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

Step 1: Ensure/Double Check Permissions on Sensitive Files

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

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): not needed; rw access

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

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

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 amy

sudo adduser sara

sudo adduser admin

Force users to create 16-character passwords incorporating numbers and symbols.

Command to edit pwquality.conf file:

Updates to configuration file: minlen=16 minclass=3

Force passwords to expire every 90 days.

Command to to set each new user's password to expire in 90 days (include all five users): sudo chage –M 90 –W 7 sam, sudo chage –M 90 –W 7 amy, sudo chage –M 90 –W 7 joe, sudo chage –M 90 –W 7 sara, sudo chage –M 90 –W 7 admin

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

Add an engineers group to the system.

Command to add group: sudo addgroup engineers

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 enginners sam, sudo usermod –aG enginners amy, sudo usermod –aG enginners joe, sudo usermod –aG enginners sara

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

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

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 chggrp –R engineers /home/engineers

Add the SGID bit and the sticky bit to allow collaboration between engineers in this directory.

Command to set SGID and sticky bit to shared folder:

Step 4: Lynis Auditing

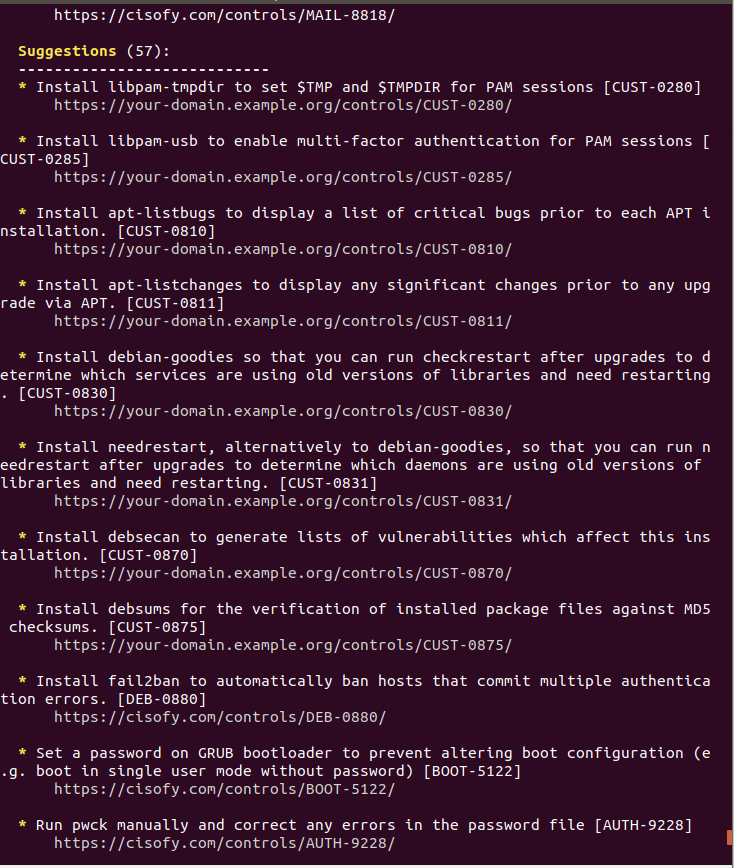
Command to install Lynis: sudo apt install Lynis or to check sudo dpkg –get-selections or sudo apt list

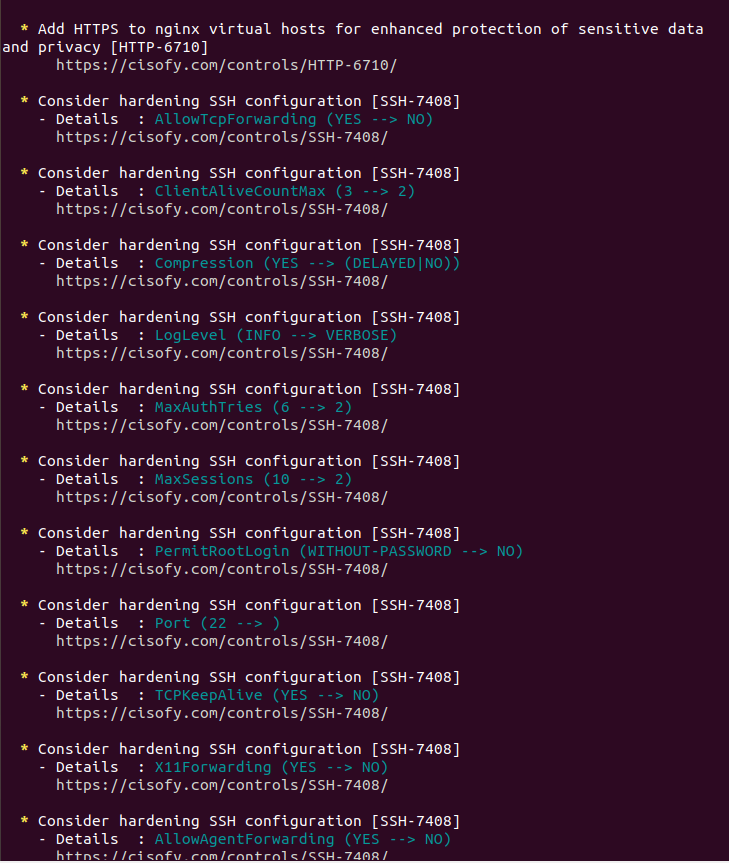
Command to see documentation and instructions: man lynis

Command to run an audit: sudo lynis system audit

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

Screenshot of report output:





Bonus

Command to install chkrootkit: sudo apt install chrootkit

Command to see documentation and instructions: man rootkit

Command to run expert mode: sudo

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

Screenshot of end of sample output:

