

IT AUDIT REPORT

Organization Name: The Baker Street Corporation (BSC)

Report Title: IT Audit – Linux Server

Audit Period: December 17, 2024-January 13, 2025

Report Date: January 13, 2025

Auditor(s): John Mallon

1. Executive Summary

An IT audit was conducted at the request of BSC on a Linux server containing confidential data. It was BSC's objective that this data be protected from security breaches. Key findings include gaps in cyber security, both local and remote access control mechanisms, and outdated software. As per BSC's instruction, these gaps have been addressed and corrected. Recommendations for the future included implementing a patch management system, enhancing user access protocols, hardening the system, and other security measures. Note that no penetration testing, or any similar methods, were carried out during this audit.

2. Scope and Objectives

Scope: BSC's Linux server containing confidential data.

Objectives: Confirm and, if necessary, make necessary remediations, to ensure that the system is properly and securely configured to mitigate the risk to BSC from security breaches.

3. Audit Methodology

The audit focused on the BSC's Linux server's systems, files, directories, users, and groups.

The approach included:

- (i) Review of policies and procedures
- (ii) Review of potential vulnerabilities
- (iii) Assessment of the system configurations

4. Key Findings

4.1 Security Vulnerabilities

- absence of auditing of users and groups (Medium).
- improper file permissions (Medium).
- absence of policies to update and enforce password policies (Critical).
- absence of policies to update and enforce sudo permissions (Medium).

JOHN MALLON

- absence of policies to validate and update permissions on files and directories (Medium).
- absence of a firewall (Critical).
- root login enabled via SSH (Critical).
- open SSH port available from the Internet (Critical).
- SSH configured to allow no password (Critical).
- unrestricted services running (High).
- inactive user accounts not disabled (Low).

4.2 Operational Issues

- absence of pre-hardening steps and patching of system inventory (Critical).
 - absence of consistent system backup (Medium).
 - absence of recovery testing procedures (Medium).
 - Insufficient capture and monitoring of system logs (Low).
-

5. Recommendations

5.1 Security

- Periodically check for running and installed packages
- Disable any unnecessary services
- Install UFW (firewall) and open only necessary ports
- Secure SSH ensuring the following is not permitted:
 - o SSH with empty password
 - o SSH with root user
 - o SSH with ports other than port 22
- Enable SSH protocol 2
- Enforce strong password policies
- Audit and restrict file and directory permissions with chown and chmod
- Lock or remove inactive user accounts

5.2 Operational

- schedule and maintain robust initial system hardening, including ensuring unnecessary services are not installed and/or running.
 - schedule and maintain patching of the system.
 - schedule backup recovery testing.
 - monitor logs to enhance operational visibility.
 - Install Lynis to perform a security audit
 - Install tripwire to provide real-time change intelligence and threat detection.
-

6. Conclusion

The audit identified critical vulnerabilities and security gaps that pose significant risks to BSC. Immediate action is required to address, mitigate and correct these issues, especially around security. Corrections have been made to limit and prevent many of these vulnerabilities, however, it is in BSC's best interest to create policies and procedures moving forward.

7. Appendices

A. Hardening Summary and Checklist.....	6
B. Hardening Script 1.....	14
C. Hardening Script 2.....	17
D. Screenshots.....	18
E. Preliminary Documentation (rough notes).....	88
F. Preliminary Audit Report (rough notes).....	96

Bibliography

Anicas M, Heidi E. UFW Essentials: Common Firewall Rules and Commands. DigitalOcean. Published December 15, 2021. <https://www.digitalocean.com/community/tutorials/ufw-essentials-common-firewall-rules-and-commands>

BashGuide.; 2024. Accessed December 20, 2024.
<https://geirha.folk.ntnu.no/bashguide.pdf>

Barrett DJ. Efficient Linux at the Command Line. “O'Reilly Media, Inc.”; 2022.

Barrett DJ. Linux Pocket Guide. “O'Reilly Media, Inc.”; 2024.

Boelen M. Lynis. Linux Audit. Published 2024. Accessed December 20, 2024. <https://linux-audit.com/lynis/>

OpenAI. (2024). ChatGPT [Large multimodal model]. <https://chat.openai.com/chat>

Cybersecurity and Compliance Solutions | Tripwire. www.tripwire.com.
<https://www.tripwire.com/>

Mackenzie D. GNU Coreutils. Accessed December 20, 2024.
<https://www.gnu.org/software/coreutils/manual/coreutils.pdf>

Overview of the Remote Shell RSH | SSH Academy. www.ssh.com.
<https://www.ssh.com/academy/ssh/rsh>

PerplexityAI. (2024). Perplexity [Large language model]. <https://www.perplexity.ai>
ukcybersecuritygroupLtd. What makes Telnet vulnerable? UK Cyber Security Group Ltd. Published July 11, 2023. <https://www.ukcybersecurity.co.uk/blog/news-advice/what-makes-telnet-vulnerable/>

APPENDIX A: HARDENING SUMMARY AND CHECKLIST**OS Information**

Customer	Baker Street Corporation
Hostname	Baker_Street_Linux_Server hostname
OS Version	Ubuntu 22.04.5 LTS (jammy) cat /etc/os-release
Memory information	Total 15G Used 1.4G free -h
Uptime information	1.46 uptime (Noticed my screenshot was wrong and redid)

Checklist

Completed	Activity	Script(s) used / Tasks completed / Screenshots
✓	OS backup	<pre>sudo tar -cvpzf /baker_street_backup.tar.gz --exclude='/.bzr' --exclude='/.hg' --exclude='/.git' --exclude='/.svn' --exclude='/.bzr' --exclude='/.hg' --exclude='/.git' --exclude='/.svn' --exclude='proc' --exclude='tmp' --exclude='mnt' --exclude='sys' --exclude='dev' --exclude='run' /</pre>
✓	Auditing users and groups	<p>Remove Terminated Users and Home/files</p> <pre>sudo deluser —remove -home username sudo deluser —remove -home lestrade sudo deluser —remove -home irene sudo deluser —remove -home mary sudo deluser —remove -home gregsoon</pre> <p>Lock Account Users on Leave</p> <pre>sudo usermod -L moriarty sudo usermod -L mrs_hudson</pre> <p>Lock Password Users on Leave (extra measure)</p> <pre>sudo passwd -l moriarty sudo passwd -l mrs_hudson</pre> <p>Unlock all Users Employed</p> <pre>sudo passwd -U sherlock</pre>

JOHN MALLON

		<pre>sudo passwd -U watson sudo passwd -U mycroft sudo passwd -U toby sudo passwd -U adler</pre> Verify Locked Account Employees on Leave <pre>passwd -S moriarty passwd -S mrs_hudson</pre> Toby and Adler passwordless account, set password <pre>sudo passwd username password sudo passwd toby Pa\$\$w0rd sudo passwd adler Pa\$\$w0rd</pre> Confirm unlocked accounts <pre>passwd -S toby passwd -S adler</pre> List Groups <pre>cat /etc/group</pre> Check members marketing group <pre>getent group marketing NO MEMBERS</pre> Delete marketing group <pre>group del marketing</pre> Create group research
--	--	--

PROJECT 1 – HARDENING A LINUX SERVER

		<p>sudo groupadd research</p> <p>According to Assistant Instructor, add all employed and temporary leave employees to research</p> <p>sudo gpasswd -a username research</p> <p>sudo gpasswd -a sherlock research</p> <p>sudo gpasswd -a watson research</p> <p>sudo gpasswd -a mycroft research</p> <p>sudo gpasswd -a moriarty research</p> <p>sudo gpasswd -a mrs_hudson research</p> <p>sudo gpasswd -a toby research</p> <p>sudo gpasswd -a adler research</p> <p>Check membership of research</p> <p>getent group research</p>
<input checked="" type="checkbox"/>	Updating and enforcing password policies	<p>sudo nano /etc/pam.d/common-password</p> <p>password requisite pam_pwquality.so retry=2 minlen=8 uccredit=-1 occredit=-1</p>
<input checked="" type="checkbox"/>	Updating and enforcing sudo permissions	<p>sudo visudo</p> <p>sherlock ALL=(ALL:ALL) ALL under root</p> <p>Comment out admin</p> <p>Comment out sudo ALL....</p>

JOHN MALLON

		<p>watson and mycroft should only run script</p> <p>watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh mycroft ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh</p> <p>All users in research group may run following</p> <p>%research ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh</p>
✓	Validating and updating permissions on files and directories	<p>ls -lar /home/* lists all users files in their home</p> <p>Remove any world permissions for every user (assuming sysadmin applies)</p> <pre>chmod -o=rwx * /home/adler/ chmod -o=rwx * /home/moriarty/ chmod -o=rwx * /home/mrs_hudson/ chmod -o=rwx * /home/mycroft/ chmod -o=rwx * /home/sherlock/ chmod -o=rwx * /home/sysadmin/ chmod -o=rwx * /home/toby/ chmod -o=rwx * /home/watson/</pre> <p>Find engineering scripts and only members of engineering group may view, edit, or execute</p> <pre>From /home/# find /home -type f -iname "*engineering*"</pre> <p>For each user home directory</p> <pre>chmod o-rwx *Engineering*</pre> <p>Find research scripts and only members of research group may view, edit, or execute</p>

PROJECT 1 – HARDENING A LINUX SERVER

		<p>From /home/#</p> <p>Find /home -type f -iname “*research*” - no result</p> <p>Find finance scripts and only members of the finance group may view, edit, or execute</p> <p>From /home/#</p> <p>Find /home -type f -iname “*finance*”</p> <p>For each user home directory</p> <p>chmod o-rwx “*inance*”</p> <p>Find files with hidden passwords and delete</p> <p>Used cat to view txt files, etc. in employee home directories and found no passwords. Is this a real thing?</p>
<input checked="" type="checkbox"/>	Optional: Updating password hashing configuration	?????
<input checked="" type="checkbox"/>	Auditing and securing SSH	<p>nano /etc/ssh/ssd_config</p> <p>Change PermitEmptyPasswords to No</p> <p>Change PermitRootLogin No</p> <p>Comment out ports, add Port 22</p> <p>Enable SSH protocol 2 - does not say to remove 1</p> <p>At prompt#service ssh restart</p>

JOHN MALLON

PROJECT 1 – HARDENING A LINUX SERVER

<input checked="" type="checkbox"/>	<p>Reviewing and updating system packages</p>	<pre>apt update apt upgrade -y apt list --installed > package_list.txt cat package_list.txt verify contents grep "telnet" package_list.txt grep "rsh-client" package_list.txt sudo apt remove telnet } confirm removal with Sudo apt remove rsh-client } package_list2.txt apt autoremove -y (forgot - in front of y first time) Researched why they have security issues. sudo apt install ufw sudo apt install lynis sudo apt install tripwire - asks how to configure, 1 for no config. No to create/use local key passphrase Researched the hardening features these three can provide.</pre>
<input checked="" type="checkbox"/>	<p>Disabling unnecessary services</p>	<pre>system has not been booted with systemd Service --status --all > service_list.txt cat service_list.txt mysql and samba installed but not running [-] sudo apt remove mysql -client mysql -server -y sudo rm -rf /etc/mysql /var/lib/mysql /var/.log/mysql sudo apt autoremove -y sudo apt remove samba -y sudo rm -rf /etc/samba /var/lib/samba /var/log/samba sudo apt autoremove -y cd /etc/init.d rm mysql rm samba-ad-dc</pre>

JOHN MALLON

PROJECT 1 – HARDENING A LINUX SERVER

✓	Enabling and configuring logging	<pre>cd /etc/systemd/ Nano journald.conf Remove # and storage=persistent Remove # and systemMaxUse=300 cd .. nano logrotate.conf #weekly daily #rotate 4 rotate 7</pre>
✓	Scripts created	<pre>hardening_script1.sh hardening_script2.sh</pre>
✓	Scripts scheduled with cron	<p>Make scripts executable:</p> <pre>chmod +770 /usr/local/sbin/hardening_script1.sh chmod +770 /usr/local/sbin/hardening_script2.sh</pre> <p>cron -e (edit cron)</p> <p>Add following two lines</p> <pre>0 0 1 * * /usr/local/sbin/hardening_script1.sh 0 0 * * 1 /usr/local/sbin/hardening_script2.sh</pre>

APPENDIX B: HARDENING SCRIPT 1

```
#!/bin/bash

# Variable for the report output file, choose an output file name
REPORT_FILE="hardening_script1.txt"

# Output the hostname
echo "Gathering hostname..."
echo "Hostname: $(hostname)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Output the OS version
echo "Gathering OS version..."
echo "OS Version: $(cat /etc/os-release)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Output memory information
echo "Gathering memory information..."
echo "Memory Information: $(free -h)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Output uptime information
echo "Gathering uptime information..."
echo "Uptime Information: $(uptime)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Backup the OS
echo "Backing up the OS..."
```

JOHN MALLON

```
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

# Output the sudoers file to the report

echo "Gathering 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..."

sudo find /home/ -type f -perm -o=rwx -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."

sudo find / -type f -iname '*engineering*' -exec chown :engineering {}+

sudo find / -type f -iname '*engineering*' -exec chmod 770 {}+

echo "Permissions updated for Engineering scripts." >> $REPORT_FILE

printf "\n" >> $REPORT_FILE

echo "Updating permissions for Research scripts..."
```

JOHN MALLON

```
sudo find / -type f -iname '*research*' -exec chown :research {}+
sudo find / -type f -iname '*research*' -exec chmod 770 {}+
```

```
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"
sudo find / -type f -iname '*finance*' -exec chown :finance {}+
sudo find / -type f -iname '*finance*' -exec chmod 770 {}+
```

```
echo "Permissions updated for Finance scripts." >> $REPORT_FILE
printf "\n" >> $REPORT_FILE
```

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

APPENDIX C: HARDENING SCRIPT 2

```
#!/bin/bash

# Variable for the report output file, choose a NEW output file name
REPORT_FILE="hardening_script2.txt"

# Output the sshd configuration file
echo "Gathering details from 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”
sudo apt update
sudo apt upgrade -y

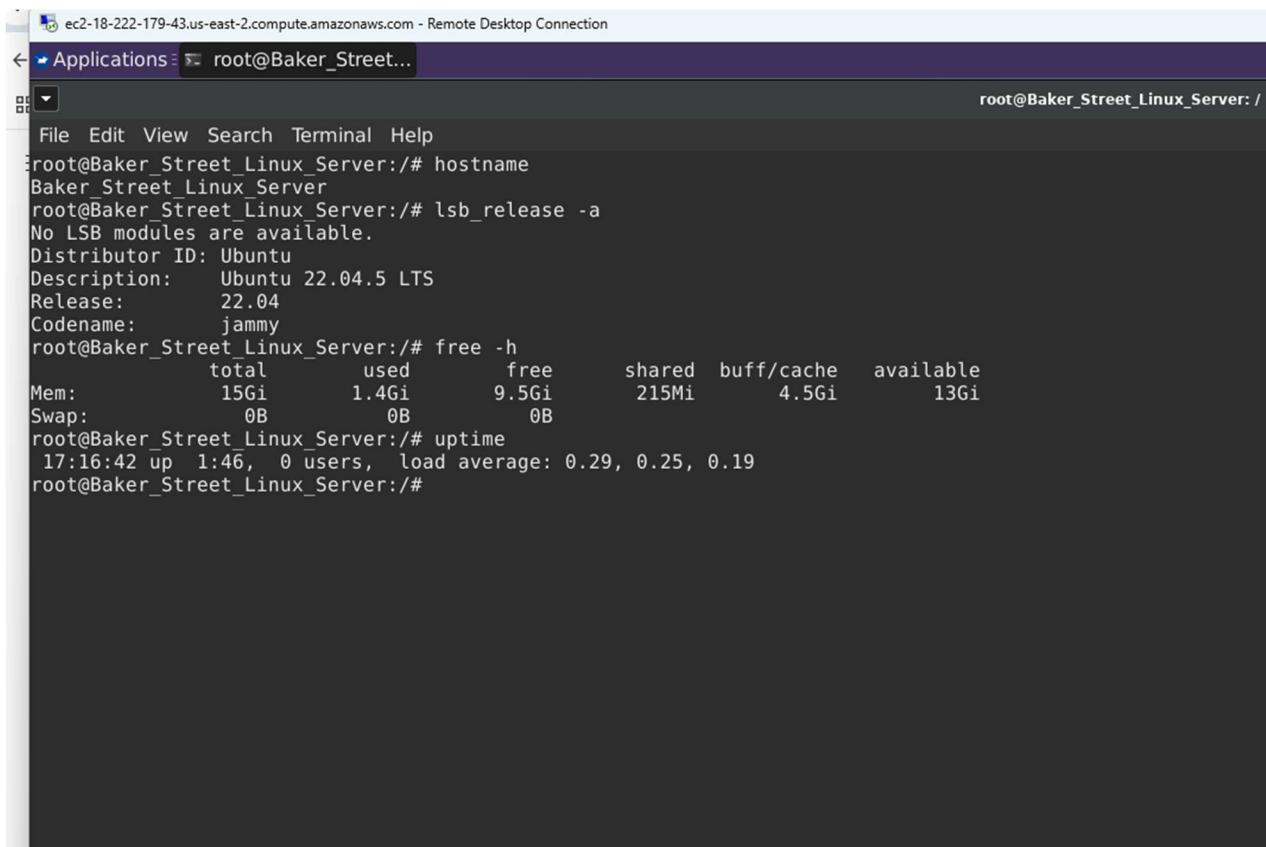
echo "Packages have been updated and upgraded" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

echo "Installed Packages:$(dpkg -l)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

echo “Printing out logging configuration data”
echo "journald.conf file data: $(cat /etc/systemd/journald.conf)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE
echo "logrotate.conf file data:$(cat /etc/systemd/logrotate.conf)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

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

JOHN MALLON

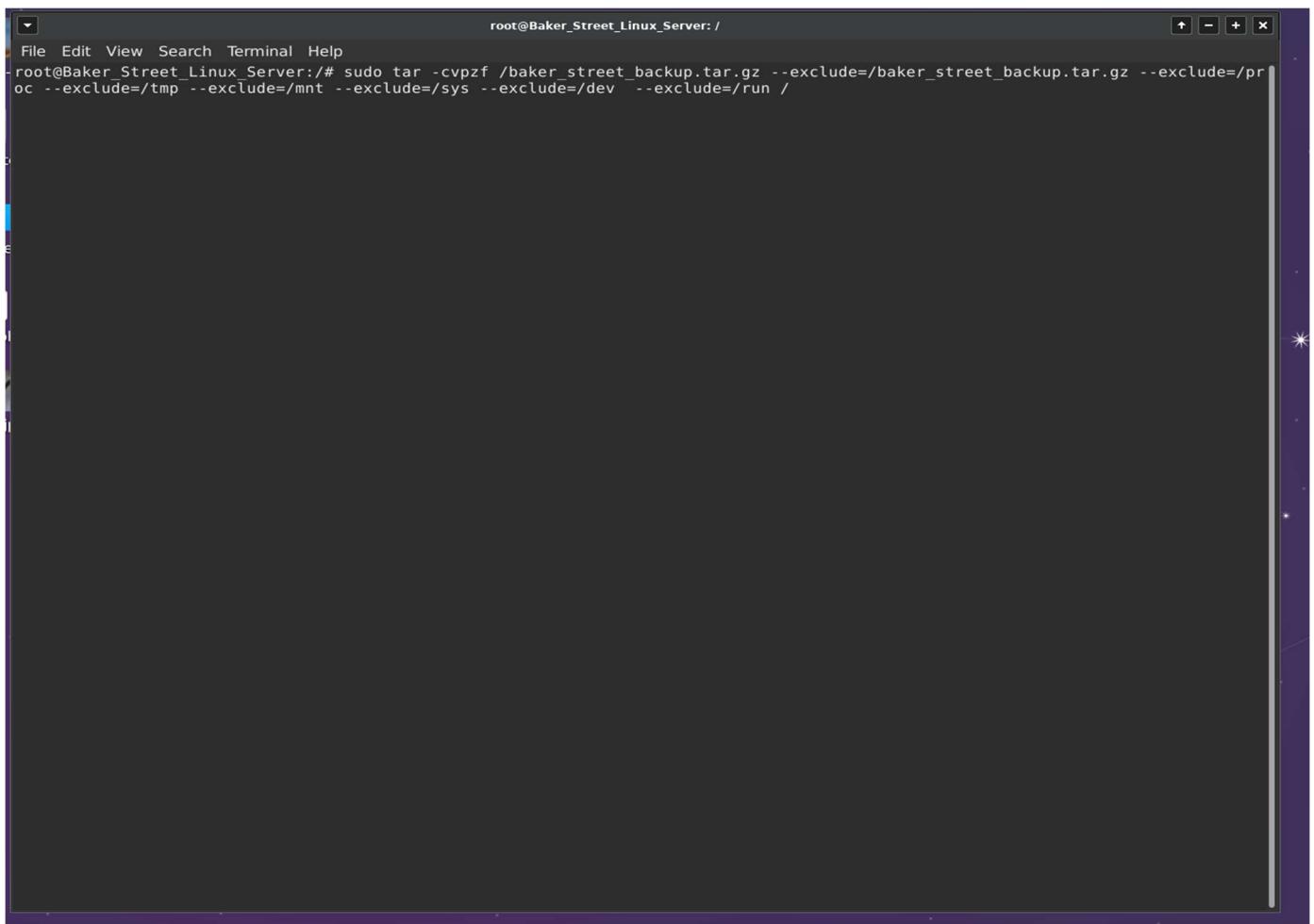
APPENDIX D: SCREENSHOTS

The screenshot shows a terminal window titled "ec2-18-222-179-43.us-east-2.compute.amazonaws.com - Remote Desktop Connection". The window title bar also includes "Applications" and "root@Baker_Street...". The terminal prompt is "root@Baker_Street_Linux_Server: /". The terminal displays the following commands and their outputs:

```
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# hostname
Baker_Street_Linux_Server
root@Baker_Street_Linux_Server:/# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 22.04 LTS
Release:        22.04
Codename:       jammy
root@Baker_Street_Linux_Server:/# free -h
              total        used        free      shared  buff/cache   available
Mem:         15Gi       1.4Gi       9.5Gi     215Mi       4.5Gi       13Gi
Swap:          0B          0B          0B
root@Baker_Street_Linux_Server:/# uptime
17:16:42 up 1:46, 0 users, load average: 0.29, 0.25, 0.19
root@Baker_Street_Linux_Server:/#
```

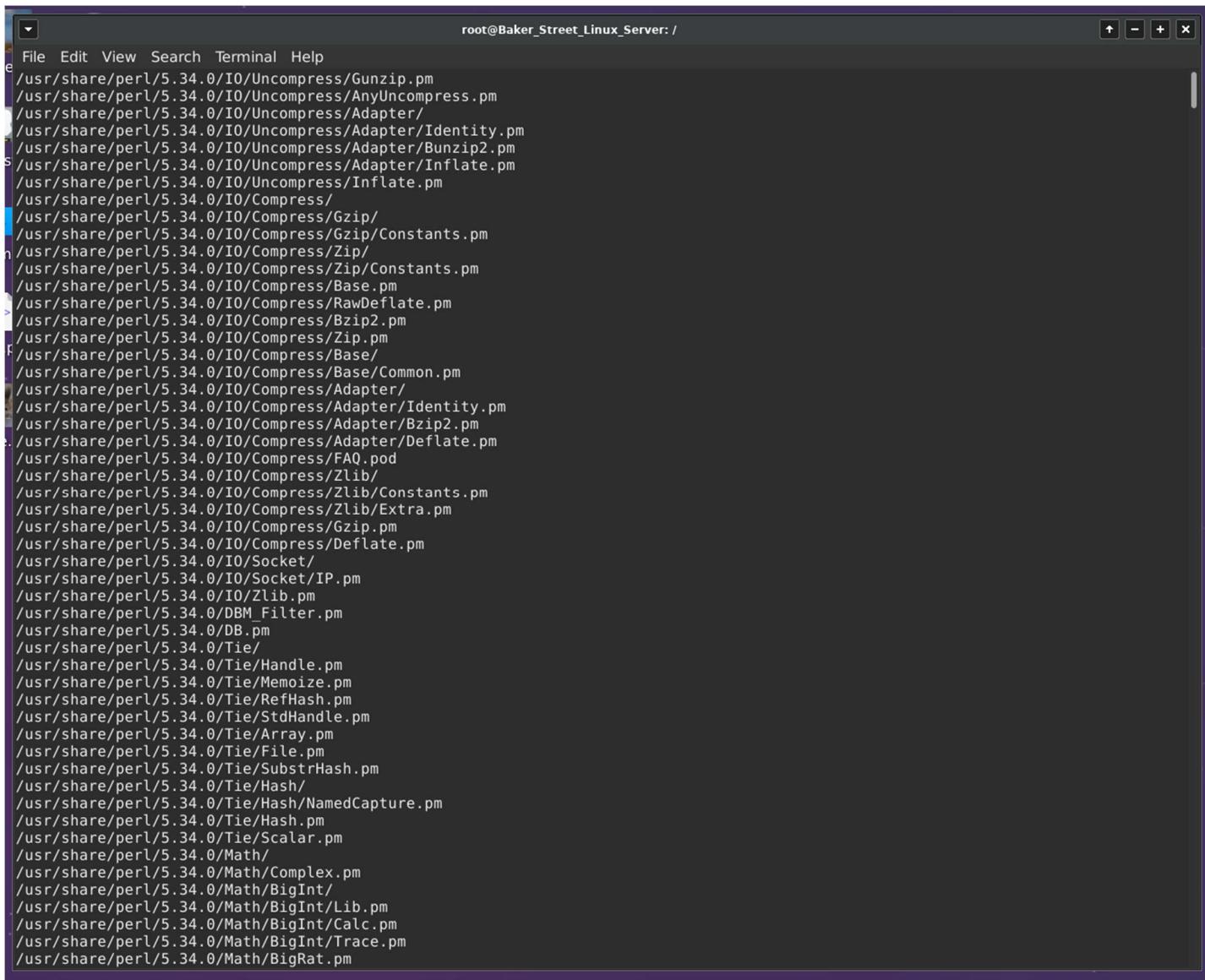
PART 1: This step obtained the Hostname, OS Version, memory information, and the uptime.

PROJECT 1 – HARDENING A LINUX SERVER



A screenshot of a terminal window titled "root@Baker_Street_Linux_Server: /". The window shows a command being entered: "root@Baker_Street_Linux_Server:/# 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 /". The terminal has a dark background and light-colored text.

This command completed the OS backup.



The screenshot shows a terminal window with a dark theme. The title bar reads "root@Baker_Street_Linux_Server: /". The window contains a list of file paths under "/usr/share/perl/5.34.0/IO/Compress/" and "/usr/share/perl/5.34.0/Math/". The files listed include various compression and mathematical modules like Gunzip.pm, AnyUncompress.pm, Uncompress.pm, Adapter.pm, Identity.pm, Bunzip2.pm, Inflate.pm, Inflate.pm, Compress.pm, Gzip.pm, Constants.pm, Zip.pm, Zip.pm, Base.pm, RawDeflate.pm, Bzip2.pm, Zip.pm, Compress.pm, Base.pm, Common.pm, Adapter.pm, Identity.pm, Bzip2.pm, Deflate.pm, FAQ.pod, Zlib.pm, Zlib.pm, Constants.pm, Extra.pm, Gzip.pm, Deflate.pm, Socket.pm, IP.pm, Zlib.pm, DBM_Filter.pm, DB.pm, Tie.pm, Handle.pm, Memoize.pm, RefHash.pm, StdHandle.pm, Array.pm, File.pm, SubstrHash.pm, Hash.pm, Hash.pm, NamedCapture.pm, Hash.pm, Scalar.pm, Math.pm, Complex.pm, BigInt.pm, Lib.pm, Calc.pm, BigInt.pm, Trace.pm, BigRat.pm.

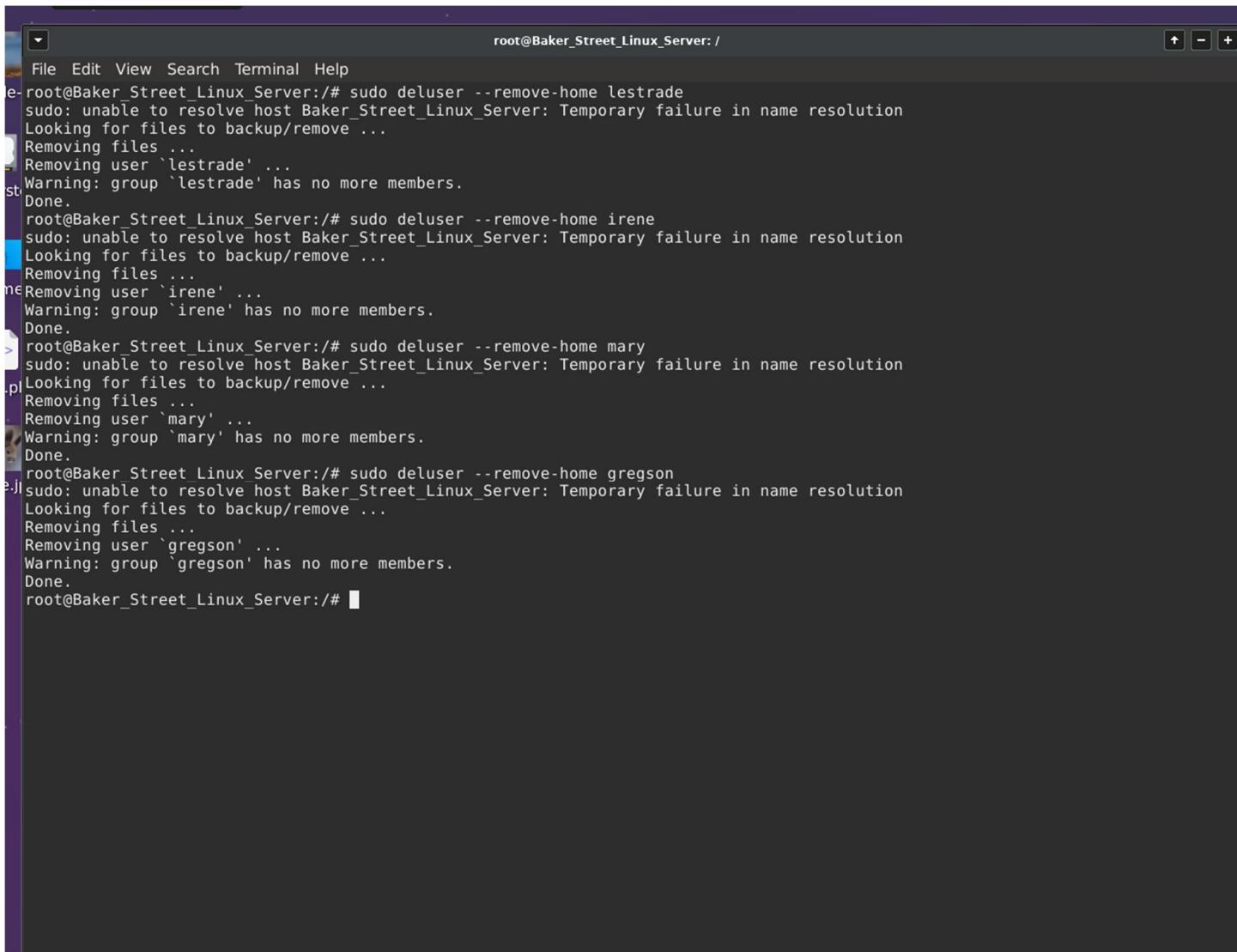
```
File Edit View Search Terminal Help
/usr/share/perl/5.34.0/IO/Uncompress/Gunzip.pm
/usr/share/perl/5.34.0/IO/Uncompress/AnyUncompress.pm
/usr/share/perl/5.34.0/IO/Uncompress/Adapter/
/usr/share/perl/5.34.0/IO/Uncompress/Adapter/Identity.pm
/usr/share/perl/5.34.0/IO/Uncompress/Adapter/Bunzip2.pm
/usr/share/perl/5.34.0/IO/Uncompress/Adapter/Inflate.pm
/usr/share/perl/5.34.0/IO/Uncompress/Inflate.pm
/usr/share/perl/5.34.0/IO/Compress/
/usr/share/perl/5.34.0/IO/Compress/Gzip/
/usr/share/perl/5.34.0/IO/Compress/Gzip/Constants.pm
/usr/share/perl/5.34.0/IO/Compress/Zip/
/usr/share/perl/5.34.0/IO/Compress/Zip/Constants.pm
/usr/share/perl/5.34.0/IO/Compress/Base.pm
/usr/share/perl/5.34.0/IO/Compress/RawDeflate.pm
/usr/share/perl/5.34.0/IO/Compress/Bzip2.pm
/usr/share/perl/5.34.0/IO/Compress/Zip.pm
/usr/share/perl/5.34.0/IO/Compress/Base/
/usr/share/perl/5.34.0/IO/Compress/Base/Common.pm
/usr/share/perl/5.34.0/IO/Compress/Adapter/
/usr/share/perl/5.34.0/IO/Compress/Adapter/Identity.pm
/usr/share/perl/5.34.0/IO/Compress/Adapter/Bzip2.pm
/usr/share/perl/5.34.0/IO/Compress/Adapter/Deflate.pm
/usr/share/perl/5.34.0/IO/Compress/FAQ.pod
/usr/share/perl/5.34.0/IO/Compress/Zlib/
/usr/share/perl/5.34.0/IO/Compress/Zlib/Constants.pm
/usr/share/perl/5.34.0/IO/Compress/Zlib/Extra.pm
/usr/share/perl/5.34.0/IO/Compress/Gzip.pm
/usr/share/perl/5.34.0/IO/Compress/Deflate.pm
/usr/share/perl/5.34.0/IO/Socket/
/usr/share/perl/5.34.0/IO/Socket/IP.pm
/usr/share/perl/5.34.0/IO/Zlib.pm
/usr/share/perl/5.34.0/DBM_Filter.pm
/usr/share/perl/5.34.0/DB.pm
/usr/share/perl/5.34.0/Tie/
/usr/share/perl/5.34.0/Tie/Handle.pm
/usr/share/perl/5.34.0/Tie/Memoize.pm
/usr/share/perl/5.34.0/Tie/RefHash.pm
/usr/share/perl/5.34.0/Tie/StdHandle.pm
/usr/share/perl/5.34.0/Tie/Array.pm
/usr/share/perl/5.34.0/Tie/File.pm
/usr/share/perl/5.34.0/Tie/SubstrHash.pm
/usr/share/perl/5.34.0/Tie/Hash/
/usr/share/perl/5.34.0/Tie/Hash/NamedCapture.pm
/usr/share/perl/5.34.0/Tie/Hash.pm
/usr/share/perl/5.34.0/Tie/Scalar.pm
/usr/share/perl/5.34.0/Math/
/usr/share/perl/5.34.0/Math/Complex.pm
/usr/share/perl/5.34.0/Math/BigInt/
/usr/share/perl/5.34.0/Math/BigInt/Lib.pm
/usr/share/perl/5.34.0/Math/BigInt/Calc.pm
/usr/share/perl/5.34.0/Math/BigInt/Trace.pm
/usr/share/perl/5.34.0/Math/BigRat.pm
```

Showing the OS backup progress.

PROJECT 1 – HARDENING A LINUX SERVER

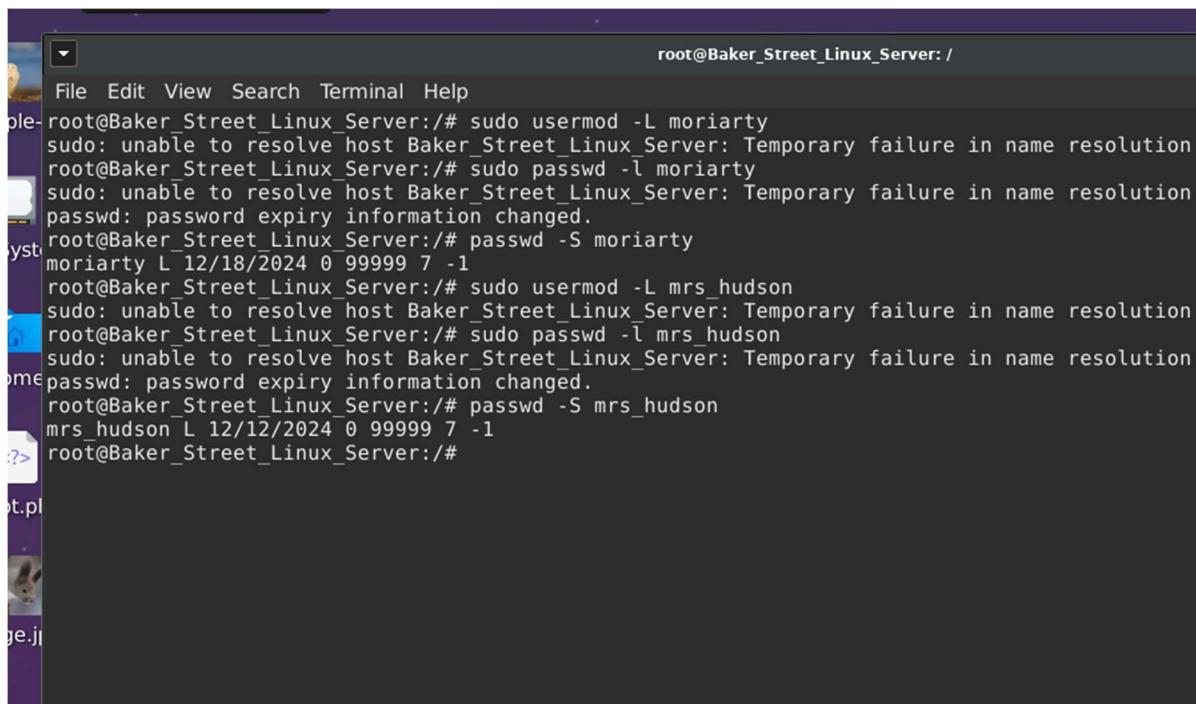
```
root@Baker_Street_Linux_Server: /  
File Edit View Search Terminal Help  
/etc/libibverbs.d/hfilverbs.driver  
/etc/libibverbs.d/mthca.driver  
/etc/libibverbs.d/ocrdma.driver  
/etc/libibverbs.d/efa.driver  
/etc/libibverbs.d/bnxt_re.driver  
/etc/libibverbs.d/cxgb4.driver  
/etc/libibverbs.d/siw.driver  
/etc/libibverbs.d/ipathverbs.driver  
/etc/libibverbs.d/vmw_pvrdma.driver  
/etc/libibverbs.d/qedr.driver  
/etc/iproute2/  
/etc/iproute2/ematch_map  
/etc/iproute2/bpf_pinning  
/etc/iproute2/rt_tables  
/etc/iproute2/rt_protos  
/etc/iproute2/rt_protos.d/  
/etc/iproute2/rt_protos.d/README  
/etc/iproute2/rt_tables.d/  
/etc/iproute2/rt_tables.d/README  
/etc/iproute2/rt_scopes  
/etc/iproute2/group  
/etc/iproute2/nl_protos  
/etc/iproute2/rt_realms  
/etc/iproute2/rt_dsfield  
/etc/libnl-3/  
/etc/libnl-3/pktloc  
/etc/libnl-3/classid  
/etc/rpc  
/etc/ufw/  
/etc/ufw/applications.d/  
/etc/ufw/applications.d/samba  
/etc/ufw/applications.d/openssh-server  
/etc/ca-certificates.conf  
/etc/perl/  
/etc/perl/Net/  
/etc/perl/Net/libnet.cfg  
/etc/ethertypes  
/etc/cron.hourly/  
/etc/cron.hourly/.placeholder  
/etc/dbus-1/  
/etc/dbus-1/system.d/  
/etc/dbus-1/session.d/  
/etc/python3.10/  
/etc/python3.10/sitecustomize.py  
/boot/  
/media/  
/lib32  
/sbin  
.dockerenv  
tar: ./ file changed as we read it  
root@Baker_Street_Linux_Server:/#
```

Shows completion of backup progress.



```
root@Baker_Street_Linux_Server:/# sudo deluser --remove-home lestrade
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Looking for files to backup/remove ...
Removing files ...
Removing user `lestrade' ...
Warning: group `lestrade' has no more members.
Done.
root@Baker_Street_Linux_Server:/# sudo deluser --remove-home irene
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Looking for files to backup/remove ...
Removing files ...
Removing user `irene' ...
Warning: group `irene' has no more members.
Done.
root@Baker_Street_Linux_Server:/# sudo deluser --remove-home mary
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Looking for files to backup/remove ...
Removing files ...
Removing user `mary' ...
Warning: group `mary' has no more members.
Done.
root@Baker_Street_Linux_Server:/# sudo deluser --remove-home gregson
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Looking for files to backup/remove ...
Removing files ...
Removing user `gregson' ...
Warning: group `gregson' has no more members.
Done.
root@Baker_Street_Linux_Server:/#
```

Part 2: Auditing Users and Groups. This step is deleting the all staff that has been terminated, including any files, home directories and groups.

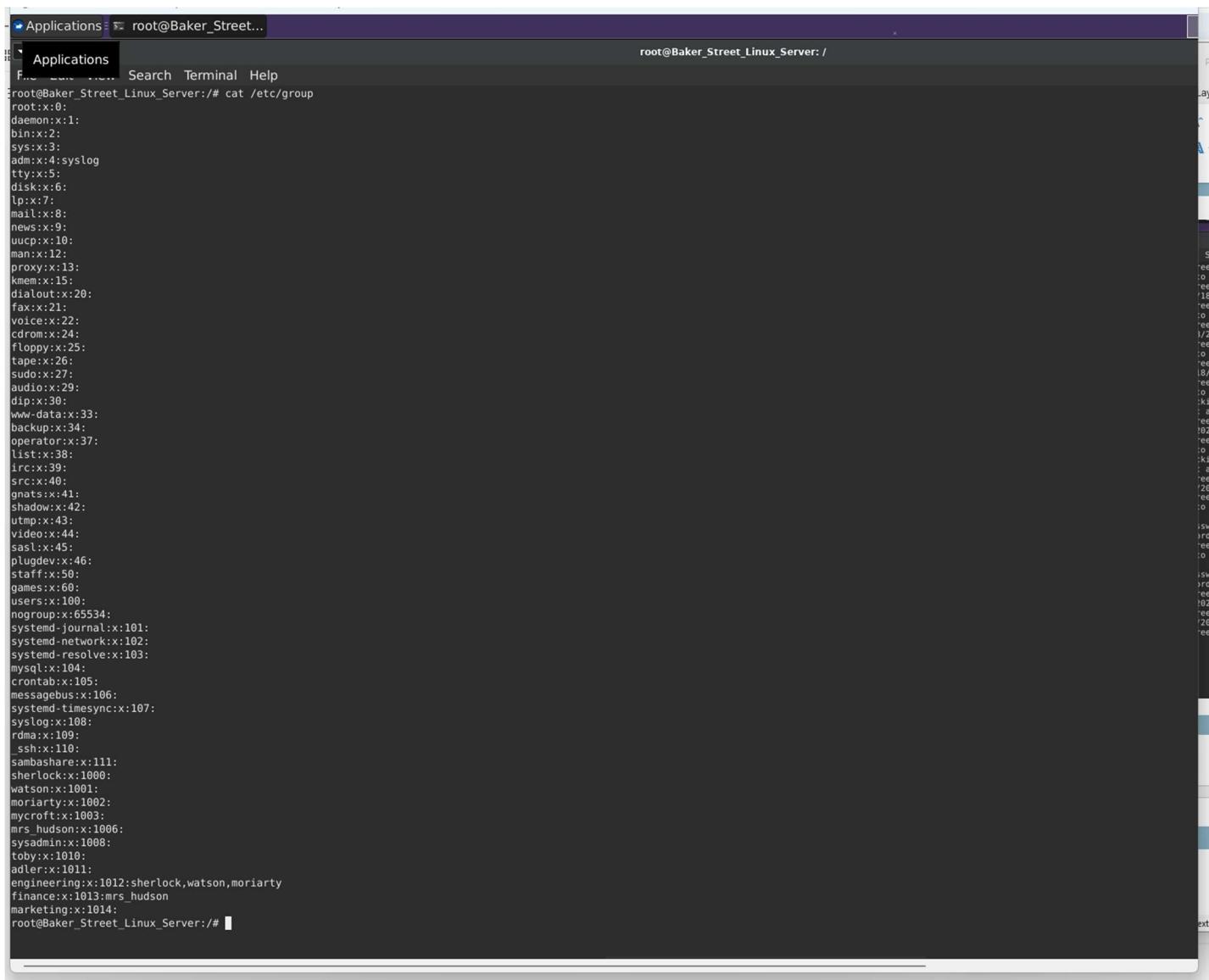


A screenshot of a terminal window titled "root@Baker_Street_Linux_Server:/". The terminal shows the following command-line session:

```
root@Baker_Street_Linux_Server:/# sudo usermod -L moriarty
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
root@Baker_Street_Linux_Server:/# sudo passwd -l moriarty
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
passwd: password expiry information changed.
root@Baker_Street_Linux_Server:/# passwd -S moriarty
moriarty L 12/18/2024 0 99999 7 -1
root@Baker_Street_Linux_Server:/# sudo usermod -L mrs_hudson
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
root@Baker_Street_Linux_Server:/# sudo passwd -l mrs_hudson
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
passwd: password expiry information changed.
root@Baker_Street_Linux_Server:/# passwd -S mrs_hudson
mrs_hudson L 12/12/2024 0 99999 7 -1
root@Baker_Street_Linux_Server:/#
```

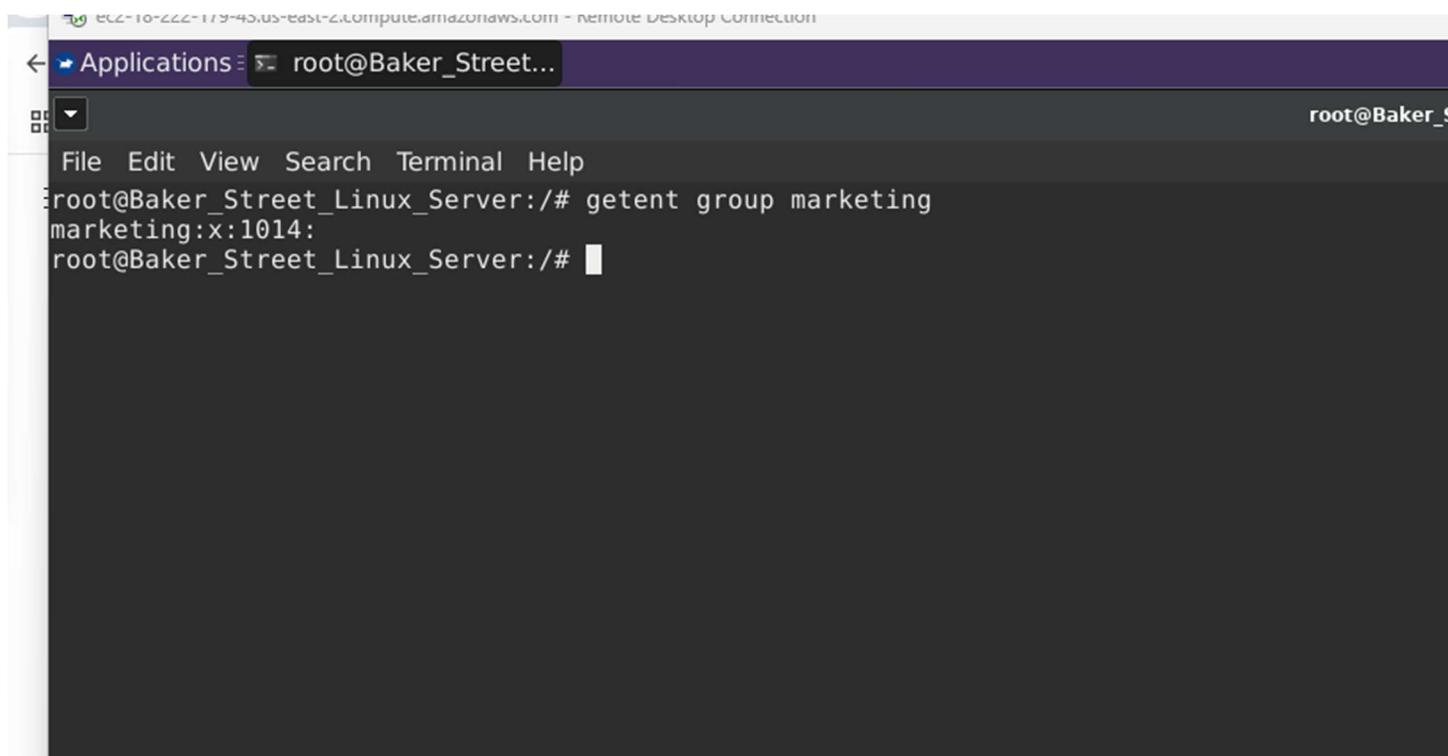
This step locks all user accounts of staff on temporary leave and unlocks any users who are employed.

PROJECT 1 – HARDENING A LINUX SERVER



```
root@Baker_Street_Linux_Server:/# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:
floppy:x:25:
tape:x:26:
sudo:x:27:
audio:x:29:
dip:x:30:
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
asl:x:45:
plugdev:x:46:
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
mysql:x:104:
crontab:x:105:
messagebus:x:106:
systemd-timesync:x:107:
syslog:x:108:
rdma:x:109:
ssh:x:110:
sambashare:x:111:
sherlock:x:1000:
watson:x:1001:
moriarty:x:1002:
mycroft:x:1003:
mrs hudson:x:1006:
sysadmin:x:1008:
toby:x:1010:
adler:x:1011:
engineering:x:1012:sherlock,watson,moriarty
finance:x:1013:mrs_hudson
marketing:x:1014:
root@Baker_Street_Linux_Server:/#
```

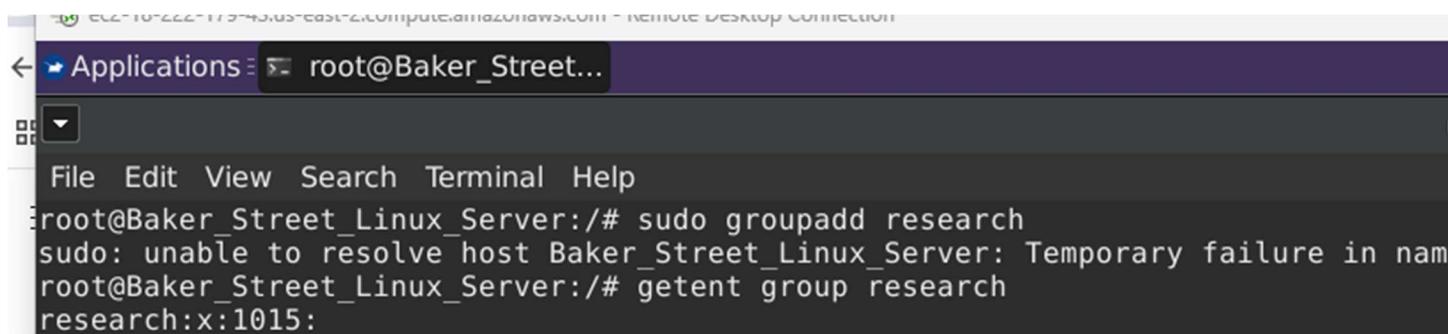
This step lists all the groups and membership of any users in these groups.



Terminal window showing a root shell on a Linux server. The user runs the command 'getent group marketing' which outputs:

```
root@Baker_Street_Linux_Server:/# getent group marketing
marketing:x:1014:
root@Baker_Street_Linux_Server:/#
```

Getting information on the group marketing.

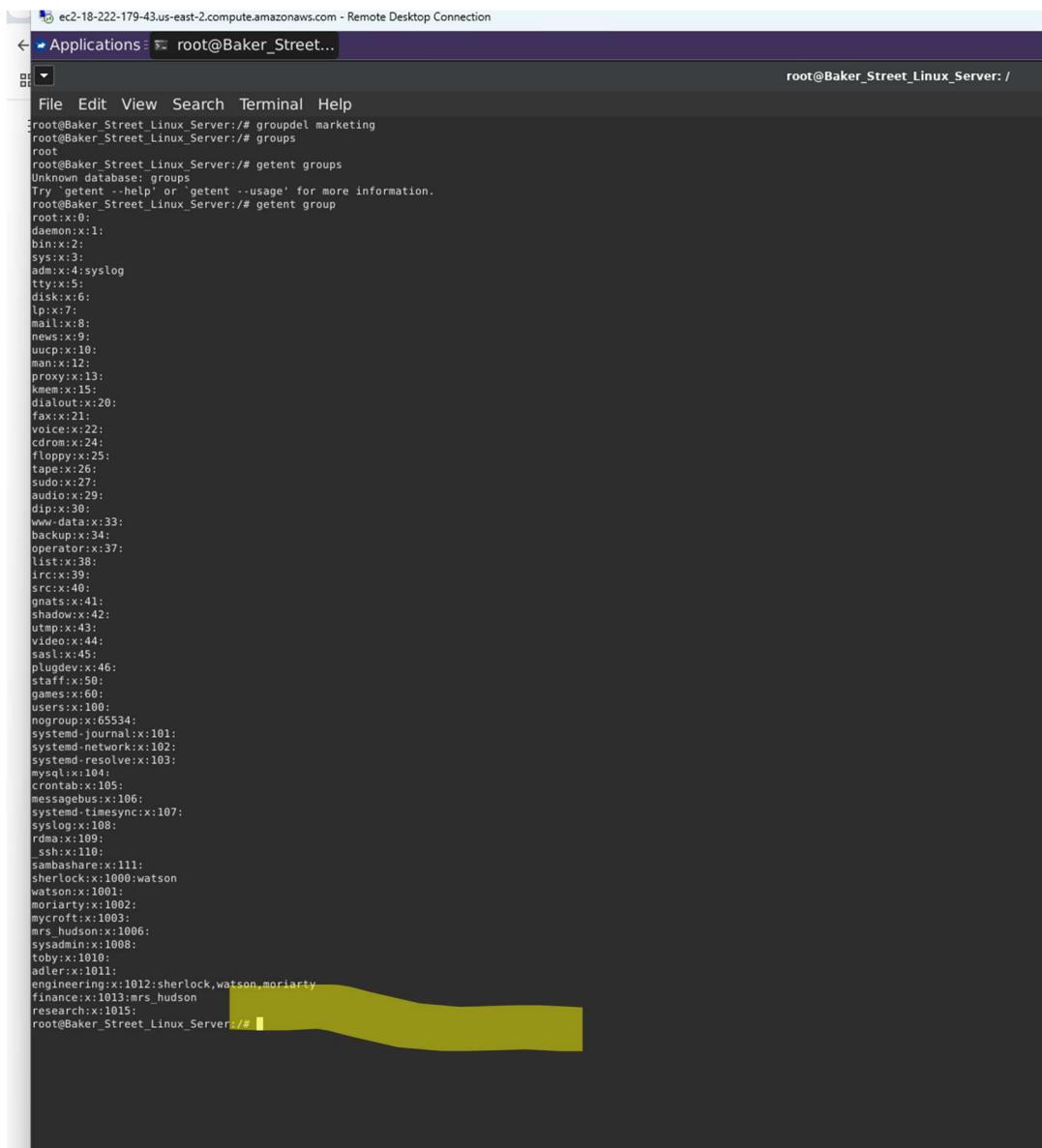


Terminal window showing a root shell on a Linux server. The user runs the command 'sudo groupadd research' which fails due to a host resolution issue, and then runs 'getent group research' which outputs:

```
root@Baker_Street_Linux_Server:/# sudo groupadd research
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
root@Baker_Street_Linux_Server:/# getent group research
research:x:1015:
```

Creating new group research.

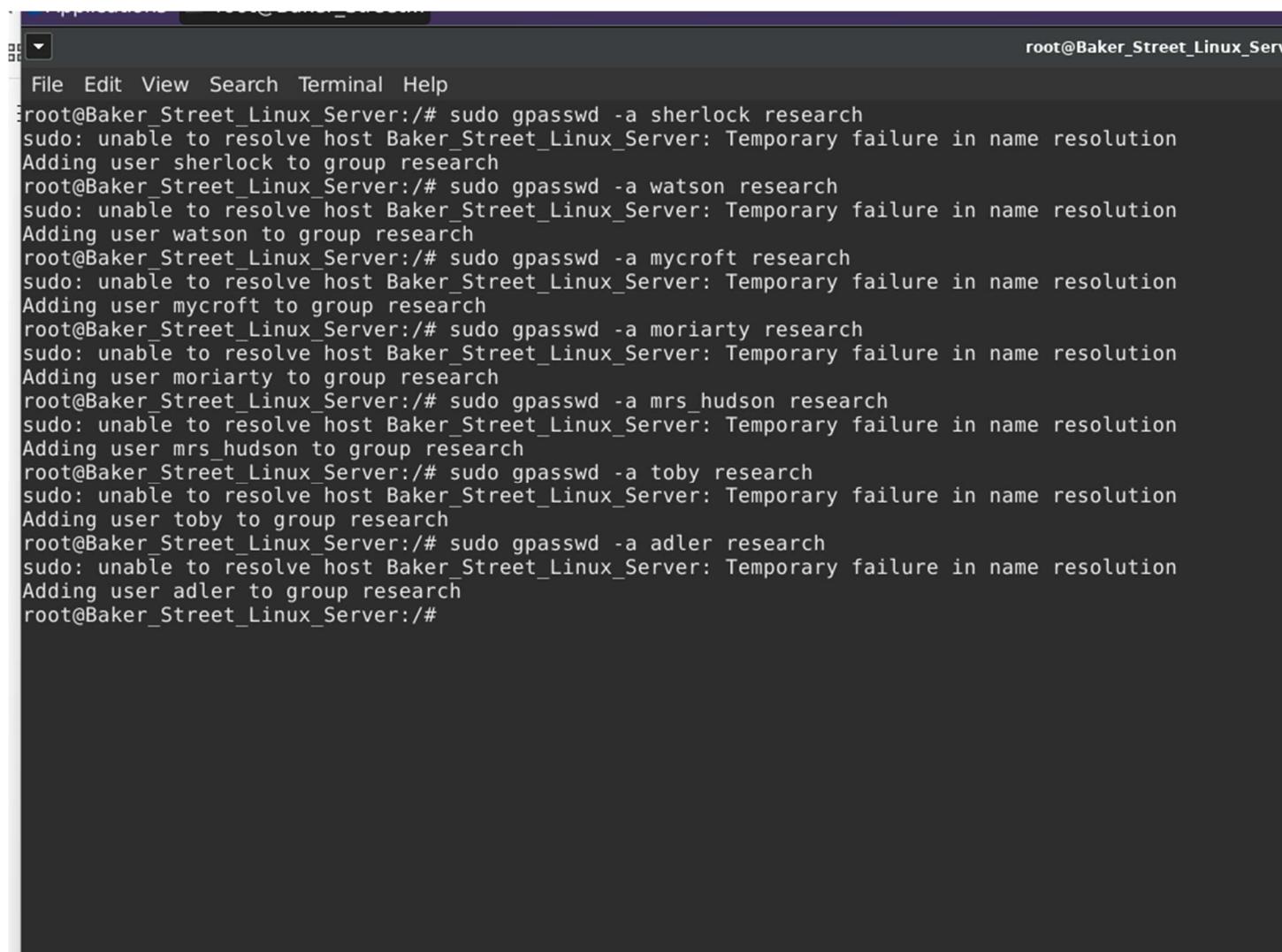
PROJECT 1 – HARDENING A LINUX SERVER



The screenshot shows a terminal window titled "Applications" with the command line "root@Baker_Street_Linux_Server: /". The terminal displays the following sequence of commands:

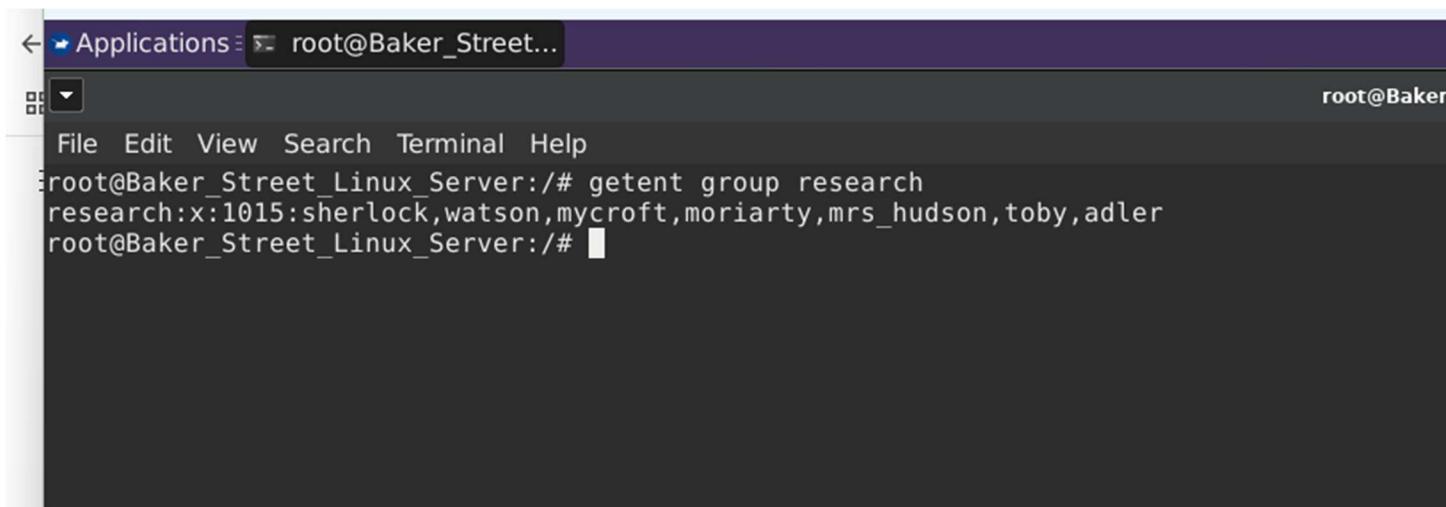
```
root@Baker_Street_Linux_Server:/# groupdel marketing
root@Baker_Street_Linux_Server:/# groups
root@Baker_Street_Linux_Server:/# getent groups
Unknown database: groups
Try 'getent --help' or 'getent --usage' for more information.
root@Baker_Street_Linux_Server:/# getent group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:
floppy:x:25:
tape:x:26:
sudo:x:27:
audio:x:29:
dip:x:30:
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
stargate:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
mysql:x:104:
crontab:x:105:
messagebus:x:106:
systemd-timesync:x:107:
syslog:x:108:
rdma:x:109:
_ssh:x:110:
sambashare:x:111:
sherlock:x:1000:watson
watson:x:1001:
moriarty:x:1002:
mycroft:x:1003:
mrs_hudson:x:1006:
sysadmin:x:1008:
toby:x:1010:
adler:x:1011:
engineering:x:1012:sherlock,watson,moriarty
finance:x:1013:mrs_hudson
research:x:1015:
root@Baker_Street_Linux_Server:/#
```

Listing all the groups on the system, deleting marketing, and showing new group research has been created.



```
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# sudo gpasswd -a sherlock research
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Adding user sherlock to group research
root@Baker_Street_Linux_Server:/# sudo gpasswd -a watson research
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Adding user watson to group research
root@Baker_Street_Linux_Server:/# sudo gpasswd -a mycroft research
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Adding user mycroft to group research
root@Baker_Street_Linux_Server:/# sudo gpasswd -a moriarty research
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Adding user moriarty to group research
root@Baker_Street_Linux_Server:/# sudo gpasswd -a mrs_hudson research
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Adding user mrs_hudson to group research
root@Baker_Street_Linux_Server:/# sudo gpasswd -a toby research
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Adding user toby to group research
root@Baker_Street_Linux_Server:/# sudo gpasswd -a adler research
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Adding user adler to group research
root@Baker_Street_Linux_Server:/#
```

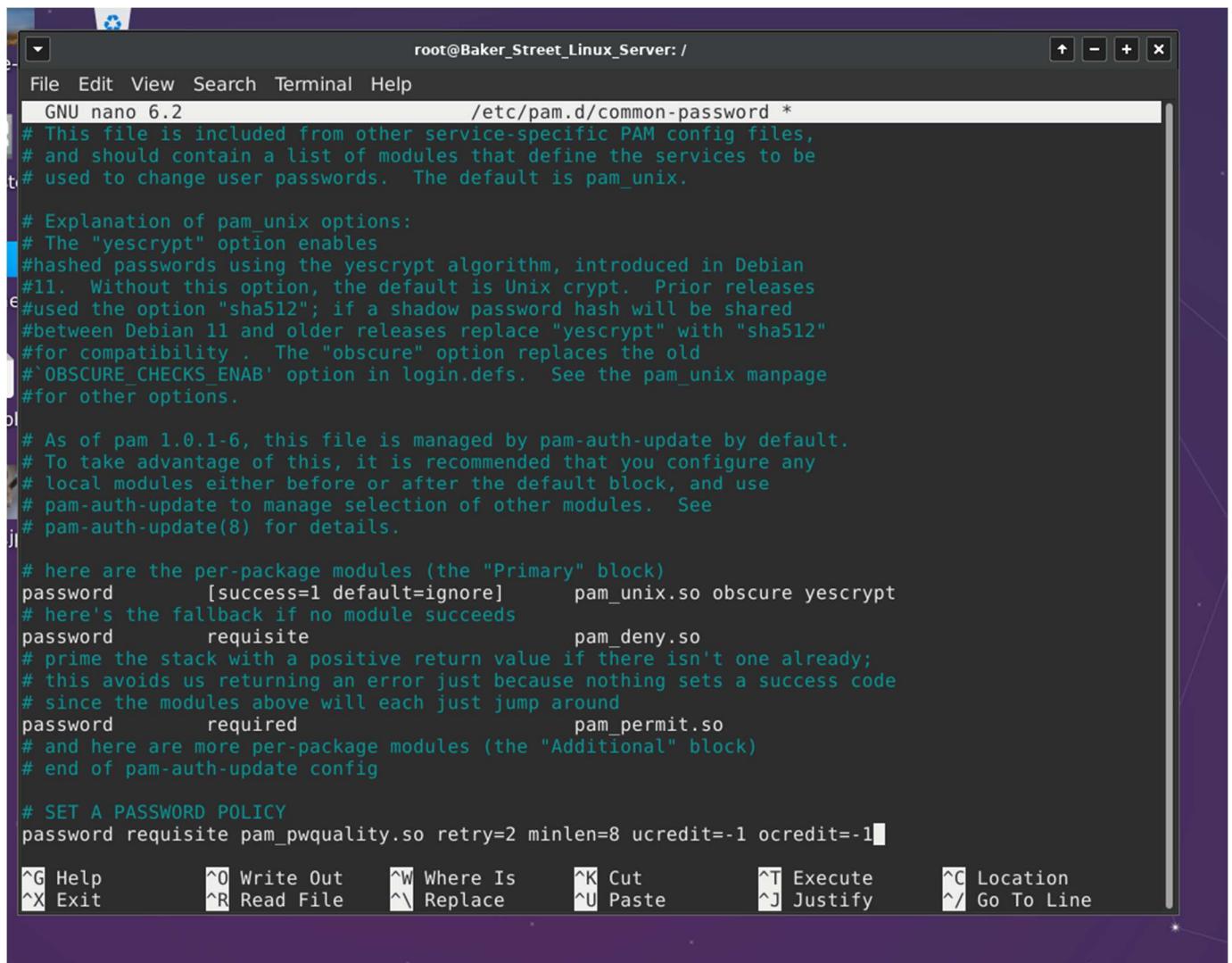
As per Assistant Instructor, all the current employees should be added to the group research.



A screenshot of a terminal window titled "root@Baker_Street...". The window shows the following command and its output:

```
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# getent group research
research:x:1015:sherlock,watson,mycroft,moriarty,mrs_hudson,toby,adler
root@Baker_Street_Linux_Server:/#
```

Listing members of research group confirming that all the current employees are members.



```

root@Baker_Street_Linux_Server: /etc/pam.d/common-password *
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.

# Explanation of pam_unix options:
# The "yescrypt" option enables
# hashed passwords using the yescrypt algorithm, introduced in Debian
# 11. Without this option, the default is Unix crypt. Prior releases
# used the option "sha512"; if a shadow password hash will be shared
# between Debian 11 and older releases replace "yescrypt" with "sha512"
# for compatibility. The "obscure" option replaces the old
# `OBSCURE_CHECKS_ENAB` option in login.defs. See the pam_unix manpage
# for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password      [success=1 default=ignore]      pam_unix.so obscure yescrypt
# here's the fallback if no module succeeds
password      requisite                  pam_deny.so
# 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      required                  pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config

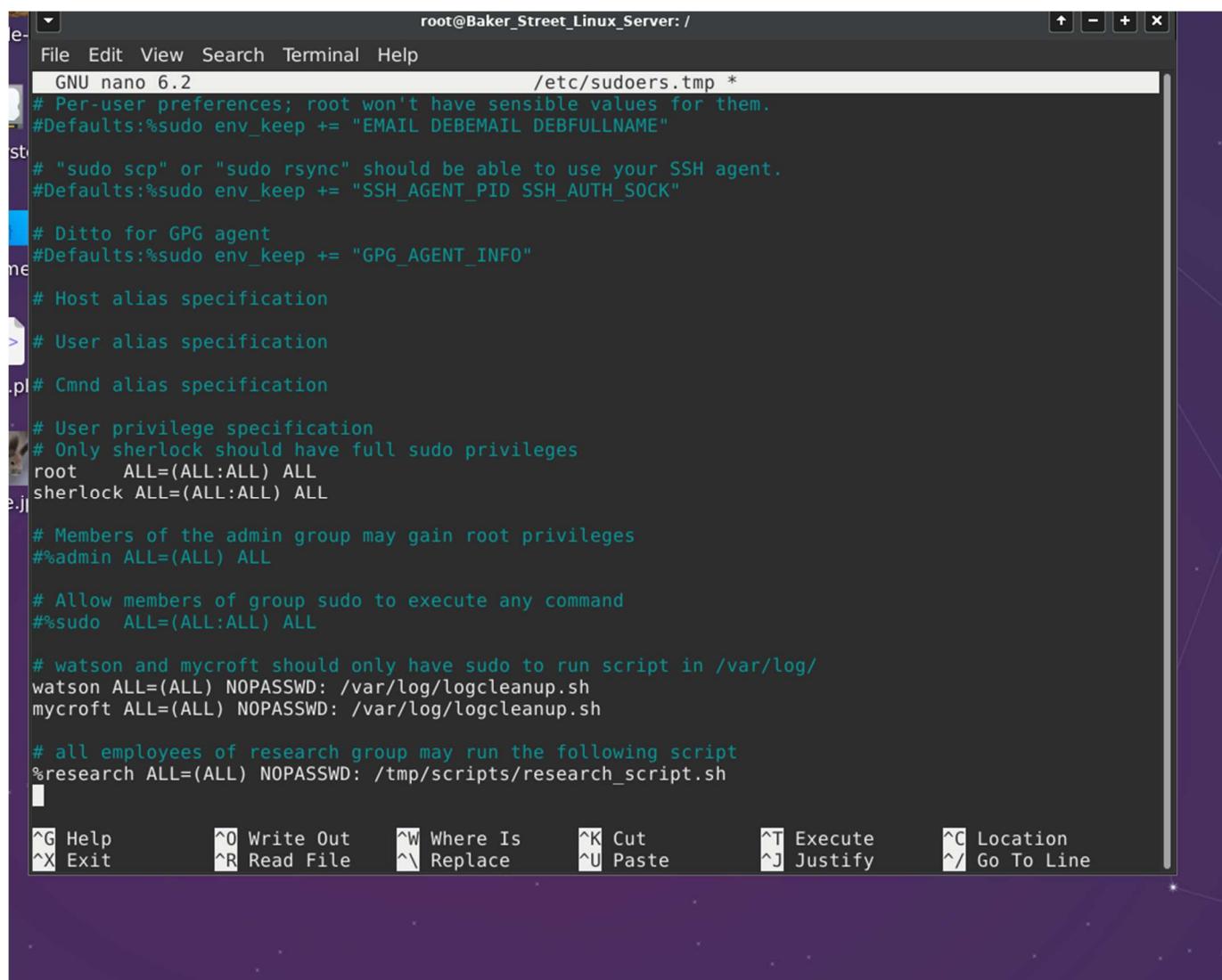
# SET A PASSWORD POLICY
password requisite pam_pwquality.so retry=2 minlen=8 ucredit=-1 ocredit=-1

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location
^X Exit         ^R Read File     ^\ Replace        ^U Paste         ^J Justify       ^/ Go To Line

```

Part 3: Updating and Enforcing Password Policies

Editing the common-password file to add minimum password requirements.



```

root@Baker_Street_Linux_Server: / 
GNU nano 6.2          /etc/sudoers.tmp *
# Per-user preferences; root won't have sensible values for them.
Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"
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
# Only sherlock should have full sudo privileges
root    ALL=(ALL:ALL) ALL
sherlock 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
# watson and mycroft should only have sudo to run script in /var/log/
watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh
mycroft ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh
# all employees of research group may run the following script
%research ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh
[G] Help      [^O] Write Out     [^W] Where Is      [^K] Cut      [^T] Execute      [^C] Location
[X] Exit      [^R] Read File     [^V] Replace      [^U] Paste      [^J] Justify      [^/]

```

Part 4: Updating and Enforcing sudo Permissions

Modifying which users can use sudo and, those that are permitted, only very specific tasks.

```

root@Baker_Street_Linux_Server:/# ls -lar /home/*
/home/watson:
total 32
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 my_file.txt
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 deduction.doc_2.txt
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 deduction.doc_1.txt
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 deduction.doc_0.txt
-t-rwxr-xr-x 1 root      root     47 Dec 12 07:45 Finance_script.sh_script2.sh
-t-rwxr-xr-x 1 root      root     47 Dec 12 07:45 Finance_script.sh_script1.sh
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 Finance_script.sh_3.txt
-t-rw-r--r-- 1 watson    watson   807 Jan  6 2022 .profile
-t-rw-r--r-- 1 watson    watson  3771 Jan  6 2022 .bashrc
-t-rw-r--r-- 1 watson    watson  220 Jan  6 2022 .bash_logout
drwxr-xr-x 1 root      root    4096 Dec 18 16:34 ..
drwxr-xr-x 1 watson    watson  4096 Dec 12 07:45 .

/home/toby:
total 32
-t-rwxr-xr-x 1 root      root    45 Dec 12 07:45 elementary.txt_script2.sh
-t-rwxr-xr-x 1 root      root    45 Dec 12 07:45 elementary.txt_script1.sh
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 elementary.txt_3.txt
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 elementary.txt_0.txt
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 deduction.doc_1.txt
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 Engineering_script.sh_2.txt
-t-rw-r--r-- 1 toby      toby    807 Jan  6 2022 .profile
-t-rw-r--r-- 1 toby      toby  3771 Jan  6 2022 .bashrc
-t-rw-r--r-- 1 toby      toby  220 Jan  6 2022 .bash_logout
drwxr-xr-x 1 root      root    4096 Dec 18 16:34 ..
drwxr-xr-x 1 toby      toby  4096 Dec 12 07:45 .

/home/sysadmin:
total 24
-t-rw-r--r-- 1 sysadmin  sysadmin  807 Jan  6 2022 .profile
-t-rw-r--r-- 1 sysadmin  sysadmin  3771 Jan  6 2022 .bashrc
-t-rw-r--r-- 1 sysadmin  sysadmin  220 Jan  6 2022 .bash_logout
drwxr-xr-x 1 root      root    4096 Dec 18 16:34 ..
drwxr-xr-x 2 sysadmin  sysadmin  4096 Dec 12 07:45 .

/home/sherlock:
total 32
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 my_file.txt
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 game_is_afoot.txt_2.txt
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 game_is_afoot.txt_1.txt
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 elementary.txt_0.txt
-t-rwxr-xr-x 1 root      root     49 Dec 12 07:45 deduction.doc_script2.sh
-t-rwxr-xr-x 1 root      root     49 Dec 12 07:45 deduction.doc_script1.sh
-t-rw-r--r-- 1 root      root      0 Dec 12 07:45 deduction.doc_3.txt
-t-rw-r--r-- 1 sherlock  sherlock  807 Jan  6 2022 .profile

```

Part 5: Validating and Updating Permissions on Files and Directories

Listing users files and the permissions.

```

root@Baker_Street_Linux_Server: / 
File Edit View Search Terminal Help
drwxr-xr-x 1 root      root      4096 Dec 18 16:34 ..
drwxr-x--- 2 sysadmin  sysadmin  4096 Dec 12 07:45 .

st/home/sherlock:
total 32
-rw-r--r-- 1 root      root      0 Dec 12 07:45 my_file.txt
-rw-r--r-- 1 root      root      0 Dec 12 07:45 game_is_afoot.txt_2.txt
-rw-r--r-- 1 root      root      0 Dec 12 07:45 game_is_afoot.txt_1.txt
-rw-r--r-- 1 root      root      0 Dec 12 07:45 elementary.txt_0.txt
-rw-r-xr-x 1 root      root     49 Dec 12 07:45 deduction.doc_script2.sh
-rw-r-xr-x 1 root      root     49 Dec 12 07:45 deduction.doc_script1.sh
-rw-r--r-- 1 root      root      0 Dec 12 07:45 deduction.doc_3.txt
-rw-r--r-- 1 sherlock  sherlock  807 Jan  6 2022 .profile
-rw-r--r-- 1 sherlock  sherlock 3771 Jan  6 2022 .bashrc
pl-rw-r--r-- 1 sherlock  sherlock 220 Jan  6 2022 .bash_logout
drwxr-xr-x 1 root      root      4096 Dec 18 16:34 ..
drwxr-x--- 1 sherlock  sherlock  4096 Dec 12 07:45 .

/home/mycroft:
total 32
-rw-r--r-- 1 root      root      0 Dec 12 07:45 deduction.doc_2.txt
-rw-r--r-- 1 root      root      0 Dec 12 07:45 deduction.doc_1.txt
-rwxr-xr-x 1 root      root     48 Dec 12 07:45 Finance_script.sh_script2.sh
-rwxr-xr-x 1 root      root     48 Dec 12 07:45 Finance_script.sh_script1.sh
-rw-r--r-- 1 root      root      0 Dec 12 07:45 Finance_script.sh_3.txt
-rw-r--r-- 1 root      root      0 Dec 12 07:45 Engineering_script.sh_0.txt
-rw-r--r-- 1 mycroft  mycroft  807 Jan  6 2022 .profile
-rw-r--r-- 1 mycroft  mycroft 3771 Jan  6 2022 .bashrc
-rw-r--r-- 1 mycroft  mycroft 220 Jan  6 2022 .bash_logout
drwxr-xr-x 1 root      root      4096 Dec 18 16:34 ..
drwxr-x--- 1 mycroft  mycroft  4096 Dec 12 07:45 .

/home/mrs_hudson:
total 32
-rwxr-xr-x 1 root      root      51 Dec 12 07:45 elementary.txt_script2.sh
-rwxr-xr-x 1 root      root      51 Dec 12 07:45 elementary.txt_script1.sh
-rw-r--r-- 1 root      root      0 Dec 12 07:45 elementary.txt_3.txt
-rw-r--r-- 1 root      root      0 Dec 12 07:45 deduction.doc_2.txt
-rw-r--r-- 1 root      root      0 Dec 12 07:45 deduction.doc_0.txt
-rw-r--r-- 1 root      root      0 Dec 12 07:45 Engineering_script.sh_1.txt
-rw-r--r-- 1 mrs_hudson mrs_hudson 807 Jan  6 2022 .profile
-rw-r--r-- 1 mrs_hudson mrs_hudson 3771 Jan  6 2022 .bashrc
-rw-r--r-- 1 mrs_hudson mrs_hudson 220 Jan  6 2022 .bash_logout
drwxr-xr-x 1 root      root      4096 Dec 18 16:34 ..
drwxr-x--- 1 mrs_hudson mrs_hudson 4096 Dec 12 07:45 .

/home/moriarty:
total 32

```

Continuing to list the users files and permissions.

```

root@Baker_Street_Linux_Server: /
File Edit View Search Terminal Help
-rw-r--r-- 1 mycroft mycroft 3771 Jan  6 2022 .bashrc
-rw-r--r-- 1 mycroft mycroft 220 Jan  6 2022 .bash_logout
drwxr-xr-x 1 root    root   4096 Dec 18 16:34 ..
drwxr-x--- 1 mycroft mycroft 4096 Dec 12 07:45 .

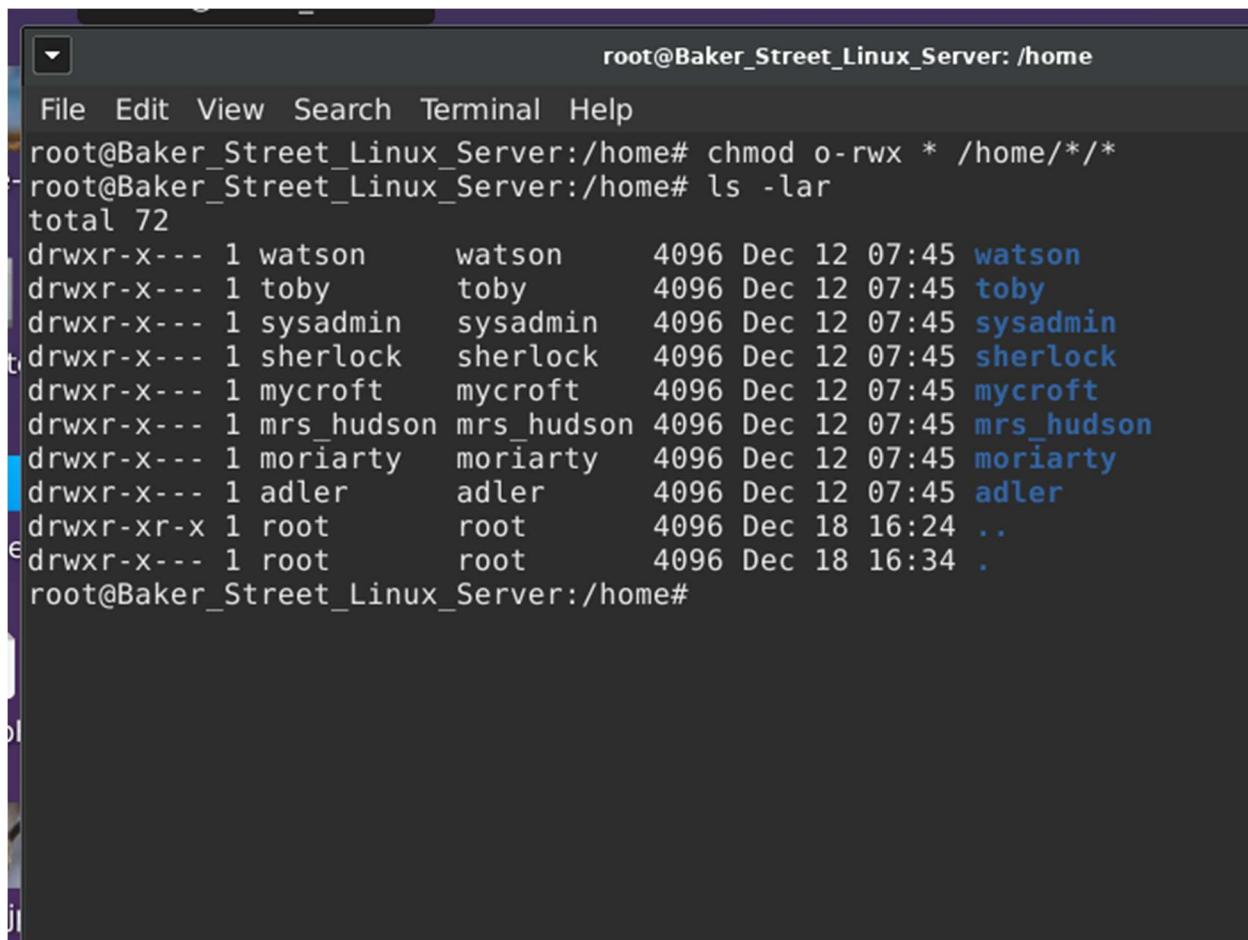
/home/mrs_hudson:
total 32
-rwxr-xr-x 1 root    root   51 Dec 12 07:45 elementary.txt_script2.sh
-rwxr-xr-x 1 root    root   51 Dec 12 07:45 elementary.txt_script1.sh
-rw-r--r-- 1 root    root   0 Dec 12 07:45 elementary.txt_3.txt
-rw-r--r-- 1 root    root   0 Dec 12 07:45 deduction.doc_2.txt
-rw-r--r-- 1 root    root   0 Dec 12 07:45 deduction.doc_0.txt
-rw-r--r-- 1 root    root   0 Dec 12 07:45 Engineering_script.sh_1.txt
-rw-r--r-- 1 mrs_hudson mrs_hudson 807 Jan  6 2022 .profile
-rw-r--r-- 1 mrs_hudson mrs_hudson 3771 Jan  6 2022 .bashrc
-rw-r--r-- 1 mrs_hudson mrs_hudson 220 Jan  6 2022 .bash_logout
drwxr-xr-x 1 root    root   4096 Dec 18 16:34 ..
drwxr-x--- 1 mrs_hudson mrs_hudson 4096 Dec 12 07:45 .

/home/moriarty:
total 32
-rw-r--r-- 1 root    root   0 Dec 12 07:45 my_file.txt
-rwxr-xr-x 1 root    root   49 Dec 12 07:45 game_is_afoot.txt_script2.sh
-rwxr-xr-x 1 root    root   49 Dec 12 07:45 game_is_afoot.txt_script1.sh
-rw-r--r-- 1 root    root   0 Dec 12 07:45 game_is_afoot.txt_3.txt
-rw-r--r-- 1 root    root   0 Dec 12 07:45 elementary.txt_1.txt
-rw-r--r-- 1 root    root   0 Dec 12 07:45 Finance_script.sh_2.txt
-rw-r--r-- 1 root    root   0 Dec 12 07:45 Finance_script.sh_0.txt
-rw-r--r-- 1 moriarty moriarty 807 Jan  6 2022 .profile
-rw-r--r-- 1 moriarty moriarty 3771 Jan  6 2022 .bashrc
-rw-r--r-- 1 moriarty moriarty 220 Jan  6 2022 .bash_logout
drwxr-xr-x 1 root    root   4096 Dec 18 16:34 ..
drwxr-x--- 1 moriarty moriarty 4096 Dec 12 07:45 .

/home/adler:
total 32
-rw-r--r-- 1 root    root   0 Dec 12 07:45 game_is_afoot.txt_1.txt
-rw-r--r-- 1 root    root   0 Dec 12 07:45 deduction.doc_2.txt
-rwxr-xr-x 1 root    root   46 Dec 12 07:45 Engineering_script.sh_script2.sh
-rwxr-xr-x 1 root    root   46 Dec 12 07:45 Engineering_script.sh_script1.sh
-rw-r--r-- 1 root    root   0 Dec 12 07:45 Engineering_script.sh_3.txt
-rw-r--r-- 1 root    root   0 Dec 12 07:45 Engineering_script.sh_0.txt
-rw-r--r-- 1 adler   adler  807 Jan  6 2022 .profile
-rw-r--r-- 1 adler   adler  3771 Jan  6 2022 .bashrc
-rw-r--r-- 1 adler   adler  220 Jan  6 2022 .bash_logout
drwxr-xr-x 1 root    root   4096 Dec 18 16:34 ..
drwxr-x--- 1 adler   adler  4096 Dec 12 07:45 .
root@Baker_Street_Linux_Server:/#

```

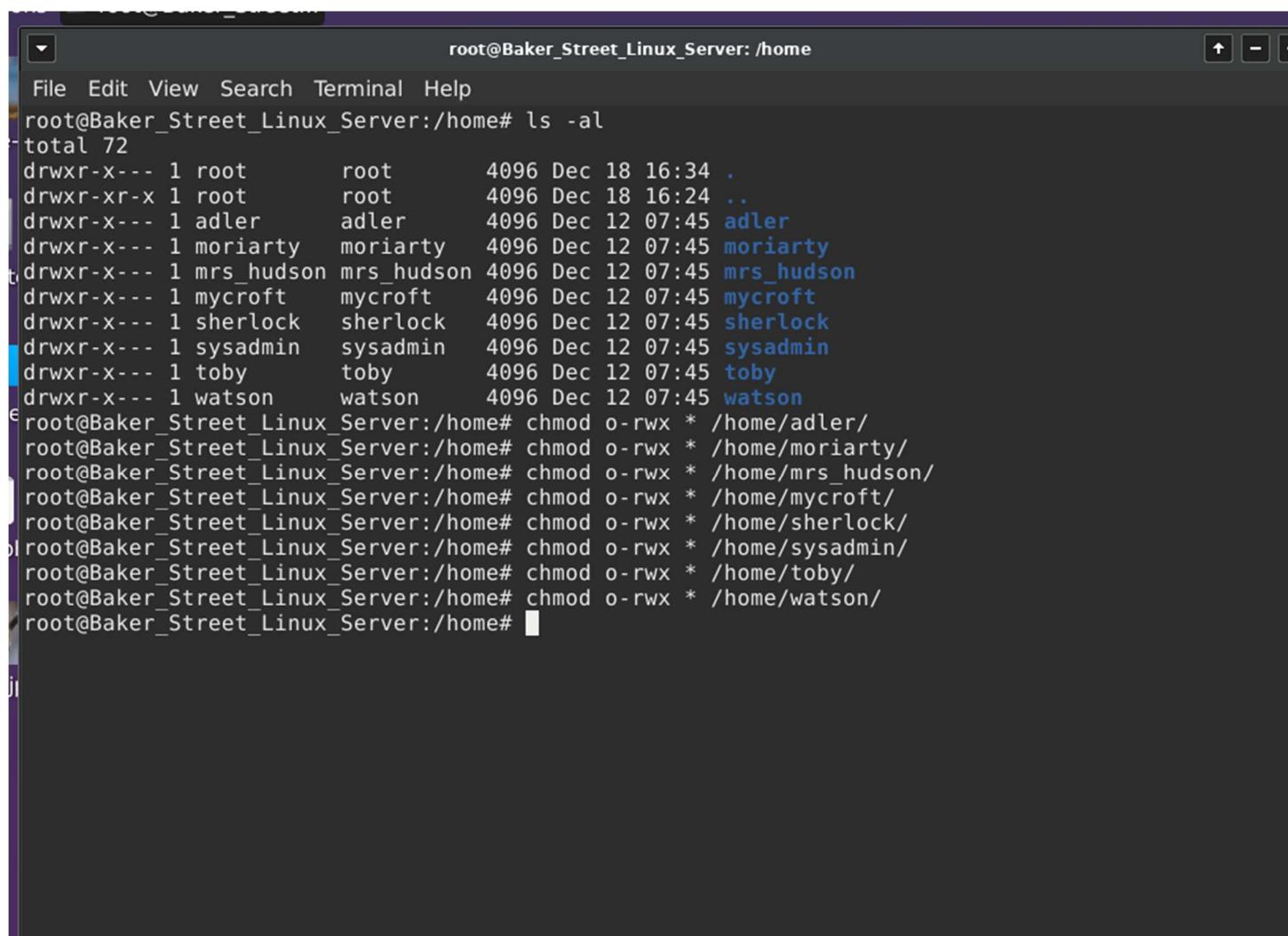
Continuing to list the users files and permissions.



The screenshot shows a terminal window titled "root@Baker_Street_Linux_Server: /home". The terminal interface includes a menu bar with File, Edit, View, Search, Terminal, and Help. The command history at the top shows "root@Baker_Street_Linux_Server:/home# chmod o-rwx * /home/**" and "root@Baker_Street_Linux_Server:/home# ls -lar". The output of the "ls -lar" command lists files and directories in the home directory with their permissions, ownership, and timestamps. The listing includes entries for "watson", "toby", "sysadmin", "sherlock", "mycroft", "mrs_hudson", "moriarty", "adler", and two entries for "root". The "root" entries show permissions "drwxr-xr-x" and "drwxr-x---". The "ls" command also shows the entries ".." and ".". The terminal prompt "root@Baker_Street_Linux_Server:/home#" is visible at the bottom.

```
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/home# chmod o-rwx * /home/***
root@Baker_Street_Linux_Server:/home# ls -lar
total 72
drwxr-x--- 1 watson      watson      4096 Dec 12 07:45 watson
drwxr-x--- 1 toby        toby        4096 Dec 12 07:45 toby
drwxr-x--- 1 sysadmin    sysadmin    4096 Dec 12 07:45 sysadmin
drwxr-x--- 1 sherlock   sherlock   4096 Dec 12 07:45 sherlock
drwxr-x--- 1 mycroft    mycroft    4096 Dec 12 07:45 mycroft
drwxr-x--- 1 mrs_hudson mrs_hudson 4096 Dec 12 07:45 mrs_hudson
drwxr-x--- 1 moriarty    moriarty    4096 Dec 12 07:45 moriarty
drwxr-x--- 1 adler       adler       4096 Dec 12 07:45 adler
drwxr-xr-x 1 root        root        4096 Dec 18 16:24 ..
drwxr-x--- 1 root        root        4096 Dec 18 16:34 .
root@Baker_Street_Linux_Server:/home#
```

Command to remove any world permissions on files in the user's home directory.



The screenshot shows a terminal window titled "root@Baker_Street_Linux_Server: /home". The terminal displays the following command and its output:

```
root@Baker_Street_Linux_Server:/home# ls -al
total 72
drwxr-x--- 1 root      root      4096 Dec 18 16:34 .
drwxr-xr-x  1 root      root      4096 Dec 18 16:24 ..
drwxr-x--- 1 adler     adler     4096 Dec 12 07:45 adler
drwxr-x--- 1 moriarty   moriarty  4096 Dec 12 07:45 moriarty
drwxr-x--- 1 mrs_hudson mrs_hudson 4096 Dec 12 07:45 mrs_hudson
drwxr-x--- 1 mycroft   mycroft   4096 Dec 12 07:45 mycroft
drwxr-x--- 1 sherlock   sherlock  4096 Dec 12 07:45 sherlock
drwxr-x--- 1 sysadmin   sysadmin  4096 Dec 12 07:45 sysadmin
drwxr-x--- 1 toby      toby     4096 Dec 12 07:45 toby
drwxr-x--- 1 watson    watson   4096 Dec 12 07:45 watson
root@Baker_Street_Linux_Server:/home# chmod o-rwx * /home/adler/
root@Baker_Street_Linux_Server:/home# chmod o-rwx * /home/moriarty/
root@Baker_Street_Linux_Server:/home# chmod o-rwx * /home/mrs_hudson/
root@Baker_Street_Linux_Server:/home# chmod o-rwx * /home/mycroft/
root@Baker_Street_Linux_Server:/home# chmod o-rwx * /home/sherlock/
root@Baker_Street_Linux_Server:/home# chmod o-rwx * /home/sysadmin/
root@Baker_Street_Linux_Server:/home# chmod o-rwx * /home/toby/
root@Baker_Street_Linux_Server:/home# chmod o-rwx * /home/watson/
root@Baker_Street_Linux_Server:/home#
```

Listing showing no world permissions on the user's home directory and then command to remove any world permissions within the user's home directory.

```

options Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/home# ls -lar /home/*
/home/watson:
total 36
-rw-r----- 1 root root 0 Dec 12 07:45 my_file.txt
-rw-r----- 1 root root 0 Dec 12 07:45 deduction.doc_2.txt
-rw-r----- 1 root root 0 Dec 12 07:45 deduction.doc_1.txt
-rw-r----- 1 root root 0 Dec 12 07:45 deduction.doc_0.txt
-rwxr-x--- 1 root root 47 Dec 12 07:45 Finance_script.sh_script2.sh
-rwxr-x--- 1 root root 47 Dec 12 07:45 Finance_script.sh_script1.sh
-rw-r----- 1 root root 0 Dec 12 07:45 Finance_script.sh_3.txt
-rw-r--r-- 1 watson watson 807 Jan 6 2022 .profile
-rw-r--r-- 1 watson watson 3771 Jan 6 2022 .bashrc
-rw-r--r-- 1 watson watson 220 Jan 6 2022 .bash_logout
drwxr-x--- 1 root root 4096 Dec 18 16:34 ..
drwxr-x--- 1 watson watson 4096 Dec 12 07:45 .

/home/toby:
total 36
-rwxr-x--- 1 root root 45 Dec 12 07:45 elementary.txt_script2.sh
-rwxr-x--- 1 root root 45 Dec 12 07:45 elementary.txt_script1.sh
-rw-r----- 1 root root 0 Dec 12 07:45 elementary.txt_3.txt
-rw-r----- 1 root root 0 Dec 12 07:45 elementary.txt_0.txt
-rw-r----- 1 root root 0 Dec 12 07:45 deduction.doc_1.txt
-rw-r----- 1 root root 0 Dec 12 07:45 Engineering_script.sh_2.txt
-rw-r--r-- 1 toby toby 807 Jan 6 2022 .profile
-rw-r--r-- 1 toby toby 3771 Jan 6 2022 .bashrc
-rw-r--r-- 1 toby toby 220 Jan 6 2022 .bash_logout
drwxr-x--- 1 root root 4096 Dec 18 16:34 ..
drwxr-x--- 1 toby toby 4096 Dec 12 07:45 .

/home/sysadmin:
total 24
-rw-r--r-- 1 sysadmin sysadmin 807 Jan 6 2022 .profile
-rw-r--r-- 1 sysadmin sysadmin 3771 Jan 6 2022 .bashrc
-rw-r--r-- 1 sysadmin sysadmin 220 Jan 6 2022 .bash_logout
drwxr-x--- 1 root root 4096 Dec 18 16:34 ..
drwxr-x--- 1 sysadmin sysadmin 4096 Dec 12 07:45 .

/home/sherlock:
total 36
-rw-r----- 1 root root 0 Dec 12 07:45 my_file.txt
-rw-r----- 1 root root 0 Dec 12 07:45 game_is_afoot.txt_2.txt
-rw-r----- 1 root root 0 Dec 12 07:45 game_is_afoot.txt_1.txt
-rw-r----- 1 root root 0 Dec 12 07:45 elementary.txt_0.txt
-rwxr-x--- 1 root root 49 Dec 12 07:45 deduction.doc_script2.sh
-rwxr-x--- 1 root root 49 Dec 12 07:45 deduction.doc_script1.sh
-rw-r----- 1 root root 0 Dec 12 07:45 deduction.doc_3.txt
-rw-r--r-- 1 sherlock sherlock 807 Jan 6 2022 .profile

```

Listing confirming that the files in the user's home directory does not have world permissions.

```

root@Baker_Street_Linux_Server: /home
File Edit View Search Terminal Help

/home/sherlock:
total 36
-rw-r---- 1 root      root      0 Dec 12 07:45 my_file.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 game_is_afoot.txt_2.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 game_is_afoot.txt_1.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 elementary.txt_0.txt
-rwxr-x-- 1 root      root      49 Dec 12 07:45 deduction.doc_script2.sh
-rwxr-x-- 1 root      root      49 Dec 12 07:45 deduction.doc_script1.sh
-rw-r---- 1 root      root      0 Dec 12 07:45 deduction.doc_3.txt
-rw-r---- 1 sherlock   sherlock  807 Jan  6 2022 .profile
-rw-r---- 1 sherlock   sherlock  3771 Jan  6 2022 .bashrc
-rw-r---- 1 sherlock   sherlock  220 Jan  6 2022 .bash_logout
drwxr-x-- 1 root      root     4096 Dec 18 16:34 ..
drwxr-x-- 1 sherlock   sherlock  4096 Dec 12 07:45 .

/home/mycroft:
total 36
-rw-r---- 1 root      root      0 Dec 12 07:45 deduction.doc_2.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 deduction.doc_1.txt
-rwxr-x-- 1 root      root      48 Dec 12 07:45 Finance_script.sh_script2.sh
-rwxr-x-- 1 root      root      48 Dec 12 07:45 Finance_script.sh_script1.sh
-rw-r---- 1 root      root      0 Dec 12 07:45 Finance_script.sh_3.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 Engineering_script.sh_0.txt
-rw-r---- 1 mycroft   mycroft   807 Jan  6 2022 .profile
-rw-r---- 1 mycroft   mycroft   3771 Jan  6 2022 .bashrc
-rw-r---- 1 mycroft   mycroft   220 Jan  6 2022 .bash_logout
drwxr-x-- 1 root      root     4096 Dec 18 16:34 ..
drwxr-x-- 1 mycroft   mycroft  4096 Dec 12 07:45 .

/home/mrs_hudson:
total 36
-rwxr-x-- 1 root      root      51 Dec 12 07:45 elementary.txt_script2.sh
-rwxr-x-- 1 root      root      51 Dec 12 07:45 elementary.txt_script1.sh
-rw-r---- 1 root      root      0 Dec 12 07:45 elementary.txt_3.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 deduction.doc_2.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 deduction.doc_0.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 Engineering_script.sh_1.txt
-rw-r---- 1 mrs_hudson mrs_hudson 807 Jan  6 2022 .profile
-rw-r---- 1 mrs_hudson mrs_hudson 3771 Jan  6 2022 .bashrc
-rw-r---- 1 mrs_hudson mrs_hudson 220 Jan  6 2022 .bash_logout
drwxr-x-- 1 root      root     4096 Dec 18 16:34 ..
drwxr-x-- 1 mrs_hudson mrs_hudson 4096 Dec 12 07:45 .

/home/moriarty:
total 36
-rw-r---- 1 root      root      0 Dec 12 07:45 my_file.txt
-rwxr-x-- 1 root      root      49 Dec 12 07:45 game_is_afoot.txt_script2.sh

```

Continuing to confirm that no world permissions exist on files in the user's home directory.

```

root@Baker_Street_Linux_Server: /home
File Edit View Search Terminal Help
-rw-r--r-- 1 mycroft mycroft 3771 Jan  6 2022 .bashrc
-rw-r--r-- 1 mycroft mycroft 220 Jan  6 2022 .bash_logout
drwxr-x--- 1 root      root    4096 Dec 18 16:34 ..
drwxr-x--- 1 mycroft mycroft 4096 Dec 12 07:45 .

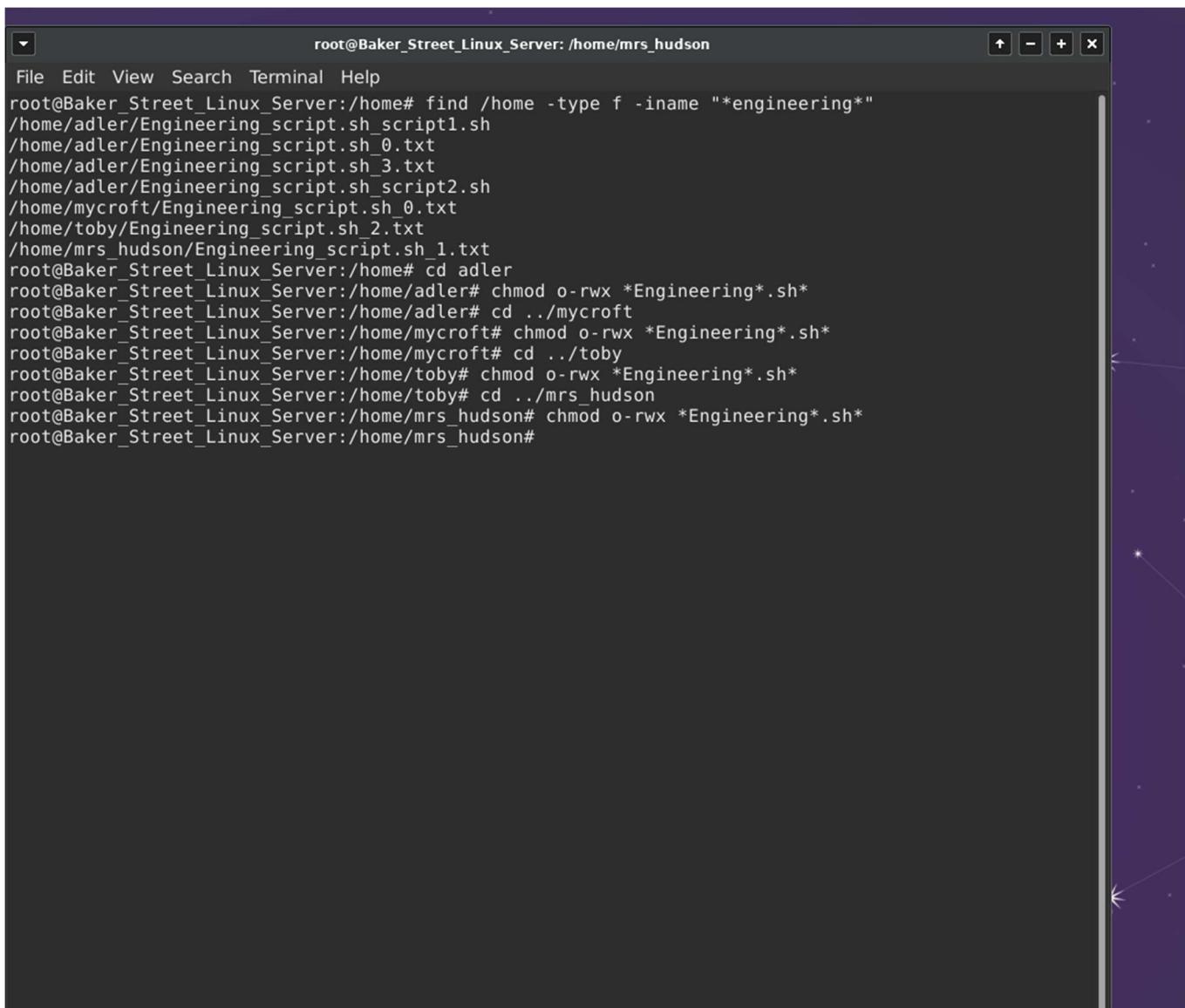
/home/mrs_hudson:
total 36
-rwxr-x--- 1 root      root    51 Dec 12 07:45 elementary.txt_script2.sh
-rwxr-x--- 1 root      root    51 Dec 12 07:45 elementary.txt_script1.sh
-rw-r----- 1 root      root    0 Dec 12 07:45 elementary.txt_3.txt
-rw-r----- 1 root      root    0 Dec 12 07:45 deduction.doc_2.txt
-rw-r----- 1 root      root    0 Dec 12 07:45 deduction.doc_0.txt
-rw-r----- 1 root      root    0 Dec 12 07:45 Engineering_script.sh_1.txt
-rw-r--r-- 1 mrs_hudson mrs_hudson 807 Jan  6 2022 .profile
-rw-r--r-- 1 mrs_hudson mrs_hudson 3771 Jan  6 2022 .bashrc
-rw-r--r-- 1 mrs_hudson mrs_hudson 220 Jan  6 2022 .bash_logout
drwxr-x--- 1 root      root    4096 Dec 18 16:34 ..
drwxr-x--- 1 mrs_hudson mrs_hudson 4096 Dec 12 07:45 .

/home/moriarty:
total 36
-rw-r----- 1 root      root    0 Dec 12 07:45 my_file.txt
-rwxr-x--- 1 root      root    49 Dec 12 07:45 game_is_afoot.txt_script2.sh
-rwxr-x--- 1 root      root    49 Dec 12 07:45 game_is_afoot.txt_script1.sh
-rw-r----- 1 root      root    0 Dec 12 07:45 game_is_afoot.txt_3.txt
-rw-r----- 1 root      root    0 Dec 12 07:45 elementary.txt_1.txt
-rw-r----- 1 root      root    0 Dec 12 07:45 Finance_script.sh_2.txt
-rw-r----- 1 root      root    0 Dec 12 07:45 Finance_script.sh_0.txt
-rw-r--r-- 1 moriarty moriarty 807 Jan  6 2022 .profile
-rw-r--r-- 1 moriarty moriarty 3771 Jan  6 2022 .bashrc
-rw-r--r-- 1 moriarty moriarty 220 Jan  6 2022 .bash_logout
drwxr-x--- 1 root      root    4096 Dec 18 16:34 ..
drwxr-x--- 1 moriarty moriarty 4096 Dec 12 07:45 .

/home/adler:
total 36
-rw-r----- 1 root      root    0 Dec 12 07:45 game_is_afoot.txt_1.txt
-rw-r----- 1 root      root    0 Dec 12 07:45 deduction.doc_2.txt
-rwxr-x--- 1 root      root    46 Dec 12 07:45 Engineering_script.sh_script2.sh
-rwxr-x--- 1 root      root    46 Dec 12 07:45 Engineering_script.sh_script1.sh
-rw-r----- 1 root      root    0 Dec 12 07:45 Engineering_script.sh_3.txt
-rw-r----- 1 root      root    0 Dec 12 07:45 Engineering_script.sh_0.txt
-rw-r--r-- 1 adler     adler   807 Jan  6 2022 .profile
-rw-r--r-- 1 adler     adler   3771 Jan  6 2022 .bashrc
-rw-r--r-- 1 adler     adler   220 Jan  6 2022 .bash_logout
drwxr-x--- 1 root      root    4096 Dec 18 16:34 ..
drwxr-x--- 1 adler     adler   4096 Dec 12 07:45 .
root@Baker_Street_Linux_Server:/home#

```

Continuing to confirm that no world permissions exist on files in the user's home directory.



```
root@Baker_Street_Linux_Server:/home/mrs_hudson
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/home# find /home -type f -iname "*engineering*"
/home/adler/Engineering_script.sh_script1.sh
/home/adler/Engineering_script.sh_0.txt
/home/adler/Engineering_script.sh_3.txt
/home/adler/Engineering_script.sh_script2.sh
/home/mycroft/Engineering_script.sh_0.txt
/home/toby/Engineering_script.sh_2.txt
/home/mrs_hudson/Engineering_script.sh_1.txt
root@Baker_Street_Linux_Server:/home# cd adler
root@Baker_Street_Linux_Server:/home/adler# chmod o-rwx *Engineering*.sh*
root@Baker_Street_Linux_Server:/home/adler# cd ../mycroft
root@Baker_Street_Linux_Server:/home/mycroft# chmod o-rwx *Engineering*.sh*
root@Baker_Street_Linux_Server:/home/mycroft# cd ../../toby
root@Baker_Street_Linux_Server:/home/toby# chmod o-rwx *Engineering*.sh*
root@Baker_Street_Linux_Server:/home/toby# cd ../../mrs_hudson
root@Baker_Street_Linux_Server:/home/mrs_hudson# chmod o-rwx *Engineering*.sh*
root@Baker_Street_Linux_Server:/home/mrs_hudson#
```

Ensuring that only members of the engineering group can view, edit, or execute engineering scripts.

PROJECT 1 – HARDENING A LINUX SERVER

```
root@Baker_Street_Linux_Server: /home/mrs_hudson
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/home# find /home -type f -iname "*engineering*"
/home/adler/Engineering_script.sh script1.sh
/home/adler/Engineering_script.sh_0.txt
/home/adler/Engineering_script.sh_3.txt
/home/adler/Engineering_script.sh_script2.sh
/home/mycroft/Engineering_script.sh_0.txt
/home/toby/Engineering_script.sh_2.txt
/home/mrs_hudson/Engineering_script.sh_1.txt
root@Baker_Street_Linux_Server:/home# cd adler
root@Baker_Street_Linux_Server:/home/adler# chmod o-rwx *Engineering*.sh*
root@Baker_Street_Linux_Server:/home/adler# cd ../mycroft
root@Baker_Street_Linux_Server:/home/mycroft# chmod o-rwx *Engineering*.sh*
root@Baker_Street_Linux_Server:/home/mycroft# cd ../toby
root@Baker_Street_Linux_Server:/home/toby# chmod o-rwx *Engineering*.sh*
root@Baker_Street_Linux_Server:/home/toby# cd ../../mrs_hudson
root@Baker_Street_Linux_Server:/home/mrs_hudson# chmod o-rwx *Engineering*.sh*
root@Baker_Street_Linux_Server:/home/mrs_hudson# ls -ld $(find /home -type f)
-rw-r--r-- 1 adler adler 220 Jan  6 2022 /home/adler/.bash_logout
-rw-r--r-- 1 adler adler 3771 Jan  6 2022 /home/adler/.bashrc
-rw-r--r-- 1 adler adler 807 Jan  6 2022 /home/adler/.profile
-rw-r----- 1 root root 0 Dec 12 07:45 /home/adler/Engineering_script.sh_0.txt
-rw-r----- 1 root root 0 Dec 12 07:45 /home/adler/Engineering_script.sh_3.txt
-rwxr-x--- 1 root root 46 Dec 12 07:45 /home/adler/Engineering_script.sh_script1.sh
-rwxr-x--- 1 root root 46 Dec 12 07:45 /home/adler/Engineering_script.sh_script2.sh
-rw-r----- 1 root root 0 Dec 12 07:45 /home/adler/deduction.doc_2.txt
-rw-r----- 1 root root 0 Dec 12 07:45 /home/adler/game_is_afoot.txt_1.txt
-rw-r----- 1 moriarty moriarty 220 Jan  6 2022 /home/moriarty/.bash_logout
-rw-r--r-- 1 moriarty moriarty 3771 Jan  6 2022 /home/moriarty/.bashrc
-rw-r----- 1 moriarty moriarty 807 Jan  6 2022 /home/moriarty/.profile
-rw-r----- 1 root root 0 Dec 12 07:45 /home/moriarty/Finance_script.sh_0.txt
-rw-r----- 1 root root 0 Dec 12 07:45 /home/moriarty/Finance_script.sh_2.txt
-rw-r----- 1 root root 0 Dec 12 07:45 /home/moriarty/elementary.txt_1.txt
-rw-r----- 1 root root 0 Dec 12 07:45 /home/moriarty/game_is_afoot.txt_3.txt
-rwxr-x--- 1 root root 49 Dec 12 07:45 /home/moriarty/game_is_afoot.txt_script1.sh
-rwxr-x--- 1 root root 49 Dec 12 07:45 /home/moriarty/game_is_afoot.txt_script2.sh
-rw-r----- 1 root root 0 Dec 12 07:45 /home/moriarty/my_file.txt
-rw-r----- 1 mrs_hudson mrs_hudson 220 Jan  6 2022 /home/mrs_hudson/.bash_logout
-rw-r--r-- 1 mrs_hudson mrs_hudson 3771 Jan  6 2022 /home/mrs_hudson/.bashrc
-rw-r----- 1 mrs_hudson mrs_hudson 807 Jan  6 2022 /home/mrs_hudson/.profile
-rw-r----- 1 root root 0 Dec 12 07:45 /home/mrs_hudson/Engineering_script.sh_1.txt
-rw-r----- 1 root root 0 Dec 12 07:45 /home/mrs_hudson/deduction.doc_0.txt
-rw-r----- 1 root root 0 Dec 12 07:45 /home/mrs_hudson/deduction.doc_2.txt
-rw-r----- 1 root root 0 Dec 12 07:45 /home/mrs_hudson/elementary.txt_3.txt
-rwxr-x--- 1 root root 51 Dec 12 07:45 /home/mrs_hudson/elementary.txt_script1.sh
-rwxr-x--- 1 root root 51 Dec 12 07:45 /home/mrs_hudson/elementary.txt_script2.sh
-rw-r----- 1 mycroft mycroft 220 Jan  6 2022 /home/mycroft/.bash_logout
-rw-r----- 1 mycroft mycroft 3771 Jan  6 2022 /home/mycroft/.bashrc
-rw-r----- 1 mycroft mycroft 807 Jan  6 2022 /home/mycroft/.profile
```

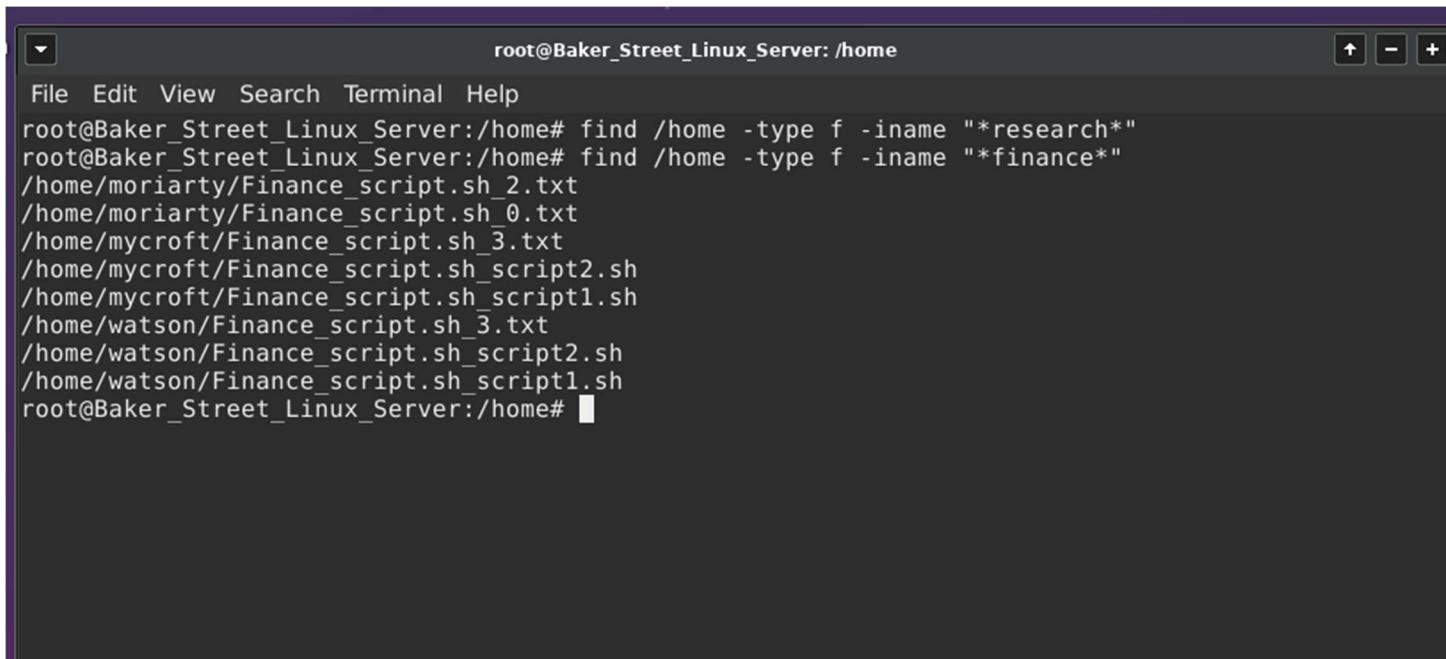
Continuing to ensure that only members of the engineering group can view, edit, or execute engineering scripts.

```

root@Baker_Street_Linux_Server:/home/mrs_hudson
File Edit View Search Terminal Help
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/mrs_hudson/Engineering_script.sh_1.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/mrs_hudson/deduction.doc_0.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/mrs_hudson/deduction.doc_2.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/mrs_hudson/elementary.txt_3.txt
-rwxr-x--- 1 root      root      51 Dec 12 07:45 /home/mrs_hudson/elementary.txt_script1.sh
-rwxr-x--- 1 root      root      51 Dec 12 07:45 /home/mrs_hudson/elementary.txt_script2.sh
-rw-r--r-- 1 mycroft   mycroft   220 Jan  6 2022 /home/mycroft/.bash_logout
-rw-r--r-- 1 mycroft   mycroft   3771 Jan  6 2022 /home/mycroft/.bashrc
-rw-r--r-- 1 mycroft   mycroft   807 Jan  6 2022 /home/mycroft/.profile
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/mycroft/Engineering_script.sh_0.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/mycroft/Finance_script.sh_3.txt
-rwxr-x--- 1 root      root      48 Dec 12 07:45 /home/mycroft/Finance_script.sh_script1.sh
-rwxr-x--- 1 root      root      48 Dec 12 07:45 /home/mycroft/Finance_script.sh_script2.sh
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/mycroft/deduction.doc_1.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/mycroft/deduction.doc_2.txt
-rw-r--r-- 1 sherlock   sherlock   220 Jan  6 2022 /home/sherlock/.bash_logout
-rw-r--r-- 1 sherlock   sherlock   3771 Jan  6 2022 /home/sherlock/.bashrc
-rw-r--r-- 1 sherlock   sherlock   807 Jan  6 2022 /home/sherlock/.profile
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/sherlock/deduction.doc_3.txt
-rwxr-x--- 1 root      root      49 Dec 12 07:45 /home/sherlock/deduction.doc_script1.sh
-rwxr-x--- 1 root      root      49 Dec 12 07:45 /home/sherlock/deduction.doc_script2.sh
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/sherlock/elementary.txt_0.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/sherlock/game_is_afoot.txt_1.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/sherlock/game_is_afoot.txt_2.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/sherlock/my_file.txt
-rw-r--r-- 1 sysadmin   sysadmin   220 Jan  6 2022 /home/sysadmin/.bash_logout
-rw-r--r-- 1 sysadmin   sysadmin   3771 Jan  6 2022 /home/sysadmin/.bashrc
-rw-r--r-- 1 sysadmin   sysadmin   807 Jan  6 2022 /home/sysadmin/.profile
-rw-r--r-- 1 toby       toby       220 Jan  6 2022 /home/toby/.bash_logout
-rw-r--r-- 1 toby       toby       3771 Jan  6 2022 /home/toby/.bashrc
-rw-r--r-- 1 toby       toby       807 Jan  6 2022 /home/toby/.profile
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/toby/Engineering_script.sh_2.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/toby/deduction.doc_1.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/toby/elementary.txt_0.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/toby/elementary.txt_3.txt
-rwxr-x--- 1 root      root      45 Dec 12 07:45 /home/toby/elementary.txt_script1.sh
-rwxr-x--- 1 root      root      45 Dec 12 07:45 /home/toby/elementary.txt_script2.sh
-rw-r--r-- 1 watson    watson    220 Jan  6 2022 /home/watson/.bash_logout
-rw-r--r-- 1 watson    watson    3771 Jan  6 2022 /home/watson/.bashrc
-rw-r--r-- 1 watson    watson    807 Jan  6 2022 /home/watson/.profile
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/watson/Finance_script.sh_3.txt
-rwxr-x--- 1 root      root      47 Dec 12 07:45 /home/watson/Finance_script.sh_script1.sh
-rwxr-x--- 1 root      root      47 Dec 12 07:45 /home/watson/Finance_script.sh_script2.sh
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/watson/deduction.doc_0.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/watson/deduction.doc_1.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/watson/deduction.doc_2.txt
-rw-r----- 1 root      root      0 Dec 12 07:45 /home/watson/my_file.txt
root@Baker_Street_Linux_Server:/home/mrs_hudson#

```

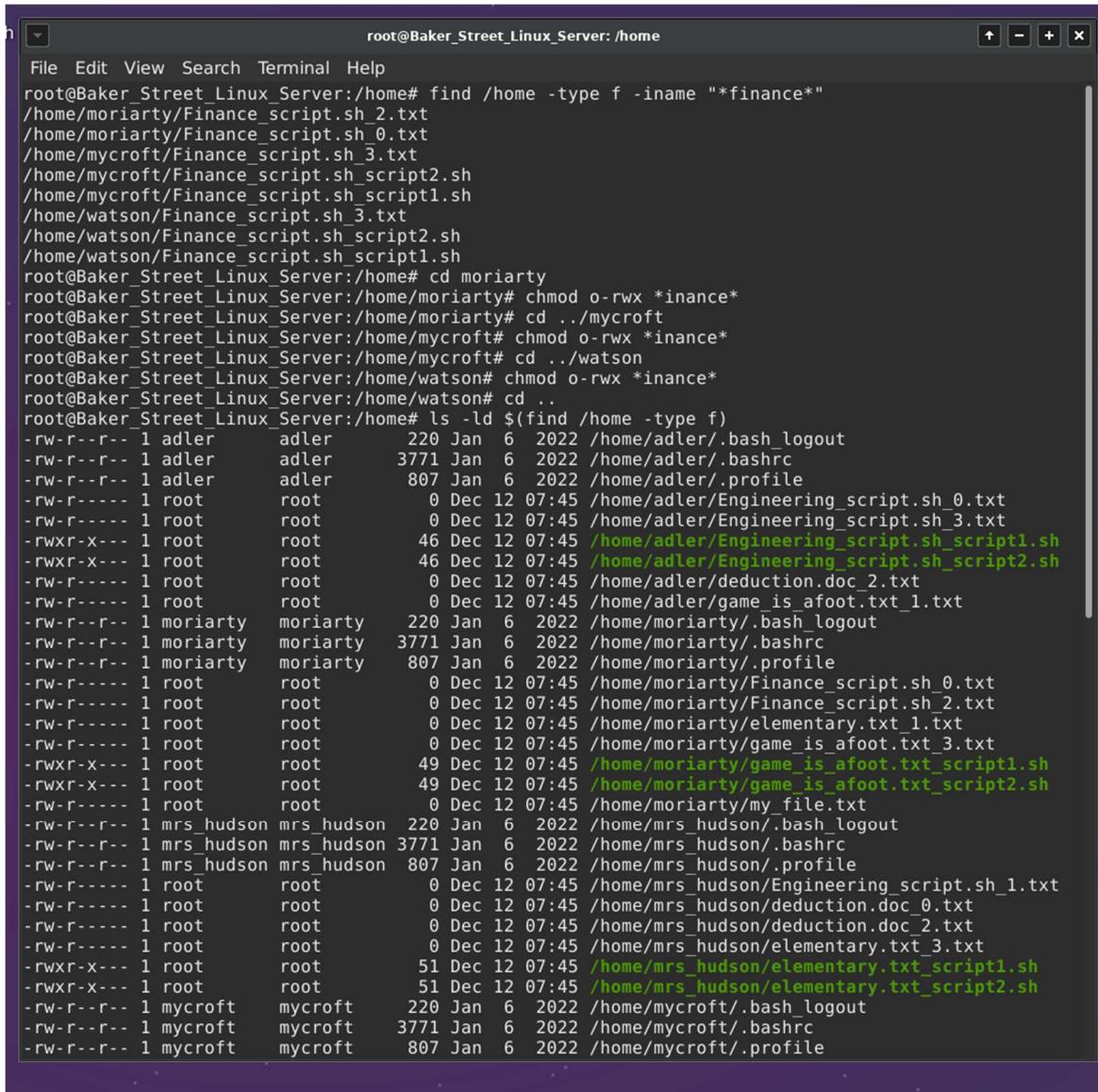
Continuing to ensure that only members of the engineering group can view, edit, or execute engineering scripts.



The screenshot shows a terminal window titled "root@Baker_Street_Linux_Server: /home". The terminal is displaying the output of a command that finds files in the "/home" directory with names containing either "research" or "finance". The results are as follows:

```
root@Baker_Street_Linux_Server:/home# find /home -type f -iname "*research*"
root@Baker_Street_Linux_Server:/home# find /home -type f -iname "*finance*"
/home/moriarty/Finance_script.sh_2.txt
/home/moriarty/Finance_script.sh_0.txt
/home/mycroft/Finance_script.sh_3.txt
/home/mycroft/Finance_script.sh_script2.sh
/home/mycroft/Finance_script.sh_script1.sh
/home/watson/Finance_script.sh_3.txt
/home/watson/Finance_script.sh_script2.sh
/home/watson/Finance_script.sh_script1.sh
root@Baker_Street_Linux_Server:/home#
```

Looking for research and finance scripts.



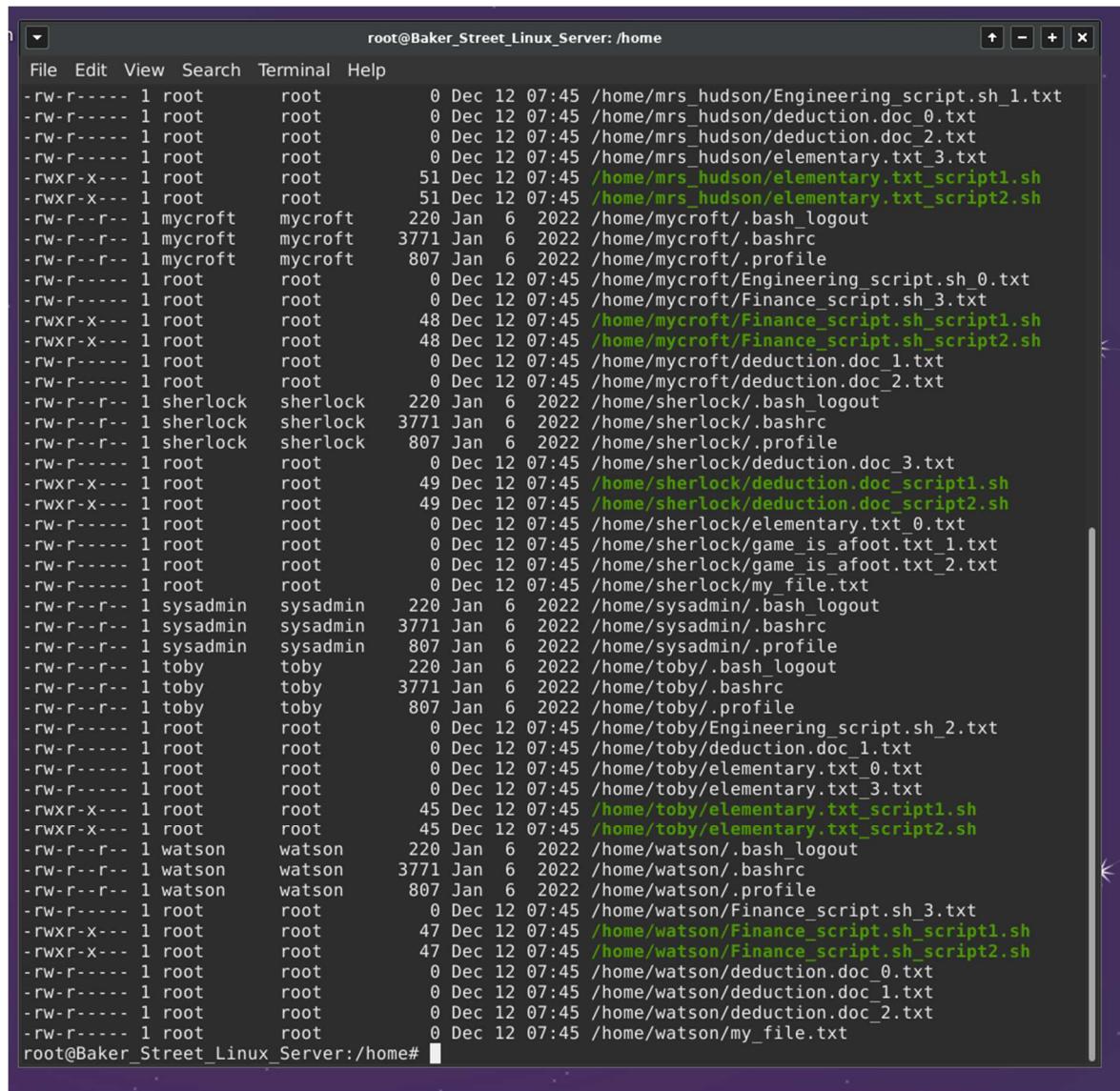
```

root@Baker_Street_Linux_Server:/home# find /home -type f -iname "*finance*"
/home/moriarty/Finance_script.sh_2.txt
/home/moriarty/Finance_script.sh_0.txt
/home/mycroft/Finance_script.sh_3.txt
/home/mycroft/Finance_script.sh_script2.sh
/home/mycroft/Finance_script.sh_script1.sh
/home/watson/Finance_script.sh_3.txt
/home/watson/Finance_script.sh_script2.sh
/home/watson/Finance_script.sh_script1.sh
root@Baker_Street_Linux_Server:/home# cd moriarty
root@Baker_Street_Linux_Server:/home/moriarty# chmod o-rwx *inance*
root@Baker_Street_Linux_Server:/home/moriarty# cd ../mycroft
root@Baker_Street_Linux_Server:/home/mycroft# chmod o-rwx *inance*
root@Baker_Street_Linux_Server:/home/mycroft# cd ../watson
root@Baker_Street_Linux_Server:/home/watson# chmod o-rwx *inance*
root@Baker_Street_Linux_Server:/home/watson# cd ..
root@Baker_Street_Linux_Server:/home# ls -ld $(find /home -type f)
-rw-r--r-- 1 adler      adler    220 Jan  6 2022 /home/adler/.bash_logout
-rw-r--r-- 1 adler      adler   3771 Jan  6 2022 /home/adler/.bashrc
-rw-r--r-- 1 adler      adler   807 Jan  6 2022 /home/adler/.profile
-rw-r----- 1 root       root     0 Dec 12 07:45 /home/adler/Engineering_script.sh_0.txt
-rw-r----- 1 root       root     0 Dec 12 07:45 /home/adler/Engineering_script.sh_3.txt
-rwxr-x--- 1 root       root    46 Dec 12 07:45 /home/adler/Engineering_script.sh_script1.sh
-rwxr-x--- 1 root       root    46 Dec 12 07:45 /home/adler/Engineering_script.sh_script2.sh
-rw-r----- 1 root       root     0 Dec 12 07:45 /home/adler/deduction.doc_2.txt
-rw-r----- 1 root       root     0 Dec 12 07:45 /home/adler/game_is_afoot.txt_1.txt
-rw-r--r-- 1 moriarty   moriarty 220 Jan  6 2022 /home/moriarty/.bash_logout
-rw-r--r-- 1 moriarty   moriarty 3771 Jan  6 2022 /home/moriarty/.bashrc
-rw-r--r-- 1 moriarty   moriarty 807 Jan  6 2022 /home/moriarty/.profile
-rw-r----- 1 root       root     0 Dec 12 07:45 /home/moriarty/Finance_script.sh_0.txt
-rw-r----- 1 root       root     0 Dec 12 07:45 /home/moriarty/Finance_script.sh_2.txt
-rw-r----- 1 root       root     0 Dec 12 07:45 /home/moriarty/elementary.txt_1.txt
-rw-r----- 1 root       root     0 Dec 12 07:45 /home/moriarty/game_is_afoot.txt_3.txt
-rwxr-x--- 1 root       root    49 Dec 12 07:45 /home/moriarty/game_is_afoot.txt_script1.sh
-rwxr-x--- 1 root       root    49 Dec 12 07:45 /home/moriarty/game_is_afoot.txt_script2.sh
-rw-r----- 1 root       root     0 Dec 12 07:45 /home/moriarty/my_file.txt
-rw-r--r-- 1 mrs_hudson mrs_hudson 220 Jan  6 2022 /home/mrs_hudson/.bash_logout
-rw-r--r-- 1 mrs_hudson mrs_hudson 3771 Jan  6 2022 /home/mrs_hudson/.bashrc
-rw-r--r-- 1 mrs_hudson mrs_hudson 807 Jan  6 2022 /home/mrs_hudson/.profile
-rw-r----- 1 root       root     0 Dec 12 07:45 /home/mrs_hudson/Engineering_script.sh_1.txt
-rw-r----- 1 root       root     0 Dec 12 07:45 /home/mrs_hudson/deduction.doc_0.txt
-rw-r----- 1 root       root     0 Dec 12 07:45 /home/mrs_hudson/deduction.doc_2.txt
-rw-r----- 1 root       root     0 Dec 12 07:45 /home/mrs_hudson/elementary.txt_3.txt
-rwxr-x--- 1 root       root    51 Dec 12 07:45 /home/mrs_hudson/elementary.txt_script1.sh
-rwxr-x--- 1 root       root    51 Dec 12 07:45 /home/mrs_hudson/elementary.txt_script2.sh
-rw-r--r-- 1 mycroft   mycroft   220 Jan  6 2022 /home/mycroft/.bash_logout
-rw-r--r-- 1 mycroft   mycroft   3771 Jan  6 2022 /home/mycroft/.bashrc
-rw-r--r-- 1 mycroft   mycroft   807 Jan  6 2022 /home/mycroft/.profile

```

Ensuring that only members of the finance group can view, edit, or execute finance scripts.

PROJECT 1 – HARDENING A LINUX SERVER



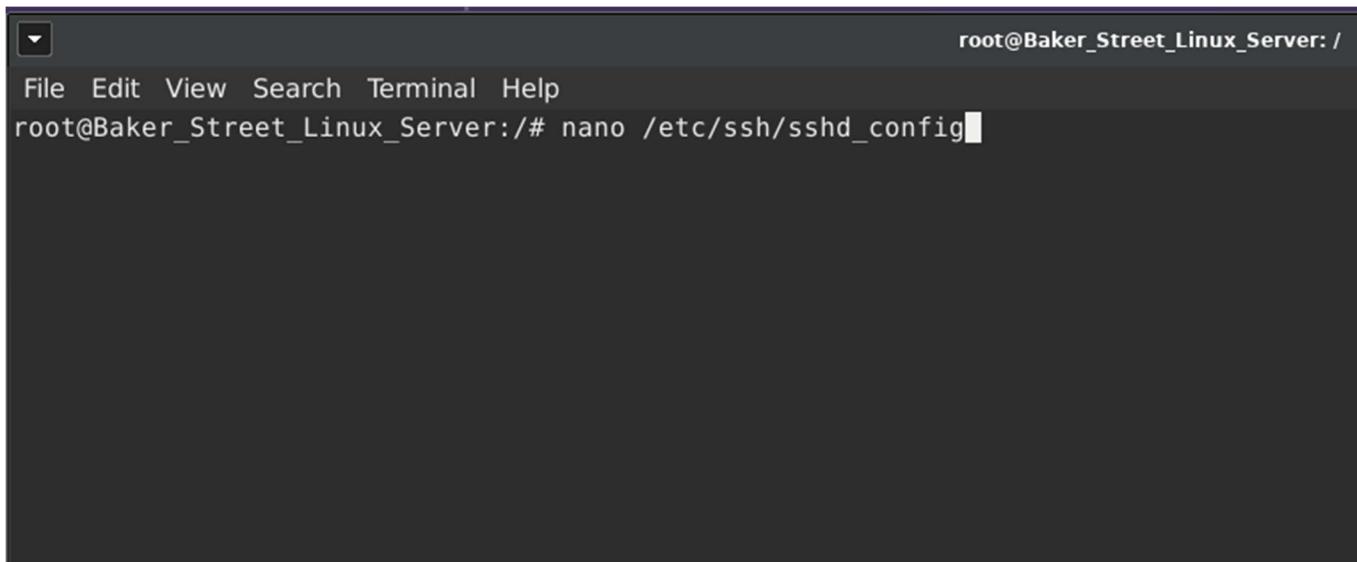
The terminal window shows a listing of files in the /home directory. The files are color-coded by owner: root (dark blue), mycroft (light blue), sherlock (purple), sysadmin (red), and watson (yellow). The files are categorized into several groups:

- Root-owned files:** Engineering_script.sh_1.txt, deduction.doc_0.txt, deduction.doc_2.txt, elementary.txt_3.txt, mrs_hudson_elementary.txt_script1.sh, mrs_hudson_elementary.txt_script2.sh, bash_logout, bashrc, profile.
- Mycroft-owned files:** mycroft/.bash_logout, mycroft/.bashrc, mycroft/.profile.
- Sherlock-owned files:** sherlock/.bash_logout, sherlock/.bashrc, sherlock/.profile.
- System Admin-owned files:** sysadmin/.bash_logout, sysadmin/.bashrc, sysadmin/.profile.
- Watson-owned files:** watson/.bash_logout, watson/.bashrc, watson/.profile.
- Common files:** deduction.doc_1.txt, deduction.doc_2.txt, elementary.txt_0.txt, game_is_afoot.txt_1.txt, game_is_afoot.txt_2.txt, my_file.txt.
- Scripted files:** mrs_hudson_elementary.txt_script1.sh, mrs_hudson_elementary.txt_script2.sh, toby_elementary.txt_script1.sh, toby_elementary.txt_script2.sh, watson_Finance_script.sh_3.txt, watson_Finance_script.sh_script1.sh, watson_Finance_script.sh_script2.sh.

```
root@Baker_Street_Linux_Server: /home
File Edit View Search Terminal Help
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/mrs_hudson/Engineering_script.sh_1.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/mrs_hudson/deduction.doc_0.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/mrs_hudson/deduction.doc_2.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/mrs_hudson/elementary.txt_3.txt
-rwxr-x--- 1 root      root      51 Dec 12 07:45 /home/mrs_hudson/elementary.txt_script1.sh
-rwxr-x--- 1 root      root      51 Dec 12 07:45 /home/mrs_hudson/elementary.txt_script2.sh
-rw-r--r-- 1 mycroft  mycroft   220 Jan  6 2022 /home/mycroft/.bash_logout
-rw-r--r-- 1 mycroft  mycroft   3771 Jan  6 2022 /home/mycroft/.bashrc
-rw-r--r-- 1 mycroft  mycroft   807 Jan  6 2022 /home/mycroft/.profile
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/mycroft/Engineering_script.sh_0.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/mycroft/Finance_script.sh_3.txt
-rwxr-x--- 1 root      root      48 Dec 12 07:45 /home/mycroft/Finance_script.sh_script1.sh
-rwxr-x--- 1 root      root      48 Dec 12 07:45 /home/mycroft/Finance_script.sh_script2.sh
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/mycroft/deduction.doc_1.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/mycroft/deduction.doc_2.txt
-rw-r--r-- 1 sherlock  sherlock   220 Jan  6 2022 /home/sherlock/.bash_logout
-rw-r--r-- 1 sherlock  sherlock   3771 Jan  6 2022 /home/sherlock/.bashrc
-rw-r--r-- 1 sherlock  sherlock   807 Jan  6 2022 /home/sherlock/.profile
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/sherlock/deduction.doc_3.txt
-rwxr-x--- 1 root      root      49 Dec 12 07:45 /home/sherlock/deduction.doc_script1.sh
-rwxr-x--- 1 root      root      49 Dec 12 07:45 /home/sherlock/deduction.doc_script2.sh
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/sherlock/elementary.txt_0.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/sherlock/game_is_afoot.txt_1.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/sherlock/game_is_afoot.txt_2.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/sherlock/my_file.txt
-rw-r--r-- 1 sysadmin  sysadmin   220 Jan  6 2022 /home/sysadmin/.bash_logout
-rw-r--r-- 1 sysadmin  sysadmin   3771 Jan  6 2022 /home/sysadmin/.bashrc
-rw-r--r-- 1 sysadmin  sysadmin   807 Jan  6 2022 /home/sysadmin/.profile
-rw-r--r-- 1 toby      toby      220 Jan  6 2022 /home/toby/.bash_logout
-rw-r--r-- 1 toby      toby      3771 Jan  6 2022 /home/toby/.bashrc
-rw-r--r-- 1 toby      toby      807 Jan  6 2022 /home/toby/.profile
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/toby/Engineering_script.sh_2.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/toby/deduction.doc_1.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/toby/elementary.txt_0.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/toby/elementary.txt_3.txt
-rwxr-x--- 1 root      root      45 Dec 12 07:45 /home/toby/elementary.txt_script1.sh
-rwxr-x--- 1 root      root      45 Dec 12 07:45 /home/toby/elementary.txt_script2.sh
-rw-r--r-- 1 watson    watson    220 Jan  6 2022 /home/watson/.bash_logout
-rw-r--r-- 1 watson    watson    3771 Jan  6 2022 /home/watson/.bashrc
-rw-r--r-- 1 watson    watson    807 Jan  6 2022 /home/watson/.profile
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/watson/Finance_script.sh_3.txt
-rwxr-x--- 1 root      root      47 Dec 12 07:45 /home/watson/Finance_script.sh_script1.sh
-rwxr-x--- 1 root      root      47 Dec 12 07:45 /home/watson/Finance_script.sh_script2.sh
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/watson/deduction.doc_0.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/watson/deduction.doc_1.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/watson/deduction.doc_2.txt
-rw-r---- 1 root      root      0 Dec 12 07:45 /home/watson/my_file.txt
root@Baker_Street_Linux_Server:/home#
```

Continuing to ensure that only members of the finance group can view, edit, or execute finance scripts.

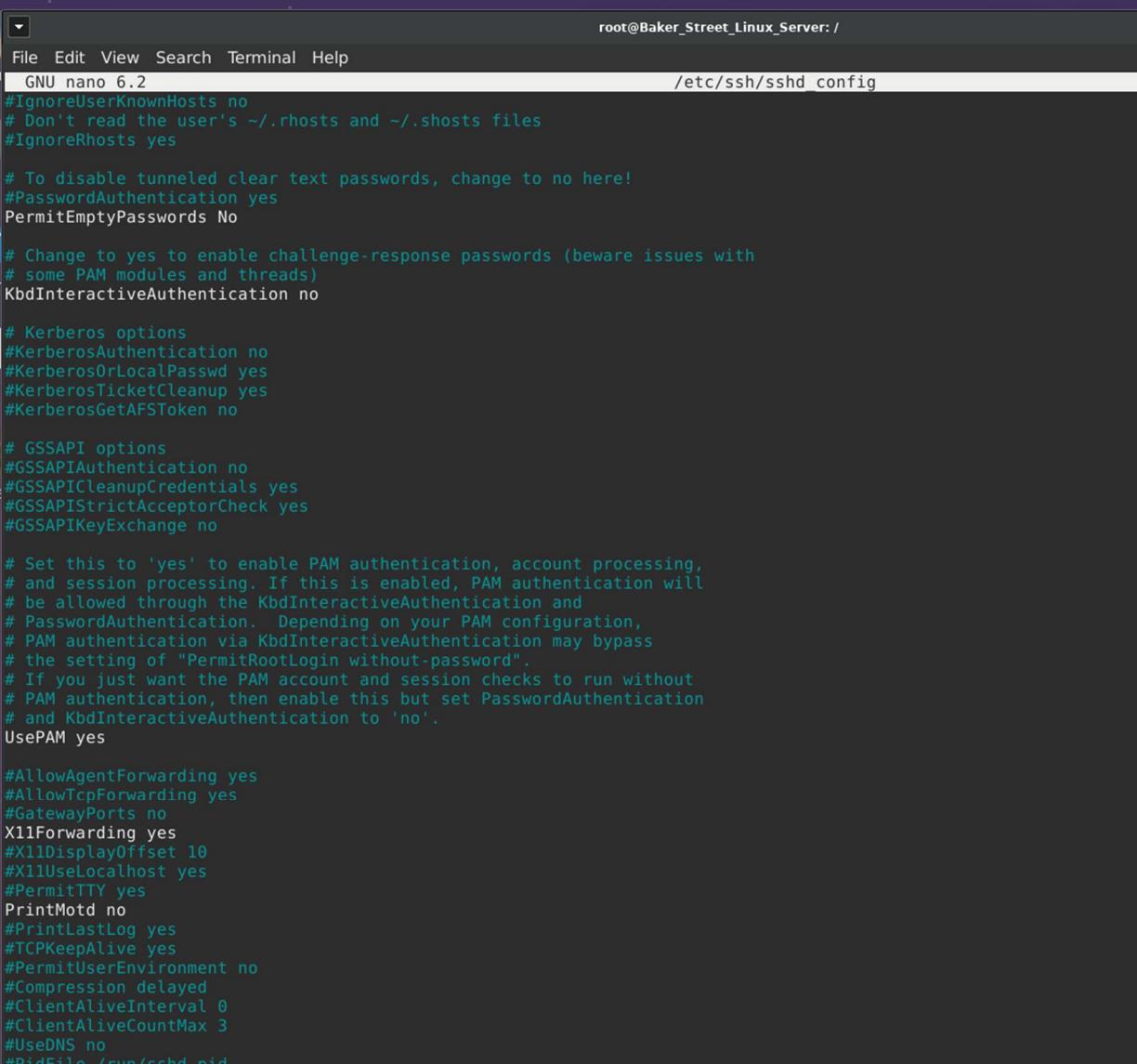
10.2 Project 1 Day 2 Activity Guide



A screenshot of a terminal window. The title bar says "root@Baker_Street_Linux_Server: /". The menu bar includes "File Edit View Search Terminal Help". The command "root@Baker_Street_Linux_Server:/# nano /etc/ssh/sshd_config" is visible in the terminal window.

Part 1: Auditing and Security SSH

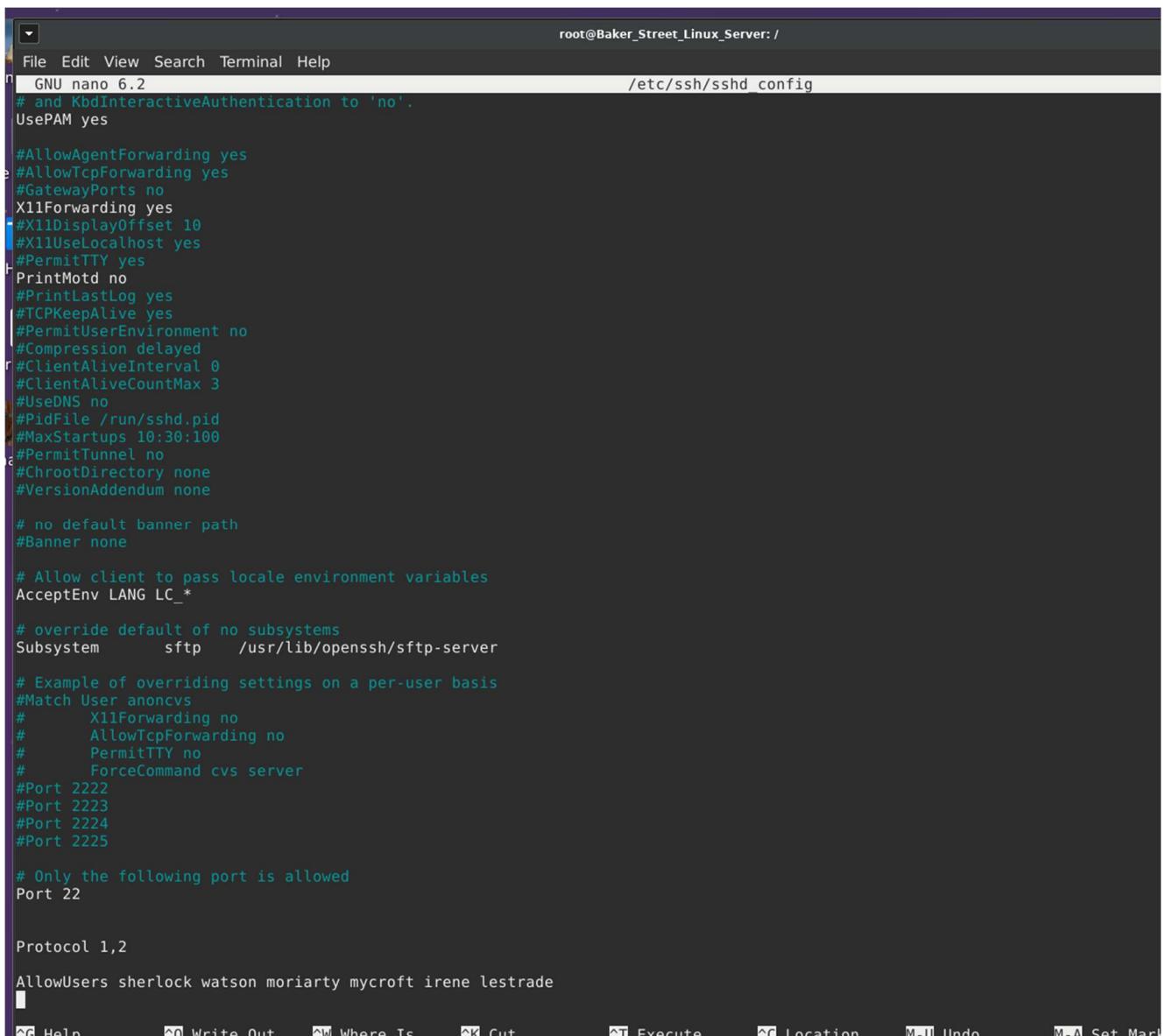
Open the SSH Configuration file to edit.



The screenshot shows a terminal window titled "root@Baker_Street_Linux_Server: /". The window title bar also displays the path "/etc/ssh/sshd_config". The terminal menu bar includes "File Edit View Search Terminal Help". The main content area of the terminal shows the configuration file for the sshd service, specifically the /etc/ssh/sshd_config file. The file contains numerous commented-out lines starting with "#", which represent various SSH configuration options. Some of the visible options include "IgnoreUserKnownHosts no", "PasswordAuthentication yes", "PermitEmptyPasswords No", "KbdInteractiveAuthentication no", "Kerberos options", "GSSAPI options", "UsePAM yes", and "AllowAgentForwarding yes". The configuration file is displayed in a monospaced font.

Editing SSH to harden SSH with strict controls.

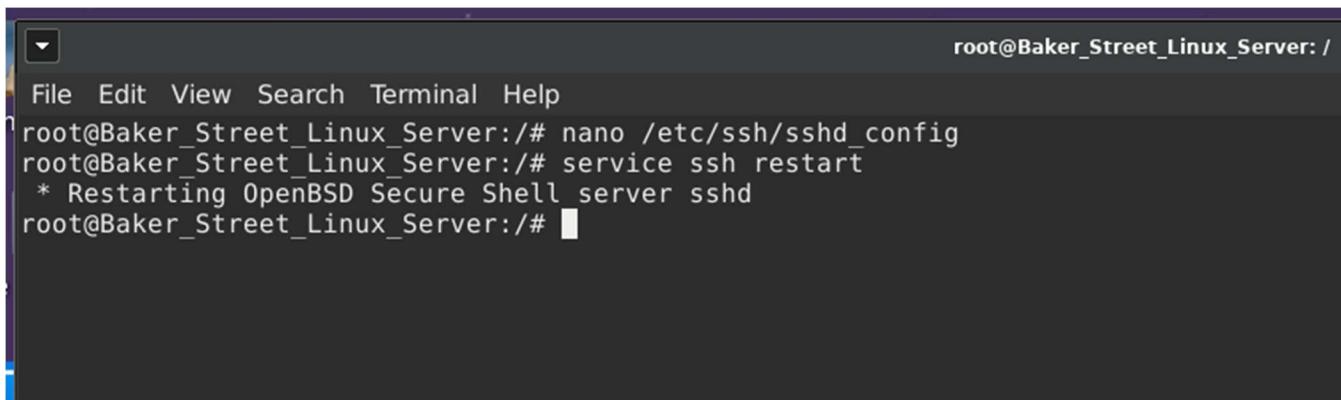
PROJECT 1 – HARDENING A LINUX SERVER



The screenshot shows a terminal window titled "root@Baker_Street_Linux_Server: /". The window contains the configuration file for the SSH daemon, /etc/ssh/sshd_config. The file is being edited in the GNU nano 6.2 text editor. The configuration includes various parameters such as X11Forwarding, PermitTTY, and Port settings. The terminal also shows standard Linux navigation keys at the bottom.

```
GNU nano 6.2                                     root@Baker_Street_Linux_Server: /  
# and KbdInteractiveAuthentication to 'no'.  
UsePAM yes  
  
#AllowAgentForwarding yes  
#AllowTcpForwarding yes  
#GatewayPorts no  
X11Forwarding yes  
#X11DisplayOffset 10  
#X11UseLocalhost yes  
#PermitTTY yes  
PrintMotd no  
#PrintLastLog yes  
#TCPKeepAlive yes  
#PermitUserEnvironment no  
#Compression delayed  
#ClientAliveInterval 0  
#ClientAliveCountMax 3  
#UseDNS no  
#PidFile /run/sshd.pid  
#MaxStartups 10:30:100  
#PermitTunnel no  
#ChrootDirectory none  
#VersionAddendum none  
  
# no default banner path  
#Banner none  
  
# Allow client to pass locale environment variables  
AcceptEnv LANG LC_*  
  
# override default of no subsystems  
Subsystem sftp /usr/lib/openssh/sftp-server  
  
# Example of overriding settings on a per-user basis  
#Match User anoncvs  
#     X11Forwarding no  
#     AllowTcpForwarding no  
#     PermitTTY no  
#     ForceCommand cvs server  
#Port 2222  
#Port 2223  
#Port 2224  
#Port 2225  
  
# Only the following port is allowed  
Port 22  
  
Protocol 1,2  
  
AllowUsers sherlock watson moriarty mycroft irene lestrade  
■  
G Help   W Write Out   Cw Where Is   CK Cut   CT Execute   CC Location   M-U Undo   M-A Set Mark
```

Continuing to edit the SSH configuration file.



The screenshot shows a terminal window titled "root@Baker_Street_Linux_Server: /". The user has run the command "nano /etc/ssh/sshd_config" to edit the SSH configuration file. After making changes, they have run "service ssh restart" to apply the changes. The terminal shows the output of the restart command, which indicates that the OpenBSD Secure Shell server (sshd) is restarting.

```
File Edit View Search Terminal Help  
root@Baker_Street_Linux_Server:/# nano /etc/ssh/sshd_config  
root@Baker_Street_Linux_Server:/# service ssh restart  
* Restarting OpenBSD Secure Shell server sshd  
root@Baker_Street_Linux_Server:/# ■
```

JOHN MALLON

Restarting the SSH service to set the configuration updates.

```
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# apt update
Get:1 http://archive.ubuntu.com/ubuntu jammy InRelease [270 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [266 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [17.5 MB]
Get:7 http://archive.ubuntu.com/ubuntu jammy/main amd64 Packages [1792 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy/restricted amd64 Packages [164 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1517 kB]
Get:10 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2817 kB]
Get:11 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [53.3]
Get:12 http://archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [3588]
Get:13 http://archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [37.0]
Get:14 http://archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [111 kB]
Get:15 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [1226]
Get:16 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [45.]
Get:17 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [2506 kB]
Get:18 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [343
Fetched 35.7 MB in 13s (2797 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
root@Baker_Street_Linux_Server:/# █
```

Part 2: Review, Update, and Add System Packages

Commands to update system packages.

```
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# apt update
Get:1 http://archive.ubuntu.com/ubuntu jammy InRelease [270 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [266 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [17.5 MB]
Get:7 http://archive.ubuntu.com/ubuntu jammy/main amd64 Packages [1792 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy/restricted amd64 Packages [164 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages
Get:10 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [28 kB]
Get:11 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages
Get:12 http://archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages
Get:13 http://archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages
Get:14 http://archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [164 kB]
Get:15 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages
Get:16 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages
Get:17 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [164 kB]
Get:18 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages
Fetched 35.7 MB in 13s (2797 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
root@Baker_Street_Linux_Server:/# apt upgrade -y
```

Command to upgrade system packages.

```
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# apt update
Get:1 http://archive.ubuntu.com/ubuntu jammy InRelease [270 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [266 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [17.5 MB]
Get:7 http://archive.ubuntu.com/ubuntu jammy/main amd64 Packages [1792 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy/restricted amd64 Packages [164 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1517 kB]
Get:10 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2817 kB]
Get:11 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [53.3 kB]
Get:12 http://archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [3588 kB]
Get:13 http://archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [37.0 kB]
Get:14 http://archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [111 kB]
Get:15 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [1226 kB]
Get:16 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [45.4 kB]
Get:17 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [2506 kB]
Get:18 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [343 kB]
Fetched 35.7 MB in 13s (2797 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
root@Baker_Street_Linux_Server:/# apt upgrade -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@Baker_Street_Linux_Server:/# █
```

Confirmation of the upgrade to the packages.

```

root@Baker_Street_Linux_Server:/# apt list --installed
Listing... Done
adduser/jammy,now 3.118ubuntu5 all [installed]
apt/jammy-updates,now 2.4.13 amd64 [installed]
attr/jammy,now 1:2.5.1-1build1 amd64 [installed,automatic]
base-files/jammy-updates,now 12ubuntu4.7 amd64 [installed]
base-passwd/jammy,now 3.5.52build1 amd64 [installed]
bash/jammy-updates,jammy-security,now 5.1-6ubuntul.1 amd64 [installed]
bsdutils/jammy-updates,jammy-security,now 1:2.37.2-4ubuntu3.4 amd64 [installed]
ca-certificates/jammy-updates,jammy-security,now 20240203-22.04.1 all [installed,automatic]
coreutils/jammy-updates,now 8.32-4.lubuntul.2 amd64 [installed]
cron/jammy,now 3.0pll-137ubuntu3 amd64 [installed,automatic]
dash/jammy,now 0.5.11+git20210903+057cd650a4ed-3build1 amd64 [installed]
dbus/jammy-updates,jammy-security,now 1.12.20-2ubuntu4.1 amd64 [installed,automatic]
debconf/jammy,now 1.5.79ubuntu1 all [installed]
debianutils/jammy,now 5.5-lubuntu2 amd64 [installed]
diffutils/jammy,now 1:3.8-0ubuntu2 amd64 [installed]
dirmngr/jammy-updates,jammy-security,now 2.2.27-3ubuntu2.1 amd64 [installed,automatic]
distro-info-data/jammy-updates,now 0.52ubuntu0.8 all [installed,automatic]
dmsetup/jammy,now 2:1.02.175.2.lubuntu4 amd64 [installed,automatic]
dpkg/jammy-updates,now 1.21.lubuntu2.3 amd64 [installed]
e2fsprogs/jammy-updates,now 1.46.5-2ubuntu2 amd64 [installed]
findutils/jammy,now 4.8.0-1ubuntu3 amd64 [installed]
gcc-12-base/jammy-updates,jammy-security,now 12.3.0-1ubuntul-22.04 amd64 [installed]
gir1.2-glib-2.0/jammy,now 1.72.0-1 amd64 [installed,automatic]
gnupg-l10n/jammy-updates,jammy-security,now 2.2.27-3ubuntu2.1 all [installed,automatic]
gnupg-utils/jammy-updates,jammy-security,now 2.2.27-3ubuntu2.1 amd64 [installed,automatic]
gnupg/jammy-updates,jammy-security,now 2.2.27-3ubuntu2.1 all [installed,automatic]
gpg-agent/jammy-updates,jammy-security,now 2.2.27-3ubuntu2.1 amd64 [installed,automatic]
gpg-wks-client/jammy-updates,jammy-security,now 2.2.27-3ubuntu2.1 amd64 [installed,automatic]
gpg-wks-server/jammy-updates,jammy-security,now 2.2.27-3ubuntu2.1 amd64 [installed,automatic]
gpg/jammy-updates,jammy-security,now 2.2.27-3ubuntu2.1 amd64 [installed,automatic]
gpgconf/jammy-updates,jammy-security,now 2.2.27-3ubuntu2.1 amd64 [installed,automatic]
gpgsm/jammy-updates,jammy-security,now 2.2.27-3ubuntu2.1 amd64 [installed,automatic]
gpgv/jammy-updates,jammy-security,now 2.2.27-3ubuntu2.1 amd64 [installed]
grep/jammy,now 3.7-1build1 amd64 [installed]
gzip/jammy-updates,now 1.10-4ubuntu4.1 amd64 [installed]
hostname/jammy,now 3.23ubuntu2 amd64 [installed]
ibverbs-providers/jammy,now 39.0-1 amd64 [installed,automatic]
init-system-helpers/jammy,now 1.62 all [installed]
iproute2/jammy,now 5.15.0-1ubuntu2 amd64 [installed]
john-data/jammy,now 1.8.0-4ubuntu3 all [installed,automatic]
john/jammy,now 1.8.0-4ubuntu3 amd64 [installed]
libacl1/jammy,now 2.3.1-1 amd64 [installed]
libaiol/jammy,now 0.3.112-13build1 amd64 [installed,automatic]
libapparmor1/jammy-updates,jammy-security,now 3.0.4-2ubuntu2.4 amd64 [installed,automatic]
libapt-pkg0.0/jammy-updates,now 2.4.13 amd64 [installed]
libargon2-1/jammy,now 0-20171227-0.3 amd64 [installed,automatic]
libassuan0/jammy,now 2.5.5-1build1 amd64 [installed,automatic]
libatm1/jammy,now 1:2.5.1-4build2 amd64 [installed,automatic]
libattr1/jammy,now 1:2.5.1-1build1 amd64 [installed]
libaudit-common/jammy,now 1:3.0.7-1build1 all [installed]
libaudit1/jammy,now 1:3.0.7-1build1 amd64 [installed]
libavahi-client3/jammy-updates,jammy-security,now 0.8-5ubuntu5.2 amd64 [installed,automatic]
libavahi-common-data/jammy-updates,jammy-security,now 0.8-5ubuntu5.2 amd64 [installed,automatic]
libavahi-common3/jammy-updates,jammy-security,now 0.8-5ubuntu5.2 amd64 [installed,automatic]

```

Listing all installed packages.

PROJECT 1 – HARDENING A LINUX SERVER

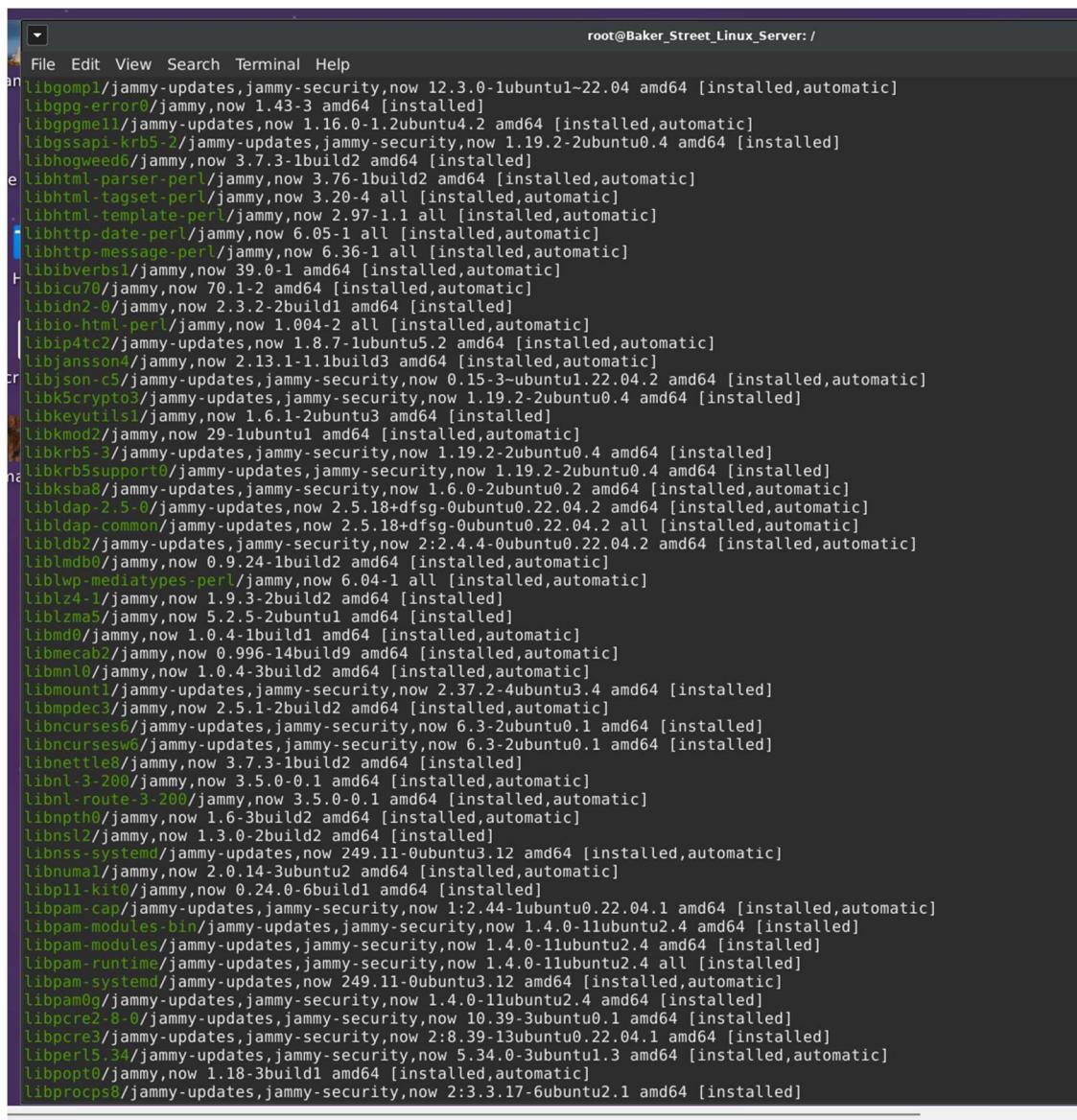


```
root@Baker_Street_Linux_Server:/home/mallon
File Edit View Search Terminal Help
libavahi-common-data/jammy-updates,jammy-security,now 0.8-5ubuntu5.2 amd64 [installed,automatic]
libavahi-common3/jammy-updates,jammy-security,now 0.8-5ubuntu5.2 amd64 [installed,automatic]
libblkid/jammy-updates,jammy-security,now 2.37.2-4ubuntu3.4 amd64 [installed]
libboost-iostreams1.74.0/jammy,now 1.74.0-14ubuntu3 amd64 [installed,automatic]
libboost-thread1.74.0/jammy,now 1.74.0-14ubuntu3 amd64 [installed,automatic]
libbpf0/jammy-updates,jammy-security,now 1:0.5.0-1ubuntu22.04.1 amd64 [installed,automatic]
libbsd0/jammy,now 0.11.5-1 amd64 [installed,automatic]
libbz2-1.0/jammy,now 1.0.8-5build1 amd64 [installed]
libc-bin/jammy-updates,jammy-security,now 2.35-0ubuntu3.8 amd64 [installed]
libcap6/jammy-updates,jammy-security,now 2.35-0ubuntu3.8 amd64 [installed]
libcap-ng0/jammy,now 0.7.9-2.2build3 amd64 [installed]
libcap2-bin/jammy-updates,jammy-security,now 1:2.44-1ubuntu0.22.04.1 amd64 [installed,automatic]
libcap2/jammy-updates,jammy-security,now 1:2.44-1ubuntu0.22.04.1 amd64 [installed]
libccb0.8/jammy,now 0.8.0-2ubuntu1 amd64 [installed,automatic]
libcephfs2/jammy-updates,now 17.2.7-0ubuntu0.22.04.1 amd64 [installed,automatic]
libcfast-perl/jammy,now 1:2.15-1 all [installed,automatic]
libcgipm-perl/jammy,now 4.54-1 all [installed,automatic]
libclone-perl/jammy,now 0.45-1build3 amd64 [installed,automatic]
libcomerr2/jammy-updates,now 1.46.5-2ubuntu1.2 amd64 [installed]
libcrypt1/jammy,now 1:4.4.27-1 amd64 [installed]
libcryptsetup12/jammy-updates,now 2:2.4.3-1ubuntu1.2 amd64 [installed,automatic]
libcurl2/jammy-updates,jammy-security,now 2.4.10p1-1ubuntu4.11 amd64 [installed,automatic]
libd5.3/jammy,now 5.3.28+dfsg1-0.8ubuntu3 amd64 [installed]
libdbus-1-3/jammy-updates,jammy-security,now 1.12.20-2ubuntu4.1 amd64 [installed,automatic]
libdebconfclient0/jammy,now 0.261ubuntu1 amd64 [installed]
libdevmapper1.02.1/jammy,now 2:1.02.175-2.1ubuntu4 amd64 [installed,automatic]
libedit2/jammy,now 3.1-20210910-1build1 amd64 [installed,automatic]
libelf1/jammy,now 0.186-1build1 amd64 [installed,automatic]
libencode-locale-perl/jammy,now 1.05-1.1 all [installed,automatic]
libestr0/jammy,now 1.0.10-2.1build3 amd64 [installed,automatic]
libevent-2.1-7/jammy,now 2.1.12-stable-1build3 amd64 [installed,automatic]
libevent-core-2.1-7/jammy,now 2.1.12-stable-1build3 amd64 [installed,automatic]
libevent-pthreads-2.1-7/jammy,now 2.1.12-stable-1build3 amd64 [installed,automatic]
libexpat1/jammy-updates,jammy-security,now 2.4.7-1ubuntu0.5 amd64 [installed,automatic]
libext2fs2/jammy-updates,now 1.46.5-2ubuntu1.2 amd64 [installed]
libfastjson4/jammy,now 0.99.9-1build2 amd64 [installed,automatic]
libfcgi-bin/jammy,now 2.4.2-2build2 amd64 [installed,automatic]
libfcgi-perl/jammy,now 0.82+ds-1build1 amd64 [installed,automatic]
libfcgi0ldbl/jammy,now 2.4.2-2build2 amd64 [installed,automatic]
libffi8/jammy,now 3.4.2-4 amd64 [installed]
libfido2-1/jammy,now 1.10.0-1 amd64 [installed,automatic]
libgcc-s1/jammy-updates,jammy-security,now 12.3.0-1ubuntu1~22.04 amd64 [installed]
libgcrypt20/jammy,now 1.9.4-3ubuntu3 amd64 [installed]
libgdbm-compat4/jammy,now 1.23-1 amd64 [installed,automatic]
libgdbm6/jammy,now 1.23-1 amd64 [installed,automatic]
libgfp10/jammy-updates,jammy-security,now 10.1-1ubuntu0.2 amd64 [installed,automatic]
libgfrpc8/jammy-updates,jammy-security,now 10.1-1ubuntu0.2 amd64 [installed,automatic]
libgwdx0/jammy-updates,jammy-security,now 10.1-1ubuntu0.2 amd64 [installed,automatic]
libgitrepository-1.0-1/jammy,now 1.72.0-1 amd64 [installed,automatic]
libglib2.0-0/jammy-updates,jammy-security,now 2.72.4-0ubuntu2.4 amd64 [installed,automatic]
libglib2.0-data/jammy-updates,jammy-security,now 2.72.4-0ubuntu2.4 all [installed,automatic]
libglusterfs8/jammy-updates,jammy-security,now 10.1-1ubuntu0.2 amd64 [installed,automatic]
libgnutls30/jammy-updates,jammy-security,now 3.7.3-4ubuntu1.5 amd64 [installed]
libgomp1/jammy-updates,jammy-security,now 12.3.0-1ubuntu1~22.04 amd64 [installed,automatic]
libgpg-error0/jammy,now 1.43-3 amd64 [installed]
```

Continuing list of all installed packages.

JOHN MALLON

PROJECT 1 – HARDENING A LINUX SERVER



```
root@Baker_Street_Linux_Server: /  
libgomp1/jammy-updates,jammy-security,now 12.3.0-1ubuntu1-22.04 amd64 [installed,automatic]  
libgpg-error0/jammy,now 1.43-3 amd64 [installed]  
libgpmel1/jammy-updates,now 1.16.0-1.2ubuntu4.2 amd64 [installed,automatic]  
libgssapi-krb5-2/jammy-updates,jammy-security,now 1.19.2-2ubuntu0.4 amd64 [installed]  
libhogweed6/jammy,now 3.7.3-1build2 amd64 [installed]  
libhtml-parser-perl/jammy,now 3.76-1build2 amd64 [installed,automatic]  
libhtml-tagset-perl/jammy,now 3.20-4 all [installed,automatic]  
libhtml-template-perl/jammy,now 2.97-1.1.all [installed,automatic]  
libhttp-date-perl/jammy,now 6.05-1 all [installed,automatic]  
libhttp-message-perl/jammy,now 6.36-1 all [installed,automatic]  
libibverbs1/jammy,now 39.0-1 amd64 [installed,automatic]  
libicu70/jammy,now 70.1-2 amd64 [installed,automatic]  
libidn2-0/jammy,now 2.3.2-2build1 amd64 [installed]  
libio-html-perl/jammy,now 1.004-2 all [installed,automatic]  
libip4tc2/jammy-updates,now 1.8.7-1ubuntu5.2 amd64 [installed,automatic]  
libjansson4/jammy,now 2.13.1-1.1build3 amd64 [installed,automatic]  
libjson-c5/jammy-updates,jammy-security,now 0.15-3-ubuntu1.22.04.2 amd64 [installed,automatic]  
libk5crypto3/jammy-updates,jammy-security,now 1.19.2-2ubuntu0.4 amd64 [installed]  
libkeyutils1/jammy,now 1.6.1-2ubuntu3 amd64 [installed]  
libkmod2/jammy,now 29-1ubuntu1 amd64 [installed,automatic]  
libkrb5-3/jammy-updates,jammy-security,now 1.19.2-2ubuntu0.4 amd64 [installed]  
libkrb5support0/jammy-updates,jammy-security,now 1.19.2-2ubuntu0.4 amd64 [installed]  
libksba8/jammy-updates,jammy-security,now 1.6.0-2ubuntu0.2 amd64 [installed,automatic]  
libldap-2.5-0/jammy-updates,now 2.5.18+dfsg-0ubuntu0.22.04.2 amd64 [installed,automatic]  
libldap-common/jammy-updates,now 2.5.18+dfsg-0ubuntu0.22.04.2 all [installed,automatic]  
libldb2/jammy-updates,jammy-security,now 2:2.4.4-0ubuntu0.22.04.2 amd64 [installed,automatic]  
liblmdb0/jammy,now 0.9.24-1build2 amd64 [installed,automatic]  
liblwp-mediatypes-perl/jammy,now 6.04-1 all [installed,automatic]  
liblz4-1/jammy,now 1.9.3-2build2 amd64 [installed]  
liblzma5/jammy,now 5.2.5-2ubuntu1 amd64 [installed]  
libmd0/jammy,now 1.0.4-1build1 amd64 [installed,automatic]  
libmecab2/jammy,now 0.996-14build9 amd64 [installed,automatic]  
libmnl0/jammy,now 1.0.4-3build2 amd64 [installed,automatic]  
libmount3/jammy-updates,jammy-security,now 2.37.2-4ubuntu3.4 amd64 [installed]  
libmpdec3/jammy,now 2.5.1-2build2 amd64 [installed,automatic]  
libncurses6/jammy-updates,jammy-security,now 6.3-2ubuntu0.1 amd64 [installed]  
libncursesw6/jammy-updates,jammy-security,now 6.3-2ubuntu0.1 amd64 [installed]  
libnettle8/jammy,now 3.7.3-1build2 amd64 [installed]  
libnl-3-200/jammy,now 3.5.0-0.1 amd64 [installed,automatic]  
libnl-route-3-200/jammy,now 3.5.0-0.1 amd64 [installed,automatic]  
libnpth0/jammy,now 1.6-3build2 amd64 [installed,automatic]  
libns12/jammy,now 1.3.0-2build2 amd64 [installed]  
libnss-systemd/jammy-updates,now 249.11-0ubuntu3.12 amd64 [installed,automatic]  
libnumal/jammy,now 2.0.14-3ubuntu2 amd64 [installed,automatic]  
libp11-kit0/jammy,now 0.24.0-6build1 amd64 [installed]  
libpam-cap/jammy-updates,jammy-security,now 1:2.44-1ubuntu0.22.04.1 amd64 [installed,automatic]  
libpam-modules-bin/jammy-updates,jammy-security,now 1.4.0-11ubuntu2.4 amd64 [installed]  
libpam-modules/jammy-updates,jammy-security,now 1.4.0-11ubuntu2.4 amd64 [installed]  
libpam-runtime/jammy-updates,jammy-security,now 1.4.0-11ubuntu2.4 all [installed]  
libpam-systemd/jammy-updates,now 249.11-0ubuntu3.12 amd64 [installed,automatic]  
libpam0g/jammy-updates,jammy-security,now 1.4.0-11ubuntu2.4 amd64 [installed]  
libpcre2-8-0/jammy-updates,jammy-security,now 10.39-3ubuntu0.1 amd64 [installed]  
libpcre3/jammy-updates,jammy-security,now 2:8.39-13ubuntu0.22.04.1 amd64 [installed]  
libperl5.34/jammy-updates,jammy-security,now 5.34.0-3ubuntu1.3 amd64 [installed,automatic]  
libpopt0/jammy,now 1.18-3build1 amd64 [installed,automatic]  
libprocps8/jammy-updates,jammy-security,now 2:3.3.17-6ubuntu2.1 amd64 [installed]
```

Continuing list of all installed packages.

JOHN MALLON

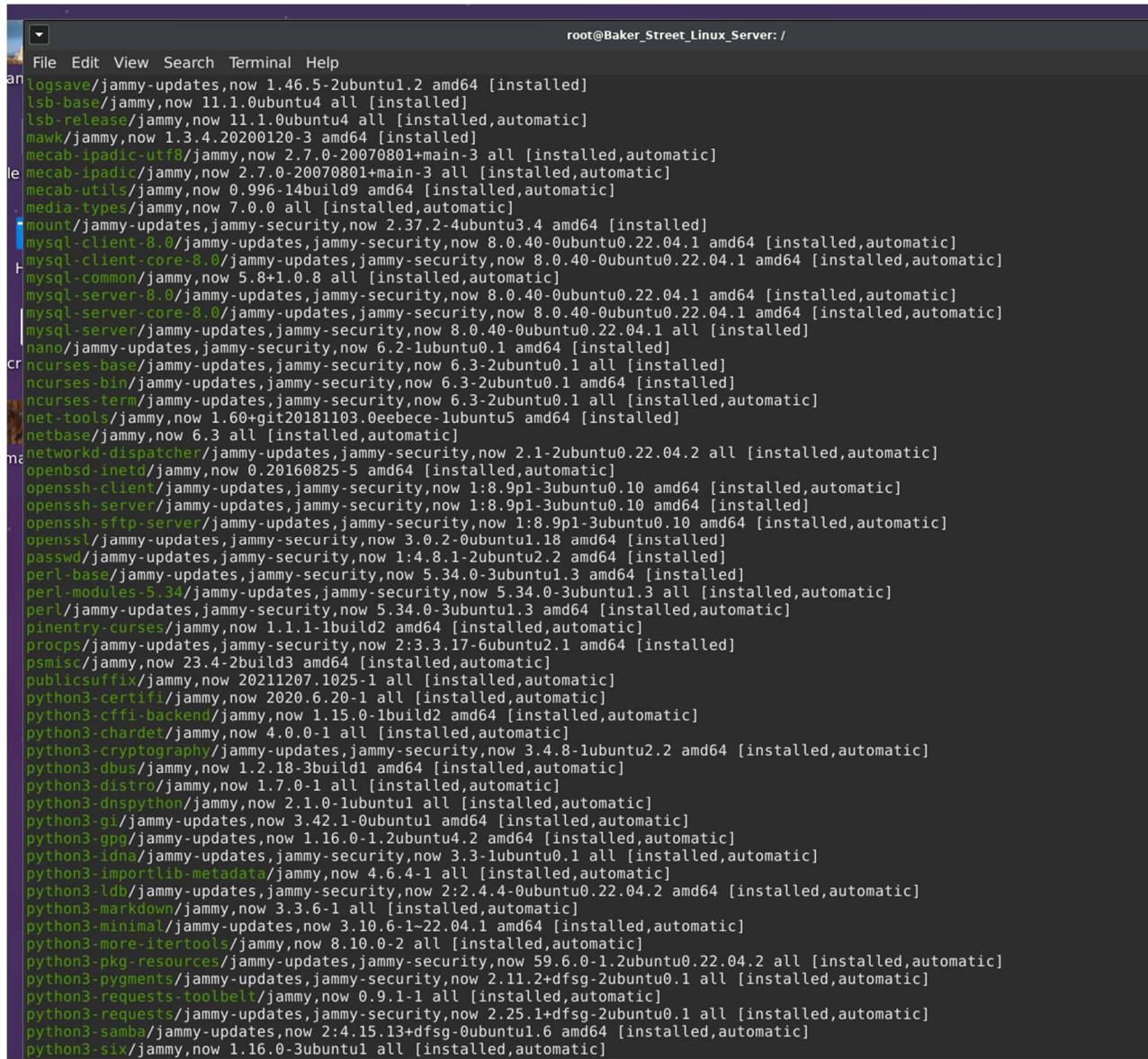
```

root@Baker_Street_Linux_Server: /
File Edit View Search Terminal Help
libpopt0/jammy,now 1.18-3build1 amd64 [installed,automatic]
libprocps8/jammy-updates,jammy-security,now 2:3.3.17-6ubuntu2.1 amd64 [installed]
libprotobuf-lite23/jammy-updates,jammy-security,now 3.12.4-1ubuntu7.22.04.1 amd64 [installed,automatic]
libpsl5/jammy,now 0.21.0-1.2build2 amd64 [installed,automatic]
libpython3-stdlib10/jammy-updates,now 3.10.6-1-22.04.1 amd64 [installed,automatic]
libpython3.10-minimal/jammy-updates,jammy-security,now 3.10.12-1-22.04.7 amd64 [installed,automatic]
libpython3.10-stdlib/jammy-updates,jammy-security,now 3.10.12-1-22.04.7 amd64 [installed,automatic]
libpython3.10/jammy-updates,jammy-security,now 3.10.12-1-22.04.7 amd64 [installed,automatic]
librados2/jammy-updates,now 17.2.7-2-0ubuntu0.22.04.1 amd64 [installed,automatic]
librdmacm1/jammy,now 39.0-1 amd64 [installed,automatic]
libreadline8/jammy,now 8.1.2-1 amd64 [installed,automatic]
libssasl2-2/jammy-updates,now 2.1.27+dfsg2-3ubuntu1.2 amd64 [installed,automatic]
libssl2-modules-db/jammy-updates,now 2.1.27+dfsg2-3ubuntu1.2 amd64 [installed,automatic]
libssl2-modules/jammy-updates,now 2.1.27+dfsg2-3ubuntu1.2 amd64 [installed,automatic]
libseccomp2/jammy,now 2.5.3-2ubuntu2 amd64 [installed]
libselinux1/jammy,now 3.3-1build2 amd64 [installed]
libsemanage-common/jammy,now 3.3-1build2 all [installed]
libsemanage2/jammy,now 3.3-1build2 amd64 [installed]
libsep0l2/jammy,now 3.3-1build1 amd64 [installed]
libsmartcols1/jammy-updates,jammy-security,now 2.37.2-4ubuntu3.4 amd64 [installed]
libsqlite3-0/jammy-updates,jammy-security,now 3.37.2-2ubuntu0.3 amd64 [installed,automatic]
libss2/jammy-updates,now 1.46.5-2ubuntu1.2 amd64 [installed]
libstl3/jammy-updates,jammy-security,now 3.0.2-0ubuntu1.18 amd64 [installed]
libstdc++6/jammy-updates,jammy-security,now 12.3.0-1ubuntu-22.04 amd64 [installed]
libsystemd0/jammy-updates,now 249.11-0ubuntu3.12 amd64 [installed]
libtalloc2/jammy,now 2.3.3-2build1 amd64 [installed,automatic]
libtasn1-6/jammy,now 4.18.0-4build1 amd64 [installed]
libtbd1/jammy,now 1.4.5-2build1 amd64 [installed,automatic]
libtevent0/jammy,now 0.11.0-1build1 amd64 [installed,automatic]
libtimedate-perl/jammy,now 2.3300-2 all [installed,automatic]
libtinfo6/jammy-updates,jammy-security,now 6.3-2ubuntu0.1 amd64 [installed]
libtirpc-common/jammy-updates,jammy-security,now 1.3.2-2ubuntu0.1 all [installed]
libtirpc3/jammy-updates,jammy-security,now 1.3.2-2ubuntu0.1 amd64 [installed]
libudev1/jammy-updates,now 249.11-0ubuntu3.12 amd64 [installed]
libunistring2/jammy,now 1.0-1 amd64 [installed]
liburi-perl/jammy,now 5.10-1 all [installed,automatic]
liburing2/jammy,now 2.1-2build1 amd64 [installed,automatic]
libuid1/jammy-updates,jammy-security,now 2.37.2-4ubuntu3.4 amd64 [installed]
libwbclient0/jammy-updates,now 2:4.15.13+dfsg-0ubuntu1.6 amd64 [installed,automatic]
libwrap0/jammy,now 7.6.q-31build2 amd64 [installed,automatic]
libx11-6/jammy-updates,jammy-security,now 2:1.7.5-1ubuntu0.3 amd64 [installed,automatic]
libx11-data/jammy-updates,jammy-security,now 2:1.7.5-1ubuntu0.3 all [installed,automatic]
libxau6/jammy,now 1:1.0.9-1build5 amd64 [installed,automatic]
libxcb1/jammy,now 1.14-3ubuntu3 amd64 [installed,automatic]
libxdmcp6/jammy,now 1:1.1.3-0ubuntu5 amd64 [installed,automatic]
libxext6/jammy,now 2:1.3.4-1build1 amd64 [installed,automatic]
libxml2/jammy-updates,jammy-security,now 2.9.13+dfsg-1ubuntu0.4 amd64 [installed,automatic]
libxmu1/jammy,now 2:1.1.3-3 amd64 [installed,automatic]
libxtables12/jammy-updates,now 1.8.7-1ubuntu5.2 amd64 [installed,automatic]
libxhash0/jammy,now 0.8.1-1 amd64 [installed]
libyaml-0-2/jammy,now 0.2.2-1build2 amd64 [installed,automatic]
libzstd1/jammy,now 1.4.8+dfsg-3build1 amd64 [installed]
login/jammy-updates,jammy-security,now 1:4.8.1-2ubuntu2.2 amd64 [installed]
logrotate/jammy-updates,jammy-security,now 3.19.0-1ubuntu1.1 amd64 [installed,automatic]
logsave/jammy-updates,now 1.46.5-2ubuntu1.2 amd64 [installed]
lsb-base/jammy,now 11.1.0ubuntu4 all [installed]

```

Continuing list of all installed packages.

PROJECT 1 – HARDENING A LINUX SERVER



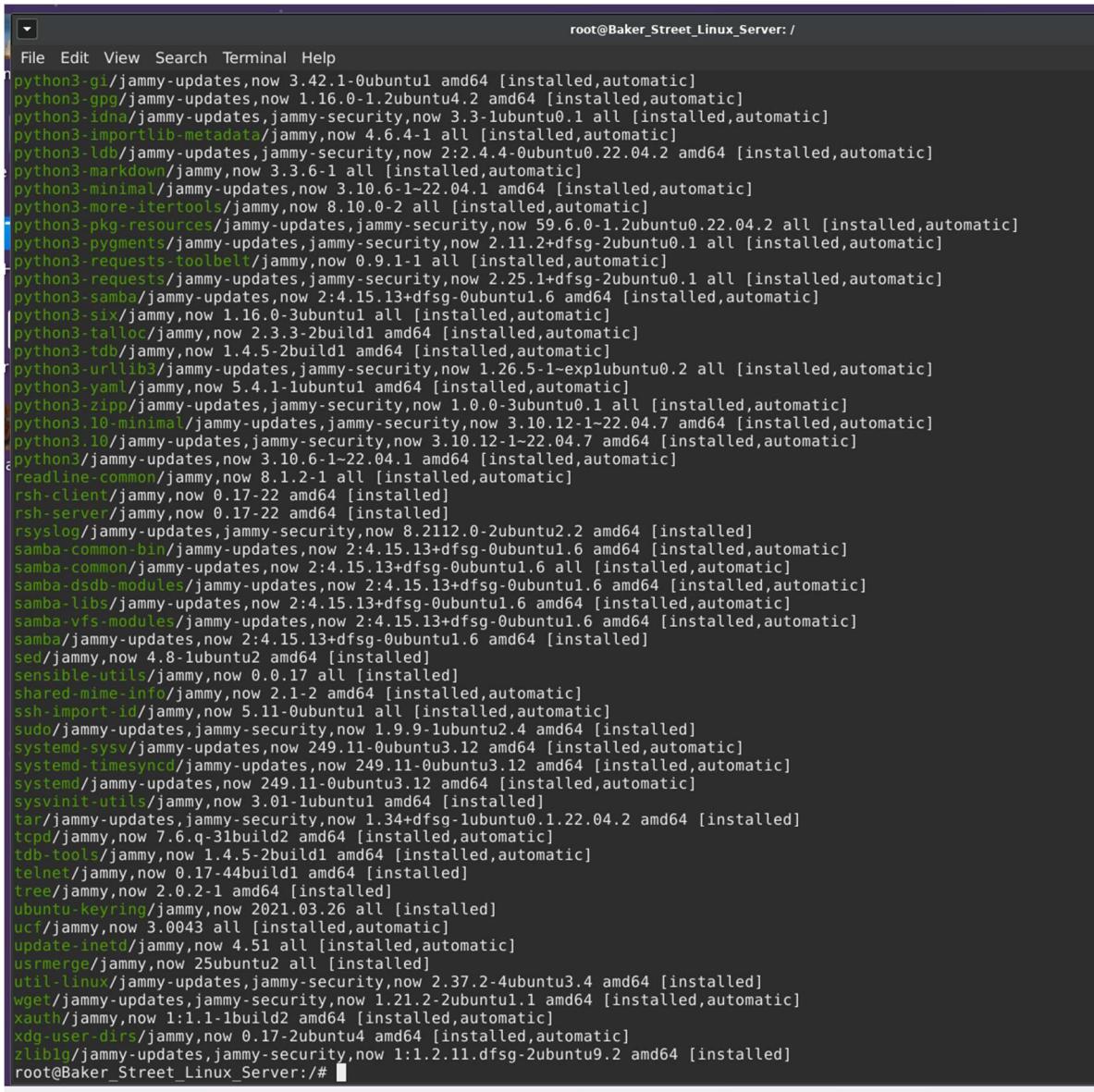
The screenshot shows a terminal window titled 'root@Baker_Street_Linux_Server: /'. The window displays a large list of installed packages, starting with 'logsave' and ending with 'python3-six'. The packages are listed with their names, versions, architectures, and installation status (installed or automatic). The terminal has a dark theme with white text on a black background.

```
logsave/jammy-updates,now 1.46.5-2ubuntu1.2 amd64 [installed]
lsb-base/jammy,now 11.1.0ubuntu4 all [installed]
lsb-release/jammy,now 11.1.0ubuntu4 all [installed,automatic]
mawk/jammy,now 1.3.4.20200120-3 amd64 [installed]
mecab-ipadic-utf8/jammy,now 2.7.0-20070801+main-3 all [installed,automatic]
mecab-ipadic/jammy,now 2.7.0-20070801+main-3 all [installed,automatic]
mecab-utils/jammy,now 0.996-14build9 amd64 [installed,automatic]
media-types/jammy,now 7.0.0 all [installed,automatic]
mount/jammy-updates,jammy-security,now 2.37.2-4ubuntu3.4 amd64 [installed]
mysql-client-8.0/jammy-updates,jammy-security,now 8.0.40-0ubuntu0.22.04.1 amd64 [installed,automatic]
mysql-client-core-8.0/jammy-updates,jammy-security,now 8.0.40-0ubuntu0.22.04.1 amd64 [installed,automatic]
mysql-common/jammy,now 5.8+1.0.8 all [installed,automatic]
mysql-server-8.0/jammy-updates,jammy-security,now 8.0.40-0ubuntu0.22.04.1 amd64 [installed,automatic]
mysql-server-core-8.0/jammy-updates,jammy-security,now 8.0.40-0ubuntu0.22.04.1 amd64 [installed,automatic]
mysql-server/jammy-updates,jammy-security,now 8.0.40-0ubuntu0.22.04.1 all [installed]
nano/jammy-updates,jammy-security,now 6.2-1ubuntu0.1 amd64 [installed]
ncurses-base/jammy-updates,jammy-security,now 6.3-2ubuntu0.1 all [installed]
ncurses-bin/jammy-updates,jammy-security,now 6.3-2ubuntu0.1 amd64 [installed]
ncurses-term/jammy-updates,jammy-security,now 6.3-2ubuntu0.1 all [installed,automatic]
net-tools/jammy,now 1.60+git20181103.0ebebe1ubuntu5 amd64 [installed]
netbase/jammy,now 6.3 all [installed,automatic]
networkd-dispatcher/jammy-updates,jammy-security,now 2.1-2ubuntu0.22.04.2 all [installed,automatic]
openbsd-inetd/jammy,now 0.20160825-5 amd64 [installed,automatic]
openssh-client/jammy-updates,jammy-security,now 1:8.9p1-3ubuntu0.10 amd64 [installed,automatic]
openssh-server/jammy-updates,jammy-security,now 1:8.9p1-3ubuntu0.10 amd64 [installed]
openssh-sftp-server/jammy-updates,jammy-security,now 1:8.9p1-3ubuntu0.10 amd64 [installed,automatic]
openssl/jammy-updates,jammy-security,now 3.0.2-0ubuntu1.18 amd64 [installed]
passwd/jammy-updates,jammy-security,now 1:4.8.1-2ubuntu2.2 amd64 [installed]
perl-base/jammy-updates,jammy-security,now 5.34.0-3ubuntu1.3 amd64 [installed]
perl-modules-5.34/jammy-updates,jammy-security,now 5.34.0-3ubuntu1.3 all [installed,automatic]
perl/jammy-updates,jammy-security,now 5.34.0-3ubuntu1.3 amd64 [installed,automatic]
pinentry-curses/jammy,now 1.1.1-1build2 amd64 [installed,automatic]
procps/jammy-updates,jammy-security,now 2:3.3.17-6ubuntu2.1 amd64 [installed]
psmisc/jammy,now 23.4-2build3 amd64 [installed,automatic]
publicsuffix/jammy,now 20211207.1025-1 all [installed,automatic]
python3-certifi/jammy,now 2020.6.20-1 all [installed,automatic]
python3-cffi-backend/jammy,now 1.15.0-1build2 amd64 [installed,automatic]
python3-chardet/jammy,now 4.0.0-1 all [installed,automatic]
python3-cryptography/jammy-updates,jammy-security,now 3.4.8-1ubuntu2.2 amd64 [installed,automatic]
python3-dbus/jammy,now 1.2.18-3build1 amd64 [installed,automatic]
python3-distro/jammy,now 1.7.0-1 all [installed,automatic]
python3-dnspython/jammy,now 2.1.0-1ubuntu1 all [installed,automatic]
python3-gi/jammy-updates,now 3.42.1-0ubuntu1 amd64 [installed,automatic]
python3-gpg/jammy-updates,now 1.16.0-1.2ubuntu4.2 amd64 [installed,automatic]
python3-idna/jammy-updates,jammy-security,now 3.3-1ubuntu0.1 all [installed,automatic]
python3-importlib-metadata/jammy,now 4.6.4-1 all [installed,automatic]
python3-ldb/jammy-updates,jammy-security,now 2:2.4.4-0ubuntu0.22.04.2 amd64 [installed,automatic]
python3-markdown/jammy,now 3.3.6-1 all [installed,automatic]
python3-minimal/jammy-updates,now 3.10.6-1-22.04.1 amd64 [installed,automatic]
python3-more-itertools/jammy,now 8.10.0-2 all [installed,automatic]
python3-pkg-resources/jammy-updates,jammy-security,now 59.6.0-1.2ubuntu0.22.04.2 all [installed,automatic]
python3-pygments/jammy-updates,jammy-security,now 2.11.2+dfsg-2ubuntu0.1 all [installed,automatic]
python3-requests-toolbelt/jammy,now 0.9.1-1 all [installed,automatic]
python3-requests/jammy-updates,jammy-security,now 2.25.1+dfsg-2ubuntu0.1 all [installed,automatic]
python3-samba/jammy-updates,now 2:4.15.13+dfsg-0ubuntu1.6 amd64 [installed,automatic]
python3-six/jammy,now 1.16.0-3ubuntu1 all [installed,automatic]
```

Continuing list of all installed packages.

JOHN MALLON

PROJECT 1 – HARDENING A LINUX SERVER

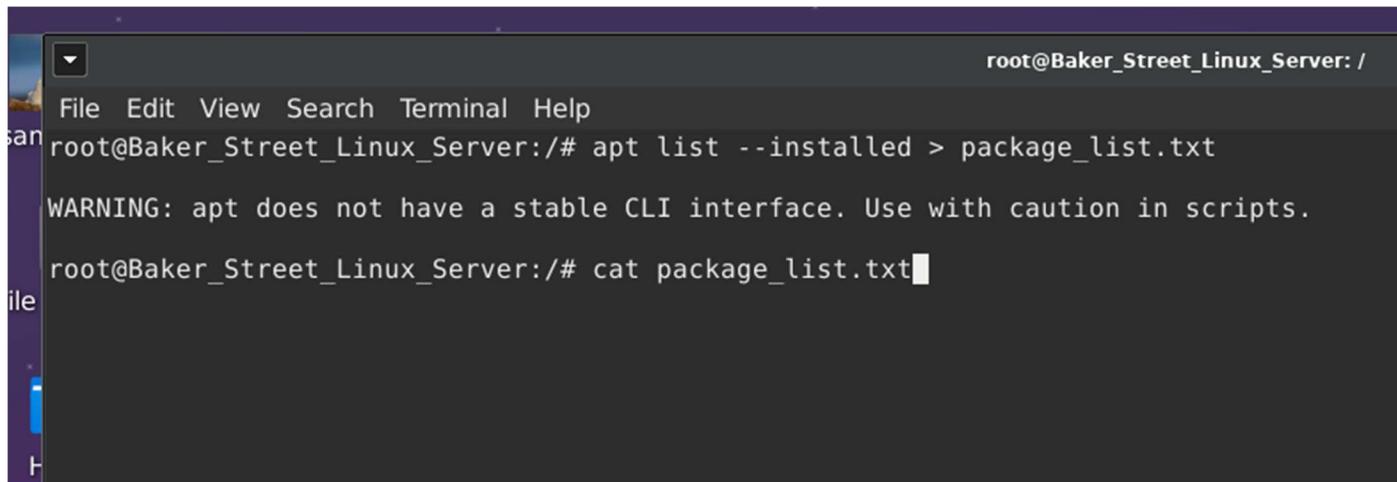


The screenshot shows a terminal window titled "root@Baker_Street_Linux_Server:/". The window displays a large list of installed packages, primarily from the "jammy" release, including various Python modules, system utilities, and security patches. The list is scrollable, indicating many packages are present.

```
root@Baker_Street_Linux_Server:/ 
File Edit View Search Terminal Help
python3-gi/jammy-updates,now 3.42.1-0ubuntu1 amd64 [installed,automatic]
python3-gpg/jammy-updates,now 1.16.0-1.2ubuntu4.2 amd64 [installed,automatic]
python3-idna/jammy-updates,jammy-security,now 3.3-1ubuntu0.1 all [installed,automatic]
python3-importlib-metadata/jammy,now 4.6.4-1 all [installed,automatic]
python3-ldb/jammy-updates,jammy-security,now 2:2.4.4-0ubuntu0.22.04.2 amd64 [installed,automatic]
python3-markdown/jammy,now 3.3.6-1 all [installed,automatic]
python3-minimal/jammy-updates,now 3.10.6-1-22.04.1 amd64 [installed,automatic]
python3-more-itertools/jammy,now 8.10.0-2 all [installed,automatic]
python3-pkg-resources/jammy-updates,jammy-security,now 59.6.0-1.2ubuntu0.22.04.2 all [installed,automatic]
python3-pgments/jammy-updates,jammy-security,now 2.11.2+dfsg-2ubuntu0.1 all [installed,automatic]
python3-requests-toolbelt/jammy,now 0.9.1-1 all [installed,automatic]
python3-requests/jammy-updates,jammy-security,now 2.25.1+dfsg-2ubuntu0.1 all [installed,automatic]
python3-samba/jammy-updates,now 2:4.15.13+dfsg-0ubuntu1.6 amd64 [installed,automatic]
python3-six/jammy,now 1.16.0-3ubuntu1 all [installed,automatic]
python3-talloc/jammy,now 2.3.3-2build1 amd64 [installed,automatic]
python3-tdb/jammy,now 1.4.5-2build1 amd64 [installed,automatic]
python3-urllib3/jammy-updates,jammy-security,now 1.26.5-1-explubuntu0.2 all [installed,automatic]
python3-yaml/jammy,now 5.4.1-1ubuntu1 amd64 [installed,automatic]
python3-zipp/jammy-updates,jammy-security,now 1.0.0-3ubuntu0.1 all [installed,automatic]
python3.10-minimal/jammy-updates,jammy-security,now 3.10.12-1~22.04.7 amd64 [installed,automatic]
python3.10/jammy-updates,jammy-security,now 3.10.12-1~22.04.7 amd64 [installed,automatic]
python3/jammy-updates,now 3.10.6-1-22.04.1 amd64 [installed,automatic]
readline-common/jammy,now 8.1.2-1 all [installed,automatic]
rsh-client/jammy,now 0.17-22 amd64 [installed]
rsh-server/jammy,now 0.17-22 amd64 [installed]
rsyslog/jammy-updates,jammy-security,now 8.2112.0-2ubuntu2.2 amd64 [installed]
samba-common-bin/jammy-updates,now 2:4.15.13+dfsg-0ubuntu1.6 amd64 [installed,automatic]
samba-common/jammy-updates,now 2:4.15.13+dfsg-0ubuntu1.6 all [installed,automatic]
samba-dsdb-modules/jammy-updates,now 2:4.15.13+dfsg-0ubuntu1.6 amd64 [installed,automatic]
samba-libs/jammy-updates,now 2:4.15.13+dfsg-0ubuntu1.6 amd64 [installed,automatic]
samba-vfs-modules/jammy-updates,now 2:4.15.13+dfsg-0ubuntu1.6 amd64 [installed,automatic]
samba/jammy-updates,now 2:4.15.13+dfsg-0ubuntu1.6 amd64 [installed]
sed/jammy,now 4.8-lubuntu2 amd64 [installed]
sensible-utils/jammy,now 0.0.17 all [installed]
shared-mime-info/jammy,now 2.1-2 amd64 [installed,automatic]
ssh-import-id/jammy,now 5.11-0ubuntu1 all [installed,automatic]
sudo/jammy-updates,jammy-security,now 1.9.9-1ubuntu2.4 amd64 [installed]
systemd-sysv/jammy-updates,now 249.11-0ubuntu3.12 amd64 [installed,automatic]
systemd-timesyncd/jammy-updates,now 249.11-0ubuntu3.12 amd64 [installed,automatic]
systemd/jammy-updates,now 249.11-0ubuntu3.12 amd64 [installed,automatic]
sysvinit-utils/jammy,now 3.01-1ubuntu1 amd64 [installed]
tar/jammy-updates,jammy-security,now 1.34+dfsg-lubuntu0.1.22.04.2 amd64 [installed]
tcpd/jammy,now 7.6.q-31build2 amd64 [installed,automatic]
tdb-tools/jammy,now 1.4.5-2build1 amd64 [installed,automatic]
telnet/jammy,now 0.17-44build1 amd64 [installed]
tree/jammy,now 2.0.2-1 amd64 [installed]
ubuntu-keyring/jammy,now 2021.03.26 all [installed]
ucf/jammy,now 3.0043 all [installed,automatic]
update-inetd/jammy,now 4.51 all [installed,automatic]
usrmerge/jammy,now 25ubuntu2 all [installed]
util-linux/jammy-updates,jammy-security,now 2.37.2-4ubuntu3.4 amd64 [installed]
wget/jammy-updates,jammy-security,now 1.21.2-2ubuntu1.1 amd64 [installed,automatic]
xauth/jammy,now 1:1.1-1build2 amd64 [installed,automatic]
xdg-user-dirs/jammy,now 0.17-2ubuntu4 amd64 [installed,automatic]
zlib1g/jammy-updates,jammy-security,now 1:1.2.11.dfsg-2ubuntu9.2 amd64 [installed]
root@Baker_Street_Linux_Server:/#
```

Continuing list of all installed packages.

JOHN MALLON



A screenshot of a terminal window titled "Terminal". The window shows a root shell session on a Linux server named "Baker_Street_Linux_Server". The user runs the command "apt list --installed > package_list.txt", which generates a warning about the CLI interface being unstable. Then, the user runs "cat package_list.txt" to view the contents of the file.

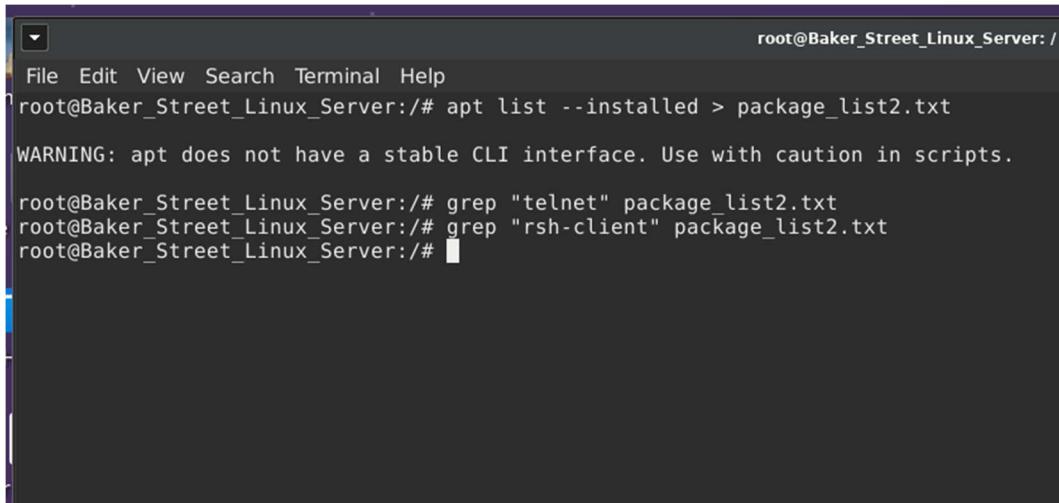
```
root@Baker_Street_Linux_Server:/# apt list --installed > package_list.txt
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.
root@Baker_Street_Linux_Server:/# cat package_list.txt
```

Create a file package_list.txt which contains all the installed packages.

PROJECT 1 – HARDENING A LINUX SERVER

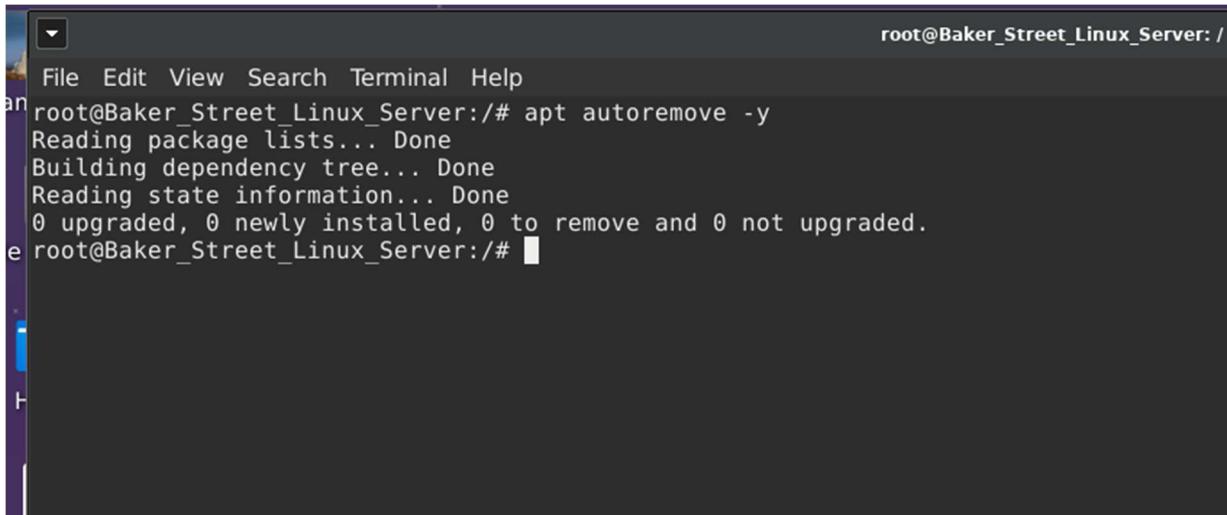
```
root@Baker_Street_Linux_Server:/ 
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# grep "telnet" package_list.txt
telnet/jammy,now 0.17-44build1 amd64 [installed]
root@Baker_Street_Linux_Server:/# grep "rsh-client" package_list.txt
rsh-client/jammy,now 0.17-22 amd64 [installed]
root@Baker_Street_Linux_Server:/# sudo apt remove telnet
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
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, 158 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 16312 files and directories currently installed.)
Removing telnet (0.17-44build1) ...
root@Baker_Street_Linux_Server:/# sudo apt remove rsh-client
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package rsh-client
root@Baker_Street_Linux_Server:/# sudo apt remove rsh-client
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  rsh-client
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 105 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 16303 files and directories currently installed.)
Removing rsh-client (0.17-22) ...
update-alternatives: using /usr/bin/scp to provide /usr/bin/rcp (rcp) in auto mode
update-alternatives: warning: skip creation of /usr/share/man/man1/rcp.1.gz because associated file /usr/share/man/man1/scp doesn't exist
update-alternatives: using /usr/bin/ssh to provide /usr/bin/rsh (rsh) in auto mode
update-alternatives: warning: skip creation of /usr/share/man/man1/rsh.1.gz because associated file /usr/share/man/man1/ssh doesn't exist
update-alternatives: using /usr/bin/slogin to provide /usr/bin/rlogin (rlogin) in auto mode
update-alternatives: warning: skip creation of /usr/share/man/man1/rlogin.1.gz because associated file /usr/share/man/man1/slogin doesn't exist
root@Baker_Street_Linux_Server:/# 
```

Identifying and removing telnet and rsh-client and all unnecessary dependencies.



```
root@Baker_Street_Linux_Server:/ 
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# apt list --installed > package_list2.txt
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.
root@Baker_Street_Linux_Server:/# grep "telnet" package_list2.txt
root@Baker_Street_Linux_Server:/# grep "rsh-client" package_list2.txt
root@Baker_Street_Linux_Server:/# 
```

Confirming telnet and rsh-client are no longer in the package list.



```
root@Baker_Street_Linux_Server:/ 
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# apt autoremove -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@Baker_Street_Linux_Server:/# 
```

Confirming telnet and rsh-client are no longer in the package list.

PROJECT 1 – HARDENING A LINUX SERVER

```
File Edit View Search Terminal Help
an root@Baker_Street_Linux_Server:/# sudo apt install ufw
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  iptables libip6tc2 libnetfilter-contrack3 libnfnetwork0 libnftnl11
Suggested packages:
  firewalld kmod nftables
The following NEW packages will be installed:
  iptables libip6tc2 libnetfilter-contrack3 libnfnetwork0 libnftnl11 ufw
0 upgraded, 6 newly installed, 0 to remove and 0 not upgraded.
Need to get 764 kB of archives.
After this operation, 4266 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 libip6tc2 amd64 1.8.7-1ubuntu5.2 [20.3 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy/main amd64 libnfnetwork0 amd64 1.0.1-3build3 [14.6 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy/main amd64 libnetfilter-contrack3 amd64 1.0.9-1 [45.3 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy/main amd64 libnftnl11 amd64 1.2.1-1build1 [65.5 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 iptables amd64 1.8.7-1ubuntu5.2 [455 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 ufw all 0.36.1-4ubuntu0.1 [162 kB]
Fetched 764 kB in 10s (75.0 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package libip6tc2:amd64.
(Reading database ... 16292 files and directories currently installed.)
Preparing to unpack .../0-libip6tc2_1.8.7-1ubuntu5.2_amd64.deb ...
Unpacking libip6tc2:amd64 (1.8.7-1ubuntu5.2) ...
Selecting previously unselected package libnfnetwork0:amd64.
Preparing to unpack .../1-libnfnetwork0_1.0.1-3build3_amd64.deb ...
Unpacking libnfnetwork0:amd64 (1.0.1-3build3) ...
Selecting previously unselected package libnetfilter-contrack3:amd64.
Preparing to unpack .../2-libnetfilter-contrack3_1.0.9-1_amd64.deb ...
Unpacking libnetfilter-contrack3:amd64 (1.0.9-1) ...
Selecting previously unselected package libnftnl11:amd64.
Preparing to unpack .../3-libnftnl11_1.2.1-1build1_amd64.deb ...
Unpacking libnftnl11:amd64 (1.2.1-1build1) ...
Selecting previously unselected package iptables.
Preparing to unpack .../4-iptables_1.8.7-1ubuntu5.2_amd64.deb ...
Unpacking iptables (1.8.7-1ubuntu5.2) ...
Selecting previously unselected package ufw.
Preparing to unpack .../5-ufw_0.36.1-4ubuntu0.1_all.deb ...
Unpacking ufw (0.36.1-4ubuntu0.1) ...
Setting up libip6tc2:amd64 (1.8.7-1ubuntu5.2) ...
Setting up libnftnl11:amd64 (1.2.1-1build1) ...
Setting up libnfnetwork0:amd64 (1.0.1-3build3) ...
Setting up libnetfilter-contrack3:amd64 (1.0.9-1) ...
Setting up iptables (1.8.7-1ubuntu5.2) ...
update-alternatives: using /usr/sbin/iptables-legacy to provide /usr/sbin/iptables (iptables) in auto mode
update-alternatives: using /usr/sbin/ip6tables-legacy to provide /usr/sbin/ip6tables (ip6tables) in auto mode
update-alternatives: using /usr/sbin/iptables-nft to provide /usr/sbin/iptables (iptables) in auto mode
update-alternatives: using /usr/sbin/ip6tables-nft to provide /usr/sbin/ip6tables (ip6tables) in auto mode
update-alternatives: using /usr/sbin/arptables-nft to provide /usr/sbin/arptables (arptables) in auto mode
update-alternatives: using /usr/sbin/ebtables-nft to provide /usr/sbin/ebtables (ebtables) in auto mode
Setting up ufw (0.36.1-4ubuntu0.1) ...
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd/Dialog.pm:11)
```

Adding ufw package.

JOHN MALLON

```
update-alternatives: using /usr/sbin/arptables-nft to provide /usr/sbin/arptables (arptables) in auto mode
update-alternatives: using /usr/sbin/ebtables-nft to provide /usr/sbin/ebtables (ebtables) in auto mode
Setting up ufw (0.36.1-4ubuntu0.1) ...
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/debconf/frontend)
debconf: falling back to frontend: Readline

Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version

Creating config file /etc/ufw/after6.rules with new version
Created symlink /etc/systemd/system/multi-user.target.wants/ufw.service → /lib/systemd/system/ufw.service.
Processing triggers for rsyslog (8.2112.0-2ubuntu2.2) ...
invoke-rc.d: unknown initscript, /etc/init.d/rsyslog not found.
invoke-rc.d: could not determine current runlevel
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...
root@Baker_Street_Linux_Server:/# █
```

Confirming ufw package install.

```
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# sudo apt install lynis
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  menu
Suggested packages:
  dnsutils apt-listbugs debsecan debsums tripwire samhain aide fail2ban menu-l10n gksu | kde-runtime |
The following NEW packages will be installed:
  lynis menu
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 581 kB of archives.
After this operation, 3164 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 lynis all 3.0.7-1 [227 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy/universe amd64 menu amd64 2.1.47ubuntu4 [354 kB]
Fetched 581 kB in 10s (57.1 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package lynis.
(Reading database ... 16659 files and directories currently installed.)
Preparing to unpack .../archives/lynis_3.0.7-1_all.deb ...
Unpacking lynis (3.0.7-1) ...
Selecting previously unselected package menu.
Preparing to unpack .../menu_2.1.47ubuntu4_amd64.deb ...
Unpacking menu (2.1.47ubuntu4) ...
Setting up lynis (3.0.7-1) ...
Created symlink /etc/systemd/system/timers.target.wants/lynis.timer → /lib/systemd/system/lynis.timer.
Setting up menu (2.1.47ubuntu4) ...
Processing triggers for menu (2.1.47ubuntu4) ...
root@Baker_Street_Linux_Server:/#
```

Installing lynis.

```
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# sudo apt install tripwire
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  cpio postfix ssl-cert
Suggested packages:
  libarchivel procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb postfix-sqlite sasl2-bin | dovecot-common
  postfix-cdb mail-reader postfix-mta-sts-resolver postfix-doc
The following NEW packages will be installed:
  cpio postfix ssl-cert tripwire
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 3199 kB of archives.
After this operation, 16.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy/main amd64 ssl-cert all 1.1.2 [17.4 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 cpio amd64 2.13+dfsg-7ubuntu0.1 [84.5 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 postfix amd64 3.6.4-1ubuntu1.3 [1248 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy/universe amd64 tripwire amd64 2.4.3.7-4 [1849 kB]
Fetched 3199 kB in 10s (313 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package ssl-cert.
(Reading database ... 16962 files and directories currently installed.)
Preparing to unpack .../ssl-cert_1.1.2_all.deb ...
Unpacking ssl-cert (1.1.2) ...
Selecting previously unselected package cpio.
Preparing to unpack .../cpio_2.13+dfsg-7ubuntu0.1_amd64.deb ...
Unpacking cpio (2.13+dfsg-7ubuntu0.1) ...
Selecting previously unselected package postfix.
Preparing to unpack .../postfix_3.6.4-1ubuntu1.3_amd64.deb ...
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd/Dialog.pm line 78.)
debconf: falling back to frontend: Readline
Postfix Configuration
-----
Please select the mail server configuration type that best meets your needs.

No configuration:
Should be chosen to leave the current configuration unchanged.
Internet site:
Mail is sent and received directly using SMTP.
Internet with smarthost:
Mail is received directly using SMTP or by running a utility such
as fetchmail. Outgoing mail is sent using a smarthost.
Satellite system:
All mail is sent to another machine, called a 'smarthost', for
delivery.
Local only:
The only delivered mail is the mail for local users. There is no
network.

1. No configuration 2. Internet Site 3. Internet with smarthost 4. Satellite system 5. Local only
General mail configuration type: 1
```

Installing tripwire.

PROJECT 1 – HARDENING A LINUX SERVER

```
root@Baker_Street_Linux_Server: /  
File Edit View Search Terminal Help  
an 1. No configuration 2. Internet Site 3. Internet with smarthost 4. Satellite system 5. Local only  
General mail configuration type: 1  
Unpacking postfix (3.6.4-1ubuntu1.3) ...  
Selecting previously unselected package tripwire.  
e Preparing to unpack .../tripwire_2.4.3.7-4_amd64.deb ...  
Unpacking tripwire (2.4.3.7-4) ...  
Setting up cpio (2.13+dfsg-7ubuntu0.1) ...  
update-alternatives: using /bin/mt-gnu to provide /bin/mt (mt) in auto mode  
update-alternatives: warning: skip creation of /usr/share/man/man1/mt-gnu.1.gz because associated file /usr/share/man/man1/mt-gnu.1.gz (c  
) doesn't exist  
Setting up ssl-cert (1.1.2) ...  
debconf: unable to initialize frontend: Dialog  
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd  
ne 78.)  
debconf: falling back to frontend: Readline  
hostname: Temporary failure in name resolution  
make-ssl-cert: Could not get FQDN, using 'Baker_Street_Linux_Server'.  
make-ssl-cert: You may want to fix your /etc/hosts and/or DNS setup and run  
make-ssl-cert: 'make-ssl-cert generate-default-snakeoil --force-overwrite'  
make-ssl-cert: again.  
Setting up postfix (3.6.4-1ubuntu1.3) ...  
debconf: unable to initialize frontend: Dialog  
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd  
ne 78.)  
debconf: falling back to frontend: Readline  
Adding group `postfix' (GID 113) ...  
Done.  
Adding system user `postfix' (UID 108) ...  
Adding new user `postfix' (UID 108) with group `postfix' ...  
Not creating home directory `/var/spool/postfix'.  
Creating /etc/postfix/dynamicmaps.cf  
Adding group `postdrop' (GID 114) ...  
Done.  
/etc/aliases does not exist, creating it.  
Postfix (main.cf) was not set up. Start with  
  cp /usr/share/postfix/main.cf.debian /etc/postfix/main.cf  
. If you need to make changes, edit /etc/postfix/main.cf (and others) as  
needed. To view Postfix configuration values, see postconf(1).  
After modifying main.cf, be sure to run 'systemctl reload postfix'.  
invoke-rc.d: could not determine current runlevel  
invoke-rc.d: policy-rc.d denied execution of start.  
Created symlink /etc/systemd/system/multi-user.target.wants/postfix.service → /lib/systemd/system/postfix.service.  
Setting up tripwire (2.4.3.7-4) ...  
debconf: unable to initialize frontend: Dialog  
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd  
ne 78.)  
debconf: falling back to frontend: Readline  
Tripwire Configuration  
-----  
Tripwire uses a pair of keys to sign various files, thus ensuring their unaltered state. By accepting here, you will be prompted for  
passphrase for the first of those keys, the site key, during the installation. You are also agreeing to create a site key if one doe
```

Tripwire installation.

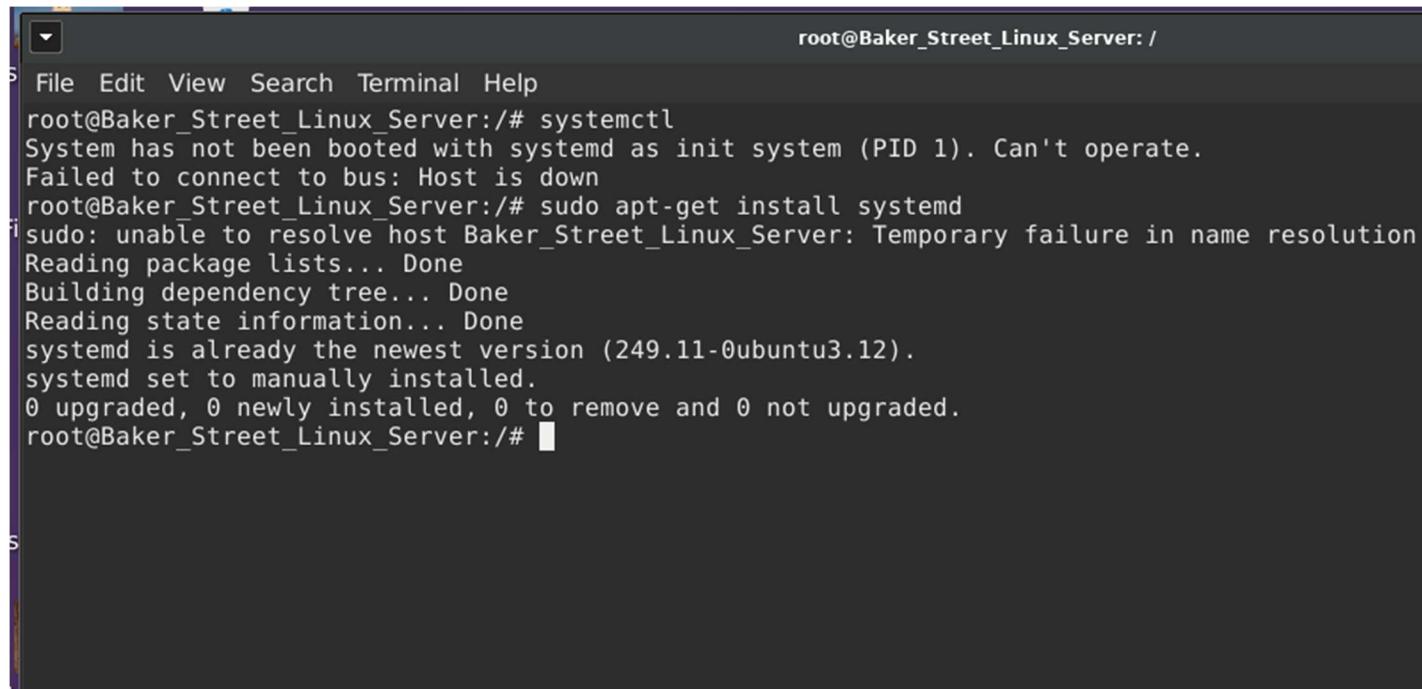
JOHN MALLON

PROJECT 1 – HARDENING A LINUX SERVER

