**### 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 “filename” /etc/shadow**

- Command to set permissions (if needed): **chmod u=rw g=rw, o=rw “file name”**

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

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

- Command to set permissions (if needed): **chmod u=rw, g=rw, o=rw “filename”**

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 “filename” /etc/group**

- Command to set permissions (if needed): **chmod u=rw, g= rwx, o= rwx “filename”**

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 “filename” /etc/passwd**

- Command to set permissions (if needed):**chmod u=rw, g=r, o=r**

**### 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):**pw\_name : “sam” ; pw\_name: “joe”; pw\_name: “amy”; pw\_name: “sara”; pw\_name: “admin”**

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

- Command to add `admin` to the `sudo` group:**usermod aG sudo username**

**### Step 3: Create User Group and Collaborative Folder**

1. Add an `engineers` group to the system.

- Command to add group: **sudo useradd 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 -a -G sam, joe, amy, sara**

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

- Command to create the shared folder:**sudo mkdir -p /home/engineers**

4. Change ownership of the new engineers' shared folder to the `engineers` group.

- Command to change ownership of engineer's shared folder to engineer group:**sudo chmod -R engineers /home/engineers/**

**### Step 4: Lynis Auditing**

1. Command to install Lynis: **sudo 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.

- Screenshot of report output:

**\*\*\\*\*\* Consider hardening SSH configuration [SSH-7408]**

**- Details : X11Forwarding (YES --> NO)**

**### Bonus**

1. Command to install chkrootkit:**apt install chkrootkit -y**

2. Command to see documentation and instructions: **man chkrootkit**

3. Command to run expert mode: **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:

**Checking `tcpd'... INFECTED**

**/usr/lib/jvm/.java-1.11.0-openjdk-amd64.jinfo /lib/modules/4.15.0-20-generic/vdso/.build-id**

**/lib/modules/4.15.0-20-generic/vdso/.build-id**

**not tested**

**enp0s3: PACKET SNIFFER(/lib/systemd/systemd-networkd[643])**

**not tested**

---

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.