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

The /etc/ directory is where system configuration files exist. Start by navigating to this directory with cd /etc/.

Inspect the file permissions of each of the files below. This should have already been completed in the activity, but let's double check! If they do not match the descriptions, please update the permissions.

1. Permissions on /etc/shadow should allow only root read and write access.

Command to inspect permissions



Command to set permissions (if needed):  
Not required as permissions are correct.

1. Permissions on /etc/gshadow should allow only root read and write access.

Command to inspect permissions:



Command to set permissions (if needed):

Not required as permissions are correct.

1. Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.

Command to inspect permissions:



Command to set permissions (if needed):

Not required as permissions are correct.

1. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.

* **Hints:**
  + Run the following command to view the file permissions: ls -l <file>
  + If permissions need to be changed or modified, use the chmod command.

Command to inspect permissions:



Command to set permissions (if needed):

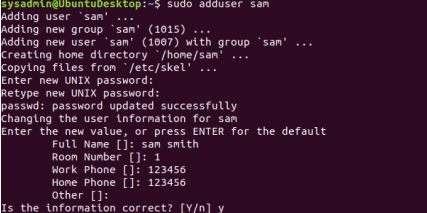
Not required as permissions are correct.

#### **Step 2: Create User Accounts**

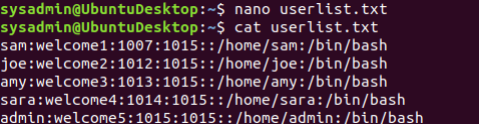
This step asks you to set up various users. These commands do not require you to be working from a specific directory.

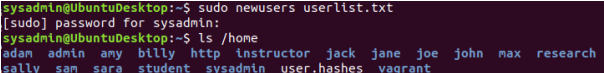
1. Add user accounts for sam, joe, amy, sara, and admin.  
   * **Hint:** In order for users to be added to the system, you need to run the command with sudo.

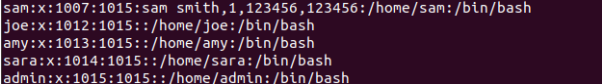
Command to add each user account (include all five users): -Add one user:



Multiple users in one hit! - userlist.txt contains the following user details







1. We want to make sure that only the admin user has general sudo group access. This requires a command that will allow user modifications.

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

Now we want to execute the commands to fully set up a group on our system.

This requires us to create a group, add users to it, create a shared group folder, set the group folder owners for these shared folders.

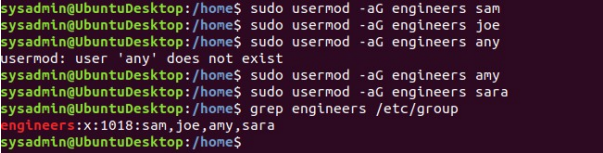
1. Add the group engineers to the system.

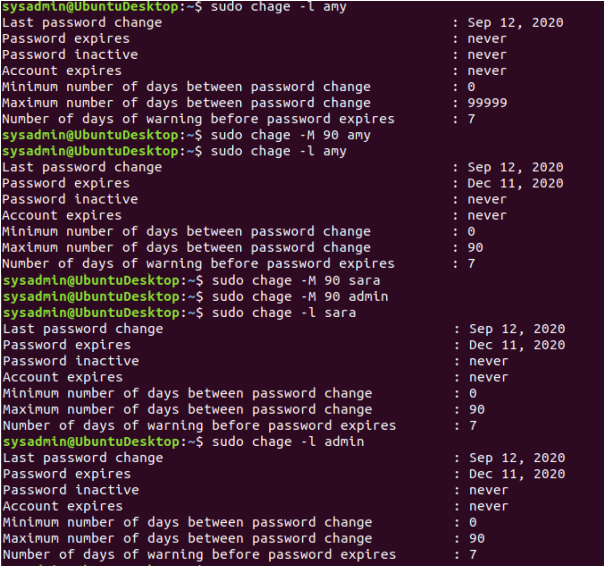
Command to add group:



1. Add users sam, joe, amy, and sara to the managed group. This will be similar to how you added admin to the sudo group in the previous exercise.

Command to add users to engineers group (include all four users):

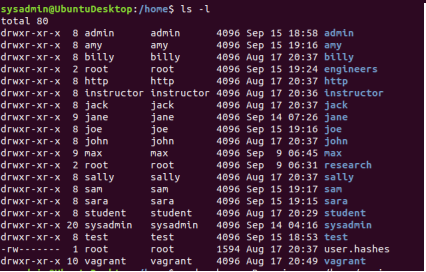




1. Create a shared folder for this group: /home/engineers.

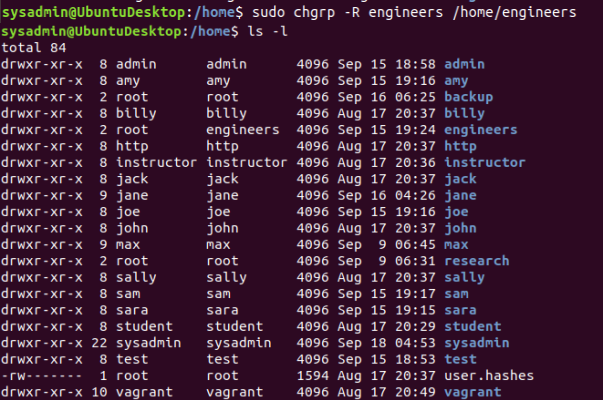
Command to create the shared folder:

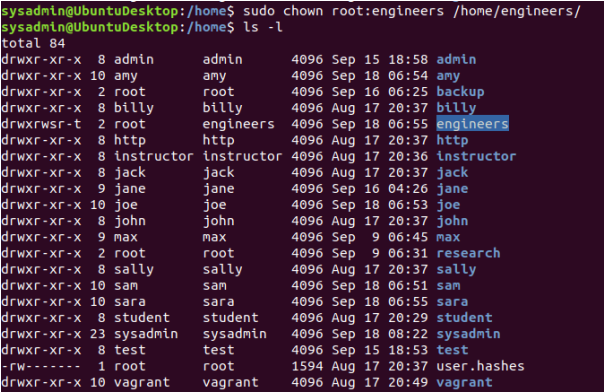




1. Change ownership on the new engineers' shared folder to the engineers group.

Command to change ownership of engineer's shared folder to engineer group:

  
Or the following command will provide the same output



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

The final step on your administrator's list involves running an audit against the system in order to harden it. You'll use the system and security auditing tool Lynis to do so.

1. Install the Lynis package to your system if it is not already installed.

1. Check the Lynis documentation for instructions on how to run a system audit.
2. Run a Lynis system audit with sudo.
3. Provide a report from the Lynis output on what more could be done to harden the system.

#### **Bonus**

Despite claims from enthusiasts, Linux is *not* immune to malware. You will need to install and run the application chkrootkit, to search for any potential rootkits installed on the system.

1. Install the chkrootkit package to your system if it is not already installed.
2. Check the chkrootkit documentation for instructions on how to run a scan to find system root kits.
3. Run chkrootkit (with sudo) in expert mode to verify the system does not have a root kit installed.
4. Provide a report from chkrootkit output on what more could be done to harden the system.