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

### **Scenario**

### **In the previous class activities, you acted as system administrator in order to troubleshoot a malfunctioning server.**

### **The senior administrator was quite pleased with your work. Now, they would like you to prepare another server to replace this server. You are tasked with completing the steps below to prepare a new server.**

### **Lab Environment**

### **Log into your local virtual machine. Use the following credentials:**

### **Username: sysadmin**

### **Password: cybersecurity**

### **In order to get started with your tasks, you will need to open the Terminal within your Ubuntu VM. If you are unsure how to do it, within your Ubuntu VM, do the following:**

### **Open the Linux terminal by pressing Ctrl+Alt+T for Windows users or Ctrl+Options+T for Mac users.**

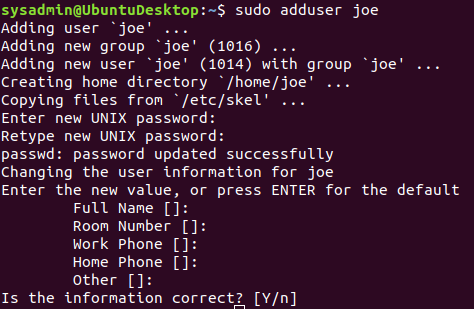
### **Alternatively, press Windows+A or Command+A for Mac users, then type "Terminal" in the search bar and select the Terminal icon (not the Xfce Terminal icon).**

### 

### **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:  
     
   * Command to set permissions (if needed):  
     
   * 
2. Permissions on /etc/gshadow should allow only root read and write access.  
   * Command to inspect permissions:   
     
   * Command to set permissions (if needed):  
     
   * 
3. 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):  
     No changes as this is correct as is
4. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.  
   * Command to inspect permissions:  
     
   * Command to set permissions (if needed):  
     No changes as this is correct as is

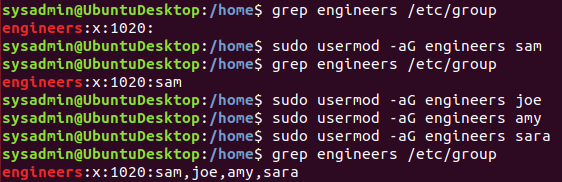
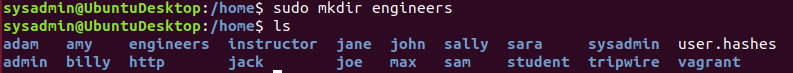
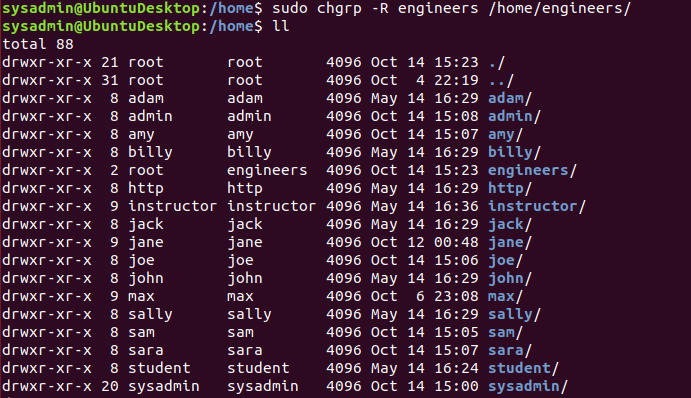
### **Step 2: Create User Accounts**

1. Add user accounts for sam, joe, amy, sara, and admin.  
   
   * Command to add each user account (include all five users):
   * 
2. Ensure that only the admin has general sudo access.  
   
   * Command to add admin to the sudo group:
   * 

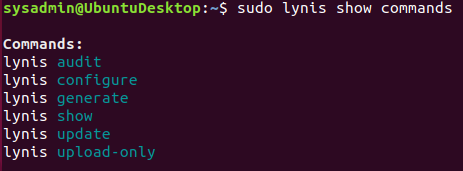
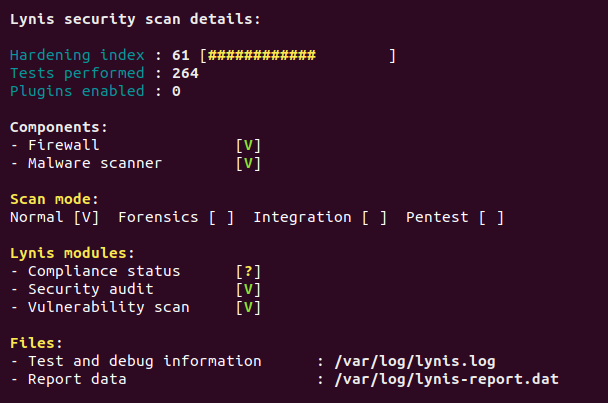
### **Step 3: Create User Group and Collaborative Folder**

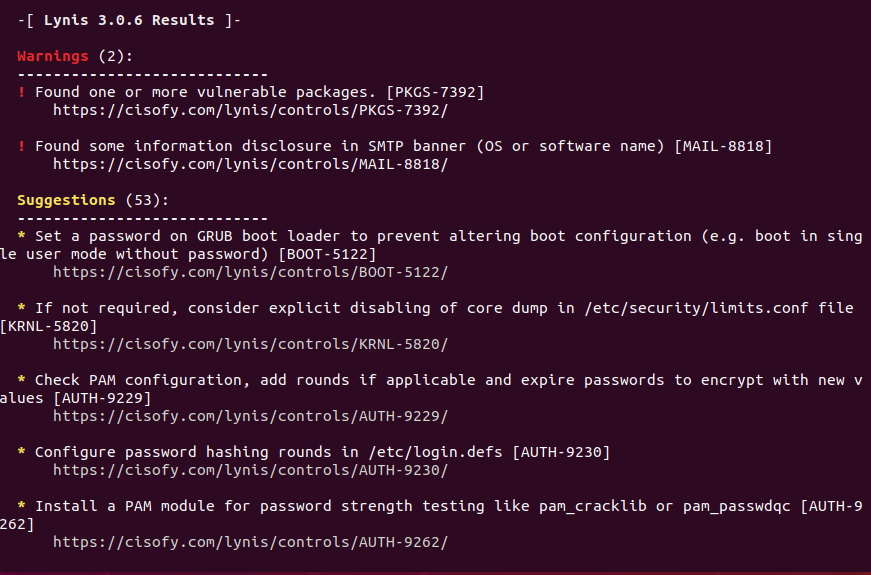
1. Add an engineers group to the system.  
   Command to add group:



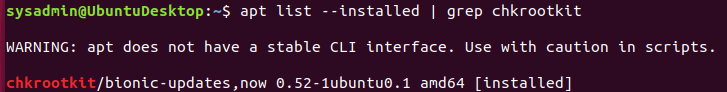
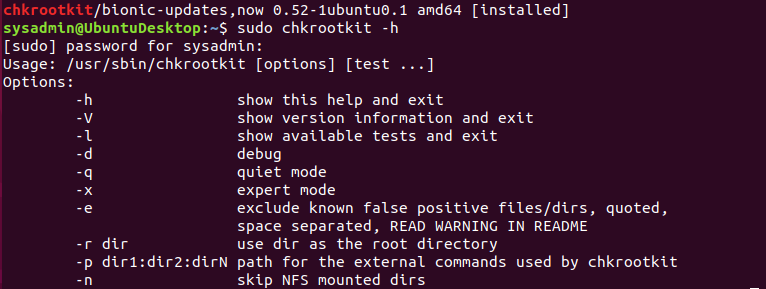
1. Add users sam, joe, amy, and sara to the managed group.
   * Command to add users to engineers group (include all four users):
   * 
2. Create a shared folder for this group at /home/engineers.
   * Command to create the shared folder:
   * 
3. Change ownership on the new engineers' shared folder to the engineers group.
   * Command to change ownership of engineer's shared folder to engineer group:
   * 

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

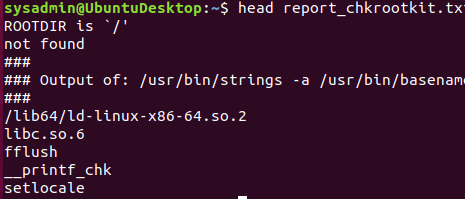
1. Command to install Lynis:  
   
2. Command to see documentation and instructions:  
   
3. Command to run an audit:  
   
4. Provide a report from the Lynis output on what can be done to harden the system.
   * Screenshot of report output:
   * 



### **Bonus**

1. Command to install chkrootkit:  
   
2. Command to see documentation and instructions:  
   
3. Command to run expert mode:  
   
4. Provide a report from the chrootkit output on what can be done to harden the system.
   * Screenshot of end of sample output:





Did not seem to work, but an attempt was made. Oh well!