



Project 1 Hardening Summary and Checklist

OS Information

Customer	Baker Street Corporation					
Hostname	<u>Baker_Street_Linux_Server</u>					
OS Version	<u>Ubuntu 22.04.5 LTS</u>					
Memory information	<u>total</u>	<u>used</u>	<u>free</u>	<u>shared</u>	<u>buff/cache</u>	<u>available</u>
	15Gi	1.3Gi	11Gi	204Mi	2.2Gi	13Gi
Uptime information	<u>up 47 minutes</u>					

Checklist

Completed	Activity	Script(s) used / Tasks completed / Screenshots
<input checked="" type="checkbox"/>	OS backup	<p>=> OS Backup:</p> <ul style="list-style-type: none"><code>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 /</code> <pre>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</pre>



Auditing users and groups

=> Deleted terminated users along with their Home directories

Command:

- ***deluser --remove-home username***

```
sherlock:$ysj9Tsk.8hsf0jC5sjhvbucTm41$hyQxtXp6zTsSm3FVokKfzHyu40tC8btm6rdXrXf5:20074:0:99999:7:::  
watson:$ysj9TsvtDjyGuA0eHCjVE7PK9T20$3dzLRqt8xlrQQx6jZ07uokC.h1.i8qbaohWfUjIm9.:20074:0:99999:7:::  
moriarty:$ysj9T$54/nwXR.yveVFMOjtkVoa.$JmXLzBKf67.kwCbtC.Cpn9D3dXFHbiQpQinmXrZezr3:20074:0:99999:7:::  
mycroft:$ysj9T$7DI/c9DLUjAVtIghNRhj.$c1wscwVqdNCNz0i0UST.l3/oF9.SZvdfvTqf3/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
```

		<p>=> To remove marketing group:</p> <ul style="list-style-type: none"> • <i>groupdel marketing</i>
☑	Updating and enforcing password policies	<ul style="list-style-type: none"> • => To update the password policies pwquality library is required <p>Password file: /etc/pam.d/common-password</p> <p>Installed the library with command:</p> <ul style="list-style-type: none"> • <i>apt install libpam-pwquality</i> <p>Updated password policies:</p> <ul style="list-style-type: none"> • Minimum 8 characters: <i>minlen=8</i> • At least one special character: <i>ocredit=-1</i> • Allow 2 retries: <i>retry=2</i> • At least one uppercase character: <i>ucredit=-1</i> <pre># 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</pre>
☑	Updating and enforcing sudo permissions	<p>=> Added the necessary paths in Sudoers file for users and groups:</p> <ul style="list-style-type: none"> • Full sudo privilege to Sherlock: <ul style="list-style-type: none"> ◦ <i>sherlock ALL=(ALL) NOPASSWD: ALL</i> • Watson and Mycroft should only have sudo privileges to run a script: <ul style="list-style-type: none"> ◦ <i>watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh</i> ◦ <i>watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh</i> • All employees who belong to the research group should have sudo privileges to run the following script: <ul style="list-style-type: none"> ◦ <i>%research ALL=(ALL:ALL) /tmp/scripts/research_script.sh</i> <pre># 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</pre>



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--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

/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--r-- 1 root root 49 Dec 12 07:45 game_is_afoot.txt_script1.sh
-rw-r--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--r-- 1 root root 51 Dec 12 07:45 elementary.txt_script1.sh
-rw-r--r-- 1 root root 51 Dec 12 07:45 elementary.txt_script2.sh

/home/mycroft:
total 48
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--r-- 1 root finance 48 Dec 12 07:45 Finance_script.sh_script1.sh
-rw-r--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--r-- 1 root root 49 Dec 12 07:45 deduction.doc_script1.sh
-rw-r--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-r--r-- 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--r-- 1 root root 45 Dec 12 07:45 elementary.txt_script1.sh
-rw-r--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-r--r-- 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--r-- 1 root finance 47 Dec 12 07:45 Finance_script.sh_script1.sh
-rw-r--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 \(-name "*.sh" -o -name "*.py" -o -name "*.pl" \) -iname "*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
```

		<p>Finance:</p> <p>From:</p> <pre> 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:/# </pre> <p>To:</p> <pre> root@Baker_Street_Linux_Server:/# chgrp finance /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:/# 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 finance 48 Dec 12 07:45 Finance_script.sh_script1.sh -rw-r--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/watson/: total 8 -rw-r--r-- 1 root root 0 Dec 12 07:45 Finance_script.sh_3.txt -rw-r--r-- 1 root finance 47 Dec 12 07:45 Finance_script.sh_script1.sh -rw-r--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 root@Baker_Street_Linux_Server:/# </pre>
<input checked="" type="checkbox"/>	Optional: Updating password hashing configuration	<p>=> Updated the packages and Libraries and then verified that the current PAM library is updated and using yescrypt and SHA512 encryption.</p> <p>/etc/pam.d/common-password</p> <pre> # Explanation of pam_unix options: # The "yescrypt" option enables # hashed passwords using the yescrypt algorithm, introduced in Debian # 11. Without this option, the default is Unix crypt. Prior releases # used the option "sha512": if a shadow password hash will be shared # between Debian 11 and older releases replace "yescrypt" with "sha512" # for compatibility. The "obscure" option replaces the old # "OBSOLETE CHECKS ENAB" option in login.defs. See the pam_unix manpage # for other options. # As of pam 1.0.1-6, this file is managed by pam-auth-update by default. # To take advantage of this, it is recommended that you configure any # local modules either before or after the default block, and use # pam-auth-update to manage selection of other modules. See # pam-auth-update(8) for details. # here are the per-package modules (the "Primary" block) password 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 password requisite pam_deny.so # prime the stack with a positive return value if there isn't one already; # this avoids us returning an error just because nothing sets a success code # since the modules above will each just jump around password required pam_permit.so # and here are more per-package modules (the "Additional" block) # end of pam-auth-update config </pre>

		<p>=> All the active accounts have “y” mentioned in their password hash, which defines that the passwords have been encrypted with yescrypt SHA256.</p> <pre> sherlock:\$ys\$9T\$6jANu079WQfItcj2GmYBp1\$JrtkRnEgLC40CV4USoZG8Sn4kbZTzwLKC//DuQYuE74:20076:0:99999:7::: watson:\$ys\$9T\$A/ZiK2441GxJ04IANXfrP1\$ASd2JYgz07x0WK1lt2R0gPT9H4gQaowR4Xrlj3Y0qvC:20076:0:99999:7::: moriarty:\$ys\$9T\$nsZUbqKQz3RlRagkM2PSc.\$ZdVcXZj600hp9S7tTnCfxig4lFKQzvZwpUVP9YVr5k0:20076:0:99999:7::: mycroft:\$ys\$9T\$xr9A40Y5d98RZY28esPXb0SzHylss04qqZ01cnIA8DnW0G1y4MwbtoVUqU.XPd/dU6:20076:0:99999:7::: mrs_hudson:\$ys\$9T\$egFL8s54pSeI2vr0rHYfG/\$67FjeLRAodkEku.QDwXtpexqXaYNZhDebsbKo3fEW1/:20076:0:99999:7::: sysadmin:\$ys\$9T\$QxrjwaWUmssusnDUL/fSI1stlE.40mdve.bRj9wGiqjR9XWls0VU.wJYyoukfqiBm.:20076:0:99999:7::: toby:\$ys\$9T\$AfU1fL9ZDr0THXjIXAGcJ0\$7AbG0UMwGFfR4lyYIbLWGRwbSDI.g20vRd42BwtT4X3:20075:0:99999:7::: adler:\$ys\$9T\$QJEZopy5V/7LTrR54mmvr0\$E1Dcdzp8WN9nMSIXgx4NMARlQ1L/gKCwzvX1W8yu9ND:20075:0:99999:7::: </pre>
<input checked="" type="checkbox"/>	<p>Auditing and securing SSH</p>	<p>=> Verified sshd_config file and found some below vulnerabilities:</p> <p>Port 22: Disabled</p> <p>Root login: Permitted</p> <p>Empty Passwords: Permitted</p> <p>Open Ports: 2222, 2223, 2224, 2225 & Protocol 1</p> <pre> #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 </pre> <p>=> Fixed the vulnerabilities by doing the following:</p> <p>Enabled Port 22</p> <ul style="list-style-type: none"> Port 22 used for Secure Shell(SSH) communication <p>Disabled Root Login</p> <ul style="list-style-type: none"> No one with Root account will be able to access <p>Disabled Empty Password login</p> <ul style="list-style-type: none"> No one will be able to login without password <p>Disabled other vulnerable ports</p> <ul style="list-style-type: none"> Ports like 2222, 2223, 2224, 2225 can lead to backdoor access <p>Applied Protocol 2</p> <ul style="list-style-type: none"> secure communications protocol that encompasses several layers of architecture, including transport, authentication, and connection <pre> Port 22 #AddressFamily any </pre>

		<pre>#LoginGraceTime 2m PermitRootLogin no # To disable tunneled clear text passwords, change to no here! #PasswordAuthentication yes PermitEmptyPasswords no #Port 2222 #Port 2223 #Port 2224 #Port 2225 Protocol 2 AllowUsers sherlock watson moriarty mycroft irene lestrade</pre>
☑	Reviewing and updating system packages	<p>=> Updated the package manager to get all the latest package versions.</p> <p>Command:</p> <ul style="list-style-type: none"> • apt update <pre>root@Baker_Street_Linux_Server:/# apt update Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease Get:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB] Hit:3 http://archive.ubuntu.com/ubuntu jammy-backports InRelease Get:4 http://archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [3614 kB] Get:5 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2830 kB] Get:6 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB] Get:7 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [2517 kB] Get:8 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [3448 kB] Fetched 12.7 MB in 26s (495 kB/s) Reading package lists... Done Building dependency tree... Done Reading state information... Done All packages are up to date. root@Baker_Street_Linux_Server:/#</pre> <p>=> Updated all installed packages to the latest version.</p> <p>Command:</p> <ul style="list-style-type: none"> • apt update -y <pre>root@Baker_Street_Linux_Server:/# apt update -y Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease Hit:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease Hit:3 http://archive.ubuntu.com/ubuntu jammy-backports InRelease Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease Reading package lists... Done Building dependency tree... Done Reading state information... Done All packages are up to date. root@Baker_Street_Linux_Server:/#</pre>
☑	Disabling unnecessary services	<p>=> Identified the unnecessary packages that may impact the system vulnerability:</p> <p>Found below packages:</p> <ul style="list-style-type: none"> • 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 remove telnet rsh-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libnss-ldap
Use 'apt autoremove' to remove it.
The following packages will be REMOVED:
  rsh-client telnet
0 upgraded, 0 newly installed, 2 to remove and 0 not upgraded.
After this operation, 263 kB disk space will be freed.
Do you want to continue? [Y/n] Y
(Reading database ... 16429 files and directories currently installed.)
Removing rsh-client (0.17-22) ...
update-alternatives: using /usr/bin/scp to provide /usr/bin/rcp (rcp) in auto mode
update-alternatives: warning: skip creation of /usr/share/man/man1/rcp.1.gz because associated file /usr/share/man/man1/scp.1.gz (of link group rcp) doesn't exist
update-alternatives: using /usr/bin/rsh to provide /usr/bin/rsh (rsh) in auto mode
update-alternatives: warning: skip creation of /usr/share/man/man1/rsh.1.gz because associated file /usr/share/man/man1/ssh.1.gz (of link group rsh) doesn't exist
update-alternatives: using /usr/bin/rlogin to provide /usr/bin/rlogin (rlogin) in auto mode
update-alternatives: warning: skip creation of /usr/share/man/man1/rlogin.1.gz because associated file /usr/share/man/man1/slogin.1.gz (of link group rlogin) doesn't exist
Removing telnet (0.17-44build1) ...
root@Baker_Street_Linux_Server:/#
```

```
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 smb 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 mysql
    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 mysql_safe
  292 root       20   0   81516  16736 13688 S   0.0   0.1   0:00.03 smb
  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
[ - ] procp
[ - ] 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

```
GNU nano 6.2 /etc/systemd/journald.conf
# This file is part of systemd.
#
# systemd is free software; you can redistribute it and/or modify it under the
# terms of the GNU Lesser General Public License as published by the Free
# Software Foundation; either version 2.1 of the License, or (at your option)
# any later version.
#
# Entries in this file show the compile time defaults. Local configuration
# should be created by either modifying this file, or by creating "drop-ins" in
# the journald.conf.d/ subdirectory. The latter is generally recommended.
# Defaults can be restored by simply deleting this file and all drop-ins.
#
# Use 'systemd-analyze cat-config systemd/journald.conf' to display the full config.
#
# See journald.conf(5) for details.

[Journal]
Storage=persistent
#Compress=yes
#Seal=yes
#SplitMode=uid
#SyncIntervalSec=5m
#RateLimitIntervalSec=30s
#RateLimitBurst=10000
SystemMaxUse=300M
#SystemKeepFree=
#SystemMaxFileSize=
#SystemMaxFiles=100
#RuntimeMaxUse=
#RuntimeKeepFree=
#RuntimeMaxFileSize=
#RuntimeMaxFiles=100
#MaxRetentionSec=
#MaxFileSec=1month
#ForwardToSyslog=yes
#ForwardToKMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelKMsg=notice
#MaxLevelConsole=info
#MaxLevelWall=emerg
```

=> 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

```
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

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

# keep 4 weeks worth of backlogs
rotate 7

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
#dateext

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may also be configured here.
```

<input checked="" type="checkbox"/>	Scripts created	<p>Change the permission before running this script:</p> <p>Commands:</p> <ul style="list-style-type: none"> • <i>chmod 744 hardening_script1.sh</i> • <i>chmod 744 hardening_script2.sh</i> <p>Download the script files below:</p> <ul style="list-style-type: none"> • hardening_script1.sh • hardening_script2.sh
<input checked="" type="checkbox"/>	Scripts scheduled with cron	<p>Scheduled the scripts accordingly</p> <p>Command:</p> <ul style="list-style-type: none"> • <i>crontab -e</i> <p>Hardening_script1.sh scheduled to run at midnight 1st day of the month</p> <ul style="list-style-type: none"> • <i>0 0 1 * * /etc/cron.monthly/hardening_script1.sh</i> <p>Hardening_script2.sh scheduled to run at midnight every Monday</p> <ul style="list-style-type: none"> • <i>0 0 * * 1 /etc/cron.weekly/hardening_script2.sh</i> <pre> 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 </pre>