Adolfo G. Chavez
OrbitzSaturn@gmail.com

Cybersecurity

Project 1 Hardening a Linux System

OS Information

Customer	Baker Street Corporation
Hostname	**172.22.117.219**
OS Version	**Ubuntu 24.04**
Memory information	**914 total // 742 used // 86 free**
Uptime information	**03:06:30 up 10 min, 1 user, load average: 0.00, 0.13, 0.13**

Checklist

Completed	Activity	Script(s) used / Tasks completed / Screenshots
☑	OS backup	Before i began my Linux System Hardening i gathered system info by running the following commands: **hostname:** prints the hostname **Uname -a :** prints the machine OS version **Free -h :** for memory information **Uptime:** shows uptime details I then ran **sudo tar -cvpzf /baker_street_backup.tar.gz --exclude=/baker_street_backup.tar.gz --exclude=/proc --exclude=/tmp --exclude=/mnt --exclude=/sys --excls -lh /baker_street_backup.tar.gzlude=/dev --exclude=/run /** and verified with ls **-lh /baker_street_backup.tar.gz** **Screenshots:** https://imgur.com/a/AVccplq

☑	Auditing users and groups	I began to remove all terminated employees by running **userdel -r <username>** and i verified using **id <username>** I then proceeded locking all accounts on temp leave using **sudo usermod -s /usr/sbin/nologin <username>** and i unlocked all required employees using **sudo passwd -u <username>** I create a new group using **sudo groupadd <groupname>** and i move the users from the previous group using **sudo gpasswd -a <user> research** I then remove the previous group using **sudo groupdel <groupname>** **Screenshots:** https://imgur.com/a/4SryQhW
☑	Updating and enforcing password policies	I begin to implement a password policy to update the minimum complexity and to force users to update their passwords on the next login. I edit the **/etc/pam.d/common-password** file using: **password requisite pam_pwquality.so retry=2 minlen=8 ucredit=-1 ocredit=-1** I then proceed with forcing password reset on all Users **Screenshots:** https://imgur.com/a/mO7KrLm
☑	Updating and enforcing sudo permissions	I used the command: **sudo visudo** to edit the sudoer file and i assigned necessary permissions and removed unauthorized permissions using: **sherlock ALL=(ALL:ALL) ALL** **watson,mycroft ALL=(ALL:ALL) /var/log/logcleanup.sh** **%research ALL=(ALL:ALL) /tmp/scripts/research_script.sh** I verify the permission changes using **su <username>** **Screenshot:** https://imgur.com/a/Sb5p8jw
☑	Validating and updating permissions on files and directories	I began by confirming that world permissions were removed for all users using : **find /home -type f -perm -0077 -exec chmod o-rwx {} \;** and i confirm using **find /home -type f -perm -0077** I used: **find /home -type f -iname '*engineering*'** to locate any files with engineering in the name. I then made sure that engineering is the only group with read write execute permissions. I proceeded to do the same process with the rest of the groups. I verify **Screenshots: https://imgur.com/a/i0Jz3Aa**

☑	Auditing and securing SSH	I edited the **/etc/ssh/sshd_config** and i configured SSH to not allow communication with any port besides **port 22** using the # symbol to comment these unnecessary ports out. I also configured the SSH config file to not allow communication with the root user and enabled SSH Protocol 2 I removed the ability to login with an empty password I then applied these changes using the **sudo systemctl restart ssh command** **Screenshot: https://imgur.com/a/JBmvQ9f**
☑	Reviewing and updating system packages	I first started with running an **apt update && apt upgrade -y** and i verified by running the same command. I then created a list of installed packages to help identify potential insecure packages and remove them. I identified Telnet and Rsh client which i removed using **sudo apt remove telnet rsh-client -y** , and i used **sudo apt autoremove -y** to remove unnecessary dependencies. I proceeded to install Tripwire to further harden the system by monitoring file integrity. I used : **sudo apt install ufw lynis tripwire -y** Screenshots: https://imgur.com/a/WKMjJw2
☑	Disabling unnecessary services	I created a text file to check all running services and identified mysql and samba using **systemctl status <service>** These services shouldnt be running on this system so i stopped and disabled them using **sudo systemctl stop <service> sudo systemctl disable <service>** I then ran **sudo apt remove mysql-server samba -y** to remove these services **Screenshots: https://imgur.com/a/36PWqdA**
☑	Enabling and configuring logging	I started by opening the **/etc/systemd/journald.conf** file using **nano** and setting **storage** to **persistent** and **SystemMaxUse** to **300M** Edited the **lograte.conf** file so that logs rotate daily **Screenshots: https://imgur.com/a/2BCp5Pd**

☑	Automation Scripts created	I created two bash script using bash and made it executable to be able to run the hardening tasks we have completed. Screenshots: Script 1 - https://imgur.com/a/eXsDAj0 Script 2 - https://imgur.com/a/HF9z8Ub
☑	Scripts scheduled with cron	I ran **sudo crontab -e** to edit the current cron jobs and added both scripts to the cron jobs. I configured Script 1 to run on every 1st of the month and script 2 to run on every Monday **Screenshots: https://imgur.com/a/bW9OEqB**