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 604 /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 604 /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. sudo adduser joe. sudo adduser sara. sudo adduser admin.**
2. Ensure that only the admin has general sudo access.
    - Command to add admin to the sudo group: **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 -aG engineers sam, joe, amy, sara**
3. Create a shared folder for this group at /home/engineers.

    - Command to create the shared folder: **touch shared_folder /home/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: **chown shared_folder engineers**

Step 4: Lynis Auditing

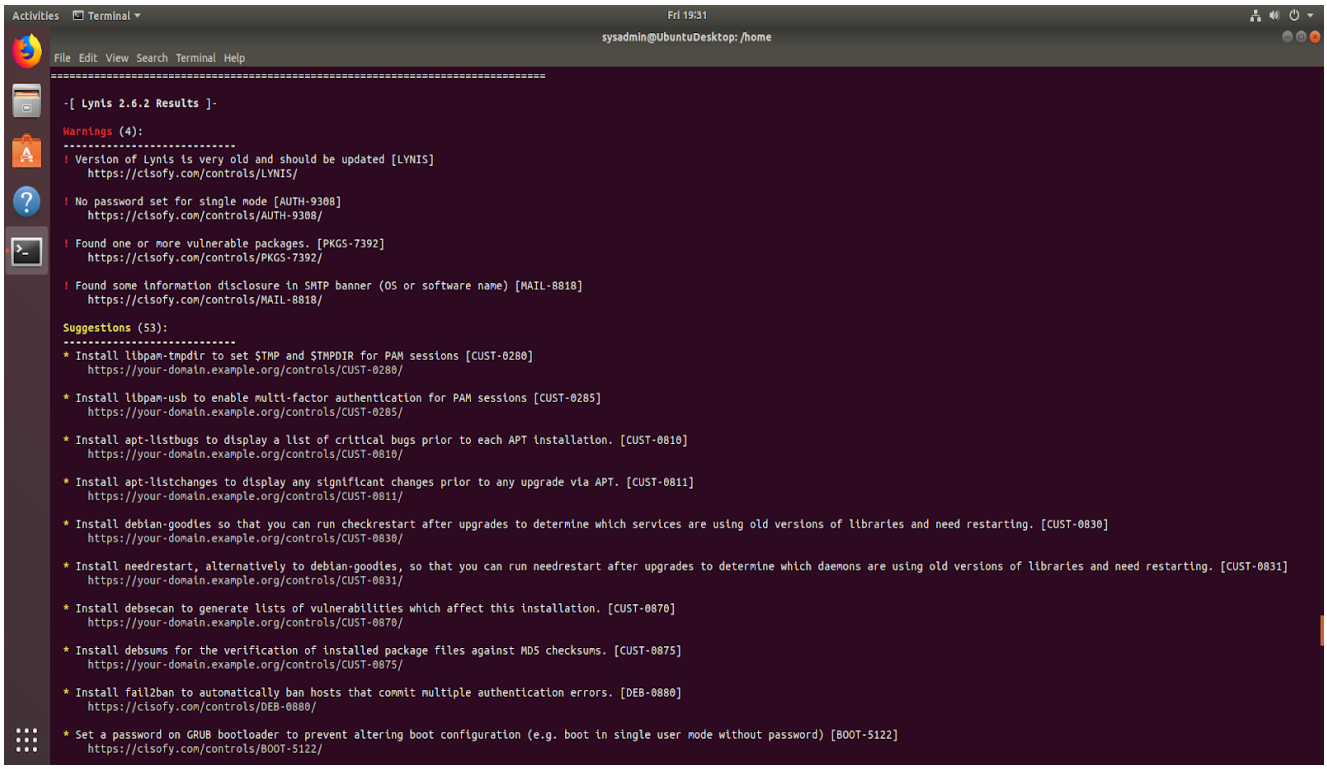
1. Command to install Lynis: **lynis install**

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

3. Command to run an audit: **lynis audit system**

4. Provide a report from the Lynis output on what can be done to harden the system.

    - Screenshot of report output:


Activities
Terminal
Fri 19:31
sysadmin@UbuntuDesktop: /home
File Edit View Search Terminal Help
-[Lynis 2.6.2 Results]-
Warnings (4):
! Version of Lynis is very old and should be updated [LYNIS]
https://cisofy.com/controls/LYNIS/
! No password set for single mode [AUTH-9308]
https://cisofy.com/controls/AUTH-9308/
! Found one or more vulnerable packages. [PKGS-7392]
https://cisofy.com/controls/PKGS-7392/
! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
https://cisofy.com/controls/MAIL-8818/
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 [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/
* Install debsecan to generate lists of vulnerabilities which affect this installation. [CUST-0870]
https://your-domain.example.org/controls/CUST-0870/
* Install debsums for the verification of installed package files against MD5 checksums. [CUST-0875]
https://your-domain.example.org/controls/CUST-0875/
* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
https://cisofy.com/controls/DEB-0880/
* Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
https://cisofy.com/controls/BOOT-5122/