

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.
 - o Command to inspect permissions: `ls -l /etc/shadow`
 - o Command to set permissions (if needed): `sudo chmod 600 /etc/shadow`
2. Permissions on `/etc/gshadow` should allow only `root` read and write access.
 - o Command to inspect permissions: `ls -l /etc/gshadow`
 - o 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.
 - o Command to inspect permissions: `ls -l /etc/group`
 - o 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.
 - o Command to inspect permissions: `ls -l /etc/passwd`
 - o 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`.
 - o Command to add each user account (include all five users): `sudo adduser sam, sudo adduser joe, sudo adduser amy, sudo adduser sara, sudo adduser admin`
2. Ensure that only the `admin` has general sudo access.
 - o Command to add `admin` to the `sudo` group: `sudo usermod -aG sudo admin`

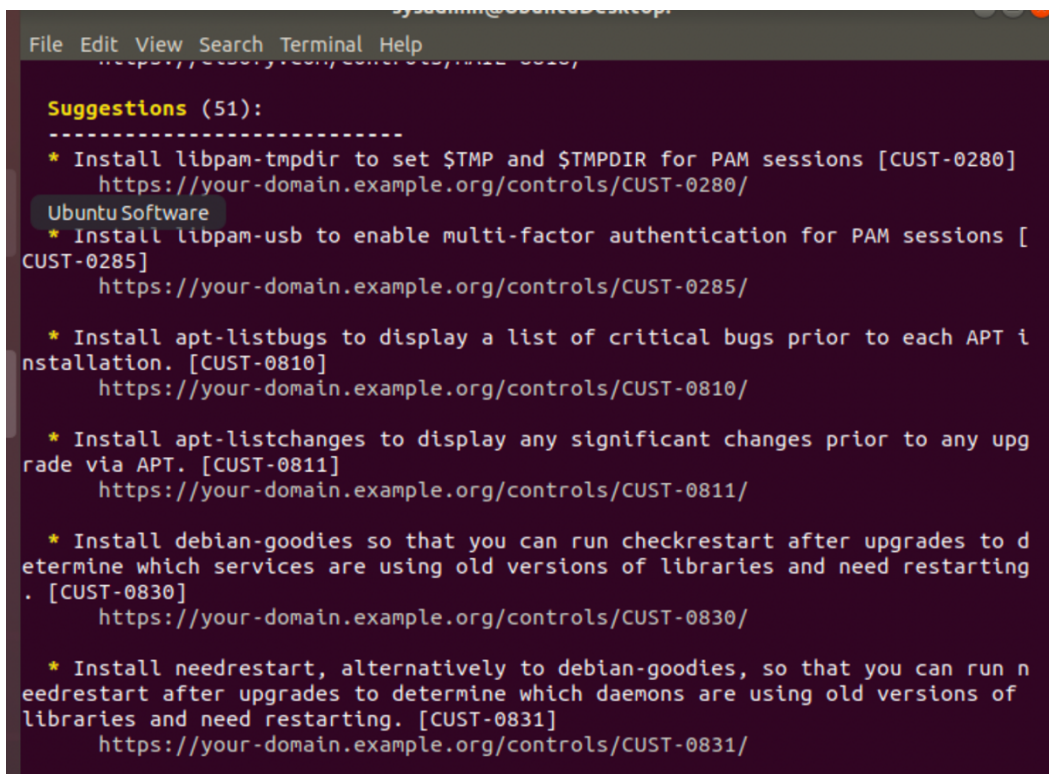
Step 3: Create User Group and Collaborative Folder

1. Add an `engineers` group to the system.
 - o Command to add group: `sudo addgroup engineers`

2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.
 - o 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`.
 - o Command to create the shared folder: `mkdir /home/engineers`
4. Change ownership on the new engineers' shared folder to the `engineers` group.
 - o 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.
 - o Screenshot of report output:



The screenshot shows a terminal window with a dark background and light-colored text. The window title is "lynis@ubuntu-desktop". The terminal output displays a section titled "Suggestions (51):" followed by a list of recommendations. Each recommendation is preceded by an asterisk and includes a brief description, a reference code in brackets, and a URL. The recommendations listed are:

- * 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/>

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.
 - o Screenshot of end of sample output:

```
/bin/ls: cannot access '//sbin/rootedoor': No such file or directory
###
### Output of: /bin/ls -l //bin/rootedoor
###
/bin/ls: cannot access '//bin/rootedoor': No such file or directory
###
### Output of: /bin/ls -l //snap/bin/rootedoor
###
/bin/ls: cannot access '//snap/bin/rootedoor': No such file or directory
###
### Output of: /bin/ls -l /etc/.enyeOCULTAR.ko
###
/bin/ls: cannot access '/etc/.enyeOCULTAR.ko': No such file or directory
###
### Output of: cat //var/spool/cron/crontabs | egrep var/tmp
###
cat: //var/spool/cron/crontabs: Is a directory
###
### Output of: /bin/ls -l /tmp/ss0-[0-]9*
###
/bin/ls: cannot access '/tmp/ss0-[0-]9*': No such file or directory
###
### Output of: /bin/ls -l /tmp/kk0-[0-]9*
###
/bin/ls: cannot access '/tmp/kk0-[0-]9*': No such file or directory
###
### Output of: /bin/ls -l /home/
###
total 72
```