## **Hayley Paul**

## **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 -la /etc/shadow**
   * Command to set permissions (if needed): **not needed**
2. Permissions on /etc/gshadow should allow only root read and write access.  
   * Command to inspect permissions:**# ls -la /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 -la /etc/group**
   * Command to set permissions (if needed):**# sudo chmod 604 /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: **Since I was already in the directory, I used relative path : # ls -la passwd**
   * Command to set permissions (if needed): **(used relative path again)**

**# sudo chmod 604 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 adduser sam**

**# sudo adduser joe**

**# sudo adduser amy**

**# sudo adduser sara**

**# sudo adduser 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 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**

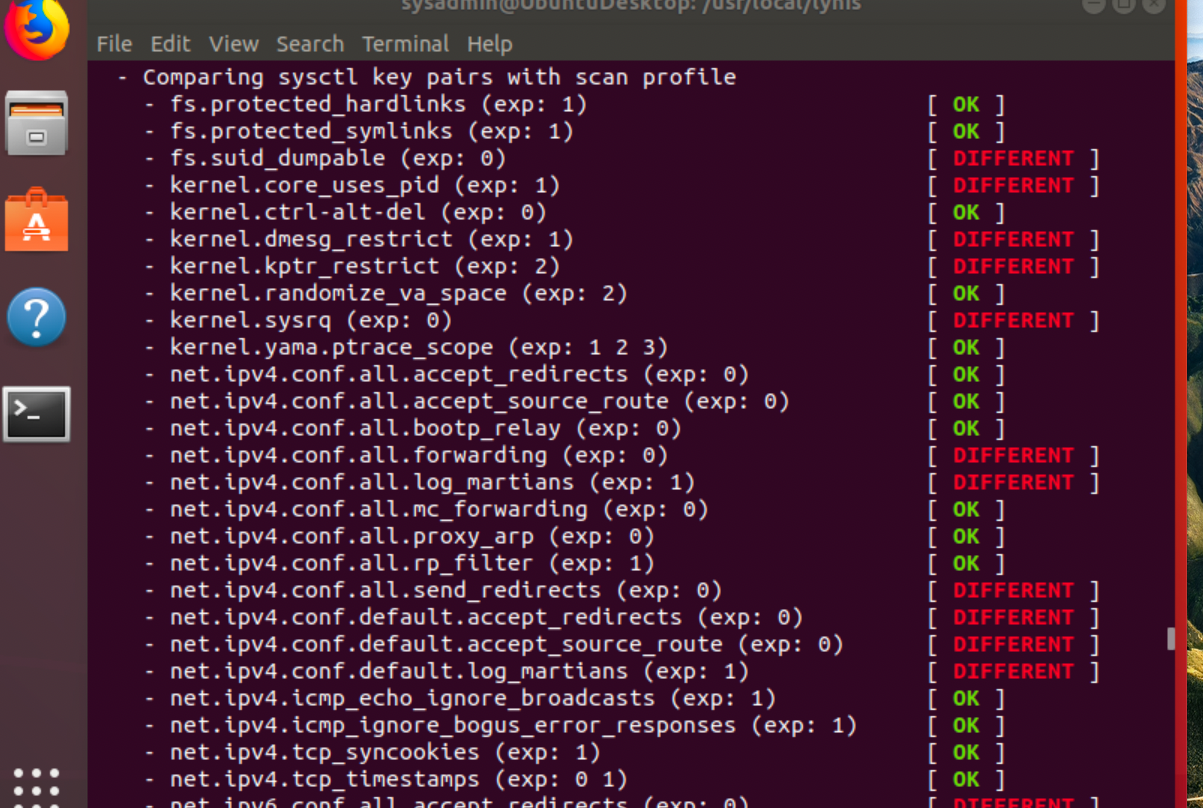
**# sudo usermod -aG engineers sara**

1. Create a shared folder for this group at /home/engineers.  
   * Command to create the shared folder: **# sudo mkdir engineers**
2. 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 root:engineers engineers**

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

1. Command to install Lynis: **# sudo git clone https://github.com/CISOfy/lynis**
2. Command to see documentation and instructions: **# cd lynis**

**# cat README**

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.  
   **Link to Audit Report and Suggestions here:** [**https://docs.google.com/document/d/1ImRFI88VT-bAylkG6Exn3nkYorGJL2dkXdMd8VgaZKU/edit?usp=sharing**](https://docs.google.com/document/d/1ImRFI88VT-bAylkG6Exn3nkYorGJL2dkXdMd8VgaZKU/edit?usp=sharing)
   * **Screenshot of report output:** 

### **Bonus**

1. Command to install chkrootkit: **# sudo apt 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.  
   * I couldn’t get a report to populate - kept saying I didn’t have permission.