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 Key findings include gaps in cyber security, both local and remote access control mechanisms, and outdated software.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).

- 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:
    - SSH with empty password
    - SSH with root user
    - 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

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	**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' /**
√	Auditing users and groups	**Remove Terminated Users and Home/files** 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 **Lock Account Users on Leave** sudo usermod -L moriarty sudo usermod -L mrs_hudson **Lock Password Users on Leave (extra measure)** sudo passwd -l moriarty sudo passwd -l mrs_hudson **Unlock all Users Employed** sudo passwd -U sherlock

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

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

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

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

√	Reviewing and updating system packages	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.**
√	Disabling unnecessary services	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

√	Enabling and configuring logging	cd /etc/systemd/ Nano journald.conf Remove # and storage=persistent Remove # and systemMaxUse=300 cd .. nano logrotate.conf #weekly daily #rotate 4 rotate 7
√	Scripts created	hardening_script1.sh hardening _script2.sh
√	Scripts scheduled with cron	**Make scripts executable:** chmod +770 /usr/local/sbin/hardening_script1.sh chmod +770 /usr/local/sbin/hardening_script2.sh **cron -e (edit cron)** **Add following two lines** 0 0 1 * * /usr/local/sbin/hardening_script1.sh 0 0 * * 1 /usr/local/sbin/hardening_script2.sh

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..."
```

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..."

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

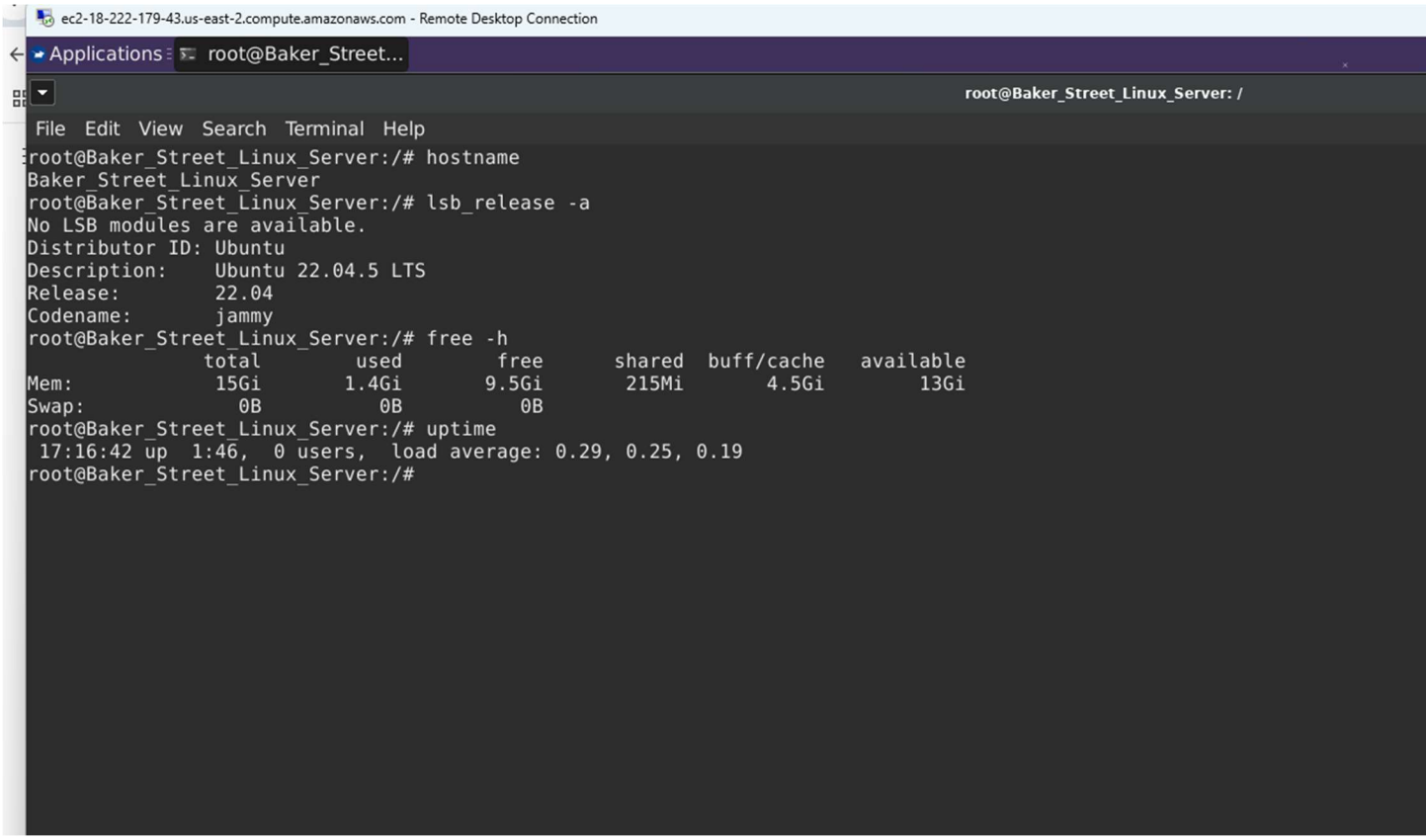
printf "\n" >> $REPORT_FILE

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

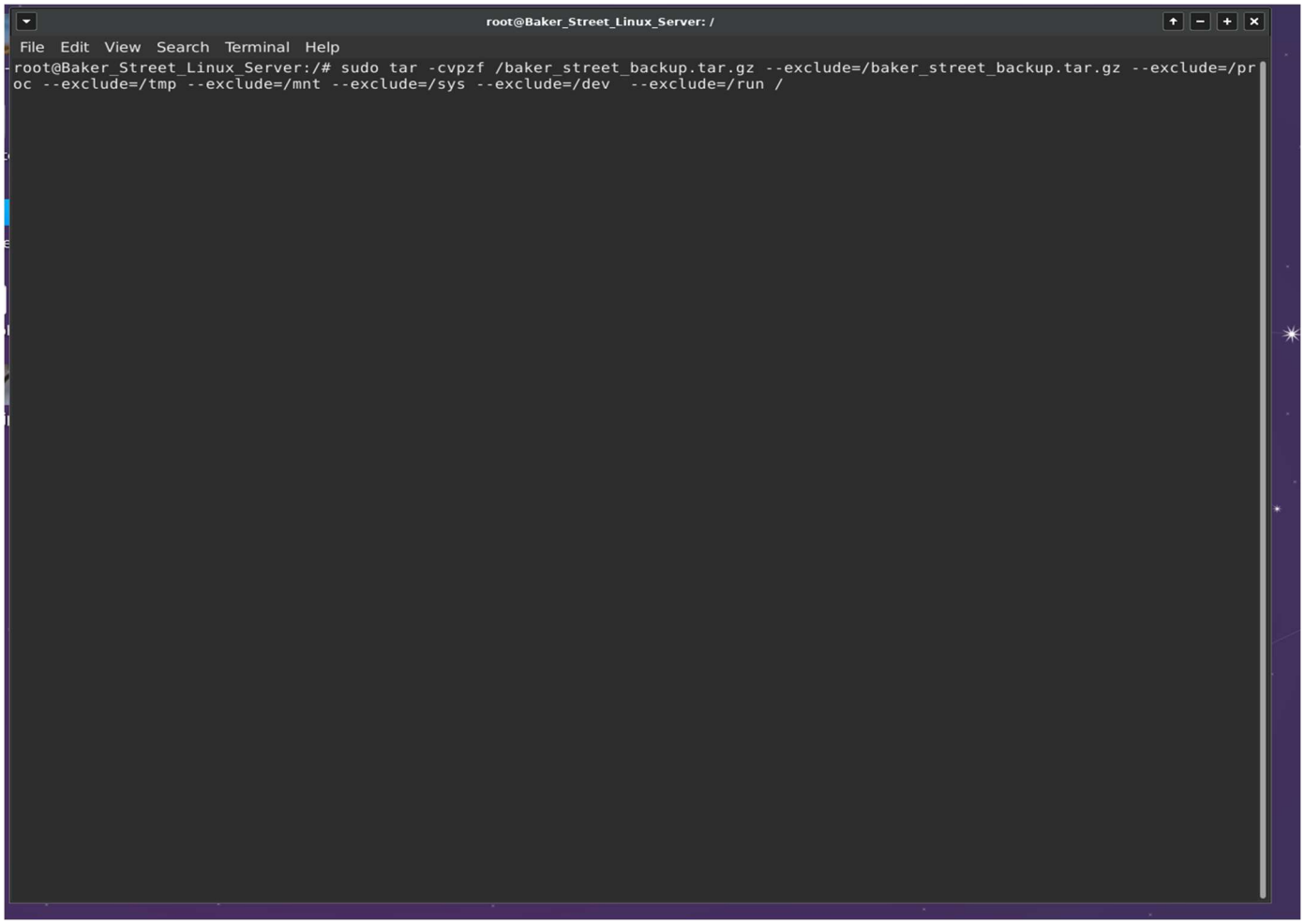
APPENDIX C: HARDENING SCRIPT 2

