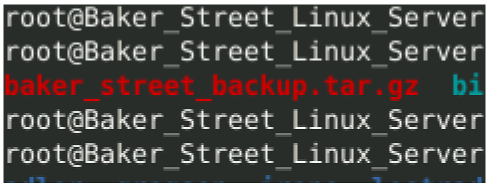
Cybersecurity

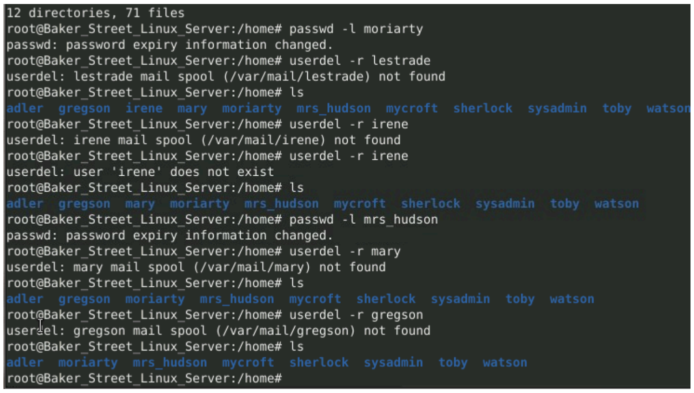
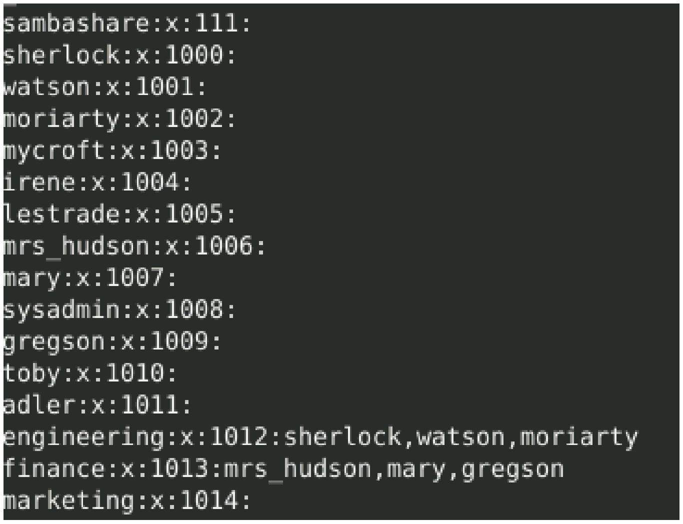
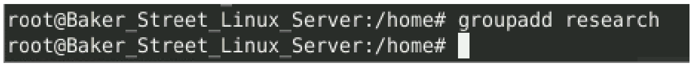
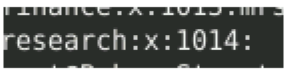
Project 1 Hardening Summary and Checklist

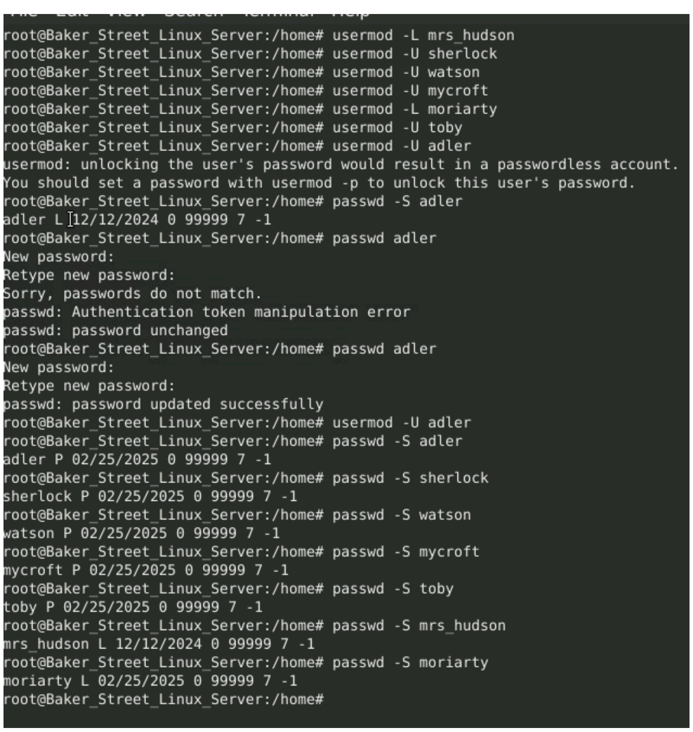
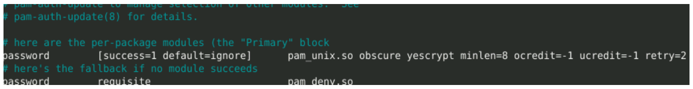
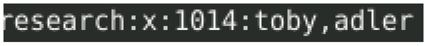
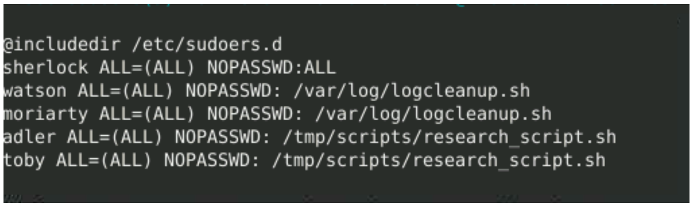
OS Information

Customer	Baker Street Corporation
Hostname	**Baker_Street_Linux_Server**
OS Version	**Unbuntu 22.04.5 LTS**
Memory information	**Total: 15gi, Used:1.5gi, Free: 8.3gi, Shared 200mi, buff/cache: 5.6gi, Available: 13gi**
Uptime information	**2:11:52 up 49 min, 0 users, load average: 1.27, 1.24, 0.91**

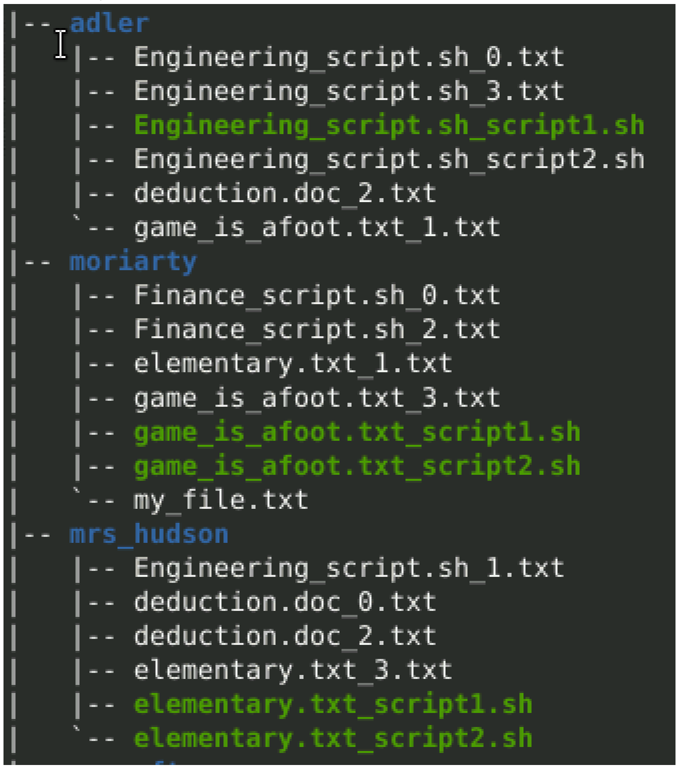
Checklist

Completed	Activity	Script(s) used / Tasks completed / Screenshots
☑	OS backup	This is the command I used to create a backup. *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 /*  root@Baker_Street_Linux_Server root@Baker_Street_Linux_Server baker_street_backup.tar.gz bi root@Baker_Street_Linux_Server root@Baker_Street_Linux_Server

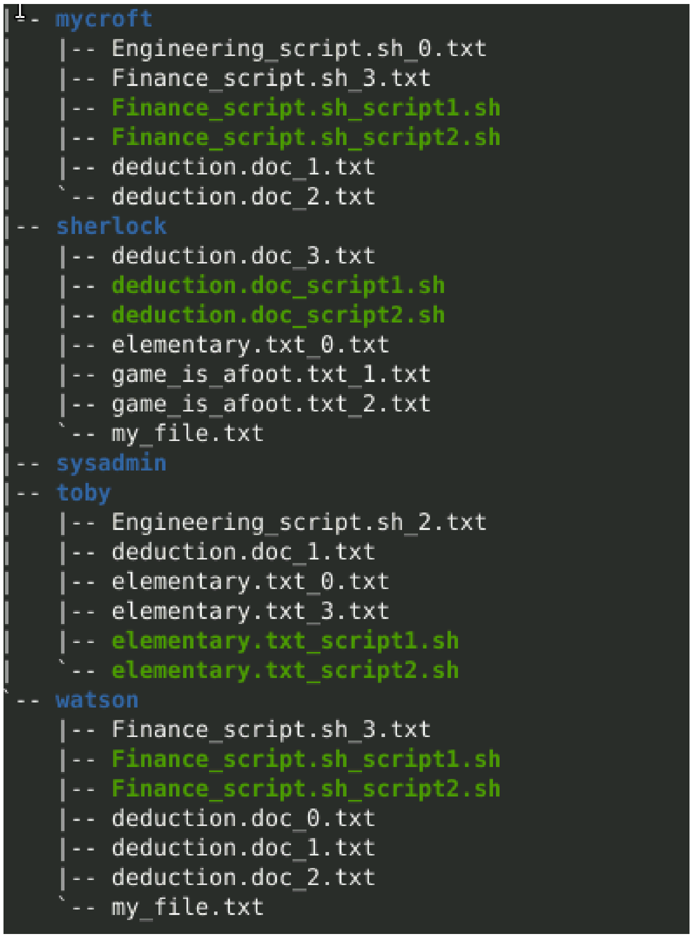
☑	Auditing users and groups	Went through and used the userdel -r username command to delete all the terminated employees and their home directories.  12 directories, 71 files root@Baker_Street_Linux_Server:/home# passwd -l moriarty passwd: password expiry information changed. root@Baker_Street_Linux_Server:/home# userdel -r lestrade userdel: lestrade mail spool (/var/mail/lestrade) not found root@Baker_Street_Linux_Server:/home# ls adler gregson irene mary moriarty mrs_hudson mycroft sherlock sysadmin toby watson root@Baker_Street_Linux_Server:/home# userdel -r irene userdel: irene mail spool (/var/mail/irene) not found root@Baker_Street_Linux_Server:/home# userdel -r irene userdel: user 'irene' does not exist root@Baker_Street_Linux_Server:/home# ls adler gregson mary moriarty mrs_hudson mycroft sherlock sysadmin toby watson root@Baker_Street_Linux_Server:/home# passwd -l mrs_hudson passwd: password expiry information changed. root@Baker_Street_Linux_Server:/home# userdel -r mary userdel: mary mail spool (/var/mail/mary) not found root@Baker_Street_Linux_Server:/home# ls adler gregson moriarty mrs_hudson mycroft sherlock sysadmin toby watson root@Baker_Street_Linux_Server:/home# userdel -r gregson userdel: gregson mail spool (/var/mail/gregson) not found root@Baker_Street_Linux_Server:/home# ls adler moriarty mrs_hudson mycroft sherlock sysadmin toby watson root@Baker_Street_Linux_Server:/home# I used the command getent group to see what groups are on the system. I noticed that there was no one in the marketing group so I used the command groupdel marketing. Then I used to command groupadd research to make that group anyway.  sambashare:x:111: sherlock:x:1000: watson:x:1001: moriarty:x:1002: mycroft:x:1003: irene:x:1004: lestrade:x:1005: mrs_hudson:x:1006: mary:x:1007: sysadmin:x:1008: gregson:x:1009: toby:x:1010: adler:x:1011: engineering:x:1012:sherlock,watson,moriarty finance:x:1013:mrs_hudson,mary,gregson marketing:x:1014:  root@Baker_Street_Linux_Server:/home# groupadd research root@Baker_Street_Linux_Server:/home#  research:x:1014: Then I used the usermod -U on sherlock, watson, mycroft and unlocked them. I had to set passwords for toby and adler in order to unlock those accounts. Then I used the command usermod -L on moriarty and mrs_hudson to lock those accounts.

		 root@Baker_Street_Linux_Server:/home# usermod -L mrs_hudson root@Baker_Street_Linux_Server:/home# usermod -U sherlock root@Baker_Street_Linux_Server:/home# usermod -U watson root@Baker_Street_Linux_Server:/home# usermod -U mycroft root@Baker_Street_Linux_Server:/home# usermod -L moriarty root@Baker_Street_Linux_Server:/home# usermod -U toby root@Baker_Street_Linux_Server:/home# usermod -U adler usermod: unlocking the user's password would result in a passwordless account. You should set a password with usermod -p to unlock this user's password. root@Baker_Street_Linux_Server:/home# passwd -S adler adler L 12/12/2024 0 99999 7 -1 root@Baker_Street_Linux_Server:/home# passwd adler New password: Retype new password: Sorry, passwords do not match. passwd: Authentication token manipulation error passwd: password unchanged root@Baker_Street_Linux_Server:/home# passwd adler New password: Retype new password: passwd: password updated successfully root@Baker_Street_Linux_Server:/home# usermod -U adler root@Baker_Street_Linux_Server:/home# passwd -S adler adler P 02/25/2025 0 99999 7 -1 root@Baker_Street_Linux_Server:/home# passwd -S sherlock sherlock P 02/25/2025 0 99999 7 -1 root@Baker_Street_Linux_Server:/home# passwd -S watson watson P 02/25/2025 0 99999 7 -1 root@Baker_Street_Linux_Server:/home# passwd -S mycroft mycroft P 02/25/2025 0 99999 7 -1 root@Baker_Street_Linux_Server:/home# passwd -S toby toby P 02/25/2025 0 99999 7 -1 root@Baker_Street_Linux_Server:/home# passwd -S mrs_hudson mrs_hudson L 12/12/2024 0 99999 7 -1 root@Baker_Street_Linux_Server:/home# passwd -S moriarty moriarty L 02/25/2025 0 99999 7 -1 root@Baker_Street_Linux_Server:/home#
☑	Updating and enforcing password policies	I opened nano /etc/pam.d/common-password to edit the password permissions. According to the Activty guide there wasn't a password requisite pam_pwquaity.so. I did some research and everything I found told me to add it to the pam_unix.so line. So this is what I added.  # 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 minlen=8 ocredit=-1 ucredit=-1 retry=2 # here's the fallback if no module succeeds password requisite pam_deny.so
□	Updating and enforcing sudo permissions	I did notice that Toby and adler had no group so in order to get more practice with visudo, and permissions I added them to the research group. Then added permissions for the /tmp/scripts/research group.  research:x:1014:toby,adler  @includedir /etc/sudoers.d sherlock ALL=(ALL) NOPASSWD:ALL watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh moriarty ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh adler ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh toby ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh

<table>
<tr>
<td>□</td>
<td>Validating and updating permissions on files and directories</td>
<td>This one took me a while to figure out. BUT I think I got it.
First I checked who was in what group. Then I used the tree command to see what was in each person’s directory

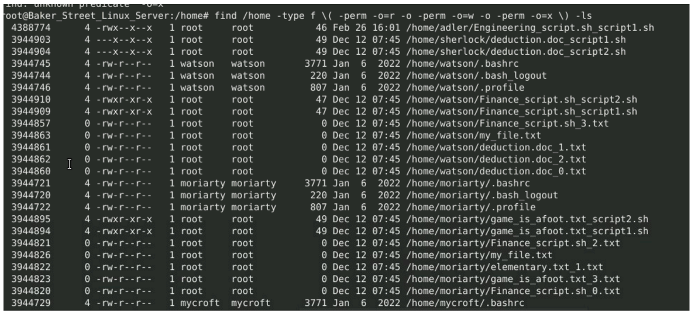


```
|-- adler
|   |-- Engineering_script.sh_0.txt
|   |-- Engineering_script.sh_3.txt
|   |-- Engineering_script.sh_script1.sh
|   |-- Engineering_script.sh_script2.sh
|   |-- deduction.doc_2.txt
|   `-- game_is_afoot.txt_1.txt
|-- moriarty
|   |-- Finance_script.sh_0.txt
|   |-- Finance_script.sh_2.txt
|   |-- elementary.txt_1.txt
|   |-- game_is_afoot.txt_3.txt
|   |-- game_is_afoot.txt_script1.sh
|   |-- game_is_afoot.txt_script2.sh
|   `-- my_file.txt
|-- mrs_hudson
|   |-- Engineering_script.sh_1.txt
|   |-- deduction.doc_0.txt
|   |-- deduction.doc_2.txt
|   |-- elementary.txt_3.txt
|   |-- elementary.txt_script1.sh
|   `-- elementary.txt_script2.sh
```
</td>
</tr>
</table>

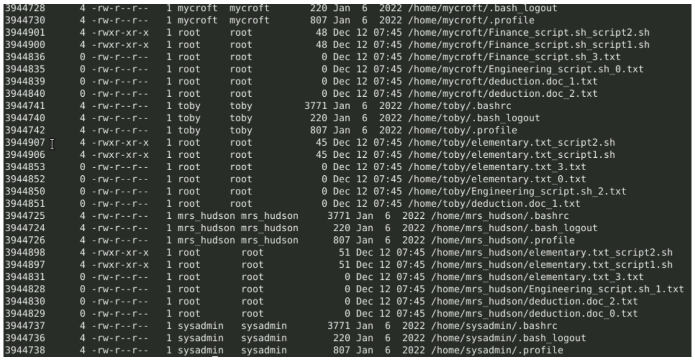


```
|-- mycroft
|   |-- Engineering_script.sh_0.txt
|   |-- Finance_script.sh_3.txt
|   |-- Finance_script.sh_script1.sh
|   |-- Finance_script.sh_script2.sh
|   |-- deduction.doc_1.txt
|   `-- deduction.doc_2.txt
|-- sherlock
|   |-- deduction.doc_3.txt
|   |-- deduction.doc_script1.sh
|   |-- deduction.doc_script2.sh
|   |-- elementary.txt_0.txt
|   |-- game_is_afoot.txt_1.txt
|   |-- game_is_afoot.txt_2.txt
|   `-- my_file.txt
|-- sysadmin
|-- toby
|   |-- Engineering_script.sh_2.txt
|   |-- deduction.doc_1.txt
|   |-- elementary.txt_0.txt
|   |-- elementary.txt_3.txt
|   |-- elementary.txt_script1.sh
|   `-- elementary.txt_script2.sh
`-- watson
    |-- Finance_script.sh_3.txt
    |-- Finance_script.sh_script1.sh
    |-- Finance_script.sh_script2.sh
    |-- deduction.doc_0.txt
    |-- deduction.doc_1.txt
    |-- deduction.doc_2.txt
    `-- my_file.txt
```

Then I used the find command to find all the files with world permissions in the home directory.

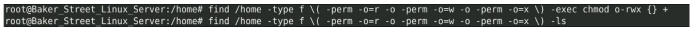


```
ind: unknown predicate '-o=x'
oot@Baker_Street_Linux_Server:/home# find /home -type f \( -perm -o=r -o -perm -o=w -o -perm -o=x \) -ls
 4388774      4 -rwx--x--x   1 root     root           46 Feb 26 16:01 /home/adler/Engineering_script.sh_script1.sh
 3944903      4 ---x--x--x   1 root     root           49 Dec 12 07:45 /home/sherlock/deduction.doc_script1.sh
 3944904      4 ---x--x--x   1 root     root           49 Dec 12 07:45 /home/sherlock/deduction.doc_script2.sh
 3944745      4 -rw-r--r--   1 watson   watson       3771 Jan  6  2022 /home/watson/.bashrc
 3944744      4 -rw-r--r--   1 watson   watson        220 Jan  6  2022 /home/watson/.bash_logout
 3944746      4 -rw-r--r--   1 watson   watson        807 Jan  6  2022 /home/watson/.profile
 3944910      4 -rwxr-xr-x   1 root     root           47 Dec 12 07:45 /home/watson/Finance_script.sh_script2.sh
 3944909      4 -rwxr-xr-x   1 root     root           47 Dec 12 07:45 /home/watson/Finance_script.sh_script1.sh
 3944857      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/watson/Finance_script.sh_3.txt
 3944863      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/watson/my_file.txt
 3944861      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/watson/deduction.doc_1.txt
 3944862      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/watson/deduction.doc_2.txt
 3944860      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/watson/deduction.doc_0.txt
 3944721      4 -rw-r--r--   1 moriarty moriarty     3771 Jan  6  2022 /home/moriarty/.bashrc
 3944720      4 -rw-r--r--   1 moriarty moriarty      220 Jan  6  2022 /home/moriarty/.bash_logout
 3944722      4 -rw-r--r--   1 moriarty moriarty      807 Jan  6  2022 /home/moriarty/.profile
 3944895      4 -rwxr-xr-x   1 root     root           49 Dec 12 07:45 /home/moriarty/game_is_afoot.txt_script2.sh
 3944894      4 -rwxr-xr-x   1 root     root           49 Dec 12 07:45 /home/moriarty/game_is_afoot.txt_script1.sh
 3944821      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/moriarty/Finance_script.sh_2.txt
 3944826      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/moriarty/my_file.txt
 3944822      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/moriarty/elementary.txt_1.txt
 3944823      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/moriarty/game_is_afoot.txt_3.txt
 3944820      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/moriarty/Finance_script.sh_0.txt
 3944729      4 -rw-r--r--   1 mycroft  mycroft      3771 Jan  6  2022 /home/mycroft/.bashrc
```

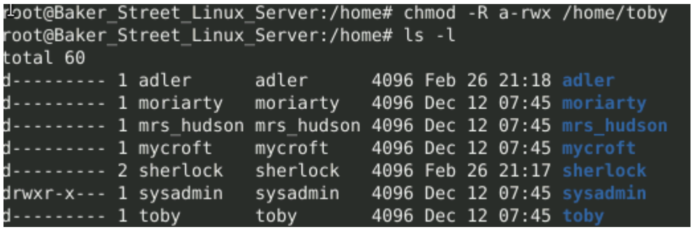


```
3944728      4 -rw-r--r--   1 mycroft  mycroft       220 Jan  6  2022 /home/mycroft/.bash_logout
3944730      4 -rw-r--r--   1 mycroft  mycroft       807 Jan  6  2022 /home/mycroft/.profile
3944901      4 -rwxr-xr-x   1 root     root           48 Dec 12 07:45 /home/mycroft/Finance_script.sh_script2.sh
3944900      4 -rwxr-xr-x   1 root     root           48 Dec 12 07:45 /home/mycroft/Finance_script.sh_script1.sh
3944836      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/mycroft/Finance_script.sh_3.txt
3944835      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/mycroft/Engineering_script.sh_0.txt
3944839      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/mycroft/deduction.doc_1.txt
3944840      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/mycroft/deduction.doc_2.txt
3944741      4 -rw-r--r--   1 toby     toby         3771 Jan  6  2022 /home/toby/.bashrc
3944740      4 -rw-r--r--   1 toby     toby          220 Jan  6  2022 /home/toby/.bash_logout
3944742      4 -rw-r--r--   1 toby     toby          807 Jan  6  2022 /home/toby/.profile
3944907      4 -rwxr-xr-x   1 root     root           45 Dec 12 07:45 /home/toby/elementary.txt_script2.sh
3944906      4 -rwxr-xr-x   1 root     root           45 Dec 12 07:45 /home/toby/elementary.txt_script1.sh
3944853      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/toby/elementary.txt_3.txt
3944852      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/toby/elementary.txt_0.txt
3944850      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/toby/Engineering_script.sh_2.txt
3944851      0 -rw-r--r--   1 root     root            0 Dec 12 07:45 /home/toby/deduction.doc_1.txt
3944725      4 -rw-r--r--   1 mrs_hudson mrs_hudson     3771 Jan  6  2022 /home/mrs_hudson/.bashrc
3944724      4 -rw-r--r--   1 mrs_hudson mrs_hudson      220 Jan  6  2022 /home/mrs_hudson/.bash_logout
3944726      4 -rw-r--r--   1 mrs_hudson mrs_hudson      807 Jan  6  2022 /home/mrs_hudson/.profile
3944898      4 -rwxr-xr-x   1 root       root             51 Dec 12 07:45 /home/mrs_hudson/elementary.txt_script2.sh
3944897      4 -rwxr-xr-x   1 root       root             51 Dec 12 07:45 /home/mrs_hudson/elementary.txt_script1.sh
3944831      0 -rw-r--r--   1 root       root              0 Dec 12 07:45 /home/mrs_hudson/elementary.txt_3.txt
3944828      0 -rw-r--r--   1 root       root              0 Dec 12 07:45 /home/mrs_hudson/Engineering_script.sh_1.txt
3944830      0 -rw-r--r--   1 root       root              0 Dec 12 07:45 /home/mrs_hudson/deduction.doc_2.txt
3944829      0 -rw-r--r--   1 root       root              0 Dec 12 07:45 /home/mrs_hudson/deduction.doc_0.txt
3944737      4 -rw-r--r--   1 sysadmin   sysadmin       3771 Jan  6  2022 /home/sysadmin/.bashrc
3944736      4 -rw-r--r--   1 sysadmin   sysadmin        220 Jan  6  2022 /home/sysadmin/.bash_logout
3944738      4 -rw-r--r--   1 sysadmin   sysadmin        807 Jan  6  2022 /home/sysadmin/.profile
```

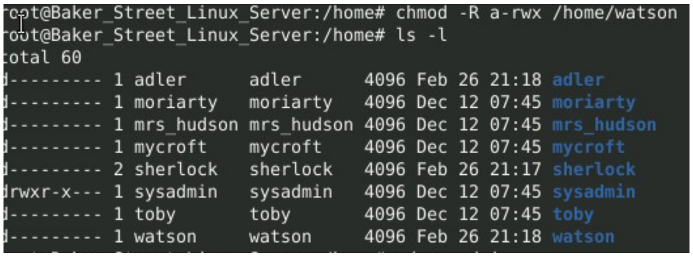
To verify I ran the find command again as shown below.



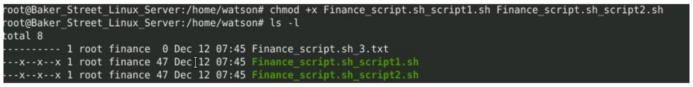
```
root@Baker_Street_Linux_Server:/home# find /home -type f \( -perm -o=r -o -perm -o=w -o -perm -o=x \) -exec chmod o-rwx {} +
root@Baker_Street_Linux_Server:/home# find /home -type f \( -perm -o=r -o -perm -o=w -o -perm -o=x \) -ls
```



```
root@Baker_Street_Linux_Server:/home# chmod -R a-rwx /home/toby
root@Baker_Street_Linux_Server:/home# ls -l
total 60
d--------- 1 adler      adler      4096 Feb 26 21:18 adler
d--------- 1 moriarty   moriarty   4096 Dec 12 07:45 moriarty
d--------- 1 mrs_hudson mrs_hudson 4096 Dec 12 07:45 mrs_hudson
d--------- 1 mycroft    mycroft    4096 Dec 12 07:45 mycroft
d--------- 2 sherlock   sherlock   4096 Feb 26 21:17 sherlock
drwxr-x--- 1 sysadmin   sysadmin   4096 Dec 12 07:45 sysadmin
d--------- 1 toby       toby       4096 Dec 12 07:45 toby
```

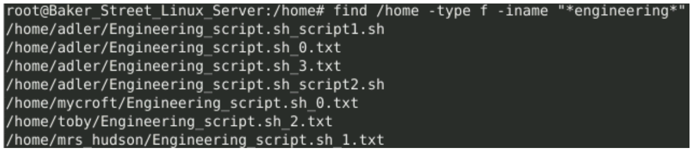


```
root@Baker_Street_Linux_Server:/home# chmod -R a-rwx /home/watson
root@Baker_Street_Linux_Server:/home# ls -l
total 60
d--------- 1 adler      adler      4096 Feb 26 21:18 adler
d--------- 1 moriarty   moriarty   4096 Dec 12 07:45 moriarty
d--------- 1 mrs_hudson mrs_hudson 4096 Dec 12 07:45 mrs_hudson
d--------- 1 mycroft    mycroft    4096 Dec 12 07:45 mycroft
d--------- 2 sherlock   sherlock   4096 Feb 26 21:17 sherlock
drwxr-x--- 1 sysadmin   sysadmin   4096 Dec 12 07:45 sysadmin
d--------- 1 toby       toby       4096 Dec 12 07:45 toby
d--------- 1 watson     watson     4096 Feb 26 21:18 watson
```

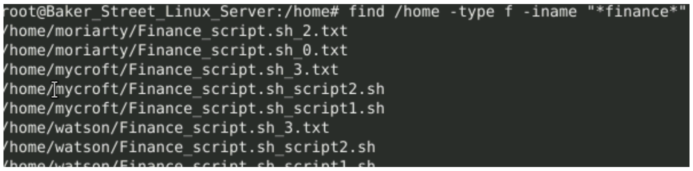


```
root@Baker_Street_Linux_Server:/home/watson# chmod +x Finance_script.sh_script1.sh Finance_script.sh_script2.sh
root@Baker_Street_Linux_Server:/home/watson# ls -l
total 8
---------- 1 root finance  0 Dec 12 07:45 Finance_script.sh_3.txt
---x--x--x 1 root finance 47 Dec 12 07:45 Finance_script.sh_script1.sh
---x--x--x 1 root finance 47 Dec 12 07:45 Finance_script.sh_script2.sh
```

Then used the find command to find scripts with engineering and finance in the filename.

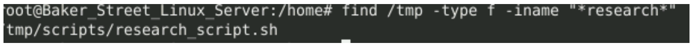


```
root@Baker_Street_Linux_Server:/home# find /home -type f -iname "*engineering*"
/home/adler/Engineering_script.sh_script1.sh
/home/adler/Engineering_script.sh_0.txt
/home/adler/Engineering_script.sh_3.txt
/home/adler/Engineering_script.sh_script2.sh
/home/mycroft/Engineering_script.sh_0.txt
/home/toby/Engineering_script.sh_2.txt
/home/mrs_hudson/Engineering_script.sh_1.txt
```



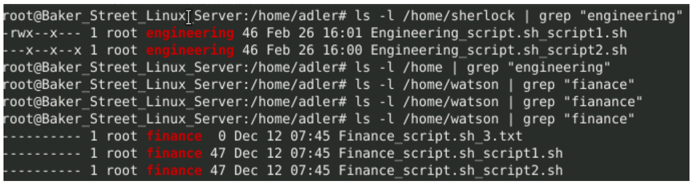
```
root@Baker_Street_Linux_Server:/home# find /home -type f -iname "*finance*"
/home/moriarty/Finance_script.sh_2.txt
/home/moriarty/Finance_script.sh_0.txt
/home/mycroft/Finance_script.sh_3.txt
/home/mycroft/Finance_script.sh_script2.sh
/home/mycroft/Finance_script.sh_script1.sh
/home/watson/Finance_script.sh_3.txt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

There wasn’t any scripts with research in the home directory but I did find a research script in the tmp directory



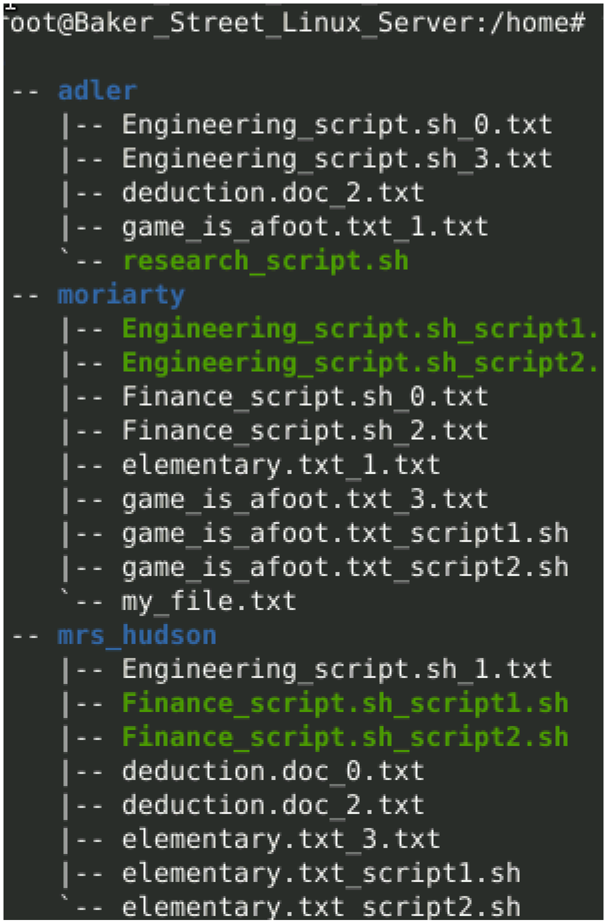
```
root@Baker_Street_Linux_Server:/home# find /tmp -type f -iname "*research*"
/tmp/scripts/research_script.sh
```

Then I ran chown :groupname scriptname.sh to change ownership of the scripts

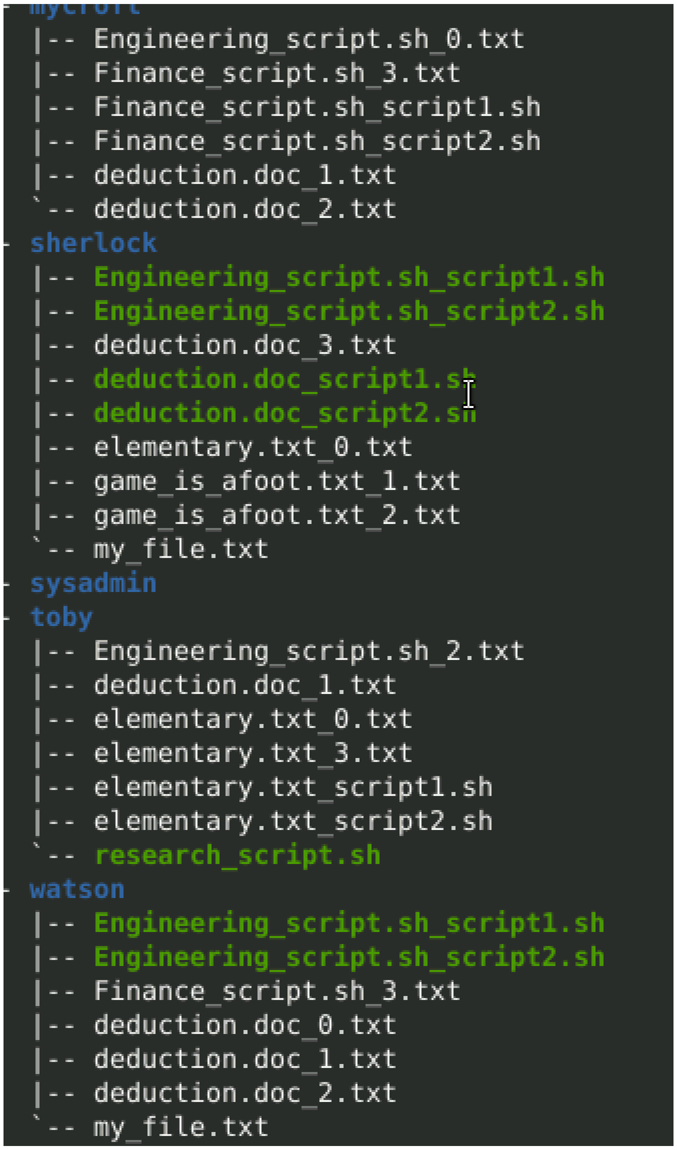


```
root@Baker_Street_Linux Server:/home/adler# ls -l /home/sherlock | grep "engineering"
-rwx--x--- 1 root engineering 46 Feb 26 16:01 Engineering_script.sh_script1.sh
---x--x--x 1 root engineering 46 Feb 26 16:00 Engineering_script.sh_script2.sh
root@Baker_Street_Linux_Server:/home/adler# ls -l /home | grep "engineering"
root@Baker_Street_Linux_Server:/home/adler# ls -l /home/watson | grep "fianace"
root@Baker_Street_Linux_Server:/home/adler# ls -l /home/watson | grep "fianance"
root@Baker_Street_Linux_Server:/home/adler# ls -l /home/watson | grep "finance"
---------- 1 root finance  0 Dec 12 07:45 Finance_script.sh_3.txt
---------- 1 root finance 47 Dec 12 07:45 Finance_script.sh_script1.sh
---------- 1 root finance 47 Dec 12 07:45 Finance_script.sh_script2.sh
```

Then I used the mv and cp commands to move scripts to the proper directories then I used the tree command to verify.

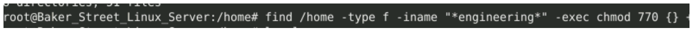


```
root@Baker_Street_Linux_Server:/home#

-- adler
    |-- Engineering_script.sh_0.txt
    |-- Engineering_script.sh_3.txt
    |-- deduction.doc_2.txt
    |-- game_is_afoot.txt_1.txt
    `-- research_script.sh
-- moriarty
    |-- Engineering_script.sh_script1.
    |-- Engineering_script.sh_script2.
    |-- Finance_script.sh_0.txt
    |-- Finance_script.sh_2.txt
    |-- elementary.txt_1.txt
    |-- game_is_afoot.txt_3.txt
    |-- game_is_afoot.txt_script1.sh
    |-- game_is_afoot.txt_script2.sh
    `-- my_file.txt
-- mrs_hudson
    |-- Engineering_script.sh_1.txt
    |-- Finance_script.sh_script1.sh
    |-- Finance_script.sh_script2.sh
    |-- deduction.doc_0.txt
    |-- deduction.doc_2.txt
    |-- elementary.txt_3.txt
    |-- elementary.txt_script1.sh
    `-- elementary.txt_script2.sh
```

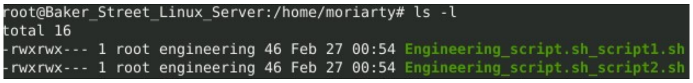


```
- mycroft
  |-- Engineering_script.sh_0.txt
  |-- Finance_script.sh_3.txt
  |-- Finance_script.sh_script1.sh
  |-- Finance_script.sh_script2.sh
  |-- deduction.doc_1.txt
  `-- deduction.doc_2.txt
- sherlock
  |-- Engineering_script.sh_script1.sh
  |-- Engineering_script.sh_script2.sh
  |-- deduction.doc_3.txt
  |-- deduction.doc_script1.sh
  |-- deduction.doc_script2.sh
  |-- elementary.txt_0.txt
  |-- game_is_afoot.txt_1.txt
  |-- game_is_afoot.txt_2.txt
  `-- my_file.txt
- sysadmin
- toby
  |-- Engineering_script.sh_2.txt
  |-- deduction.doc_1.txt
  |-- elementary.txt_0.txt
  |-- elementary.txt_3.txt
  |-- elementary.txt_script1.sh
  |-- elementary.txt_script2.sh
  `-- research_script.sh
- watson
  |-- Engineering_script.sh_script1.sh
  |-- Engineering_script.sh_script2.sh
  |-- Finance_script.sh_3.txt
  |-- deduction.doc_0.txt
  |-- deduction.doc_1.txt
  |-- deduction.doc_2.txt
  `-- my_file.txt
```

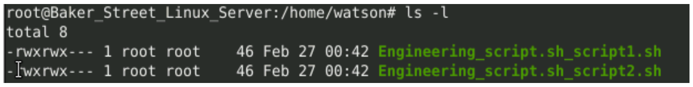
And last but not least i changed permissions to each group



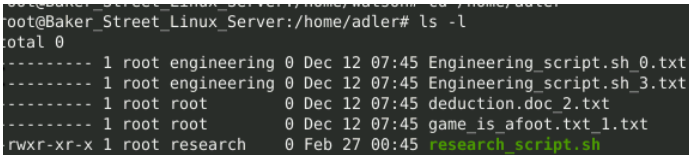
```
root@Baker_Street_Linux_Server:/home# find /home -type f -iname "*engineering*" -exec chmod 770 {}
```



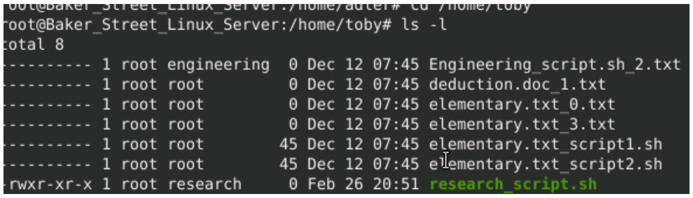
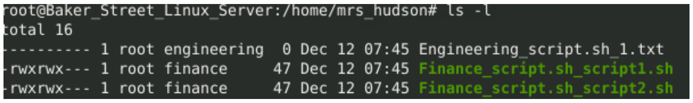
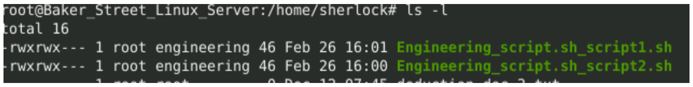
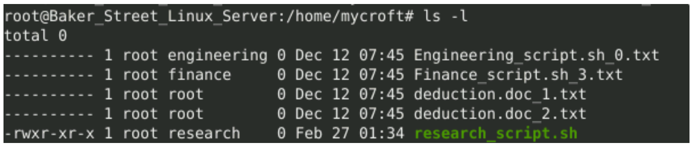
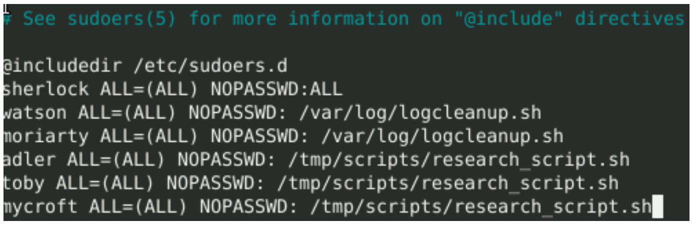
```
root@Baker_Street_Linux_Server:/home/moriarty# ls -l
total 16
-rwxrwx--- 1 root engineering 46 Feb 27 00:54 Engineering_script.sh_script1.sh
-rwxrwx--- 1 root engineering 46 Feb 27 00:54 Engineering_script.sh_script2.sh
```

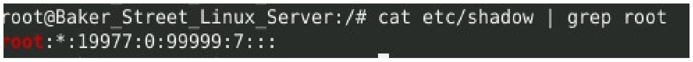
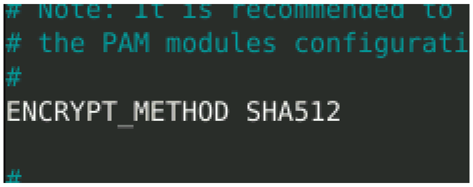


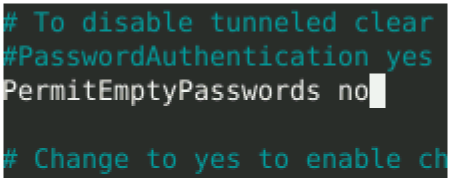
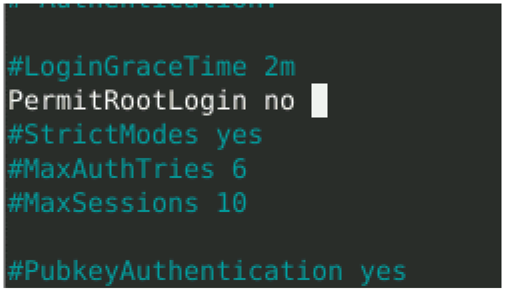
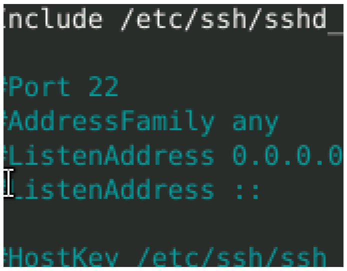
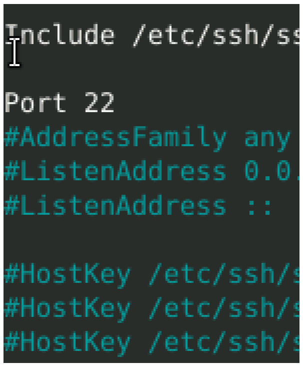
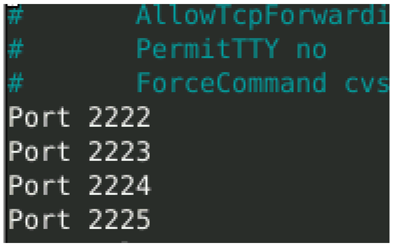
```
root@Baker_Street_Linux_Server:/home/watson# ls -l
total 8
-rwxrwx--- 1 root root    46 Feb 27 00:42 Engineering_script.sh_script1.sh
-rwxrwx--- 1 root root    46 Feb 27 00:42 Engineering_script.sh_script2.sh
```



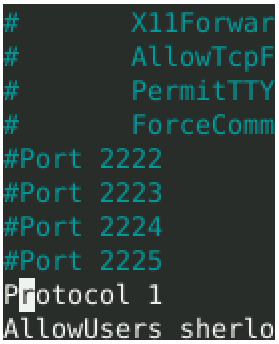
```
oot@Baker_Street_Linux_Server:/home/adler# ls -l
otal 0
--------- 1 root engineering 0 Dec 12 07:45 Engineering_script.sh_0.txt
--------- 1 root engineering 0 Dec 12 07:45 Engineering_script.sh_3.txt
--------- 1 root root        0 Dec 12 07:45 deduction.doc_2.txt
--------- 1 root root        0 Dec 12 07:45 game_is_afoot.txt_1.txt
rwxr-xr-x 1 root research    0 Feb 27 00:45 research_script.sh
```

		
		`root@Baker_Street_Linux_Server:/home/adler# cd /home/toby`
		`root@Baker_Street_Linux_Server:/home/toby# ls -l`
		`total 8`
		`---------- 1 root engineering  0 Dec 12 07:45 Engineering_script.sh_2.txt`
		`---------- 1 root root         0 Dec 12 07:45 deduction.doc_1.txt`
		`---------- 1 root root         0 Dec 12 07:45 elementary.txt_0.txt`
		`---------- 1 root root         0 Dec 12 07:45 elementary.txt_3.txt`
		`---------- 1 root root        45 Dec 12 07:45 elementary.txt_script1.sh`
		`---------- 1 root root        45 Dec 12 07:45 elementary.txt_script2.sh`
		`-rwxr-xr-x 1 root research     0 Feb 26 20:51 research_script.sh`
		
		`root@Baker_Street_Linux_Server:/home/mrs_hudson# ls -l`
		`total 16`
		`---------- 1 root engineering  0 Dec 12 07:45 Engineering_script.sh_1.txt`
		`-rwxrwx--- 1 root finance     47 Dec 12 07:45 Finance_script.sh_script1.sh`
		`-rwxrwx--- 1 root finance     47 Dec 12 07:45 Finance_script.sh_script2.sh`
		
		`root@Baker_Street_Linux_Server:/home/sherlock# ls -l`
		`total 16`
		`-rwxrwx--- 1 root engineering 46 Feb 26 16:01 Engineering_script.sh_script1.sh`
		`-rwxrwx--- 1 root engineering 46 Feb 26 16:00 Engineering_script.sh_script2.sh`
		Mycroft also didn’t have a group so I added them to research.
		
		`root@Baker_Street_Linux_Server:/home/mycroft# ls -l`
		`total 0`
		`---------- 1 root engineering 0 Dec 12 07:45 Engineering_script.sh_0.txt`
		`---------- 1 root finance     0 Dec 12 07:45 Finance_script.sh_3.txt`
		`---------- 1 root root        0 Dec 12 07:45 deduction.doc_1.txt`
		`---------- 1 root root        0 Dec 12 07:45 deduction.doc_2.txt`
		`-rwxr-xr-x 1 root research    0 Feb 27 01:34 research_script.sh`
		Then I updated visudo
		
		`# See sudoers(5) for more information on "@include" directives`
		
		`@includedir /etc/sudoers.d`
		`sherlock ALL=(ALL) NOPASSWD:ALL`
		`watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh`
		`moriarty ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh`
		`adler ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh`
		`toby ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh`
		`mycroft ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh`
		I hope I don’t get docked for adding people into the research group. It was a lot of fun to get the practice in.

☑	Optional: Updating password hashing configuration	I ran the command cat etc/shadow | grep root and it gave me this output
		
		`root@Baker_Street_Linux_Server:/# cat etc/shadow | grep root`
		`root:*:19977:0:99999:7:::`
		I went into nano and found this line,
		
		`# Note: It is recommended to`
		`# the PAM modules configurati`
		`#`
		`ENCRYPT_METHOD SHA512`
		
		`#`
		When I was researching how to do this it said to change it to YESCRYPT for stronger security. So I did,
		
		You can also update it through the /etc/pam.d/common-password file as well.

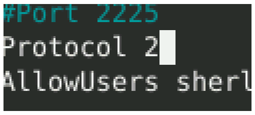
☑	Auditing and securing SSH	I ran the command nano /etc/ssh/sshd_config.
		I found the line that says PermitEmptyPasswords yes and I changed it to no.
		
		`# To disable tunneled clear`
		`#PasswordAuthentication yes`
		`PermitEmptyPasswords no`
		
		`# Change to yes to enable ch`
		Then I found the line that says PermitRootLogin yes and I changed it to no.
		
		`#LoginGraceTime 2m`
		`PermitRootLogin no`
		`#StrictModes yes`
		`#MaxAuthTries 6`
		`#MaxSessions 10`
		
		`#PubkeyAuthentication yes`
		I found the line that said port 22 and it uncommented it.
		
		`nclude /etc/ssh/sshd_`
		
		`#Port 22`
		`#AddressFamily any`
		`#ListenAddress 0.0.0.0`
		`#ListenAddress ::`
		
		`#HostKey /etc/ssh/ssh`
		
		`Include /etc/ssh/ss`
		
		`Port 22`
		`#AddressFamily any`
		`#ListenAddress 0.0.`
		`#ListenAddress ::`
		
		`#HostKey /etc/ssh/s`
		`#HostKey /etc/ssh/s`
		`#HostKey /etc/ssh/s`
		I found additional ports and I commented them in
		
		`#       AllowTcpForwardi`
		`#       PermitTTY no`
		`#       ForceCommand cvs`
		`Port 2222`
		`Port 2223`
		`Port 2224`
		`Port 2225`

<table>
<tr>
<td></td>
<td></td>
<td>



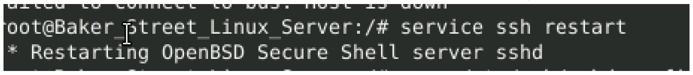
```
#       X11Forwar
#       AllowTcpF
#       PermitTTY
#       ForceComm
#Port 2222
#Port 2223
#Port 2224
#Port 2225
Protocol 1
AllowUsers sherlo
```

I found the line that said protocol one and I changed it to:



```
#Port 2225
Protocol 2
AllowUsers sherl
```

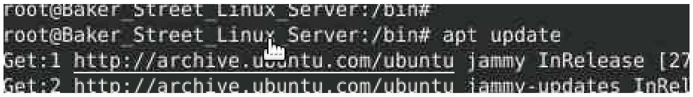
Then I restarted the ssh with these changes



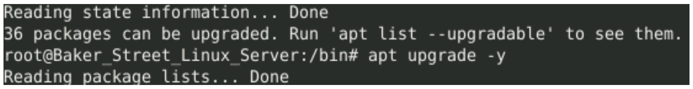
```
oot@Baker_Street_Linux_Server:/# service ssh restart
 * Restarting OpenBSD Secure Shell server sshd
```

.
</td>
</tr>
<tr>
<td>☑</td>
<td>Reviewing and updating system packages</td>
<td>

I ran apt update then I upgraded the packages

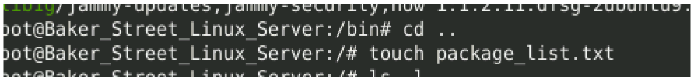


```
root@Baker_Street_Linux_Server:/bin#
root@Baker_Street_Linux_Server:/bin# apt update
Get:1 http://archive.ubuntu.com/ubuntu jammy InRelease [27
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates InRel
```



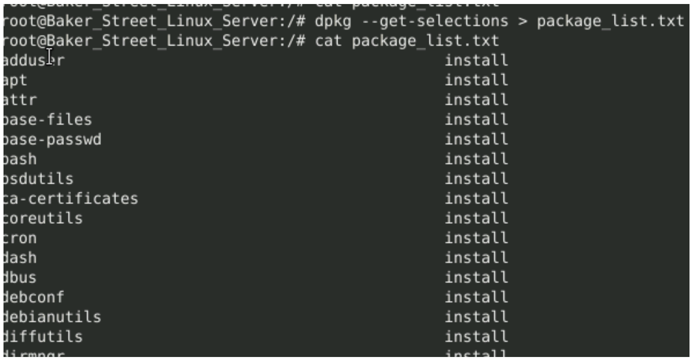
```
Reading state information... Done
36 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@Baker_Street_Linux_Server:/bin# apt upgrade -y
Reading package lists... Done
```

Then I ran the command touch package_list.txt to create a new file.



```
oot@Baker_Street_Linux_Server:/bin# cd ..
oot@Baker_Street_Linux_Server:/# touch package_list.txt
```

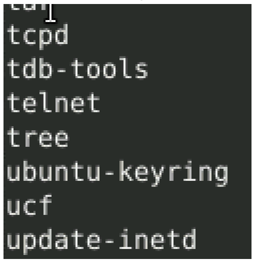
I ran the command dpkg –get-selections > package_list.txt and it put all the newly installed packages into this file. I ran the cat package_list.txt to confirm they were all there.



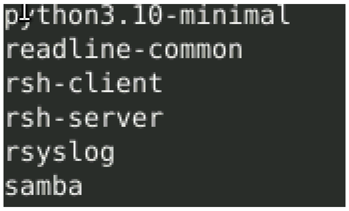
```
root@Baker_Street_Linux_Server:/# dpkg --get-selections > package_list.txt
root@Baker_Street_Linux_Server:/# cat package_list.txt
adduser                                         install
apt                                             install
attr                                            install
base-files                                      install
base-passwd                                     install
bash                                            install
bsdutils                                        install
ca-certificates                                 install
coreutils                                       install
cron                                            install
dash                                            install
dbus                                            install
debconf                                         install
debianutils                                     install
diffutils                                       install
```

The reason why telnet is a security risk is that the communication between the client and server is not
</td>
</tr>
</table>

encrypted.
Rsh-client is a security risk due to its dependence on weak authentication methods, making it vulnerable to IP spoofing and DNS spoofing attacks.
I found they were indeed on the list.

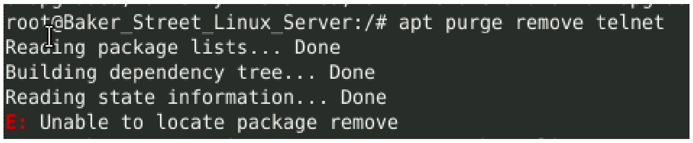


```
tcpd
tdb-tools
telnet
tree
ubuntu-keyring
ucf
update-inetd
```



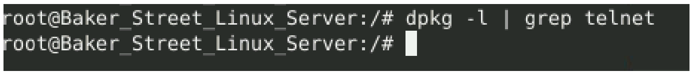
```
python3.10-minimal
readline-common
rsh-client
rsh-server
rsyslog
samba
```

Then I removed the packages using the apt remove command then I updated my package_list. I noticed that telnet's configuration files were left behind so at first I used the apt purge telnet. But it said it was unable to locate the package to remove



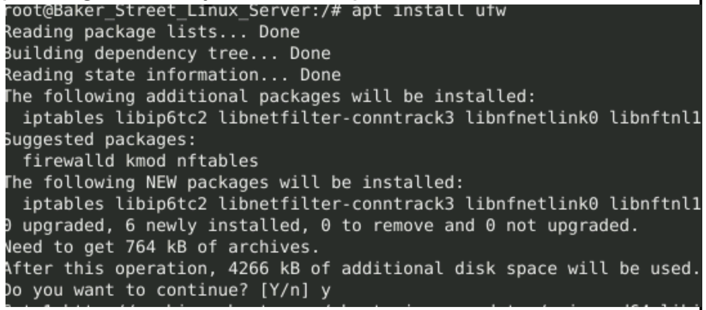
```
root@Baker_Street_Linux_Server:/# apt purge remove telnet
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package remove
```

So then I used the command dpkg –purge –force-all telnet. Then I used the command dpkg -l | grep telnet and it came up with nothing meaning it was removed.

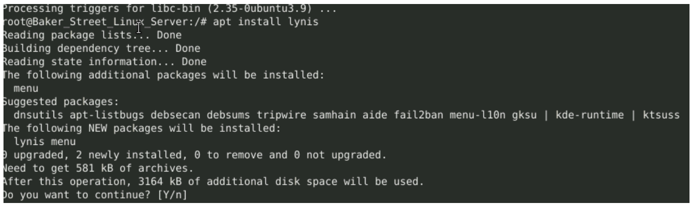


```
root@Baker_Street_Linux_Server:/# dpkg -l | grep telnet
root@Baker_Street_Linux_Server:/#
```

Then I ran the apt autoremove -y.
Then using the apt install command to install the packages ufw, lynis, and tripwire.

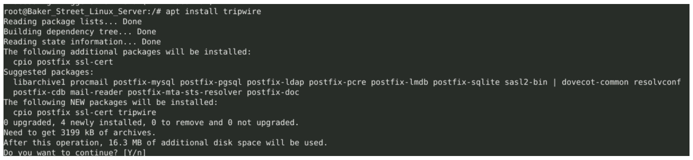


```
root@Baker_Street_Linux_Server:/# apt install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  iptables libip6tc2 libnetfilter-conntrack3 libnfnetlink0 libnftnl1
Suggested packages:
  firewalld kmod nftables
The following NEW packages will be installed:
  iptables libip6tc2 libnetfilter-conntrack3 libnfnetlink0 libnftnl1
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
```



```
Processing triggers for libc-bin (2.35-0ubuntu3.9) ...
root@Baker_Street_Linux_Server:/# apt install lynis
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  menu
Suggested packages:
  dnsutils apt-listbugs debsecan debsums tripwire samhain aide fail2ban menu-l10n gksu | kde-runtime | ktsuss
The following NEW packages will be installed:
  lynis menu
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 581 kB of archives.
After this operation, 3164 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

<table>
<tr>
<td></td>
<td></td>
<td>



```
root@Baker_Street_Linux_Server:/# apt install tripwire
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:
  libarchive1 procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb postfix-sqlite sasl2-bin | dovecot-common resolvconf
  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]
```

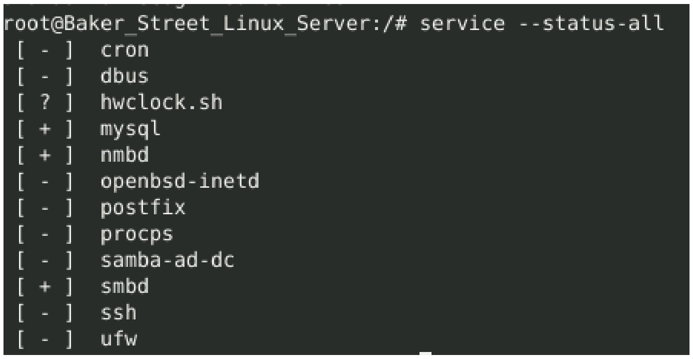
Ufw stands for uncomplicated firewall and it provides a user-friendly interface for managing firewall rules, simplifies common firewall tasks and helps protect against unauthorized access. It denies all incoming connections and allows all outgoing connections. It uses a default deny for incoming traffic that only allows connections. It provides logging capabilities to monitor firewall activity.

Lynis is a security auditing tool that provides guidance for system hardening, it detects vulnerabilities, and assists with security compliance testing. It provides specific recommendations and suggestions for hardening the system. It performs in depth security scans and identifies any potential weakness a system might have.

Tripwire provides hardening features through its file integrity monitoring and security configuration management. They help companies reduce their attack surface, maintain system integrity and ensure continuous compliance. It monitors for suspicious or unauthorized changes to critical assets by recording specific attributes of files, i.e. hashes and timestamps. It can also detect unauthorized file and directory modifications on local systems.

</td>
</tr>
<tr>
<td>☑</td>
<td>Disabling unnecessary services</td>
<td>

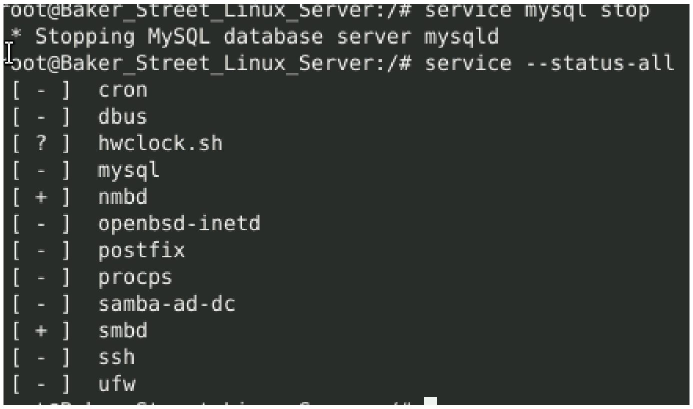
I learned that this web lab is a sysvinit based system and the systemctl -t service - -all didn't work but I did some research and service - - status-all was the one that worked.



```
root@Baker_Street_Linux_Server:/# service --status-all
 [ - ]  cron
 [ - ]  dbus
 [ ? ]  hwclock.sh
 [ + ]  mysql
 [ + ]  nmbd
 [ - ]  openbsd-inetd
 [ - ]  postfix
 [ - ]  procps
 [ - ]  samba-ad-dc
 [ + ]  smbd
 [ - ]  ssh
 [ - ]  ufw
```

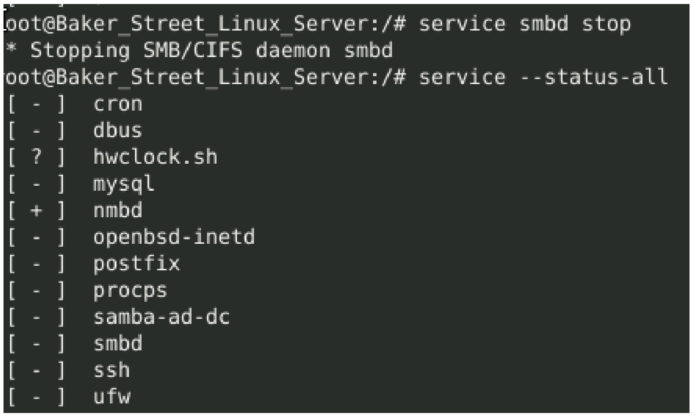
</td>
</tr>
</table>

Then to save that to a file I ran the command service - -status-all > service_list.txt then I ran the cat command to verify. For some reason [?] hwclock.sh didn't go in there.
I used the command service - -status-all mysql to stop that service then I ran the command to list all the services to verify that it stopped.



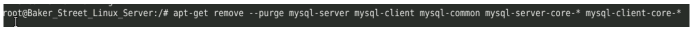
```
root@Baker_Street_Linux_Server:/# service mysql stop
 * Stopping MySQL database server mysqld
oot@Baker_Street_Linux_Server:/# service --status-all
 [ - ]  cron
 [ - ]  dbus
 [ ? ]  hwclock.sh
 [ - ]  mysql
 [ + ]  nmbd
 [ - ]  openbsd-inetd
 [ - ]  postfix
 [ - ]  procps
 [ - ]  samba-ad-dc
 [ + ]  smbd
 [ - ]  ssh
 [ - ]  ufw
```

Samba-ad-dc was already stopped but, I heard someone in class say that smbd was also a part of samba so I stopped that one as well and verified

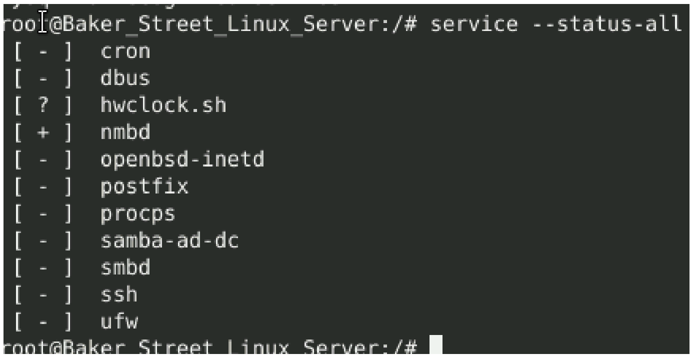


```
oot@Baker_Street_Linux_Server:/# service smbd stop
* Stopping SMB/CIFS daemon smbd
root@Baker_Street_Linux_Server:/# service --status-all
[ - ]  cron
[ - ]  dbus
[ ? ]  hwclock.sh
[ - ]  mysql
[ + ]  nmbd
[ - ]  openbsd-inetd
[ - ]  postfix
[ - ]  procps
[ - ]  samba-ad-dc
[ - ]  smbd
[ - ]  ssh
[ - ]  ufw
```

So chkconfig isn't on this version. So I used the command apt-get remove --purge mysql-server mysql-client mysql-common mysql-server-core-* mysql-client-core-* then I ran the apt-get autoremove -y to get rid of any dependencies. Then I verified that it was removed.

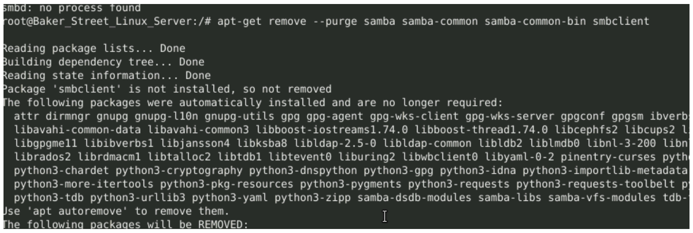


```
root@Baker_Street_Linux_Server:/# apt-get remove --purge mysql-server mysql-client mysql-common mysql-server-core-* mysql-client-core-*
```

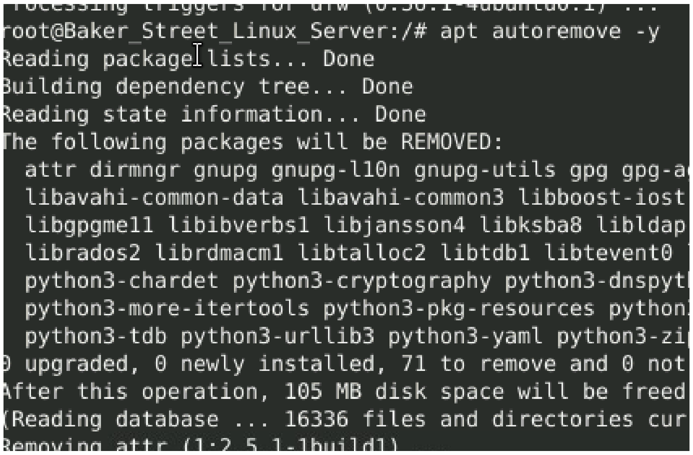


```
root@Baker_Street_Linux_Server:/# service --status-all
 [ - ]  cron
 [ - ]  dbus
 [ ? ]  hwclock.sh
 [ + ]  nmbd
 [ - ]  openbsd-inetd
 [ - ]  postfix
 [ - ]  procps
 [ - ]  samba-ad-dc
 [ - ]  smbd
 [ - ]  ssh
 [ - ]  ufw
root@Baker_Street_Linux_Server:/# 
```

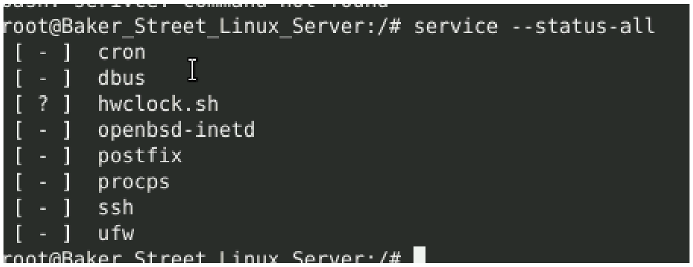
Then in order to run the smbd and samba-ad-dc packages I ran the command apt-get remove --purged samba samba-common-bin smbclient Then I ran apt autoremove -y to clear out any dependencies. Then I verified it was removed.



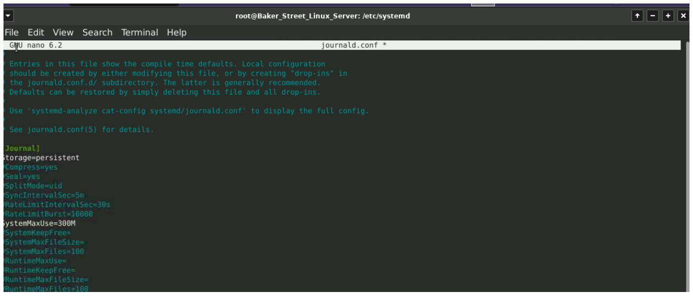
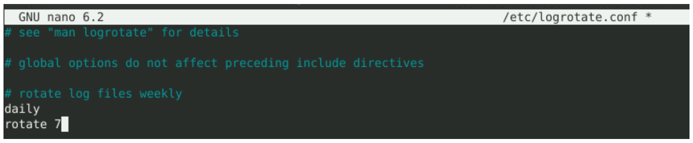
```
smbd: no process found
root@Baker_Street_Linux_Server:/# apt-get remove --purge samba samba-common samba-common-bin smbclient

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package 'smbclient' is not installed, so not removed
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 ibverb
  libavahi-common-data libavahi-common3 libboost-iostreams1.74.0 libboost-thread1.74.0 libcephfs2 libcups2 l
  libgpgme11 libibverbs1 libjansson4 libksba8 libldap-2.5-0 libldap-common libldb2 liblmdb0 libnl-3-200 libn
  librados2 librdmacm1 libtalloc2 libtdb1 libtevent0 liburing2 libwbclient0 libyaml-0-2 pinentry-curses pyth
  python3-chardet python3-cryptography python3-dnspython python3-gpg python3-idna python3-importlib-metadata
  python3-more-itertools python3-pkg-resources python3-pygments python3-requests python3-requests-toolbelt p
  python3-tdb python3-urllib3 python3-yaml python3-zipp samba-dsdb-modules samba-libs samba-vfs-modules tdb-
Use 'apt autoremove' to remove them.
The following packages will be REMOVED:
```



```
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
root@Baker_Street_Linux_Server:/# apt autoremove -y
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-a
  libavahi-common-data libavahi-common3 libboost-iost
  libgpgme11 libibverbs1 libjansson4 libksba8 libldap
  librados2 librdmacm1 libtalloc2 libtdb1 libtevent0 
  python3-chardet python3-cryptography python3-dnspyt
  python3-more-itertools python3-pkg-resources python
  python3-tdb python3-urllib3 python3-yaml python3-zi
0 upgraded, 0 newly installed, 71 to remove and 0 not
After this operation, 105 MB disk space will be freed
(Reading database ... 16336 files and directories cur
Removing attr (1:2.5.1-1build1) ...
```



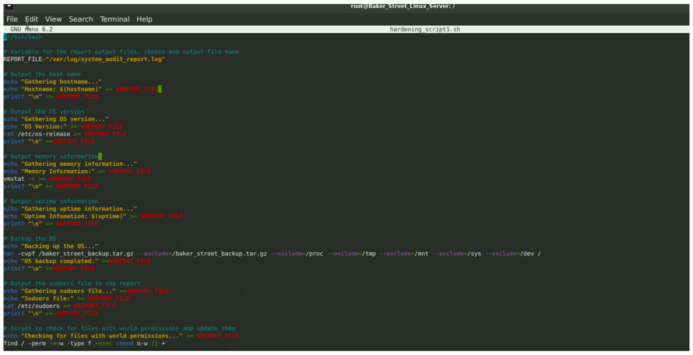
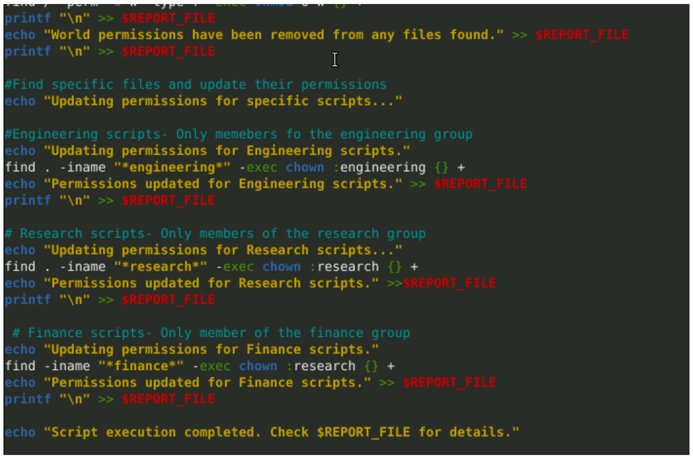
```
bash: service: command not found
root@Baker_Street_Linux_Server:/# service --status-all
 [ - ]  cron
 [ - ]  dbus
 [ ? ]  hwclock.sh
 [ - ]  openbsd-inetd
 [ - ]  postfix
 [ - ]  procps
 [ - ]  ssh
 [ - ]  ufw
root@Baker_Street_Linux_Server:/# 
```

☑	Enabling and configuring logging	This step was pretty easy. I went through and updated the logrotate nano.  

root@Baker_Street_Linux_Server: /etc/systemd

```
GNU nano 6.2                                   journald.conf *
#
# 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
```

```
  GNU nano 6.2                                   /etc/logrotate.conf *
# see "man logrotate" for details

# global options do not affect preceding include directives

# rotate log files weekly
daily
rotate 7
```

☑	Scripts created	 

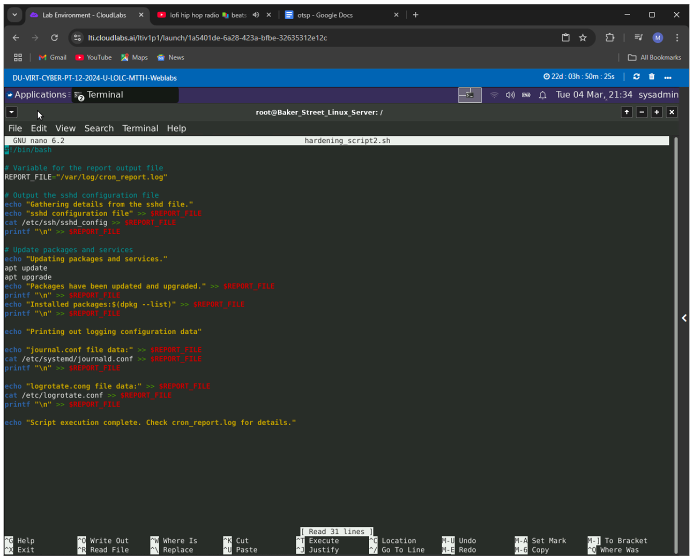
root@Baker_Street_Linux_Server: /

```
GNU nano 6.2                                   hardening_script1.sh
#!/bin/bash

# Variable for the report output files, choose and output file name
REPORT_FILE="/var/log/system_audit_report.log"

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

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

# Output memory informarion
echo "Gathering memory information..."
echo "Memory Information:" >> $REPORT_FILE
vmstat -s >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

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

# Backup the OS
echo "Backing up the OS..."
tar -cvpf /baker_street_backup.tar.gz --exclude=/baker_street_backup.tar.gz --exclude=/proc --exclude=/tmp --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..." >>$REPORT_FILE
echo "Sudoers file:" >> $REPORT_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..." >> $REPORT_FILE
find / -perm -o=w -type f -exec chmod o-w {} +
```

```
printf "\n" >> $REPORT_FILE
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 memebers fo the engineering group
echo "Updating permissions for Engineering scripts."
find . -iname "*engineering*" -exec chown :engineering {} +
echo "Permissions updated for Engineering scripts." >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Research scripts- Only members of the research group
echo "Updating permissions for Research scripts..."
find . -iname "*research*" -exec chown :research {} +
echo "Permissions updated for Research scripts." >>$REPORT_FILE
printf "\n" >> $REPORT_FILE

 # Finance scripts- Only member of the finance group
echo "Updating permissions for Finance scripts."
find -iname "*finance*" -exec chown :research {} +
echo "Permissions updated for Finance scripts." >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

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

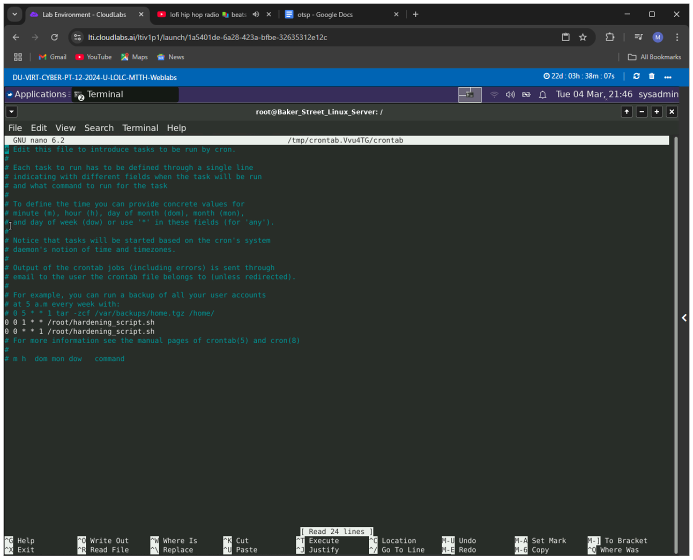
☑

Scripts scheduled with cron



```
  GNU nano 6.2                                    hardening_script2.sh
#!/bin/bash

# Variable for the report output file
REPORT_FILE="/var/log/cron_report.log"

# Output the sshd configuration file
echo "Gathering details from the sshd file."
echo "sshd configuration file" >> $REPORT_FILE
cat /etc/ssh/sshd_config >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

# Update packages and services
echo "Updating packages and services."
apt update
apt upgrade
echo "Packages have been updated and upgraded." >> $REPORT_FILE
printf "\n" >> $REPORT_FILE
echo "Installed packages:$(dpkg --list)" >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

echo "Printing out logging configuration data"

echo "journal.conf file data:" >> $REPORT_FILE
cat /etc/systemd/journald.conf >> $REPORT_FILE
printf "\n" >> $REPORT_FILE

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

echo "Script execution complete. Check cron_report.log for details."

                                      [ Read 31 lines ]
```

Once you understand what you are doing, writing scripts is actually pretty fun.
Then I scheduled the cron jobs



```
  GNU nano 6.2                                 /tmp/crontab.Vvu4TG/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
0 0 1 * * /root/hardening_script.sh
0 0 * * 1 /root/hardening_script.sh
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

                                      [ Read 24 lines ]
```