```
root@Baker_Street_Linux_Server: /  
File Edit View Search Terminal Help  
1. If you need to make changes, edit /etc/postfix/main.cf (and others) as  
needed. To view Postfix configuration values, see postconf(1).  
After modifying main.cf, be sure to run 'systemctl reload postfix'.  
invoke-rc.d: could not determine current runlevel  
invoke-rc.d: policy-rc.d denied execution of start.  
Created symlink /etc/systemd/system/multi-user.target.wants/postfix.service → /lib/systemd/system/postfix.service.  
Setting up tripwire (2.4.3.7-4) ...  
debconf: unable to initialize frontend: Dialog  
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/Frontend/Dialog.pm 78.)  
debconf: falling back to frontend: Readline  
Tripwire Configuration  
-----  
Tripwire uses a pair of keys to sign various files, thus ensuring their unaltered state. By accepting here, you will be prompted for  
passphrase for the first of those keys, the site key, during the installation. You are also agreeing to create a site key if one does  
already. Tripwire uses the site key to sign files that may be common to multiple systems, e.g. the configuration & policy files. See  
for more information.  
Unfortunately, due to the Debian installation process, there is a period of time where this passphrase exists in an unencrypted format.  
attacker to have access to your machine during this period, he could possibly retrieve your passphrase and use it at some later point.  
If you would rather not have this exposure, decline here. You will then need to create a site key, configuration file & policy file  
twadmin(8) for more information.  
Do you wish to create/use your site key passphrase during installation? [yes/no] n  
Tripwire uses a pair of keys to sign various files, thus ensuring their unaltered state. By accepting here, you will be prompted for  
passphrase for the second of those keys, the local key, during the installation. You are also agreeing to create a local key if one does  
already. Tripwire uses the local key to sign files that are specific to this system, e.g. the tripwire database. See twfiles(5) for  
information.  
Unfortunately, due to the Debian installation process, there is a period of time where this passphrase exists in an unencrypted format.  
attacker to have access to your machine during this period, he could possibly retrieve your passphrase and use it at some later point.  
If you would rather not have this exposure, decline here. You will then need to create a local key file by hand. See twadmin(8) for  
information.  
Do you wish to create/use your local key passphrase during installation? [yes/no] no  
chmod: cannot access '/etc/tripwire/site.key': No such file or directory  
chmod: cannot access '/etc/tripwire/Baker_Street_Linux_Server-local.key': No such file or directory  
Tripwire has been installed  
The Tripwire binaries are located in /usr/sbin and the database is located in /var/lib/tripwire. It is strongly advised that these be  
stored on write-protected media (e.g. mounted RO floppy). See /usr/share/doc/tripwire/README.Debian for details.  
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...  
Processing triggers for rsyslog (8.2112.0-2ubuntu2.2) ...  
invoke-rc.d: unknown initscript, /etc/init.d/rsyslog not found.  
invoke-rc.d: could not determine current runlevel  
root@Baker_Street_Linux_Server:/#
```

Tripwire installation.

JOHN MALLON

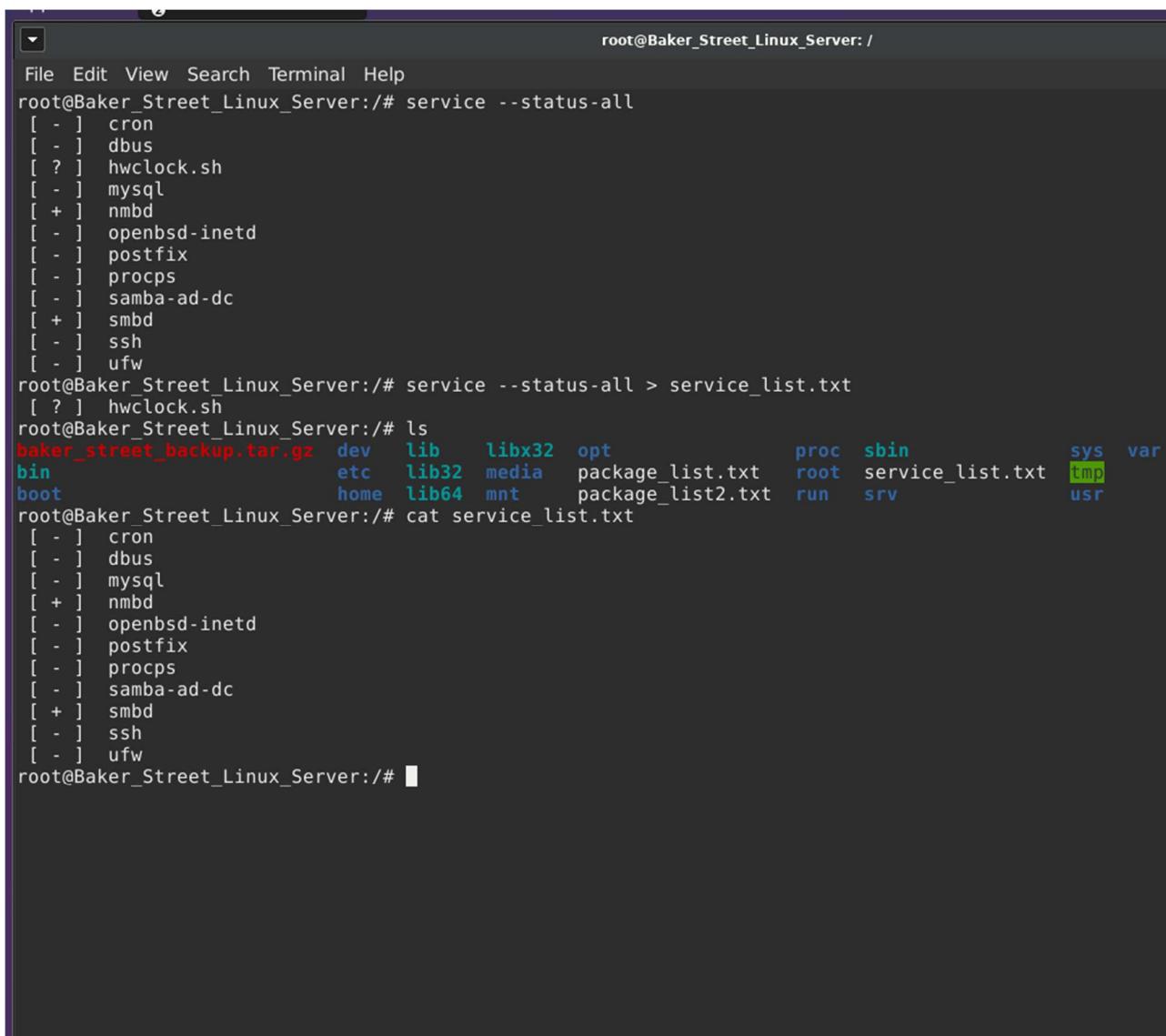


The screenshot shows a terminal window with a dark background and light-colored text. At the top right, it says "root@Baker_Street_Linux_Server: /". The terminal output is as follows:

```
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# systemctl
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
root@Baker_Street_Linux_Server:/# sudo apt-get install systemd
[sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
systemd is already the newest version (249.11-0ubuntu3.12).
systemd set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@Baker_Street_Linux_Server:/# ]
```

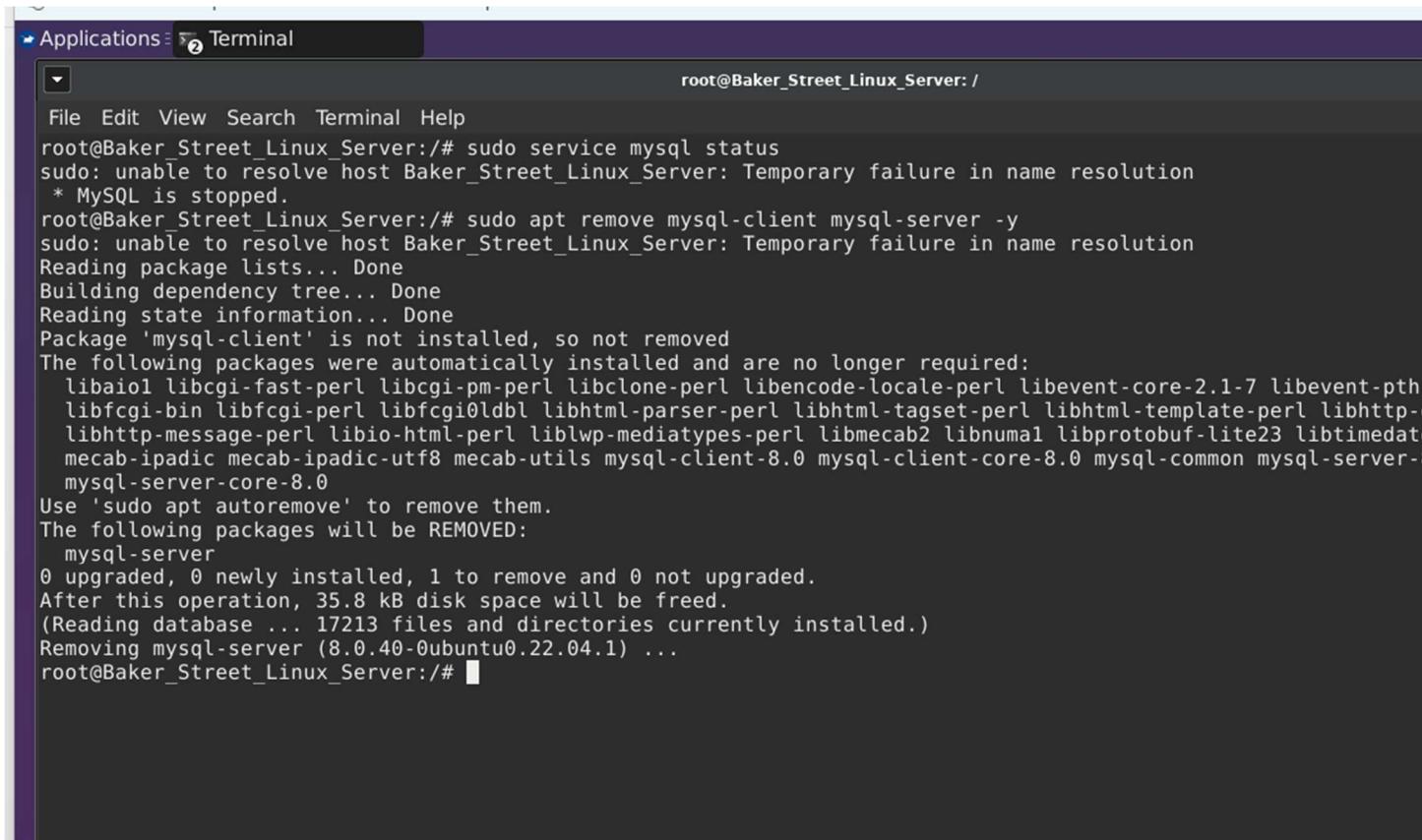
Part 3: Disabling Unnecessary Services

Attempt to run the systemctl command as instructed, but it is not and cannot be installed.



```
root@Baker_Street_Linux_Server:/# service --status-all
[ - ] cron
[ - ] dbus
[ ? ] hwclock.sh
[ - ] mysql
[ + ] nmbd
[ - ] openbsd-inetd
[ - ] postfix
[ - ] procps
[ - ] samba-ad-dc
[ + ] smbd
[ - ] ssh
[ - ] ufw
root@Baker_Street_Linux_Server:/# service --status-all > service_list.txt
[ ? ] hwclock.sh
root@Baker_Street_Linux_Server:/# ls
baker_street_backup.tar.gz  dev  lib   lib32  opt      proc  sbin    sys  var
bin                         etc  lib32 media package_list.txt  root  service_list.txt  tmp
boot                        home lib64 mnt   package_list2.txt run   srv     usr
root@Baker_Street_Linux_Server:/# cat service_list.txt
[ - ] cron
[ - ] dbus
[ - ] mysql
[ + ] nmbd
[ - ] openbsd-inetd
[ - ] postfix
[ - ] procps
[ - ] samba-ad-dc
[ + ] smbd
[ - ] ssh
[ - ] ufw
root@Baker_Street_Linux_Server:/# █
```

Listing services.

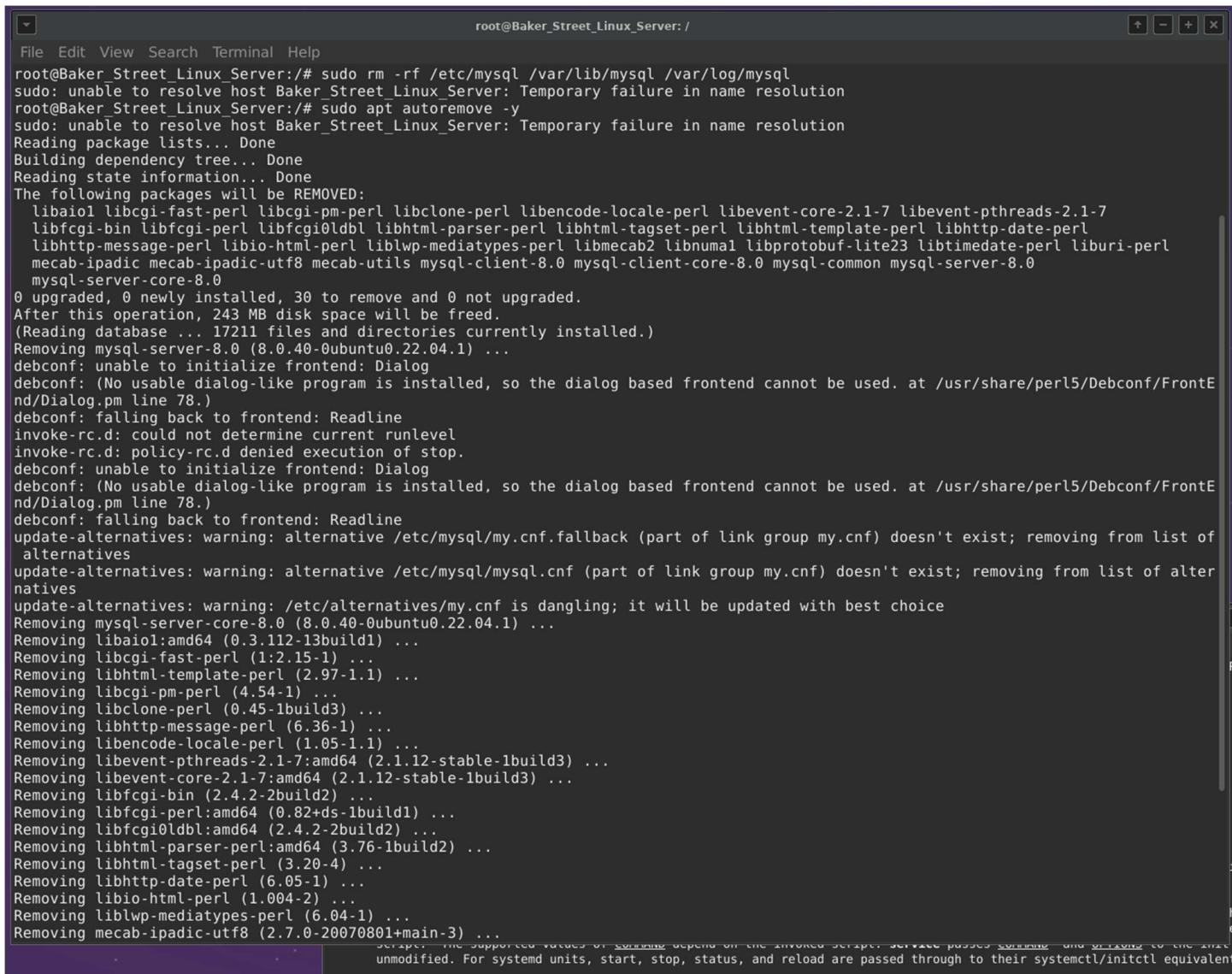


The screenshot shows a terminal window titled "Terminal" under "Applications". The command "sudo apt remove mysql-client mysql-server -y" is run as root. The output shows that MySQL is stopped and removed, along with its dependencies like libaio1, libcgifast-perl, etc. The process is completed successfully.

```
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# sudo service mysql status
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
 * MySQL is stopped.
root@Baker_Street_Linux_Server:/# sudo apt remove mysql-client mysql-server -y
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
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:
  libaio1 libcgifast-perl libcgipm-perl libclone-perl libencode-locale-perl libevent-core-2.1-7 libevent-pth
  libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-parser-perl libhtml-tsgt-perl libhtml-template-perl libhttp-
  libhttp-message-perl libio-html-perl liblwp-mediatypes-perl libmecab2 libnumua libprotobuf-lite23 libtimedat
  mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0 mysql-client-core-8.0 mysql-common mysql-server-
  mysql-server-core-8.0
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  mysql-server
  0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 35.8 kB disk space will be freed.
(Reading database ... 17213 files and directories currently installed.)
Removing mysql-server (8.0.40-0ubuntu0.22.04.1) ...
root@Baker_Street_Linux_Server:/#
```

Ensuring mysql is stopped and removed.

PROJECT 1 – HARDENING A LINUX SERVER



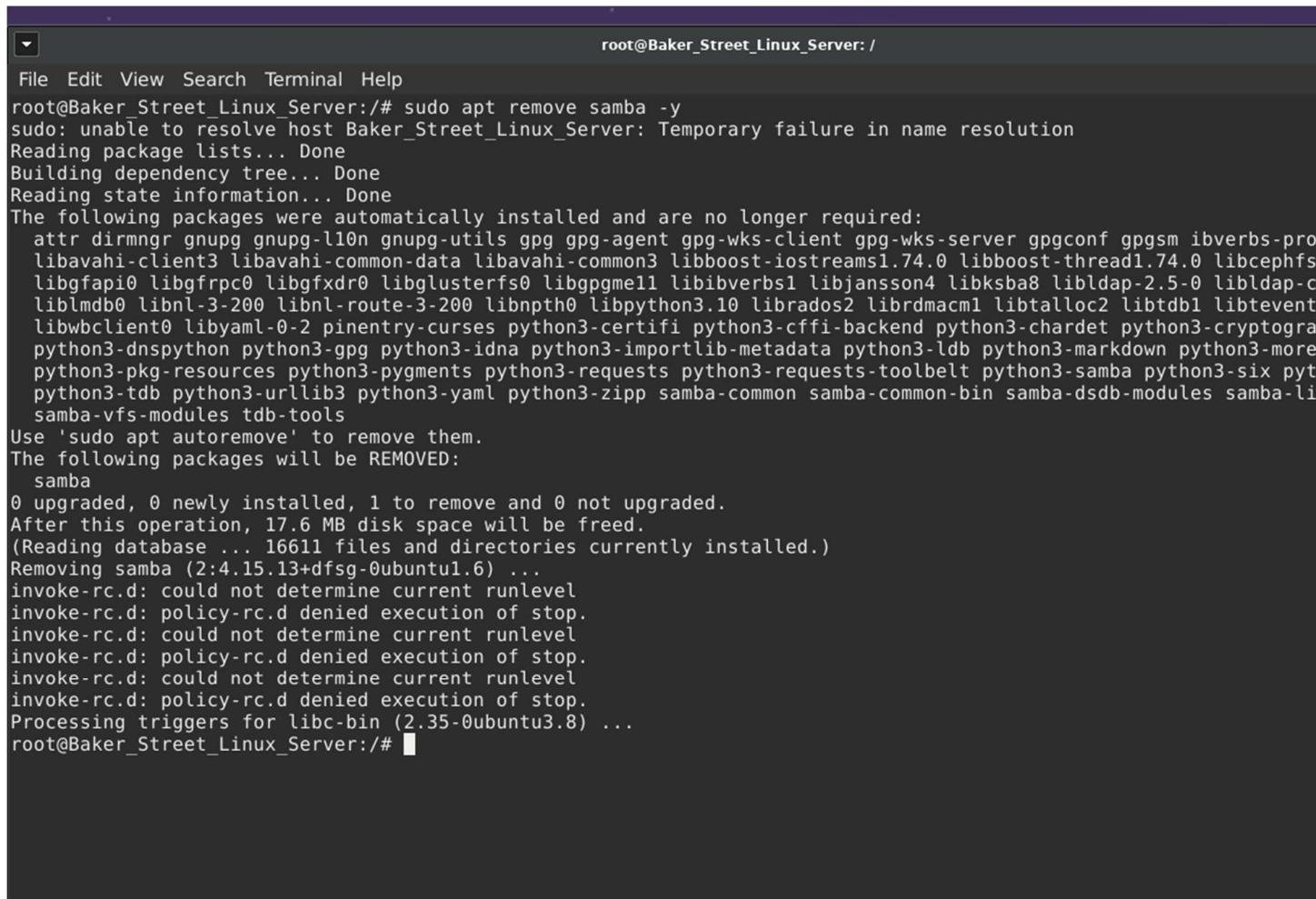
```
root@Baker_Street_Linux_Server:/# sudo rm -rf /etc/mysql /var/lib/mysql /var/log/mysql
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
root@Baker_Street_Linux_Server:/# sudo apt autoremove -y
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  libaio1 libcgi-fast-perl libcgi-pm-perl libclone-perl libencode-locale-perl libevent-core-2.1-7 libevent-pthreads-2.1-7
  libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-parser-perl libhtml-tagset-perl libhtml-template-perl libhttp-date-perl
  libhttp-message-perl libio-html-perl liblwp-mediatypes-perl libmecab2 libnumal libprotobuf-lite23 libtimage-perl liburi-perl
  mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0 mysql-client-core-8.0 mysql-common mysql-server-8.0
  mysql-server-core-8.0
0 upgraded, 0 newly installed, 30 to remove and 0 not upgraded.
After this operation, 243 MB disk space will be freed.
(Reading database ... 17211 files and directories currently installed.)
Removing mysql-server-8.0 (8.0.40-0ubuntu0.22.04.1) ...
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd/Dialog.pm line 78.)
debconf: falling back to frontend: Readline
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd/Dialog.pm line 78.)
debconf: falling back to frontend: Readline
update-alternatives: warning: alternative /etc/mysql/my.cnf.fallback (part of link group my.cnf) doesn't exist; removing from list of alternatives
update-alternatives: warning: alternative /etc/mysql/mysql.cnf (part of link group my.cnf) doesn't exist; removing from list of alternatives
update-alternatives: warning: /etc/alternatives/my.cnf is dangling; it will be updated with best choice
Removing mysql-server-core-8.0 (8.0.40-0ubuntu0.22.04.1) ...
Removing libaio1:amd64 (0.3.112-13build1) ...
Removing libcgi-fast-perl (1:2.15-1) ...
Removing libhtml-template-perl (2.97-1.1) ...
Removing libcgi-pm-perl (4.54-1) ...
Removing libclone-perl (0.45-1build3) ...
Removing libhttp-message-perl (6.36-1) ...
Removing libencode-locale-perl (1.05-1.1) ...
Removing libevent-pthreads-2.1-7:amd64 (2.1.12-stable-1build3) ...
Removing libevent-core-2.1-7:amd64 (2.1.12-stable-1build3) ...
Removing libfcgi-bin (2.4.2-2build2) ...
Removing libfcgi-perl:amd64 (0.82+ds-1build1) ...
Removing libfcgi0ldbl:amd64 (2.4.2-2build2) ...
Removing libhtml-parser-perl:amd64 (3.76-1build2) ...
Removing libhtml-tagset-perl (3.20-4) ...
Removing libhttp-date-perl (6.05-1) ...
Removing libio-html-perl (1.004-2) ...
Removing liblwp-mediatypes-perl (6.04-1) ...
Removing mecab-ipadic-utf8 (2.7.0-20070801+main-3) ...
Script: The supported values of control depend on the invoked script. service passes control and options to the initctl command. systemctl passes control unmodified. For systemd units, start, stop, status, and reload are passed through to their systemctl/initctl equivalent.
```

Ensuring mysql is stopped and removed.

JOHN MALLON

```
root@Baker_Street_Linux_Server:/#
File Edit View Search Terminal Help
0 upgraded, 0 newly installed, 30 to remove and 0 not upgraded.
After this operation, 243 MB disk space will be freed.
(Reading database ... 17211 files and directories currently installed.)
Removing mysql-server-8.0 (8.0.40-0ubuntu0.22.04.1) ...
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/Frontend/Dialog.pm line 78.)
debconf: falling back to frontend: Readline
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/Frontend/Dialog.pm line 78.)
debconf: falling back to frontend: Readline
update-alternatives: warning: alternative /etc/mysql/my.cnf.fallback (part of link group my.cnf) doesn't exist; removing from list of alternatives
update-alternatives: warning: alternative /etc/mysql/mysql.cnf (part of link group my.cnf) doesn't exist; removing from list of alternatives
update-alternatives: warning: /etc/alternatives/my.cnf is dangling; it will be updated with best choice
Removing mysql-server-core-8.0 (8.0.40-0ubuntu0.22.04.1) ...
Removing libaiol:amd64 (0.3.112-13build1) ...
Removing libcgi-fast-perl (1:2.15-1) ...
Removing libhtml-template-perl (2.97-1.1) ...
Removing libcgi-pm-perl (4.54-1) ...
Removing libclone-perl (0.45-1build3) ...
Removing libhttp-message-perl (6.36-1) ...
Removing libencode-locale-perl (1.05-1.1) ...
Removing libevent-pthreads-2.1-7:amd64 (2.1.12-stable-1build3) ...
Removing libevent-core-2.1-7:amd64 (2.1.12-stable-1build3) ...
Removing libfcgi-bin (2.4.2-2build2) ...
Removing libfcgi-perl:amd64 (0.82+ds-1build1) ...
Removing libfcgi0ldbl:amd64 (2.4.2-2build2) ...
Removing libhtml-parser-perl:amd64 (3.76-1build2) ...
Removing libhtml-tagset-perl (3.20-4) ...
Removing libhttp-date-perl (6.05-1) ...
Removing libio-html-perl (1.004-2) ...
Removing liblwp-mediatypes-perl (6.04-1) ...
Removing mecab-ipadic-utf8 (2.7.0-20070801+main-3) ...
update-alternatives: using /var/lib/mecab/dic/ipadic to provide /var/lib/mecab/dic/debian (mecab-dictionary) in auto mode
Removing mecab-ipadic (2.7.0-20070801+main-3) ...
Removing mecab-utils (0.996-14build9) ...
Removing libmecab2:amd64 (0.996-14build9) ...
Removing libnumual:amd64 (2.0.14-3ubuntu2) ...
Removing libprotobuf-lite23:amd64 (3.12.4-1ubuntu7.22.04.1) ...
Removing libtimedate-perl (2.3300-2) ...
Removing liburi-perl (5.10-1) ...
Removing mysql-client-8.0 (8.0.40-0ubuntu0.22.04.1) ...
Removing mysql-client-core-8.0 (8.0.40-0ubuntu0.22.04.1) ...
Removing mysql-common (5.8+1.0.8) ...
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...
root@Baker_Street_Linux_Server:/#
```

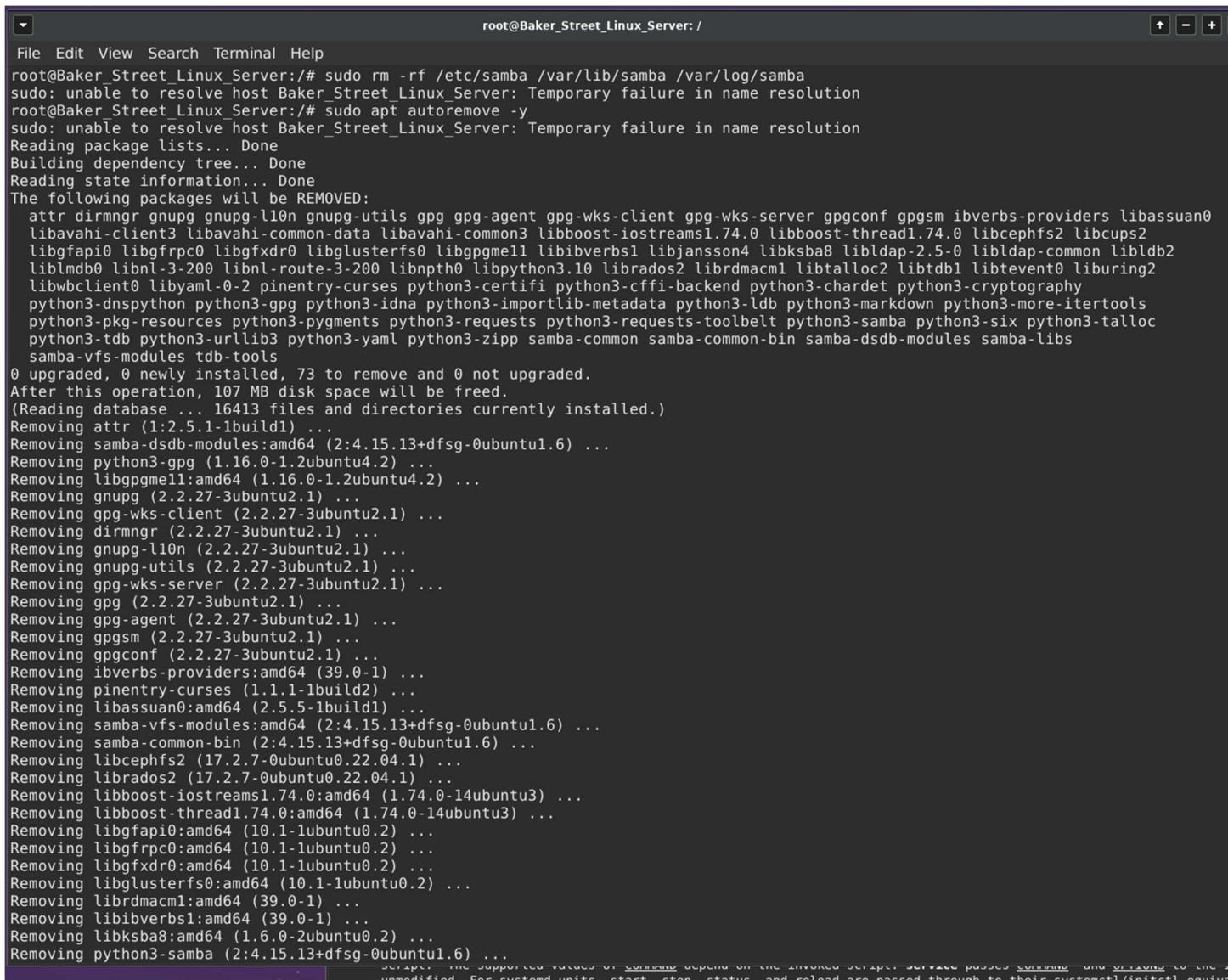
Ensuring mysql is stopped and removed.



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it says "root@Baker_Street_Linux_Server:/". The user runs the command "sudo apt remove samba -y". The output shows that the host name "Baker_Street_Linux_Server" could not be resolved. It then lists packages that were automatically installed and are no longer required, including various Python modules and system libraries. It asks the user to use "sudo apt autoremove" to remove them. It then lists packages that will be removed, specifically "samba". It shows that 0 packages were upgraded, 0 were newly installed, 1 was to be removed, and 0 were not upgraded. It also shows that 17.6 MB of disk space would be freed. The process continues with removing the "samba" package and its dependencies, including "libc-bin". The terminal ends with "root@Baker_Street_Linux_Server:/#".

```
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# sudo apt remove samba -y
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  attr dirmngr gnupg gnupg-l10n gnupg-utils gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf gpgsm ibverbs-proto
  libavahi-client3 libavahi-common-data libavahi-common3 libboost-iostreams1.74.0 libboost-thread1.74.0 libcephfs
  libgfapi0 libgfrpc0 libgfrpc0 libglusterfs0 libgpgme11 libibverbs1 libjansson4 libksba8 libldap-2.5-0 libldap-c
  liblmbdb0 libnl-3-200 libnl-route-3-200 libnpth0 libpython3.10 librados2 librdmacm1 libtalloc2 libtdb1 libtevent
  libwbclient0 libyaml-0-2 pinentry-curses python3-certifi python3-cffi-backend python3-chardet python3-cryptogra
  python3-dnspython python3-gpg python3-idna python3-importlib-metadata python3-ldb python3-markdown python3-more
  python3-pkg-resources python3-pgments python3-requests python3-requests-toolbelt python3-samba python3-six pyt
  python3-tdb python3-urllib3 python3-yaml python3-zipp samba-common samba-common-bin samba-dsdb-modules samba-li
  samba-vfs-modules tdb-tools
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  samba
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 17.6 MB disk space will be freed.
(Reading database ... 16611 files and directories currently installed.)
Removing samba (2:4.15.13+dfsg-0ubuntu1.6) ...
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...
root@Baker_Street_Linux_Server:/#
```

Ensuring samba is stopped and removed.



The screenshot shows a terminal window titled 'root@Baker_Street_Linux_Server: /'. The user is running a series of 'sudo rm' commands to remove Samba-related files from the '/etc/samba', '/var/lib/samba', and '/var/log/samba' directories. This results in numerous errors indicating that the host cannot be resolved. Subsequent 'sudo apt autoremove -y' commands are run, which attempt to remove the packages listed in the removal log. The log shows a large number of packages being identified for removal, including various GPG tools, CephFS, and Samba components. The process continues until all specified packages are removed.

```

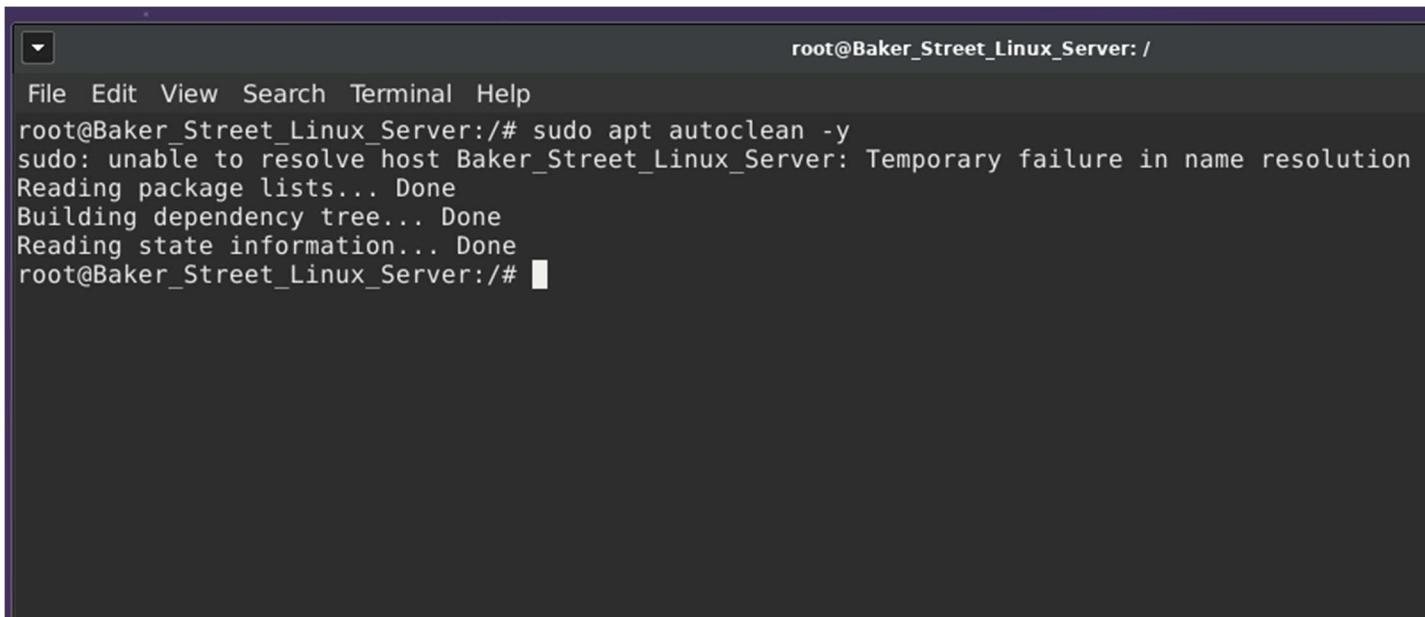
root@Baker_Street_Linux_Server:/# sudo rm -rf /etc/samba /var/lib/samba /var/log/samba
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
root@Baker_Street_Linux_Server:/# sudo apt autoremove -y
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  attr dirmngr gnupg gnupg-l10n gnupg-utils gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf gpgsm ibverbs-providers libassuan0
  libavahi-client3 libavahi-common libavahi-common-data libboost-iostreams1.74.0 libboost-thread1.74.0 libcephfs2 libcups2
  libgfapi0 libgfrpc0 libgwdxdr0 libglusterfs0 libgpgme11 libibverbs1 libjansson4 libksba8 libldap-2.5.0 libldap-common libldb2
  liblmdb0 liblmbc-3-200 liblnl-route-3-200 liblpth0 libpython3.10 librados2 librdmacm1 libtalloc2 libtldb1 libtevent0 liburing2
  libwbclient0 libyaml-0-2 pinentry-curses python3-certifi python3-cffi-backend python3-chardet python3-cryptography
  python3-dnspython python3-gpg python3-idna python3-importlib-metadata python3-ldb python3-markdown python3-more-itertools
  python3-pkg-resources python3-pymgents python3-requests python3-requests-toolbelt python3-samba python3-six python3-talloc
  python3-tdb python3-urllib3 python3-yaml python3-zipp samba-common samba-common-bin samba-common-modules samba-dsdb-modules samba-libs
  samba-vfs-modules tdb-tools
0 upgraded, 0 newly installed, 73 to remove and 0 not upgraded.
After this operation, 107 MB disk space will be freed.
(Reading database ... 16413 files and directories currently installed.)
Removing attr (1:2.5.1-1build1) ...
Removing samba-dsdb-modules:amd64 (2:4.15.13+dfsg-0ubuntu1.6) ...
Removing python3-gpg (1.16.0-1.2ubuntu4.2) ...
Removing libgpgme11:amd64 (1.16.0-1.2ubuntu4.2) ...
Removing gnupg (2.2.27-3ubuntu2.1) ...
Removing gpg-wks-client (2.2.27-3ubuntu2.1) ...
Removing dirmngr (2.2.27-3ubuntu2.1) ...
Removing gnupg-l10n (2.2.27-3ubuntu2.1) ...
Removing gnupg-utils (2.2.27-3ubuntu2.1) ...
Removing gpg-wks-server (2.2.27-3ubuntu2.1) ...
Removing gpg (2.2.27-3ubuntu2.1) ...
Removing gpg-agent (2.2.27-3ubuntu2.1) ...
Removing gpgsm (2.2.27-3ubuntu2.1) ...
Removing gpgconf (2.2.27-3ubuntu2.1) ...
Removing ibverbs-providers:amd64 (39.0-1) ...
Removing pinentry-curses (1.1.1-1build2) ...
Removing libassuan0:amd64 (2.5.5-1build1) ...
Removing samba-vfs-modules:amd64 (2:4.15.13+dfsg-0ubuntu1.6) ...
Removing samba-common-bin (2:4.15.13+dfsg-0ubuntu1.6) ...
Removing libcephfs2 (17.2.7-0ubuntu0.22.04.1) ...
Removing librados2 (17.2.7-0ubuntu0.22.04.1) ...
Removing libboost-iostreams1.74.0:amd64 (1.74.0-14ubuntu3) ...
Removing libboost-thread1.74.0:amd64 (1.74.0-14ubuntu3) ...
Removing libgfapi0:amd64 (10.1-1ubuntu0.2) ...
Removing libgfrpc0:amd64 (10.1-1ubuntu0.2) ...
Removing libgwdxdr0:amd64 (10.1-1ubuntu0.2) ...
Removing libglusterfs0:amd64 (10.1-1ubuntu0.2) ...
Removing librdmacm1:amd64 (39.0-1) ...
Removing libibverbs1:amd64 (39.0-1) ...
Removing libksba8:amd64 (1.6.0-2ubuntu0.2) ...
Removing python3-samba (2:4.15.13+dfsg-0ubuntu1.6) ...

```

Ensuring samba is stopped and removed.

