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 -l /etc/shadow"
    - Command to set permissions (if needed): "sudo chmod 600 /etc/shadow"
2. Permissions on `/etc/gshadow` should allow only `root` read and write access.
    - Command to inspect permissions: "ls -l /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 -l /etc/group"
    - Command to set permissions (if needed): "sudo chmod 644 /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: "ls -l /etc/group"
    - Command to set permissions (if needed): "sudo chmod 644 /etc/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 newusers newusers.txt"
        - Created the "newusers.txt" file with the following: sam:password::::/home/sam:/bin/bash joe:password::::/home/joe:/bin/bash amy:password::::/home/amy:/bin/bash sara:password::::/home/sara:/bin/bash admin:password::::/home/admin:/bin/bash
2. Ensure that only the `admin` has general sudo access.
    - Command to add `admin` to the `sudo` group: "sudo usermod -aG sudo admin"
        - I would then view the "/etc/group" file to make sure "admin" was the only user in "sudo" group. It "admin" wasn't the only user then I could edit the "group" file directly with "sudo vigr" command.

Step 3: Create User Group and Collaborative Folder

1. Add an `engineers` group to the system.
    - Command to add group: "sudo groupadd 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 gpasswd -M sam,joe,amy,sara engineers"
3. Create a shared folder for this group at `/home/engineers`.
    - Command to create the shared folder: "sudo mkdir /home/engineers"
4. 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 chgrp engineers /home/engineers"

Step 4: Lynis Auditing

1. Command to install Lynis: "sudo apt install lynis"
2. Command to see documentation and instructions: "man lynis"
3. Command to run an audit: "sudo lynis audit " ("system" is the most common type)
4. Provide a report from the Lynis output on what can be done to harden the system.
    - Screenshot of report output: PDF report of the output (see the "Suggestions" section: https://drive.google.com/file/d/1vqRkYS7wOoC5gSWnnKYLkiGR_0JvmLXB/view?usp=sharing

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: PDF report of the output: https://drive.google.com/file/d/1q6MKhH4JLl3rrubgRoQkZGKtbNU7FB-v/view?usp=sharing