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**
Memory information	**total used free shared buff/cache available** **15Gi 1.3Gi 11Gi 204Mi 2.2Gi 13Gi**
Uptime information	**up 47 minutes**

Checklist

Completed	Activity	Script(s) used / Tasks completed / Screenshots

☑	OS backup	**=> 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 /***
		`root@Baker_Street_Linux_Server:/# ls -lh`
		`total 211M`
		`-rw-r--r--  1 root root 211M Dec 18 00:11 baker_street_backup.tar.gz`

☑	Auditing users and groups	**=> Deleted terminated users along with their Home directories**
		
		Command:
		● ***deluser --remove-home username***
		`sherlock:$y$j9T$k.8hsf0jC5sjhvbcuCtm41$hYQxtXp6zTsTSm3FlVokKfzHyu4OtC8btsm6rdXrXf5:20074:0:99999:7:::`
		`watson:$y$j9T$vtDjyGuA0eHCjVE7PK9T20$3dzLRqt8xlrQQx6jZO7uokC.h1.i8qbuaohWFUjim9.:20074:0:99999:7:::`
		`moriarty:!$y$j9T$S4/nwXR.yveVfMOjtKVoa.$JmXlzBKf67.kWCbtc.Cpn9D3dXFHbiQpQinmXrZezr3:20074:0:99999:7:::`
		`mycroft:$y$j9T$j7DI/c9DLUjAVtIghNRhj.$c1wcswVqdNCNzOi0UST.l3/oF9.SZvdvfTqf3/WzT50:20074:0:99999:7:::`
		`mrs_hudson:!:20069:0:99999:7:::`
		`sysadmin:!:20069:0:99999:7:::`
		`toby:!:20069:0:99999:7:::`
		`adler:!:20069:0:99999:7:::`
		`root@Baker_Street_Linux_Server:/#`
		
		=> Locked the user accounts, who were on temporary leave
		
		Command:
		● ***passwd -l username***
		Status of the users:
		`root@Baker_Street_Linux_Server:/# passwd -S moriarty`
		`moriarty L 12/17/2024 0 99999 7 -1`
		`root@Baker_Street_Linux_Server:/# passwd -S mrs_hudson`
		`mrs_hudson L 12/12/2024 0 99999 7 -1`
		`root@Baker_Street_Linux_Server:/#`
		
		=> Unlocked the active employees accounts
		(Changed the password and they were unlocked)
		Verify the account status:
		● ***passwd -S username***
		`root@Baker_Street_Linux_Server:/# passwd -S sherlock`
		`sherlock P 12/17/2024 0 99999 7 -1`
		`root@Baker_Street_Linux_Server:/# passwd -S watson`
		`watson P 12/17/2024 0 99999 7 -1`
		`root@Baker_Street_Linux_Server:/# passwd -S mycroft`
		`mycroft P 12/17/2024 0 99999 7 -1`
		`root@Baker_Street_Linux_Server:/# passwd -S toby`
		`toby P 12/18/2024 0 99999 7 -1`
		`root@Baker_Street_Linux_Server:/# passwd -S adler`
		`adler P 12/18/2024 0 99999 7 -1`
		`root@Baker_Street_Linux_Server:/#`
		
		=> No users found in Marketing group:
		`root@Baker_Street_Linux_Server:/# cat /etc/group | grep marketing`
		`marketing:x:1014:`
		As per the instructions from TAs, the user(s) who does not belong to any group add them to the marketing group and then move them to the research group.
		
		=> Created new group:
		● ***groupadd research***
		
		=> Adding users to group:
		● ***usermod -aG research username***
		Output:
		`root@Baker_Street_Linux_Server:/# cat /etc/group | grep research`
		`research:x:1015:mycroft,toby,adler`

		=> To remove marketing group: • ***groupdel marketing***

☑	Updating and enforcing password policies	• **=>** To update the **password** policies **pwquality** library is required
		
		Password file: **/etc/pam.d/common-password**
		
		Installed the library with command:
		• ***apt install libpam-pwquality***
		
		Updated password policies:
		• Minimum 8 characters: ***minlen=8***
		• At least one special character: ***ocredit=-1***
		• Allow 2 retries: ***retry=2***
		• At least one uppercase character: ***ucredit=-1***
		
		`# here are the per-package modules (the "Primary" block)`
		`password  requisite  pam_pwquality.so minlen=8 ocredit=-1 retry=2 ucredit=-1`
		`password  [success=1 default=ignore]  pam_unix.so obscure use_authtok try_first_pass yescrypt`
		`# here's the fallback if no module succeeds`

☑	Updating and enforcing sudo permissions	**=>** Added the necessary paths in **Sudoers** file for users and groups:
		• Full sudo privilege to **Sherlock:**
		  ○ ***sherlock ALL=(ALL) NOPASSWD ALL***
		• Watson and Mycroft should only have sudo privileges to run a script:
		  ○ ***watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh***
		  ○ ***watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh***
		• All employees who belong to the **research** group should have sudo privileges to run the following script:
		  ○ ***%research ALL=(ALL:ALL) /tmp/scripts/research_script.sh***
		
		`# Allow members of group sudo to execute any command`
		`%sudo  ALL=(ALL:ALL) ALL`
		`%research ALL=(ALL:ALL) /tmp/scripts/research_script.sh`
		`# 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`
		`mycroft ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh`

☑	Validating and updating permissions on files and directories	**=>** Found the files with world permissions.
		Command:
		• ***find /home -type f -perm -o=rwx 2> /dev/null***
		
		Output:
		`root@Baker_Street_Linux_Server:/# find /home -type f \( -perm -u=rwx -o -perm -g=rwx -o -perm -o=rwx 2> /dev/null ' )`
		`/home/adler/Engineering_script.sh_script1.sh`
		`/home/adler/Engineering_script.sh_script2.sh`
		`/home/mycroft/Finance_script.sh_script2.sh`
		`/home/mycroft/Finance_script.sh_script1.sh`
		`/home/toby/elementary.txt_script2.sh`
		`/home/toby/elementary.txt_script1.sh`
		`/home/watson/Finance_script.sh_script2.sh`
		`/home/watson/Finance_script.sh_script1.sh`
		`/home/sherlock/deduction.doc_script1.sh`
		`/home/sherlock/deduction.doc_script2.sh`
		`/home/moriarty/game_is_afoot.txt_script2.sh`
		`/home/moriarty/game_is_afoot.txt_script1.sh`
		`/home/mrs_hudson/elementary.txt_script2.sh`
		`/home/mrs_hudson/elementary.txt_script1.sh`
		
		=> Changed **permissions** to normal as **640(rw-r—)** for all world permission files, example given below.:
		Command:
		• ***find /home -type f -perm -o=rwx 2> /dev/null -exec chmod 640 {} \;***
		
		Final result after changes to all files:
		`/home/adler:`
		`total 40`
		`drwxr-x--- 1 adler adler 4096 Dec 18 19:08 .`
		`drwxr-xr-x 1 root root 4096 Dec 18 00:21 ..`
		`-rw------- 1 adler adler 18 Dec 18 17:38 .bash_history`
		`-rw-r--r-- 1 adler adler 220 Jan 6 2022 .bash_logout`
		`-rw-r--r-- 1 adler adler 3771 Jan 6 2022 .bashrc`
		`-rw-r--r-- 1 adler adler 807 Jan 6 2022 .profile`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 Engineering_script.sh_0.txt`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 Engineering_script.sh_3.txt`
		`-rw-r----- 1 root engineering 46 Dec 12 07:45 Engineering_script.sh_script1.sh`
		`-rw-r----- 1 root engineering 46 Dec 12 07:45 Engineering_script.sh_script2.sh`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 deduction.doc_2.txt`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 game_is_afoot.txt_1.txt`
		
		`/home/moriarty:`
		`total 36`
		`drwxr-x--- 1 moriarty moriarty 4096 Dec 12 07:45 .`
		`drwxr-xr-x 1 root root 4096 Dec 18 00:21 ..`
		`-rw-r--r-- 1 moriarty moriarty 220 Jan 6 2022 .bash_logout`
		`-rw-r--r-- 1 moriarty moriarty 3771 Jan 6 2022 .bashrc`
		`-rw-r--r-- 1 moriarty moriarty 807 Jan 6 2022 .profile`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 Finance_script.sh_0.txt`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 Finance_script.sh_2.txt`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 elementary.txt_1.txt`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 game_is_afoot.txt_3.txt`
		`-rw-r----- 1 root root 49 Dec 12 07:45 game_is_afoot.txt_script1.sh`
		`-rw-r----- 1 root root 49 Dec 12 07:45 game_is_afoot.txt_script2.sh`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 my_file.txt`
		
		`/home/mrs_hudson:`
		`total 40`
		`drwxr-x--- 1 mrs_hudson mrs_hudson 4096 Dec 19 18:25 .`
		`drwxr-xr-x 1 root root 4096 Dec 18 00:21 ..`
		`-rw------- 1 mrs_hudson mrs_hudson 12 Dec 19 18:25 .bash_history`
		`-rw-r--r-- 1 mrs_hudson mrs_hudson 220 Jan 6 2022 .bash_logout`
		`-rw-r--r-- 1 mrs_hudson mrs_hudson 3771 Jan 6 2022 .bashrc`
		`-rw-r--r-- 1 mrs_hudson mrs_hudson 807 Jan 6 2022 .profile`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 Engineering_script.sh_1.txt`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 deduction.doc_0.txt`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 deduction.doc_2.txt`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 elementary.txt_3.txt`
		`-rw-r----- 1 root root 51 Dec 12 07:45 elementary.txt_script1.sh`
		`-rw-r----- 1 root root 51 Dec 12 07:45 elementary.txt_script2.sh`
		
		`/home/mycroft:`
		`total 40`
		`drwxr-x--- 1 mycroft mycroft 4096 Dec 18 02:01 .`
		`drwxr-xr-x 1 root root 4096 Dec 18 00:21 ..`
		`-rw------- 1 mycroft mycroft 44 Dec 18 02:01 .bash_history`
		`-rw-r--r-- 1 mycroft mycroft 220 Jan 6 2022 .bash_logout`
		`-rw-r--r-- 1 mycroft mycroft 3771 Jan 6 2022 .bashrc`
		`-rw-r--r-- 1 mycroft mycroft 807 Jan 6 2022 .profile`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 Engineering_script.sh_0.txt`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 Finance_script.sh_3.txt`
		`-rw-r----- 1 root finance 48 Dec 12 07:45 Finance_script.sh_script1.sh`
		`-rw-r----- 1 root finance 48 Dec 12 07:45 Finance_script.sh_script2.sh`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 deduction.doc_1.txt`
		`-rw-r--r-- 1 root root 0 Dec 12 07:45 deduction.doc_2.txt`

```
/home/sherlock:
total 36
drwxr-x--- 1 sherlock sherlock 4096 Dec 12 07:45 .
drwxr-xr-x 1 root     root     4096 Dec 18 00:21 ..
-rw-r--r-- 1 sherlock sherlock  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 sherlock sherlock 3771 Jan  6  2022 .bashrc
-rw-r--r-- 1 sherlock sherlock  807 Jan  6  2022 .profile
-rw-r--r-- 1 root     root        0 Dec 12 07:45 deduction.doc_3.txt
-rw-r----- 1 root     root       49 Dec 12 07:45 deduction.doc_script1.sh
-rw-r----- 1 root     root       49 Dec 12 07:45 deduction.doc_script2.sh
-rw-r--r-- 1 root     root        0 Dec 12 07:45 elementary.txt_0.txt
-rw-r--r-- 1 root     root        0 Dec 12 07:45 game_is_afoot.txt_1.txt
-rw-r--r-- 1 root     root        0 Dec 12 07:45 game_is_afoot.txt_2.txt
-rw-r--r-- 1 root     root        0 Dec 12 07:45 my_file.txt

/home/sysadmin:
total 24
drwxr-x--- 2 sysadmin sysadmin 4096 Dec 12 07:45 .
drwxr-xr-x 1 root     root     4096 Dec 18 00:21 ..
-rw-r--r-- 1 sysadmin sysadmin  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 sysadmin sysadmin 3771 Jan  6  2022 .bashrc
-rw-r--r-- 1 sysadmin sysadmin  807 Jan  6  2022 .profile

/home/toby:
total 40
drwxr-x--- 1 toby toby 4096 Dec 18 16:22 .
drwxr-xr-x 1 root root 4096 Dec 18 00:21 ..
-rw------- 1 toby toby   17 Dec 18 16:22 .bash_history
-rw-r--r-- 1 toby toby  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 toby toby 3771 Jan  6  2022 .bashrc
-rw-r--r-- 1 toby toby  807 Jan  6  2022 .profile
-rw-r--r-- 1 root root    0 Dec 12 07:45 Engineering_script.sh_2.txt
-rw-r--r-- 1 root root    0 Dec 12 07:45 deduction.doc_1.txt
-rw-r--r-- 1 root root    0 Dec 12 07:45 elementary.txt_0.txt
-rw-r--r-- 1 root root    0 Dec 12 07:45 elementary.txt_3.txt
-rw-r----- 1 root root   45 Dec 12 07:45 elementary.txt_script1.sh
-rw-r----- 1 root root   45 Dec 12 07:45 elementary.txt_script2.sh

/home/watson:
total 40
drwxr-x--- 1 watson watson  4096 Dec 18 01:44 .
drwxr-xr-x 1 root   root    4096 Dec 18 00:21 ..
-rw------- 1 watson watson   200 Dec 18 19:48 .bash_history
-rw-r--r-- 1 watson watson   220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 watson watson  3771 Jan  6  2022 .bashrc
-rw-r--r-- 1 watson watson   807 Jan  6  2022 .profile
-rw-r--r-- 1 root   root       0 Dec 12 07:45 Finance_script.sh_3.txt
-rw-r----- 1 root   finance   47 Dec 12 07:45 Finance_script.sh_script1.sh
-rw-r----- 1 root   finance   47 Dec 12 07:45 Finance_script.sh_script2.sh
-rw-r--r-- 1 root   root       0 Dec 12 07:45 deduction.doc_0.txt
-rw-r--r-- 1 root   root       0 Dec 12 07:45 deduction.doc_1.txt
-rw-r--r-- 1 root   root       0 Dec 12 07:45 deduction.doc_2.txt
-rw-r--r-- 1 root   root       0 Dec 12 07:45 my_file.txt
```

=> Found the Engineering, Finance and research script files

Commands:

- ***find / -type f \(-name "*.sh" -o -name "*.py" -o -name "*.pl" \) -iname "*engineering*" 2> /dev/null***
- ***find / -type f \(-name "*.sh" -o -name "*.py" -o -name "*.pl" \) -iname "*research*" 2> /dev/null***
- ***find / -type f \(-name "*.sh" -o -name "*.py" -o -name "*.pl" \) -iname "*finance*" 2> /dev/null***

Output:

```
root@Baker_Street_Linux_Server:/# find / -type f \( -name "*.sh" -o -name "*.py" -o -name "*.pl" \) -iname "*Engineering*" 2> /dev/null
/home/adler/Engineering_script.sh_script1.sh
/home/adler/Engineering_script.sh_script2.sh
root@Baker_Street_Linux_Server:/# find / -type f \( -name "*.sh" -o -name "*.py" -o -name "*.pl" \) -iname "*research*" 2> /dev/null
/tmp/scripts/research_script.sh
root@Baker_Street_Linux_Server:/# find / -type f \( -name "*.sh" -o -name "*.py" -o -name "*.pl" \) -iname "*finance*" 2> /dev/null
/home/mycroft/Finance_script.sh_script2.sh
/home/mycroft/Finance_script.sh_script1.sh
/home/watson/Finance_script.sh_script2.sh
/home/watson/Finance_script.sh_script1.sh
root@Baker_Street_Linux_Server:/#
```

=> Changed the **group access** to associated users only

Commands:

Engineering*:*

- ***find /home/ -type f \(-name "*.sh" -o -name "*.py" -o -name "*.pl" \) -iname "*engineering*" 2> /dev/null -exec chown :engineering {} +***

Research*:*

- ***find /home/ -type f \(-name "*.sh" -o -name "*.py" -o -name "*.pl" \) -name "*Research*" 2> /dev/null -exec chown :research {} +***

Finance:

- ***find /home/ -type f \(-name "*.sh" -o -name "*.py" -o -name "*.pl" \) -iname "*Finance*" 2> /dev/null -exec chown :finance {} +***

Output examples:

Engineering:

From:

```
root@Baker_Street_Linux_Server:/home/adler# ls -l
total 8
-rw-r--r-- 1 root root  0 Dec 12 07:45 Engineering_script.sh_0.txt
-rw-r--r-- 1 root root  0 Dec 12 07:45 Engineering_script.sh_3.txt
-rw-r--r-- 1 root root 46 Dec 12 07:45 Engineering_script.sh_script1.sh
-rw-r--r-- 1 root root 46 Dec 12 07:45 Engineering_script.sh_script2.sh
-rw-r--r-- 1 root root  0 Dec 12 07:45 deduction.doc_2.txt
-rw-r--r-- 1 root root  0 Dec 12 07:45 game_is_afoot.txt_1.txt
```

To:

```
root@Baker_Street_Linux_Server:/home/adler# chgrp engineering Engineering_script.sh_script2.sh Engineering_script.sh_script1.sh
root@Baker_Street_Linux_Server:/home/adler# ls -l
total 8
-rw-r--r-- 1 root root         0 Dec 12 07:45 Engineering_script.sh_0.txt
-rw-r--r-- 1 root root         0 Dec 12 07:45 Engineering_script.sh_3.txt
-rw-r--r-- 1 root engineering 46 Dec 12 07:45 Engineering_script.sh_script1.sh
-rw-r--r-- 1 root engineering 46 Dec 12 07:45 Engineering_script.sh_script2.sh
-rw-r--r-- 1 root root         0 Dec 12 07:45 deduction.doc_2.txt
-rw-r--r-- 1 root root         0 Dec 12 07:45 game_is_afoot.txt_1.txt
root@Baker_Street_Linux_Server:/home/adler#
```

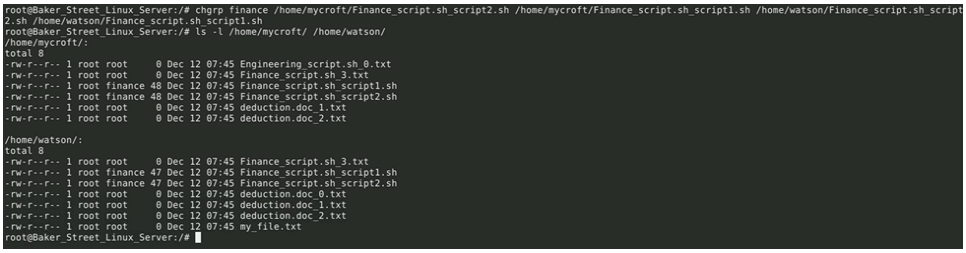
Research:

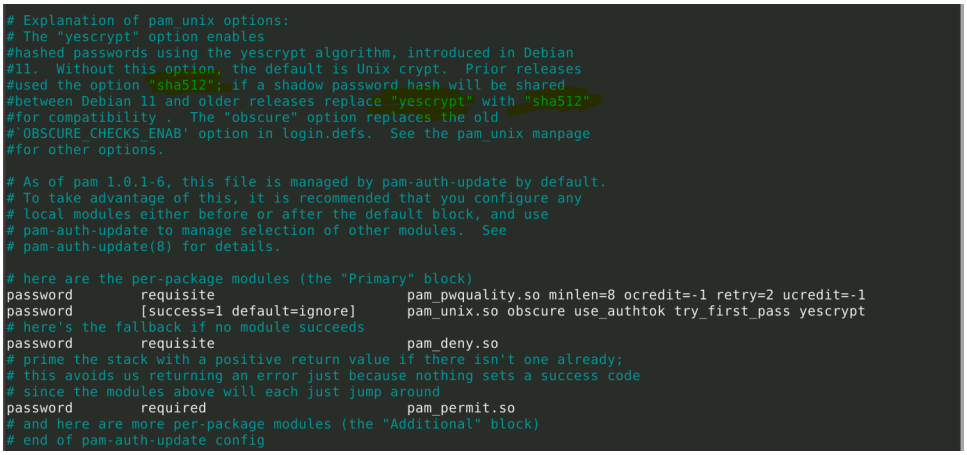
From:

```
root@Baker_Street_Linux_Server:/tmp/scripts# ls -l
total 0
-rwxr-xr-x 1 root root 0 Dec 18 17:23 research_script.sh
```

To:

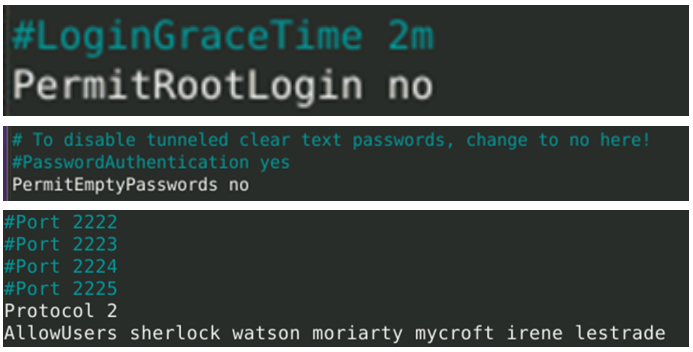
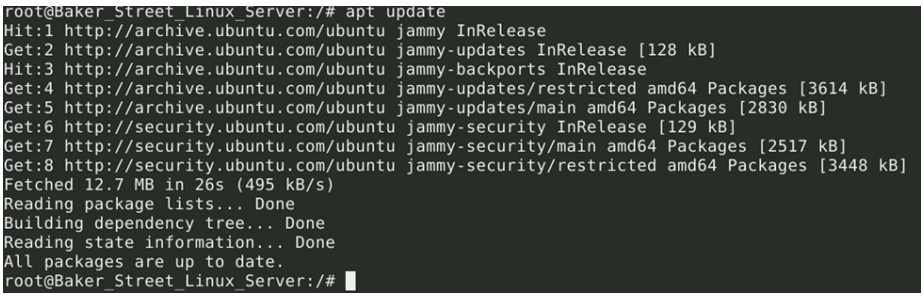
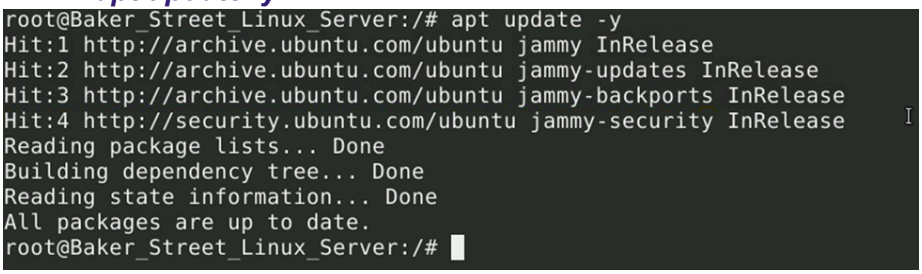
```
root@Baker_Street_Linux_Server:/tmp/scripts# chgrp research research_script.sh
root@Baker_Street_Linux_Server:/tmp/scripts# ls -l
total 0
-rwxr-xr-x 1 root research 0 Dec 18 17:23 research_script.sh
```

		Finance:
		From:
		`root@Baker_Street_Linux_Server:/# ls -l /home/mycroft/ /home/watson/`
		`/home/mycroft/:`
		`total 8`
		`-rw-r--r-- 1 root root  0 Dec 12 07:45 Engineering_script.sh_0.txt`
		`-rw-r--r-- 1 root root  0 Dec 12 07:45 Finance_script.sh_3.txt`
		`-rw-r--r-- 1 root root 48 Dec 12 07:45 Finance_script.sh_script1.sh`
		`-rw-r--r-- 1 root root 48 Dec 12 07:45 Finance_script.sh_script2.sh`
		`-rw-r--r-- 1 root root  0 Dec 12 07:45 deduction.doc_1.txt`
		`-rw-r--r-- 1 root root  0 Dec 12 07:45 deduction.doc_2.txt`
		
		`/home/watson/:`
		`total 8`
		`-rw-r--r-- 1 root root  0 Dec 12 07:45 Finance_script.sh_3.txt`
		`-rw-r--r-- 1 root root 47 Dec 12 07:45 Finance_script.sh_script1.sh`
		`-rw-r--r-- 1 root root 47 Dec 12 07:45 Finance_script.sh_script2.sh`
		`-rw-r--r-- 1 root root  0 Dec 12 07:45 deduction.doc_0.txt`
		`-rw-r--r-- 1 root root  0 Dec 12 07:45 deduction.doc_1.txt`
		`-rw-r--r-- 1 root root  0 Dec 12 07:45 deduction.doc_2.txt`
		`-rw-r--r-- 1 root root  0 Dec 12 07:45 my_file.txt`
		`root@Baker_Street_Linux_Server:/#`
		To:
		 

☑	Optional: Updating password hashing configuration	**=>** Updated the **packages** and **Libraries** and then verified that the current PAM library is updated and using **yescrypt** and **SHA512** encryption. ***/etc/pam.d/common-password*** 

		=> All the active accounts have **“y”** mentioned in their password hash, which defines that the passwords have been encrypted with **yescrypt SHA256**.
		`sherlock:$y$j9T$6jANuO79WQfItcj2GmYBp1$JrtkRnEgLc40CV4USoZG8Sn4kbZTzwlKC//DuQYuE74:20076:0:99999:7:::`
		`watson:$y$j9T$A/ZiK2441GxJ04IANXfrP1$ASd2JYgzO7x0WK1lt2ROgPT9H4gQAoWR4Xrlj3Y0qvC:20076:0:99999:7:::`
		`moriarty:!$y$j9T$nsZUbgKQz3RlRagkM2PSc.$ZdVcXZj600hp9S7tTnCfxig41FKQzvZwpUVP9YVr5k0:20076:0:99999:7:::`
		`mycroft:$y$j9T$xR9A4OY5d98RZY28esPXb0$zHylss04qqZ01cnIA8DnWOG1y4MWbtoVUqU.XPd/dU6:20076:0:99999:7:::`
		`mrs_hudson:!$y$j9T$egFL8sS4pSeI2vrOrHYfG/$67FjeLRAodkEku.QDWxTpexqXaYNZhDebsbKo3fEW1/:20076:0:99999:7:::`
		`sysadmin:$y$j9T$QxrjwaWUmssusnDUl/fSI1$tlE.40mdve.bRj9wGiqjR9XW1s0VU.wJYyoukfqIbM.:20076:0:99999:7:::`
		`toby:$y$j9T$AfU1Fl9ZDrOTHXjIxAGcJ0$7AbGOUMwGFfR41yYIbLWGRwbSDI.g2OvRd42BWtT4X3:20075:0:99999:7:::`
		`adler:$y$j9T$qJEZopy5V/7LTRrS4mmvr0$E1Dcdzp8WN9nMSIXgx4NMaRlQil/gKCwzvX1W8yu9ND:20075:0:99999:7:::`

☑	Auditing and securing SSH	**=>** Verified ***sshd_config*** file and found some below vulnarabilities:
		Port 22: Disabled
		Root login: Permitted
		Empty Passwords: Permitted
		Open Ports: 2222, 2223, 2224, 2225 & Protocol 1
		`#Port 22`
		`#LoginGraceTime 2m`
		`PermitRootLogin yes`
		`#PasswordAuthentication yes`
		`PermitEmptyPasswords yes`
		`# Example of overriding settings on a per-user basis`
		`#Match User anoncvs`
		`#  X11Forwarding no`
		`#  AllowTcpForwarding no`
		`#  PermitTTY no`
		`#  ForceCommand cvs server`
		`Port 2222`
		`Port 2223`
		`Port 2224`
		`Port 2225`
		`Protocol 1`
		`AllowUsers sherlock watson moriarty mycroft irene lestrade`
		
		=> Fixed the vulnerabilities by doing the following:
		Enabled Port 22
		● Port 22 used for Secure Shell(SSH) communication
		Disabled Root Login
		● No one with **Root** account will be able to access
		Disabled Empty Password login
		● No one will be able to login without password
		Disabled other vulnerable ports
		● Ports like 2222, 2223, 2224, 2225 can lead to backdoor access
		Applied Protocol 2
		● secure communications protocol that encompasses several layers of architecture, including transport, authentication, and connection
		
		`Port 22`
		`#AddressFamily any`

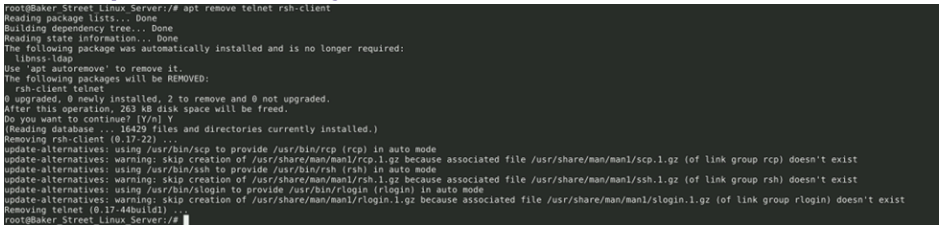
		
☑	Reviewing and updating system packages	**=> Updated** the package manager to get all the latest package versions. **Command:** • ***apt update***  **=> Updated** all installed packages to the latest version. **Command:** • ***apt update -y*** 
☑	Disabling unnecessary services	**=> Identified** the **unnecessary packages** that may impact the system vulnerability: **Found below packages:** • ***telnet***: telnet command in Linux is a networking tool that allows users to interact with other systems through text-based communication • ***rsh-client*****:** enables you to execute a command on a remote machine and receive the results on your local machine

```
root@Baker_Street_Linux_Server:/# cat package_list.txt | grep telnet
telnet/jammy,now 0.17-44build1 amd64 [installed]
root@Baker_Street_Linux_Server:/# cat package_list.txt | grep rsh-client
rsh-client/jammy,now 0.17-22 amd64 [installed]
```

=> Removed the packages along with their dependencies:

Command:

- ***apt remove telnet rsh-client***
- ***apt autoremove -y telnet rsh-client***




```
root@Baker_Street_Linux_Server:/# apt autoremove -y telnet rsh-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package 'telnet' is not installed, so not removed
Package 'rsh-client' is not installed, so not removed
The following packages will be REMOVED:
  libnss-ldap
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 182 kB disk space will be freed.
(Reading database ... 16409 files and directories currently installed.)
Removing libnss-ldap:amd64 (265-5ubuntu2) ...
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
root@Baker_Street_Linux_Server:/#
```

=> Installed below packages to **harden** the system:

- ***Ufw*: A firewall configuration tool in Linux**
- ***lynis*: A security auditing tool that scans systems running Linux and Unix based OS**
- ***tripwire*: a tool that monitors a Linux system for changes to critical files and directories**

Command:

- ***apt install package_name***

```
root@Baker_Street_Linux_Server:/# cat updated_package_list2.txt | grep -E ufw
ufw/jammy-updates,now 0.36.1-4ubuntu0.1 all [installed]
root@Baker_Street_Linux_Server:/# cat updated_package_list2.txt | grep -E lynis
lynis/jammy,now 3.0.7-1 all [installed]
root@Baker_Street_Linux_Server:/# cat updated_package_list2.txt | grep -E tripwire
tripwire/jammy,now 2.4.3.7-4 amd64 [installed]
```

=> Disabled & removed unnecessary services

- ***Samba(Smbd)***: a free, open-source software that allows Linux and Unix systems to share files, printers, and other resources with Windows systems
- ***Mysql***: MySQL is a relational database management system (RDBMS) that can be used in Linux to store, access, and process data

Commands:

- ***service smbd stop***
- ***service mysql stop***

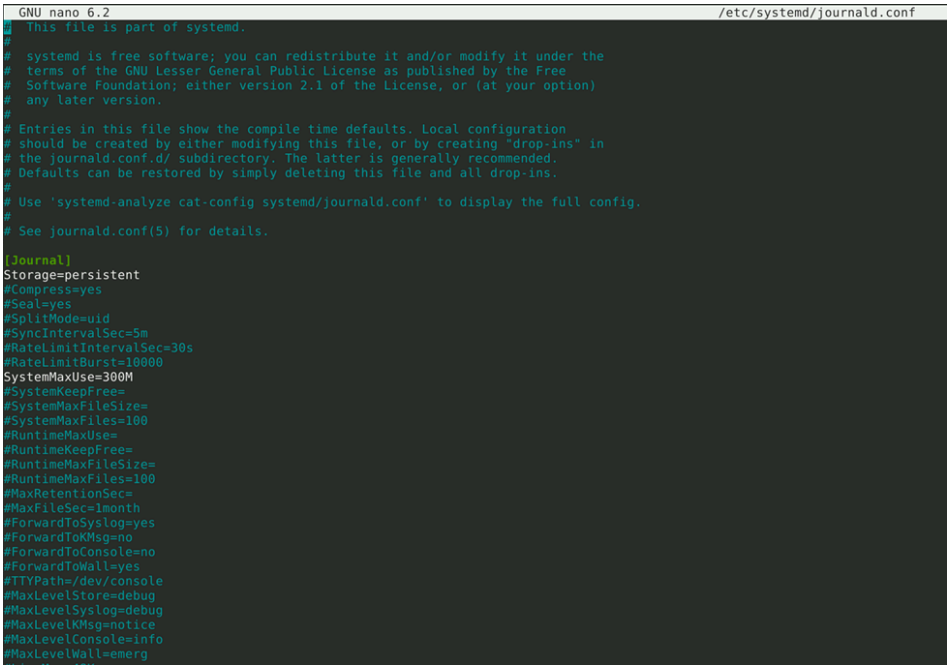
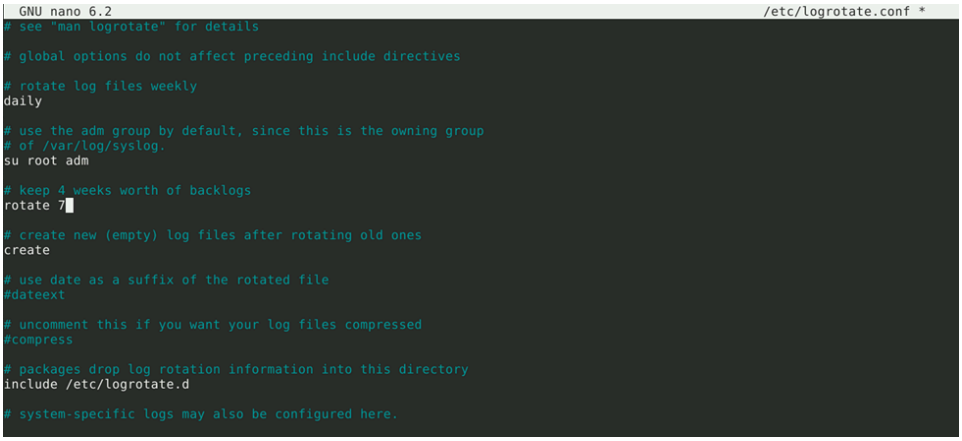
```
File  Edit  View  Search  Terminal  Help
top - 17:12:31 up 4 min,  0 users,  load average: 0.44, 0.39, 0.19
Tasks:  12 total,   1 running,  11 sleeping,   0 stopped,   0 zombie
%Cpu(s):  4.8 us,  1.2 sy,  0.0 ni, 91.5 id,  0.0 wa,  0.0 hi,  0.1 si,  2.4 st
MiB Mem :  15803.5 total,  12870.2 free,   1355.2 used,   1578.1 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used.  13945.6 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    208 mysql     20   0 2440212 392008  35224 S   0.3   2.4   0:01.33 mysqld
      1 root      20   0    4364   3280   3032 S   0.0   0.0   0:00.07 start_services.
     61 mysql     20   0    2892   1788   1628 S   0.0   0.0   0:00.00 mysqld_safe
    292 root      20   0   81516  16736  13688 S   0.0   0.1   0:00.03 smbd
    301 root      20   0   79040   9444   6668 S   0.0   0.1   0:00.00 smbd-notifyd
    302 root      20   0   79032   6552   3776 S   0.0   0.0   0:00.00 cleanupd
    303 root      20   0   80424  19416  16664 S   0.0   0.1   0:00.04 samba-bgqd
    309 root      20   0   65360   8456   6332 S   0.0   0.1   0:00.00 nmbd
    320 root      20   0   15432   3772   2152 S   0.0   0.0   0:00.00 sshd
    327 root      20   0    2824   1056    960 S   0.0   0.0   0:00.00 tail
    328 root      20   0    4628   3820   3240 S   0.0   0.0   0:00.02 bash
    336 root      20   0    7368   3408   2812 R   0.0   0.0   0:00.00 top
```

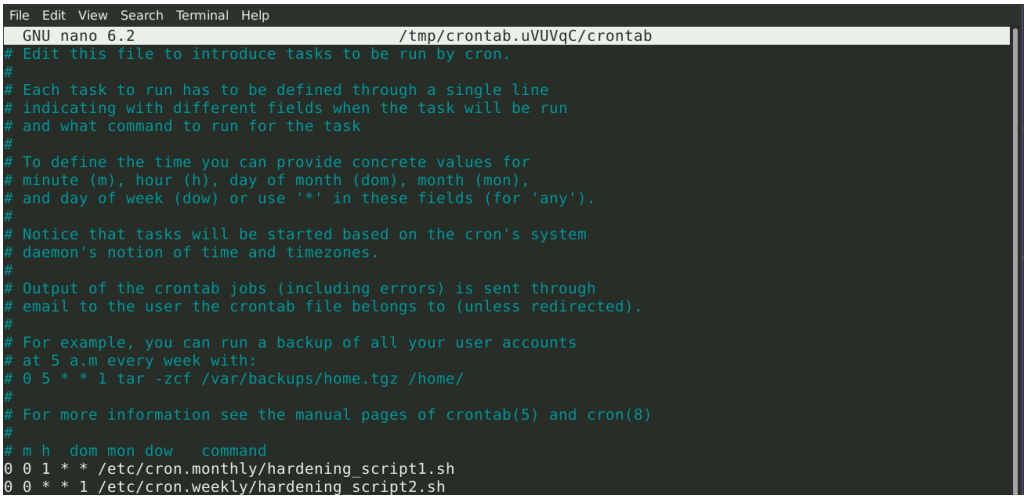
=> Removed packages after disabling the service

Commands:

- ***apt-get remove --purge mysql-server mysql-client mysql-common mysql-server-core-* mysql-client-core-****
- ***apt-get remove --purge samba samba-common samba-common-bin smbclient samba-libs***

```
The following packages will be REMOVED:
  samba*
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 17.6 MB disk space will be freed.
Do you want to continue? [Y/n] Y
(Reading database ... 17076 files and directories currently installed.)
Removing samba (2:4.15.13+dfsg-0ubuntu1.6) ...
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...
(Reading database ... 16878 files and directories currently installed.)
Purging configuration files for samba (2:4.15.13+dfsg-0ubuntu1.6) ...
dpkg: warning: while removing samba, directory '/var/lib/samba/printers/x64' not empty so not removed
dpkg: warning: while removing samba, directory '/var/lib/samba/printers/W32X86' not empty so not removed
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
root@Baker_Street_Linux_Server:/# service --status-all
 [ - ]  cron
 [ - ]  dbus
 [ ? ]  hwclock.sh
 [ ? ]  libnss-ldap
 [ - ]  openbsd-inetd
 [ - ]  postfix
 [ - ]  procps
 [ - ]  ssh
 [ - ]  ufw
root@Baker_Street_Linux_Server:/# top
```

☑	Enabling and configuring logging	**=> Updated** the **logging** process in system to harden the process **Path: /etc/systemd/journald.conf** ● Set "**storage=persistent**" This setting will save the logs locally on the machine ● Set "**systemMaxUse=300M**" This setting configures the maximum disk space the logs can utilize  **=>** Updated the log **Rotation** as well: **Path: /etc/logrotate.conf** ● Changed the log rotation from weekly to daily. ● Rotate out the logs after 7 days 

☑	Scripts created	Change the permission before running this script: **Commands:** ● ***chmod 744 hardening_script1.sh*** ● ***chmod 744 hardening_script2.sh*** **Download the script files below:** ● **hardening_script1.sh** ● **hardening_script2.sh**
☑	Scripts scheduled with cron	**Scheduled the scripts accordingly** **Command:** ● ***crontab -e*** **Hardening_script1.sh** scheduled to run at **midnight 1st day of the month** ● ***0 0 1 * * /etc/cron.monthly/hardening_script1.sh*** **Hardening_script2.sh** scheduled to run at **midnight every Monday** ● ***0 0 * * 1 /etc/cron.weekly/hardening_script2.sh*** 

```
File  Edit  View  Search  Terminal  Help
  GNU nano 6.2                          /tmp/crontab.uVUVqC/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/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
0 0 1 * * /etc/cron.monthly/hardening_script1.sh
0 0 * * 1 /etc/cron.weekly/hardening_script2.sh
```