```
root@Baker_Street_Linux_Server:/  
File Edit View Search Terminal Help  
Removing libglusterfs0:amd64 (10.1-1ubuntu0.2) ...  
Removing librdmacm1:amd64 (39.0-1) ...  
Removing libibverbs1:amd64 (39.0-1) ...  
Removing libksba8:amd64 (1.6.0-2ubuntu0.2) ...  
Removing python3-samba (2:4.15.13+dfsg-0ubuntu1.6) ...  
Removing libldap-common (2.5.18+dfsg-0ubuntu0.22.04.2) ...  
Removing libnl-route-3-200:amd64 (3.5.0-0.1) ...  
Removing libnl-3-200:amd64 (3.5.0-0.1) ...  
Removing libnpth0:amd64 (1.6-3build2) ...  
Removing tdb-tools (1.4.5-2build1) ...  
Removing python3-tdb (1.4.5-2build1) ...  
Removing liburing2:amd64 (2.1-2build1) ...  
Removing python3-yaml (5.4.1-1ubuntu1) ...  
Removing libyaml-0-2:amd64 (0.2.2-1build2) ...  
Removing python3-requests-toolbelt (0.9.1-1) ...  
Removing python3-requests (2.25.1+dfsg-2ubuntu0.1) ...  
Removing python3-certifi (2020.6.20-1) ...  
Removing python3-cryptography (3.4.8-1ubuntu2.2) ...  
Removing python3-cffi-backend:amd64 (1.15.0-1build2) ...  
Removing python3-chardet (4.0.0-1) ...  
Removing python3-dnspython (2.1.0-1ubuntu1) ...  
Removing python3-idna (3.3-1ubuntu0.1) ...  
Removing python3-markdown (3.3.6-1) ...  
Removing python3-importlib-metadata (4.6.4-1) ...  
Removing python3-zipp (1.0.0-3ubuntu0.1) ...  
Removing python3-more-itertools (8.10.0-2) ...  
Removing python3-pgments (2.11.2+dfsg-2ubuntu0.1) ...  
Removing python3-pkg-resources (59.6.0-1.2ubuntu0.22.04.2) ...  
Removing python3-urllib3 (1.26.5-1-exp1ubuntu0.2) ...  
Removing python3-six (1.16.0-3ubuntu1) ...  
Removing samba-common (2:4.15.13+dfsg-0ubuntu1.6) ...  
Removing samba-libs:amd64 (2:4.15.13+dfsg-0ubuntu1.6) ...  
Removing libcups2:amd64 (2.4.1op1-1ubuntu4.11) ...  
Removing libavahi-client3:amd64 (0.8-5ubuntu5.2) ...  
Removing libavahi-common3:amd64 (0.8-5ubuntu5.2) ...  
Removing libavahi-common-data:amd64 (0.8-5ubuntu5.2) ...  
Removing libjansson4:amd64 (2.13.1-1.1build3) ...  
Removing python3-ldb (2:2.4.4-0ubuntu0.22.04.2) ...  
Removing python3-talloc:amd64 (2.3.3-2build1) ...  
Removing libpython3.10:amd64 (3.10.12-1-22.04.7) ...  
Removing libwbclient0:amd64 (2:4.15.13+dfsg-0ubuntu1.6) ...  
Removing libldb2:amd64 (2:2.4.4-0ubuntu0.22.04.2) ...  
Removing libldap-2.5-0:amd64 (2.5.18+dfsg-0ubuntu0.22.04.2) ...  
Removing liblmdb0:amd64 (0.9.24-1build2) ...  
Removing libtevent0:amd64 (0.11.0-1build1) ...  
Removing libtalloc2:amd64 (2.3.3-2build1) ...  
Removing libtdb1:amd64 (1.4.5-2build1) ...  
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...  
root@Baker_Street_Linux_Server:/# █
```

Ensuring samba is stopped and removed.



The screenshot shows a terminal window with a dark background and light-colored text. At the top right, it says "root@Baker_Street_Linux_Server: /". The menu bar includes "File Edit View Search Terminal Help". The command entered was "sudo apt autoclean -y". The output shows an error message: "sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution". It then continues with standard package management output: "Reading package lists... Done", "Building dependency tree... Done", and "Reading state information... Done". The command prompt "root@Baker_Street_Linux_Server:/#" is visible at the bottom.

```
root@Baker_Street_Linux_Server:/# sudo apt autoclean -y
sudo: unable to resolve host Baker_Street_Linux_Server: Temporary failure in name resolution
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
root@Baker_Street_Linux_Server:/# █
```

Running autoclean.

```

root@Baker_Street_Linux_Server:/etc/init.d
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/# cd /etc/init.d
root@Baker_Street_Linux_Server:/etc/init.d# ls
cron dbus hwclock.sh mysql nmbd openbsd-inetd postfix procps samba-ad-dc smbd ssh ufw
root@Baker_Street_Linux_Server:/etc/init.d# ls -lar
total 64
-rwxr-xr-x 1 root root 2083 Sep 19 2021 ufw
-rwxr-xr-x 1 root root 4060 Mar 13 2024 ssh
-rwxr-xr-x 1 root root 2061 Jan 5 2024 smbd
-rwxr-xr-x 1 root root 2259 Jan 5 2024 samba-ad-dc
-rwxr-xr-x 1 root root 959 Feb 25 2022 procps
-rwxr-xr-x 1 root root 3089 Mar 30 2023 postfix
-rwxr-xr-x 1 root root 2444 Dec 26 2016 openbsd-inetd
-rwxr-xr-x 1 root root 1934 Jan 5 2024 nmbd
-rwxr-xr-x 1 root root 5607 Jun 14 2023 mysql
-rwxr-xr-x 1 root root 1748 Feb 20 2022 hwclock.sh
-rwxr-xr-x 1 root root 3152 Jun 28 2021 dbus
-rwxr-xr-x 1 root root 3062 Mar 17 2021 cron
drwxr-xr-x 1 root root 4096 Dec 20 01:55 ..
drwxr-xr-x 1 root root 4096 Dec 19 19:04 .
root@Baker_Street_Linux_Server:/etc/init.d# rm mysql
rm: cannot remove 'mysql': No such file or directory
root@Baker_Street_Linux_Server:/etc/init.d# ls
cron dbus hwclock.sh nmbd openbsd-inetd postfix procps samba-ad-dc smbd ssh ufw
root@Baker_Street_Linux_Server:/etc/init.d# rm samba-ad-dc
root@Baker_Street_Linux_Server:/etc/init.d# 

```

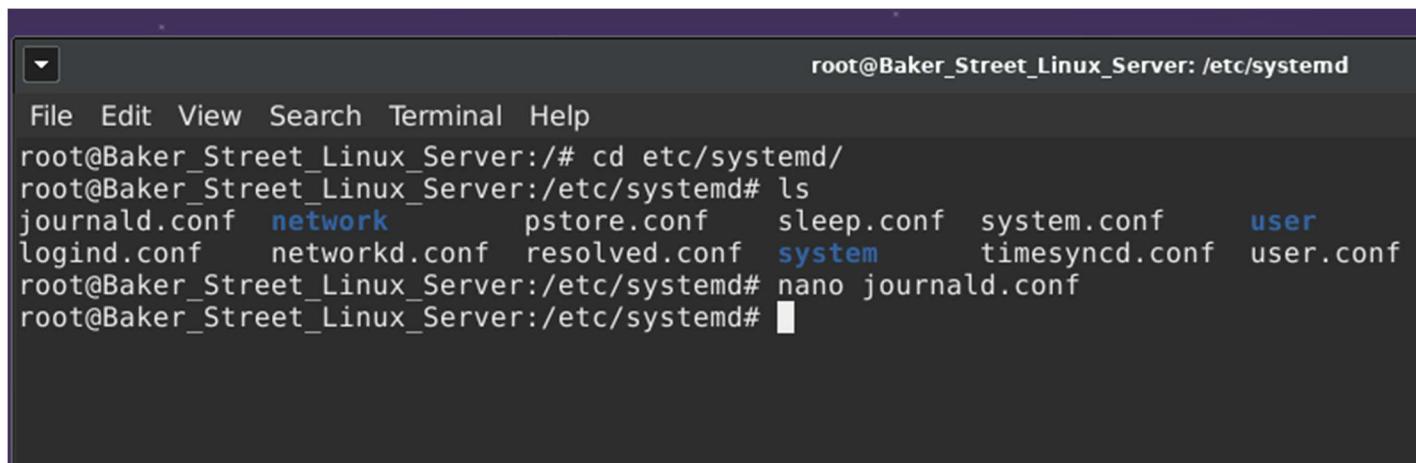
Manually removing mysql and samba.

```

root@Baker_Street_Linux_Server:/etc/init.d
File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/etc/init.d# ls
cron dbus hwclock.sh nmbd openbsd-inetd postfix procps smbd ssh ufw
root@Baker_Street_Linux_Server:/etc/init.d#

```

Confirming mysql and samba removed.

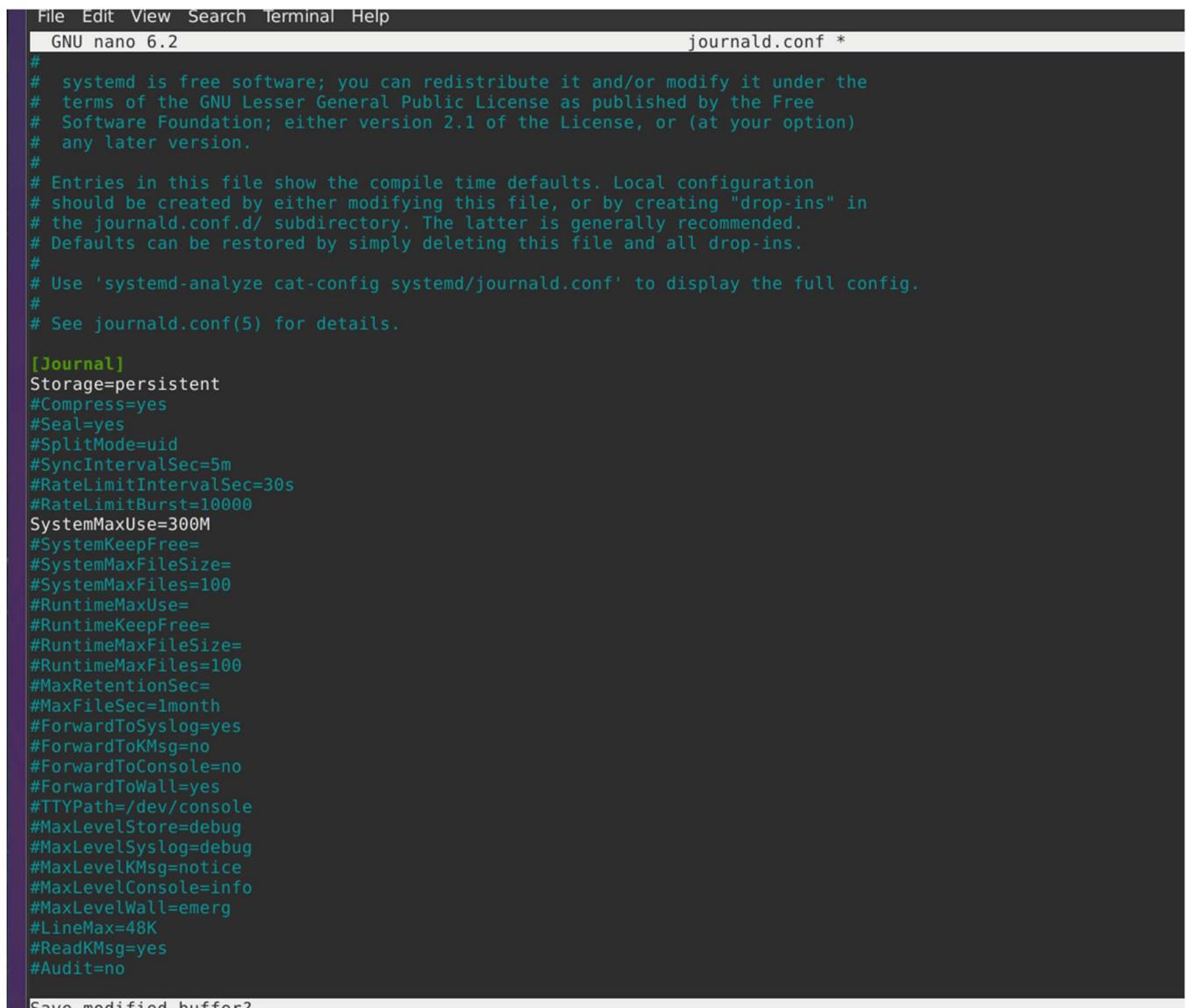


A screenshot of a terminal window titled "root@Baker_Street_Linux_Server: /etc/systemd". The window shows a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal command history is as follows:

```
root@Baker_Street_Linux_Server:/# cd etc/systemd/
root@Baker_Street_Linux_Server:/etc/systemd# ls
journald.conf  network          pstore.conf   sleep.conf   system.conf    user
logind.conf    networkd.conf    resolved.conf  system       timesyncd.conf user.conf
root@Baker_Street_Linux_Server:/etc/systemd# nano journald.conf
root@Baker_Street_Linux_Server:/etc/systemd#
```

Part 4: Enabling and Configuring Logging

Access **journald.conf** file to edit in editor.



The screenshot shows a terminal window with the nano text editor open. The title bar says "File Edit View Search Terminal Help" and "GNU nano 6.2". The file name is "journald.conf *". The content of the file is the configuration for the journald service, specifically the [Journal] section. It includes settings like Storage=persistent, SyncIntervalSec=5m, RateLimitIntervalSec=30s, RateLimitBurst=10000, SystemMaxUse=300M, and various log levels and retention policies. At the bottom of the file, there is a prompt "Save modified buffer?".

```

File Edit View Search Terminal Help
GNU nano 6.2                                     journald.conf *
#
# 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 by creating "drop-ins" in
# the journald.conf.d/ subdirectory. The latter is generally recommended.
# Defaults can be restored by simply deleting this file and all drop-ins.
#
# 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=
#SystemMaxFileSize=
#SystemMaxFiles=100
#RuntimeMaxUse=
#RuntimeKeepFree=
#RuntimeMaxFileSize=
#RuntimeMaxFiles=100
#MaxRetentionSec=
#MaxFileSec=1month
#ForwardToSyslog=yes
#ForwardToKMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelKMsg=notice
#MaxLevelConsole=info
#MaxLevelWall=emerg
#LineMax=48K
#ReadKMsg=yes
#Audit=no

Save modified buffer?

```

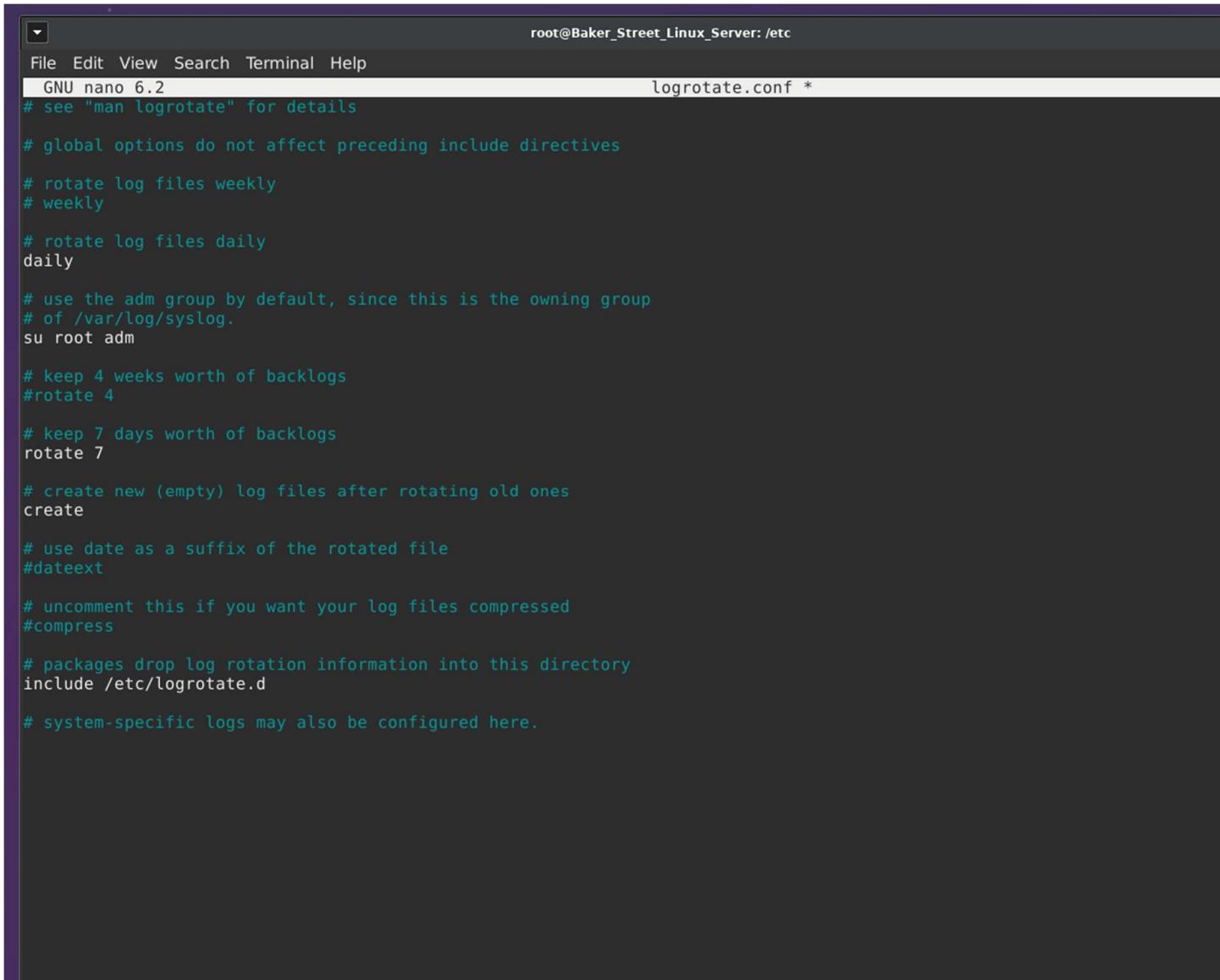
Editing journald.conf file.

```

File Edit View Search Terminal Help
root@Baker_Street_Linux_Server:/etc/systemd# cd ..
root@Baker_Street_Linux_Server:/etc# ls
X11          debian_version  hosts.equiv      login.defs        os-release   rcS.d       subuid-
adduser.conf  default        inetd.conf      logrotate.conf  pam.conf    resolv.conf sudo.co
aliases       deluser.conf   init           logrotate.d     pam.d      resolvconf sudo_lo
alternatives  dhcp          inputrc        lsb-release     passwd     rmt        sudoers
apparmor.d    dpkg          iproute2       lynis          passwd-    rpc        sudoers
apt          e2scrub.conf  inserv.conf.d machine-id     perl      rsyslog.conf sysctl.
bash.bashrc   environment   issue          menu          postfix    rsyslog.d  sysctl.
bindresvport.blacklist ethertypes   issue.net      menu-methods  ppp      security  system
binfmt.d      fstab         kernel         mime.types     profile   selinux   termini
ca-certificates  gai.conf   ld.so.cache   modules-load.d profile.d  services  tmpfile
ca-certificates.conf group       kernel         mke2fs.conf   protocols python3  shadow-
cloud         group-        ld.so.conf    mtab          python3.10 python3.10 shadow-
cron.d        gshadow      ld.so.conf.d  nanorc        rc0.d    shells   ucf.com
cron.daily    gshadow-     ldap           network       rc1.d    ssh      wgetrc
cron.hourly   gss          host.conf     libaudit.conf networkd-dispatcher rc2.d    ssl      xattr.
cron.monthly  cron.daily   hostname      libibverbs.d networks     rc3.d    su-to-rootrc xdg
cron.weekly   cron.monthly hosts         libnl-3        nsswitch.conf rc4.d    subgid-
crontab      cron.weekly  hosts.allow   logcheck      opt        rc5.d    subgid-
dbus-1        debconf.conf hosts.deny    logrotate.conf rc6.d    subuid
root@Baker_Street_Linux_Server:/etc# nano logrotate.conf
root@Baker_Street_Linux_Server:/etc# █

```

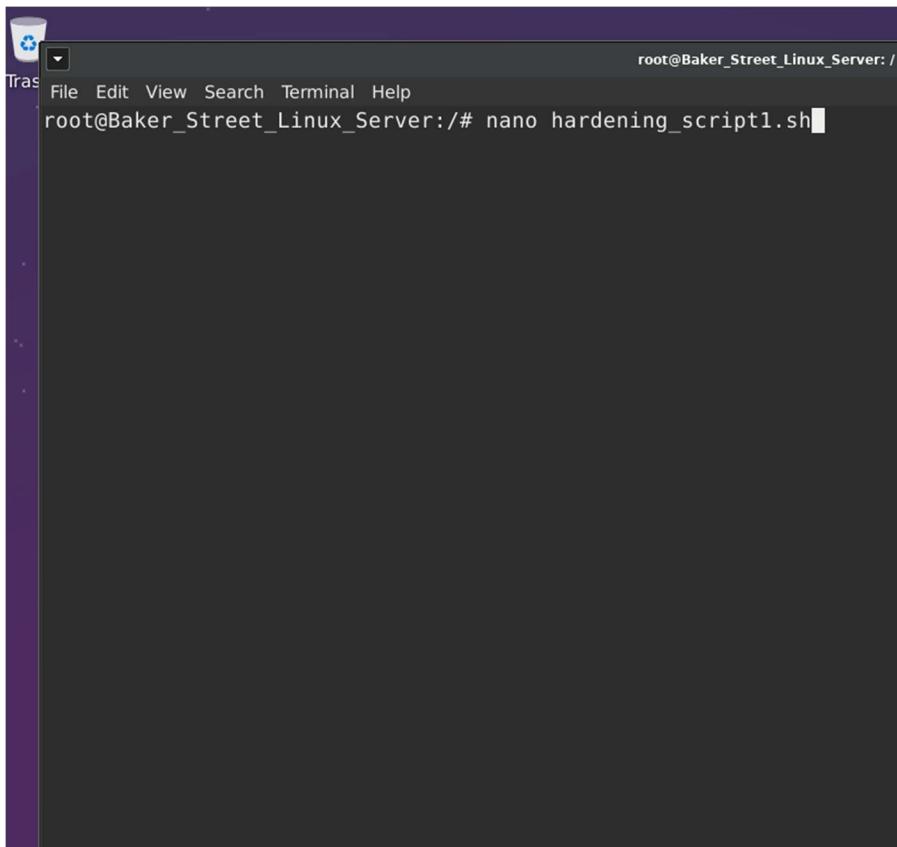
Editing journald.conf file.



The screenshot shows a terminal window titled "root@Baker_Street_Linux_Server: /etc". The window contains the configuration file for log rotation, /etc/logrotate.conf. The file is being edited with the nano text editor. The code in the file is as follows:

```
GNU nano 6.2
# see "man logrotate" for details
# global options do not affect preceding include directives
# rotate log files weekly
# weekly
# rotate log files daily
daily
# use the adm group by default, since this is the owning group
# of /var/log/syslog.
su root adm
# keep 4 weeks worth of backlogs
#rotate 4
# keep 7 days 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.
```

Editing journald.conf file to configure and check logging.



A screenshot of a terminal window titled "root@Baker_Street_Linux_Server: /". The window shows the command "root@Baker_Street_Linux_Server:/# nano hardening_script1.sh" entered at the prompt. The terminal has a dark background with light-colored text. The title bar includes the user name, host name, and current directory. The menu bar contains File, Edit, View, Search, Terminal, and Help.

10.1 Project 1 Day 3 Activity Guide

Project 1 Day 3 Scenario

Creating hardening_script1.sh file

```
File Edit View Search Terminal Help
GNU nano 6.2                                     hardening_script1.sh
#!/bin/bash

# Variable for the report output file, choose an output file name
rm hardening_script1.txt
REPORT_FILE="hardening_script1.txt"

# Output the hostname
echo "Gathering hostname..."
echo "Hostname:$(hostname)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Output the OS version
echo "Gathering OS version..."
echo "OS Version:$(cat /etc/os-release)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE
```

Editing the script 1 file.

```
# Output memory information
echo "Gathering memory information..."
echo "Memory Information:$(free -h)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Output uptime information
echo "Gathering uptime information..."
echo "Uptime Information:$(uptime)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Backup the OS
echo "Backing up the OS..."

sudo tar -cvpzf /baker_street_backup.tar.gz --exclude='/baker_street_backup.tar.gz' --exclude='/proc' --exclud
echo "OS backup completed." >> $REPORT_FILE
printf "\n" >> $REPORT_FILE
```

Editing the script 1 file.

```
echo "Gathering 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..."  
sudo find /home/ -type f -perm -o=rwx -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..."
```

Editing the script 1 file.

```
# Engineering scripts - Only members of the engineering group
echo "Updating permissions for Engineering scripts."
sudo find / -type f -iname '*engineering*' -exec chown :engineering {} +
sudo find / -type f -iname '*engineering*' -exec chmod 770 {} +
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..."
sudo find / -type f -iname '*research*' -exec chown :research {} +
sudo find / -type f -iname '*research*' -exec chmod 770 {} +
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"
sudo find / -type f -iname '*finance*' -exec chown :finance {} +
sudo find / -type f -iname '*finance*' -exec chmod 770 {} +
echo "Permissions updated for Finance scripts." >> $REPORT_FILE
```

Editing the script 1 file.

```
echo "Permissions updated for Finance scripts." >> $REPORT_FILE
printf "\n" >> $REPORT_FILE
echo "Script execution completed. Check $REPORT_FILE for details."
```

Editing the script 1 file.

Creating hardening_script2.sh file

```
#!/bin/bash

# Variable for the report output file, choose a NEW output file name
REPORT_FILE="hardening_script2.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:$(cat /etc/ssh/sshd_config)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Update packages and services
echo "Updating packages and services"
sudo apt update
sudo apt upgrade -y

echo "Packages have been updated and upgraded" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE
```

Editing the script 2 file.

```
echo "Packages have been updated and upgraded" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

echo "Installed Packages:$(dpkg -l)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

echo "Printing out logging configuration data"
echo "journald.conf file data:$(cat /etc/systemd/journald.conf)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE
echo "logrotate.conf file data:$(cat /etc/logrotate.conf)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

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

Editing the script 2 file.

APPENDIX E: PRELIMINARY DOCUMENTATION (rough notes)

Cybersecurity	
Project 1 Hardening Summary and Checklist	
<u>OS Information</u>	
Customer	Baker Street Corporation
Hostname	Baker-Street-Linux-Server
OS Version	Ubuntu 22.04.5 LTS (jammy)
Memory information	free -h Total 15GB, Used 1.4GB
Uptime information	uptime 1:12
<u>Checklist</u>	
Completed	Activity
<input checked="" type="checkbox"/>	OS backup
<input checked="" type="checkbox"/>	Auditing users and groups

JOHN MALLON

John Mallon		
<p>delete marketing groupdbf Sudo groupdb -> a sherlock research (report)</p>	<p>research group does not exist. create research group Sudo groupdb / research Add all employees + leave employee</p>	<p>Sudo password - u sherlock Watson mycroft Sudo password - m today today adler cat /etc/group getent group/marketing NO members</p>
<input checked="" type="checkbox"/>	Updating and enforcing password policies	<p>Sudo nano /etc/pam.d/common-password password requisite pam_cracklib.so retry=2 minlen=8 urepeat=-1 lcredit=-1</p>
<input checked="" type="checkbox"/>	Updating and enforcing sudo permissions	<p>sherlock ALL=(ALL:ALL) ALL remove root Watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh mycroft % research ALL=(ALL) NOPASSWD: /tmp/scripts/research-script.sh</p>
<input checked="" type="checkbox"/>	Validating and updating permissions on files and directories	<p>chmod o-rwx * in home directory find /home -type f -iname "*engineering*" "research*" "#finance*" "#files & hidden paradoxes" find chmod o-rwx *engineering* "#finance*" "#files & hidden paradoxes" find nano /etc/ssh/sshd_config change perintempty password No Way change root login to Nc from yes comment port 22 out. add port 22.</p>
<input checked="" type="checkbox"/>	Optional: Updating password hashing configuration enable protocol 2.1 doesn't say disable 1 rootless	
<input checked="" type="checkbox"/>	Auditing and securing SSH	

PROJECT 1 – HARDENING A LINUX SERVER

John Mallon

Cybersecurity

hardening_script1.sh

```
#!/bin/bash

# Variable for the report output file, choose an output file name
REPORT_FILE="PLACE_OUTPUT_FILE_NAME_HERE" - marking-script1.txt

# Output the hostname
echo "Gathering hostname..."
# Placeholder for command to get the hostname
echo "Hostname: $(PLACE_HOSTNAME_COMMAND_HERE)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE $(hostname)

# Output the OS version
echo "Gathering OS version..."
# Placeholder for command to get the OS version
echo "OS Version: $(PLACE_OS_COMMAND_HERE)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE $(lsb_release -a)
cat /etc/os-release

# Output memory information
echo "Gathering memory information..."
# Placeholder for command to get memory info
echo "Memory Information: $(PLACE_MEMORY_COMMAND_HERE)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE $(free -h)

# Output uptime information
echo "Gathering uptime information..."
# Placeholder for command to get uptime info
echo "Uptime Information: $(PLACE_UPTIME_COMMAND_HERE)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE +(uptime)

# Backup the OS
echo "Backing up the OS..."
# Placeholder for command to back up the OS

```

Gathering info

JOHN MALLON

```

sudo tar -cvzf /baker_street/backup.tar.gz --exclude=/baker_street/
        backup.tar.gz --exclude=/baker --exclude=/tmp --exclude=/proc --exclude=/tmp
Place Backup Script Here --exclude=/mnt --exclude=/sys --exclude=/dev
echo "OS backup completed." >> $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: $(Place sudoers display command here)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE $(sudo cat /etc/sudoers)
* check *

# Script to check for files with world permissions and update them
echo "Checking for files with world permissions..."
find /home/* -type f -perm -o=rwx ! while read file; do
    chmod o-rwx "$file"
# 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
echo "Place command here to only allow members of 'engineering' group to view, edit, and execute all engineering scripts"
# Placeholder for command here to only allow members of 'engineering' group to view, edit, and execute all engineering scripts
# Here is the example command for the engineering group: chown :engineering /home/engineer/.mp3
find -name "engineering" -exec chown :engineering {} +
# Permissions updated for Engineering scripts.
echo "Permissions updated for Engineering scripts." >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

```

JOHN MALLON

JOHN MALLON

```

# Research scripts - Only members of the research group
echo "Updating permissions for Research scripts..."
# Placeholder for command to update permissions
Place command here to only allow members of "research" group to view, edit, and
execute all research scripts. See above script for syntax. -->
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
Place command here to only allow members of "finance" group to view, edit, and execute
all finance scripts. See above script for syntax.
echo "Permissions updated for Finance scripts." >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

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

```

J.M.

PROJECT 1 – HARDENING A LINUX SERVER

JOHN MALLON

Cybersecurity

hardening_script2.sh

```
#!/bin/bash

# Variable for the report output file, choose a NEW output file name
REPORT_FILE="PLACE_NEW_OUTPUT_FILE_NAME_HERE" → hardening_script2.sh

# 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:$(Place sshd file display Command Here)" >> $REPORT_FILE
printf "%n" >> $REPORT_FILE → cat /etc/ssh/sshd_config

# Update packages and services
Echo "Updating packages and services"

# Placeholder for command to update packages
Place Update Packages Command Here

# Placeholder for command to upgrade packages
Place Upgrade Packages Command Here apt update
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:$(Place command to list installed packages here)" >>
$REPORT_FILE cat opt list ~installed
printf "%n" >> $REPORT_FILE

/etc/hosts
```

JOHN MALLON

```
echo "Printing out logging configuration data"

# Placeholder for command to display logging data
echo "journald.conf file data: $(Place command to output journald.conf)" >> $REPORT_FILE
print "\n" >> $REPORT_FILE
entry entry entry cut /etc/systemd/journald.conf

# Placeholder for command to display logrotate data
echo "logrotate.conf file data: $(Place command to output logrotate.conf)" >>
$REPORT_FILE
print "\n" >> $REPORT_FILE
cat logrotate.conf

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

make scripts executable chmod +x /usr/local/bin/script.sh
run as root

Complete the following:

- Using cron, schedule script 1 to run Once a month on the first of the month
- Using cron, schedule script 2 to run Once a week every Monday

Be sure to note on your checklist what you have completed
script 1. 0 0 1 * * /usr/local/bin/script.sh
minute hour dayofmonth month day of week.
script 2. 6 0 * +1 /usr/local/bin/script.sh
cron tab -e → Add.

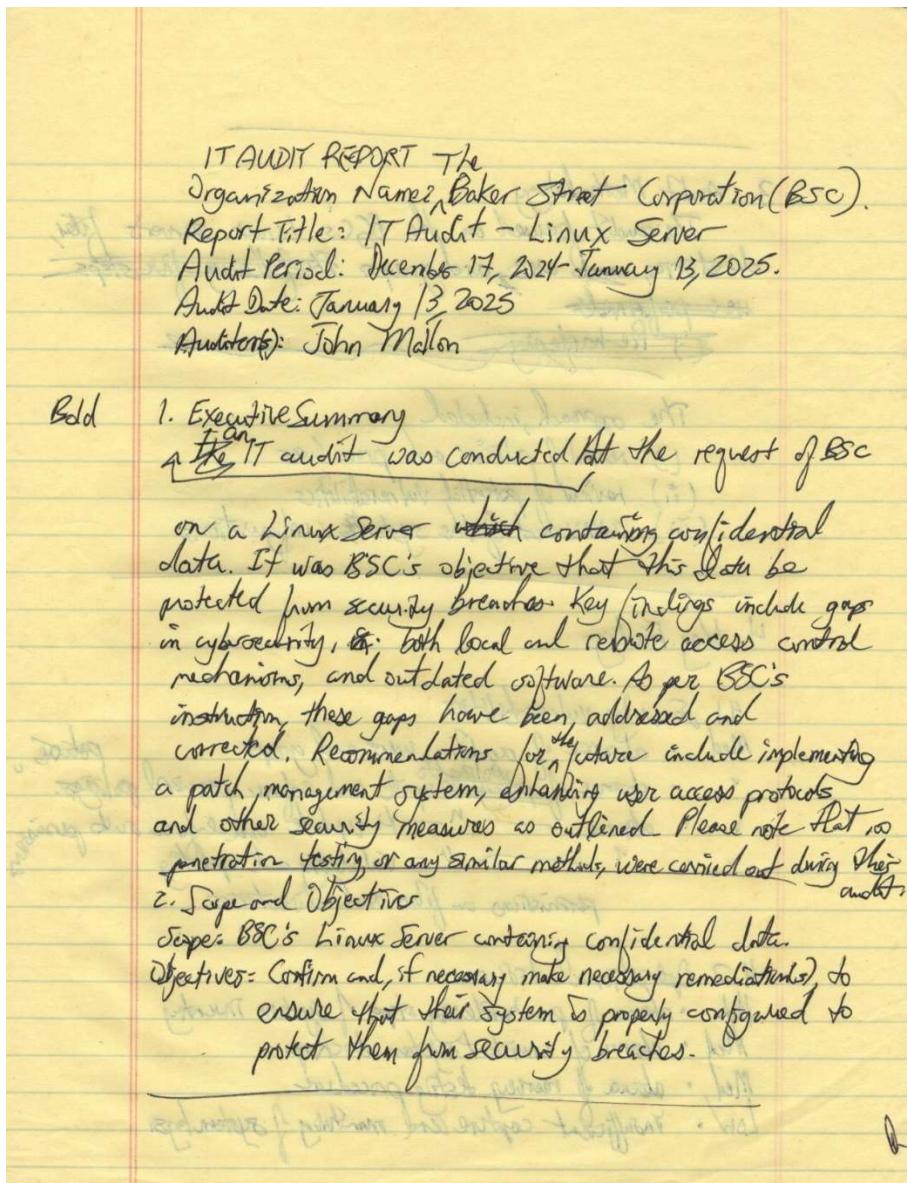
Part 3: Completing your summary report

For the final activity of your project, you are tasked with completing your summary report.

Complete the following:

- From your summary report, check off all completed tasks
- Summarize your findings of your security concerns at the conclusion of the report.
- Submit your project report in bootcampspot.

© 2024 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.

F: Preliminary Audit Report (rough notes)

Ques ANSWER TO QUES

3. Audit Methodology

The audit focused on the BGC's Linux server's files, directories, ~~and users~~, and groups. The following pre-steps were performed:

(i) Pre-hardening

The approach included:

- review of policies and procedures
- review of potential vulnerabilities
- assessment of the system configurations.

4. Key Findings

4.1 Security Vulnerabilities

Med:

- absence of auditing user and groups.
- absence of ~~policy~~ update and enforce ~~current~~ policies.
- absence " " to update and enforce ~~current~~ permissions.
- " " validating and updating permissions on files and directories.

High:

- absence of pre-hardening steps of system inventory

Med:

- absence of consistent system backups

Med:

- absence of recovery testing procedure

Low:

- insufficient capture and monitoring of system logs

