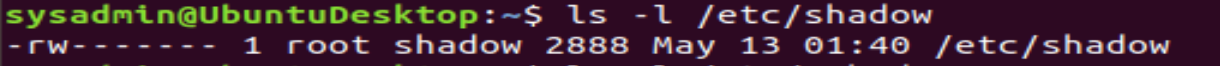
### **Step 1: Ensure Permissions on Sensitive Files**

1. Permissions on /etc/shadow should allow only root read and write access.  
   * Command to inspect permissions:

ls -l /etc/shadow

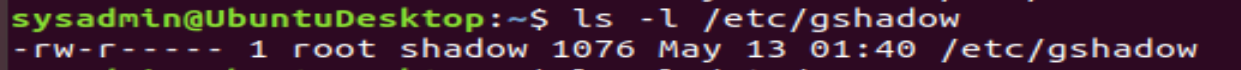


* + Command to set permissions (if needed):

Sudo chmod 600 /etc/shadow

1. 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

1. 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

1. 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

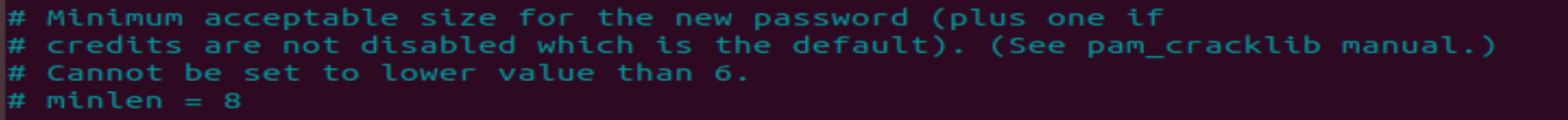
Force users to create 16-character passwords incorporating numbers and symbols.

* + Command to edit pwquality.conf file:

Sudo vi /etc/security/pwquality.conf

* + Updates to configuration file:

Change the value of ‘minlen’ from 8 to 16



1. 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 sam

Sudo chage -M 90 joe

Sudo chage -M 90 amy

Sudo chage -M 90 sara

Sudo chage -M 90 admin

1. 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 groupadd engineers

1. 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

1. Create a shared folder for this group at /home/engineers.  
   * Command to create the shared folder:

Sudo mkdir -p home/engineers/wrench

1. 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 sam /home/engineers/wrench

Sudo chown -R joe /home/engineers/wrench

Sudo chown -R amy /home/engineers/wrench

Sudo chown -R sara /home/engineers/wrench

1. 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:

Sudo chmod g+s /home/engineers/wrench

Sudo chmod o+t /home/engineers/wrench

### **Step 4: Lynis Auditing**

1. Command to install Lynis:

Sudo apt install lynis

1. Command to see documentation and instructions:

Sudo lynis

1. Command to run an audit:  
   sudo lynis audit system
2. 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 -y

1. Command to see documentation and instructions:

Sudo /usr/sbin/chkrootkit --help

1. Command to run expert mode:

Sudo /usr/sbin/chkrootkit

1. Provide a report from the chrootkit output on what can be done to harden the system.  
   * Screenshot of end of sample output:

