Skye Falzett

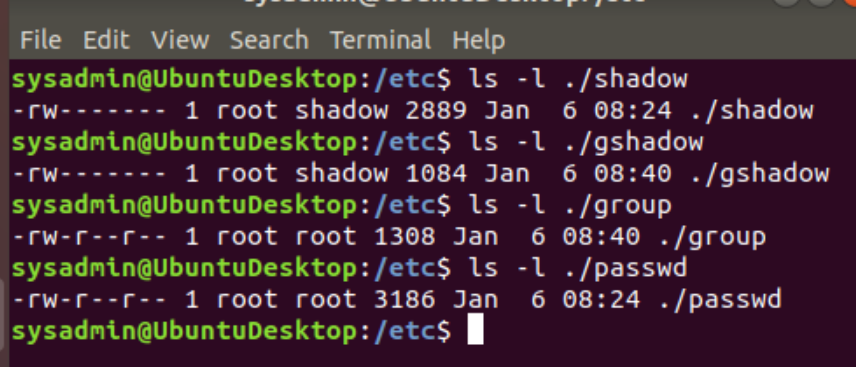
2022.01.06

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

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

**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 ./shadow

* Command to set permissions (if needed):

n/a

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

ls -l ./gshadow

* Command to set permissions (if needed):

n/a

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 ./group

* Command to set permissions (if needed):

n/a

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 ./passwd

* Command to set permissions (if needed):

n/a

**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 adduser sam

sudo adduser joe

sudo adduser amy

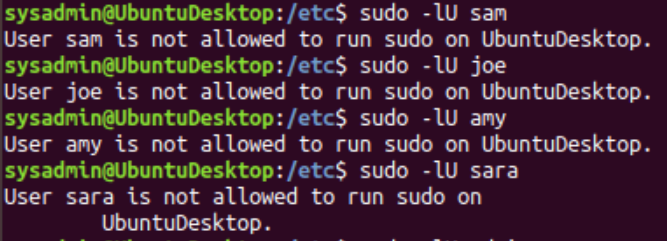
sudo adduser sara

sudo adduser admin

(\*set up passwords when prompted to 'newuser' for sam, joe, amy, and sara and to 'admin' for admin)

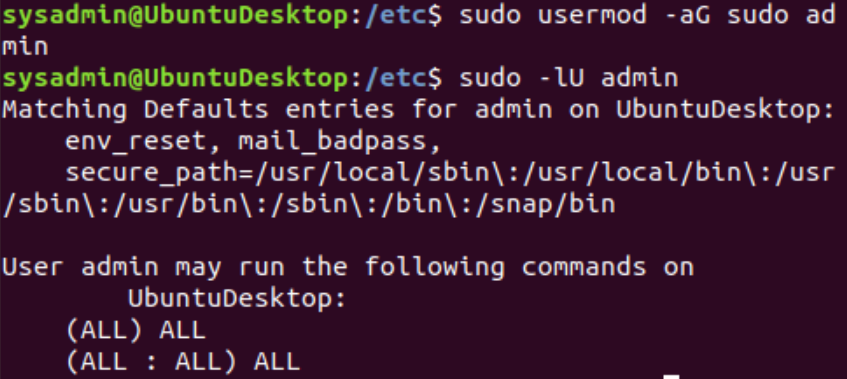
1. Ensure that only the admin has general sudo access.

verified with sudo -lU <user>



* Command to add admin to the sudo group:

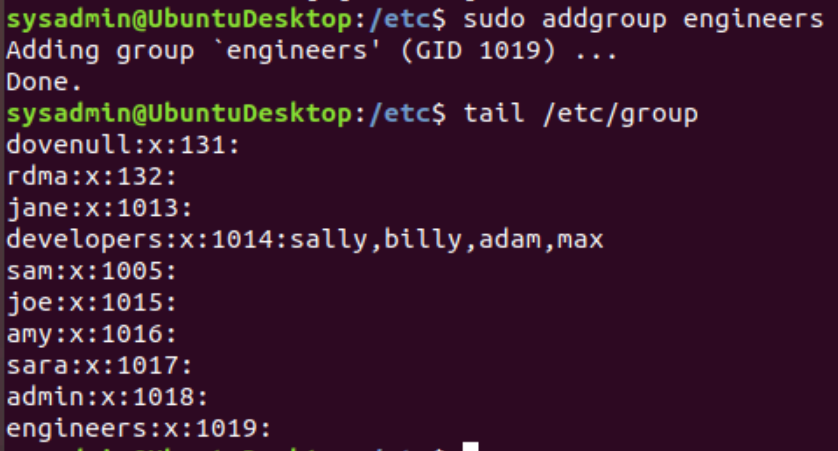
sudo usermod -aG sudo admin



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

1. Add an engineers group to the system.
   * Command to add group:

sudo addgroup engineers



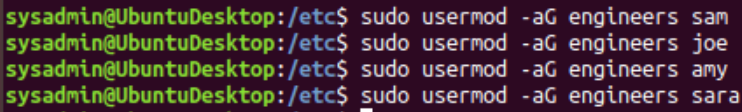
1. Add users sam, joe, amy, and sara to the managed group.
   * Command to add users to engineers group (include all four users):

sudo usermod -aG engineers sam

sudo usermod -aG engineers joe

sudo usermod -aG engineers amy

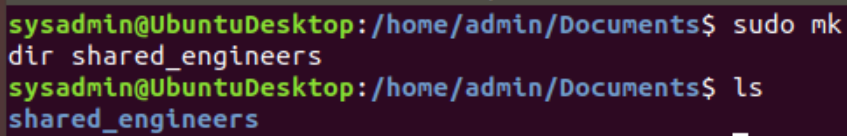
sudo usermod -aG engineers sara



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

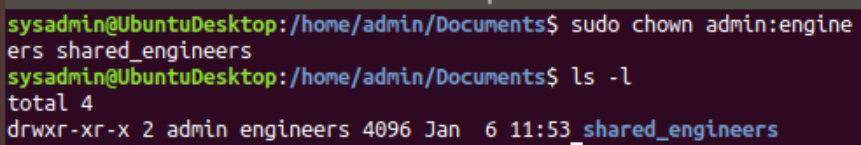
sudo mkdir shared\_engineers

I made the directory in the home/admin/Documents directory and named it shared\_engineers:



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 admin:engineers shared\_engineers



?? Wasn't sure what "ownership" meant in this sense-- I thought using chown with <user>:<group> the owner would be <user> so when it asked for ownership to be changed to the group, I tried that and got 'invalid user' response. So I used admin as the 'owner'?

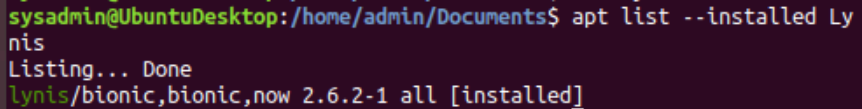
**Step 4: Lynis Auditing**

1. Command to install Lynis:

Lynis was already installed. I verified it using:

apt list --installed Lynis

and it returned:



1. Command to see documentation and instructions:

man lynis

1. Command to run an audit:

sudo lynis audit system

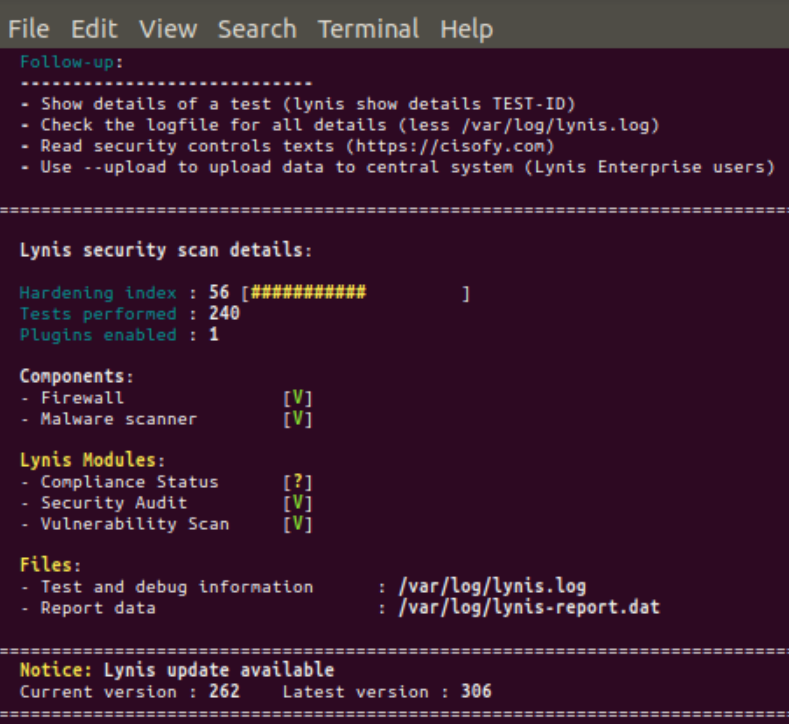
1. Provide a report from the Lynis output on what can be done to harden the system.

I created a file using:

touch lynis\_system\_audit\_jan062022

I then ran:

sudo lynis audit system >> lynis\_system\_audit\_jan062022

* Screenshot of report output: ??It was quite long. So I am going to so here is a screenshot of part of it towards the end:
* 

**Bonus**

1. Command to install chkrootkit: sudo apt install chkrootkit
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:

