## 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.

- Command to inspect permissions:
ls -l shadow
- Command to set permissions (if needed):
chmod 640 shadow
2. Permissions on `/etc/gshadow` should allow only `root` read and write access.

- Command to inspect permissions:
ls - gshadow
- Command to set permissions (if needed):
chmod 600 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 group
- Command to set permissions (if needed):
sudo chmod 644 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 passwd
- Command to set permissions (if needed):
sudo chmode 644 group
### 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 -m sam
sudo useradd -m joe
sudo useradd -m amy
sudo useradd -m sara
sudo useradd -m admin
2. Ensure that only the `admin` has general sudo access.

- Command to add `admin` to the `sudo` group:
sudo usermod -aG sudo
### 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 jow
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 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 engineers

### Step 4: Lynis Auditing
1. Command to install Lynis:
sudo apt-get install Lynis

2. Command to see documentation and instructions:
Lynis --help
man Lynis

3. Command to run an audit:
sudo lynis audit <scan Type>
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 [C
ST-0285]
     https://your-domain.example.org/controls/CUST-0285/

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

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

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

### Bonus

1. Command to install chkrootkit:

sudo apt-get 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.

- Screenshot of end of sample output:

```
INFECTED: Possible Malicious Linux.Xor.DDoS installed
/tmp/burpsuite_community_linux_v2020_11_3.sh
/tmp/vagrant-shell
/tmp/response.varfile
/tmp/str.sh
enp0s3: PACKET SNIFFER(/sbin/dhclient[1435])
 The tty of the following user process(es) were not found
 in /var/run/utmp !
```

---