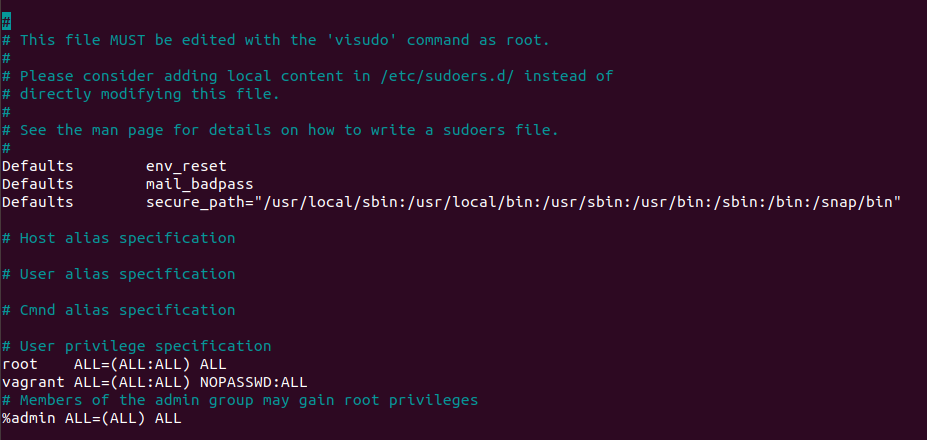
## **Week 4 Homework Submission File: Linux Systems Administration**

### Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on /etc/shadow should allow only root read and write access.
   * 1. sysadmin@UbuntuDesktop:~$ cd /etc
     2. sysadmin@UbuntuDesktop:/etc$ ls -l
   * Command to inspect permissions:
     1. sysadmin@UbuntuDesktop:/etc$ ls -l | grep shadow
        + -rw------- 1 root shadow 3619 Oct 12 20:44 shadow
   * Command to set permissions (if needed):
     1. sysadmin@UbuntuDesktop:/etc$ sudo chmod 600 shadow
        + ls -l | grep 'shadow'
        + -rw------- 1 root shadow 3619 Oct 12 20:44 shadow
2. Permissions on /etc/gshadow should allow only root read and write access.
   * Command to inspect permissions:
     1. sysadmin@UbuntuDesktop:/etc$ ls -l gshadow
        + -rw------- 1 root shadow 1189 Oct 12 21:12 gshadow
   * Command to set permissions (if needed): no change needed
3. Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.
   * Command to inspect permissions:
     1. sysadmin@UbuntuDesktop:/etc$ ls -l group
        + -rw-r--r-- 1 root root 1445 Oct 12 21:12 group
   * Command to set permissions (if needed): no change needed
4. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.
   * Command to inspect permissions:
     1. sysadmin@UbuntuDesktop:/etc$ ls -l passwd
        + -rw-r--r-- 1 root root 3471 Oct 12 20:44 passwd
   * Command to set permissions (if needed): no change needed

### Step 2: Create User Accounts

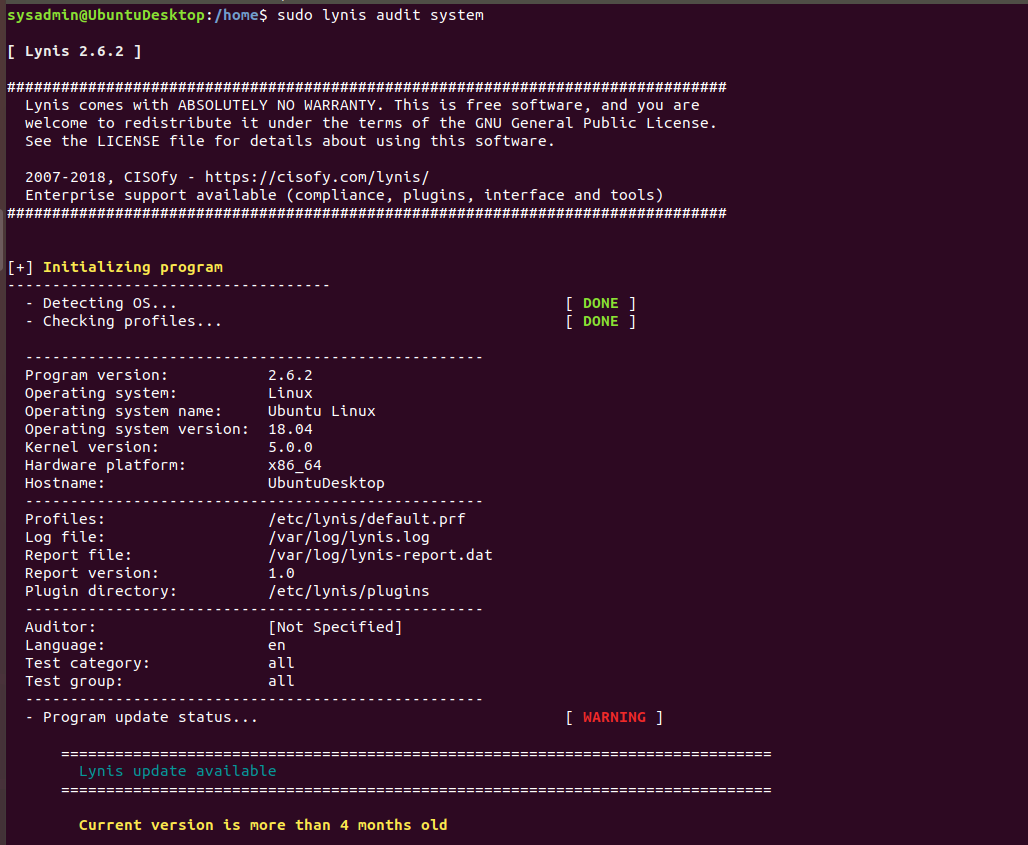
1. Add user accounts for sam, joe, amy, sara, and admin.
   * Command to add each user account (include all five users):
     1. sysadmin@UbuntuDesktop:/etc$ sudo adduser sam  
        Adding user `sam' ...  
        Adding new group `sam' (1016) ...  
        Adding new user `sam' (1006) with group `sam' ...  
        The home directory `/home/sam' already exists. Not copying from `/etc/skel'.  
        Enter new UNIX password:   
        Retype new UNIX password:   
        passwd: password updated successfully  
        Changing the user information for sam  
        Enter the new value, or press ENTER for the default  
         Full Name []:   
         Room Number []:   
         Work Phone []:   
         Home Phone []:   
         Other []:
     2. sysadmin@UbuntuDesktop:/etc$ sudo adduser joe
     3. sysadmin@UbuntuDesktop:/etc$ sudo adduser amy
     4. sysadmin@UbuntuDesktop:/etc$ sudo adduser sara
     5. sysadmin@UbuntuDesktop:/etc$ sudo adduser admin
   * **Hint:** In order for users to be added to the system, you need to run the command with sudo.
2. We want to make sure that only the admin user has general sudo group access. This requires a command that will allow user modifications
   * sysadmin@UbuntuDesktop:/etc$ sudo visudo

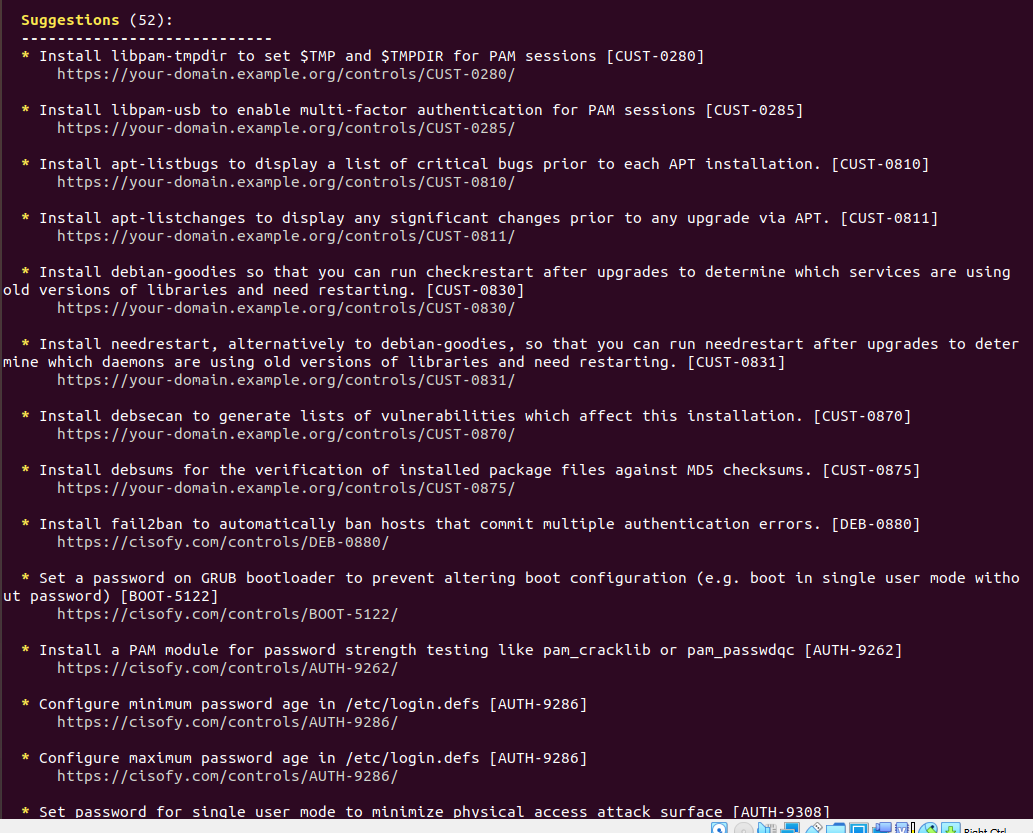


### Step 3: Create User Group and Collaborative Folder

1. Add an engineers group to the system.
   * Command to add group:
     1. sysadmin@UbuntuDesktop:/etc$ sudo groupadd engineers
2. Add users sam, joe, amy, and sara to the managed group.
   * Command to add users to engineers group (include all four users):
     1. sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG engineers sam
     2. sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG engineers joe
     3. sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG engineers amy
     4. sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG engineers sara
        + sysadmin@UbuntuDesktop:/etc$ members engineers
          - sara joe amy sam
3. Create a shared folder for this group at /home/engineers.
   * 1. sysadmin@UbuntuDesktop:/home$
        + sysadmin@UbuntuDesktop:/home$ sudo mkdir engineers
   * Command to create the shared folder:
     1. sysadmin@UbuntuDesktop:/home$ sudo chgrp -R engineers /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:
     1. sysadmin@UbuntuDesktop:/home$ sudo chown :engineers /home/engineers/

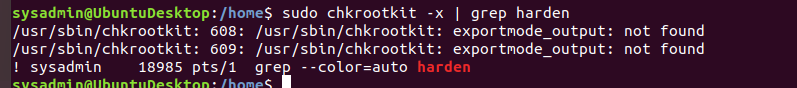
### Step 4: Lynis Auditing

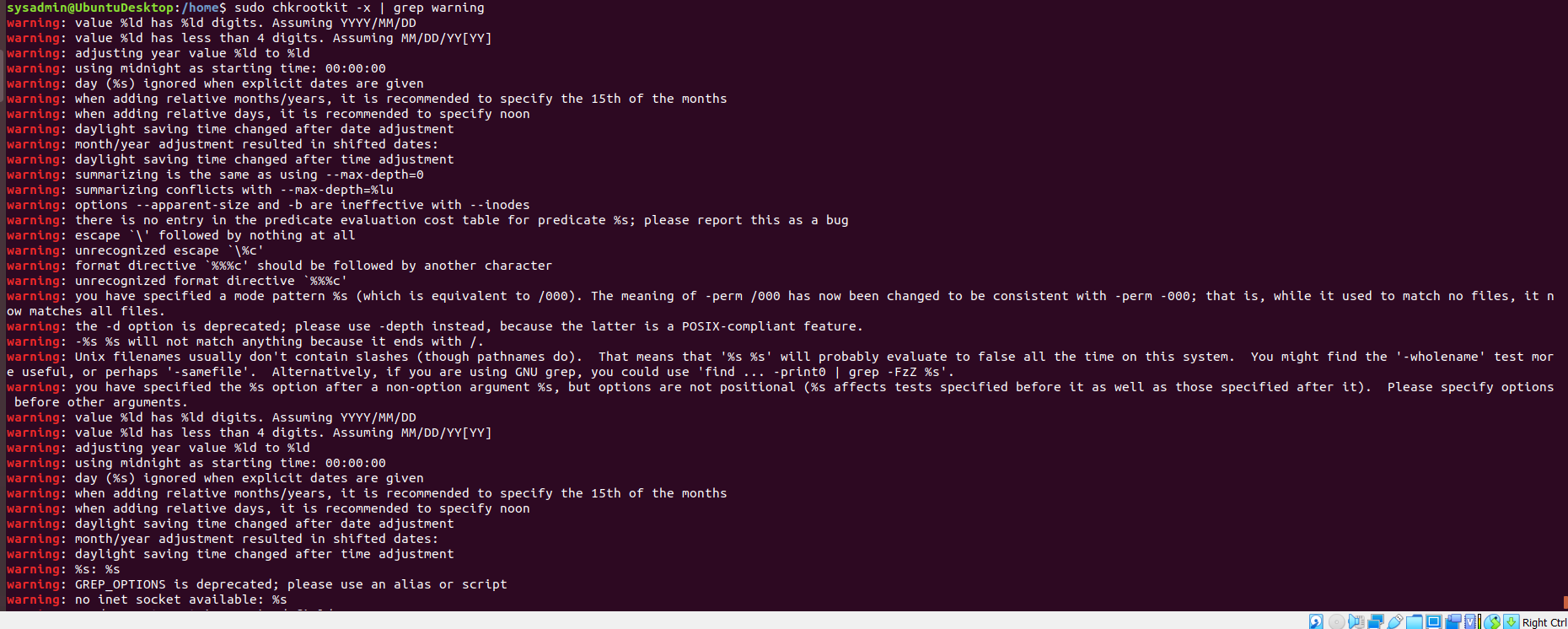
1. Command to install Lynis:
   * sysadmin@UbuntuDesktop:/home/engineers$ sudo apt install lynis
2. Command to see documentation and instructions:
   * sysadmin@UbuntuDesktop:/home$ sudo lynis
3. Command to run an audit:
4. Provide a report from the Lynis output on what can be done to harden the system.
   * Screenshot of report output:



### Bonus

1. Command to install chkrootkit:
   * sysadmin@UbuntuDesktop:/home$ sudo apt install chkrootkit
2. Command to see documentation and instructions:
   * sysadmin@UbuntuDesktop:/home$ man chkrootkit
3. Command to run expert mode:
   * sysadmin@UbuntuDesktop:/home$ 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:





© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.