# Week 4 Homework Submission File: Linux Systems Administration

### Step 1: Ensure Permissions on Sensitive Files

1. Permissions on `/etc/shadow` should allow only `root` read and write access.

- Command to inspect permissions: ls -l /etc/passwd

- Command to set permissions (if needed): not needed

2. Permissions on `/etc/gshadow` should allow only `root` read and write access.

- Command to inspect permissions: ls -l /etc/passwd

- Command to set permissions (if needed): not needed

3. Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else read$

- Command to inspect permissions: ls -l /etc/passwd

- Command to set permissions (if needed): not needed

4. Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else rea$

- Command to inspect permissions: ls -l /etc/passwd

- Command to set permissions (if needed): not needed

sysadmin@UbuntuDesktop:/etc$ ls -l shadow

-rw------- 1 root shadow 2888 Jul 14 10:16 shadow

sysadmin@UbuntuDesktop:/etc$ ls -l gshadow

-rw------- 1 root shadow 1076 Jul 14 10:16 gshadow

sysadmin@UbuntuDesktop:/etc$ ls -l /etc/group

-rw-r--r-- 1 root root 1303 Jul 14 10:16 /etc/group

sysadmin@UbuntuDesktop:/etc$ ls -l /etc/passwd

-rw-r--r-- 1 root root 3207 Aug 22 11:56 /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): adduser sam, adduser joe, adduser amy$

2. Force users to create 16-character passwords incorporating numbers and symbols.

- Command to edit `pwquality.conf` file: sudo nano pwquality.conf

- Updates to configuration file:

# Minimum acceptable size for the new password (plus one if

# credits are not disabled which is the default). (See pam\_cracklib manual.)

# Cannot be set to lower value than 6.

minlen = 16

3. Force passwords to expire every 90 days.

- Command to to set each new user's password to expire in 90 days (include all five users):

sudo chage -M 90 sam

sudo chage -M 90 joe

sudo chage -M 90 amy

sudo chage -M 90 sara

sudo chage -M 90 admin

4. Ensure that only the `admin` has general sudo access.

- Command to add `admin` to the `sudo` group:

usermod -aG sudo admin

### Step 3: Create User Group and Collaborative Folder

1. Add an `engineers` group to the system.

- Command to add group:

addgroup engineers

2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.

- Command to add users to `engineers` group (include all four users):

usermod -aG engineers joe

usermod -aG engineers amy

usermod -aG engineers sam

usermod -aG engineers sara

3. Create a shared folder for this group at `/home/engineers`.

- Command to create the shared folder:

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:

chgrp -hR engineers engineers

5. Add the SGID bit and the sticky bit to allow collaboration between engineers in this directory.

- Command to set SGID and sticky bit to shared folder:

sudo chmod g+s,o+t engineers

### Step 4: Lynis Auditing

1. Command to install Lynis:

sudo apt-get install lynis

2. Command to see documentation and instructions:

sudo man lynis

3. Command to run an audit:

lynis audit system

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

- Screenshot of report output:

