

**OS Information**

| Customer | Baker Street Corporation |
| --- | --- |
| Hostname | Baker\_Street\_Linux\_Server |
| OS Version | 22.04.5 LTS |
| Memory information | Total: 16182408 Used: 1531764 Free: 8611544 |
| Uptime information | 01:24:33 up 1:45, 0 users, load average: 0.52, 0.35, 0.54 |

**Checklist**

| **Completed** | **Activity** | **Script(s) used / Tasks completed / Screenshots** |
| --- | --- | --- |
|  |  |  |
|  | OS backup | I created a backup of the important files on the OS by running the command: *tar -cvpzf /baker\_street\_backup.tar.gz --exclude=/baker\_street\_backup.tar.gz --exclude=/proc --exclude=/tmp --exclude=/mnt --exclude=/sys --exclude=/dev --exclude=/run /* |
|  | Auditing users and groups | I removed all staff who have been terminated by running the commands: sudo userdel -r lestrade sudo userdel -r irene sudo userdel -r mary sudo userdel -r gregson  : These are the remaining users  The users moriarty and mrs\_hudson are already locked so there is no need to lock them.  I unlocked all users who are employed by using the command: sudo usermod -U (toby, adler)  But first I had to add a password to the passwordless accounts using the command: sudo passwd (toby, adler)        I created a new group by using the command: groupadd (research)  I moved all the employees who were in the marketing department to the research group by using the commands: usermod -aG research (sherlock, watson, mycroft, moriarty, mrs\_hudson, toby, adler)  I removed the marketing group by using the command: delgroup marketing |
|  | Updating and enforcing password policies | I updated the password requirements for all users to have minimum 8 characters, at least one special character, allow 2 retries and at least one uppercase character by using the commands: nano /etc/login.defs  nano /etc/pam.d/common-password |
|  | Updating and enforcing sudo permissions | I ran the following command to edit the sudoers file: sudo visudo  Then i gave sherlock full sudo privileges by adding the line: sherlock ALL=(ALL) NOPASSWD:ALL  Watson and Mycroft only have sudo privileges to run a script: /var/log/logcleanup.sh. By adding the lines: watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh  watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh  I gave all employees who belong to the research group sudo privileges to run the script: /tmp/scripts/research\_script.sh. By adding the line: %research ALL=(ALL) NOPASSWD: /tmp/scripts/research\_script.sh |
|  | Validating and updating permissions on files and directories | In every user’s home directory there’s no files that have any world permissions to read, write, or execute by using the command: chmod 750 \*.sh ; chmod 640 \*.txt ; chmod 640 .bash\_logout ; chmod 640 .bashrc ; chmod 640 .profile  Updated files so that only members of the engineering, research and finance groups can view, edit, or execute their own files. Removed files with passwords saved inside.removed using the command: rm my\_file.txt    Removed using the command: rm my\_file.txt |
|  | Auditing and securing SSH | I configured SSH to **not** allow the ability to:  SSH with empty passwords, SSH with the root user and SSH with any other ports besides 22. By first nanoing into the /etc/ssh/sshd\_config file. Then changing the PermitEmptyPasswords from yes to no.      I restarted the SSH service to set the updates using the command *service ssh restart* |
|  | Reviewing and updating system packages | I ran the command apt update to update your package manager to make sure it has the latest version of all packages.    I ran the command apt upgrade -y to update all already installed packages to the latest versions. Then I created a file called package\_list.txt, which contains all installed packages    Then I removed all unnecessary dependencies of those packages with the command *apt autoremove -y*    I added the packages ufw, lynis and tripwire  I removed any package that had telnet and rsh-client |
|  | Disabling unnecessary services |  |
|  | Enabling and configuring logging | Cd into the /etc/systemd/. Then nano into the journald.conf file.  Edited the file: /etc/logrotate.conf with by changing the log rotation from weekly to daily,  and rotating out the logs after 7 days |
|  | Scripts created | I created the files hardening\_script1.sh and hardening\_script2.sh using the command touch    Then I nano into the hardening\_script1.sh file and updated the script.    Then I nano into the hardening\_script2.sh file and updated the script. |
|  | Scripts scheduled with cron | Using cron, I scheduled script 1 to run Once a month on the first of the month and script 2 to run once a week every Monday |