Cybersecurity

Module 4 Challenge Submission File

Linux Systems Administration

Make a copy of this document to work in, and then for each step, add the solution commands below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on `/etc/shadow` should allow only `root` read and write access.
    a. Command to inspect permissions:

```
ls -la /etc/shadow
```

    b. Command to set permissions (if needed):

```
sudo chmod 600 /etc/shadow
```

2. Permissions on `/etc/gshadow` should allow only `root` read and write access.
    a. Command to inspect permissions:

```
ls -la /etc/gshadow
```

    b. 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.

a. Command to inspect permissions:

```
ls -la /etc/group
```

b. 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.

    a. Command to inspect permissions:

```
Ls -la /etc/passwd
```

    b. Command to set permissions (if needed):

```
sudo chmod 644 /etc/group
```

Step 2: Create User Accounts

1. Add user accounts for `sam`, `joe`, `amy`, `sara`, and `admin` with the `useradd` command.

    a. 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
```

2. Ensure that only the `admin` has general sudo access.

    a. 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.
    a. Command to add group:

```
sudo addgroup engineers
```

2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.
    a. 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
```

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

```
Idk why i have to use sudo now but i had to do sudo mkdir engineers
```

4. Change ownership on the new engineers' shared folder to the `engineers` group.
    a. Command to change ownership of engineers' shared folder to `engineers` group:

```
sudo chgrp engineers engineers
```

Step 4: Lynis Auditing

1. Command to install Lynis:

```
sudo apt install Lynis
```

2. Command to view documentation and instructions:

```
man Lynis
```

3. Command to run an audit:

```
lynis audit system
```

4. Provide a report from the Lynis output with recommendations for hardening the system.

    a. Screenshot of report output: uploaded to imgur because it was like 5 screenshots https://imgur.com/gallery/OWJRjQu

Bonus

1. Command to install chkrootkit:

```
sudo apt install chkrootkit
```

2. Command to view documentation and instructions:

```
man chkrootkit
```

3. Command to run expert mode:

```
sudo chkrootkit -x
```

4. Provide a report from the chrootkit output with recommendations for hardening the system.

a. Screenshot of end of sample output: https://imgur.com/gallery/8z24Hq5
Idk if this what you wanted, it did….a lot of things haha.