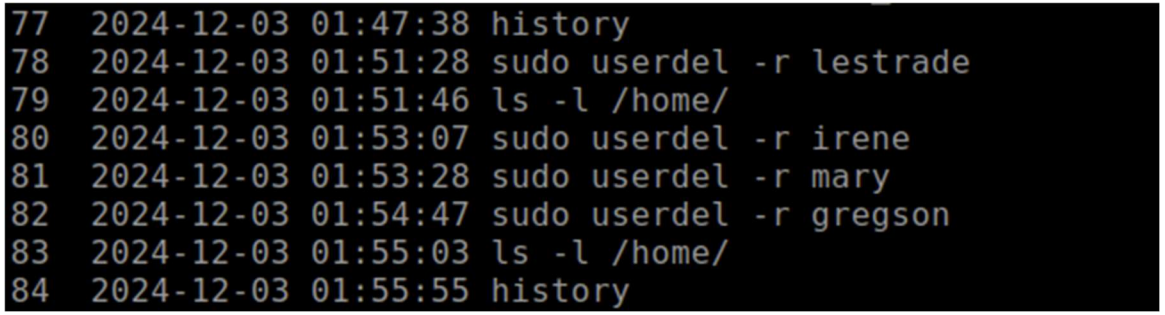
Customer	Baker Street Corporation
Hostname	ip-172-22-117-108 `root@ip-172-22-117-108:/home/sysadmin# hostname` `ip-172-22-117-108`
OS Version	Ubuntu 24.04.1 LTS (Noble Numbat) `root@ip-172-22-117-108:/home/sysadmin# cat /etc/os-release` `PRETTY_NAME="Ubuntu 24.04.1 LTS"` `NAME="Ubuntu"` `VERSION_ID="24.04"` `VERSION="24.04.1 LTS (Noble Numbat)"`
Memory information	`sysadmin@ip-172-22-117-108:~$ free -h` `total used free shared buff/cache available` `Mem: 914Mi 781Mi 114Mi 26Mi 191Mi 132Mi` `Swap: 0B 0B 0B`
Uptime information	`sysadmin@ip-172-22-117-108:~$ uptime` `01:04:28 up 21 min, 1 user, load average: 0.07, 0.03, 0.00`

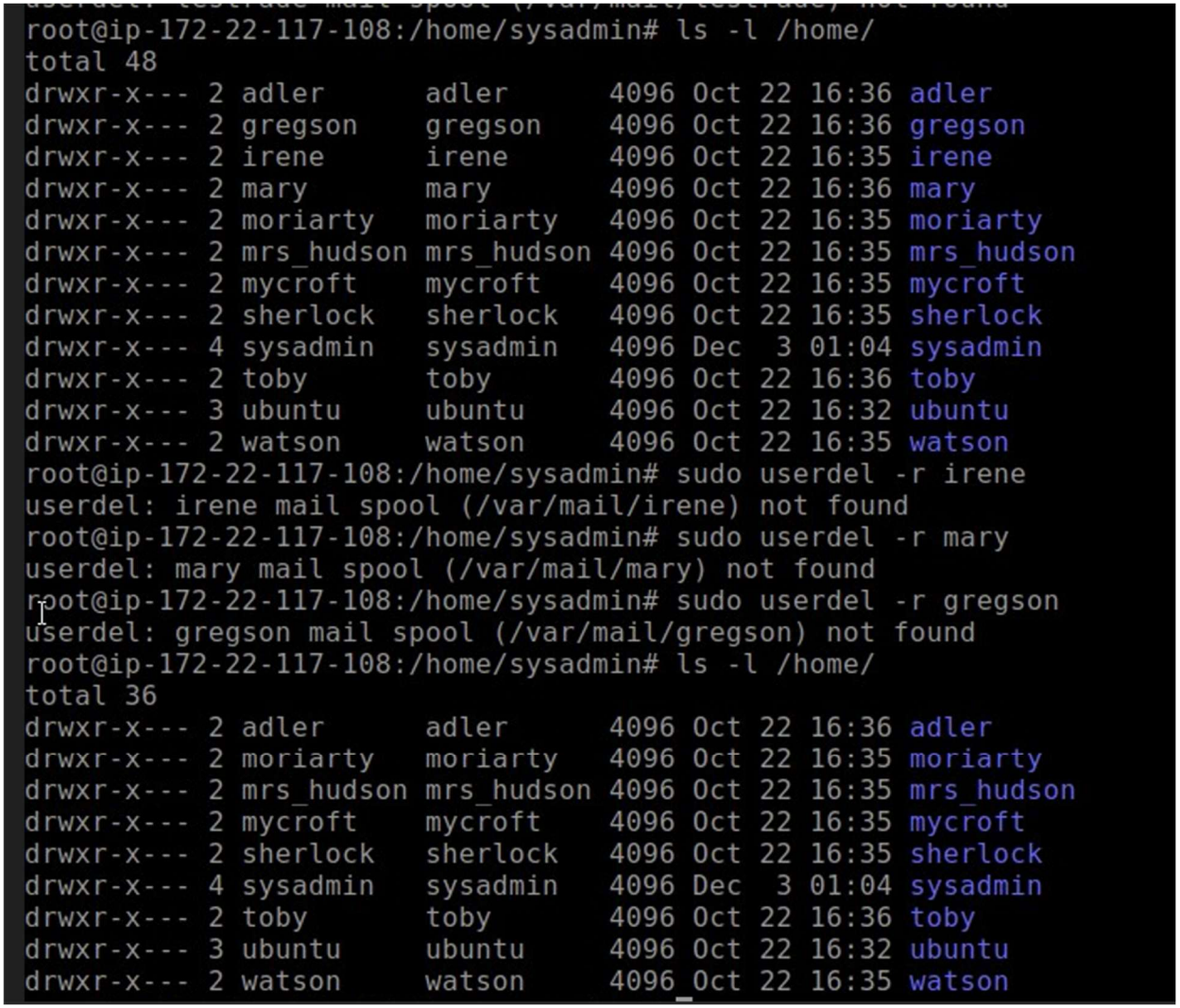
Checklist

Completed	Activity	Script(s) used / Tasks completed / Screenshots
●	OS backup	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 /

```
/etc/rc0.d/K01open-vm-tools
/etc/rc0.d/K01nmbd
/etc/rc0.d/K01mysql
/etc/rc0.d/K01cryptdisks
/etc/rc0.d/K01plymouth
/etc/rc0.d/K01openbsd-inetd
/etc/rc0.d/K01cryptdisks-early
/etc/rc0.d/K01smbd
/etc/rc0.d/K01irqbalance
/etc/rc0.d/K01chrony
/etc/rc0.d/K01samba-ad-dc
/etc/rc0.d/K01iscsid
/etc/vtrgb
/etc/subuid
/etc/gai.conf
/etc/cron.hourly/
/etc/cron.hourly/.placeholder
/etc/timezone
/etc/mtab
/etc/dpkg/
/etc/dpkg/dpkg.cfg.d/
/etc/dpkg/dpkg.cfg.d/needrestart
/etc/dpkg/origins/
/etc/dpkg/origins/ubuntu
/etc/dpkg/origins/default
/etc/dpkg/origins/debian
/etc/dpkg/dpkg.cfg
/etc/python3.12/
/etc/python3.12/sitecustomize.py
/etc/ld.so.conf
/etc/xattr.conf
root@ip-172-22-117-108:/home/sysadmin#
```

```
root@ip-172-22-117-108:/#
root@ip-172-22-117-108:/# ls -l
total 1533892
-rw-r--r--   1 root root       2746 Dec  6 02:49 Monthly_Report
-rw-r--r--   1 root root       2746 Dec  6 02:54 Monthly_Report.txt
-rw-r--r--   1 root root     113186 Dec  6 02:58 Weekly_Report.txt
-rw-r--r--   1 root root 1570480507 Dec  3 01:31 baker_street_backup.tar.gz
lrwxrwxrwx   1 root root          7 Apr 22  2024 bin -> usr/bin
```

•	Auditing users and groups	a. Remove all terminated users including their home directories and files: *ls -l /home* *sudo userdel -r lestrade* *sudo userdel -r irene* *sudo userdel -r mary* *sudo userdel -r gregson*  77 2024-12-03 01:47:38 history 78 2024-12-03 01:51:28 sudo userdel -r lestrade 79 2024-12-03 01:51:46 ls -l /home/ 80 2024-12-03 01:53:07 sudo userdel -r irene 81 2024-12-03 01:53:28 sudo userdel -r mary 82 2024-12-03 01:54:47 sudo userdel -r gregson 83 2024-12-03 01:55:03 ls -l /home/ 84 2024-12-03 01:55:55 history


root@ip-172-22-117-108:/home/sysadmin# ls -l /home/
total 48
drwxr-x--- 2 adler adler 4096 Oct 22 16:36 adler
drwxr-x--- 2 gregson gregson 4096 Oct 22 16:36 gregson
drwxr-x--- 2 irene irene 4096 Oct 22 16:35 irene
drwxr-x--- 2 mary mary 4096 Oct 22 16:36 mary
drwxr-x--- 2 moriarty moriarty 4096 Oct 22 16:35 moriarty
drwxr-x--- 2 mrs_hudson mrs_hudson 4096 Oct 22 16:35 mrs_hudson
drwxr-x--- 2 mycroft mycroft 4096 Oct 22 16:35 mycroft
drwxr-x--- 2 sherlock sherlock 4096 Oct 22 16:35 sherlock
drwxr-x--- 4 sysadmin sysadmin 4096 Dec 3 01:04 sysadmin
drwxr-x--- 2 toby toby 4096 Oct 22 16:36 toby
drwxr-x--- 3 ubuntu ubuntu 4096 Oct 22 16:32 ubuntu
drwxr-x--- 2 watson watson 4096 Oct 22 16:35 watson
root@ip-172-22-117-108:/home/sysadmin# sudo userdel -r irene
userdel: irene mail spool (/var/mail/irene) not found
root@ip-172-22-117-108:/home/sysadmin# sudo userdel -r mary
userdel: mary mail spool (/var/mail/mary) not found
root@ip-172-22-117-108:/home/sysadmin# sudo userdel -r gregson
userdel: gregson mail spool (/var/mail/gregson) not found
root@ip-172-22-117-108:/home/sysadmin# ls -l /home/
total 36
drwxr-x--- 2 adler adler 4096 Oct 22 16:36 adler
drwxr-x--- 2 moriarty moriarty 4096 Oct 22 16:35 moriarty
drwxr-x--- 2 mrs_hudson mrs_hudson 4096 Oct 22 16:35 mrs_hudson
drwxr-x--- 2 mycroft mycroft 4096 Oct 22 16:35 mycroft
drwxr-x--- 2 sherlock sherlock 4096 Oct 22 16:35 sherlock
drwxr-x--- 4 sysadmin sysadmin 4096 Dec 3 01:04 sysadmin
drwxr-x--- 2 toby toby 4096 Oct 22 16:36 toby
drwxr-x--- 3 ubuntu ubuntu 4096 Oct 22 16:32 ubuntu
drwxr-x--- 2 watson watson 4096 Oct 22 16:35 watson

Confirming terminated users, their home directories and files have been removed:
ls -l /home
id irene mary lestrade gregson

```
root@ip-172-22-117-108:/home/sysadmin# id irene mary lestrade gregson
id: ‘irene’: no such user
id: ‘mary’: no such user
id: ‘lestrade’: no such user
id: ‘gregson’: no such user
root@ip-172-22-117-108:/home/sysadmin#
```

b. Lock all user accounts of staff on temporary leave
sudo usermod -L moriarty
sudo usermod -L mrs_hudson

```
root@ip-172-22-117-108:/home/sysadmin# sudo usermod -L moriarty
root@ip-172-22-117-108:/home/sysadmin# sudo usermod -L mrs_hudson
root@ip-172-22-117-108:/home/sysadmin#
```

c. Unlock any users that are employed
Confirming status of the user accounts:
sudo passwd -S sherlock
sudo passwd -S watson
sudo passwd -S mycroft
sudo passwd -S toby
sudo passwd -S adler

```
root@ip-172-22-117-108:/home/sysadmin# sudo passwd -S sherlock && watson
sherlock P 2024-10-22 0 99999 7 -1
watson: command not found
root@ip-172-22-117-108:/home/sysadmin# sudo passwd -S watson
watson P 2024-10-22 0 99999 7 -1
root@ip-172-22-117-108:/home/sysadmin# sudo passwd -S mycroft
mycroft P 2024-10-22 0 99999 7 -1
root@ip-172-22-117-108:/home/sysadmin# sudo passwd -S toby
toby L 2024-10-22 0 99999 7 -1
root@ip-172-22-117-108:/home/sysadmin# sudo passwd -S adler
adler L 2024-10-22 0 99999 7 -1
root@ip-172-22-117-108:/home/sysadmin#
```

Change user's password to unlock them:

usermod -p password toby
usermod -p password adler

```
 103  2024-12-03 02:16:21 root@ip-172-22-117-108:/home/sysadmin# sudo usermod -U toby
 104  2024-12-03 02:16:21 usermod: unlocking the user's password would result in a passwordless account.
You should set a password with usermod -p to unlock this user's password.
 105  2024-12-03 02:16:22 root@ip-172-22-117-108:/home/sysadmin# usermod -p password toby
 106  2024-12-03 02:16:22 root@ip-172-22-117-108:/home/sysadmin# usermod -p password adler
 107  2024-12-03 02:16:22 root@ip-172-22-117-108:/home/sysadmin# sudo usermod -U toby
 108  2024-12-03 02:16:32 root@ip-172-22-117-108:/home/sysadmin# sudo usermod -U adler
 109  2024-12-03 02:16:41 root@ip-172-22-117-108:/home/sysadmin# sudo usermod -U toby
 110  2024-12-03 02:16:41 usermod: unlocking the user's password would result in a passwordless account.
You should set a password with usermod -p to unlock this user's password.
 111  2024-12-03 02:16:41 root@ip-172-22-117-108:/home/sysadmin# usermod -p password toby
 112  2024-12-03 02:16:41 root@ip-172-22-117-108:/home/sysadmin# usermod -p password adler
 113  2024-12-03 02:16:41 root@ip-172-22-117-108:/home/sysadmin# sudo usermod -U toby
```

sudo usermod -S toby
sudo usermod -S adler

```
 105  2024-12-03 02:16:22 root@ip-172-22-117-108:/home/sysadmin# usermod -p password toby
 106  2024-12-03 02:16:22 root@ip-172-22-117-108:/home/sysadmin# usermod -p password adler
 107  2024-12-03 02:16:22 root@ip-172-22-117-108:/home/sysadmin# sudo usermod -U toby
 108  2024-12-03 02:16:32 root@ip-172-22-117-108:/home/sysadmin# sudo usermod -U adler
```

d. Move employees from marketing department to new group research
Confirming members of groups for the employees:

tail -15 /etc/group

```
117  2024-12-03 02:19:18 group
118  2024-12-03 02:20:42 cat /etc/group
119  2024-12-03 02:24:41 sudo addgroup research
120  2024-12-03 02:25:11 tail /etc/group
121  2024-12-03 02:25:31 tail -15 /etc/group
```

Create new group research:

sudo addgroup research

```
 119  2024-12-03 02:24:41 sudo addgroup research
 120  2024-12-03 02:25:11 tail /etc/group
 121  2024-12-03 02:25:31 tail -15 /etc/group
```

Add user mycroft to research group and remove user from marketing group:

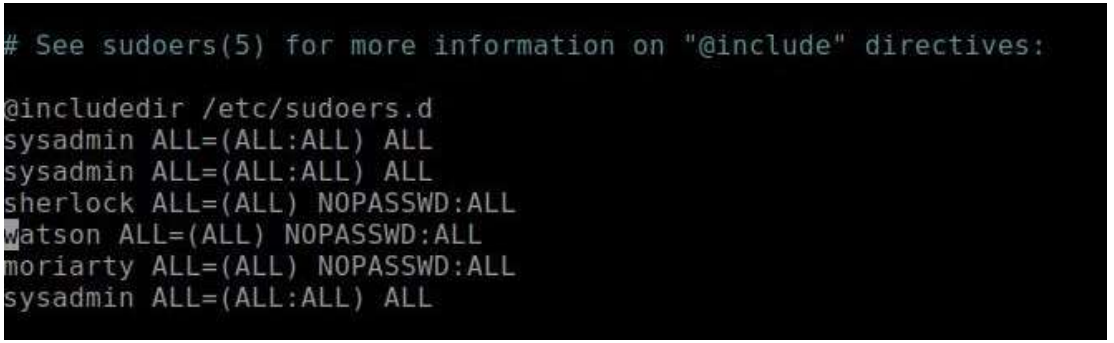
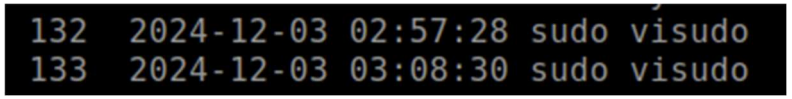
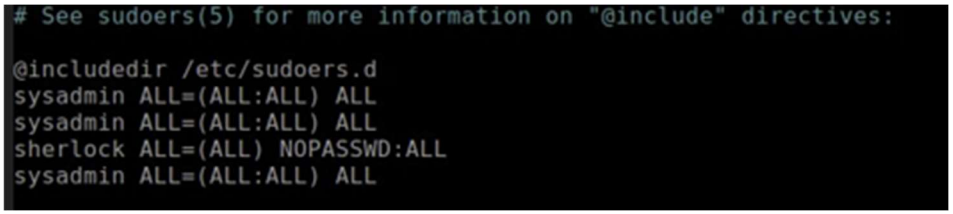
```
sudo usermod -G marketing mycroft
sudo usermod -aG research mycroft
```

```
 121  2024-12-03 02:25:31 tail -15 /etc/group
 122  2024-12-03 02:27:43 sudo usermod -aG research mycroft
 123  2024-12-03 02:28:02 tail -15 /etc/group
```

```
sudo deluser mycroft marketing
```

```
123  2024-12-03 02:28:02 tail -15 /etc/group
124  2024-12-03 02:30:33 sudo deluser mycroft marketing
125  2024-12-03 02:31:42 tail -15 /etc/group
```

		e. Remove marketing group *sudo delgroup marketing* `125 2024-12-03 02:31:42 tail -15 /etc/group` `126 2024-12-03 02:32:08 sudo delgroup marketing` `127 2024-12-03 02:32:16 tail -15 /etc/group`
•	Updating and enforcing password policies	*sudo nano /etc/pam.d/common-password* `128 2024-12-03 02:36:01 sudo nano /etc/pam.d/common-password` `129 2024-12-03 02:44:59 sudo nano /etc/pam.d/common-password` `# here are the per-package modules (the "Primary" block)` `password [success=1 default=ignore] pam_unix.so obscure yescrypt` `password requisite pam_pwquality.so minlen=8 ocredit=-1 retry=2 ucredit=-1` `password required pam_unix.so` `# here's the fallback if no module succeeds` *cat /etc/shadow* `chrony:!:19993:::::` `ubuntu:!:20018:0:99999:7:::` `sysadmin:$y$j9T$y5SnyiKCr6hWMsrZx999c/$WtLVqOXjHyejw/YD3rnaOwrrvkn0Q4fwDcfxWvj9wsB:20018:0:99999:7:::` `sherlock:$y$j9T$.hQtR8196elfFRva.Zq911$nSTABLizRMcz/Ge.WyAZ4ksUA7v7LchfXsd48EveDJ.:20018:0:99999:7:::` `watson:$y$j9T$lXq4xg3OCPuFFv9ZWjug8/$CoTk253eWAaE/7ChaPiBm9gqoLJl4yAgJJz15tzN.U.:20018:0:99999:7:::` `moriarty:!$y$j9T$8xH.cxMRyMYWUfmFfQ681.$BXMmzQWrcVdVDxJhbJjnA1kbtMw980XtJb9YazuAhC9:20018:0:99999:7:::` `mycroft:$y$j9T$FGTw.R.lTUqxnEu31T///.$NAK6Z/d/C0shBifS2qUKdtTl/RAftEjHLTGCOm6p000:20018:0:99999:7:::` `mrs_hudson:!:20018:0:99999:7:::` `toby:password:20060:0:99999:7:::` `adler:$6$Vllvd8FlgJUcRlIU$KPr4lw1R0ItBUXpapCSDV0mFNmXbELkEVRARHgAGMrSmk8NaH9VWSQbLFR5SGVwBzfweWdhMRUpBe3GKGgrm21:20061:0:99999:7:::` `mysql:!:20018:::::` `root@ip-172-22-117-108:/home/sysadmin#` Password changed but unable to switch user to confirm policy being enforced.

•	Updating and enforcing sudo permissions	1. Full sudo privileges to Sherlock only: Check sudoers file: *cat /etc/sudoers*  *sudo visudo*  Leave only Sherlock with full sudo privileges: *sherlock ALL=(ALL) NOPASSWD:ALL* 

2. Grant watson and Mycroft sudo privileges to run below script:

watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh

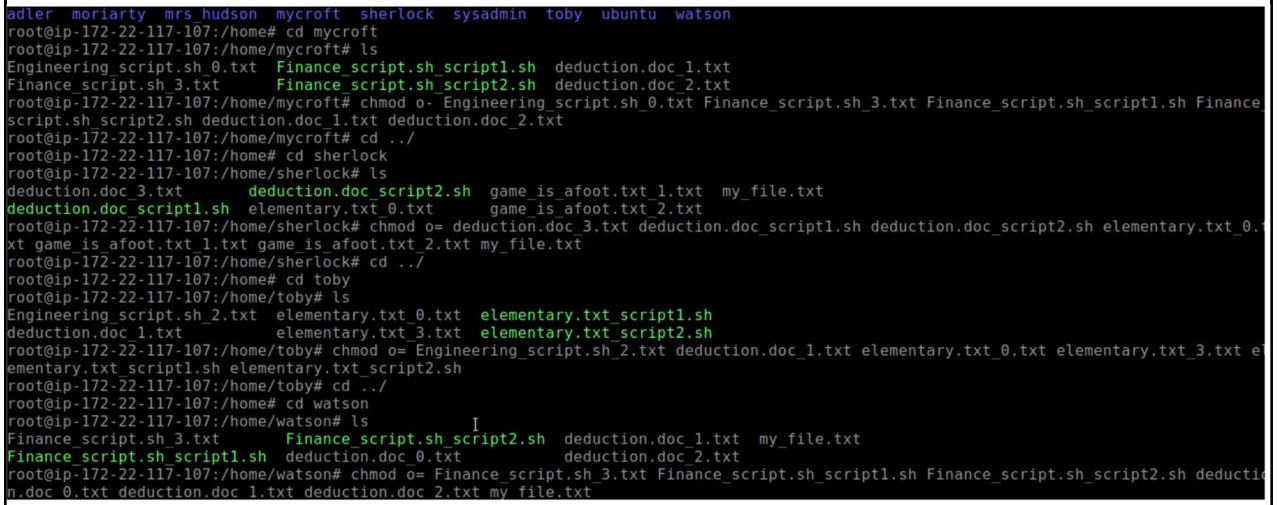
mycroft ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh

```
# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
sysadmin ALL=(ALL:ALL) ALL
sysadmin ALL=(ALL:ALL) ALL
sherlock ALL=(ALL) NOPASSWD:ALL
sysadmin ALL=(ALL:ALL) ALL
watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh
mycroft ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh
mycroft ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh
```

3. Grant all employees in research group sudo privileges to run the below script:

mycroft ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh

```
# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
sysadmin ALL=(ALL:ALL) ALL
sysadmin ALL=(ALL:ALL) ALL
sherlock ALL=(ALL) NOPASSWD:ALL
sysadmin ALL=(ALL:ALL) ALL
watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh
mycroft ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh
mycroft ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh
```

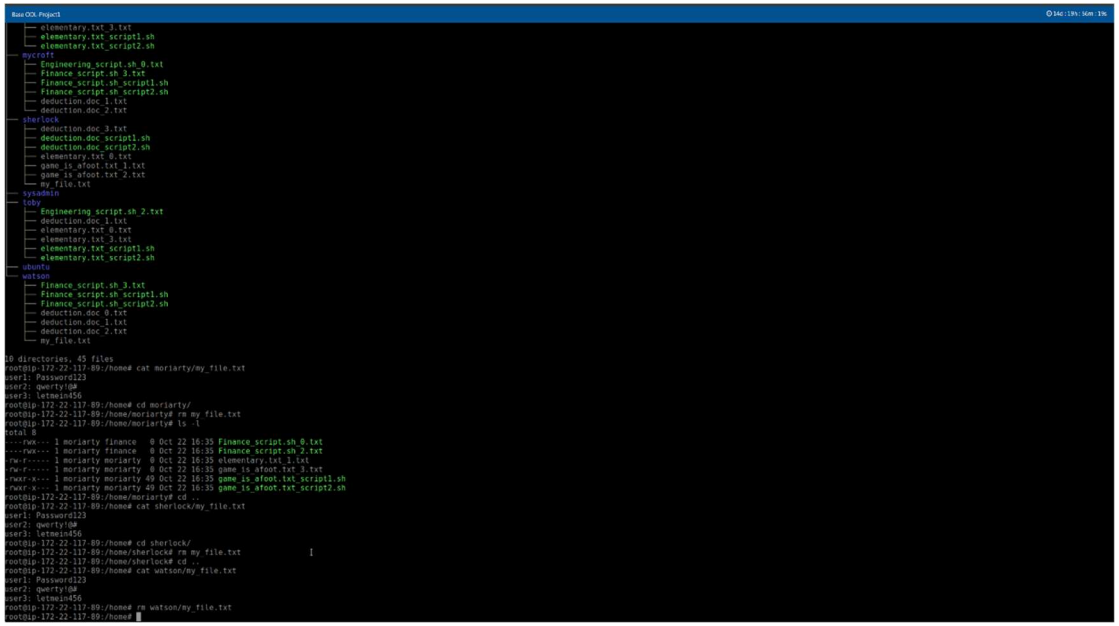
•	Validating and updating permissions on files and directories	1. *find -perm /o+rwx -exec chmod o-rwx {} +*  2. a. finds all script files and text files, that could be scripts and changes perms to only group can rwx *find /home -type f -iname *"Engineering"*"sh"	xargs chmod 070* Changing group ownership of the files to engineering *find /home -type f -iname *"Engineering"*"sh"	xargs chown :engineering* b. Finding files for research *find /home -type f -iname *"Research"*"sh"	xargs chmod 070* Changing group ownership: *find /home -type f -iname *"* Research*"*"sh"	xargs chown* :Research c. Finding files for finance

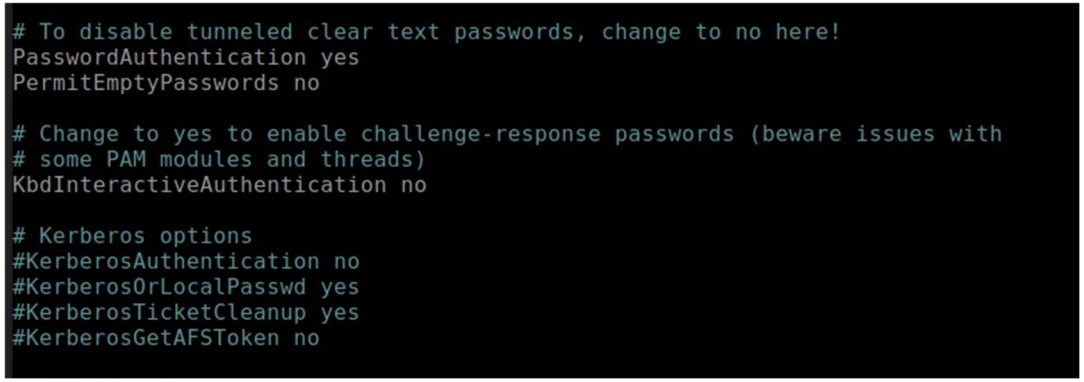
*find /home -type f -iname *"Finance"*"sh" | xargs chmod 070*

Changing ownership
*find /home -type f -iname *"Finance"*"sh" | xargs chown :finance*

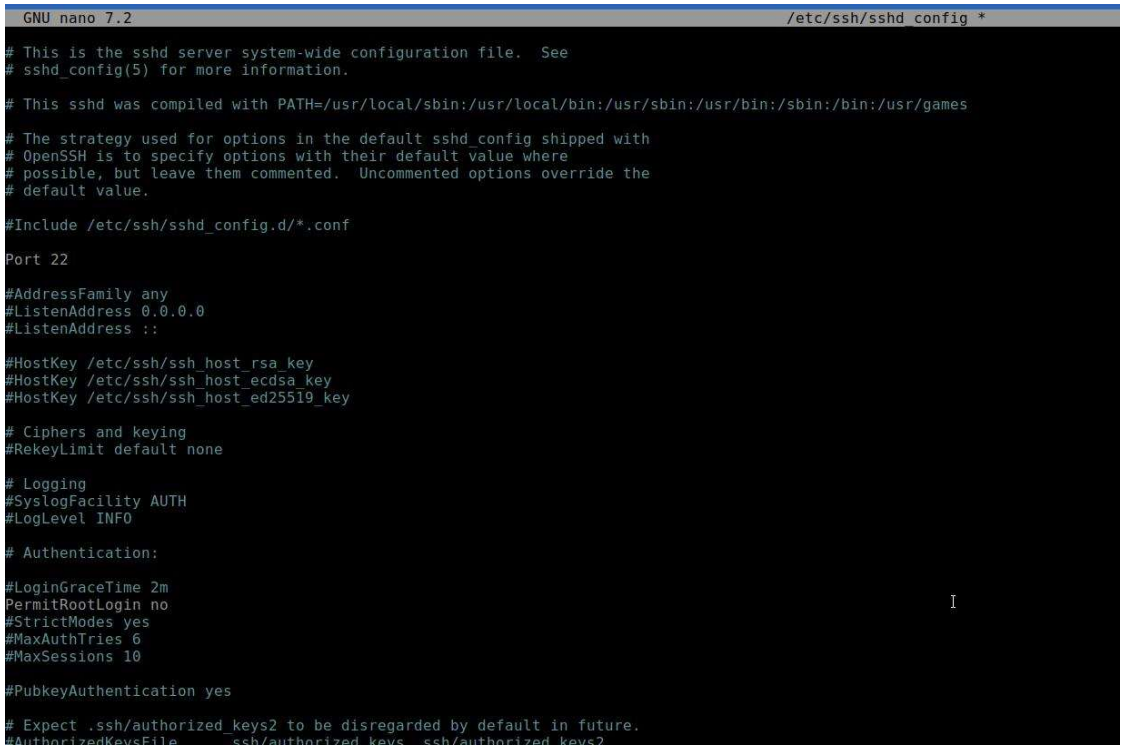
```
   89  2024-12-03 04:02:52 history
   90  2024-12-04 00:48:49 find /home -type f -iname *"Engineering"*"sh" | xargs chmod 070
   91  2024-12-04 00:50:42 find /home -type f -iname *"Engineering"*"sh" | xargs chown :engineers
   92  2024-12-04 00:51:02 find /home -type f -iname *"Engineering"*"sh" | xargs chown :Engineers
   93  2024-12-04 00:51:28 groups
   94  2024-12-04 00:52:27 find /home -type f -iname *"Engineering"*"sh" | xargs chown :engineering
   95  2024-12-04 00:54:40 find /home -type f -iname *"Research"*"sh" | xargs chmod 070
   96  2024-12-04 01:00:43 find /home -type f -iname *"Research"*"sh" | xargs chown :finance
   97  2024-12-04 01:01:19 find /home -type f -iname *"Research"*"sh" | xargs chown :research
   98  2024-12-04 01:04:14 find /home -type f -iname *"Research"*"sh"
   99  2024-12-04 01:04:59 ..\
  100  2024-12-04 01:06:10 history
root@ip-172-22-117-107:/home/sysadmin# find /home -type f -iname *"Finance"*"sh"
/home/watson/Finance_script.sh_script2.sh
/home/watson/Finance_script.sh_script1.sh
/home/mycroft/Finance_script.sh_script2.sh
/home/mycroft/Finance_script.sh_script1.sh
root@ip-172-22-117-107:/home/sysadmin# find /home -type f -iname *"Finance"*"sh" | xargs chmod 070
root@ip-172-22-117-107:/home/sysadmin# find /home -type f -iname *"Finance"*"sh" | xargs chown :Finance
chown: invalid group: ':Finance'
root@ip-172-22-117-107:/home/sysadmin# find /home -type f -iname *"Finance"*"sh" | xargs chown :finance
root@ip-172-22-117-107:/home/sysadmin# find /home -type f -iname *"Engineering"*"sh"
/home/adler/Engineering_script.sh_script2.sh
/home/adler/Engineering_script.sh_script1.sh
root@ip-172-22-117-107:/home/sysadmin# find /home -type f -iname *"Research"*"sh"
root@ip-172-22-117-107:/home/sysadmin#
```

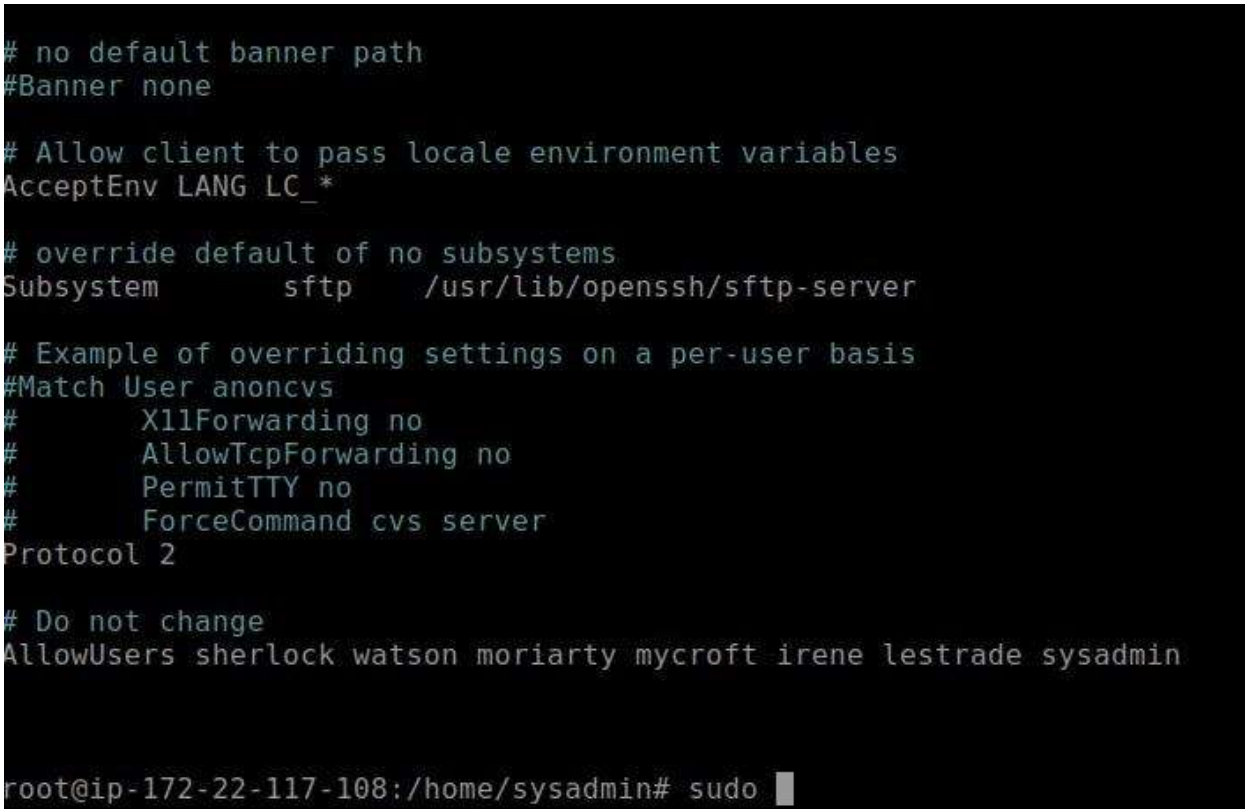
3. Look for .txt files with passwords then delete them:
   Ran tree to look for the files then deleted them:

		
•	Optional: Updating password hashing configuration	Edit PAM Password Settings: *sudo nano /etc/pam.d/common-password* *password required pam_unix.so sha512 remember=5*

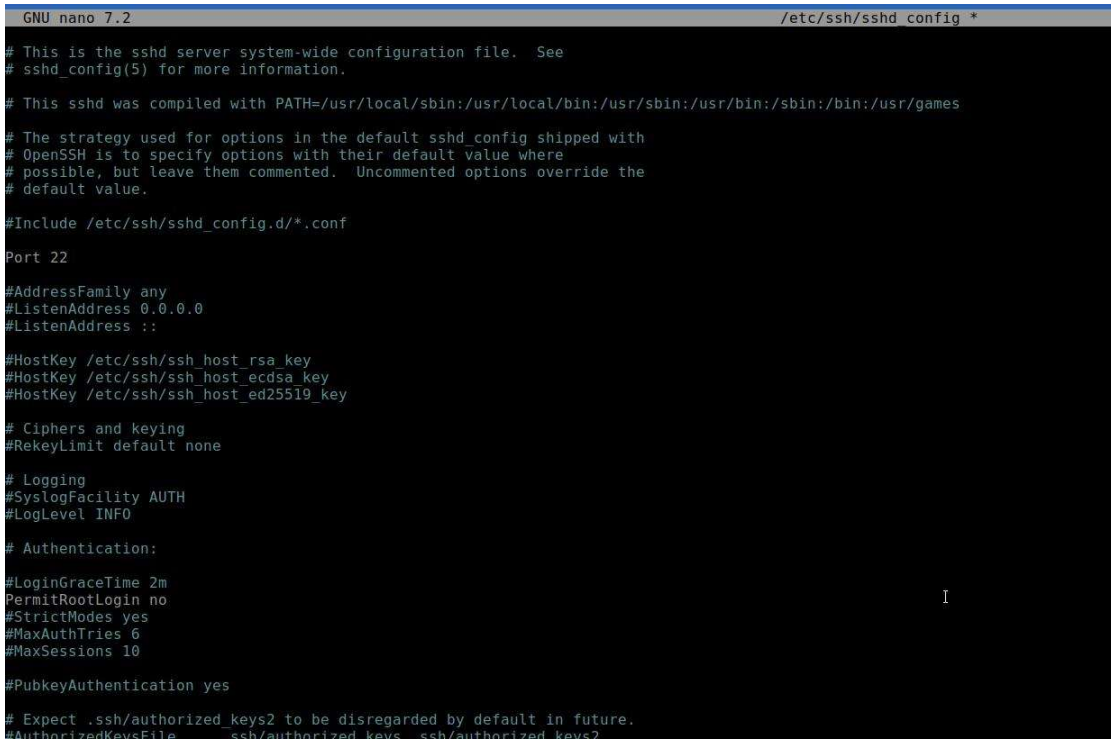
•	Auditing and securing SSH	1. Configure SSH to **NOT** allow the ability to a. No SSH with empty passwords  b. No SSH with root user 

c. SSH with no other ports apart from 22

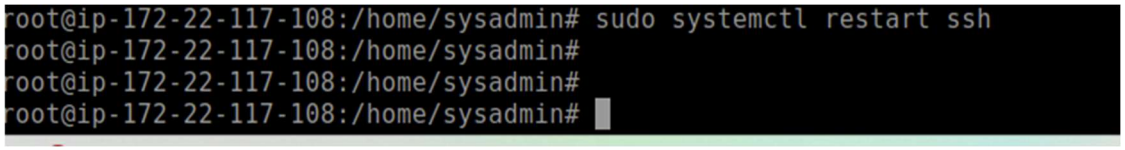


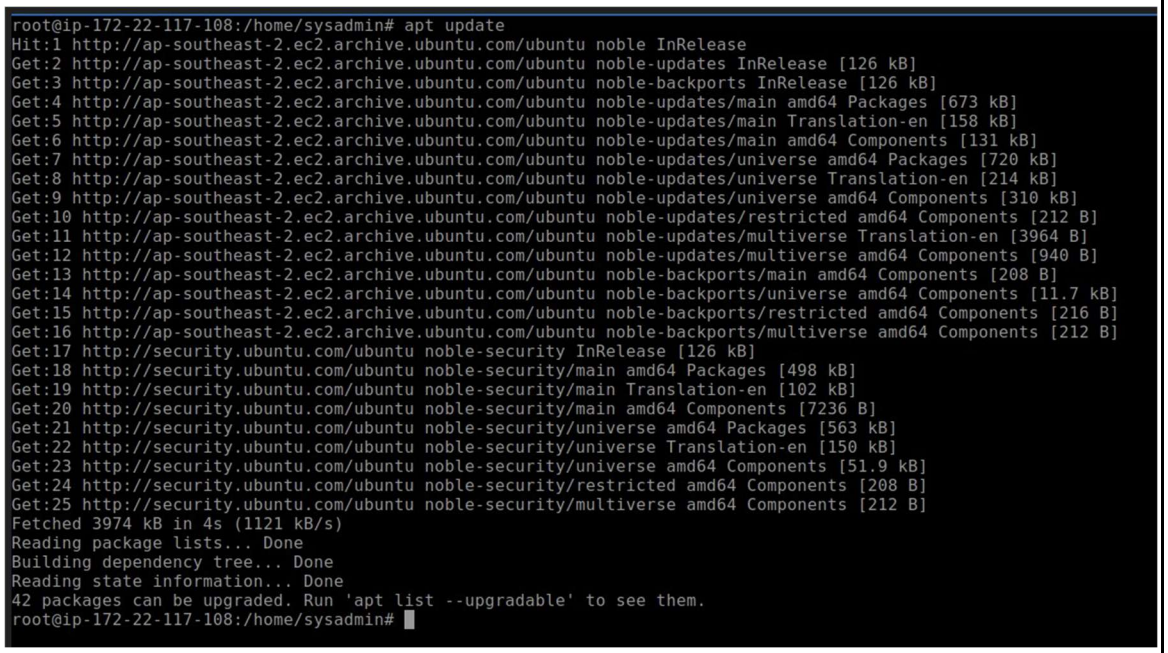
		2. Enable SSH protocol 2 

3. Edit the SSH Server Config File



4. Restart the SSH service to set your updates
   sudo systemctl restart sshd



•	Reviewing and updating system packages	1. Ran apt update *apt update*  2. Ran apt upgrade -y *sudo apt upgrade -y*

```
update-initramfs: Generating /boot/initrd.img-6.8.0-1019-aws
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...
 /etc/needrestart/restart.d/systemd-manager
 systemctl restart cron.service inetd.service nmbd.service packagekit.service smbd.servic
networkd.service systemd-resolved.service systemd-udevd.service udisks2.service

Service restarts being deferred:
 /etc/needrestart/restart.d/dbus.service
 systemctl restart systemd-logind.service

No containers need to be restarted.

User sessions running outdated binaries:
 sysadmin @ session #1: sshd[1074]
 sysadmin @ user manager service: systemd[1079]

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ip-172-22-117-107:~#
```

3. Create the file called package_list.txt

apt list --installed >>pakage_list.txt

```
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin# apt list --installed >>pakage_list.txt

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

root@ip-172-22-117-108:/home/sysadmin#
```

```
Last login: Wed Dec  4 01:23:46 2024 from 172.22.118.75
sysadmin@ip-172-22-117-108:~$ sudo su
[sudo] password for sysadmin:
root@ip-172-22-117-108:/home/sysadmin# ls -l
total 60
-rw-r--r-- 1 root root 51090 Dec  4 02:03 pakage_list.txt
-rwxr-xr-x 1 root root   283 Dec  1 21:53 system_info
-rw------- 1 root root    14 Dec  1 21:51 system_info.save
root@ip-172-22-117-108:/home/sysadmin#
```

4. ID named packages: telnet & rsh-client

   apt list --installed | grep telnet && rsh-client

```
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin# apt list --installed | grep telnet && rsh-client

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

inetutils-telnet/noble,now 2:2.5-3ubuntu4 amd64 [installed,automatic]
telnet/noble,now 0.17+2.5-3ubuntu4 all [installed]
rsh-client: command not found
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin#
```

5. Removing the packages

   apt autoremove -y telnet

```
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin# apt autoremove -y telnet
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  telnet
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 48.1 kB disk space will be freed.
(Reading database ... 103522 files and directories currently installed.)
Removing telnet (0.17+2.5-3ubuntu4) ...
root@ip-172-22-117-108:/home/sysadmin#
```

apt autoremove -y inetutils-telnet

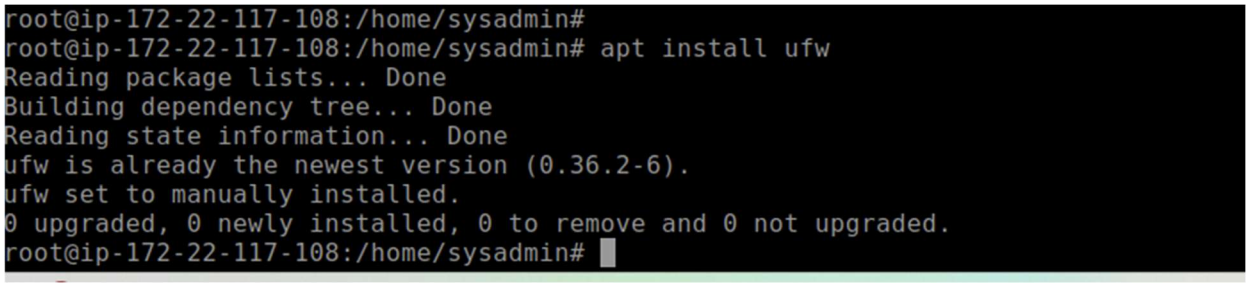
```
root@ip-172-22-117-108:/home/sysadmin# apt autoremove -y inetutils-telnet
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  inetutils-telnet
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 247 kB disk space will be freed.
(Reading database ... 103516 files and directories currently installed.)
Removing inetutils-telnet (2:2.5-3ubuntu4) ...
Processing triggers for man-db (2.12.0-4build2) ...
root@ip-172-22-117-108:/home/sysadmin#
```

no rsh-client package installed

```
root@ip-172-22-117-107:~# apt search rsh-client
Sorting... Done
Full Text Search... Done
root@ip-172-22-117-107:~#
```

telnet and rsh-client are insecure because they use unencrypted communication as well as have weak authentication mechanisms. This makes them prone to man-in-the-middle attacks.

Install new packages

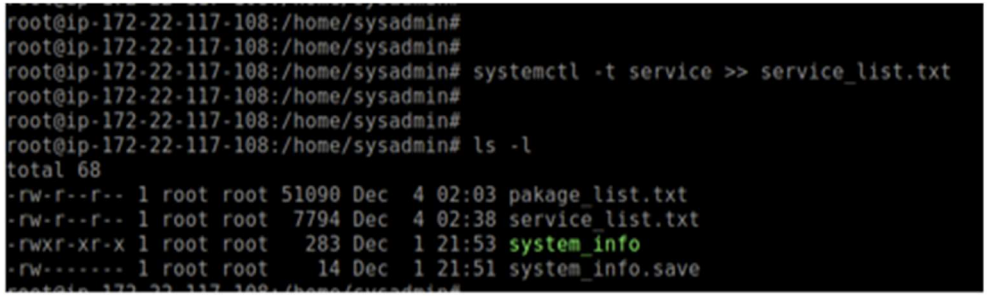
		apt install tripwire  *apt install ufw*  *apt install lynis*

```
root@ip-172-22-117-108:/home/sysadmin# apt install lynis
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  menu
Suggested packages:
  apt-listbugs debsecan debsums tripwire samhain aide fail2ban menu-l10n gksu | kde-cli-tools | ktsuss
The following NEW packages will be installed:
  lynis menu
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 602 kB of archives.
After this operation, 3202 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 lynis all 3.0.9-1 [226 kB]
Get:2 http://ap-southeast-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 menu amd64 2.1.50 [377 kB]
Fetched 602 kB in 0s (23.7 MB/s)
Selecting previously unselected package lynis.
(Reading database ... 103509 files and directories currently installed.)
Preparing to unpack .../archives/lynis_3.0.9-1_all.deb ...
Unpacking lynis (3.0.9-1) ...
Selecting previously unselected package menu.
Preparing to unpack .../archives/menu_2.1.50_amd64.deb ...
Unpacking menu (2.1.50) ...
Setting up lynis (3.0.9-1) ...
Created symlink /etc/systemd/system/timers.target.wants/lynis.timer → /usr/lib/systemd/system/lynis.timer.
lynis.service is a disabled or a static unit, not starting it.
Setting up menu (2.1.50) ...
Processing triggers for install-info (7.1-3build2) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for menu (2.1.50) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ip-172-22-117-108:/home/sysadmin#
```

Hardening features that ufw, lynis, and tripwire can provide:

UFW – it can be configured with various rules and policies to harden a system including default deny policy, specific port allowance, IP address blocking, and logging.

Lynis – Its features include security audits and compliance checks, vulnerable software detection, malware root detection, as well as scheduling audits and continuous monitoring.

		Tripwire – It helps in file integrity monitoring. Achieved through intrusion detection, change detection, providing details change reports, customizable policies and well as file integrity monitoring which is done regularly.
•	Disabling unnecessary services	1. List all services and output to service_list.txt *systemctl -t service >> service_list.txt*  2. Confirm services `grep -i "mysql" service_list.txt` `grep -i "samba" service_list.txt`

```
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin# systemctl -t service >> service_list.txt
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin# ls -l
total 68
-rw-r--r-- 1 root root 51090 Dec  4 02:03 pakage_list.txt
-rw-r--r-- 1 root root  7794 Dec  4 02:38 service_list.txt
-rwxr-xr-x 1 root root   283 Dec  1 21:53 system_info
-rw------- 1 root root    14 Dec  1 21:51 system_info.save
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin# grep -i "mysql" service_list.txt
  mysql.service                                loaded active     running      MySQL Community Server
root@ip-172-22-117-108:/home/sysadmin# grep -i "samba" service_list.txt
  nmbd.service                                 loaded active     running      Samba NMB Daemon
  smbd.service                                 loaded active     running      Samba SMB Daemon
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin#
```

3. Execute services

i.

```
systemctl stop mysql.service

systemctl disable mysql.service

sudo apt-get remove --purge mysql-server mysql-client mysql-common
```

```
447  2024-12-04 02:45:16 systemctl stop mysql.service
448  2024-12-04 02:45:50 systemctl disable mysql.service
449  2024-12-04 02:48:44 systemctl status mysql.service
```

```
root@ip-172-22-117-108:/home/sysadmin#
root@ip-172-22-117-108:/home/sysadmin# sudo apt-get remove --purge mysql-server mysql-client mysql-common
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package 'mysql-client' is not installed, so not removed
The following packages were automatically installed and are no longer required:
  libavahi-client3 libavahi-common-data libavahi-common3 libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libcgi-fast-perl libcgi-pm-perl libclone-perl libcups2t64
  libencode-locale-perl libevent-pthreads-2.1-7t64 libfcgi-bin libfcgi-perl libfcgi0t64 libhtml-parser-perl libhtml-tagset-perl libhtml-template-perl libhttp-date-perl
  libhttp-message-perl libio-html-perl libldb2 liblwp-mediatypes-perl libmecab2 libprotobuf-lite32t64 librados2 librdmacm1t64 libtalloc2 libtdb1 libtevent0t64 liburi-perl liburing2
  libwbclient0 mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-core-8.0 mysql-server-core-8.0 python3-dnspython python3-gpg python3-ldb python3-markdown python3-samba
  python3-talloc python3-tdb samba-ad-provision samba-common samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules tdb-tools
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  mysql-client-8.0* mysql-common* mysql-server* mysql-server-8.0*
0 upgraded, 0 newly installed, 4 to remove and 0 not upgraded.
After this operation, 1752 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 103935 files and directories currently installed.)
Removing mysql-server (8.0.40-0ubuntu0.24.04.1) ...
Removing mysql-server-8.0 (8.0.40-0ubuntu0.24.04.1) ...
update-alternatives: using /etc/mysql/my.cnf.fallback to provide /etc/mysql/my.cnf (my.cnf) in auto mode
Removing mysql-client-8.0 (8.0.40-0ubuntu0.24.04.1) ...
Removing mysql-common (5.8+1.1.0build1) ...
Processing triggers for man-db (2.12.0-4build2) ...
(Reading database ... 103889 files and directories currently installed.)
Purging configuration files for mysql-server-8.0 (8.0.40-0ubuntu0.24.04.1) ...
Purging configuration files for mysql-common (5.8+1.1.0build1) ...
dpkg: warning: while removing mysql-common, directory '/etc/mysql' not empty so not removed
root@ip-172-22-117-108:/home/sysadmin#
```

ii.

systemctl stop nmbd.service

systemctl disable nmbd.service

sudo apt remove nmbd.service

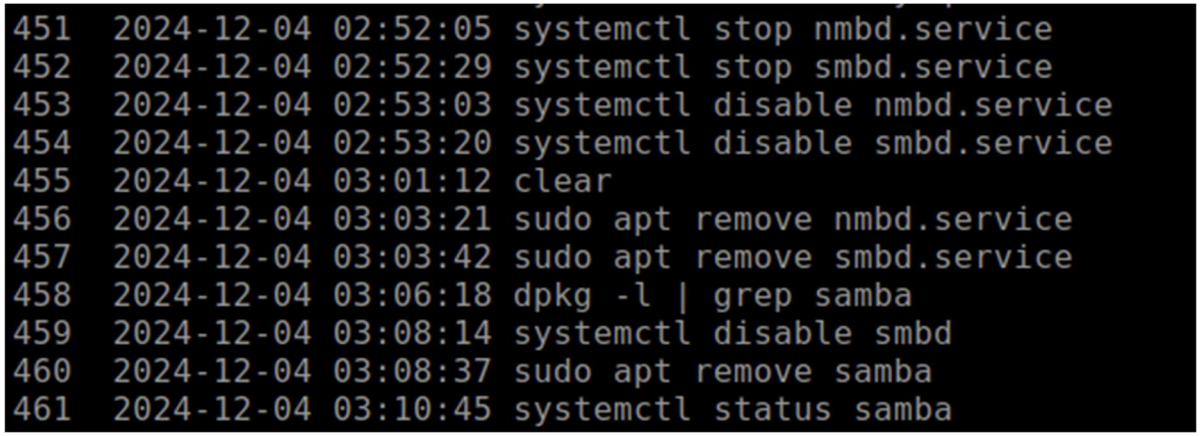
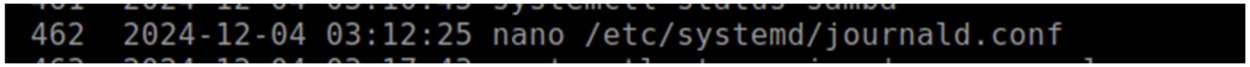
iii.

systemctl stop smbd.service

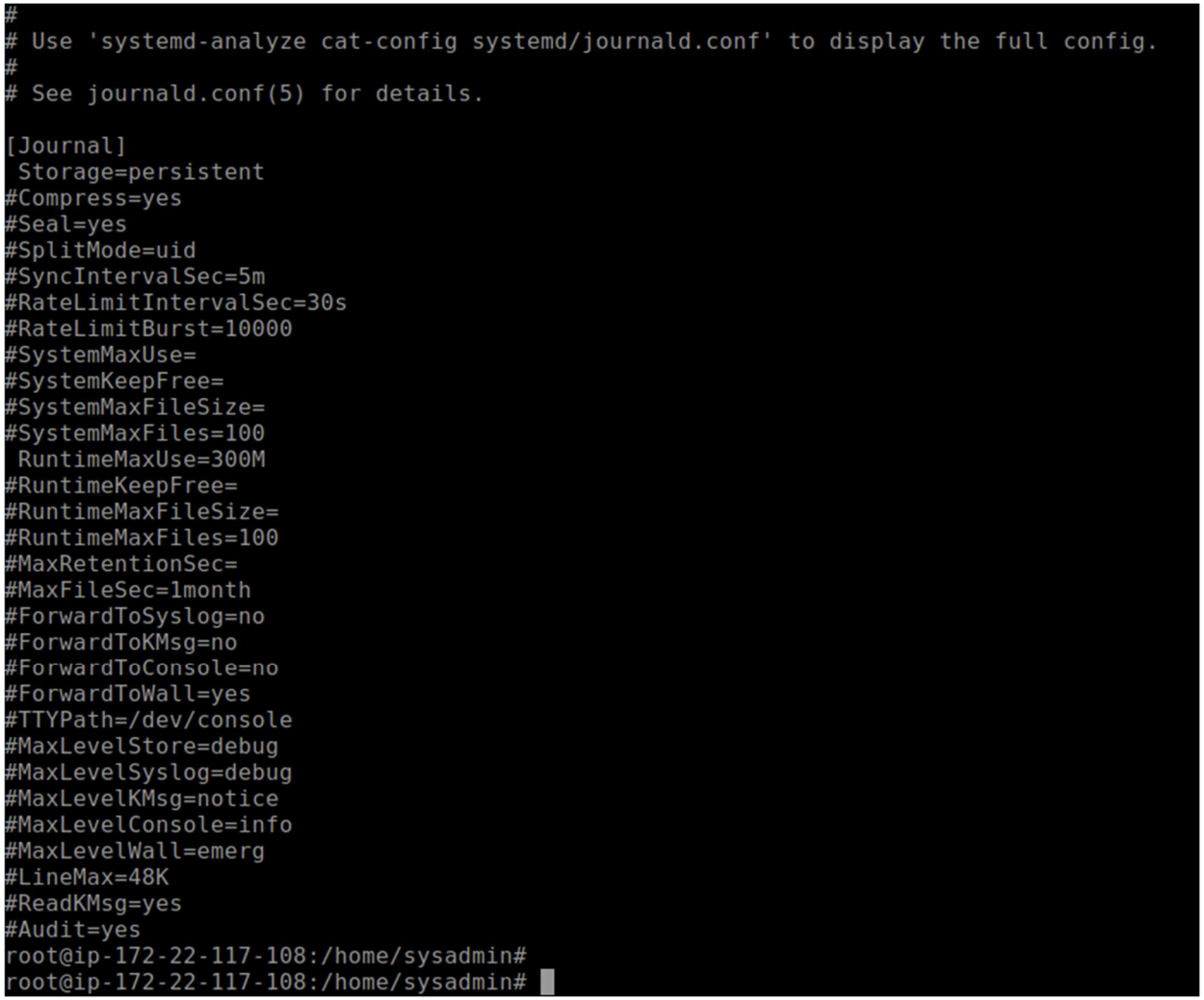
systemctl disable smbd.service

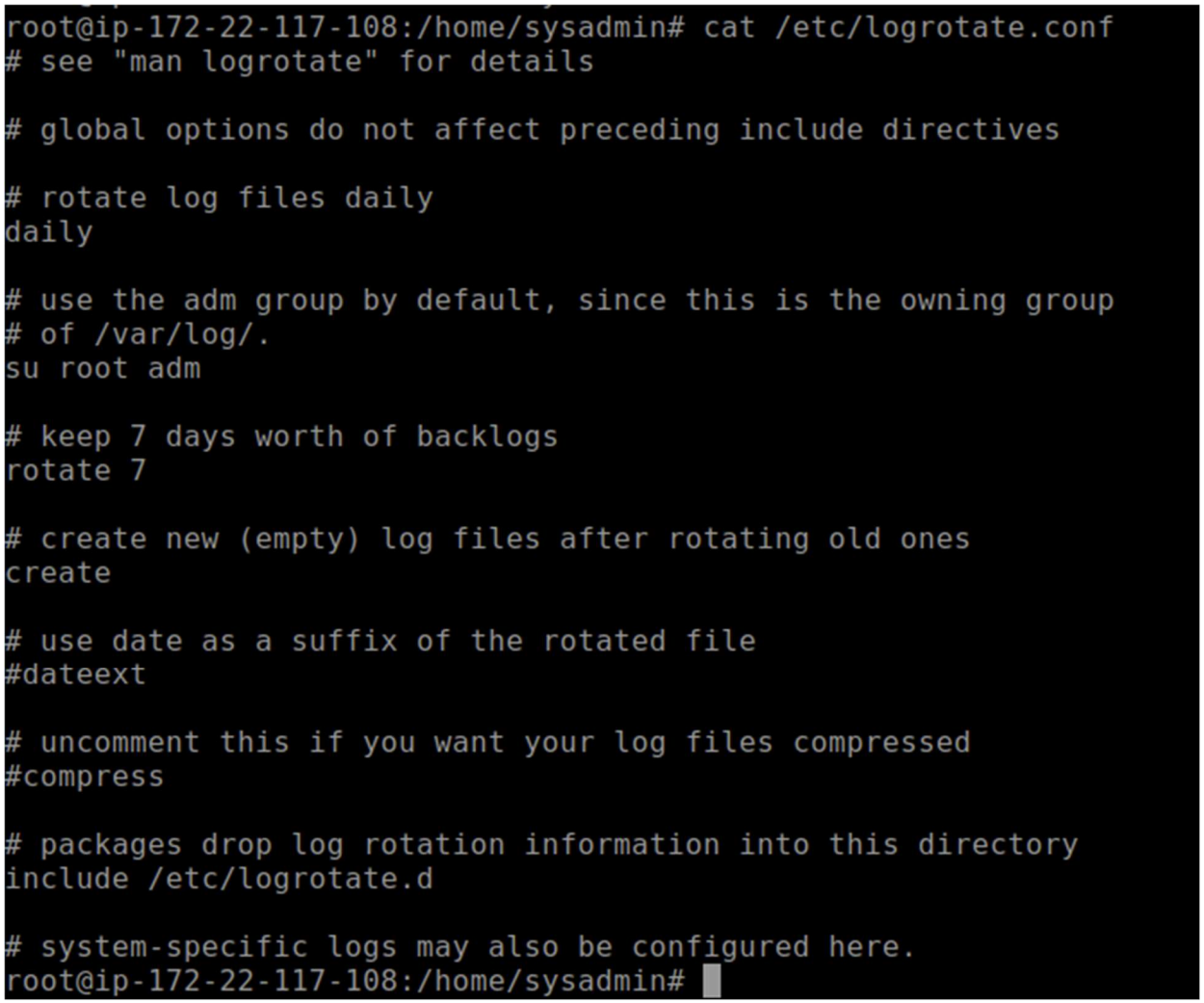
sudo apt remove smbd.service

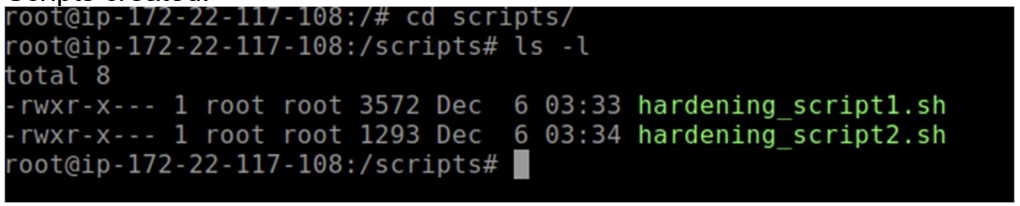
sudo apt remove samba

		
•	Enabling and configuring logging	cat /etc/systemd/journald.conf 

```
root@ip-172-22-117-108:/home/sysadmin# cat /etc/systemd/journald.conf
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it under the
#  terms of the GNU Lesser General Public License as published by the Free
#  Software Foundation; either version 2.1 of the License, or (at your option)
#  any later version.
#
# Entries in this file show the compile time defaults. Local configuration
# should be created by either modifying this file (or a copy of it placed in
# /etc/ if the original file is shipped in /usr/), or by creating "drop-ins" in
# the /etc/systemd/journald.conf.d/ directory. The latter is generally
# recommended. Defaults can be restored by simply deleting the main
# configuration file and all drop-ins located in /etc/.
#
# Use 'systemd-analyze cat-config systemd/journald.conf' to display the full config.
#
# See journald.conf(5) for details.

[Journal]
 Storage=persistent
#Compress=yes
#Seal=yes
#SplitMode=uid
#SyncIntervalSec=5m
#RateLimitIntervalSec=30s
#RateLimitBurst=10000
#SystemMaxUse=
#SystemKeepFree=
#SystemMaxFileSize=
#SystemMaxFiles=100
 RuntimeMaxUse=300M
#RuntimeKeepFree=
#RuntimeMaxFileSize=
#RuntimeMaxFiles=100
#MaxRetentionSec=
#MaxFileSec=1month
#ForwardToSyslog=no
#ForwardToKMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelKMsg=notice
```

		 # # Use 'systemd-analyze cat-config systemd/journald.conf' to display the full config. # # See journald.conf(5) for details. [Journal] Storage=persistent #Compress=yes #Seal=yes #SplitMode=uid #SyncIntervalSec=5m #RateLimitIntervalSec=30s #RateLimitBurst=10000 #SystemMaxUse= #SystemKeepFree= #SystemMaxFileSize= #SystemMaxFiles=100 RuntimeMaxUse=300M #RuntimeKeepFree= #RuntimeMaxFileSize= #RuntimeMaxFiles=100 #MaxRetentionSec= #MaxFileSec=1month #ForwardToSyslog=no #ForwardToKMsg=no #ForwardToConsole=no #ForwardToWall=yes #TTYPath=/dev/console #MaxLevelStore=debug #MaxLevelSyslog=debug #MaxLevelKMsg=notice #MaxLevelConsole=info #MaxLevelWall=emerg #LineMax=48K #ReadKMsg=yes #Audit=yes root@ip-172-22-117-108:/home/sysadmin# root@ip-172-22-117-108:/home/sysadmin#

		cat /etc/logrotate.conf  Ran *systemctl restart systemd-journald* to restart the service

•	Scripts created	Scripts created:  **Hardening_script1.sh** #!/bin/bash # Variable for the report output file, choose an output file name REPORT_FILE="**/Monthly_Report**" # 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: $(cat /etc/os-release)" >> $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

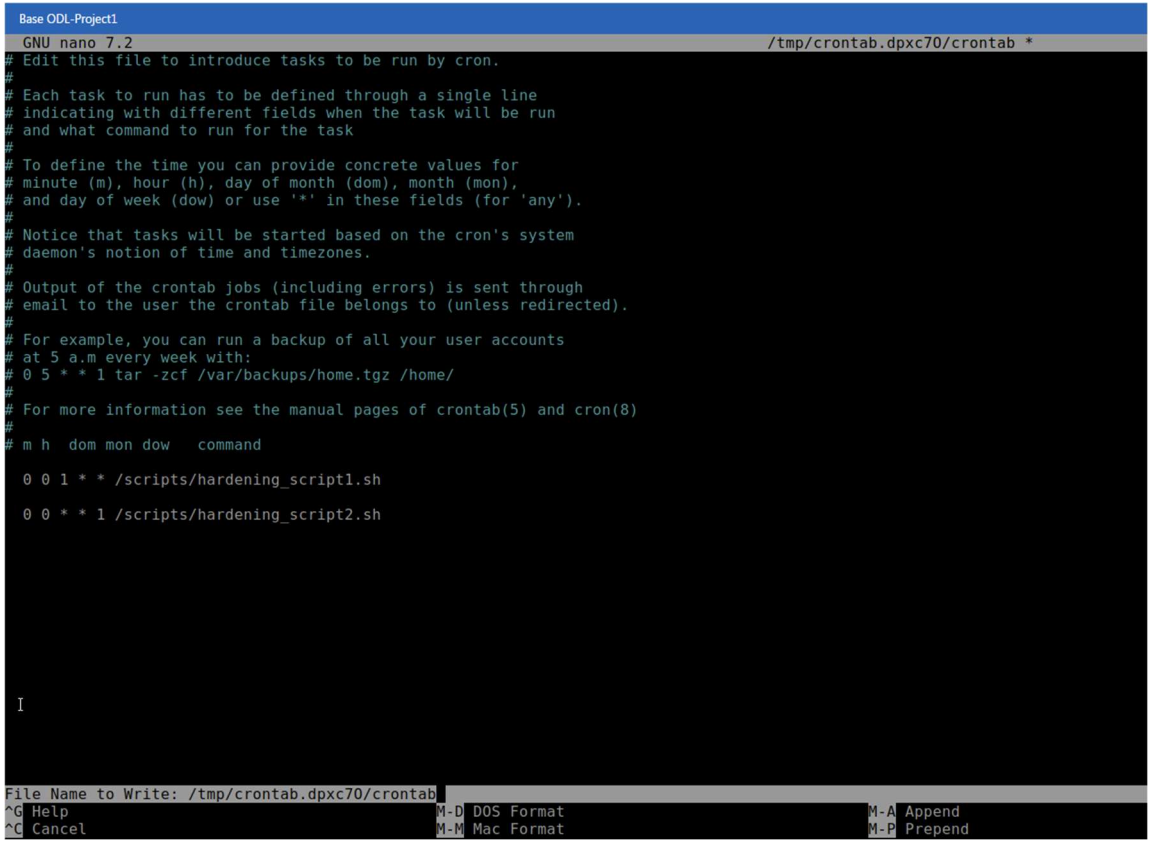
		# Output uptime information echo "Gathering uptime information..." # Placeholder for command to get uptime info echo "Uptime Information: $(uptime)" >> $REPORT_FILE printf "\n" >> $REPORT_FILE # Backup the OS echo "Backing up the OS..." # Placeholder for command to back up the OS *sudo tar -cvpzf /baker_street_backup.tar.gz --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

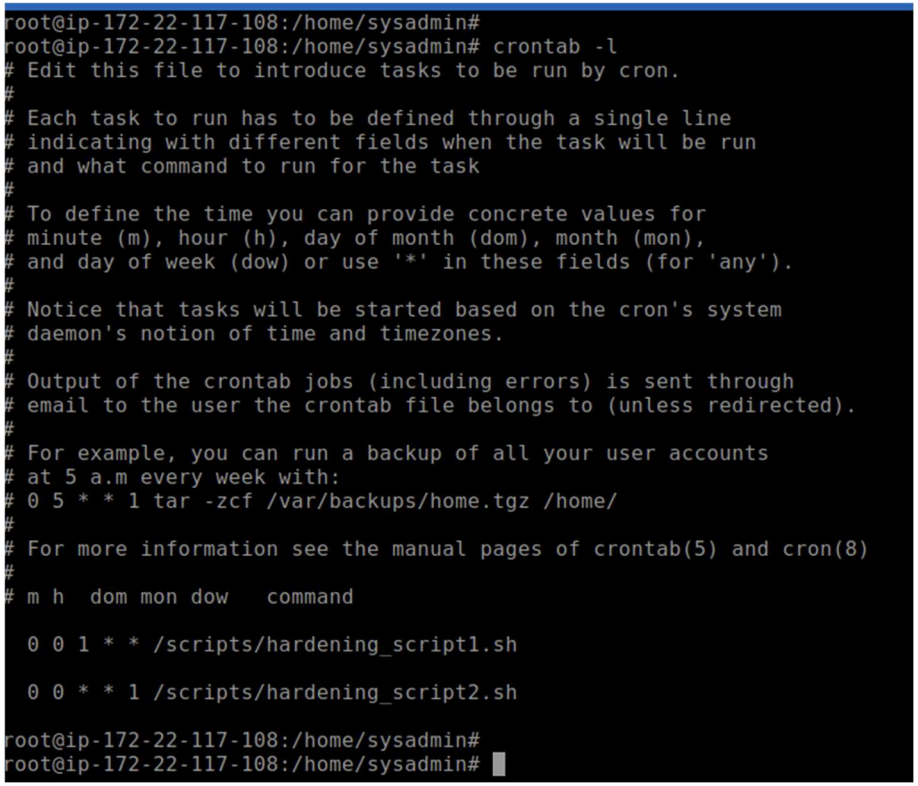
```
# Output the sudoers file to the report
echo "Gathering sudoers file..."
# Placeholder for command to output sudoers file
echo "Sudoers file:$(cat /etc/sudoers)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE


# Script to check for files with world permissions and update them
echo "Checking for files with world permissions..."

   find /home -perm /o+rwx -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 /home -type f -iname *"Engineering"*"sh" | xargs 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 /home -type f -iname *"Research"*"sh" | xargs 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 /home -type f -iname *"Finance"*"sh" | xargs chown :finance echo "Permissions updated for Finance scripts." >> $REPORT_FILE printf "\n" >> $REPORT_FILE echo "Script execution completed. Check $REPORT_FILE for details."

		Hardening_script2.sh #!/bin/bash # Variable for the report output file, choose a **NEW** output file name REPORT_FILE="/Weekly_Report" # 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:$(cat /etc/ssh/sshd_config)" >> $REPORT_FILE printf "\n" >> $REPORT_FILE # Update packages and services Echo “Updating packages and services” # Placeholder for command to update packages *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:$(*apt list –installed*)" >> $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/logrotate.conf)" >> $REPORT_FILE printf "\n" >> $REPORT_FILE echo "Script execution completed. Check $REPORT_FILE for details."

•	Scripts scheduled with cron	Scheduling scripts with cron: 

		Confirming scripts scheduled with cron:  script 1 is scheduled to run once a month, and on the first of the month. script 2 is scheduled to run once a week, every Monday at 12 am.

•	Summary Report	In this project, we were tasked with hardening a Linux server for The Baker Street Corporation (BSC). The objective was to audit the server's configuration and implement security measures to mitigate potential vulnerabilities. **Key Activities and Findings** **Pre-Hardening Steps:** Conducted a system inventory and created a backup of critical files to ensure data integrity during the hardening process. **Auditing Users and Groups:** Reviewed existing user accounts and groups to ensure only authorized personnel had the system access. Implemented the principle of least privilege by adjusting user permissions as necessary. **Password Policy Enforcement:** Updated password policies to enforce complexity requirements and forced users to change weak passwords upon next login. Updated password hashing configuration. **Sudo Permissions:** Validated and updated the sudoers file to restrict sudo access to a minimal number of trusted

		users, ensuring that only essential tasks could be performed with elevated privileges. **File and Directory Permissions:** Checked and corrected permissions on sensitive files and directories, including /etc/shadow and /etc/passwd, to prevent unauthorized access. **SSH Configuration:** Configured SSH settings to enhance security, including disabling root login and changing the default SSH port. **Unnecessary Services and Packages:** Identified and removed unnecessary services and packages to reduce the attack surface of the server. **Logging and Monitoring:** Configured logging settings to ensure that all relevant events were recorded and could be monitored for suspicious activity. **Automation of Hardening Tasks:** Developed scripts to automate repetitive hardening tasks and scheduled them with cron jobs

		for regular execution. **Conclusion** The hardening process significantly improved the security posture of the Linux server. By implementing the changes outlined above, the server is now better protected against potential threats and vulnerabilities. Future recommendations include regular audits and updates to the hardening measures to adapt to evolving security challenges.