```
#!/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 nan/etc/ssh/ssh_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."
```

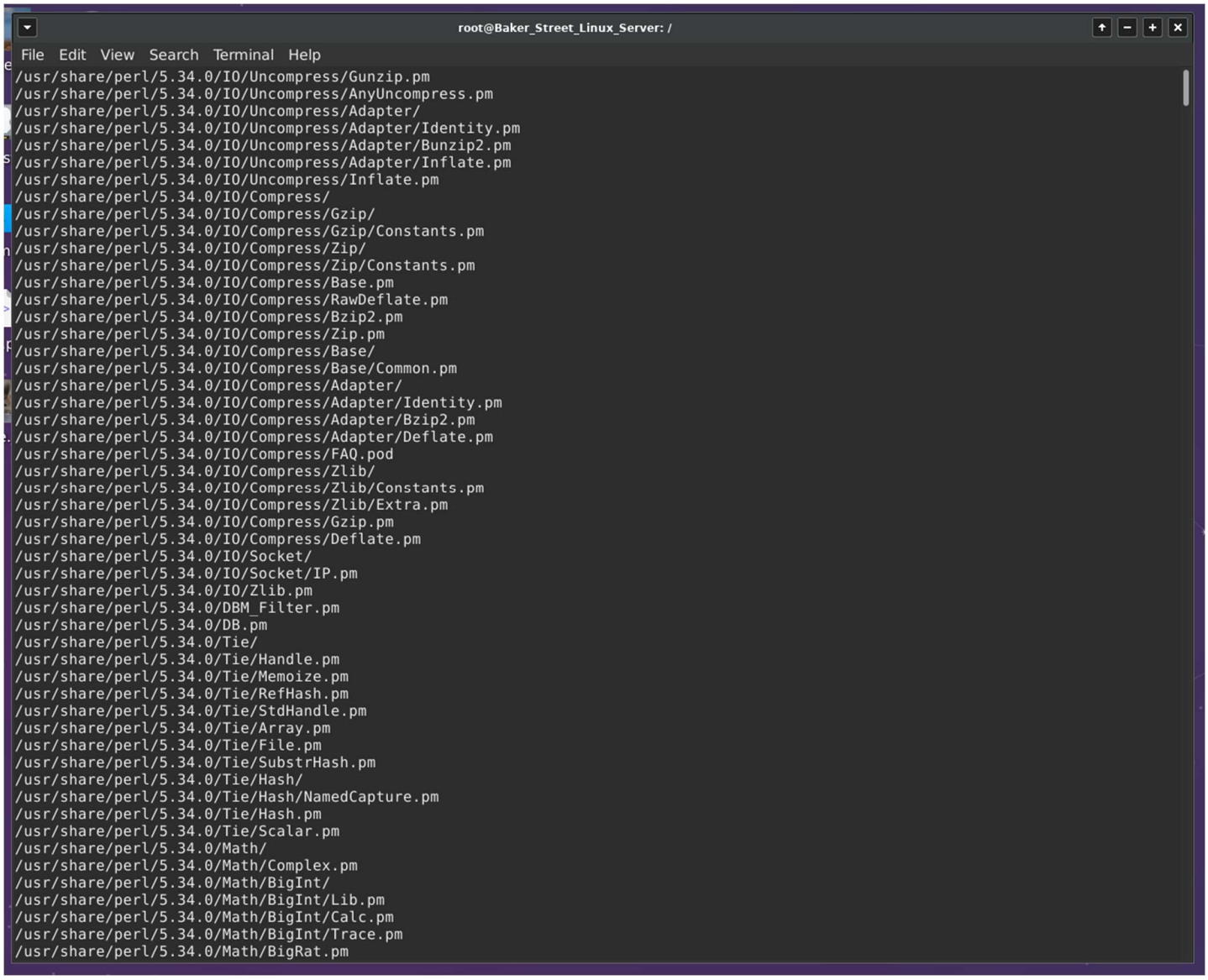
APPENDIX D: SCREENSHOTS



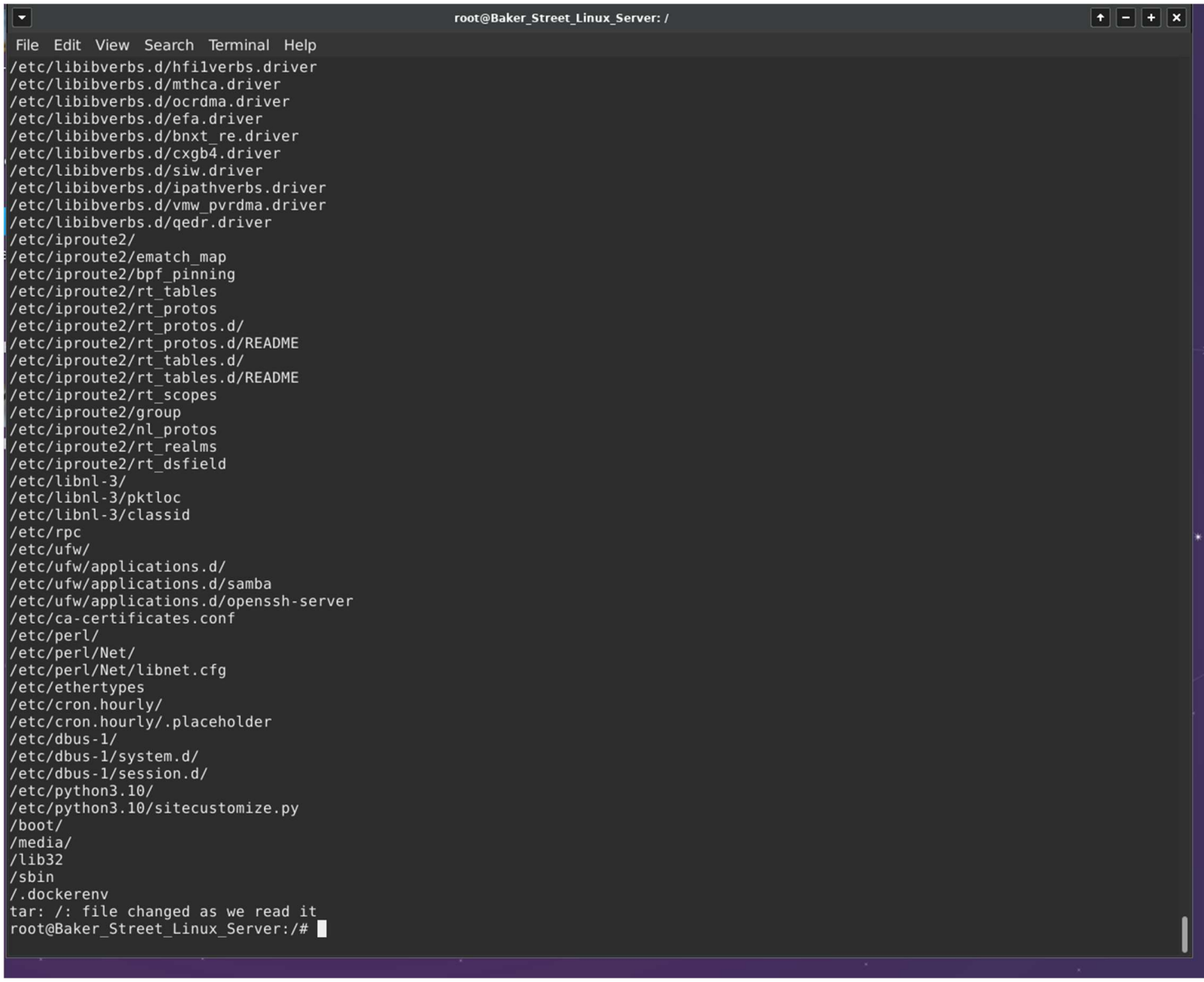
PART 1: This step obtained the Hostname, OS Version, memory information, and the uptime.



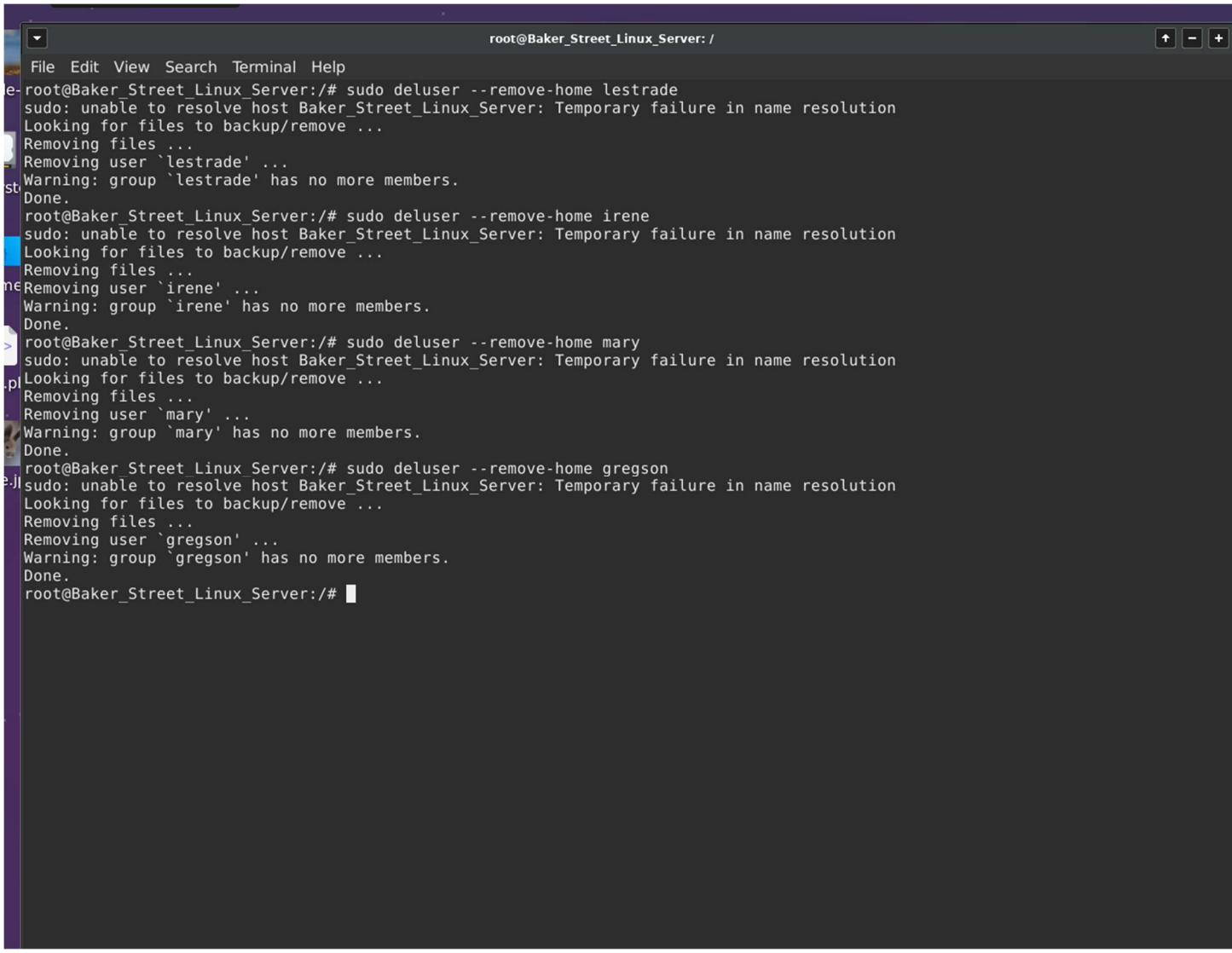
This command completed the OS backup.



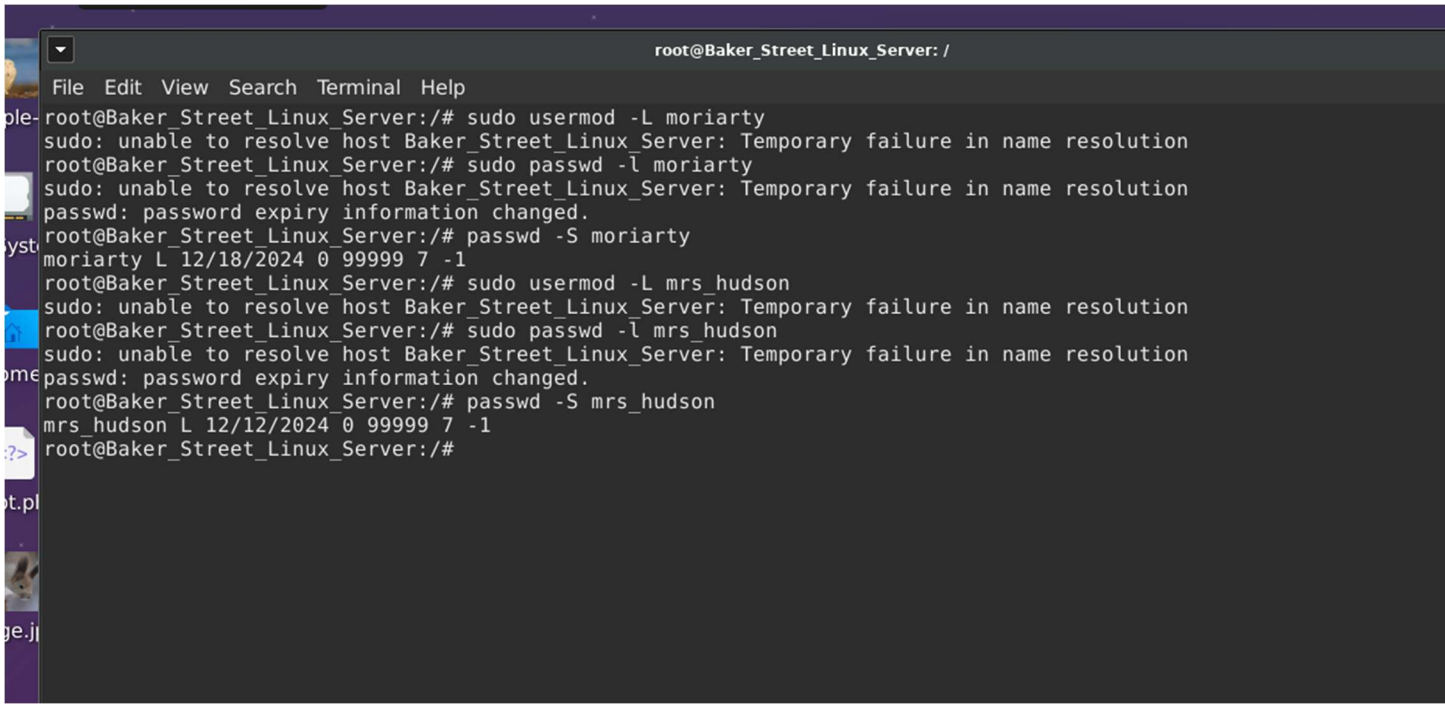
Showing the OS backup progress.



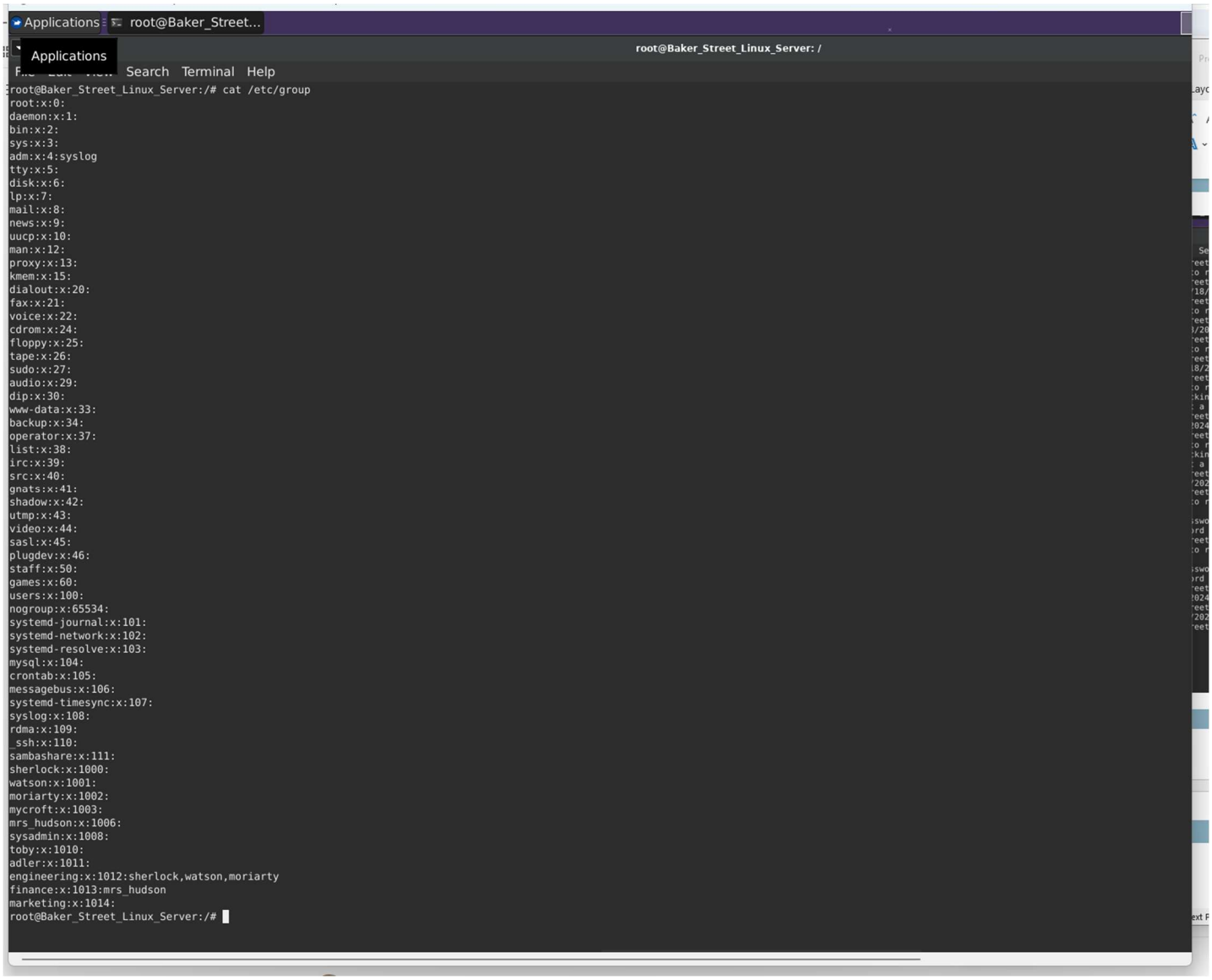
Shows completion of backup progress.



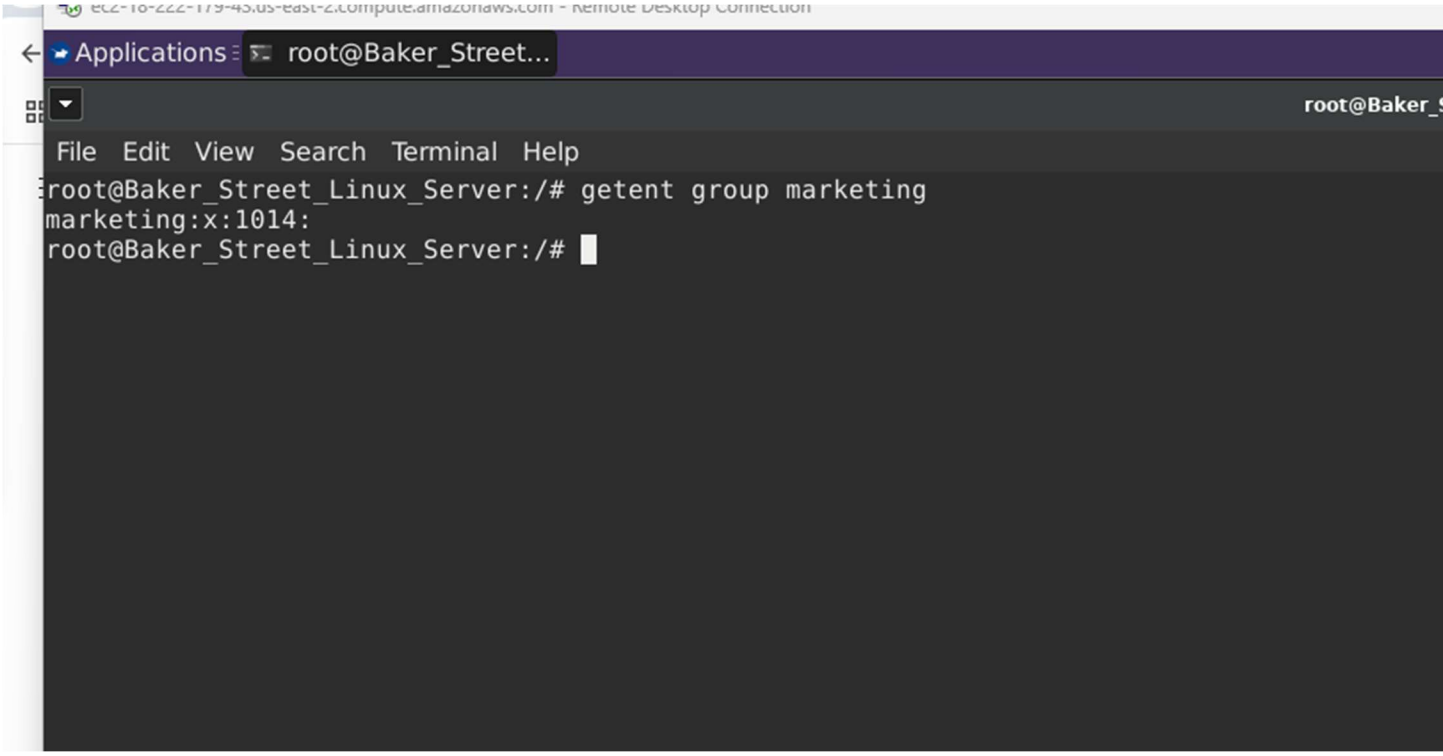
Part 2: Auditing Users and Groups. This step is deleting the all staff that has been terminated, including any files, home directories and groups.



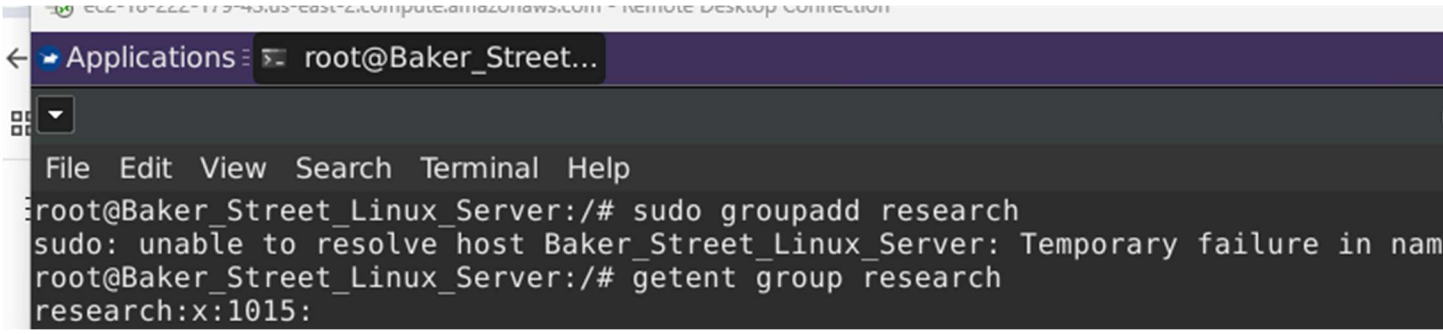
This step locks all user accounts of staff on temporary leave and unlocks any users who are employed.



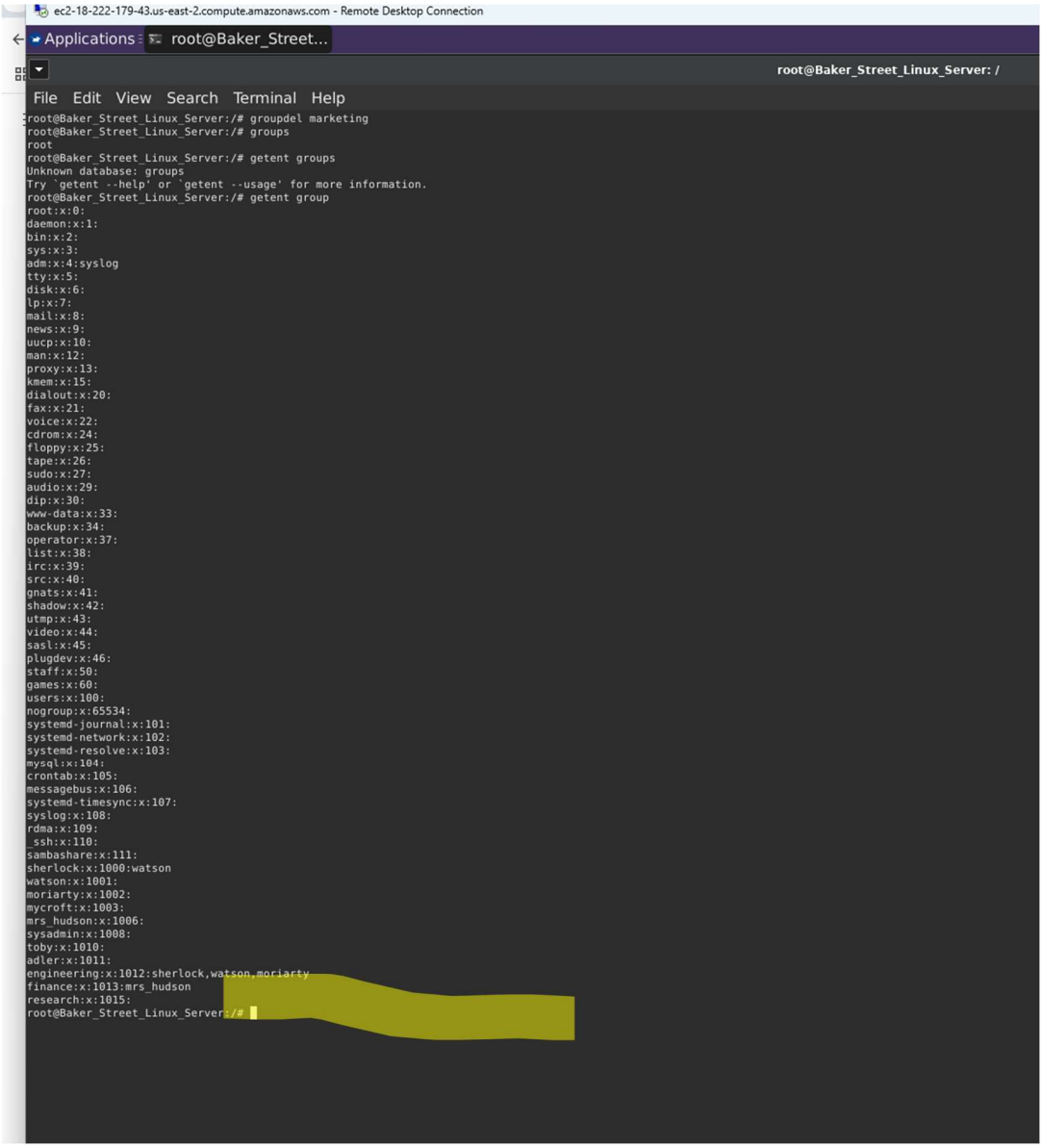
This step lists all the groups and membership of any users in these groups.



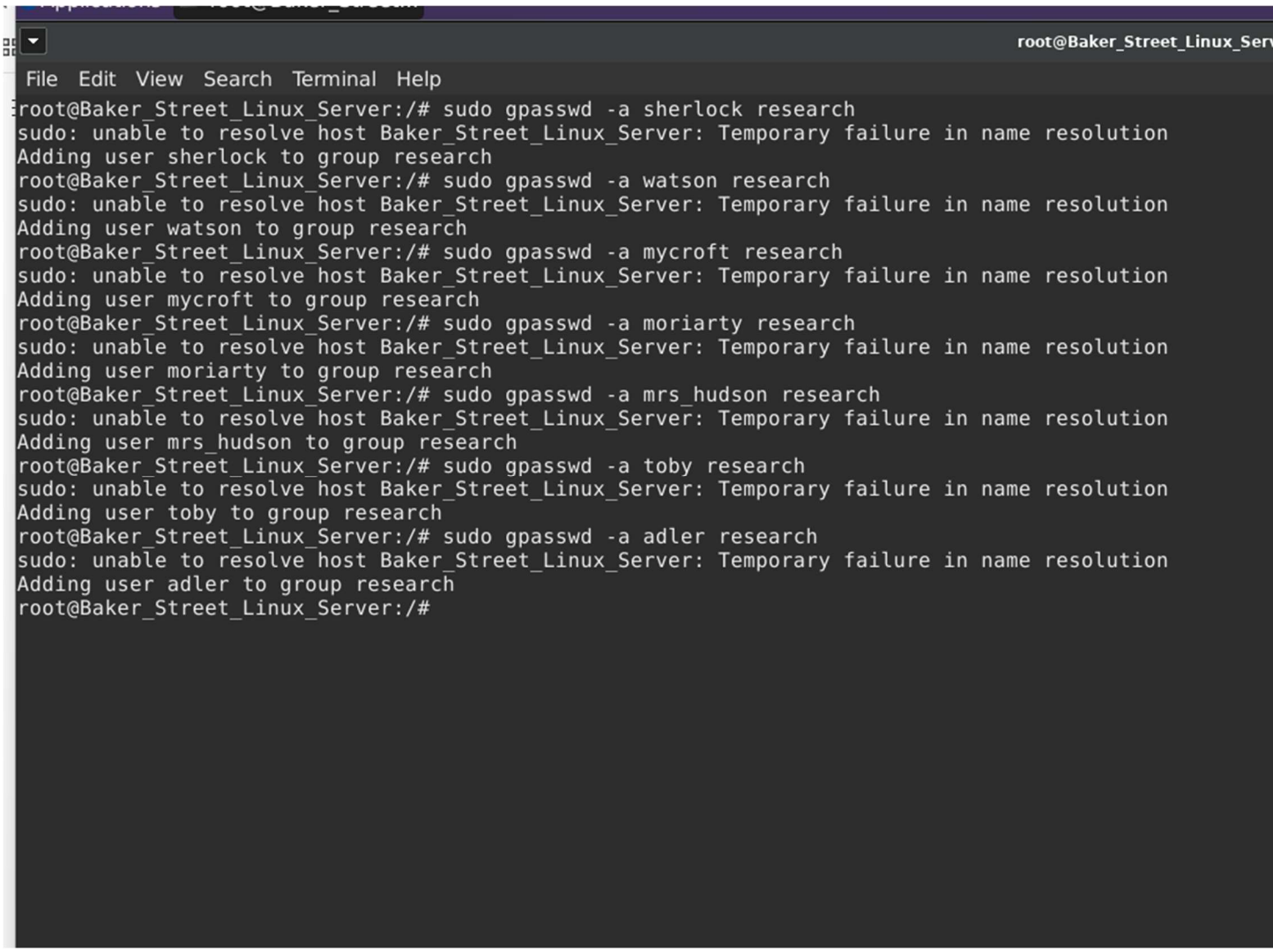
Getting information on the group marketing.



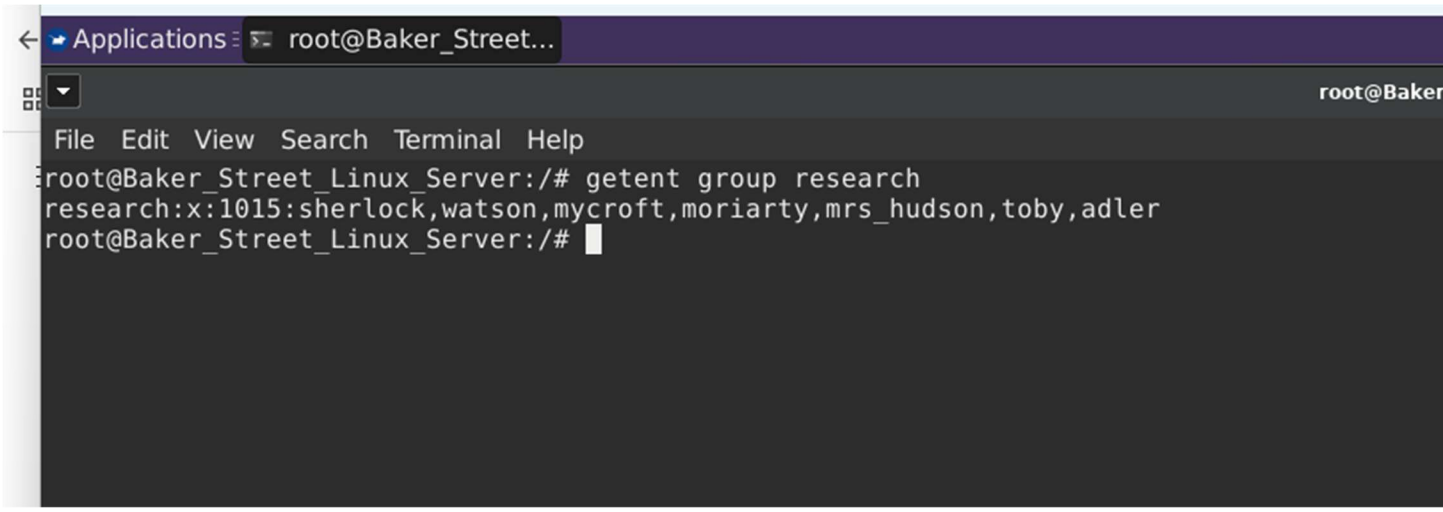
Creating new group research.



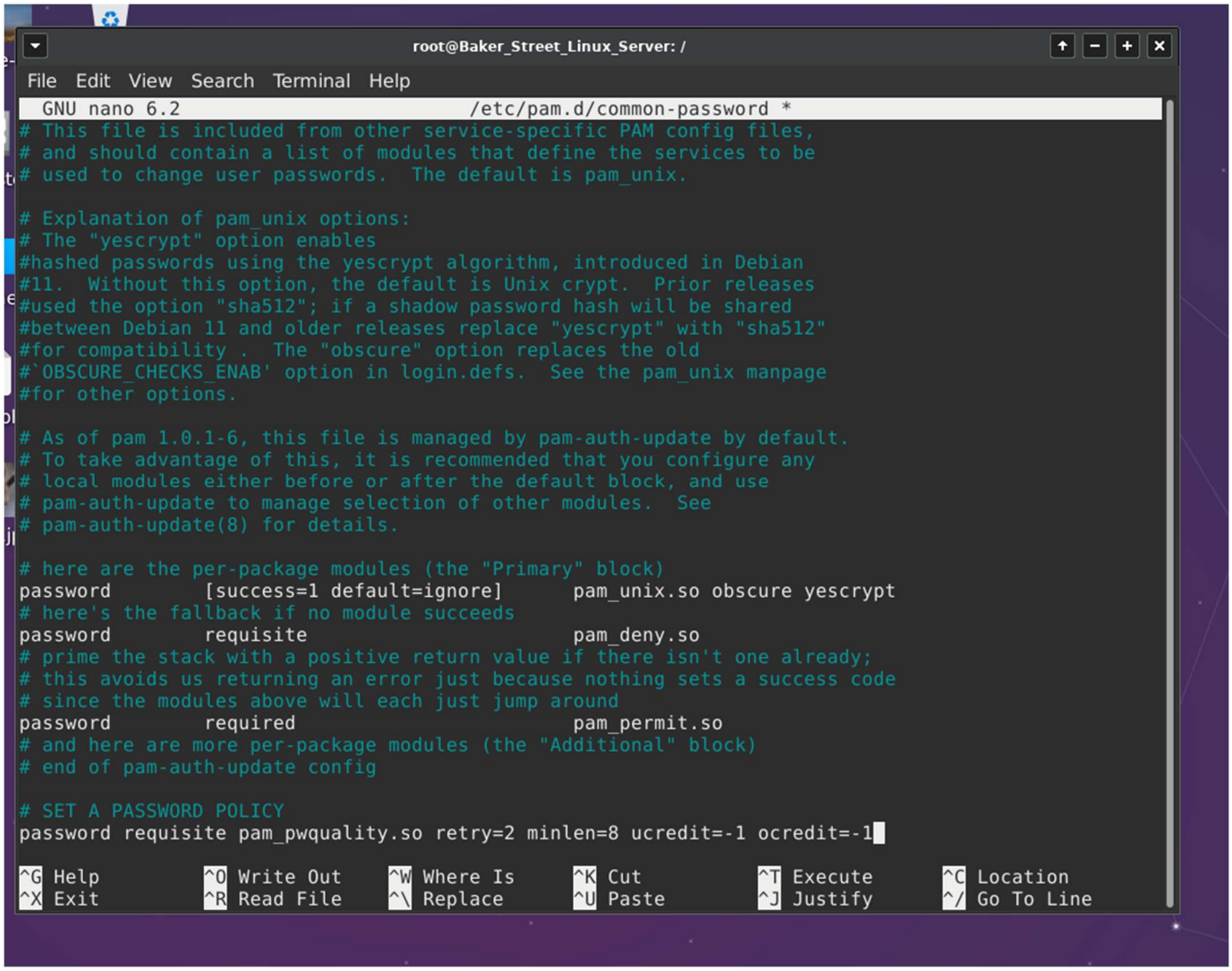
Listing all the groups on the system, deleting marketing, and showing new group research has been created.



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

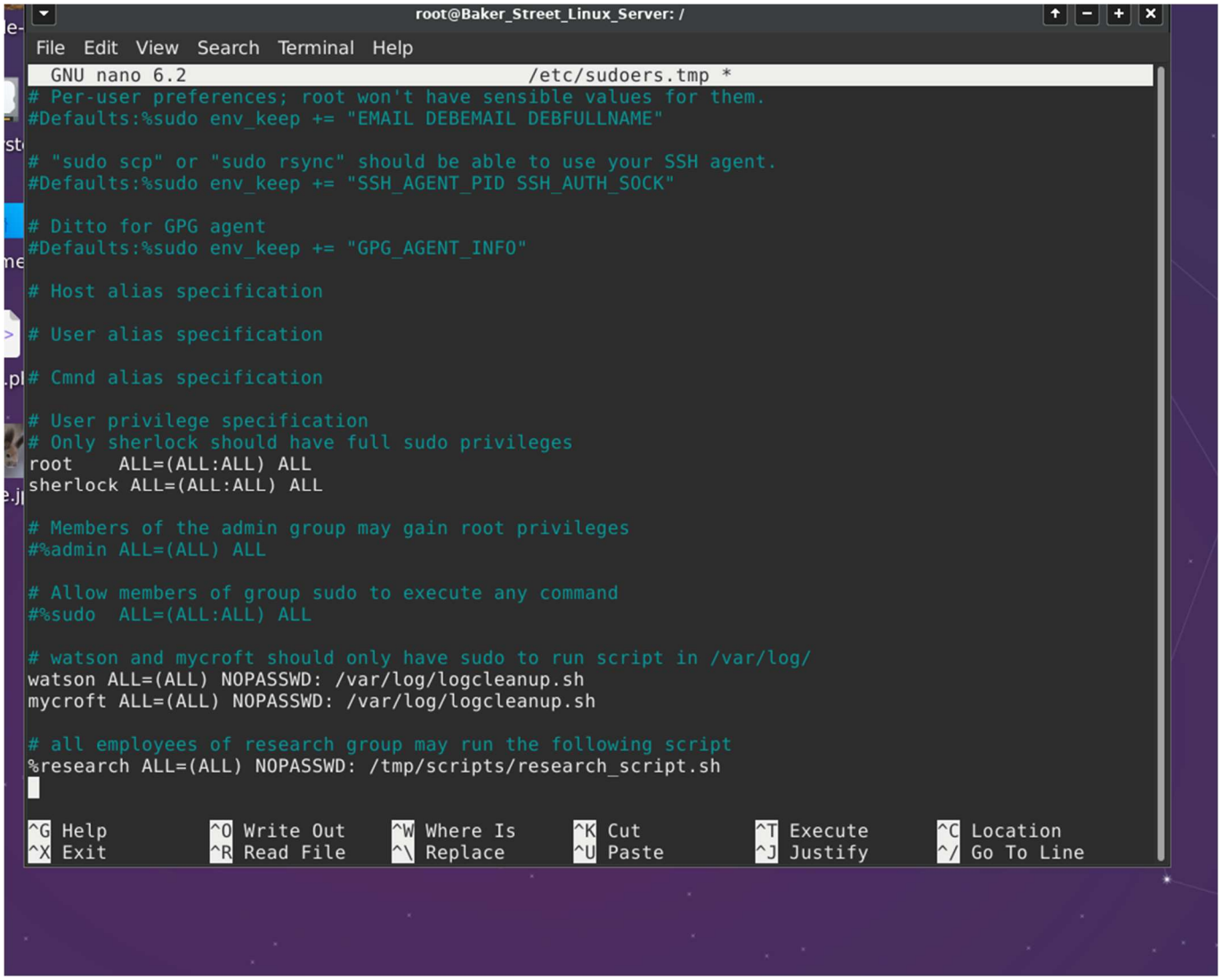


Listing members of research group confirming that all the current employees are members.



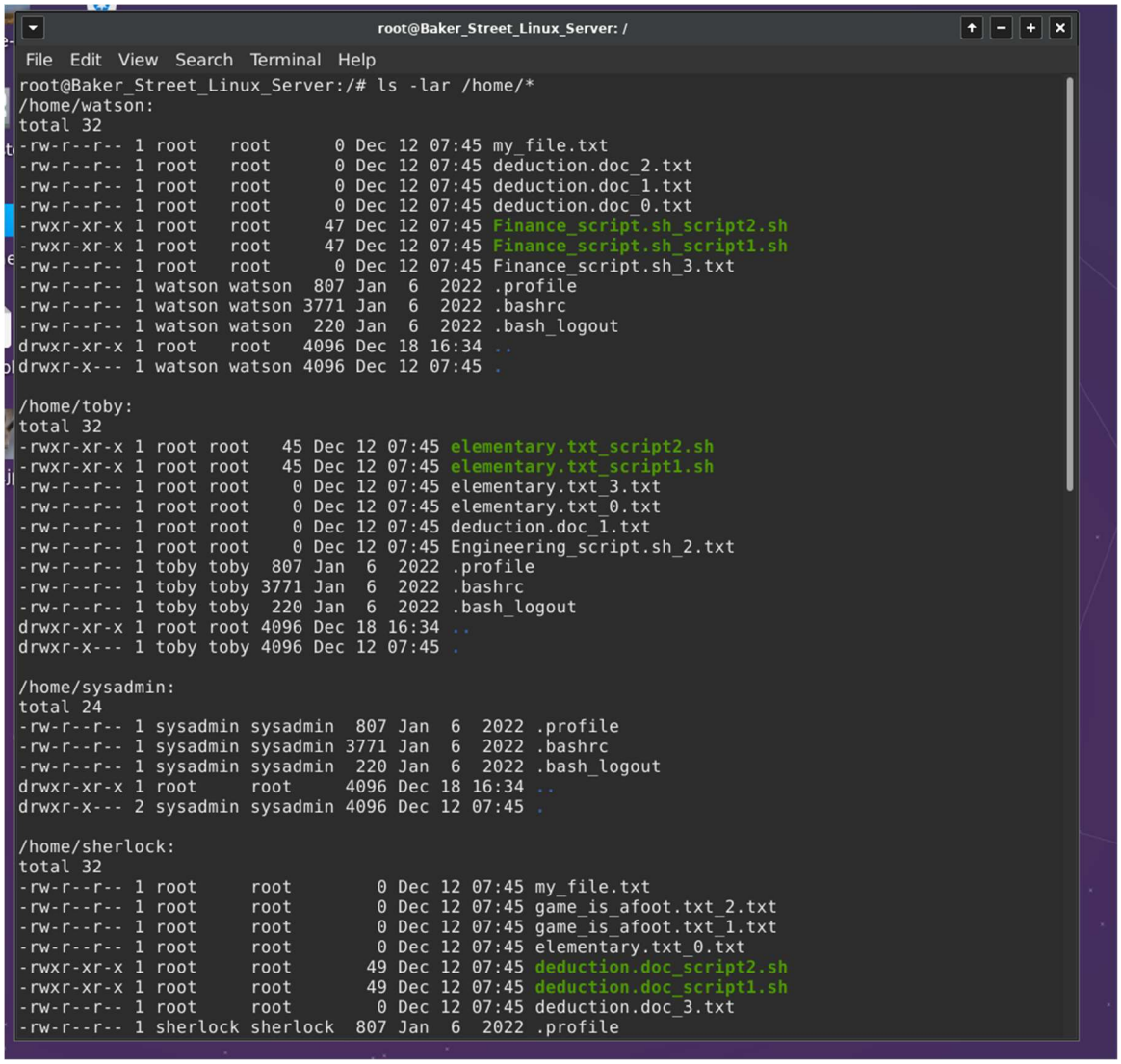
Part 3: Updating and Enforcing Password Policies

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



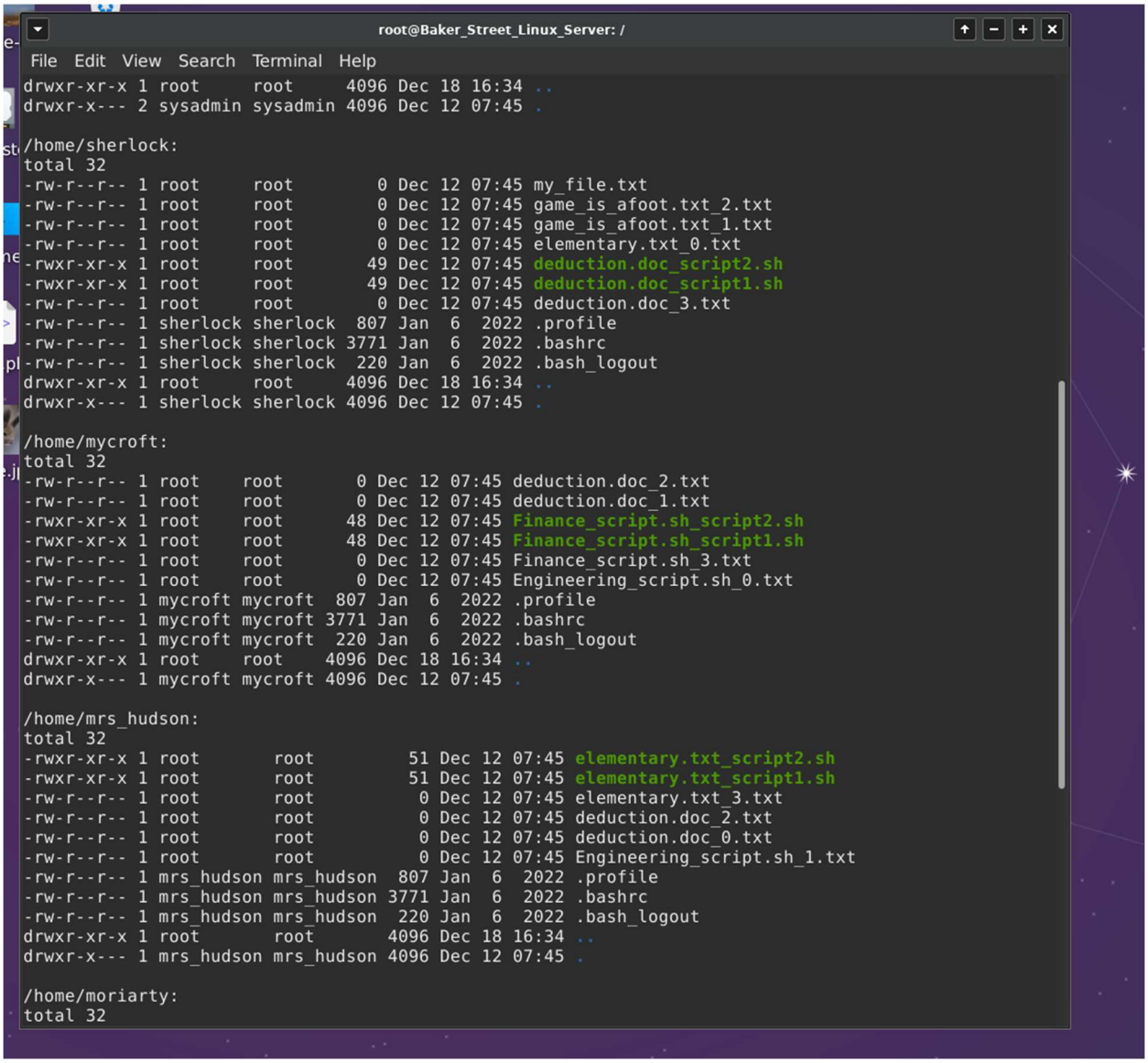
Part 4: Updating and Enforcing sudo Permissions

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

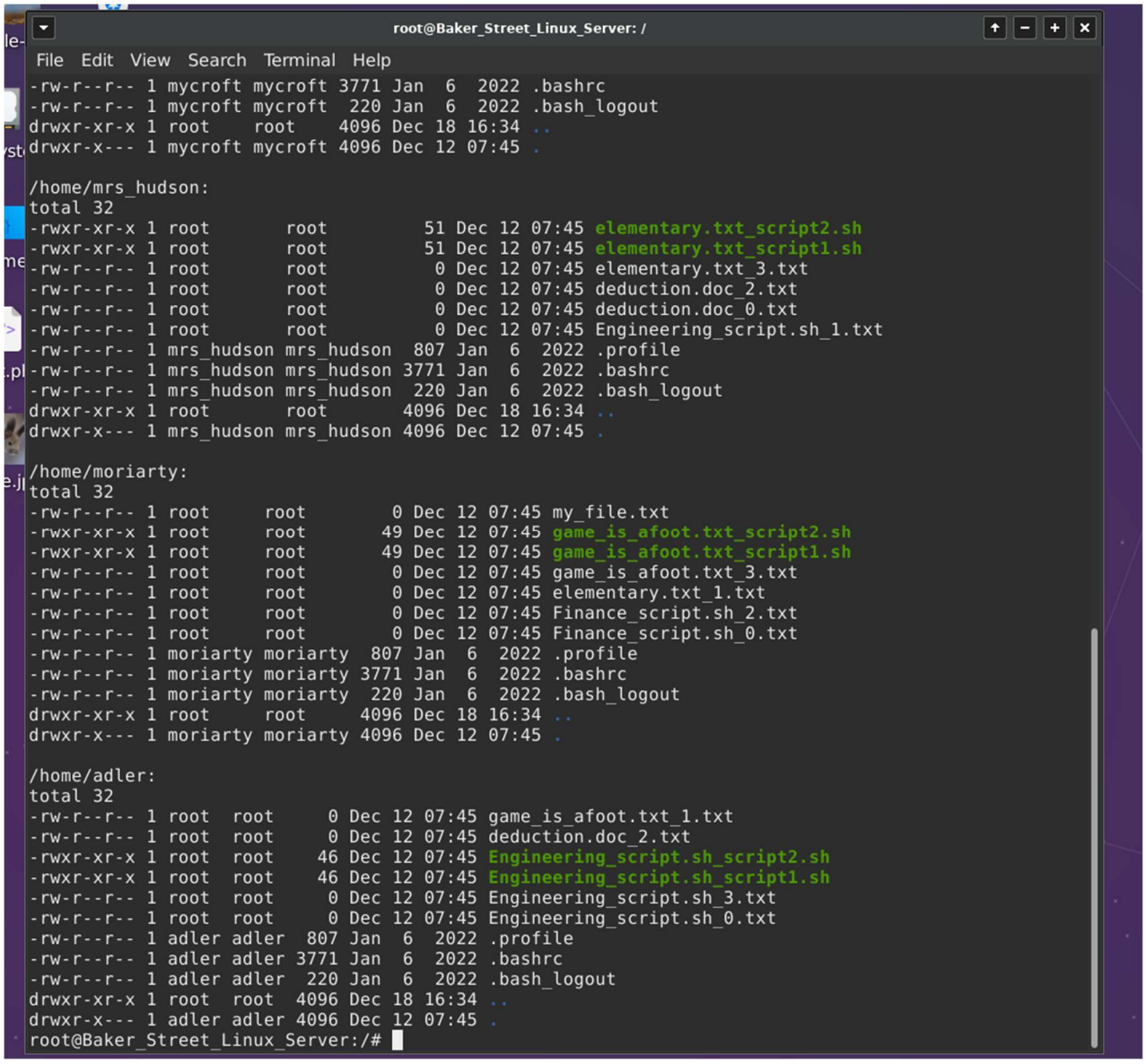


Part 5: Validating and Updating Permissions on Files and Directories

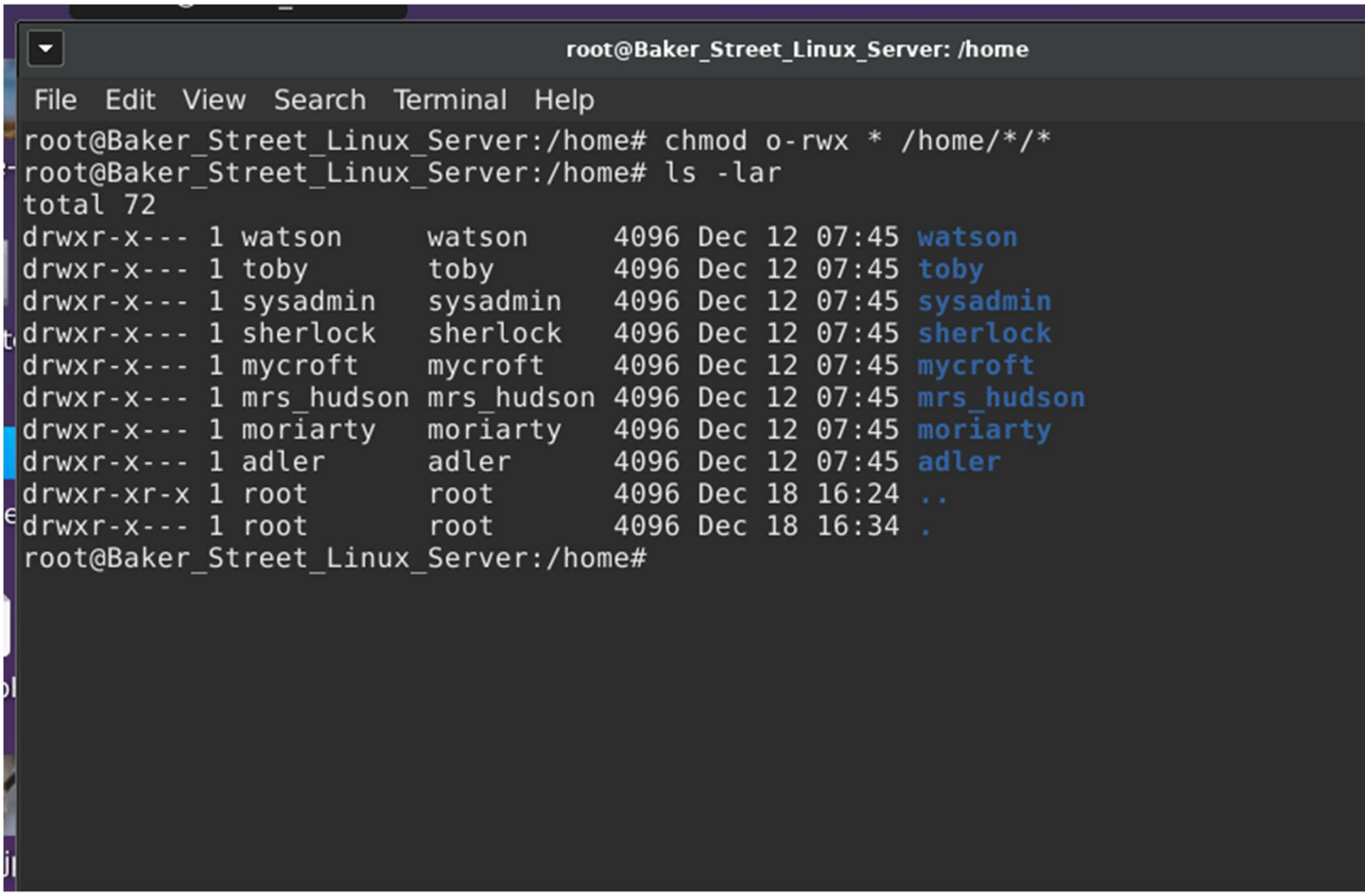
Listing users files and the permissions.



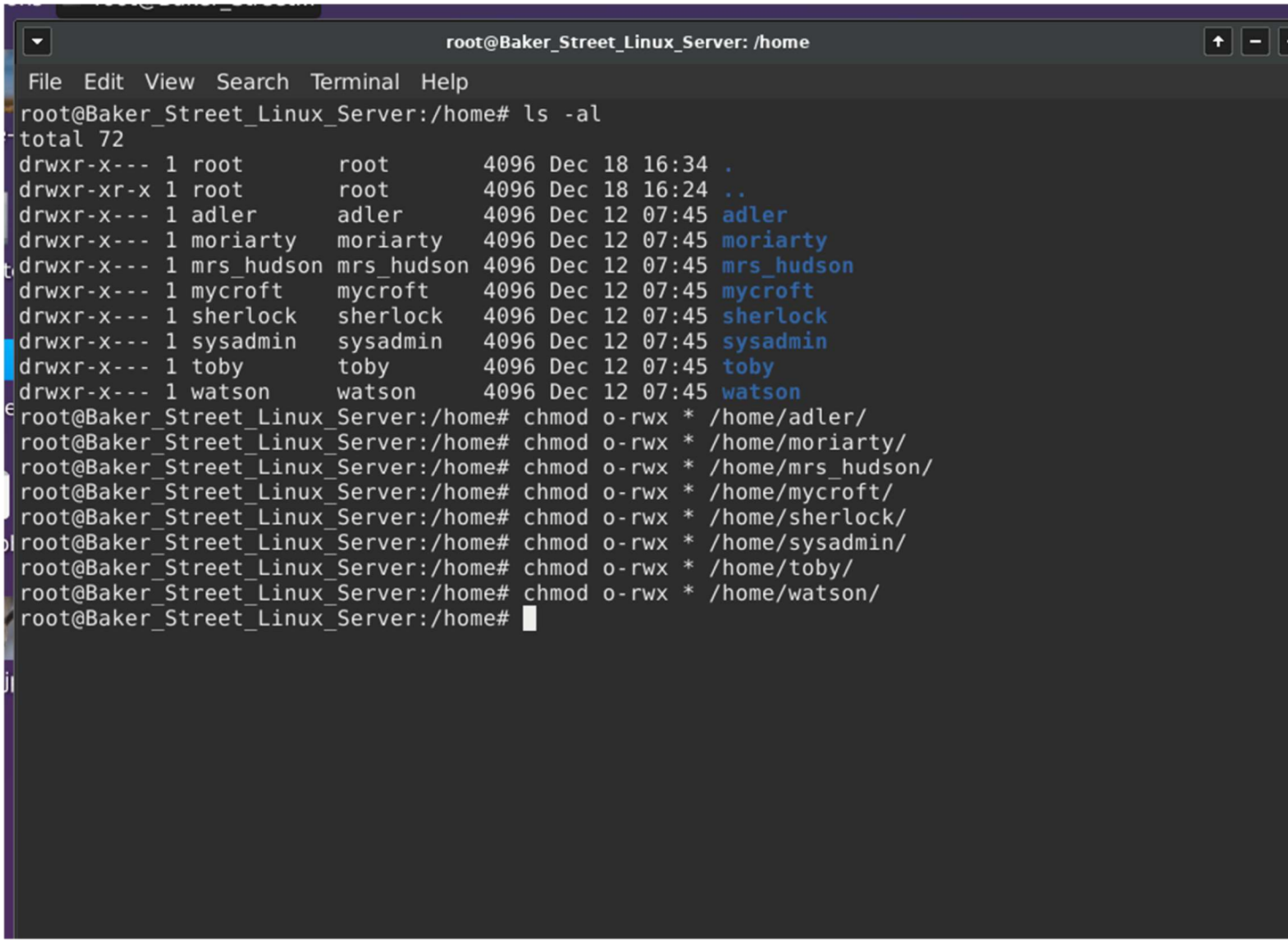
Continuing to list the users files and permissions.



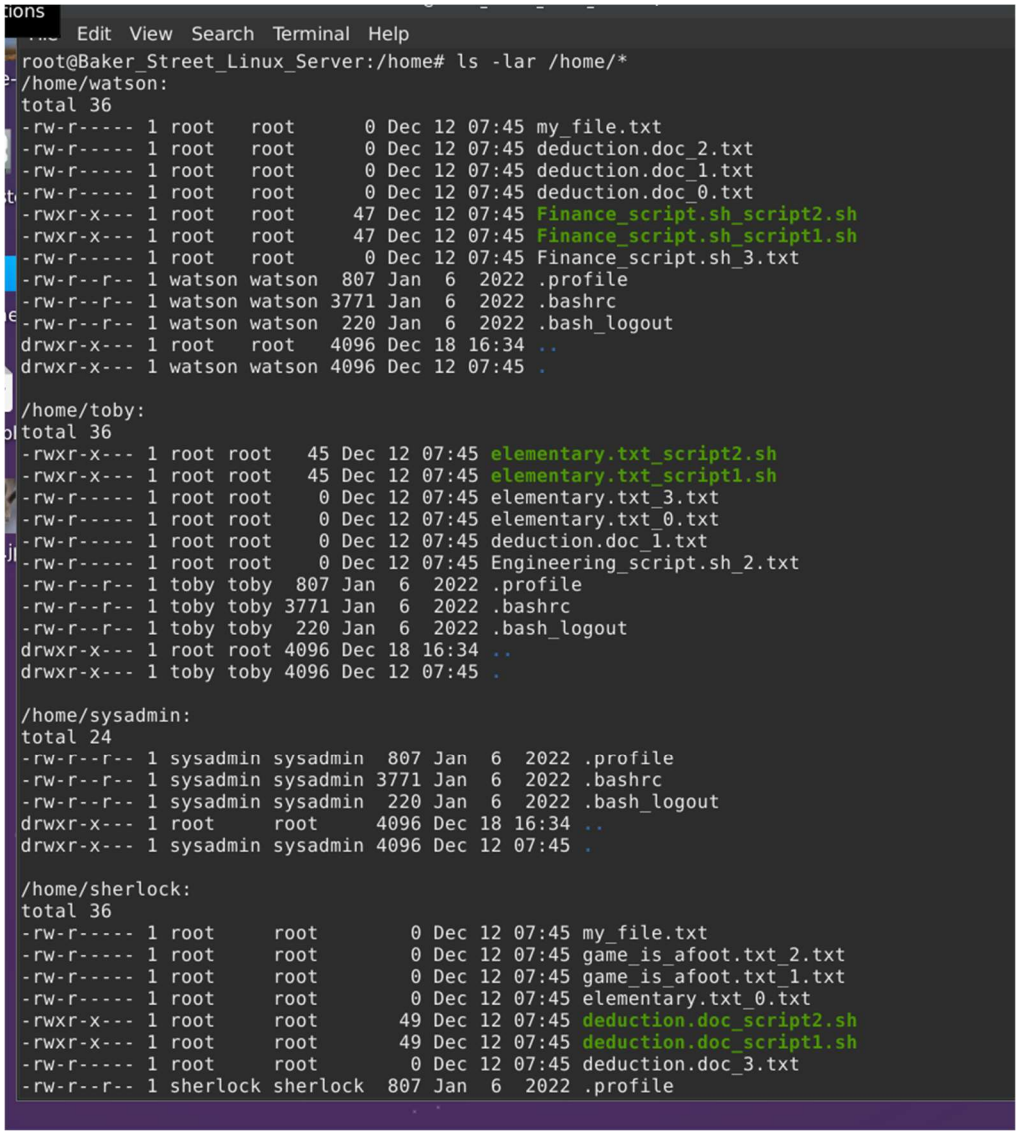
Continuing to list the users files and permissions.



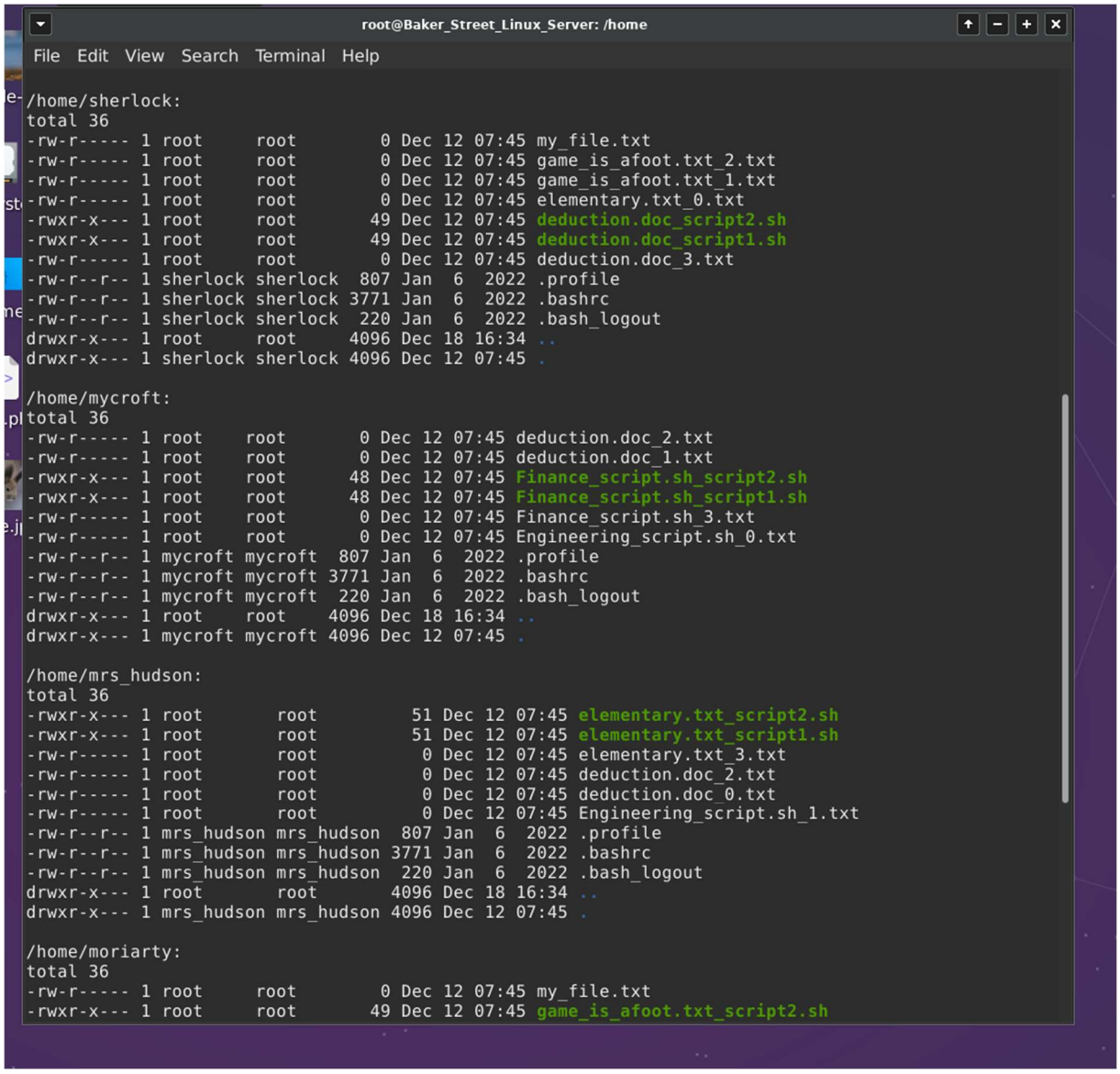
Command to remove any world permissions on files in the user's home directory.



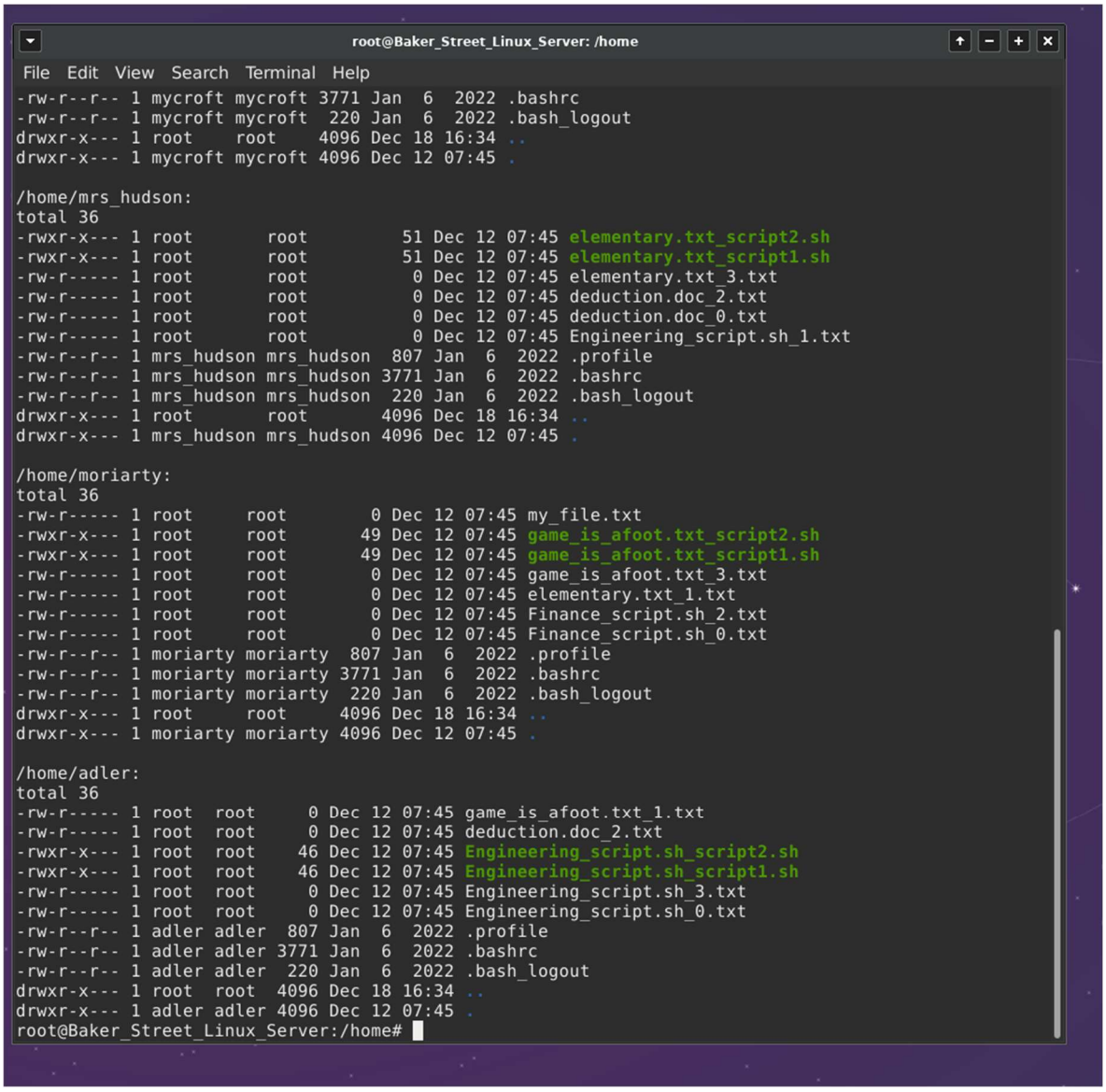
Listing showing no world permissions on the user's home directory and then command to remove any world permissions within the user's home directory.



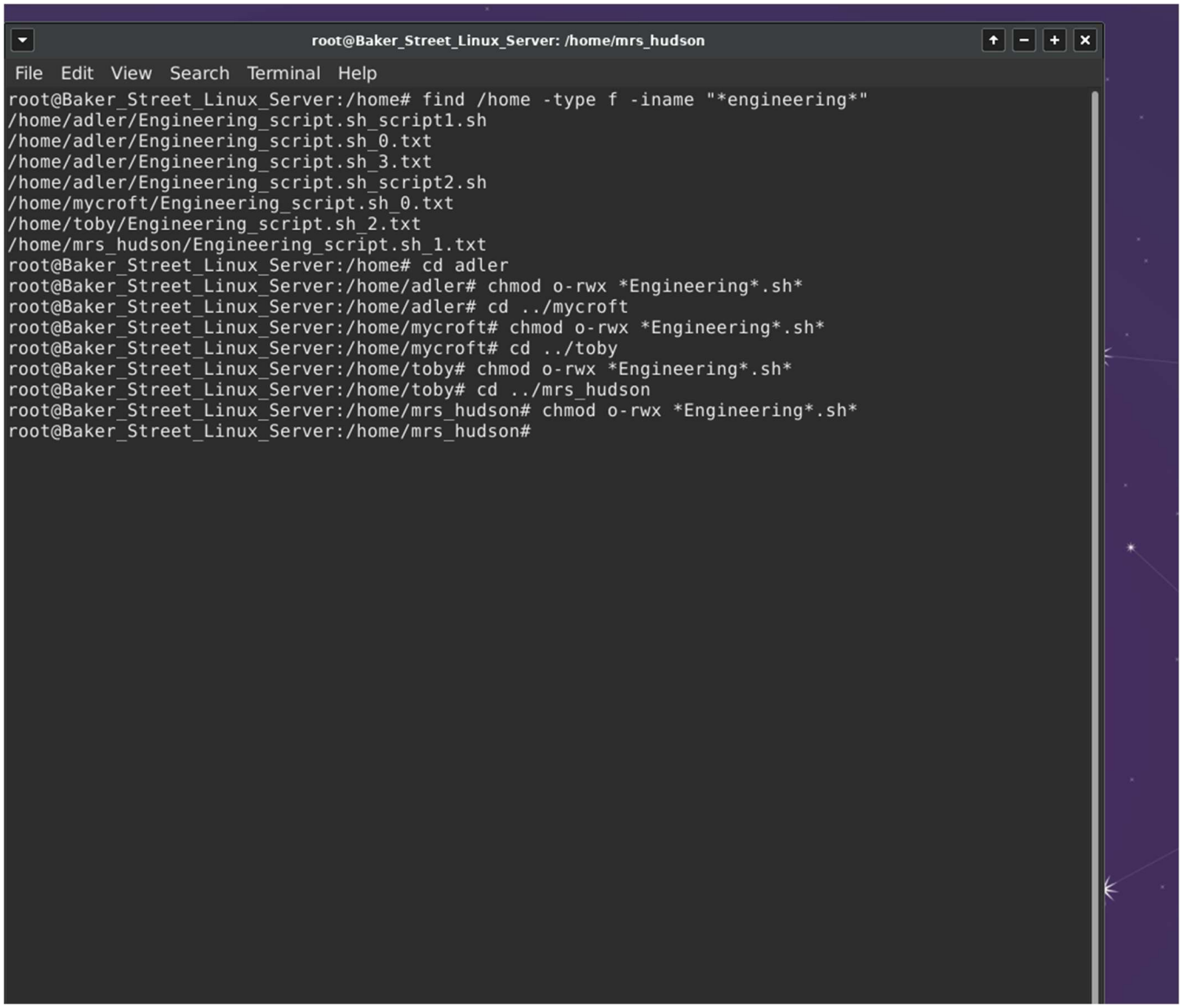
Listing confirming that the files in the user's home directory does not have world permissions.



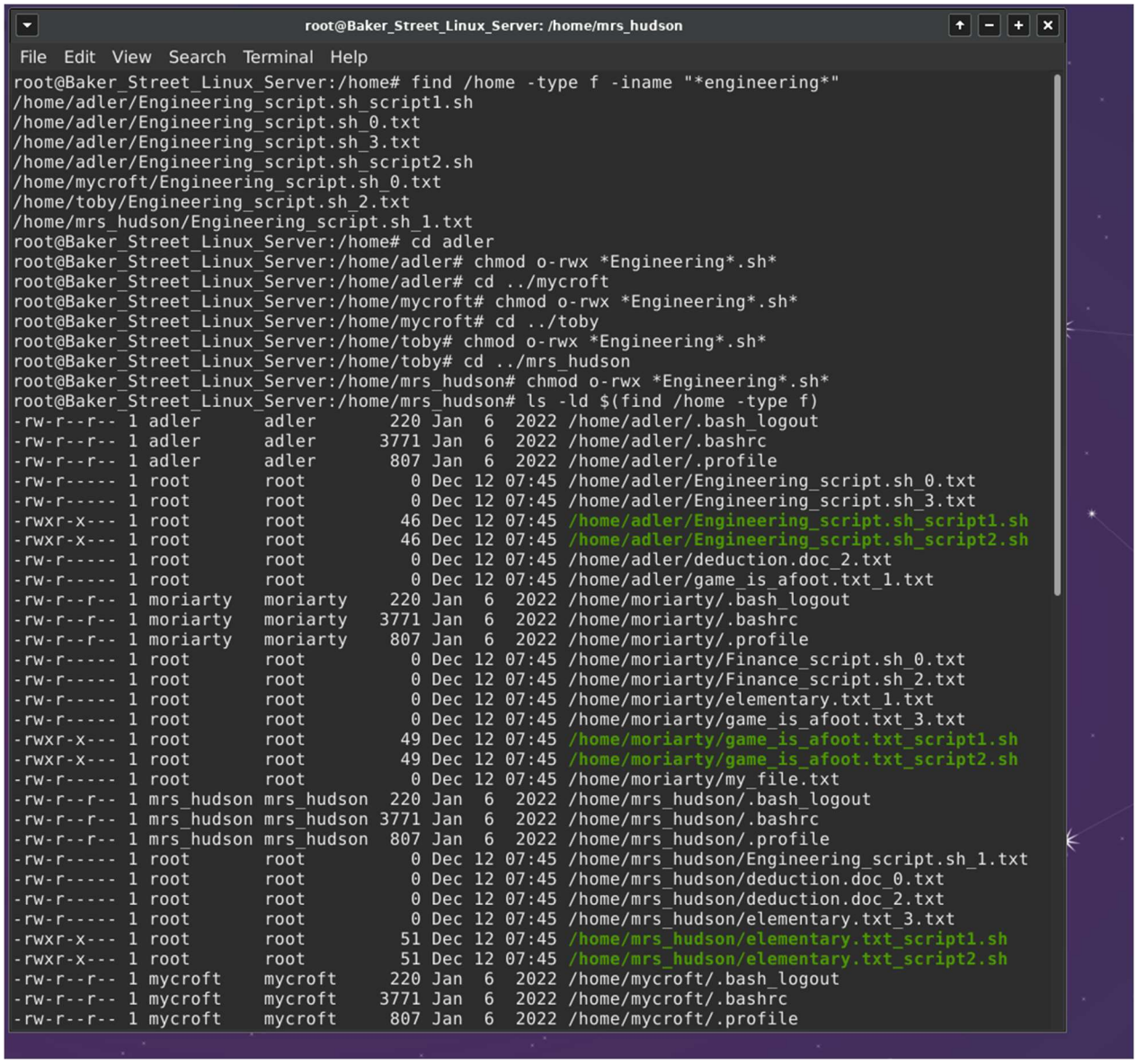
Continuing to confirm that no world permissions exist on files in the user's home directory.



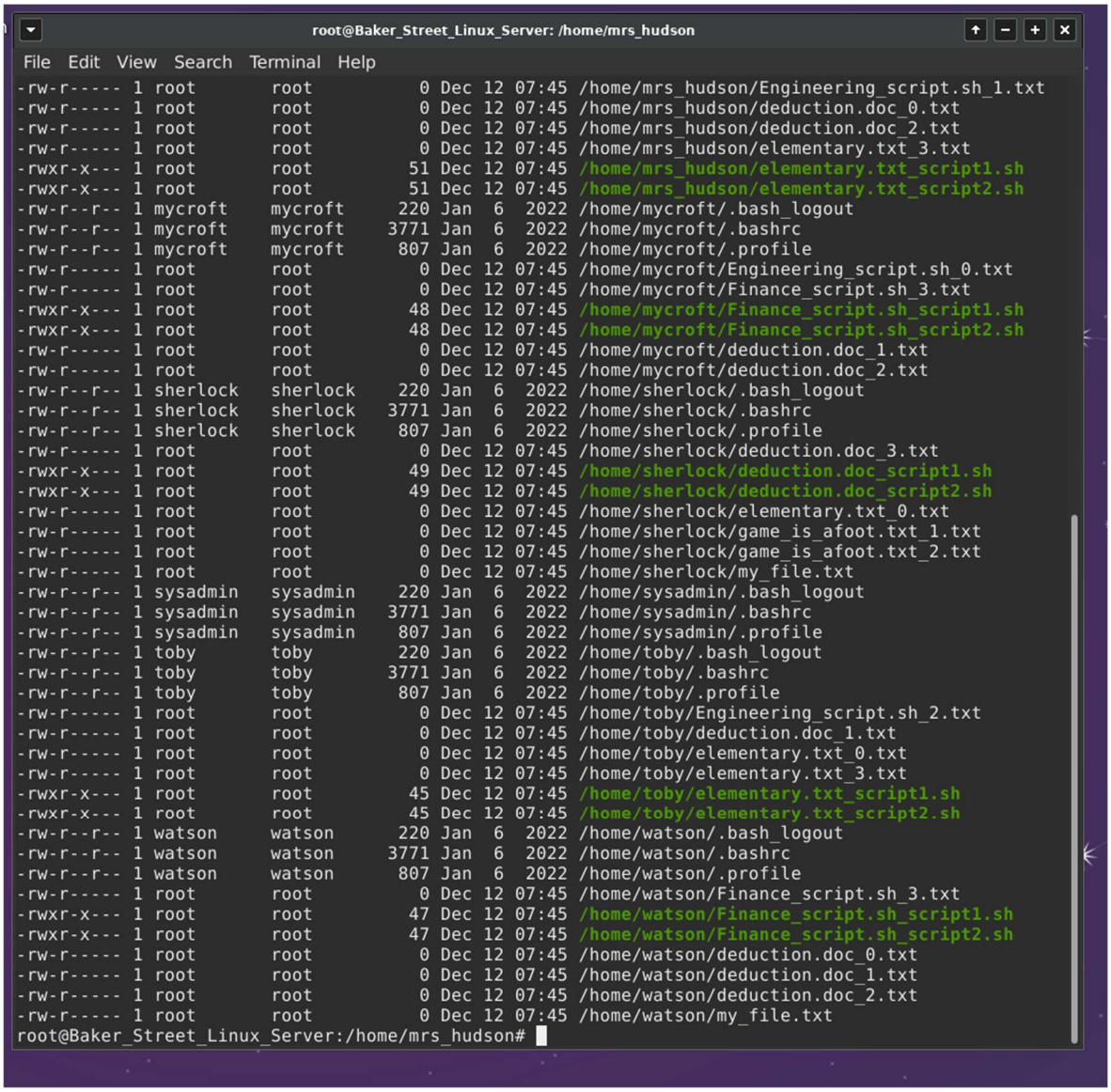
Continuing to confirm that no world permissions exist on files in the user's home directory.



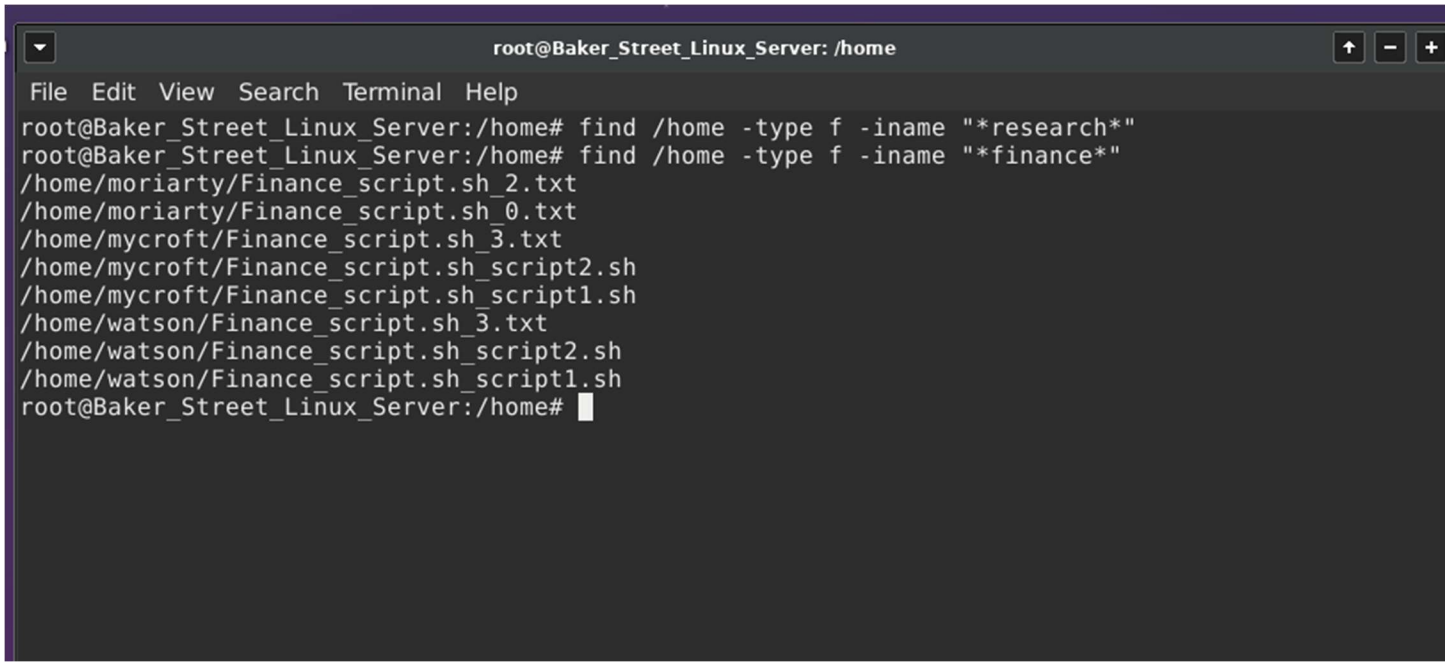
Ensuring that only members of the engineering group can view, edit, or execute engineering scripts.



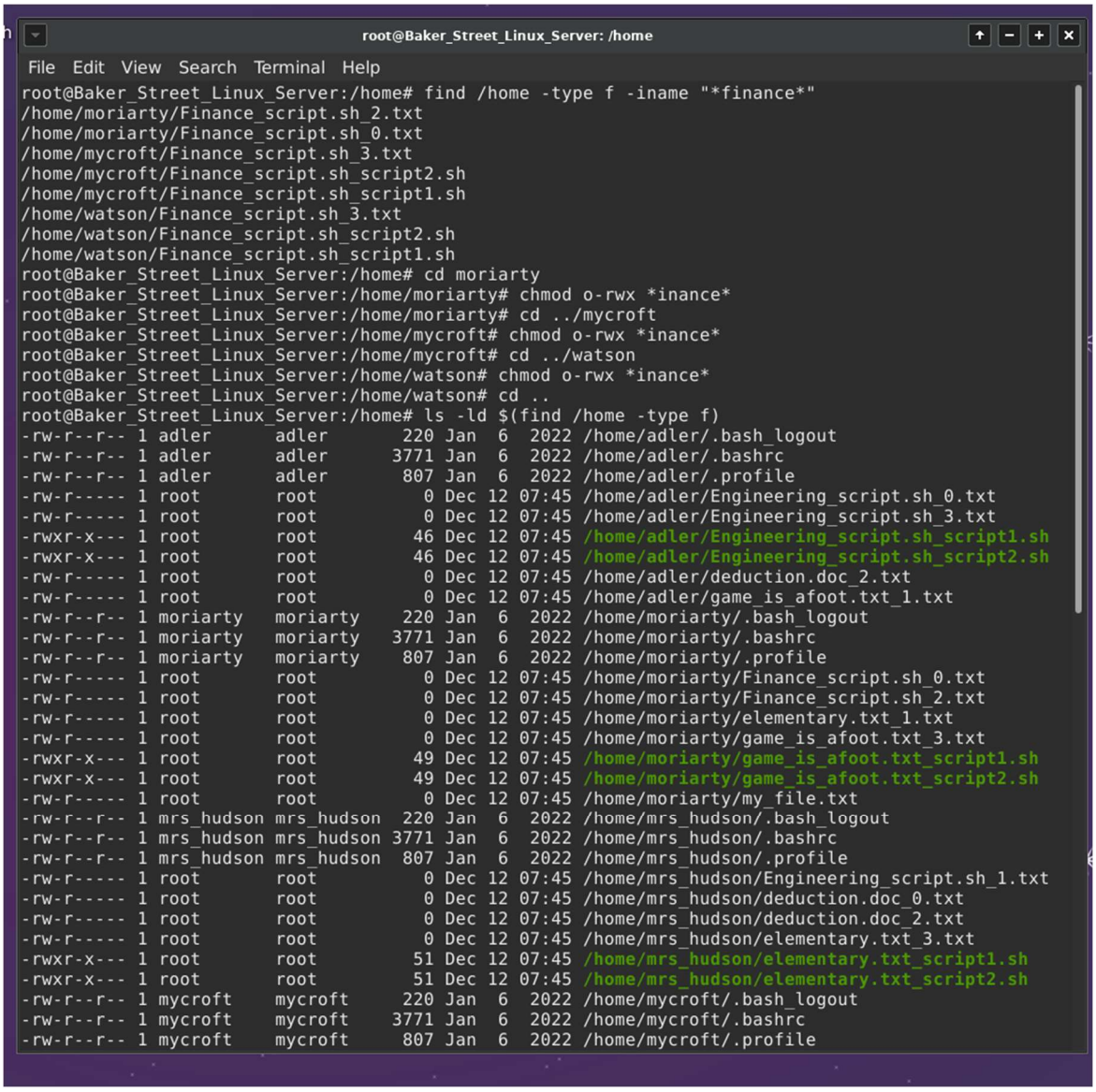
Continuing to ensure that only members of the engineering group can view, edit, or execute engineering scripts.



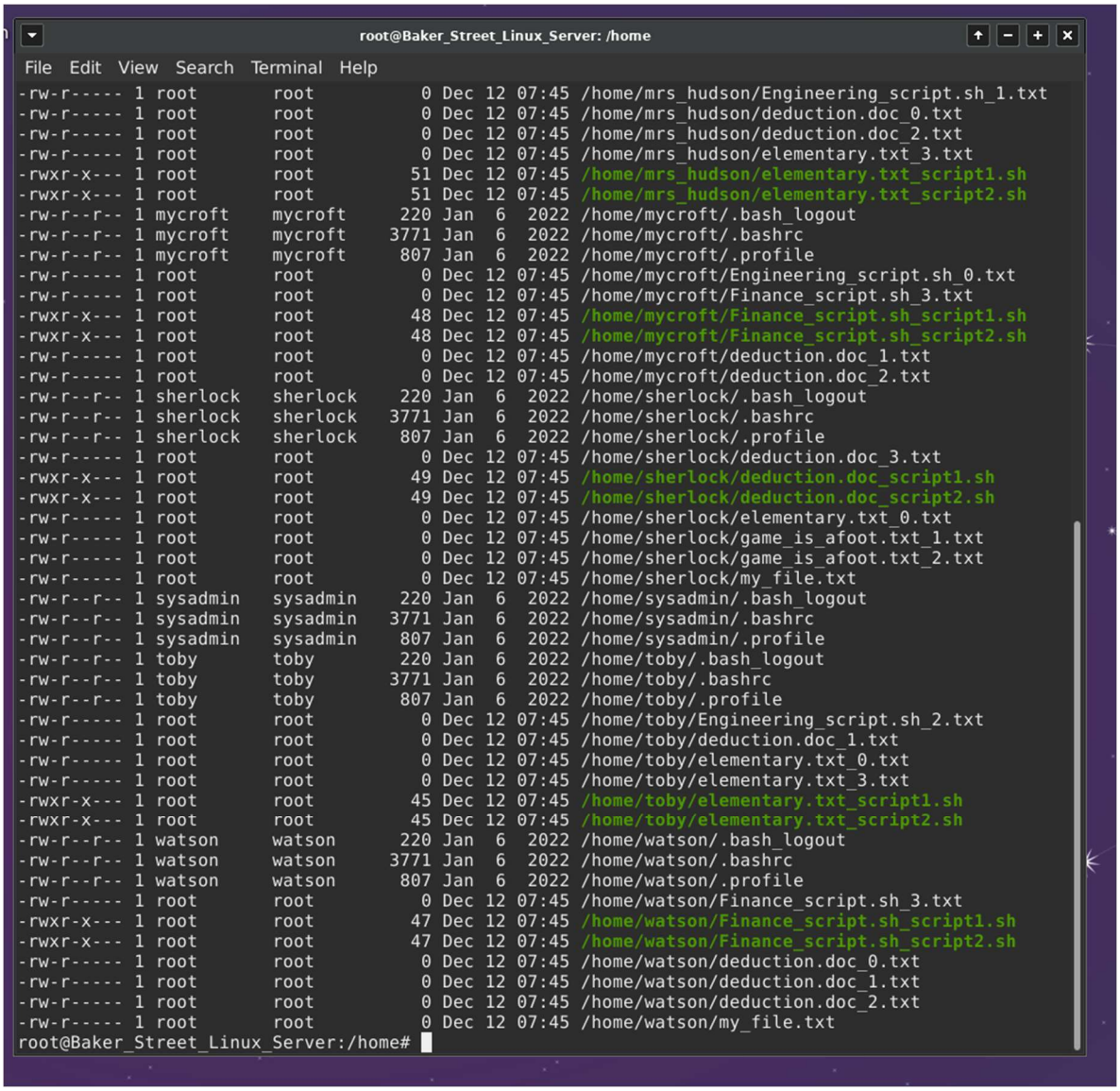
Continuing to ensure that only members of the engineering group can view, edit, or execute engineering scripts.



Looking for research and finance scripts.

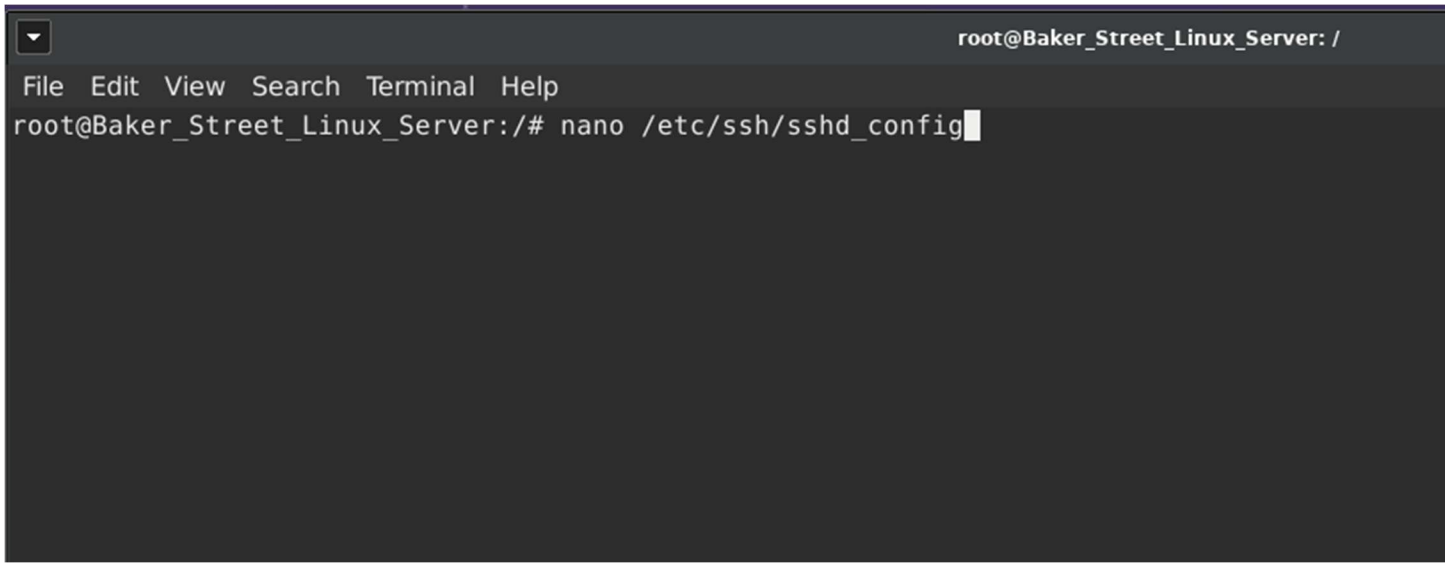


Ensuring that only members of the finance group can view, edit, or execute finance scripts.



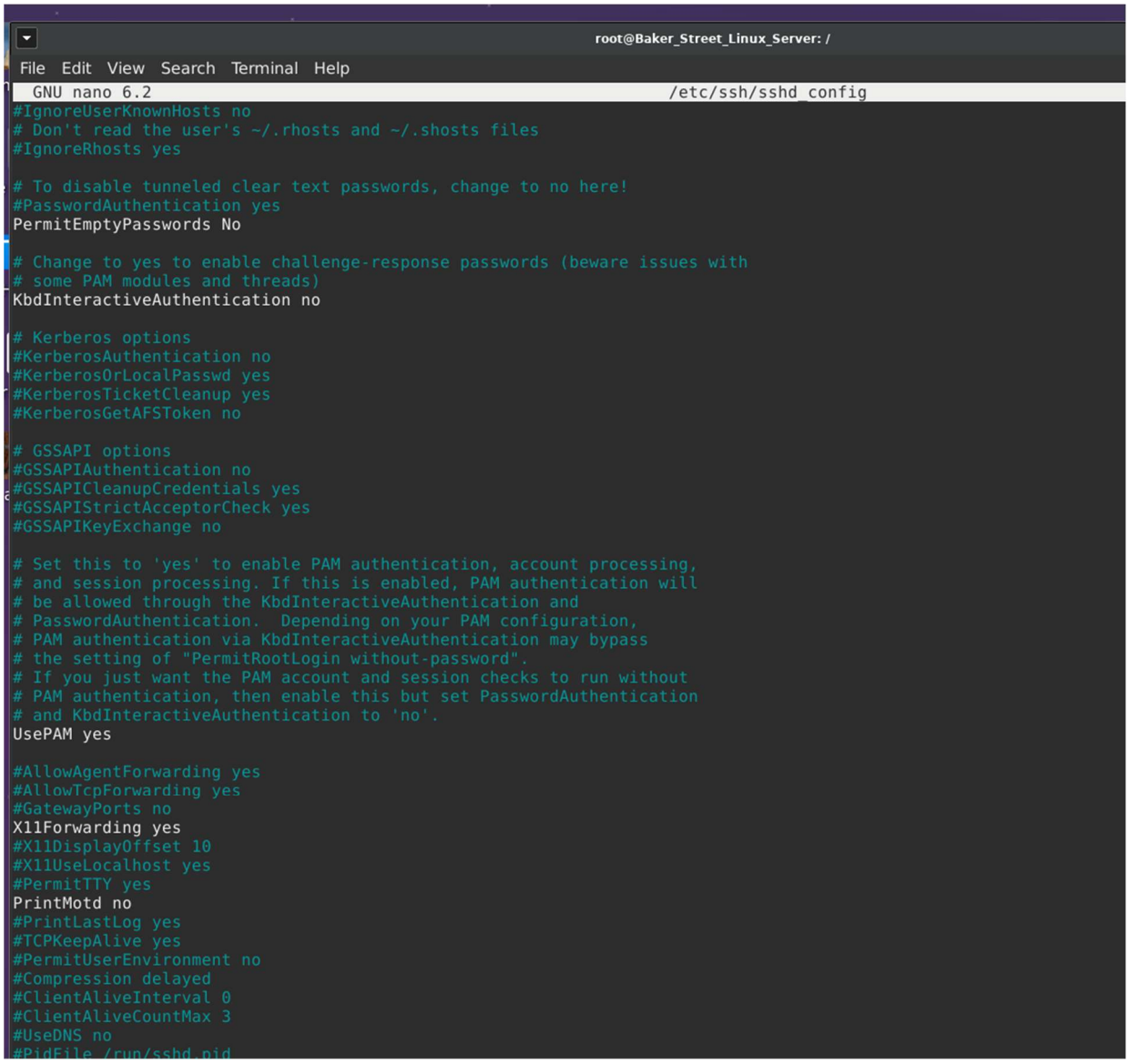
Continuing to ensure that only members of the finance group can view, edit, or execute finance scripts.

10.2 Project 1 Day 2 Activity Guide

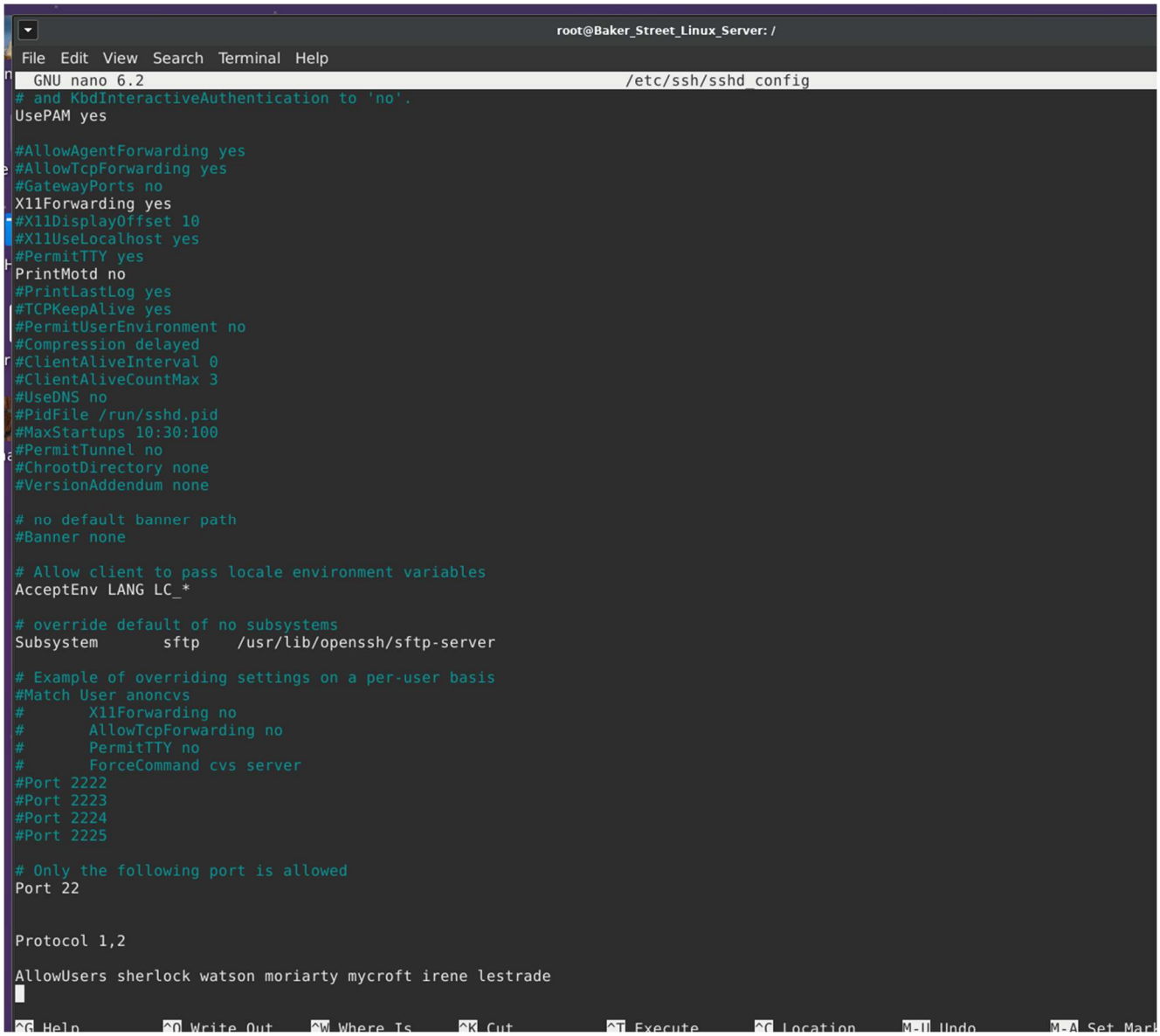


Part 1: Auditing and Security SSH

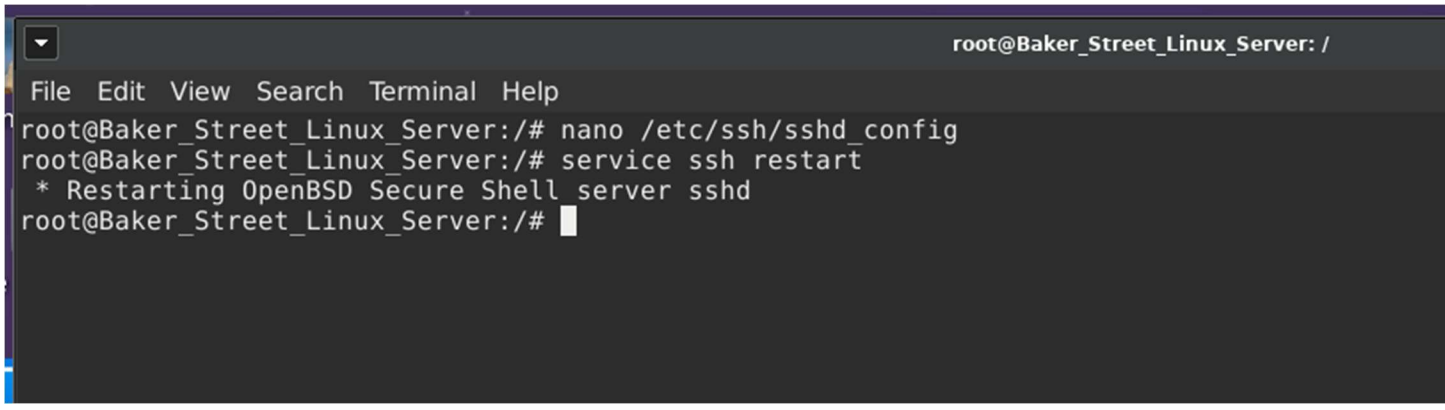
Open the SSH Configuration file to edit.



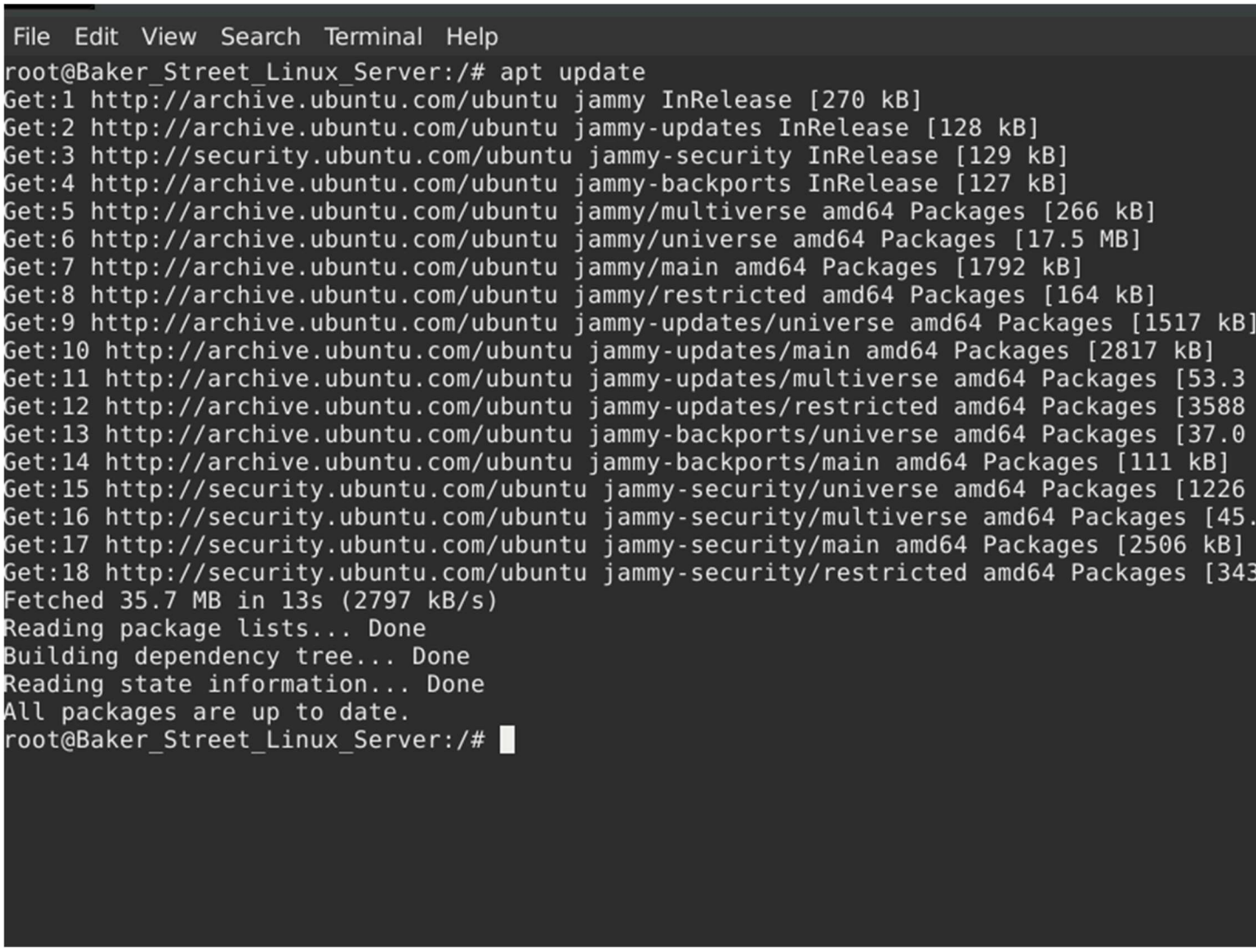
Editing SSH to harden SSH with strict controls.



Continuing to edit the SSH configuration file.

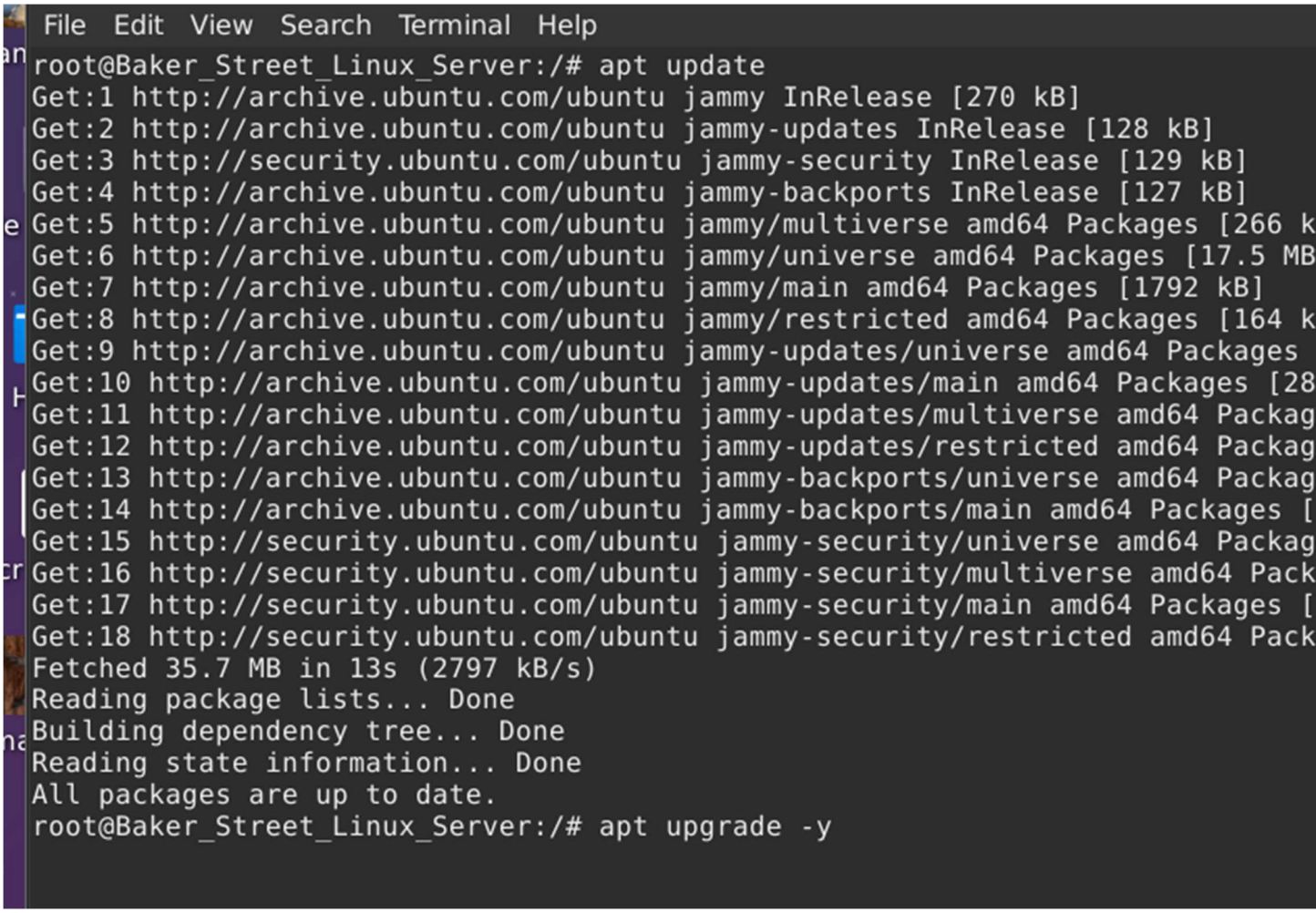


Restarting the SSH service to set the configuration updates.

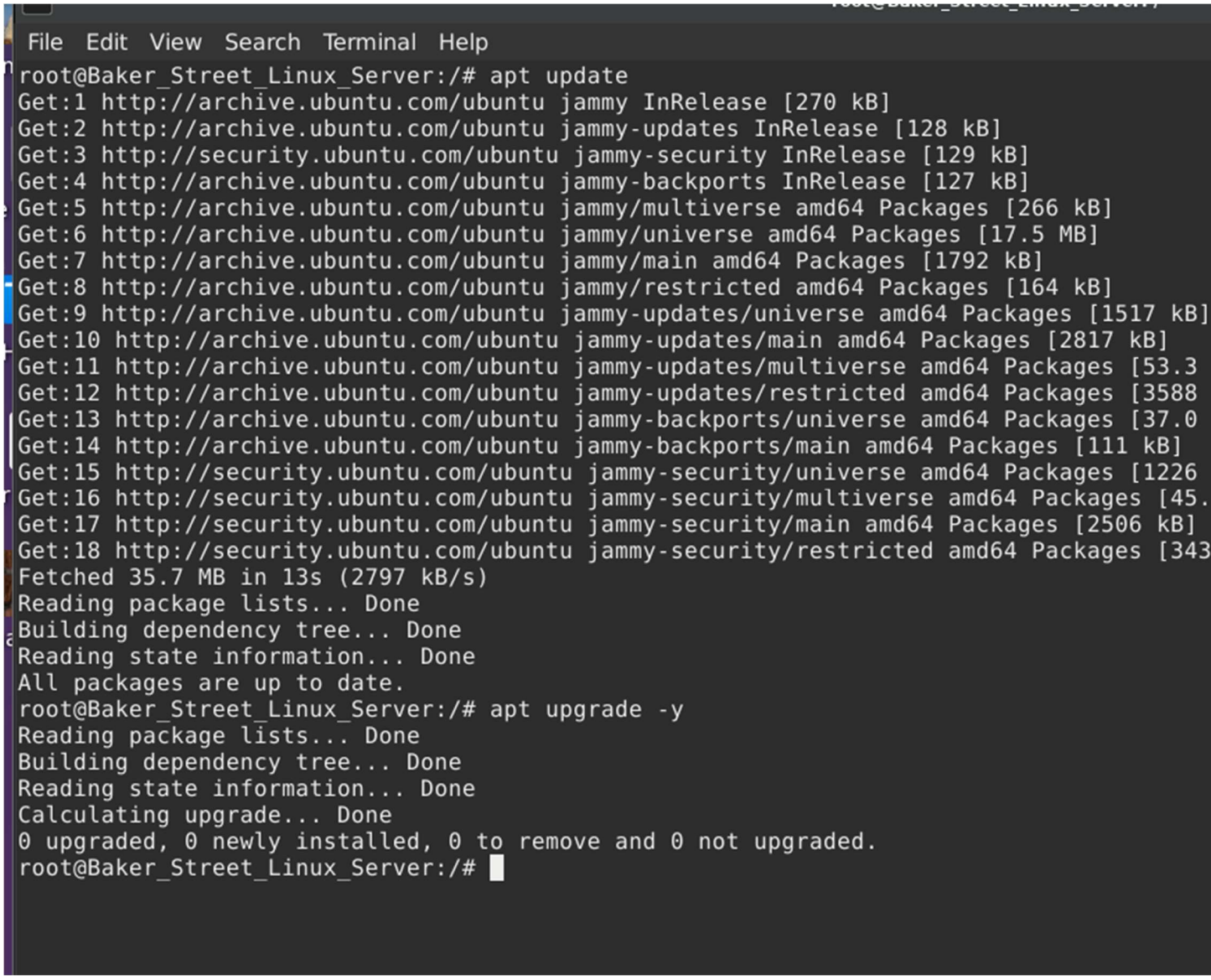


Part 2: Review, Update, and Add System Packages

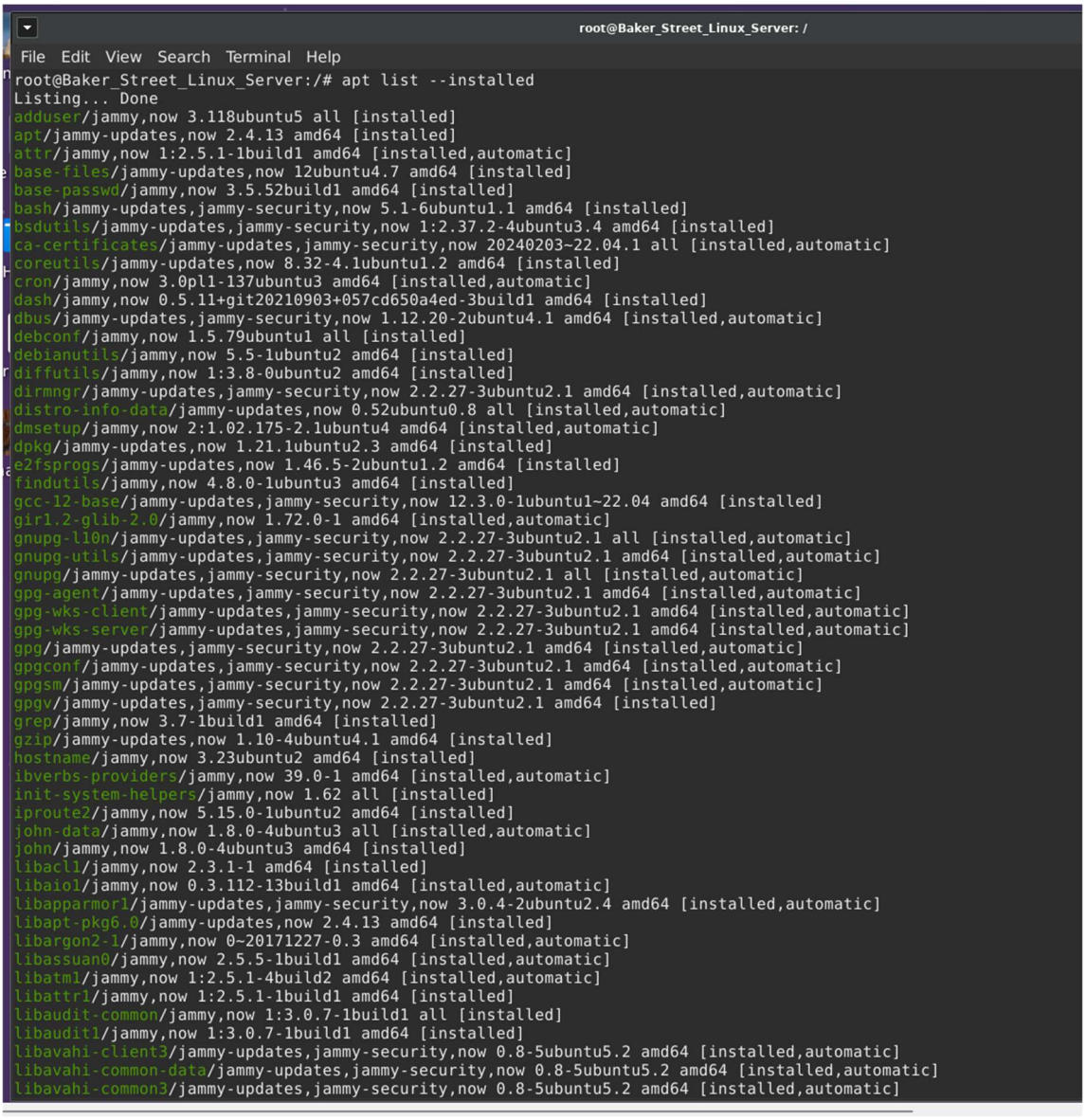
Commands to update system packages.



Command to upgrade system packages.

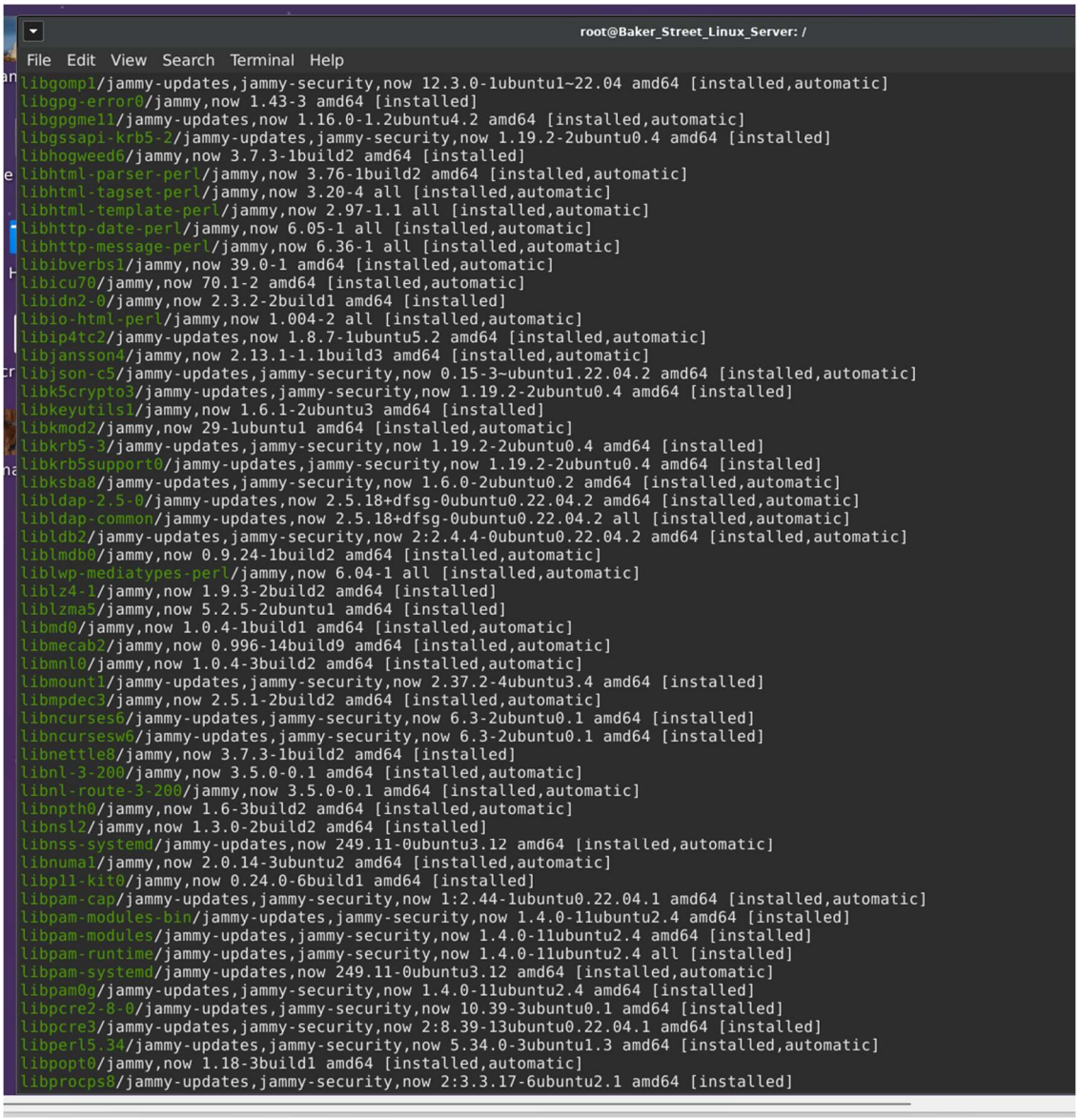


Confirmation of the upgrade to the packages.

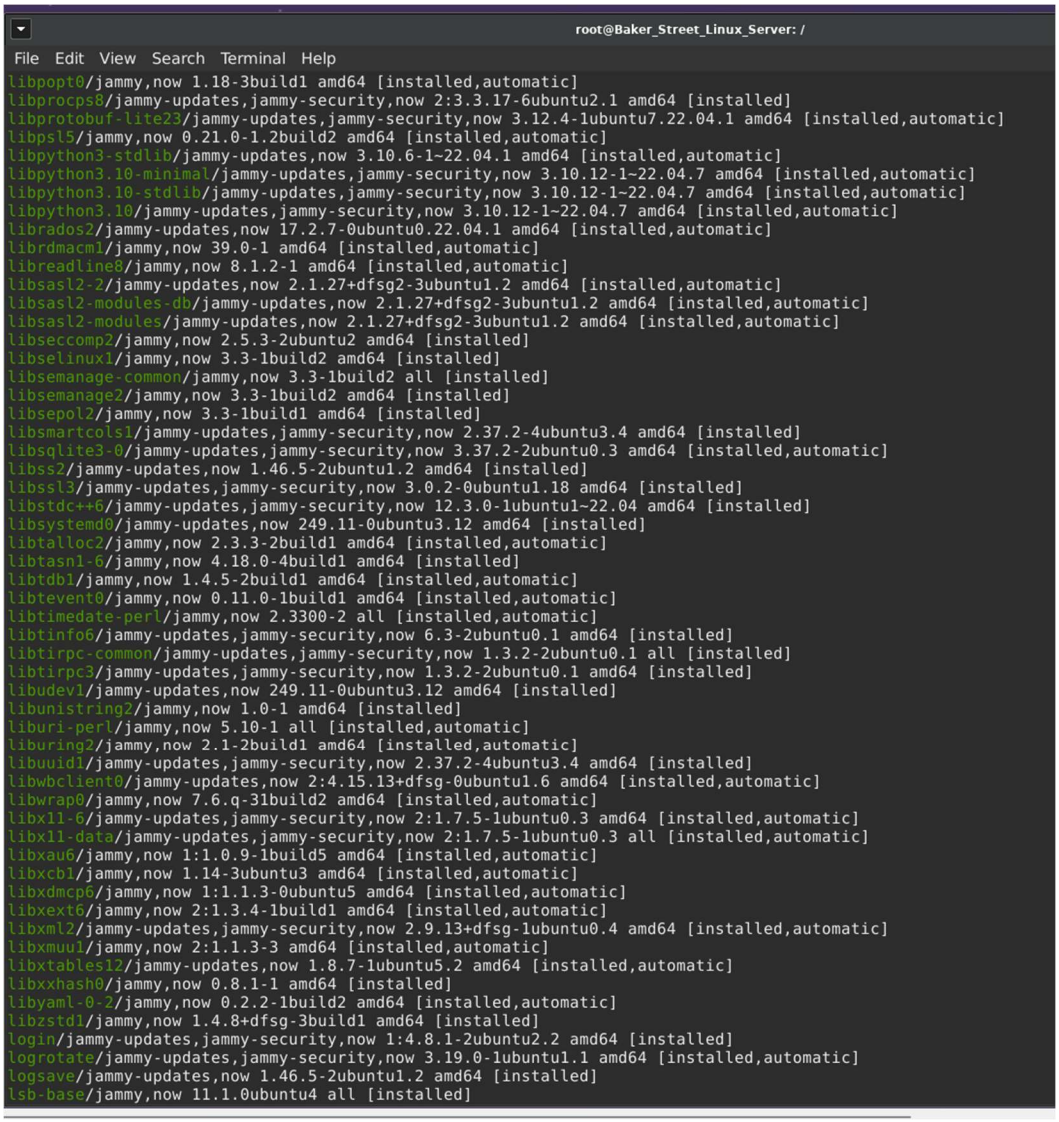


Listing all installed packages.

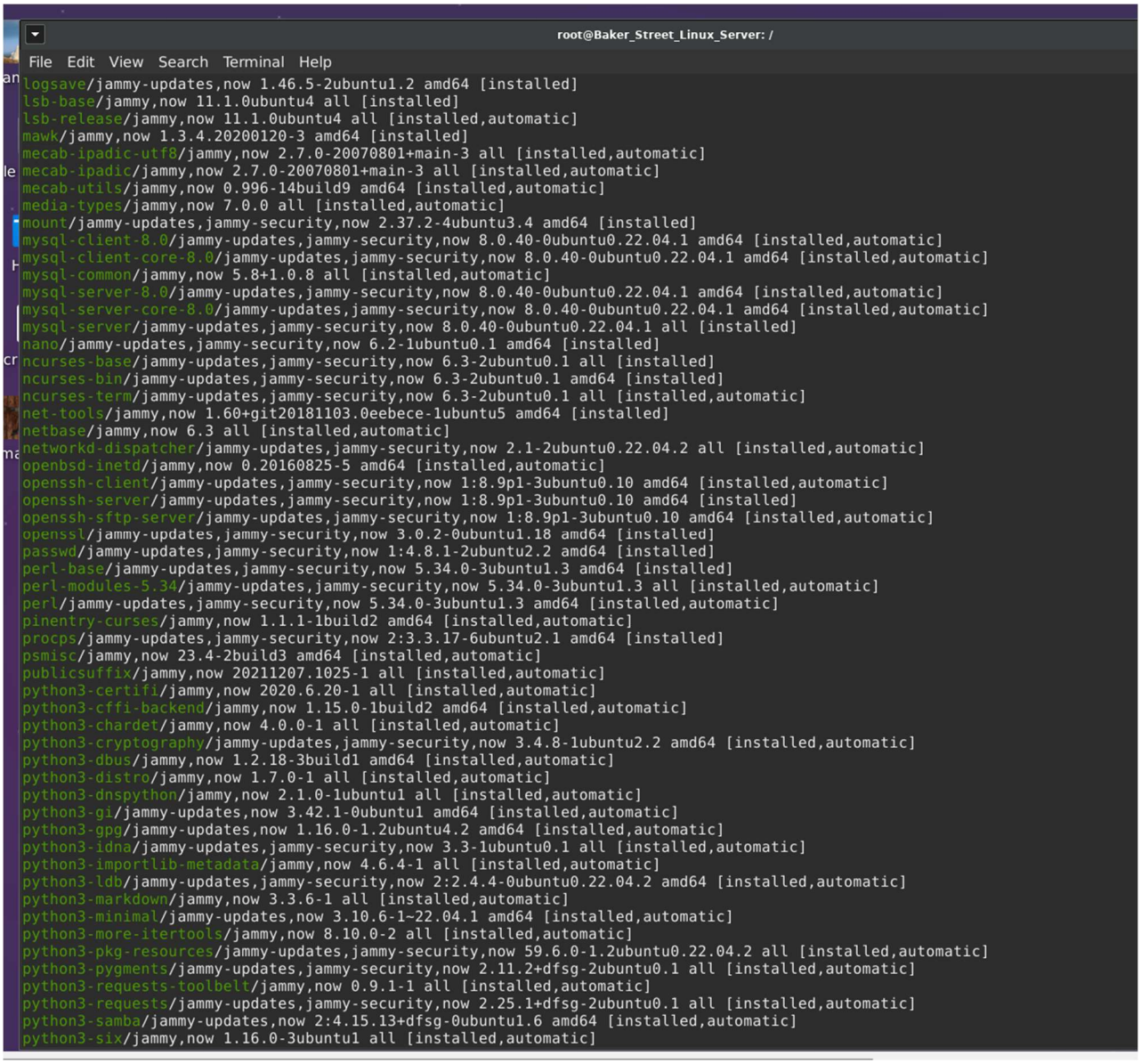
Continuing list of all installed packages.



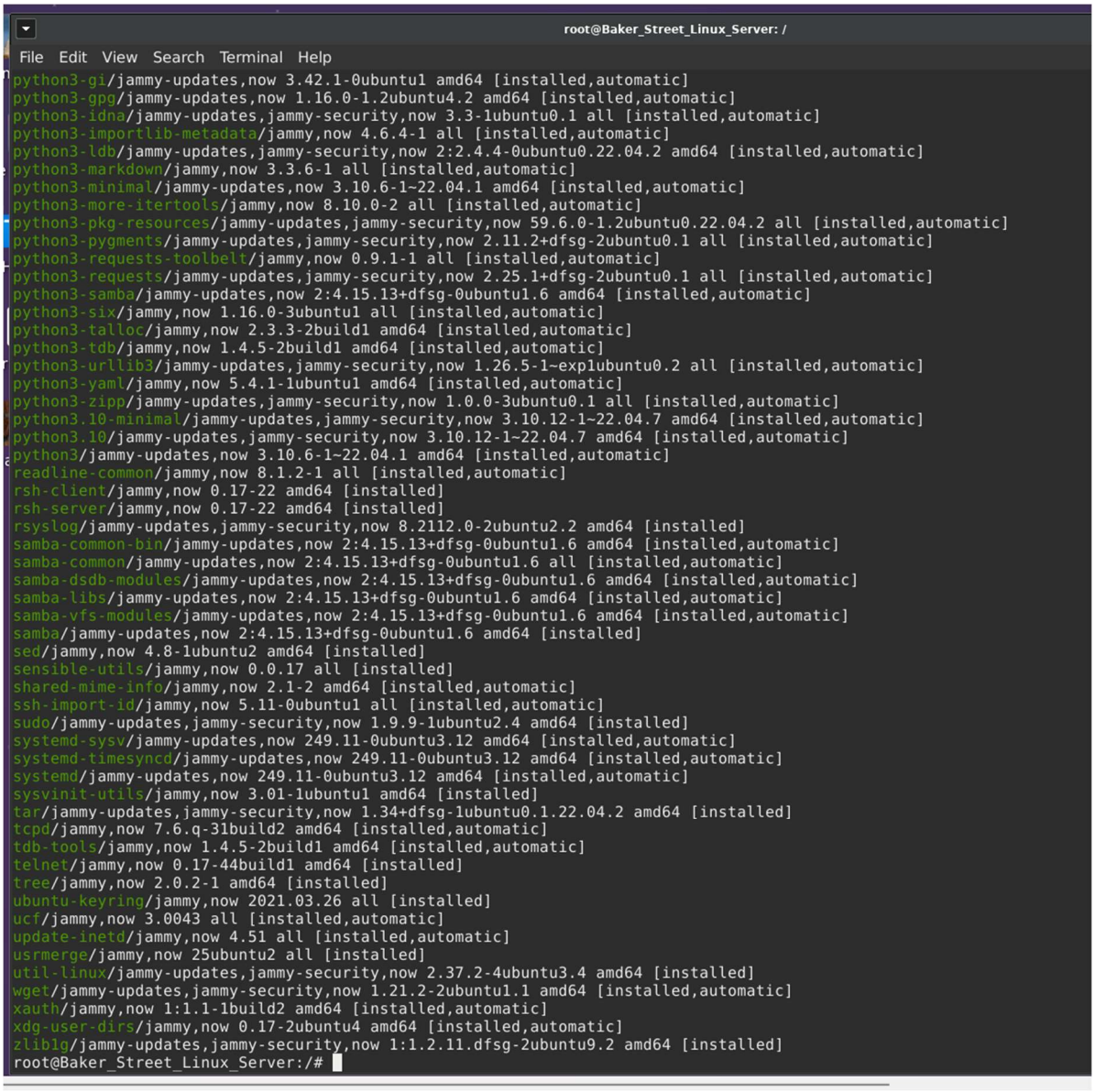
Continuing list of all installed packages.



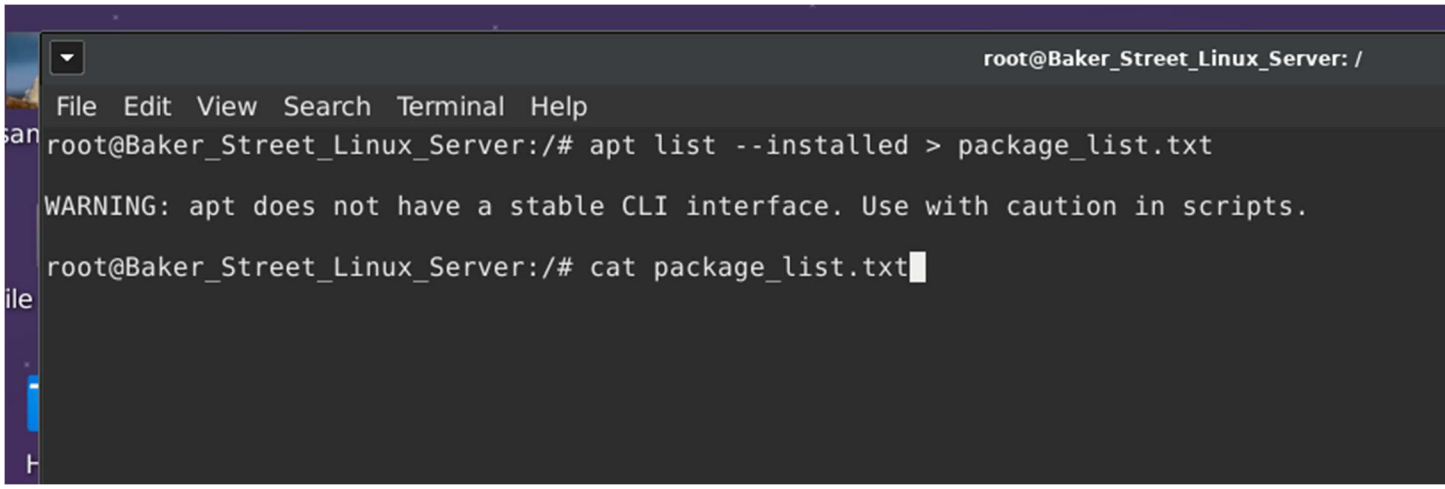
Continuing list of all installed packages.



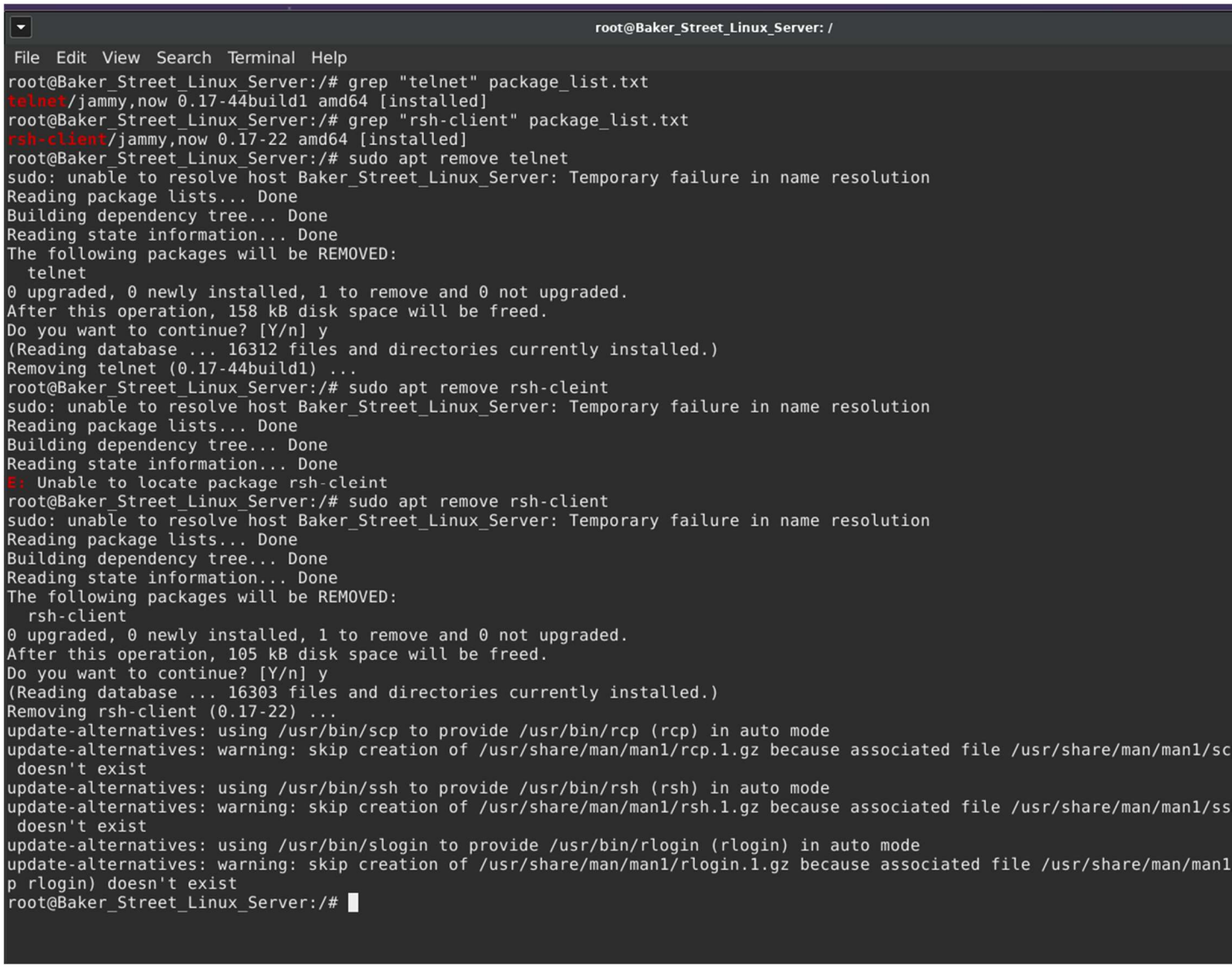
Continuing list of all installed packages.



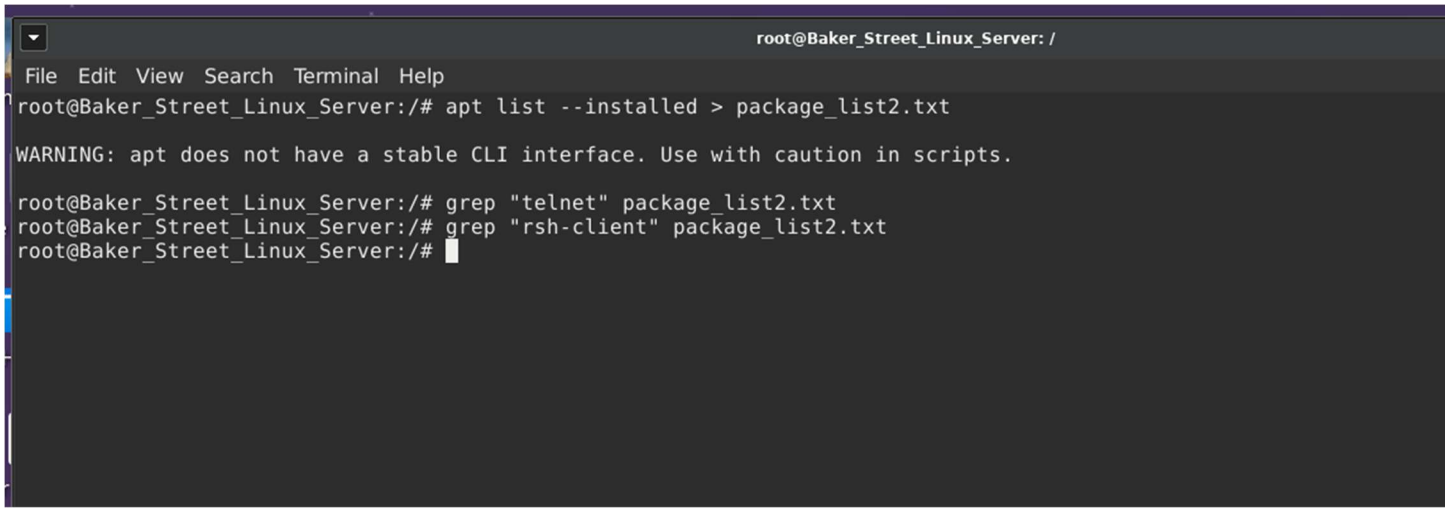
Continuing list of all installed packages.



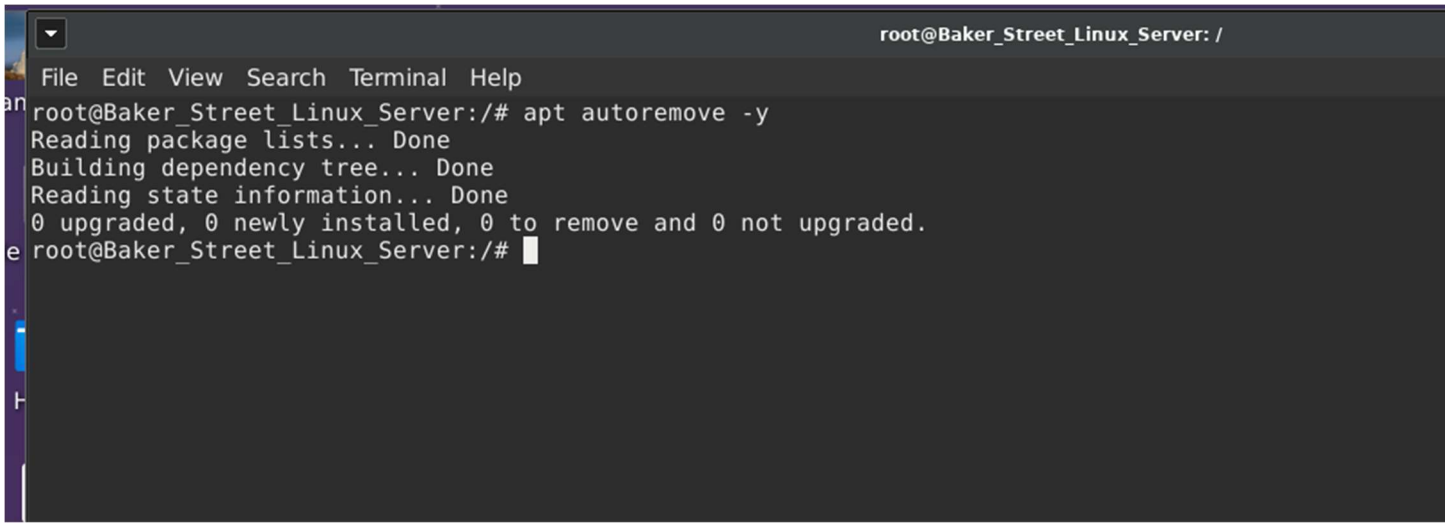
Create a file package_list.txt which contains all the installed packages.



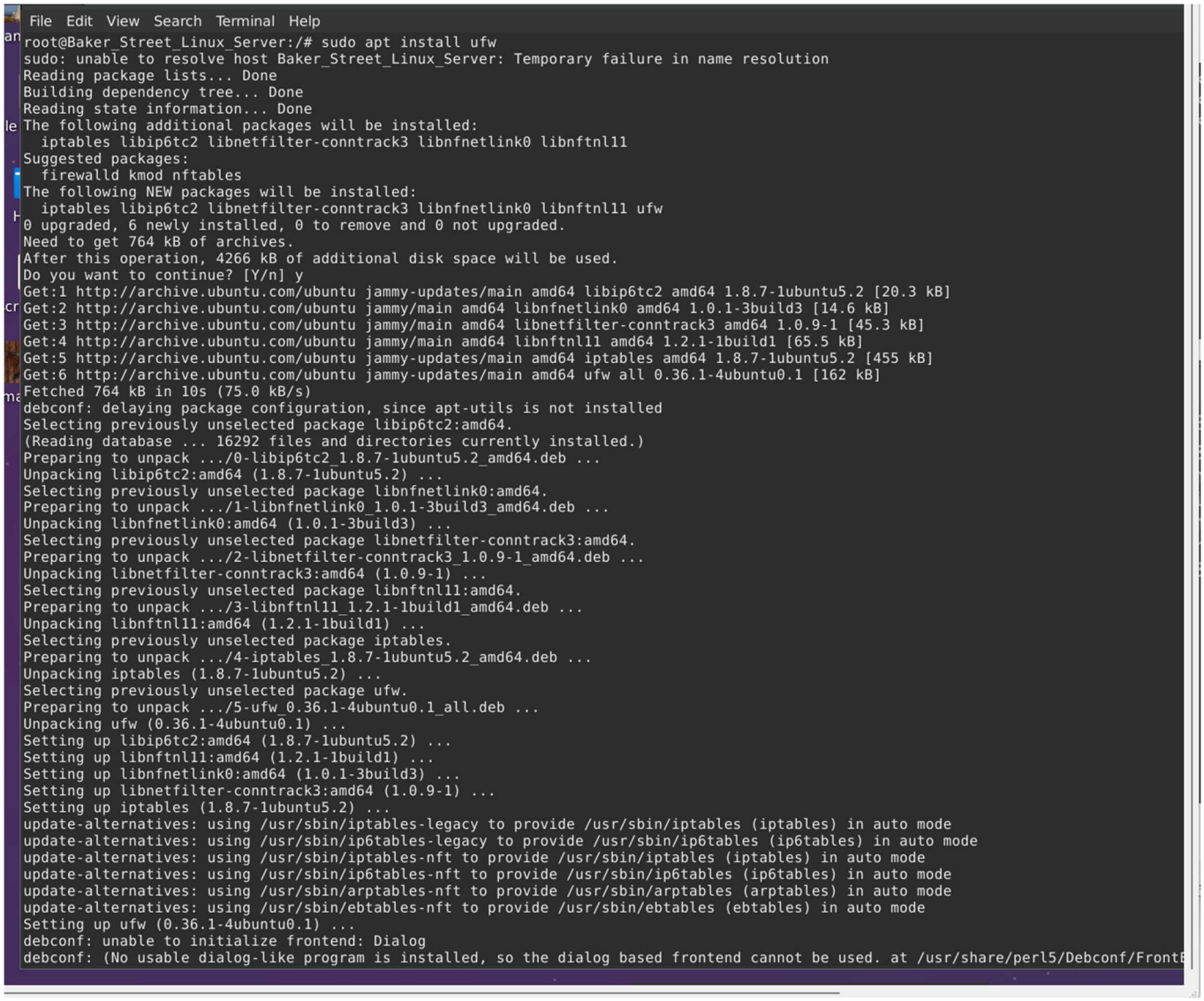
Identifying and removing telnet and rsh-client and all unnecessary dependencies.



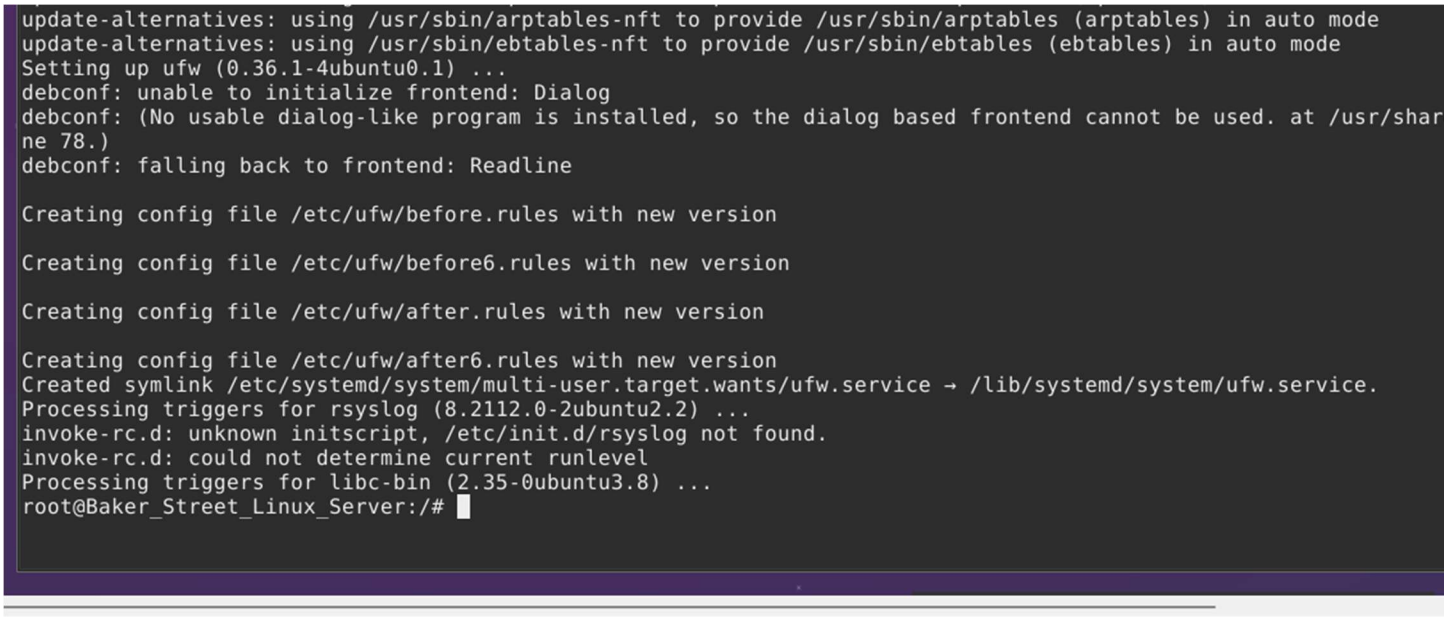
Confirming telnet and rsh-client are no longer in the package list.



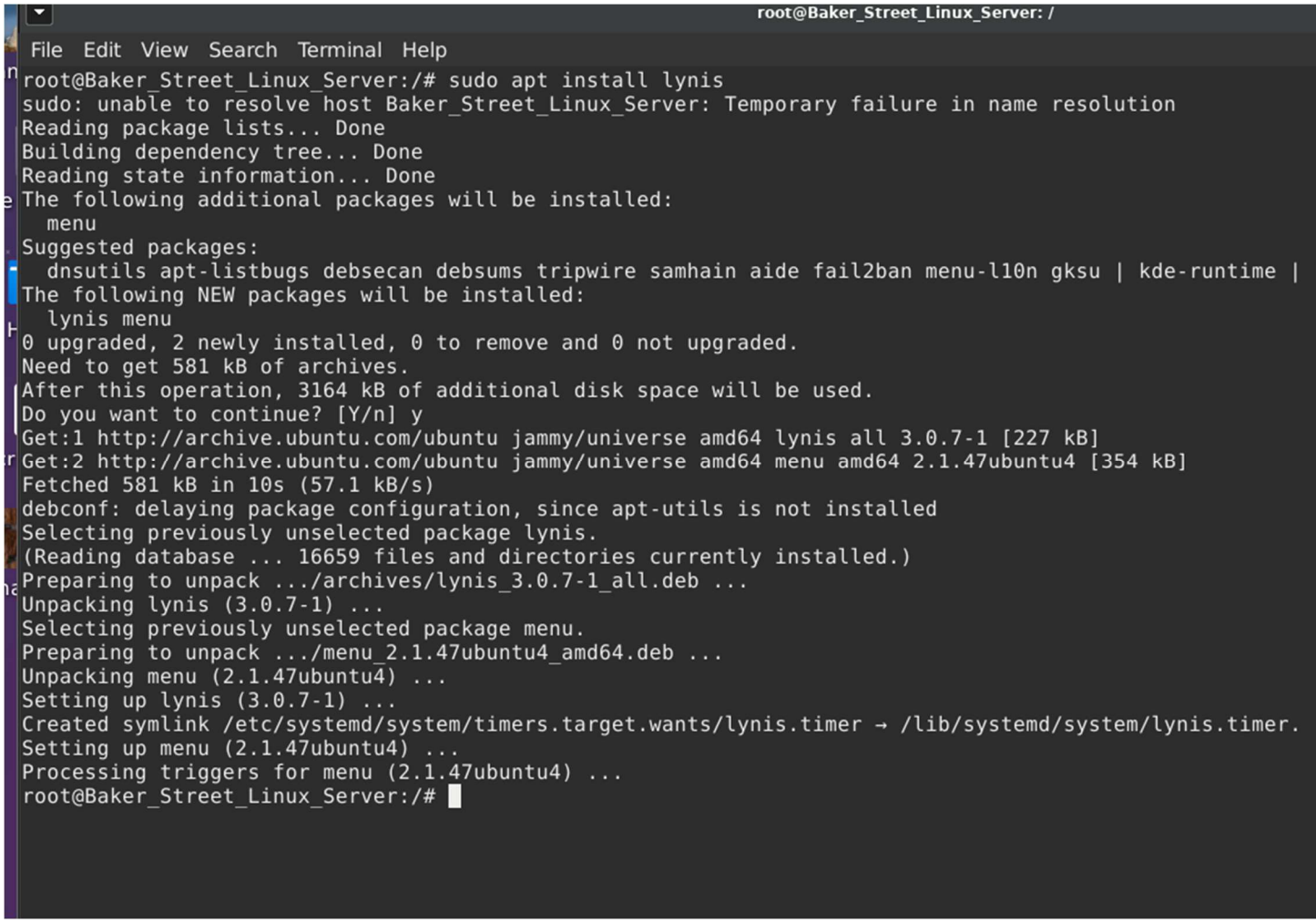
Confirming telnet and rsh-client are no longer in the package list.



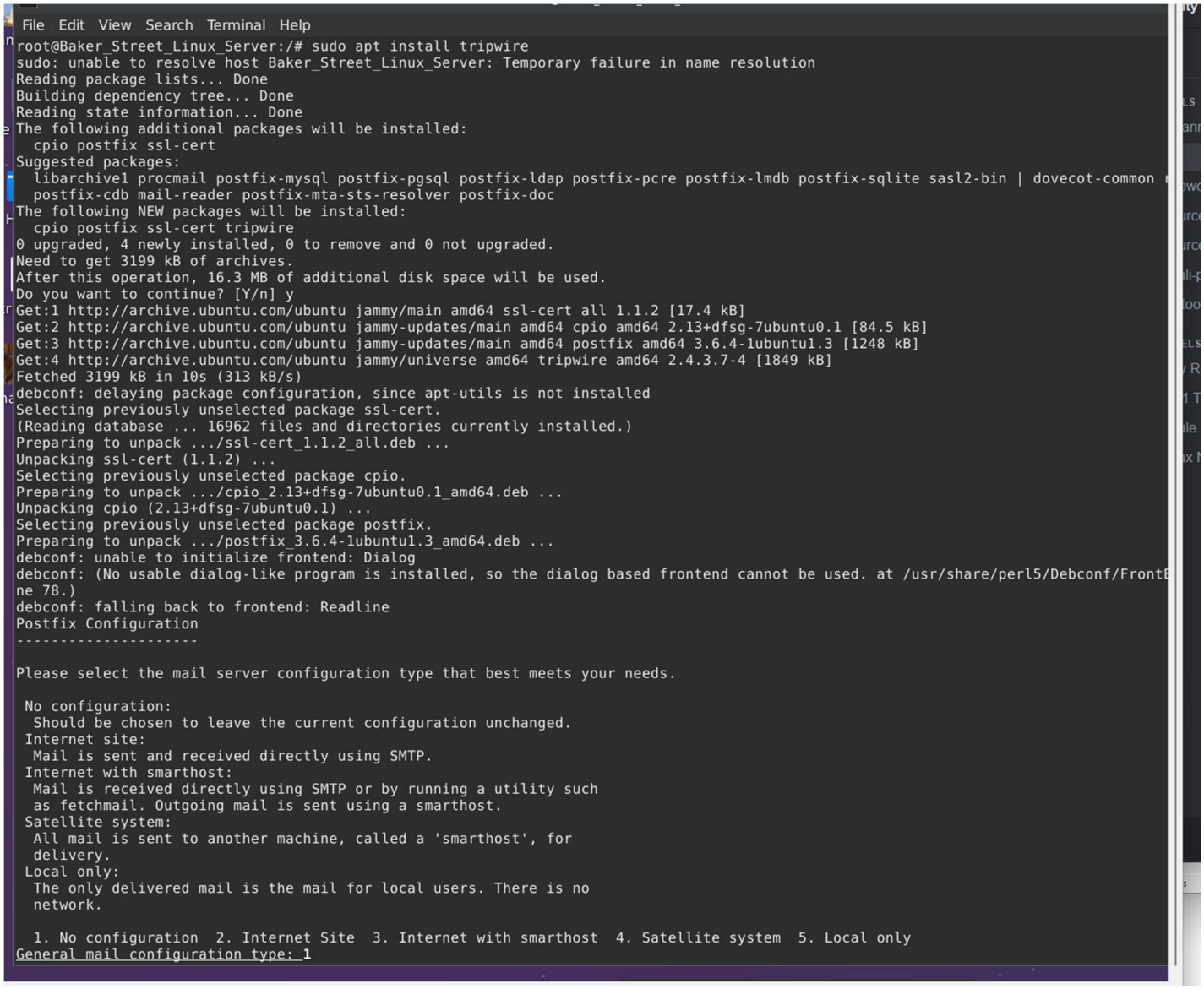
Adding ufw package.



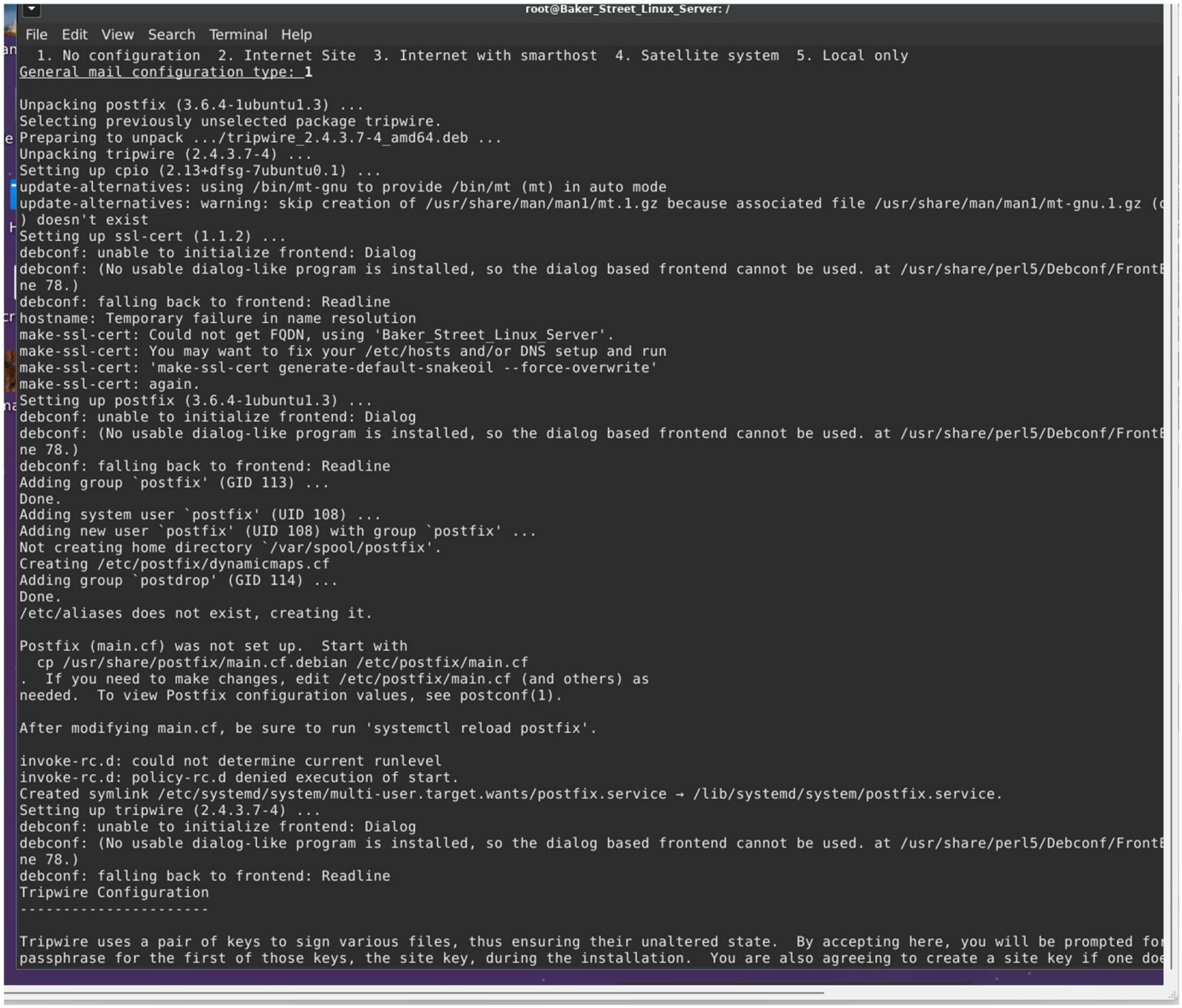
Confirming ufw package install.



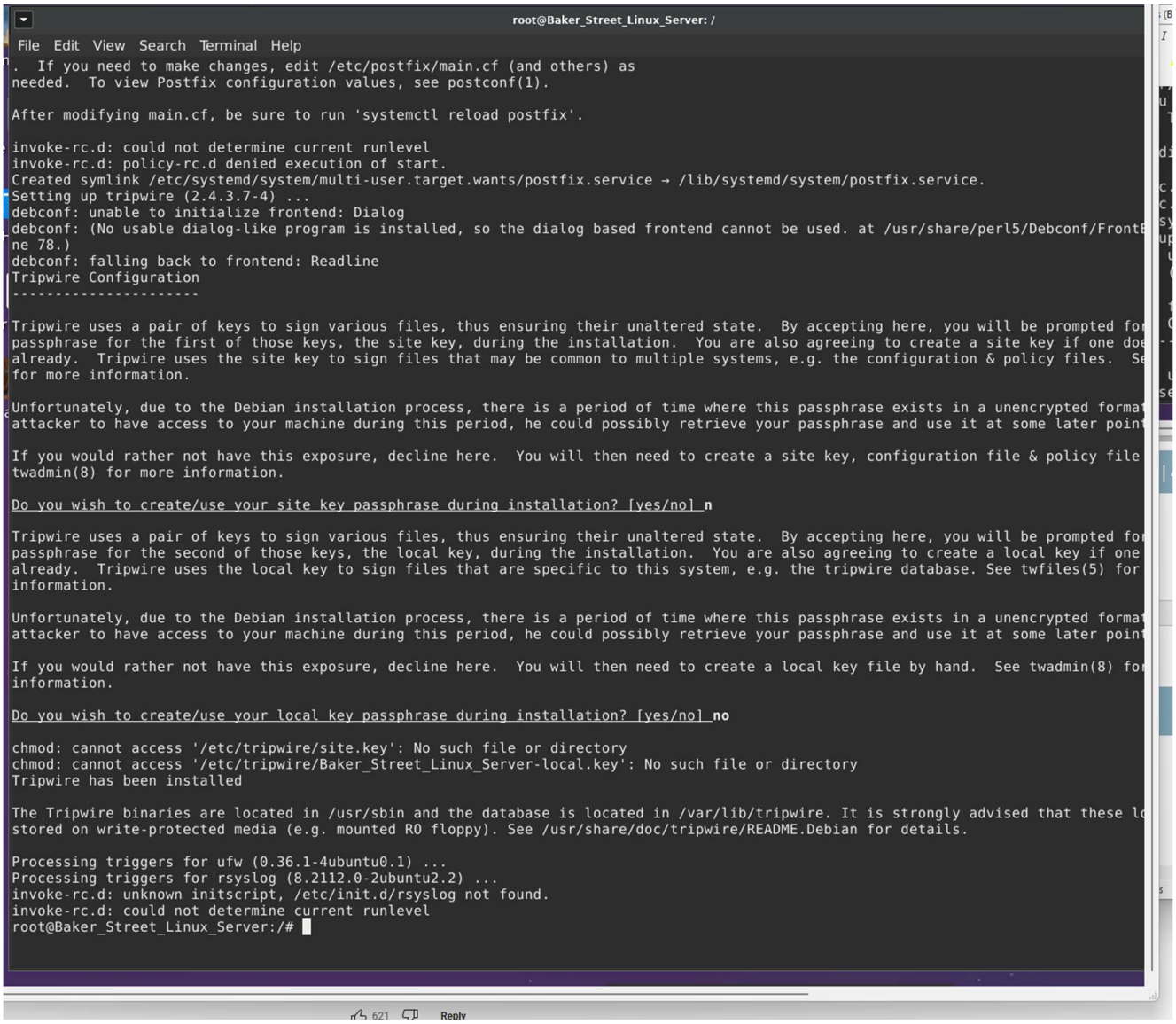
Installing lynis.



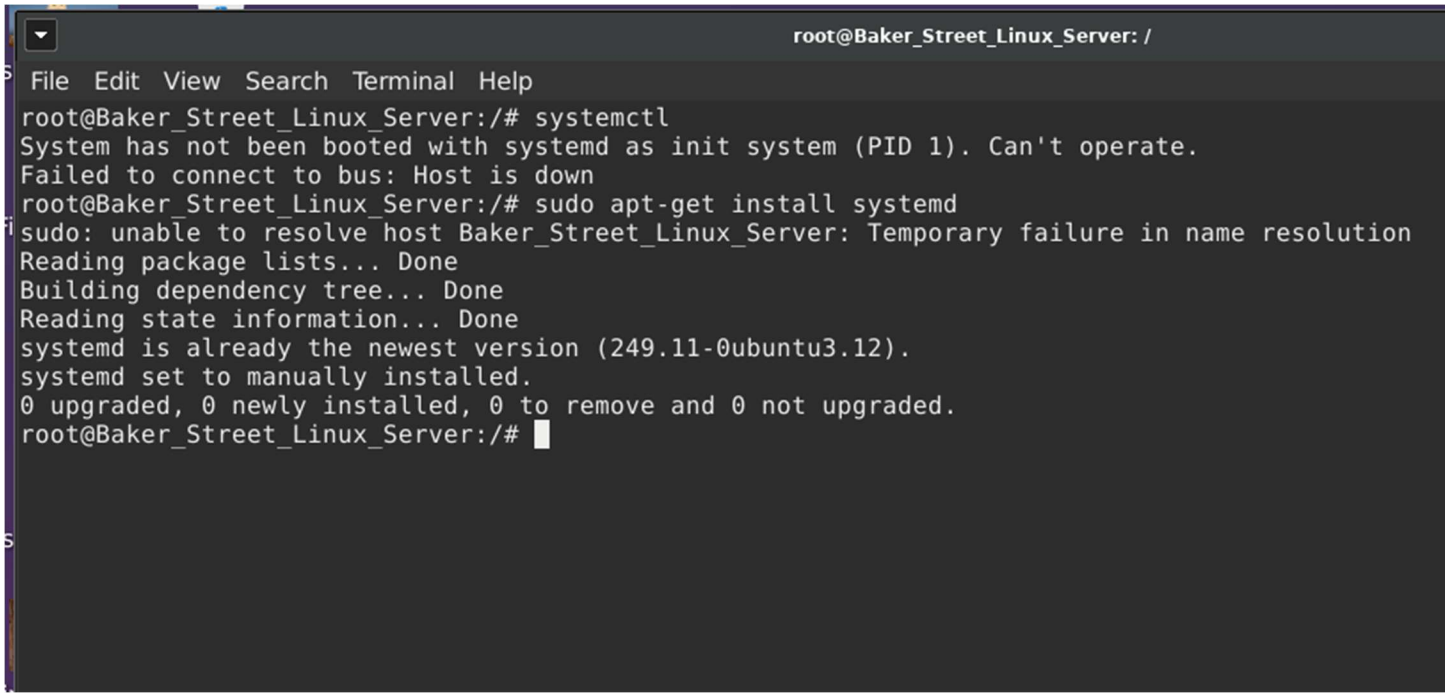
Installing tripwire.



Tripwire installation.

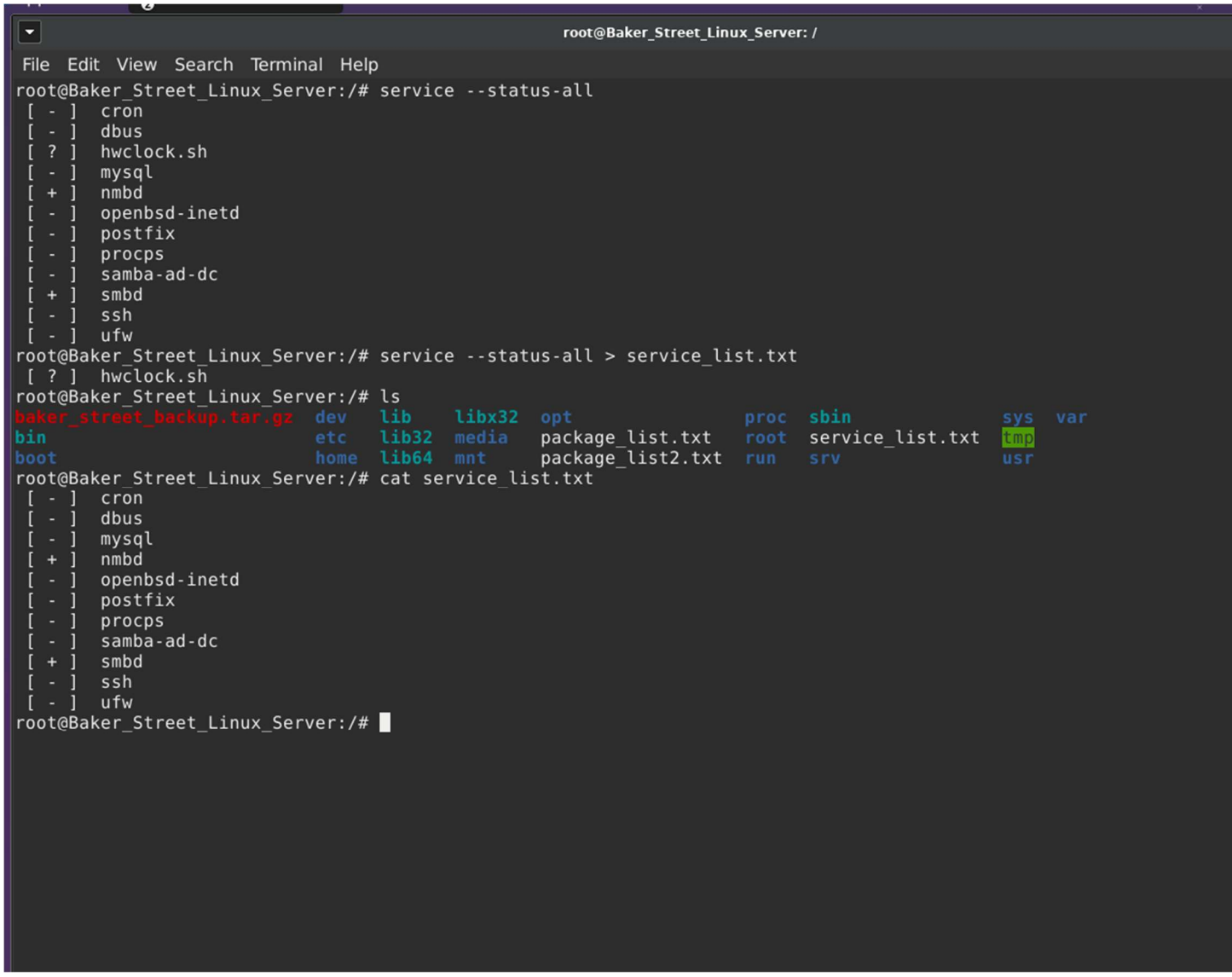


Tripwire installation.

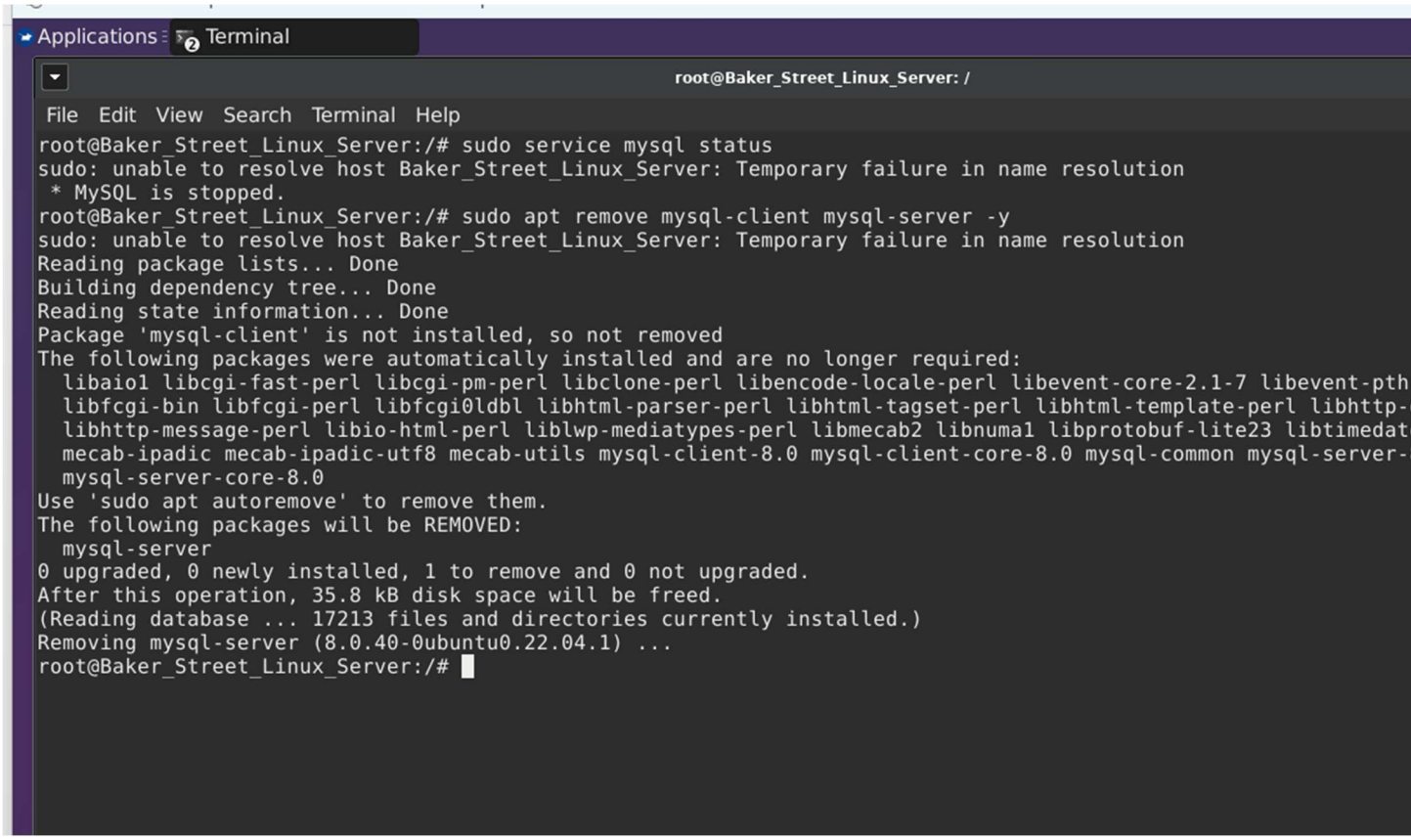


Part 3: Disabling Unnecessary Services

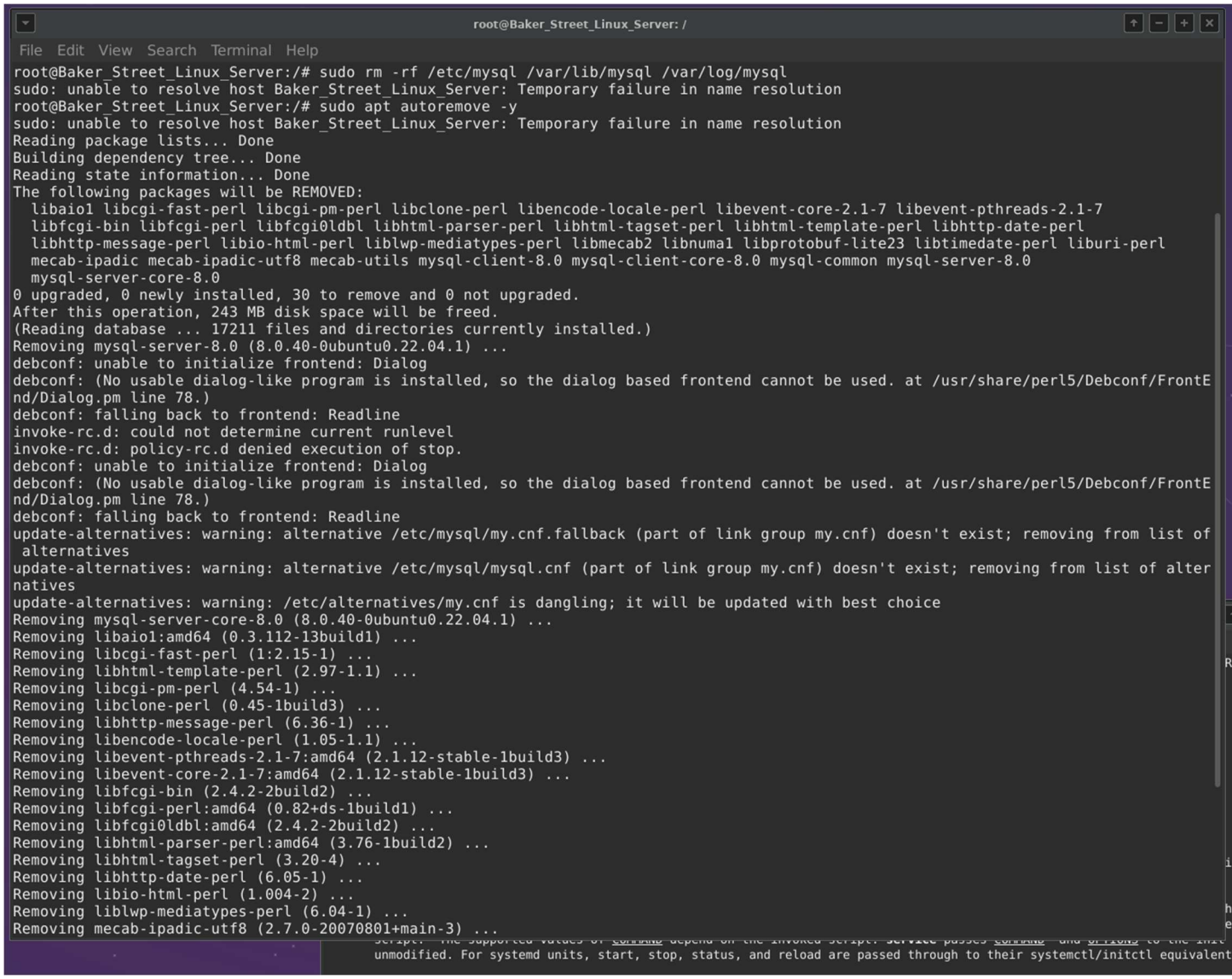
Attempt to run the systemctl command as instructed, but it is not and cannot be installed.



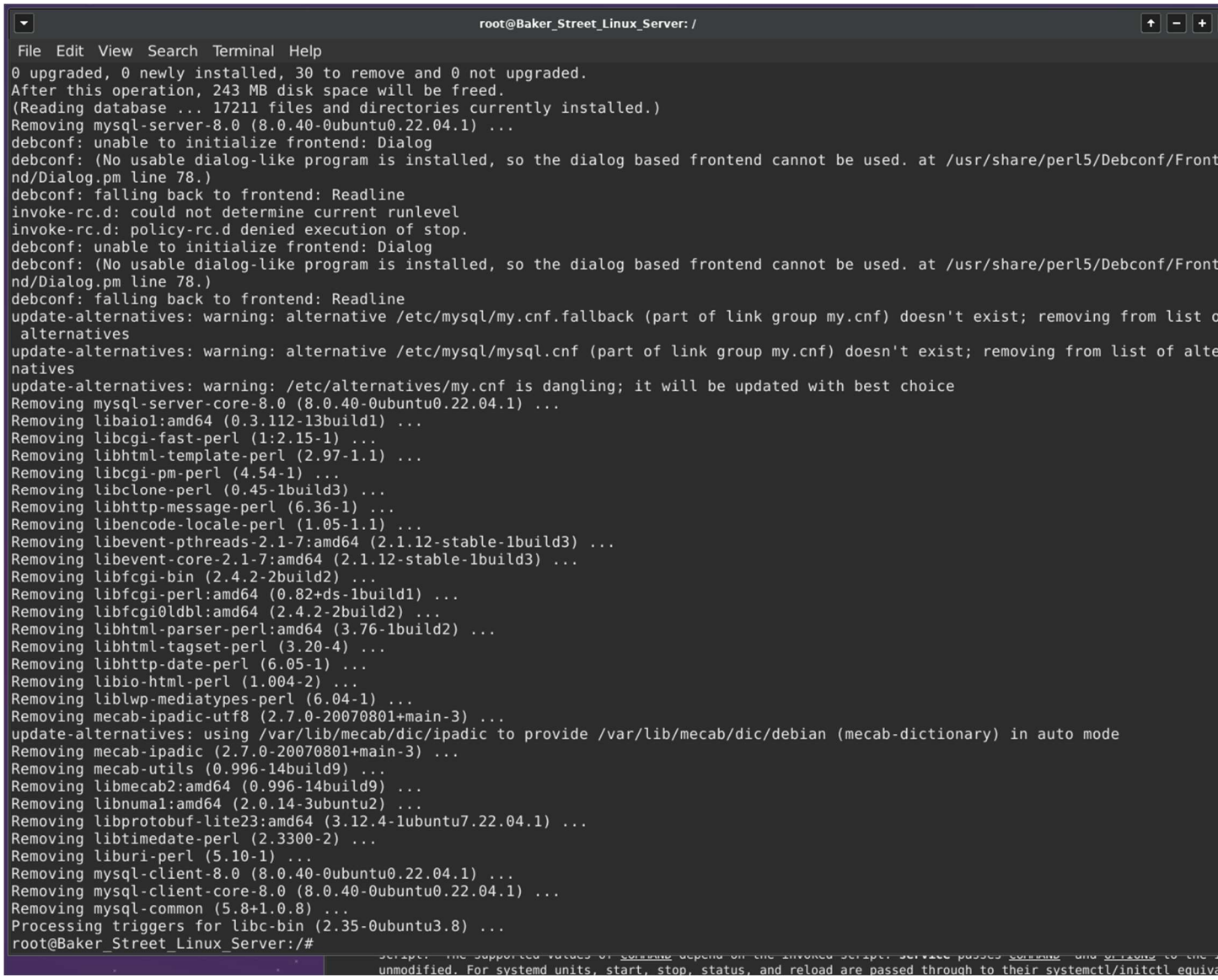
Listing services.



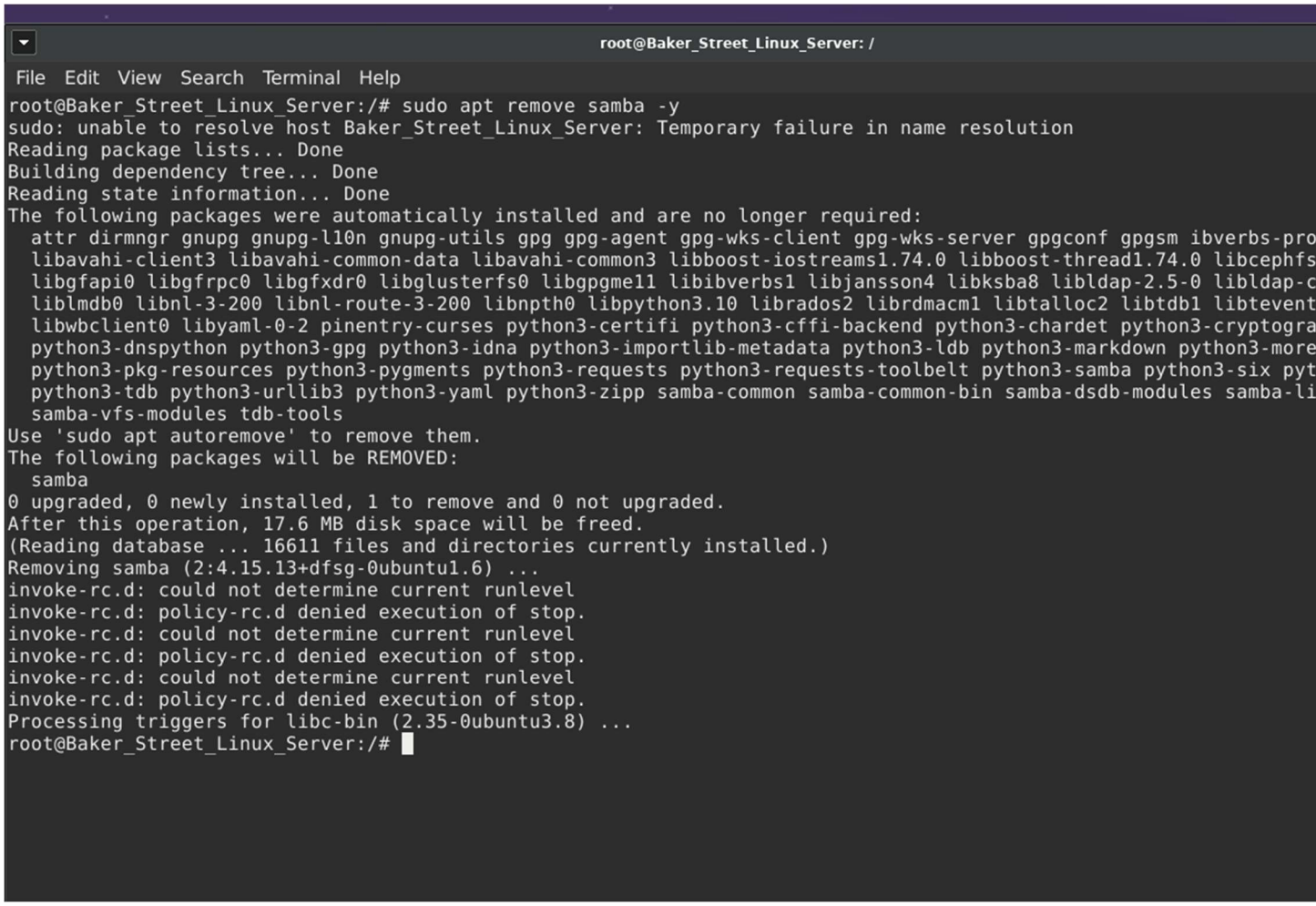
Ensuring mysql is stopped and removed.



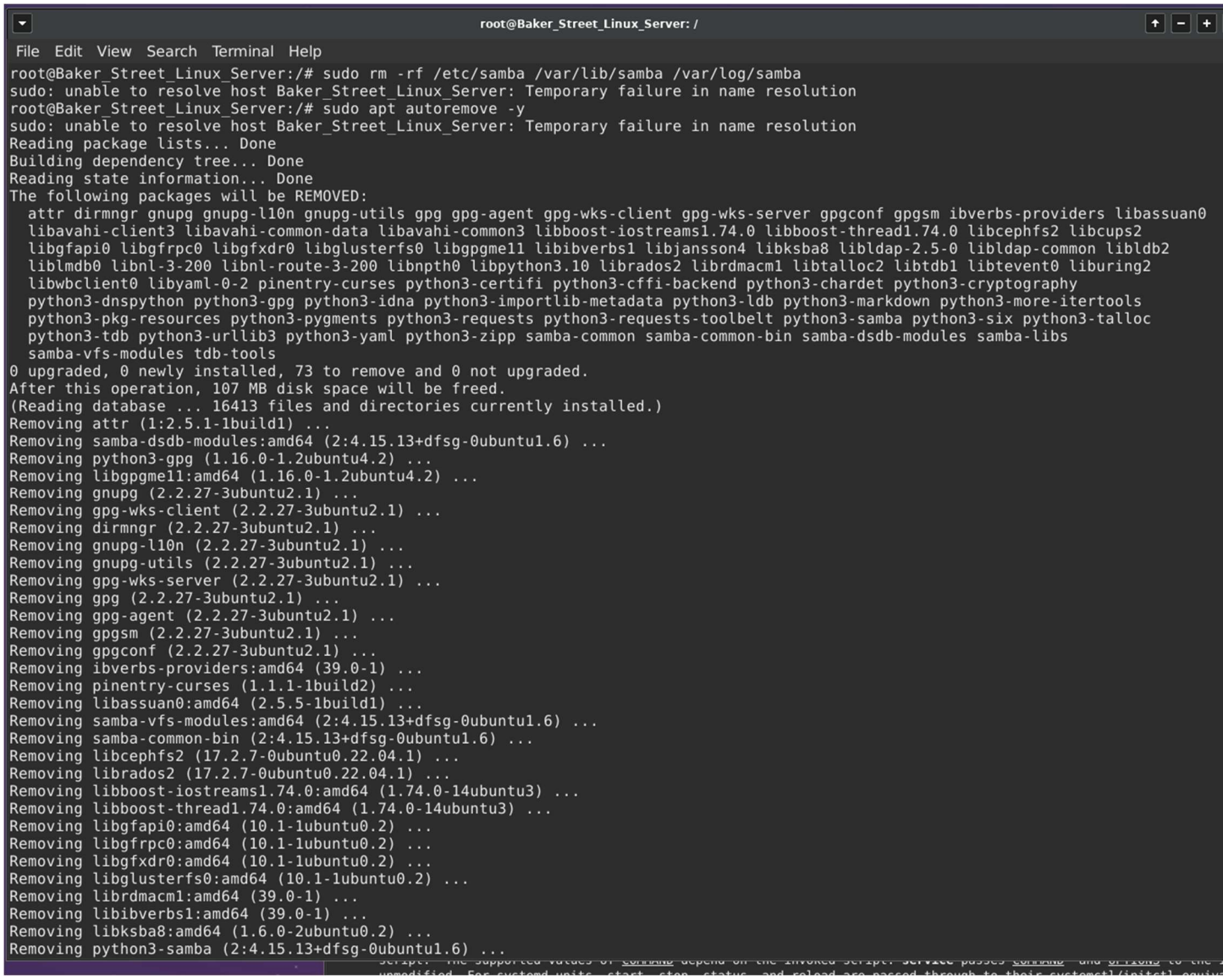
Ensuring mysql is stopped and removed.



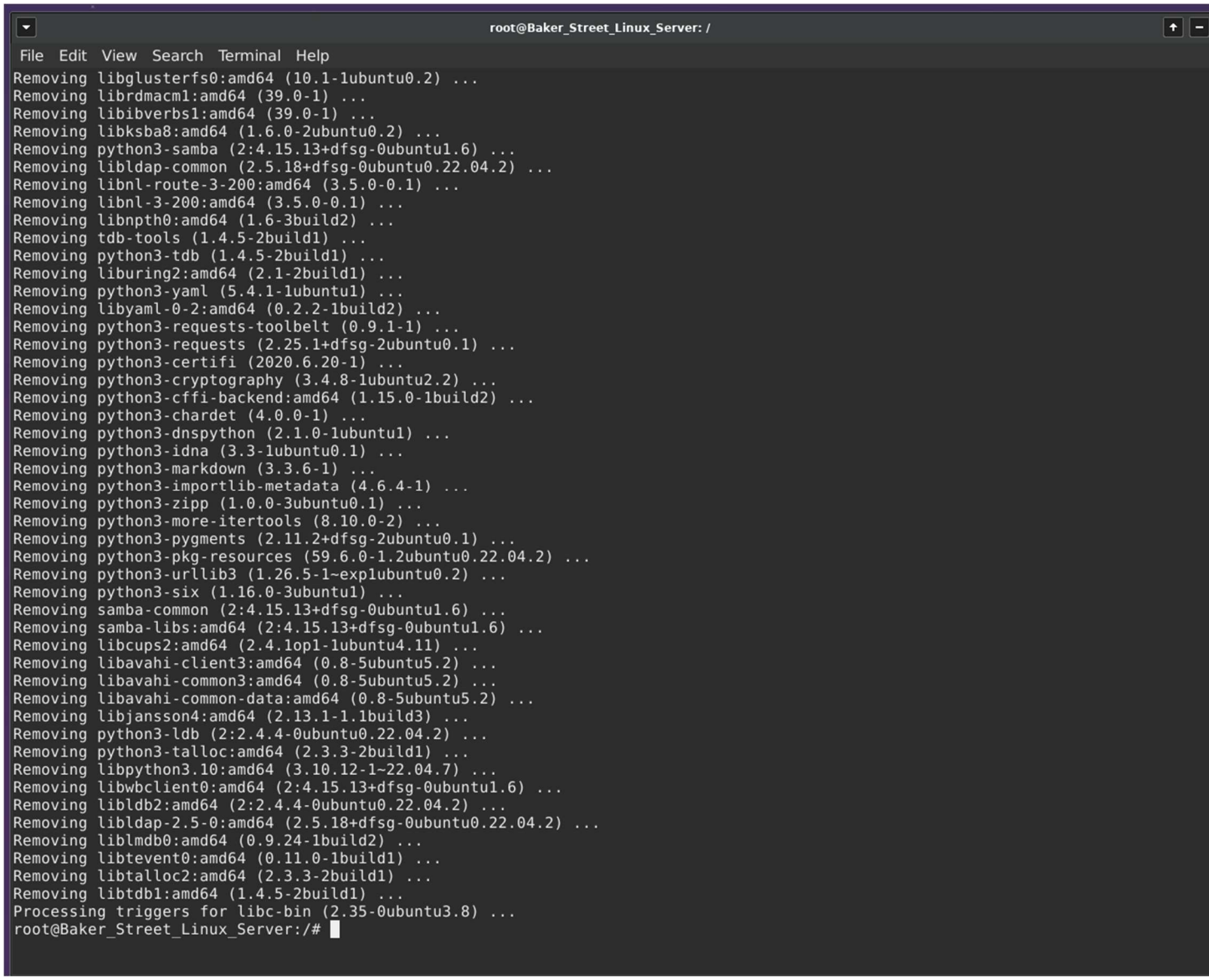
Ensuring mysql is stopped and removed.



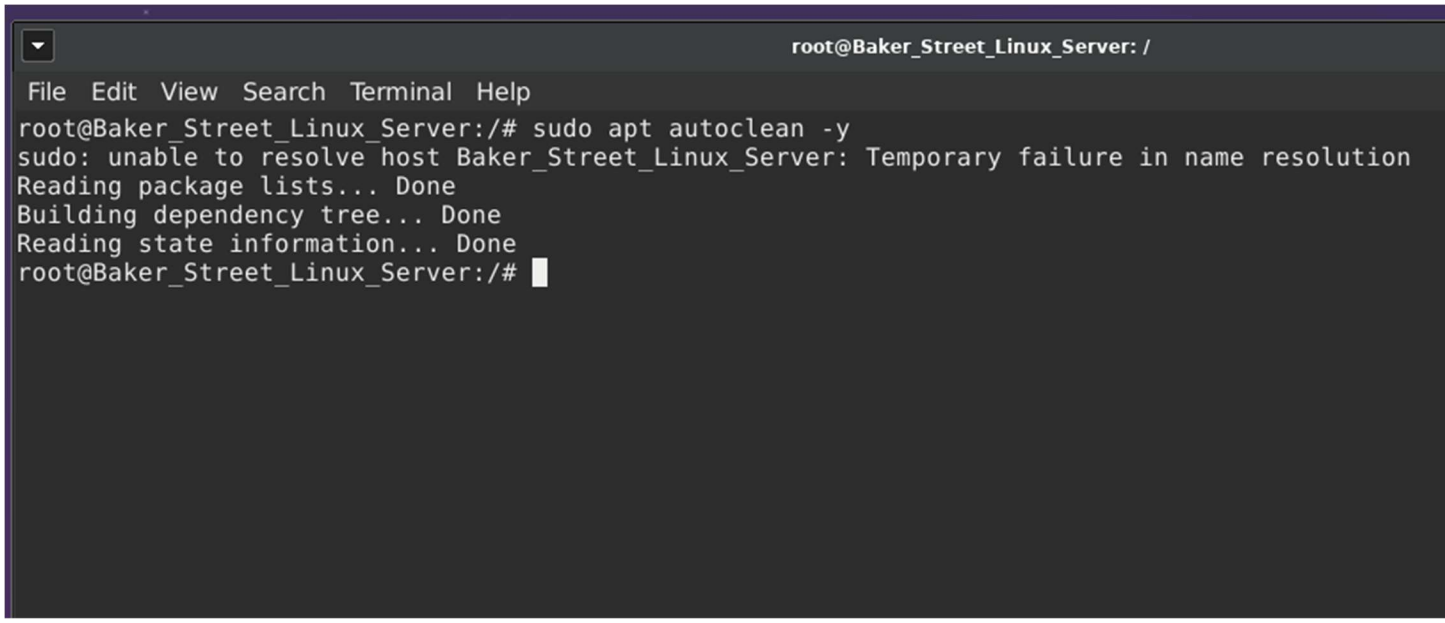
Ensuring samba is stopped and removed.



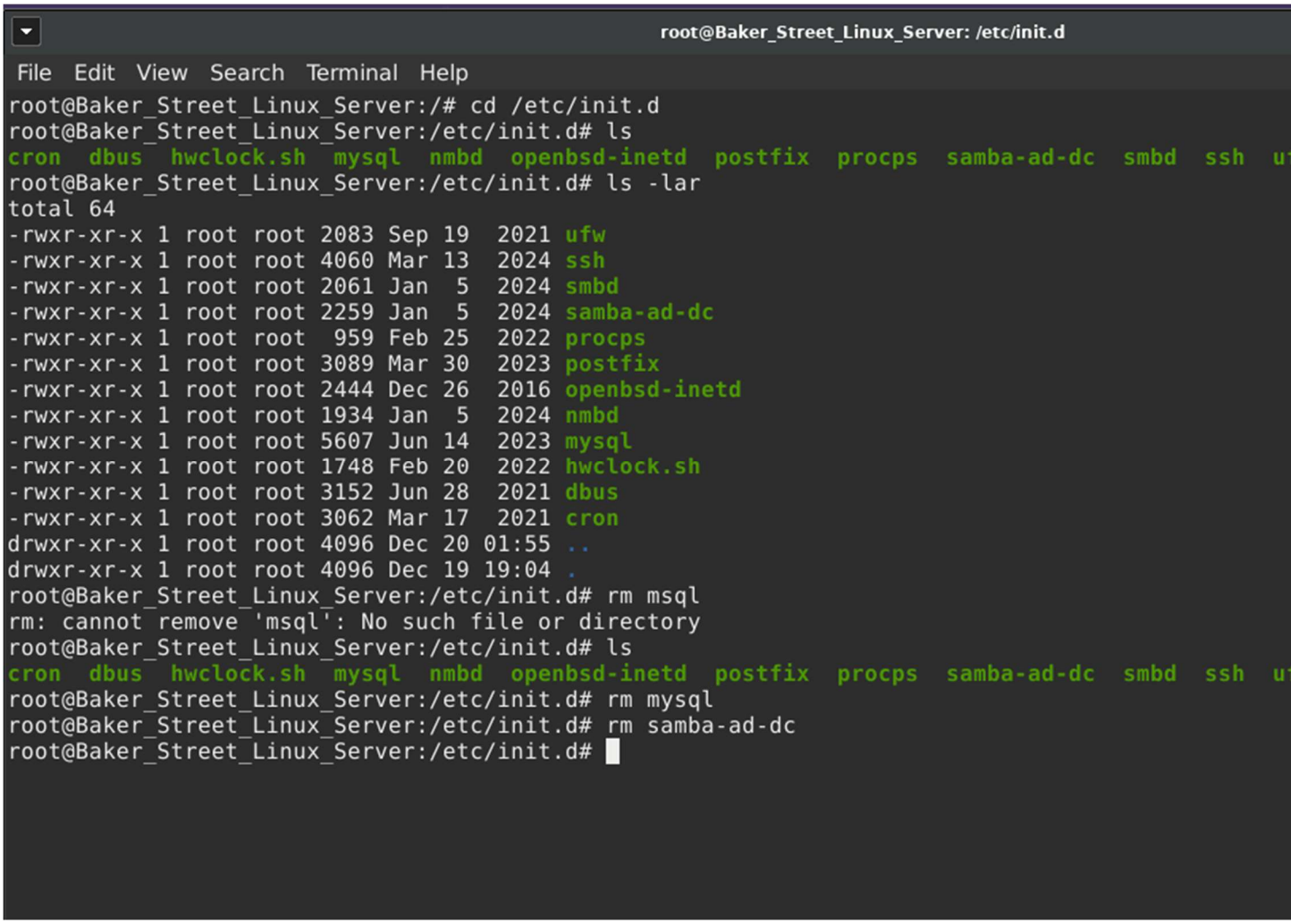
Ensuring samba is stopped and removed.



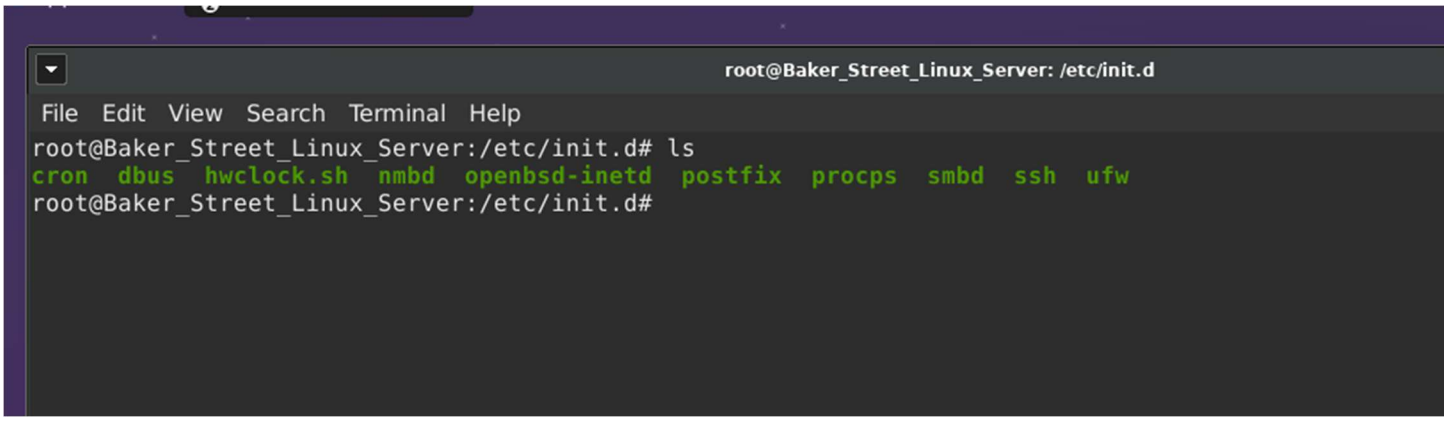
Ensuring samba is stopped and removed.



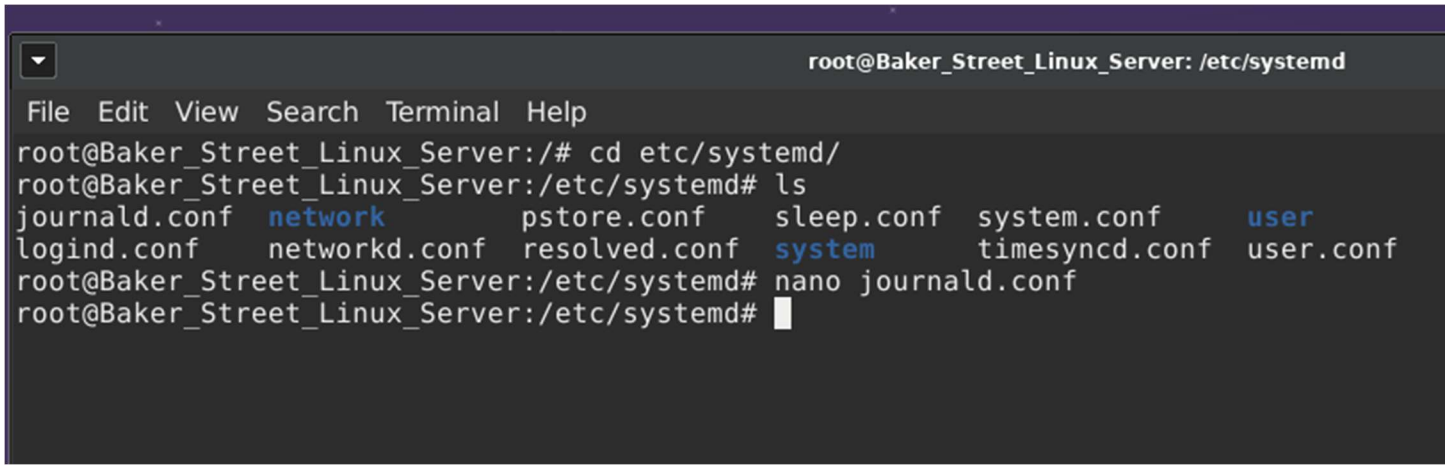
Running autoclean.



Manually removing mysql and samba.

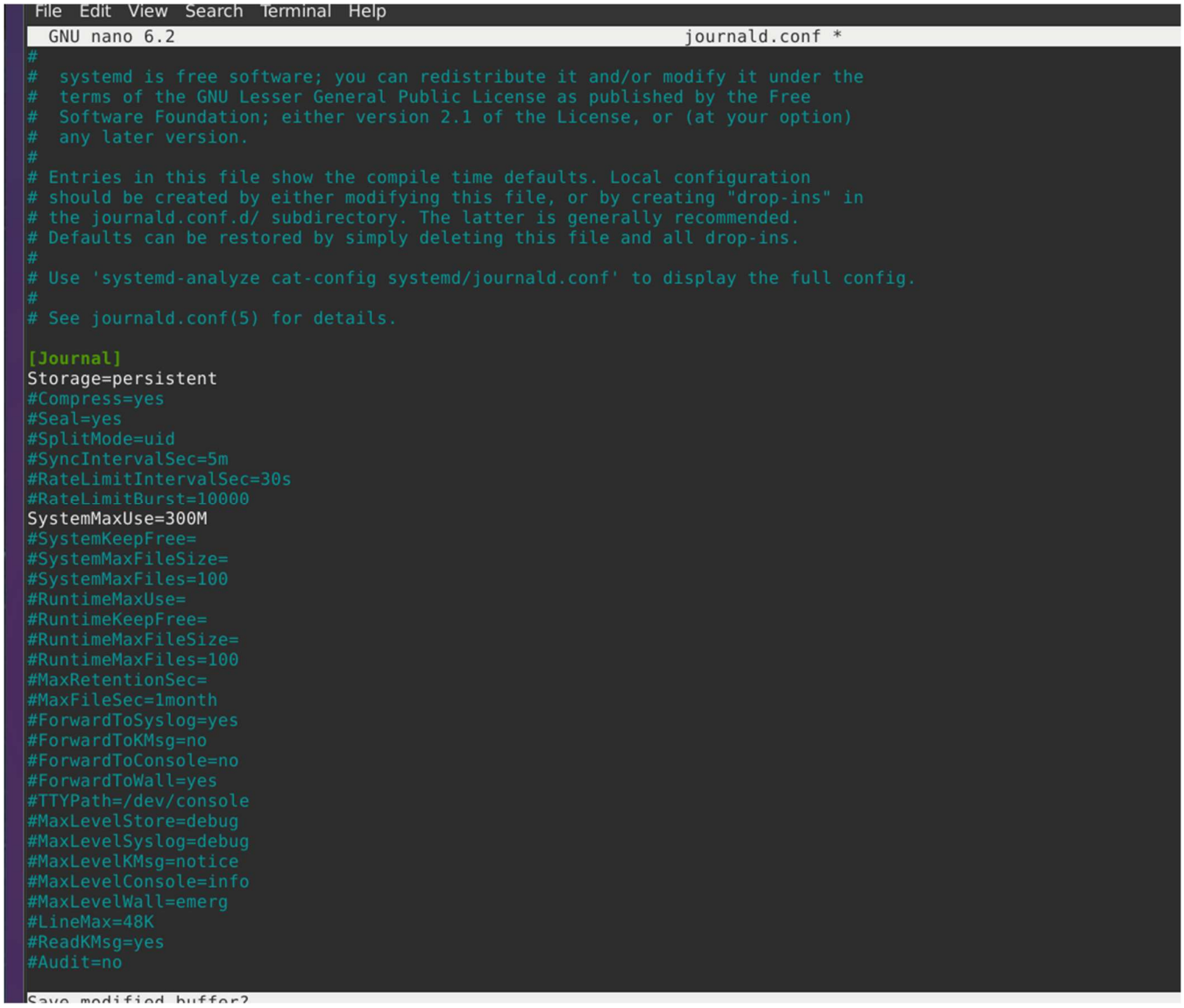


Confirming mysql and samba removed.

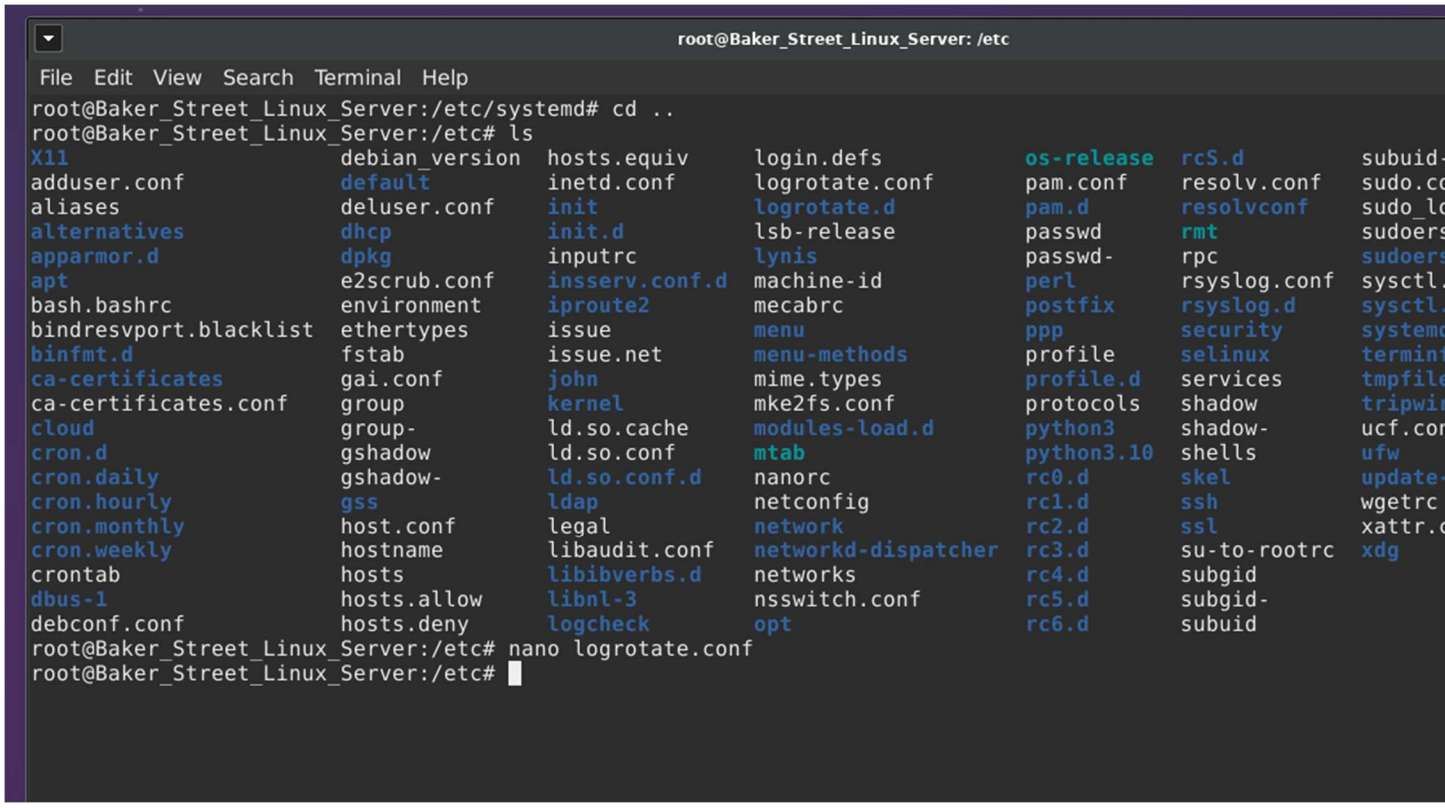


Part 4: Enabling and Configuring Logging

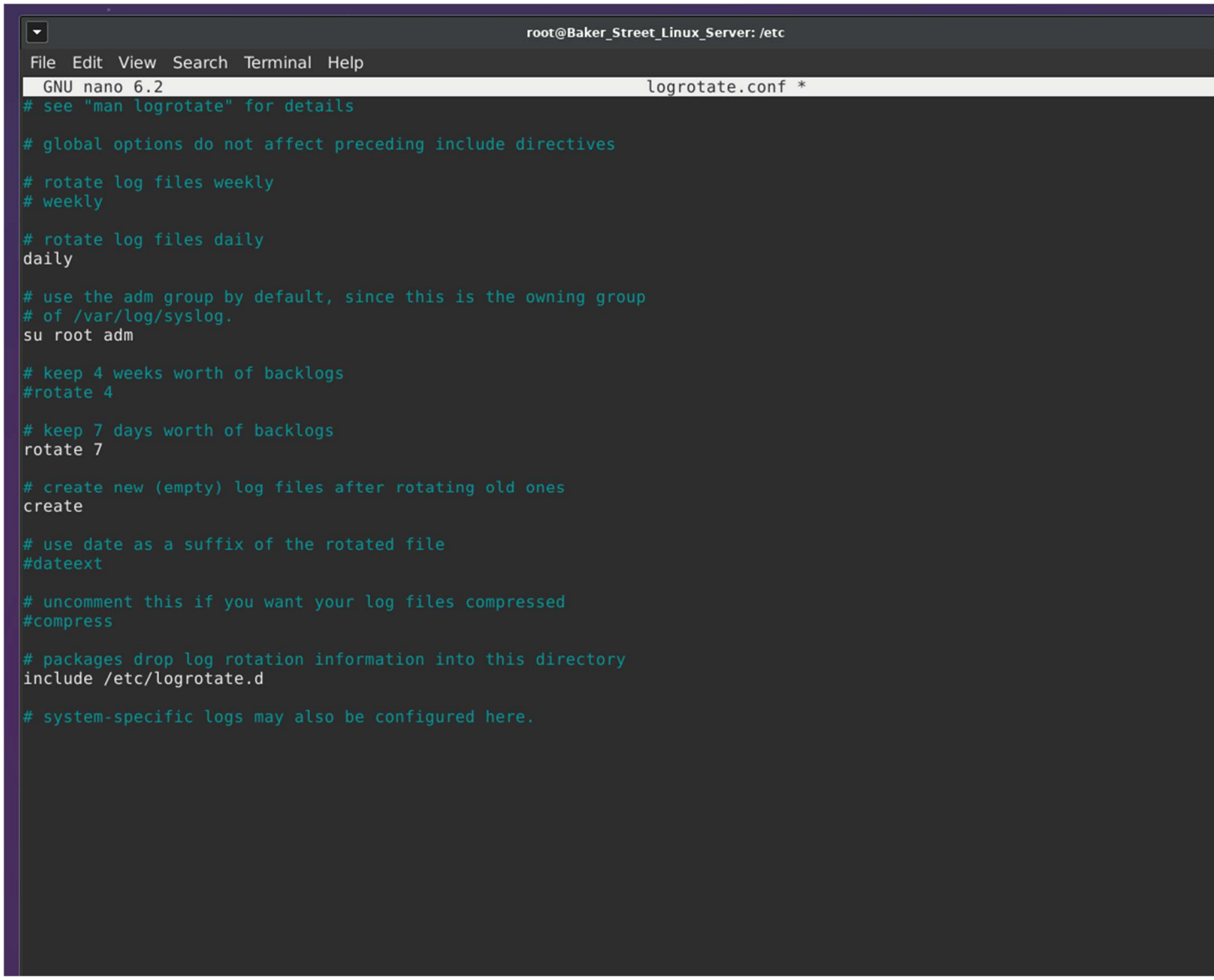
Access journald.conf file to edit in editor.



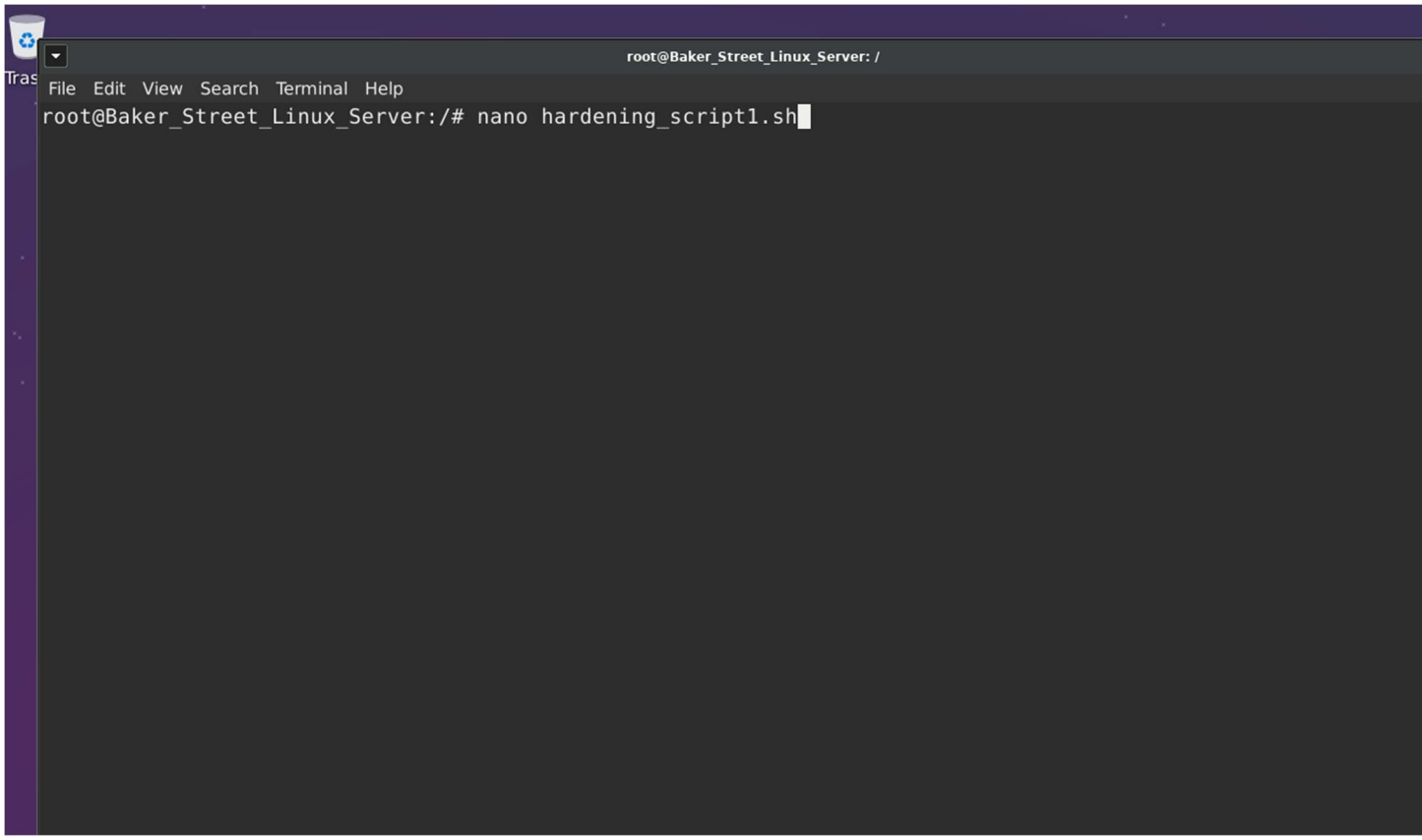
Editing journald.conf file.



Editing journald.conf file.



Editing journald.conf file to configure and check logging.



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

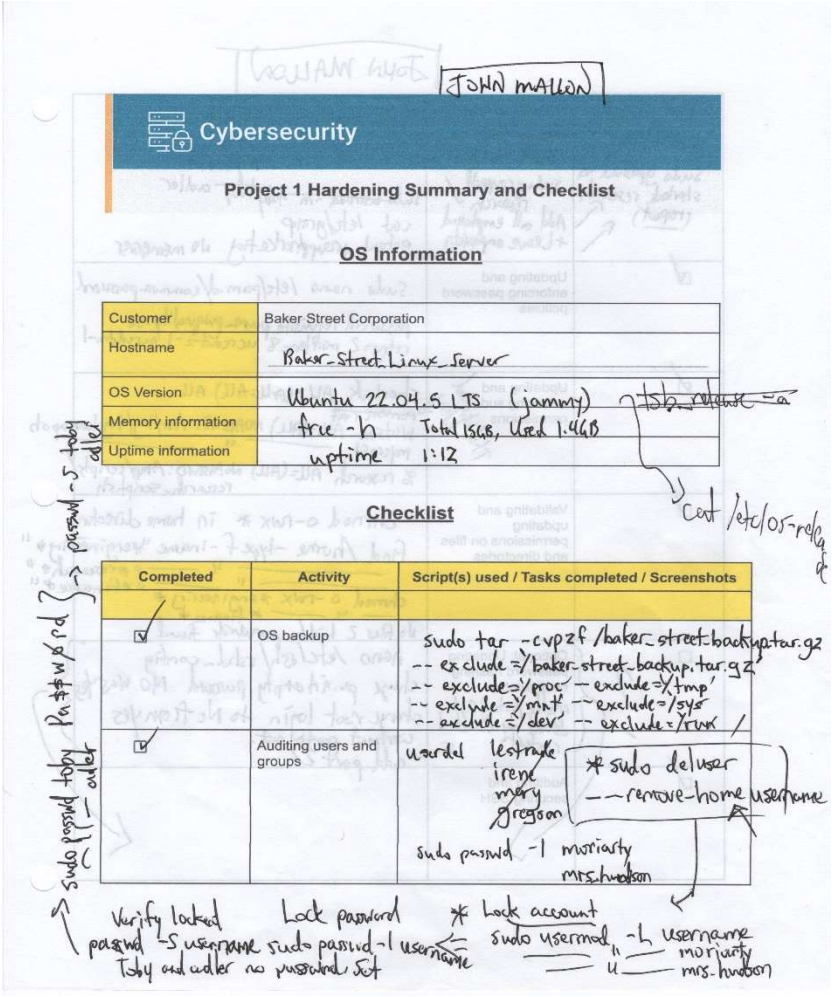
```
#!/bin/bash

# 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)



JOHN MALLON

Cybersecurity

Project 1 Hardening Summary and Checklist

OS Information

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

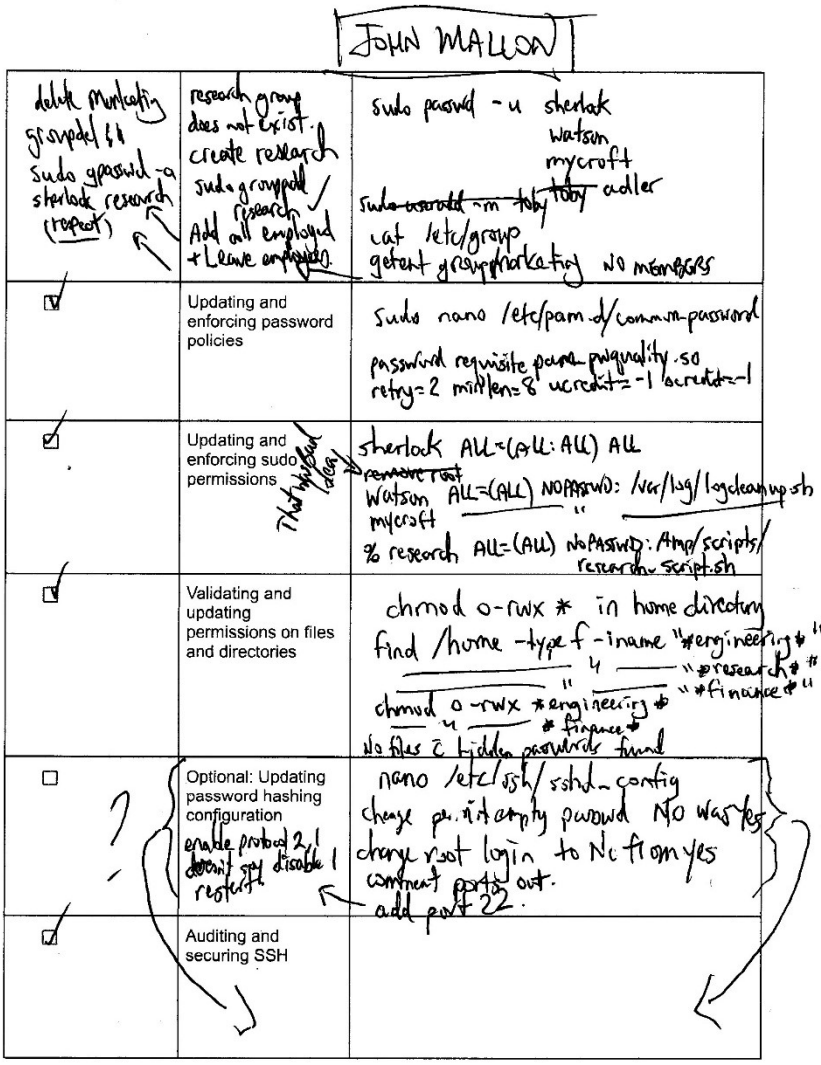
Checklist

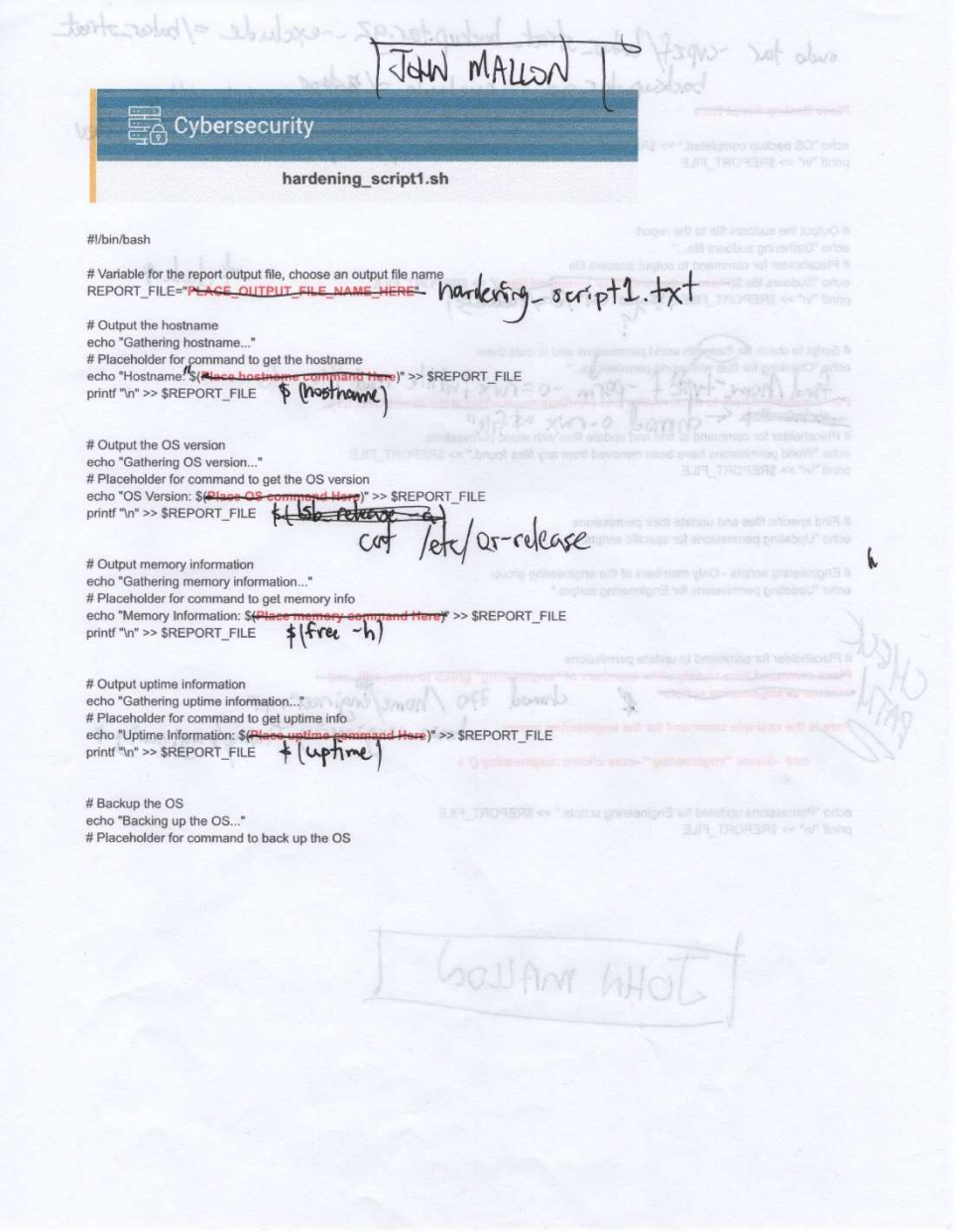
Completed	Activity	Script(s) used / Tasks completed / Screenshots
☑	OS backup	sudo tar -cvpzf /baker_street_backup.tar.gz --exclude=/baker_street_backup.tar.gz --exclude=/proc --exclude=/tmp --exclude=/mnt --exclude=/sys --exclude=/dev --exclude=/run /
☑	Auditing users and groups	userdel lestrade irene mary gregson; * sudo deluser --remove-home username; sudo passwd -l moriarty mrs.hudson

Verify locked passwd -S username Tshy and adler no password set

Lock password sudo passwd -l username

* Lock account sudo usermod -L username moriarty mrs.hudson


JOHN MALLON
delete marketing group(s) && sudo gpasswd -a sherlock research (repeat)
research group does not exist. create research sudo groupadd research
Add all employed + Leave employees.
sudo passwd -u sherlock watson mycroft toby adler
cat /etc/group
getent group marketing no managers
Updating and enforcing password policies
sudo nano /etc/pam.d/common-password
password requisite pam_pwquality.so retry=2 minlen=8 ucredit=-1 dcredit=-1
Updating and enforcing sudo permissions
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
Validating and updating permissions on files and directories
chmod o-rwx * in home directory
find /home -type f -iname "*engineering*" "*research*" "*finance*"
chmod o-rwx *engineering* *research* *finance*
No files & hidden passwords found
Optional: Updating password hashing configuration
enable protocol 2,1 doesn't say disable 1
restart
nano /etc/ssh/sshd_config
change permit empty passwd NO was yes
change root login to No from yes
comment ports out.
add port 22.
Auditing and securing SSH



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"

# 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

# 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

# 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

# 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

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

sudo tar -cvpzf /baker_street_backup.tar.gz --exclude=/baker_street_backup.tar.gz --exclude=/proc --exclude=/tmp --exclude=/mnt --exclude=/sys --exclude=/dev --exclude=/run /

~~Place Backup Script Here~~

```
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)

# 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
~~Place command here to remove all world permissions, starting at the /home directory~~
~~echo "$file"~~ chmod o-rwx "$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
~~Place command here to only allow members of "engineering" group to view, edit, and execute all engineering scripts~~
chmod 770 /home/engineer.*
Here is the example command for the engineering group:
chown :engineering /home/*engineering*
    find -iname "*engineering*" -exec chown :engineering {} +

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

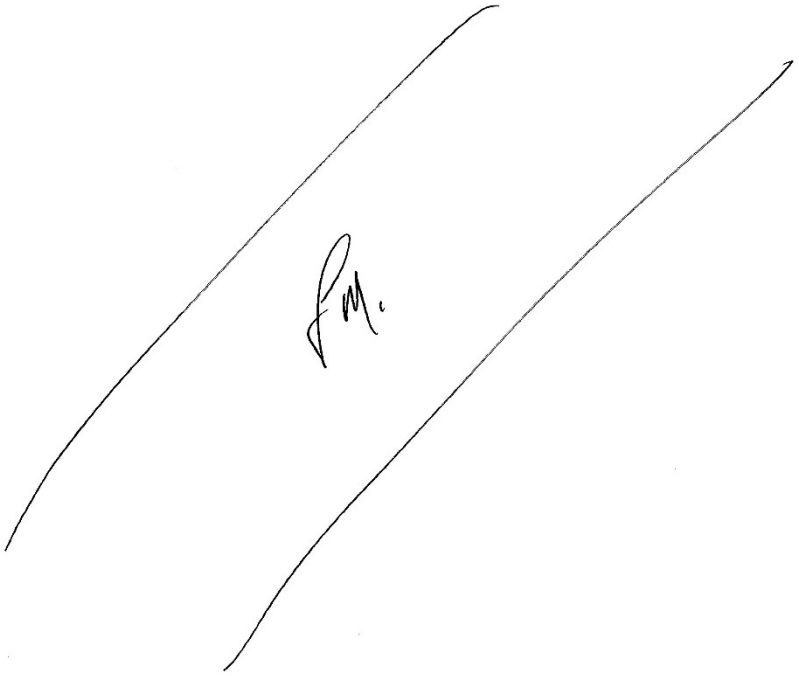
check $

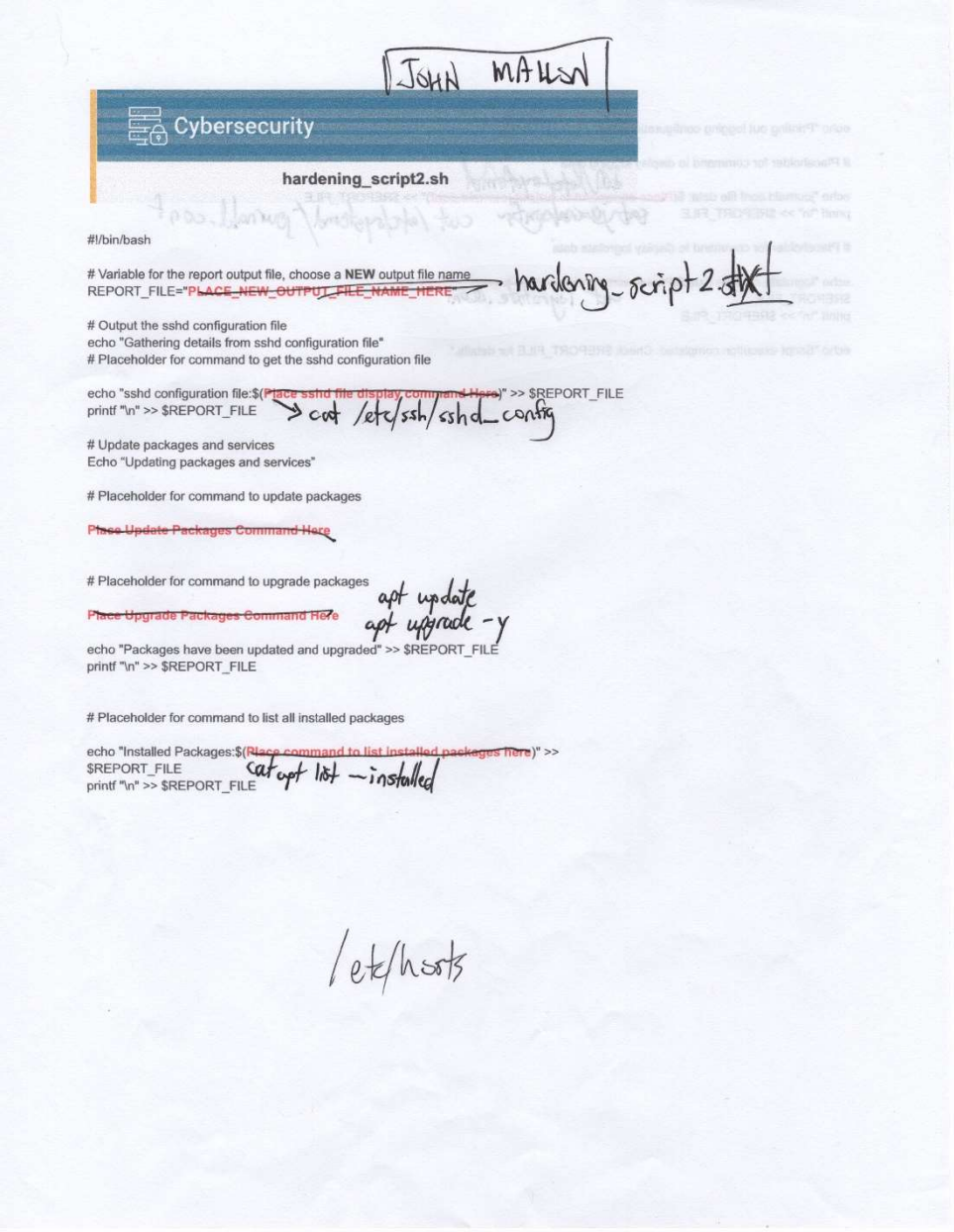
CHECK PATH

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."
```





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"

# 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

# 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

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
printf "\n" >> $REPORT_FILE
```

hardening_script2.txt

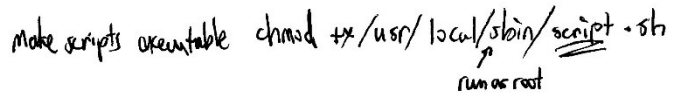
cat /etc/ssh/sshd_config

apt update
apt upgrade -y

cat apt list --installed

/etc/hosts

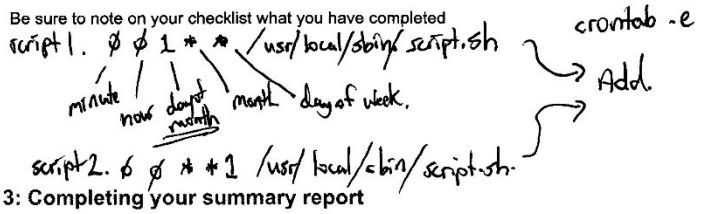
```
echo "Printing out logging configuration data"

# Placeholder for command to display logging data

echo "journald.conf file data: $(Place command to output journald.conf)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Placeholder for command to display logrotate data

echo "logrotate.conf file data:$(Place command to output logrotate.conf)" >>
$REPORT_FILE
printf "\n" >> $REPORT_FILE

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



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



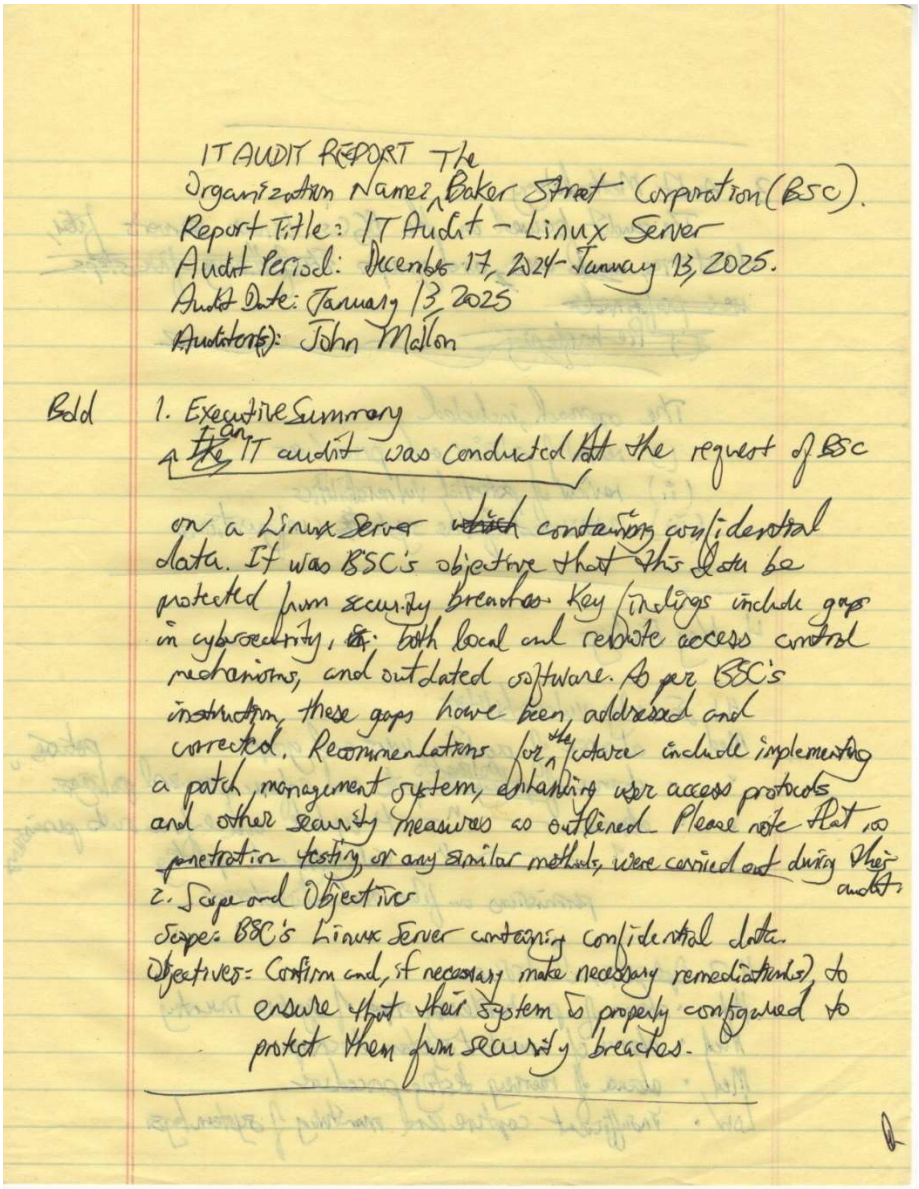
Part 3: Completing your summary report

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.

F: Preliminary Audit Report (rough notes)



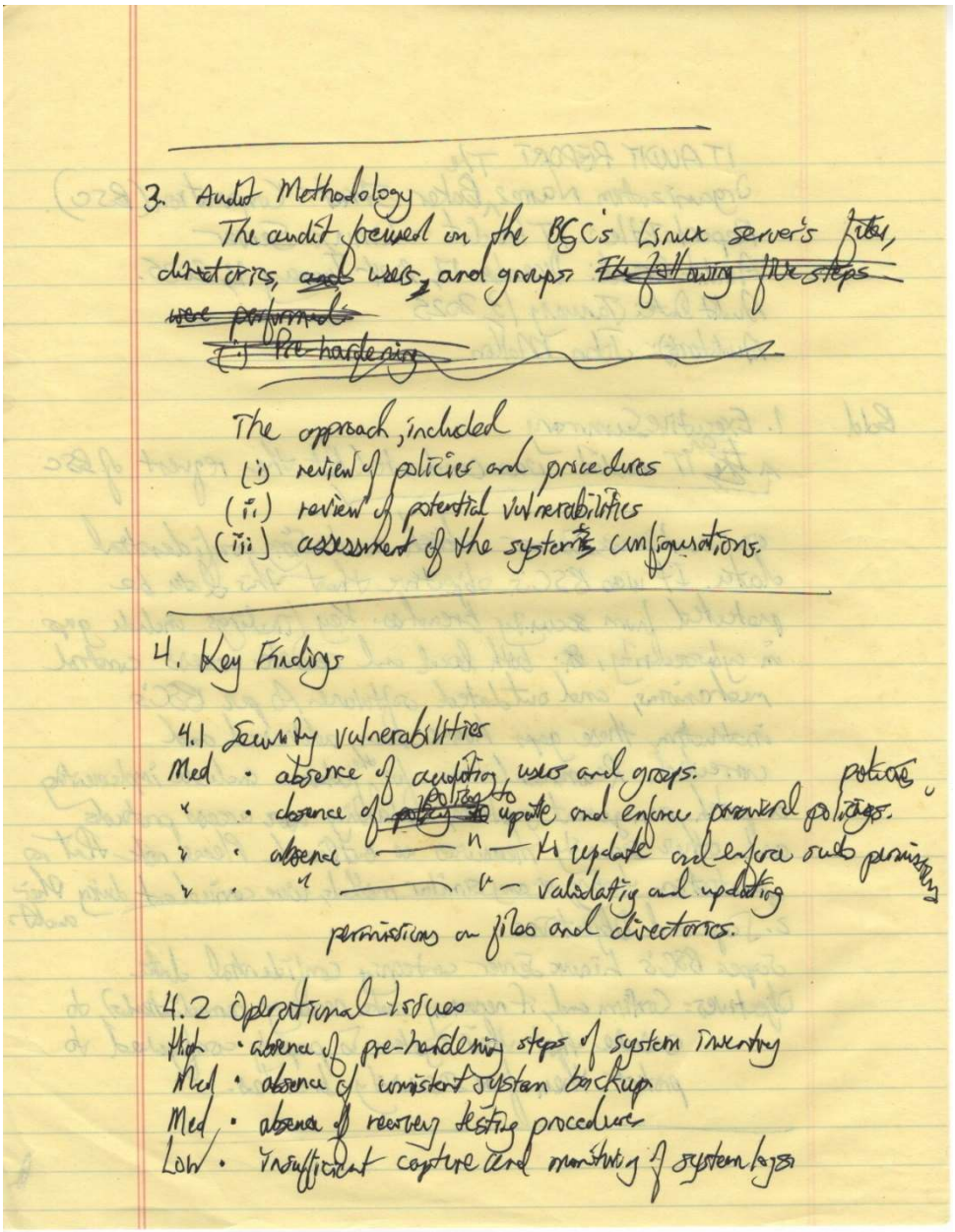
IT AUDIT REPORT The
Organization Name: Baker Street Corporation (BSC).
Report Title: IT Audit – Linux Server
Audit Period: December 17, 2024 - January 13, 2025.
Audit Date: January 13, 2025
Auditor(s): John Mallon

Bold 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 cybersecurity, eg: both local and remote access control mechanisms, and outdated software. As per BSC's instructions, these gaps have been addressed and corrected. Recommendations for future include implementing a patch management system, establishing user access protocols and other security measures as outlined. Please note that no penetration testing or any similar methods were carried out during their audit.

2. Scope and Objective

Scope: BSC's Linux Server containing confidential data.
Objectives: Confirm and, if necessary make necessary remediations, to ensure that their system is properly configured to protect them from security breaches.



3. Audit Methodology

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

~~(i) Pre-hardening~~

The approach included
(i) review of policies and procedures
(ii) review of potential vulnerabilities
(iii) assessment of the system's configurations.

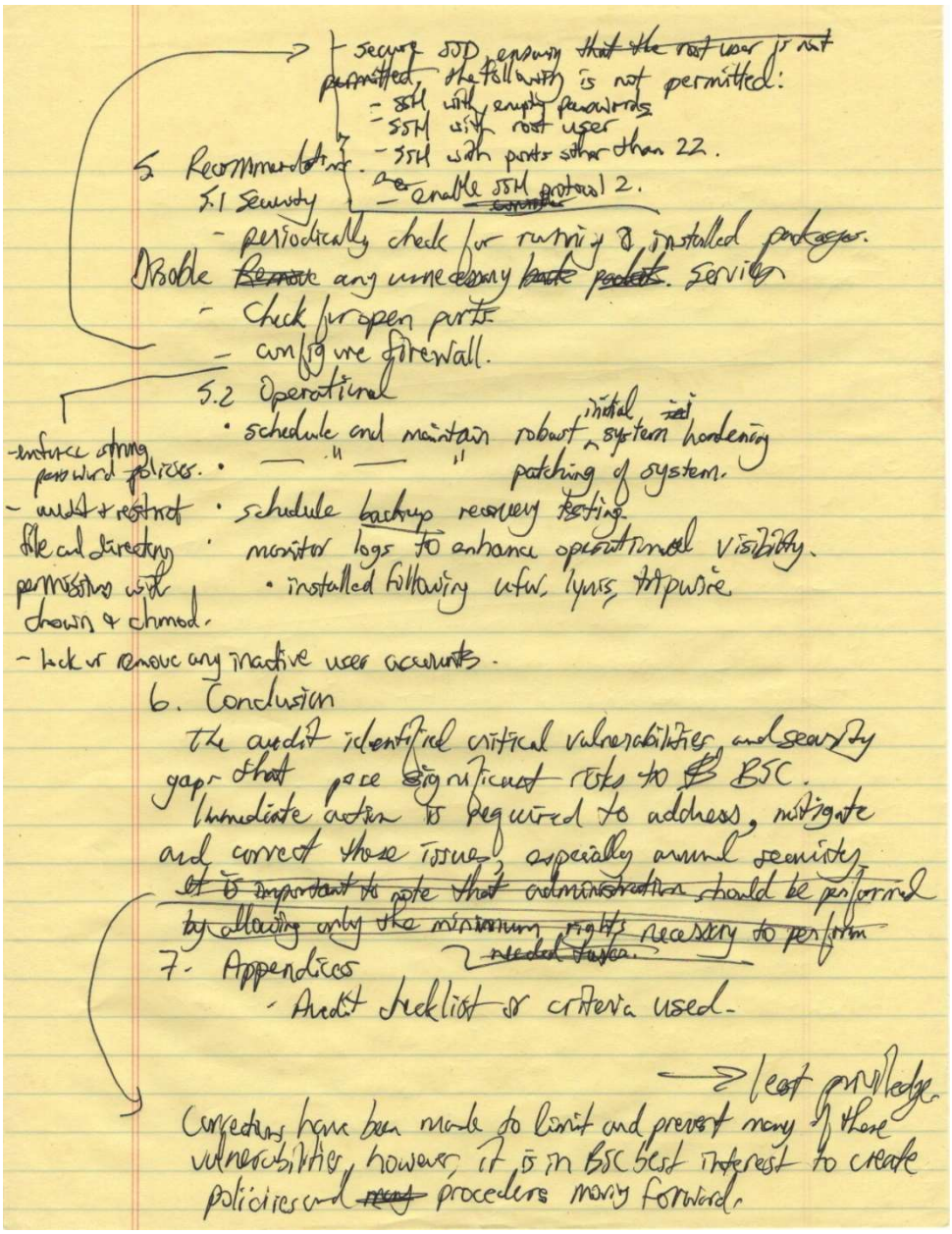
4. Key Findings

4.1 Security vulnerabilities

Med · absence of auditing users and groups.
" · absence of ~~policy to~~ update and enforce password policies.
" · absence — " — to update and enforce sudo permissions
" · " — " — validating and updating permissions on files and directories.

4.2 Operational Issues

High · absence of pre-hardening steps of system inventory
Med · absence of consistent system backups
Med · absence of recovery testing procedures
Low · Insufficient capture and monitoring of system logs


- secure SSD ensuring that the root user is not permitted, the following is not permitted:
- SSH with empty passwords
- SSH with root user
- SSH with ports other than 22.
- enable SSH protocol 2.
5. Recommendations
5.1 Security
- periodically check for running & installed packages.
Disable Remove any unnecessary packages. Services
- Check for open ports
- config we firewall.
5.2 Operational
• schedule and maintain robust initial system hardening
• — " — " patching of system.
-enforce strong password policies.
- audit + restrict file and directory permissions with chown & chmod.
• schedule backup recovery testing.
• monitor logs to enhance operational visibility.
• installed following ufw, lynis, tripwire
- lock or remove any inactive user accounts.
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 those issues, especially annul security
It is important to note that administration should be performed by allowing only the minimum rights necessary to perform needed tasks.
7. Appendices
• Audit checklist or criteria used.
→ least privilege.
Corrections have been made to limit and prevent many of these vulnerabilities, however, it is in BSC best interest to create policies and procedures moving forward.