Submission File: Linux Systems Administration Homework

Ensure permissions on sensitive files

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

- **Command to inspect permissions**: ls -l /etc/shadow

- **Command to Set Permissions (if needed)**: If needed, sudo chmod 600 /etc/shadow

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

- **Command to inspect permissions**: ls -l /etc/gshadow

- **Command to Set Permissions (if needed)**: If needed, sudo chmod 600 /etc/gshadow

Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else `read` access only:

- **Command to inspect permissions**: ls -l /etc/group

- **Command to Set Permissions (if needed)**: If needed, sudo chmod 644 /etc/group

Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else `read` access only:

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

- **Command to set permissions (if needed)**: If needed, chmod 644 /etc/passwd

Create user accounts

Add user accounts `sam`, `joe`, `amy`, `sara`, and `admin`

- **Command to add each user account (please include all 5)**:
  1) sudo useradd -m -d /sam sam
  2) sudo useradd -m -d /joe joe
  3) sudo useradd -m -d /amy amy
  4) sudo useradd -m -d /sara sara
  5) sudo useradd -m -d /admin admin

Force users to create 16 character passwords incorporating numbers and symbols

- **Command to edit `pwquality.conf` file**: sudo nano /etc/security/pwquality.conf

- **Updates to configuration file**:
  1) uncomment and change minlen = 8 to minlen = 16
  2) uncomment and make minclass = 4

Force passwords to expire every 90 days:

- **Command to to set each new user's password to expire in 90 days (please include all 5)**:

```
   1) sudo chage -M 90 sam
   2) sudo chage -M 90 joe
   3) sudo chage -M 90 amy
   4) sudo chage -M 90 sara
   5) sudo chage -M 90 admin
```

Ensure that only the `admin` has general sudo access:
   type "sudo visudo" and make sure there are no users at the bottom of the file. Delete or comment those lines.

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

```
   sudo usermod -aG sudo admin
```

Create user group and collaborative folder

Add a `engineers` group to the system.

```
   sudo groupadd engineers
```

- **Command**:

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

- **Command to add users to `engineers` group (please include all 4)**:

```
   1) sudo usermod -a -G engineers sam
   2) sudo usermod -a -G engineers joe
   3) sudo usermod -a -G engineers amy
   4) sudo usermod -a -G engineers sara
```

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

- **Command to create the shared folder**:
   sudo mkdir -p /home/engineers. After this is done, the permissions are 755. The shared folder should have
   full permissions for the group so do this afterwards: "sudo chmod g+w /home/engineers"

Change the group on the engineers directory to the `engineers` group

- **Command to change ownership of engineer's shared folder to engineer group**:

```
   sudo chgrp -R engineers /home/engineers
```

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**:
   The current permissions for the group directory is 775, so let's not change that but add SGID and the

sticky bit: "sudo chmod 3775 /home/engineers"   (sticky bit is 1### and SGID is 2###; 2 + 1 = 3)

Lynis auditing

Install and run `lynis`

- **Command to install `lynis`:**
  sudo apt-get install lynis

- **Command to see options:**
  man lynis

- **Command to run an audit**
  sudo lynis audit system

Provide a report from `lynis` output on what more could be done to harden the system.

- **Screenshot of report output**:
  sudo lynis audit system > lynisOutput1.txt. Refer to the file in the folder for more info.

Bonus: Check for Root Kits

Install and run `chkrootkit`.

- **Command to install `chkrootkit`**
  We can install chkrootkit from an Ubuntu repository using command:
  sudo apt-get install chkrootkit

- **Command to see options:**
  man chkrootkit

- **Command to run expert mode:**
  sudo chkrootkit -x

- **Screenshot of End of Sample Output:**
  Refer to the file in the submitted directory. There are two files, 1 png and 1 pdf.
  1) bonus - screenshotOfEndOfSampleOutput.png
  2) bonus - screenshotOfEndOfSampleOutput.pdf

Gavin's Corner

Interesting Linux Command: fortune. The program will put up a random fortune for the day. Use the -s option to tell
the fortune command to generate only small sized messages. To install, type "sudo apt-get install fortune-mod"