

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 /etc/shadow`
 - Command to set permissions (if needed):

`sudo chmod 600 /etc/shadow`
2. Permissions on `/etc/gshadow` should allow only root read and write access.
 - Command to inspect permissions:

`ls -l /etc/shadow`
 - Command to set permissions (if needed):

`sudo chmod 600 /etc/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 /etc/group`
 - Command to set permissions (if needed):

`sudo chmod 604 /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:

`Ls -l /etc/passwd`
 - Command to set permissions (if needed):

`sudo chmod 604 /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):

```
sudo useradd sam
sudo useradd joe
sudo useradd amy
sudo useradd sara
sudo useradd admin
```

**** OR****

```
sudo adduser --system sam
sudo adduser --system joe
sudo adduser --system amy
sudo adduser --system sara
sudo adduser --system 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 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):

```
sudo usermod -aG engineers sam
sudo usermod -aG engineers joe
sudo usermod -aG engineers amy
sudo usermod -aG engineers sara
```

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

- 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 /home/engineers
```

Step 4: Lynis Auditing

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. There are 6 warnings and 53 suggestions given to help ameliorate hardening the system. Please find below screenshots of (some) of these findings (report output)

```
Suggestions (53):
-----
* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]
  https://your-domain.example.org/controls/CUST-0280/

* Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]
  https://your-domain.example.org/controls/CUST-0285/

* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [CUST-0810]
  https://your-domain.example.org/controls/CUST-0810/

* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CUST-0811]
  https://your-domain.example.org/controls/CUST-0811/

* Install debian-goodies so that you can run checkrestart after upgrades to determine which services are using old versions of libraries and need restarting. [CUST-0830]
  https://your-domain.example.org/controls/CUST-0830/

* Install debconf-utils to allow for the configuration of debconf modules. [CUST-0831]
  https://your-domain.example.org/controls/CUST-0831/
```

```
Warnings (6):
-----
! Version of Lynis is very old and should be updated [LYNIS]
  https://cisofy.com/controls/LYNIS/

! Multiple users with UID 0 found in passwd file [AUTH-9204]
  https://cisofy.com/controls/AUTH-9204/

! Multiple accounts found with same UID [AUTH-9208]
  https://cisofy.com/controls/AUTH-9208/

! No password set for single mode [AUTH-9308]
  https://cisofy.com/controls/AUTH-9308/

! Found one or more vulnerable packages. [PKGS-7392]
  https://cisofy.com/controls/PKGS-7392/

! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
  https://cisofy.com/controls/MAIL-8818/
```

Bonus

1. Command to install chkrootkit:

```
sudo apt install chkrootkit
```

2. Command to see documentation and instructions:

man chkrootkit

3. Command to run expert mode:

```
sudo chkrootkit -x
```

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

```
sudo chkroot
```

- Screenshot of end of sample output:

```
| sysadmin      2790 tty2    /usr/lib/gnome-settings-daemon/gsd-printer  
| sysadmin      2712 tty2    /usr/lib/gnome-settings-daemon/gsd-rfkill  
| sysadmin      2713 tty2    /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy  
| sysadmin      2717 tty2    /usr/lib/gnome-settings-daemon/gsd-sharing  
| sysadmin      2721 tty2    /usr/lib/gnome-settings-daemon/gsd-smartcard  
| sysadmin      2723 tty2    /usr/lib/gnome-settings-daemon/gsd-sound  
| sysadmin      2724 tty2    /usr/lib/gnome-settings-daemon/gsd-wacom  
| sysadmin      2725 tty2    /usr/lib/gnome-settings-daemon/gsd-xsettings  
| sysadmin      2619 tty2    ibus-daemon --xim --panel disable  
| sysadmin      2623 tty2    /usr/lib/ibus/ibus-dconf  
| sysadmin      2882 tty2    /usr/lib/ibus/ibus-engine-simple  
| sysadmin      2625 tty2    /usr/lib/ibus/ibus-x11 --kill-daemon  
| sysadmin      2813 tty2    nautilus-desktop  
! root          13265 pts/0   /bin/sh /usr/sbin/chkrootkit  
! root          14091 pts/0   ./chkutmp  
! root          14093 pts/0   ps axk tty,ruser,args -o tty,pid,ruser,args  
! root          14092 pts/0   sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"  
! root          13264 pts/0   sudo chkrootkit  
! sysadmin      3111 pts/0   bash  
  
chkutmp: nothing deleted  
Checking `OSX_RSPLUG'...                               not tested  
  
sysadmin@UbuntuDesktop:~$
```