Sasha Shahidi

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 useradd sam
        sudo useradd joe

```
sudo useradd amy
sudo useradd sara
sudo useradd admin
```

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

    - 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 -aG engineers sam
sudo usermod -aG engineers joe
sudo usermod -aG engineers amy
sudo usermod -aG engineers sara
```

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

    - Command to create the shared folder: sudo mkdir /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:

```
sudo chown -R :engineers /home/engineers
```

Step 4: Lynis Auditing

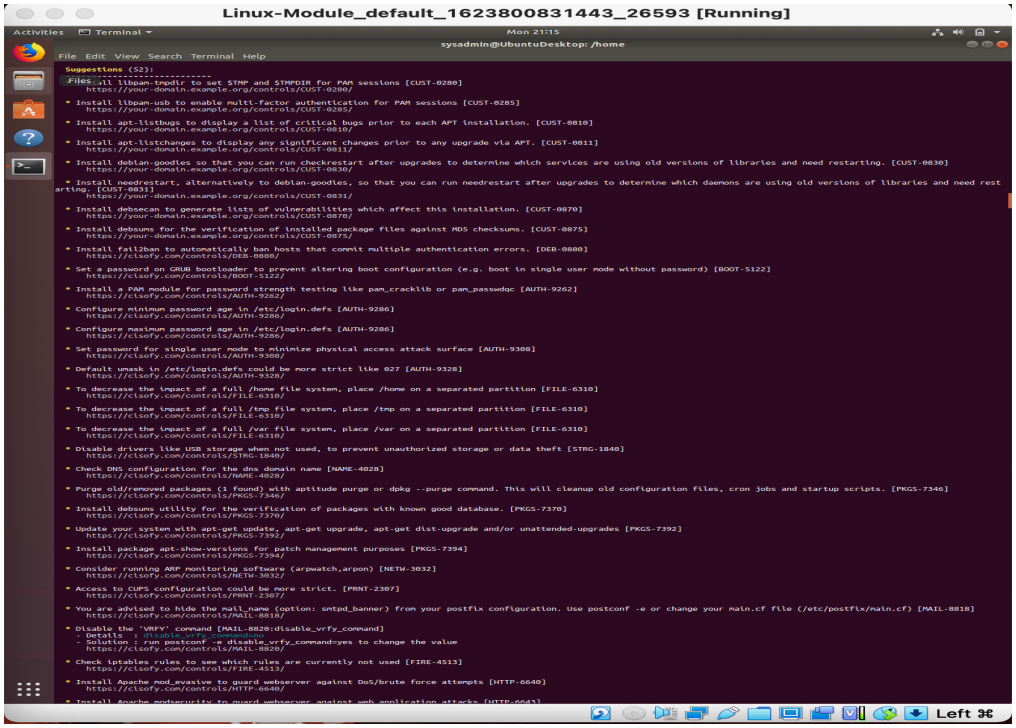
1. Command to install Lynis: sudo apt-get install -y lynis

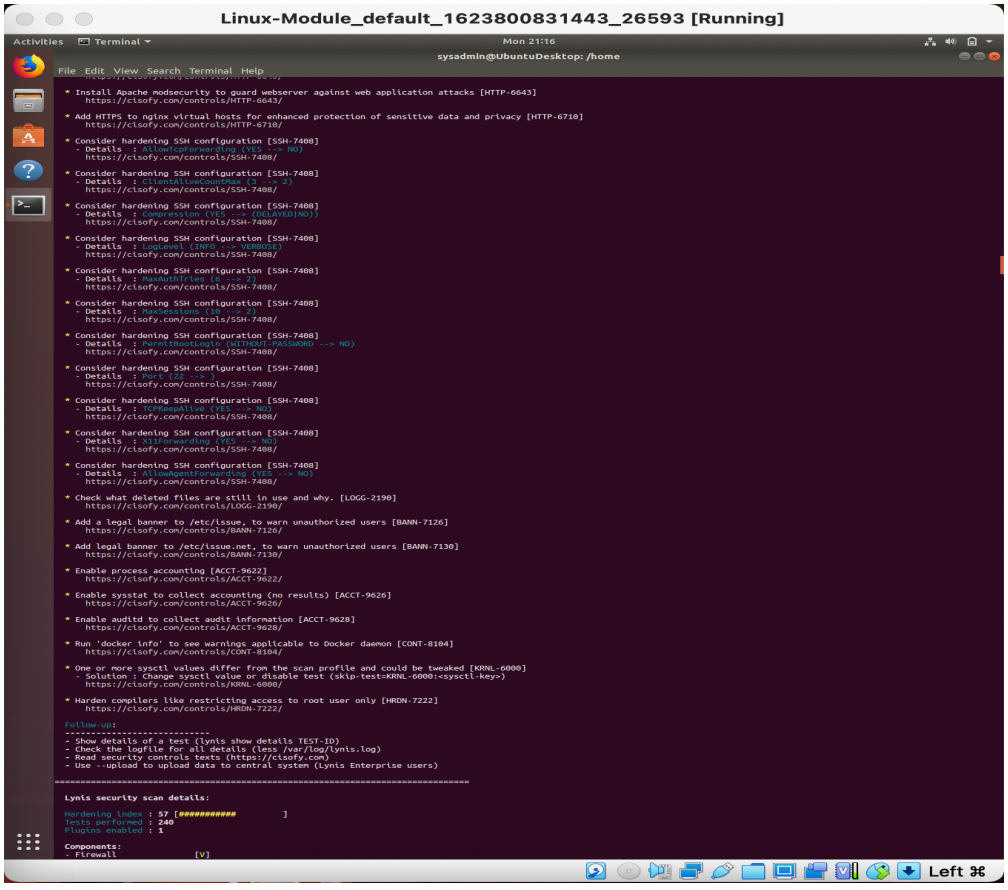
2. Command to see documentation and instructions: man lynis

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:


Linux-Module_default_1623800831443_26593 [Running]
Activities
Terminal
Mon 21:15
sysadmin@UbuntuDesktop: /home
File Edit View Search Terminal Help
Suggestions (52):
Left ⌘


Linux-Module_default_1623800831443_26593 [Running]
Activities
Terminal
Mon 21:16
sysadmin@UbuntuDesktop: /home
File Edit View Search Terminal Help
Lynis security scan details:
Hardening index : 57 [###########
Tests performed : 240
Plugins enabled : 1
Components:
Left ⌘

Bonus

1. Command to install chkrootkit: sudo apt-get install chkrootkit -y
2. Command to see documentation and instructions: man chkrootkit
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: