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 -l /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 -l /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 -l /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 -l /etc/passwd
```

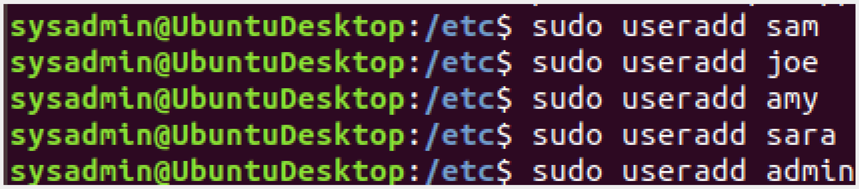
   b. Command to set permissions (if needed):

```
Sudo chmod 644 /etc/passwd
```

Step 2: Create User Accounts

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

   a. Command to add each user account (include all five users):



```
sysadmin@UbuntuDesktop:/etc$ sudo useradd sam
sysadmin@UbuntuDesktop:/etc$ sudo useradd joe
sysadmin@UbuntuDesktop:/etc$ sudo useradd amy
sysadmin@UbuntuDesktop:/etc$ sudo useradd sara
sysadmin@UbuntuDesktop:/etc$ sudo useradd admin
```

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

   a. Command to add `admin` to the sudo group:

```
Sudo usermod -G sudo admin
```

Step 3: Create User Group and Collaborative Folder

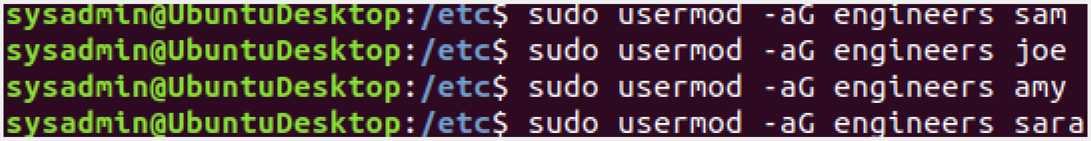
1. Add an `engineers` group to the system.

    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):



```
sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG engineers sam
sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG engineers joe
sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG engineers amy
sysadmin@UbuntuDesktop:/etc$ sudo usermod -aG engineers sara
```

3. Create a shared folder for this group at `/home/engineers`.

    a. Command to create the shared folder:

```
Sudo mkdir /home/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 chown :engineers /home/engineers
```

Step 4: Lynis Auditing

1. Command to install Lynis:

```
Sudo apt install lynis
```

2. Command to view documentation and instructions:

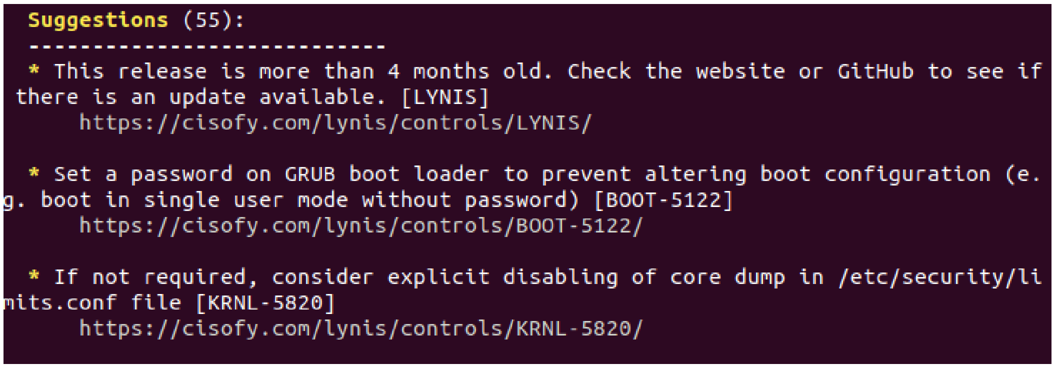
```
Sudo lynis --help
```

3. Command to run an audit:

```
Sudo lynis audit system
```

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

    a. Screenshot of report output:



```
 Suggestions (55):
 ----------------------------
 * This release is more than 4 months old. Check the website or GitHub to see if
there is an update available. [LYNIS]
     https://cisofy.com/lynis/controls/LYNIS/

 * Set a password on GRUB boot loader to prevent altering boot configuration (e.
g. boot in single user mode without password) [BOOT-5122]
     https://cisofy.com/lynis/controls/BOOT-5122/

 * If not required, consider explicit disabling of core dump in /etc/security/li
mits.conf file [KRNL-5820]
     https://cisofy.com/lynis/controls/KRNL-5820/
```

Bonus

1. Command to install chkrootkit:

```
[Enter answer here]
```

2. Command to view documentation and instructions:

```
[Enter answer here]
```

3. Command to run expert mode:

```
[Enter answer here]
```

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

    a. Screenshot of end of sample output: