Week 4 Homework Submission File: Linux Systems Administration

Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on /etc/shadow should allow only root read and write access.
    - Command to inspect permissions: ls -l shadow
    - Command to set permissions (if needed): sudo chmod 600 shadow
2. Permissions on /etc/gshadow should allow only root read and write access.
    - Command to inspect permissions:ls -l gshadow
    - Command to set permissions (if needed): sudo chmod 600 gshadow
3. Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.
    - Command to inspect permissions: ls -l group
    - Command to set permissions (if needed): sudo chmod 644 group
4. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.
    - Command to inspect permissions: ls -l passwd
    - Command to set permissions (if needed): sudo chmod 644 group

Step 2: Create User Accounts

1. Add user accounts for sam, joe, amy, sara, and admin.
    - Command to add each user account (include all five users):
    - Sudo adduser sam
    - Sudo adduser joe
    - Sudo adduser amy
    - Sudo adduser sara
    - Sudo adduser admin

2. Ensure that only the admin has general sudo access.

    - Command to add admin to the sudo group:
    - Sudo usermod -aG sudo admin

Step 3: Create User Group and Collaborative Folder

1. Add an engineers group to the system.

    - Command to add group:
    - Sudo groupadd engineers
2. Add users sam, joe, amy, and sara to the managed group.

    - Command to add users to engineers group (include all four users):
    - Sudo adduser sam engineers or sudo usermod -G engineers sam
    - Sudo adduser joe engineers or sudo usermod -G engineers joe
    - Sudo adduser amy engineers or sudo usermod -G engineers amy
    - Sudo adduser sara engineers or sudo usermod -G engineers sara

3. Create a shared folder for this group at /home/engineers.cd
    - Command to create the shared folder: sudo mkdir /home/engineers
4. Change ownership on the new engineers' shared folder to the engineers group.

    - Command to change ownership of engineer's shared folder to engineer group:
    - Sudo chown :engineers engineers

Step 4: Lynis Auditincdg

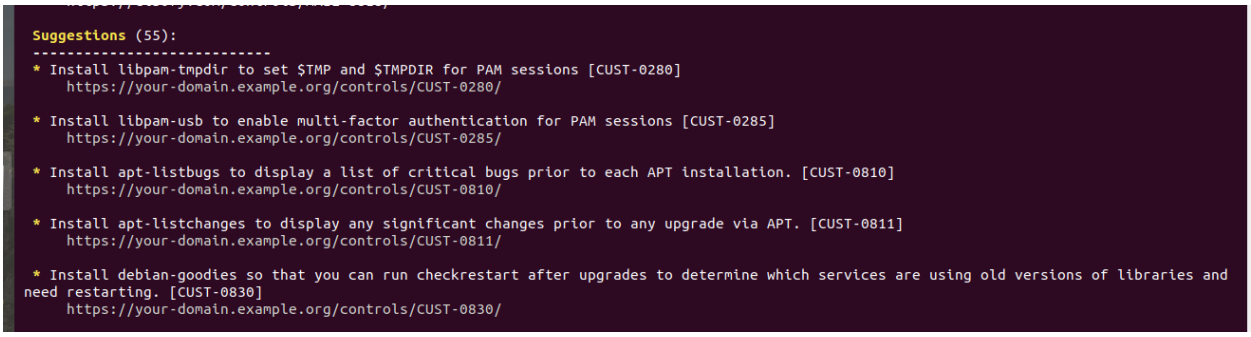
1. Command to install Lynis: sudo apt install lynis

2. Command to see documentation and instructions: man lynis

3. Command to run an audit: sudo lynis audit system

4. Provide a report from the Lynis output on what can be done to harden the system.

    - Screenshot of report output:



Bonus

1. Command to install chkrootkit:
2. Command to see documentation and instructions:
3. Command to run expert mode:
4. Provide a report from the chrootkit output on what can be done to harden the system.
    - Screenshot of end of sample output:
