**Week 4 Homework Submission File: Linux Systems Administration6**

**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

1. 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

1. 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

1. 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 adduser sam ; then enter password twice, and any other details, then y
* sudo adduser joe ; then enter password twice, and any other details, then y
* sudo adduser amy ; then enter password twice, and any other details, then y
* sudo adduser sara ; then enter password twice, and any other details, then y
* sudo adduser admin; then enter password twice, and any other details, then y

1. 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

1. 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

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

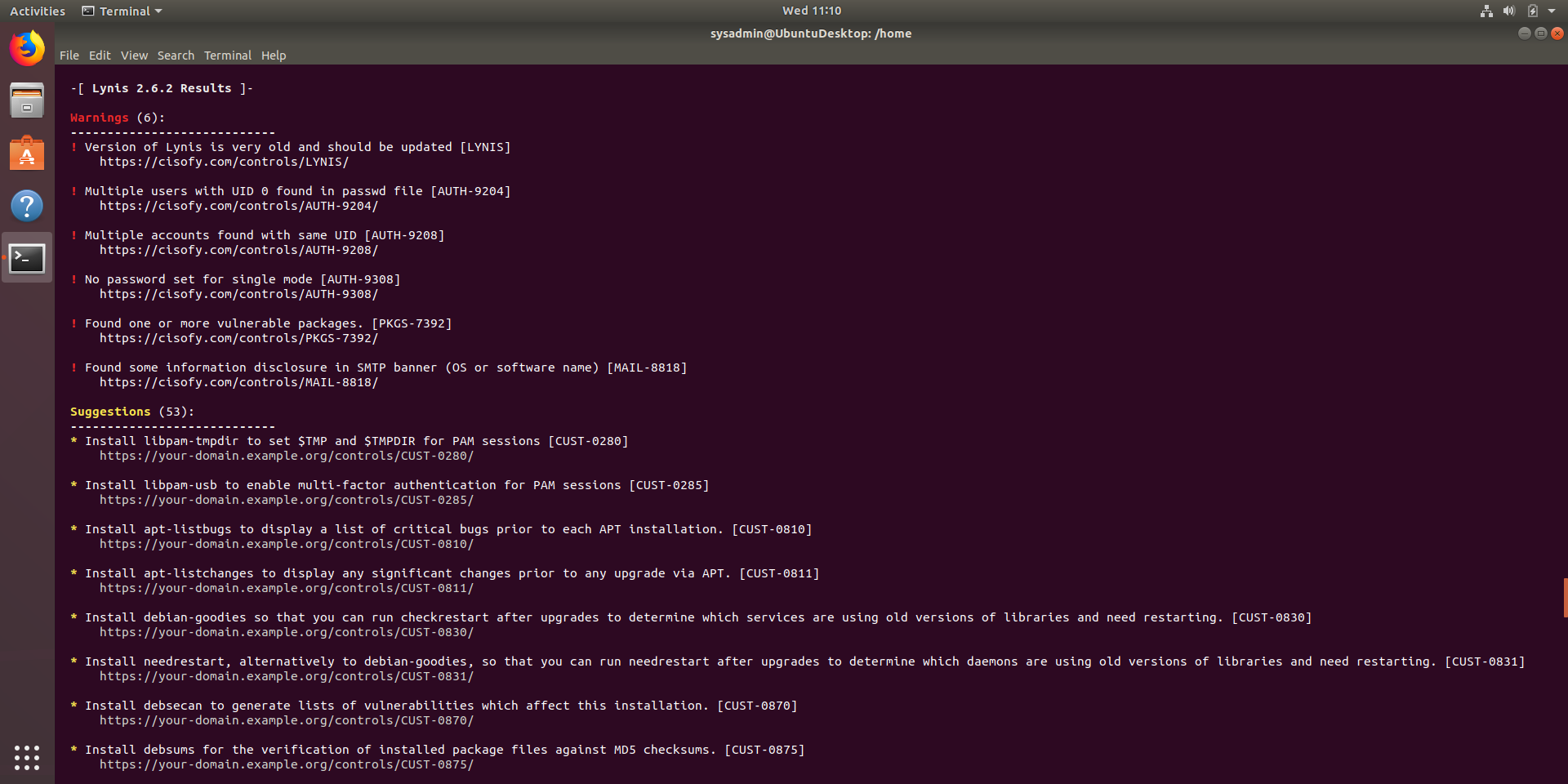
* Command to create the shared folder: sudo mkdir /home/engineers

1. 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/
* note- can't make owner engineers because engineers is not a user, just a group. But can change group of engineers directory to 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: lynis audit system (sudo lynis audit system - this will give more detail but not required)
4. Provide a report from the Lynis output on what can be done to harden the system.

* Screenshot of report output: 

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

Chkrootkit discovered one possible infection that should be checked out.

Searching for Linux.Xor.DDoS ... INFECTED: Possible Malicious Linux.Xor.DDoS installed

This same line did not show up in the expert mode.

* Screenshot of end of sample output: 