

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

## 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/gshadow`**
  - 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 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: **`ls -l /etc/passwd`**
  - Command to set permissions (if needed): **`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):
    - **`sudo useradd sam`**
    - **`sudo useradd joe`**
    - **`sudo useradd amy`**
    - **`sudo useradd sara`**
    - **`sudo useradd admin`**

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

- Command to add admin to the sudo group:
  - **sudo usermod -G 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 -G engineers sam**
    - **sudo usermod -G engineers joe**
    - **sudo usermod -G engineers amy**
    - **sudo usermod -G 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:
  - **sudo lynis --help**
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:

```

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 needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [CUST-0831]
  https://your-domain.example.org/controls/CUST-0831/

* Install debsecan to generate lists of vulnerabilities which affect this installation. [CUST-0870]
  https://your-domain.example.org/controls/CUST-0870/

* Install debsums for the verification of installed package files against MD5 checksums. [CUST-0875]
  https://your-domain.example.org/controls/CUST-0875/

* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
  https://cisofy.com/controls/DEB-0880/

* Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
  https://cisofy.com/controls/BOOT-5122/

* Run pwck manually and correct any errors in the password file [AUTH-9228]
  https://cisofy.com/controls/AUTH-9228/

* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
  https://cisofy.com/controls/AUTH-9262/

* Configure minimum password age in /etc/login.defs [AUTH-9286]
  https://cisofy.com/controls/AUTH-9286/

* Configure maximum password age in /etc/login.defs [AUTH-9286]
  https://cisofy.com/controls/AUTH-9286/

* Set password for single user mode to minimize physical access attack surface [AUTH-9308]
  https://cisofy.com/controls/AUTH-9308/

* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
  https://cisofy.com/controls/AUTH-9328/

```

## Bonus

1. Command to install chkrootkit:
  - **sudo apt install chkrootkit**
2. Command to see documentation and instructions:
  - **sudo chkrootkit --help**
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.
  - Screenshot of end of sample output:

```

File Edit View Search Terminal Help
! gdm 2205 tty1 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm 2213 tty1 /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm 2216 tty1 /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm 2222 tty1 /usr/lib/gnome-settings-daemon/gsd-sound
! gdm 2228 tty1 /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm 2155 tty1 /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm 2118 tty1 ibus-daemon --xim --panel disable
! gdm 2121 tty1 /usr/lib/ibus/ibus-dconf
! gdm 2288 tty1 /usr/lib/ibus/ibus-engine-simple
! gdm 2124 tty1 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 2368 tty2 /usr/lib/xorg/xorg vt2 displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeppty -verbose 3
! sysadmin 2366 tty2 /usr/lib/gdm3/gdm-X-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin 2398 tty2 /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin 2559 tty2 /usr/bin/gnome-shell
! sysadmin 3853 tty2 /usr/bin/gnome-software --gapplication-service
! sysadmin 2740 tty2 /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin 2741 tty2 /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin 2734 tty2 /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin 2743 tty2 /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin 2828 tty2 /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin 2746 tty2 /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin 2753 tty2 /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin 2754 tty2 /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin 2701 tty2 /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin 2702 tty2 /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin 2706 tty2 /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin 2784 tty2 /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin 2707 tty2 /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin 2710 tty2 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin 2713 tty2 /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin 2717 tty2 /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin 2718 tty2 /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin 2721 tty2 /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin 2724 tty2 /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin 2605 tty2 ibus-daemon --xim --panel disable
! sysadmin 2609 tty2 /usr/lib/ibus/ibus-dconf
! sysadmin 2913 tty2 /usr/lib/ibus/ibus-engine-simple
! sysadmin 2613 tty2 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 2825 tty2 nautilus-desktop
! sysadmin 3800 pts/0 bash
! root 24801 pts/1 /bin/sh /usr/sbin/chkrootkit -x
! root 25234 pts/1 ./chkutmp
! root 25236 pts/1 ps axk tty,ruser,args -o tty,pid,ruser,args
! root 25235 pts/1 sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root 24800 pts/1 sudo chkrootkit -x
! sysadmin 3809 pts/1 bash
chkutmp: nothing deleted
not tested
sysadmin@UbuntuDesktop:/etc$

```