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 /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 adduser sam**

2. Ensure that only the admin has general sudo access. **sudo -lU admin**
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.
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** (joe,amy,sara)

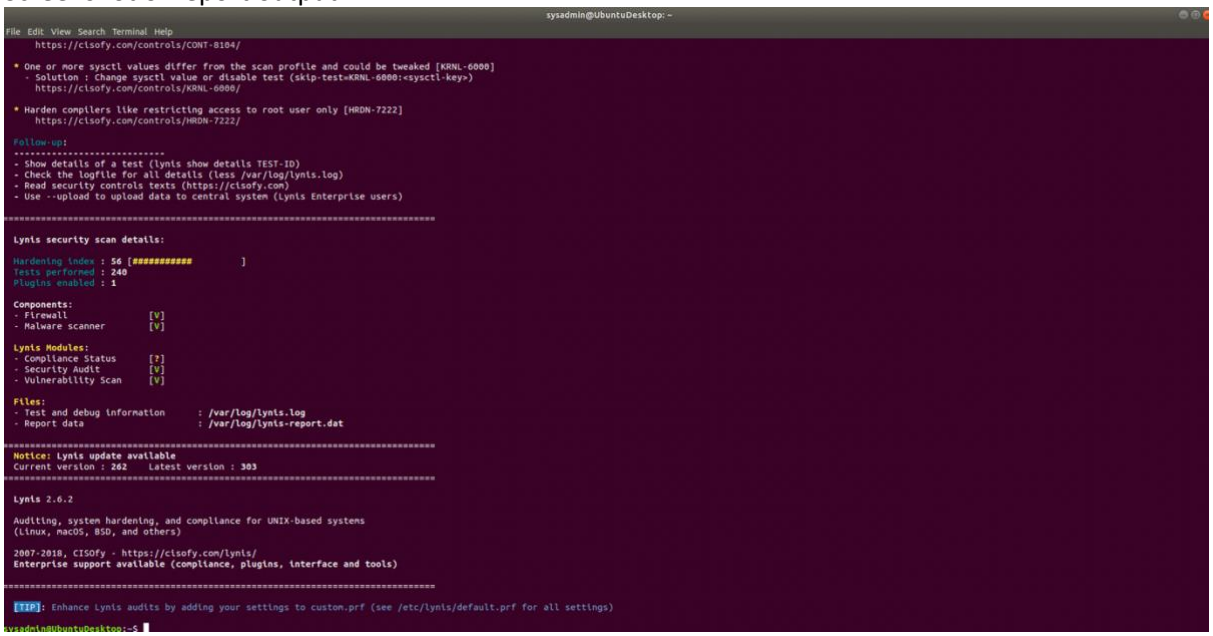
3. Create a shared folder for this group at /home/engineers .
Command to create the shared folder: **mkdir engineers**
ensam
4. Change ownership on the new engineers' shared folder to the engineers group.
Command to change ownership of engineer's shared folder to engineer group: **chgrp engineers engineers/**

Step 4: Lynis Auditing

1. Command to install Lynis: **sudo apt install Lynis**

2. Command to see documentation and instructions: **sudo lynis audit info**
3. Command to run an audit: Q **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:



Bonus

1. Command to install chkrootkit: **sudo apt install chkrootkit**
2. Command to see documentation and instructions: **sudo chkrootkit -h**
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: