**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.

**rw-r-----**

* + 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.

**rw-r-----**

* + 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.

**ok rw-r—r--**

* + Command to inspect permissions:

**ls -pl /etc/**

* + Command to set permissions (if needed):

**not needed**

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

**re-r—r--**

* + Command to inspect permissions:

**ls -l /etc/passwd**

* + Command to set permissions (if needed):

**not needed**

**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, and sudo useradd admin**

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

**Checked this and that was the case. All others had no permission to use sudo.**

* + Command to add admin to the sudo group:

**sudo -lU 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.

**sudo groupadd managed joe, sudo groupadd managed sam, sudo groupadd managed amy, and sudo groupadd managed sara**

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

**sudo usermod -aG joe, sudo usermod -aG sam, sudo usermod -aG amy, and sudo usermod -aG sara**

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

**sudo mkdir /home/engineers/engineers\_shared\_folder**

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

**sudo chown -R :engineers /home/engierrs/engineers\_shared\_folder**

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

**Step 4: Lynis Auditing**

1. Command to install Lynis:

**sudo git clone https://githum.com/CISOfy/lynis**

1. Command to see documentation and instructions:

**./lynis show options or google.com/search=lynis user manual**

1. Command to run an audit:

**sudo lynis audit system or lynis audit system**

**Without sudo it will only partially scan as it has no privileges.**

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

**see additional attached files in same homework upload link, it is the .pdf called lynis-report.dat.pdf**

**Bonus**

1. Command to install chkrootkit:

**sudo apt -get install chkrootkit -y**

1. Command to see documentation and instructions:

**chkrootkit -hl**

1. Command to run expert mode:

**chkrootkit -x (additionally -q can be used to only output “problems”)**

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

**touch chkrootkit\_output.txt**

**chmod 777 chkrootkit\_output.txt**

**sudo chkrootkit -q >> chkrootkit\_output.txt**

* + Screenshot of end of sample output:

**see additional attached file of screen shot of sample output**