**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: ***The permission for shadow is root access. The command to inspect the permissions for shadow is “ls -l /etc/shadow”***
   * Command to set permissions (if needed): ***Not applicable; the permissions are already set to root access.***
2. Permissions on /etc/gshadow should allow only root read and write access.
   * Command to inspect permissions: ***The permission for gshadow is root access. The command to inspect the permission for gshadow is “ls -l /etc/gshadow”***
   * Command to set permissions (if needed): ***Not applicable; the permissions are already set to root access.***
3. Permissions on /etc/group should allow root read and write access and allow everyone else read access only.
   * Command to inspect permissions: ***The permission on the /etc/group is root read and write access and allowing everyone else read access only. The command to inspect the permission for /etc/group is “ls -l /etc/group”***
   * Command to set permissions (if needed): ***Not applicable; the command to set the permissions is already completed. If the permissions had not been set, the command to set the permissions would be: “sudo chmod 644 /etc/group”***
4. Permissions on /etc/passwd should allow root read and write access and allow everyone else read access only.
   * Command to inspect permissions: ***The permission on the /etc/passwd allows root read/write access and everyone else read only access. The command to inspect the permission is “ls -l /etc/passwd”***
   * Command to set permissions (if needed): ***Not applicable; the command to set the permissions is already completed. If the permissions had not been set, the command to set the permissions would be: “sudo chmod 644 /etc/passwd”***

**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):
     1. Command for Sam: ***“sudo useradd sam” “ls”***
     2. Command for Joe: ***“sudo useradd joe” “ls”***
     3. Command for Amy: ***“sudo useradd amy” “ls”***
     4. Command for Sara: ***“sudo useradd sara” “ls”***
     5. Command for admin: ***“sudo useradd admin” “ls”***
2. Ensure that only the admin has general sudo access.
   * Command to add admin to the sudo group: ***To add the admin to the sudo group, the command would be: “sudo usermod -a -G 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” “ls”***
2. Add users sam, joe, amy, and sara to the managed group.
   * Command to add users to engineers group (include all four users):
     1. Add Sam to the engineers group command: ***“sudo usermod -a -G engineers sam” “ls”***
     2. Add Joe to the engineers group command line: ***“sudo usermod -a -G engineers joe” “ls”***
     3. Add Amy to the engineers group command line: ***“sudo usermod -a -G engineers amy” “ls”***
     4. Add Sara to the engineers group command line: ***“sudo usermod -a -G engineers sara” “ls”***
3. Create a shared folder for this group at /home/engineers.
   * Command to create the shared folder: *“****sudo mkdir -p /home/engineers” “ls”***
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 chmod -R 775 /home/engineers” “ls”***

**Step 4: Lynis Auditing**

1. Command to install Lynis: ***“sudo apt-get install lynis -y”***
2. Command to see documentation and instructions: ***“sudo lynis show commands”***

Text

Description automatically generated

1. Command to run an audit: ***“sudo lynis audit system”***
2. Provide a report from the Lynis output on what can be done to harden the system.
   * Screenshot of report output:

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated