




OS Information

Checklist

Completed	Activity	Script(s) used / Tasks completed / Screenshots
<input checked="" type="checkbox"/>	OS backup	 <p>The command I used was <code>sudo tar -czvf /baker_street_backup.tar.gz --exclude=/baker_street_backup.tar.gz --exclude=/proc --exclude=/tmp --exclude=/mnt --exclude=/sys --exclude=/dev --exclude=/run /</code></p> <p>command creates a compressed archive of the entire file system, excluding the current backup</p>

		archive, temporary files, and system directories, which are often unnecessary for backup.
<input checked="" type="checkbox"/>	Auditing users and groups	<pre>deluser [--conf file] [--quiet] [--verbose] [--debug] user group # remove the user from a group sysadmin@ip-172-22-117-83:/home\$ ls dler gregson irene lestrade mary moriarty mrs_hudson mycroft sherlock sysadmin toby ubuntu watson sysadmin@ip-172-22-117-83:/home\$ sudo userdel mary sysadmin@ip-172-22-117-83:/home\$ ls dler gregson irene lestrade mary moriarty mrs_hudson mycroft sherlock sysadmin toby ubuntu watson sysadmin@ip-172-22-117-83:/home\$ cd mary/ bash: cd: mary/: Permission denied sysadmin@ip-172-22-117-83:/home\$ sudo userdel -r mary userdel: user 'mary' does not exist sysadmin@ip-172-22-117-83:/home\$ sudo userdel -r gregson userdel: gregson mail spool (/var/mail/gregson) not found sysadmin@ip-172-22-117-83:/home\$ sudo userdel -r gregson userdel: user 'gregson' does not exist sysadmin@ip-172-22-117-83:/home\$ sudo userdel -r gregson userdel: user 'gregson' does not exist sysadmin@ip-172-22-117-83:/home\$</pre> <pre>sysadmin@ip-172-22-117-83:/home\$ id sherlock uid=1002(sherlock) gid=1005(sherlock) groups=1005(sherlock),1002(engineering) sysadmin@ip-172-22-117-83:/home\$ id mary id: 'mary': no such user sysadmin@ip-172-22-117-83:/home\$ id irene uid=1006(irene) gid=1009(irene) groups=1009(irene),1003(marketing) sysadmin@ip-172-22-117-83:/home\$ id lestrade id: 'lestrade': no such user sysadmin@ip-172-22-117-83:/home\$ sudo userdel -r irene userdel: irene mail spool (/var/mail/irene) not found sysadmin@ip-172-22-117-83:/home\$ id irene id: 'irene': no such user sysadmin@ip-172-22-117-83:/home\$</pre> <pre>sysadmin@ip-172-22-117-83:/home\$ sudo usermod -L moriarty sysadmin@ip-172-22-117-83:/home\$ sudo usermod -L mrs_hudson sysadmin@ip-172-22-117-83:/home\$</pre> <pre>sysadmin@ip-172-22-117-83:/home\$ sudo passwd -S -a root L 2024-09-27 0 99999 7 -1 daemon L 2024-09-27 0 99999 7 -1 bin L 2024-09-27 0 99999 7 -1 sys L 2024-09-27 0 99999 7 -1 sync L 2024-09-27 0 99999 7 -1 games L 2024-09-27 0 99999 7 -1 man L 2024-09-27 0 99999 7 -1 lp L 2024-09-27 0 99999 7 -1 mail L 2024-09-27 0 99999 7 -1 news L 2024-09-27 0 99999 7 -1 uucp L 2024-09-27 0 99999 7 -1 proxy L 2024-09-27 0 99999 7 -1 www-data L 2024-09-27 0 99999 7 -1 backup L 2024-09-27 0 99999 7 -1 list L 2024-09-27 0 99999 7 -1 irc L 2024-09-27 0 99999 7 -1 apt L 2024-09-27 0 99999 7 -1 nobody L 2024-09-27 0 99999 7 -1 systemd-network L 2024-09-27 -1 -1 -1 -1 systemd-timesync L 2024-09-27 -1 -1 -1 -1 dhcpcd L 2024-09-27 -1 -1 -1 -1 messagebus L 2024-09-27 -1 -1 -1 -1 syslog L 2024-09-27 -1 -1 -1 -1 systemd-resolve L 2024-09-27 -1 -1 -1 -1 quid L 2024-09-27 -1 -1 -1 -1 ss L 2024-09-27 -1 -1 -1 -1 sshd L 2024-09-27 -1 -1 -1 -1 collinate L 2024-09-27 -1 -1 -1 -1 cpdump L 2024-09-27 -1 -1 -1 -1 landscape L 2024-09-27 -1 -1 -1 -1 wupdt-refresh L 2024-09-27 -1 -1 -1 -1 solkitd L 2024-09-27 -1 -1 -1 -1 ec2-instance-connect L 2024-09-27 -1 -1 -1 -1 chrony L 2024-09-27 -1 -1 -1 -1 ubuntu L 2024-10-22 0 99999 7 -1 sysadmin P 2024-10-22 0 99999 7 -1 sherlock P 2025-01-07 0 99999 7 -1 watson P 2024-10-22 0 99999 7 -1 moriarty L 2024-10-22 0 99999 7 -1 mycroft P 2024-10-22 0 99999 7 -1 mrs_hudson L 2024-10-22 0 99999 7 -1 toby L 2024-10-22 0 99999 7 -1 dler P 2025-01-07 0 99999 7 -1 mysql L 2024-10-22 -1 -1 -1 -1 postfix L 2025-01-08 -1 -1 -1 -1 sysadmin@ip-172-22-117-83:/home\$</pre>

	Auditing users and groups	<pre>toby : toby sysadmin@ip-172-22-117-83:/home\$ groups mycroft mycroft : mycroft marketing sysadmin@ip-172-22-117-83:/home\$ groups watson watson : watson engineering sysadmin@ip-172-22-117-83:/home\$ sudo usermod -aG research mycroft sysadmin@ip-172-22-117-83:/home\$ sudo groupdel marketing sysadmin@ip-172-22-117-83:/home\$ ls adler lestrade mary moriarty mrs_hudson mycroft sherlock sysadmin toby ubuntu watson sysadmin@ip-172-22-117-83:/home\$ █</pre> <p>to delete a user I used the command (<code>sudo userdel -r *username*</code>) and once the user was deleted I would verify it by using the command (<code>id *username*</code>)</p> <p>Locker a user account I would use the command (<code>sudo usermod -L *username*</code>)</p>
☑	Updating and enforcing password policies	<pre>password [success=1 default=ignore] pam_unix.so obscure md5 # here's the fallback if no module succeeds password [success=1 default=ignore] pam_unix.so obscure md5 # prime the stack with a positive return value if there isn't one already; # this avoids us returning an error just because nothing sets a success code # since the modules above will each just jump around password [success=1 default=ignore] pam_unix.so obscure md5 # and here are more per-package modules (the "Additional" block) password requisite pam_pwquality.so minlen=8 ocredit=1 retry=2 ucredit=1█ # end of pam-auth-update config</pre> <p>For password requirement and while using the Day 1 activity template I used/created the line of code as follows: <code>password requisite pam_pwquality.so minlen=8 ocredit=1 retry=2 ucredit=1</code></p>
☑	Updating and enforcing sudo permissions	<pre>@includedir /etc/sudoers.d sysadmin ALL=(ALL:ALL) ALL sysadmin ALL=(ALL:ALL) ALL sherlock ALL=(ALL) NOPASSWD:ALL watson ALL=(ALL) NOPASSWD:/var/log/logcleanup.sh mycroft ALL=(ALL) NOPASSWD:/var/log/logcleanup.sh sysadmin ALL=(ALL:ALL) ALL</pre> <pre>@includedir /etc/sudoers.d sysadmin ALL=(ALL:ALL) ALL sysadmin ALL=(ALL:ALL) ALL sherlock ALL=(ALL) NOPASSWD:ALL watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh mycroft ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh sysadmin ALL=(ALL:ALL) ALL research ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh █</pre> <p>- once giving all priv var to both watson and mycroft as well as the research group, I verified it by using <code>ls -l</code></p>



Validating and updating permissions on files and directories

```
sysadmin@ip-172-22-117-83:/home$ sudo chmod -R o-rwx adler/
sysadmin@ip-172-22-117-83:/home$ sudo chmod -R o-rwx moriarty/
sysadmin@ip-172-22-117-83:/home$ sudo chmod -R o-rwx mycroft/
sysadmin@ip-172-22-117-83:/home$ sudo chmod -R o-rwx sherlock/
sysadmin@ip-172-22-117-83:/home$ sudo chmod -R o-rwx toby
sysadmin@ip-172-22-117-83:/home$ sudo chmod -R o-rwx watson/
sysadmin@ip-172-22-117-83:/home$ ls -l
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 Jan 6 23:54 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
sysadmin@ip-172-22-117-83:/home$
```

```
root@ip-172-22-117-83:/home# find /home -type f -perm /o-rwx -exec chmod o-rwx {} \;
root@ip-172-22-117-83:/home# ls -l
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 Jan 7 23:16 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-172-22-117-83:/home# cd home
bash: cd: home: No such file or directory
root@ip-172-22-117-83:/home# cd home/
bash: cd: home/: No such file or directory
root@ip-172-22-117-83:/home# ls
ls
root@ip-172-22-117-83:/home# cd home
root@ip-172-22-117-83:/home# ls
root@ip-172-22-117-83:/home# ls
adler moriarty mrs hudson mycroft sherlock sysadmin toby ubuntu watson
root@ip-172-22-117-83:/home/adler# ls -l
total 8
-rw-r----- 1 adler adler 0 Oct 22 16:36 Engineering_script.sh.0.txt
-rw-r----- 1 adler adler 0 Oct 22 16:36 Engineering_script.sh.3.txt
-rwxr-x--- 1 adler adler 48 Oct 22 16:36 Engineering_script.sh_script1.sh
-rwxr-x--- 1 adler adler 48 Oct 22 16:36 Engineering_script.sh_script2.sh
-rw-r----- 1 adler adler 0 Oct 22 16:36 deduction.doc.2.txt
-rw-r----- 1 adler adler 0 Oct 22 16:36 game_is_afoot.txt.1.txt
root@ip-172-22-117-83:/home/adler# find / -iname "engineering" -exec chown :engineering {} \;
root@ip-172-22-117-83:/home/adler# ls -l
total 8
-rw-r----- 1 adler engineering 0 Oct 22 16:36 Engineering_script.sh.0.txt
-rw-r----- 1 adler engineering 0 Oct 22 16:36 Engineering_script.sh.3.txt
-rwxr-x--- 1 adler engineering 48 Oct 22 16:36 Engineering_script.sh_script1.sh
-rwxr-x--- 1 adler engineering 48 Oct 22 16:36 Engineering_script.sh_script2.sh
-rw-r----- 1 adler adler 0 Oct 22 16:36 deduction.doc.2.txt
-rw-r----- 1 adler adler 0 Oct 22 16:36 game_is_afoot.txt.1.txt
root@ip-172-22-117-83:/home/adler# cd ../
root@ip-172-22-117-83:/home# ls
user street backup.tar.gz bin bin usr-is-merged boot dev etc home lib lib usr-is-merged lib64 lost+found media mnt opt
root@ip-172-22-117-83:/home# find / -iname "finance" -exec chown :finance {} \;
root@ip-172-22-117-83:/home# cd home/
root@ip-172-22-117-83:/home# ls
adler moriarty mrs hudson mycroft sherlock sysadmin toby ubuntu watson
root@ip-172-22-117-83:/home/mycroft# ls -l
total 8
-rw-r----- 1 mycroft engineering 0 Oct 22 16:35 Engineering_script.sh.0.txt
-rw-r----- 1 mycroft finance 0 Oct 22 16:35 Finance_script.sh.3.txt
-rwxr-x--- 1 mycroft finance 48 Oct 22 16:35 Finance_script.sh_script1.sh
-rwxr-x--- 1 mycroft finance 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
root@ip-172-22-117-83:/home/mycroft#
```

```
sysadmin@ip-172-22-117-83:/home$ sudo su watson
ls
adler moriarty mrs hudson mycroft sherlock sysadmin toby ubuntu watson
cd wat
ls
ls: .1: can't cd to wat
cd watson
ls
Finance_script.sh.3.txt Finance_script.sh_script1.sh Finance_script.sh_script2.sh deduction.doc.0.txt deduction.doc.1.txt deduction.doc.2.txt my_file.txt
cd my_file.txt
perl Password123
perl2 Query104
perl3 letmein456
ls
Finance_script.sh.3.txt Finance_script.sh_script1.sh Finance_script.sh_script2.sh deduction.doc.0.txt deduction.doc.1.txt deduction.doc.2.txt
ls
```

-by using the sudo chmod I was able to remove world permissions from all users as well using the chown command to change permissions from files to only specific members 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.

<input type="checkbox"/>	Optional: Updating password hashing configuration	
<input checked="" type="checkbox"/>	Auditing and securing SSH	<pre> host * # ForwardAgent no # ForwardX11 no # ForwardX11Trusted yes # PasswordAuthentication yes # HostbasedAuthentication no # GSSAPIAuthentication no # GSSAPIDelegateCredentials no # GSSAPIKeyExchange no # GSSAPITrustDNS no # BatchMode no # CheckHostIP no # AddressFamily any # ConnectTimeout 0 # StrictHostKeyChecking ask # IdentityFile ~/.ssh/id_rsa # IdentityFile ~/.ssh/id_dsa # IdentityFile ~/.ssh/id_ecdsa # IdentityFile ~/.ssh/id_ed25519 # Port 22 # Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc # MACs hmac-md5,hmac-sha1,umac-64@openssh.com # EscapeChar ~ # Tunnel no # TunnelDevice any:any # PermitLocalCommand no # VisualHostKey no # ProxyCommand ssh -q -W %h:%p gateway.example.com # RekeyLimit 1G 1h # UserKnownHostsFile ~/.ssh/known_hosts.d/%k SendEnv LANG LC_* HashKnownHosts yes GSSAPIAuthentication yes PermitEmptyPasswords no PermitRootLogin no Port 22 Protocol 2 </pre> <pre> sysadmin@ip-172-22-117-83:/etc/ssh\$ sudo service ssh restart sysadmin@ip-172-22-117-83:/etc/ssh\$ </pre> <p>-using the daemon config file that was in the activity file I was able to determine what to add and remove from the bash file for auditing and securing the SSH.</p> <p>- as well to restart the server i used the command (sudo service ssh restart) which allowed all the SSH updates to save</p>



Reviewing and updating system packages

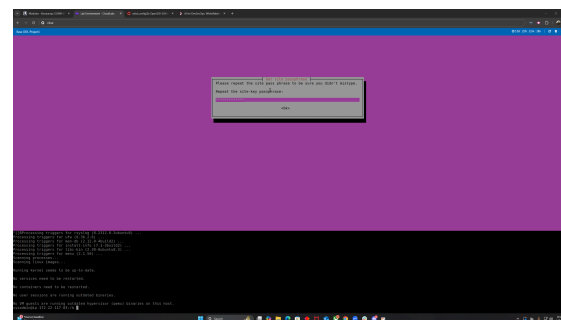
```
sysadmin@ip-172-22-117-83:/$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
45 packages can be upgraded. Run 'apt list --upgradable' to see them.
sysadmin@ip-172-22-117-83:/$ sudo apt update -y
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
45 packages can be upgraded. Run 'apt list --upgradable' to see them.
sysadmin@ip-172-22-117-83:/$
```

```
sysadmin@ip-172-22-117-83:/$ sudo su
root@ip-172-22-117-83:/# sudo apt list --installed > package_list.txt

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

root@ip-172-22-117-83:/# tail package_list.txt
xdg-user-dirs/noble,now 0.18-1build1 amd64 [installed,automatic]
xfsprogs/noble,now 6.6.0-1ubuntu2 amd64 [installed,automatic]
xkb-data/noble-updates,now 2.41-2ubuntu1.1 all [installed,automatic]
xml-core/noble,now 0.19 all [installed,automatic]
xprintidle/noble,now 0.2.5-2build1 amd64 [installed]
xkb/noble-updates,noble-security,now 2+9.1.0016-1ubuntu7.5 amd64 [installed,automatic]
xz-utils/noble-updates,now 5.6.1+really5.4.5-1build0.1 amd64 [installed,automatic]
zerofree/noble,now 1.1.1-1build5 amd64 [installed,automatic]
zlib1g/noble-updates,now 1:1.3.dfsg-3.1ubuntu2.1 amd64 [installed,automatic]
zstd/noble-updates,now 1.5.5+dfsg2-2build1.1 amd64 [installed,automatic]
```

```
root@ip-172-22-117-83:/# grep -E 'telnet|rsync-client' package_list.txt
netutils-telnet/noble,now 2:2.5-3ubuntu4 amd64 [installed,automatic]
telnet/noble,now 0.17+2.5-3ubuntu4 all [installed]
root@ip-172-22-117-83:/# grep -E 'rsync-client' package_list.txt
root@ip-172-22-117-83:/# sudo apt remove telnet -y
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 45 not upgraded.
After this operation, 48.1 kB disk space will be freed.
Reading database ... 100759 files and directories currently installed.)
Removing telnet (0.17+2.5-3ubuntu4) ...
root@ip-172-22-117-83:/# exit
exit
sysadmin@ip-172-22-117-83:/$ sudo apt remove telnet rsync-client -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package 'rsync-client' is not installed, so not removed
Package 'telnet' is not installed, so not removed
0 upgraded, 0 newly installed, 0 to remove and 45 not upgraded.
sysadmin@ip-172-22-117-83:/$
```



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

	<p>Enabling and configuring logging</p>	<div data-bbox="805 205 1487 783"><pre>GNU nano 2.2 # see "man logrotate" for details # global options do not affect preceding include directives # rotate log files weekly daily # use the adm group by default, since this is the owning group # of /var/log/. su root adm # keep 4 weeks worth of backlogs rotate 7 # create new (empty) log files after rotating old ones create # use date as a suffix of the rotated file #dateext # uncomment this if you want your log files compressed #compress # packages drop log rotation information into this directory include /etc/logrotate.d # system-specific logs may also be configured here.</pre></div> <p>-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.</p> <p>- using the same strategy and methods of using the activity file i was able to do the same with logrotate file</p>
<div data-bbox="256 1129 284 1159"><input checked="" type="checkbox"/></div>	<p>Scripts created</p>	<div data-bbox="805 1123 1305 1598"><pre>#!/bin/bash # Variable for the report output file REPORT_FILE="hardening_report.txt" # Output the hostname echo "Gathering hostname..." echo "Hostname: \$(hostname)" >> \$REPORT_FILE echo " " >> \$REPORT_FILE # Output the OS version echo "Gathering OS version..." echo "OS Version: \$(lsb_release -d)" >> \$REPORT_FILE echo " " >> \$REPORT_FILE # Output memory information echo "Gathering memory information..." echo "Memory Information: \$(free -m)" >> \$REPORT_FILE echo " " >> \$REPORT_FILE # Output uptime information echo "Gathering uptime information..." echo "Uptime Information: \$(uptime)" >> \$REPORT_FILE echo " " >> \$REPORT_FILE # Backup the OS echo "Backing up the OS..." tar -cuf /baker_street_backup.tar.gz --exclude=/baker_street_backup.tar.gz --exclude=/proc --exclude=/tmp --exclude= echo "OS backup completed." >> \$REPORT_FILE echo " " >> \$REPORT_FILE # Output the sudoers file to the report echo "Gathering sudoers file..." echo "Sudoers file: \$(cat /etc/sudoers)" >> \$REPORT_FILE</pre></div>

Scripts created

```
GNU nano 7.2 hardening_script2.sh *
#!/bin/bash

# Variable for the report output file, choose a NEW output file name
REPORT_FILE="hardening_report2.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:(sudo cat /etc/ssh/ssh_config)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Update packages and services
echo "Updating packages and services"

# Placeholder for command to update packages

sudo apt-get update

# Placeholder for command to upgrade packages

sudo apt-get 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:(sudo apt list --installed)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE
```

```
# Output the sudoers file to the report
echo "Gathering 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/ -perm /o-rwx -type f -exec chmod o-rwx {} \;
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..."
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..."
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..."
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."
```

```
# Placeholder for command to list all installed packages

echo "Installed Packages:(sudo 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:(sudo cat /etc/systemd/journald.conf)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Placeholder for command to display logrotate data

echo "logrotate.conf file data:(sudo cat /etc/logrotate.conf)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

echo "Script execution completed. Check $REPORT_FILE for details."
```

```
Script execution completed. Check hardening_report.txt for details.
sysadmin@ip-172-22-117-83:~$ sudo cat hardening_report.txt
hostname: ip-172-22-117-83

OS Version: Description: Ubuntu 24.04.1 LTS

Memory Information:
Mem:      3836      610      137      24      free  shared buff/cache available
Swap:      0         0         0

Uptime Information: 01:16:13 up 1:30, 1 user, load average: 0.00, 0.14, 0.41

OS backup completed.

Sudoers file:#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
```

Scripts created

```
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# This fixes CVE-2005-4890 and possibly breaks some versions of kdesu
# (#1011624, https://bugs.kde.org/show_bug.cgi?id=452532)
Defaults      use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
Defaults:sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
Defaults:sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
Defaults:sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
Defaults:sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

# Per-user preferences; root won't have sensible values for them.
Defaults:sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
Defaults:sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
Defaults:sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
admin    ALL=(ALL) ALL

# Allow members of group sudo to execute any command
sudo    ALL=(ALL:ALL) ALL

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

@include::/etc/sudoers.d

sysadmin ALL=(ALL:ALL) ALL
sysadmin ALL=(ALL:ALL) ALL
herlock ALL=(ALL) NOPASSWD:ALL
watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh
mycroft ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh
sysadmin ALL=(ALL:ALL) ALL
research ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh

World permissions have been removed from any files found.

Permissions updated for Engineering scripts.

Permissions updated for Research scripts.

Permissions updated for Finance scripts.

sysadmin@ip-172-22-117-83:~$
```

```
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=300M
#SystemKeepFree=
#SystemMaxFilesSize=
#SystemMaxFiles=100
#RuntimeMaxUse=
#RuntimeKeepFree=
#RuntimeMaxFileSize=
#RuntimeMaxFiles=100
#MaxRetentionSec=
#MaxFileSec=1month
#ForwardToSyslog=no
#ForwardToMq=no
#ForwardToConsole=no
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelMq=notice
#MaxLevelConsole=info
#MaxLevelMail=emerg
#LineMax=48K
#ReadMq=yes
#Audit=yes

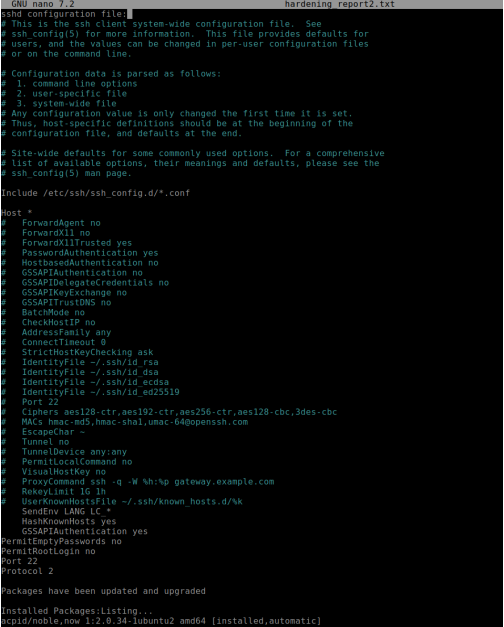
logrotate.conf file data:# see "man logrotate" for details

# global options do not affect preceding include directives

# rotate log files weekly
daily

# use the adm group by default, since this is the owning group
# of /var/log/.
su root adm

# keep 4 weeks worth of backlogs
rotate 7
```

	Scripts created	 <p>-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.</p>
<input checked="" type="checkbox"/>	Scripts scheduled with cron	 <p>- 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</p>

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.