**OS Information**

| Heads up I took screenshots while I was going through the project but they never saved because my iCloud was full. So the pictures I have of my work are going back over work I already did. | |
| --- | --- |
| Customer | Baker Street Corporation |
| Hostname | **Ip-172-22-117-96** |
| OS Version | **Uname -a ubuntu** |
| Memory information | **Free -h total 3.7 Gi** |
| Uptime information | **Uptime Up 5 min 1 user** |

**Checklist**

| **Completed** | **Activity** | **Script(s) used / Tasks completed / Screenshots** |
| --- | --- | --- |
|  |  |  |
|  | OS backup | Sudo tar -cvpzf /baker\_street\_backup.tar.gz –exclude=/baker\_street\_backup.tar.gz –exclude=/proc –exclude=/tmp –exclude=/mnt –exclude=/sys –exclude=/dev –exclude=/run/ |
|  | Auditing users and groups | To Remove all staff who have been terminated:  deluser –remove-all-files lestrade. Then do that some command for irene,mary and gregson  To lock all user accounts on temporary leave.  usermod -L moriarty. Then do the same for mrs\_hudson as well.  To unlock any users who are employed.  usermod -U sherlock. Then do the same for Watson, Mycroft, Toby and adler.  To add the research group  addgroup research  To move all the employees who were in the marketing group to the research group.  To check who is in the marketing group:  cat /etc/group  Then to move mycroft to research  usermod -G research mycroft |
|  | Updating and enforcing password policies | Update the password requirements to minimum 8 characters, At least one special character, allow 2 retries and at least one uppercase character  nano /etc/pam.d/common-password  Password requisite pam\_pwqaulity.so minlen=8 ocredit=1 retry=2 ucredit=1  Chage -d 0 Toby  Chage -d 0 adler |
|  | Updating and enforcing sudo permissions | Sudo visudo |
|  | Validating and updating permissions on files and directories | FInd all files with world permissions:  Find /home -type f -perm 004  Only members of the engineering group can view edit or execute  Find /home -type f -name ‘\**engineering\**’ -exec chmod 070 {} \;  Only members of the research group can view edit or execute  Find /home -type f -name ‘*\*research\*’*’ -exec chmod 070 {} \;  Only members of the finance group can view edit or execute  Find /home -type f -name ‘\**finance\*’*’ -exec chmod 070 {} \;  Ls -a |
|  | Optional: Updating password hashing configuration |  |
|  | Auditing and securing SSH | Sudo nano /etc/ssh/sshd\_config  Restart the ssh service.  Sudo service ssh restart |
|  | Reviewing and updating system packages | Apt update  Apt upgrade -y  Create a file  Touch package\_list.txt  View all installed packages  Apt list –installed  Remove telnet and rsh-client packages  Sudo apt autoremove telnet rsh-client -y  Add the packages, ufw, lynis, tripwire  Sudo apt install ufw  Sudo apt install lynis  Sudo apt install tripwire  Lynis: can perform in depth security audits and identify vulnerabilities across multiple systems.  Ufw: It provides an easy to use interface for managing firewall rules on Linux systems  Tripwire: It focuses on file integrity and monitoring |
|  | Disabling unnecessary services | Service –status-all  List out all services and output into a file  Service –status-all > service\_list.txt  See if any of the services are running  Systemctl status mysql  Systemctl status samba  Stop,disable and remove the services  Systemctl stop mysql  Systemctl stop samba  Systemctl disable mysql  Systemctl disable samba |
|  | Enabling and configuring logging | Access the both of the files  Nano /etc/systemd/journal.conf  Nano /etc/logrotate.conf |
|  | Scripts created | Nano myscript.sh  Nano myscript2.sh  chmod +x  cp myscript.sh hardening\_script1.sh  cp myscript2.sh hardening\_script2.sh |
|  | Scripts scheduled with cron | Crontab -e |