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):

```
sudo adduser sam
sudo adduser joe
sudo adduser sara
sudo adduser admin
sudo adduser amy
```

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

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

```
sudo usermod -G 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:

```
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 chown :engineers /home/engineers/
```

Step 4: Lynis Auditing

1. Command to install Lynis:

```
sudo apt install lynis
```

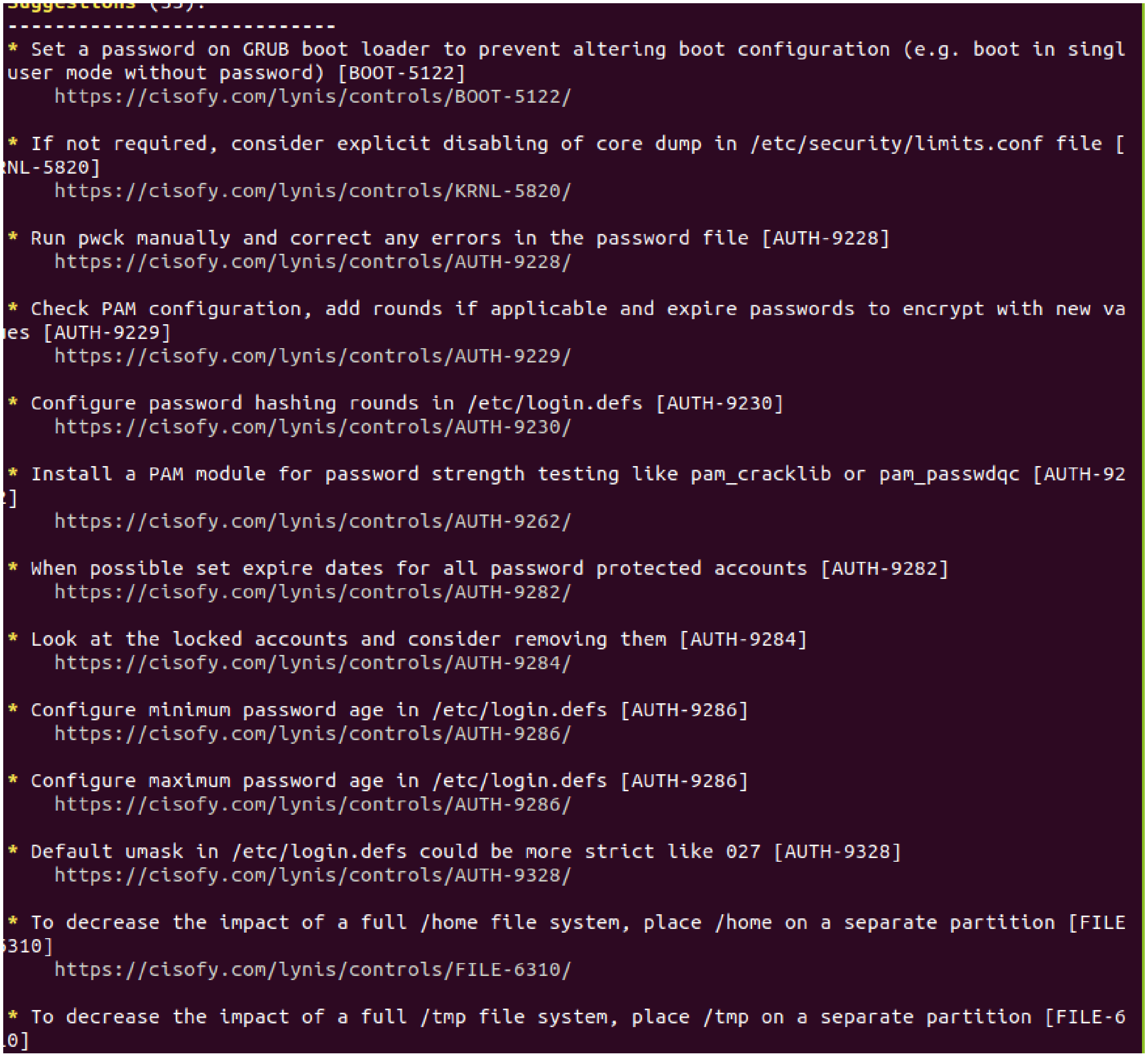
2. Command to view documentation and instructions:

```
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.



```
Suggestions (35):
----------------------------
* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in singl
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/limits.conf file [
NL-5820]
    https://cisofy.com/lynis/controls/KRNL-5820/

* Run pwck manually and correct any errors in the password file [AUTH-9228]
    https://cisofy.com/lynis/controls/AUTH-9228/

* Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new va
es [AUTH-9229]
    https://cisofy.com/lynis/controls/AUTH-9229/

* Configure password hashing rounds in /etc/login.defs [AUTH-9230]
    https://cisofy.com/lynis/controls/AUTH-9230/

* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-92
]
    https://cisofy.com/lynis/controls/AUTH-9262/

* When possible set expire dates for all password protected accounts [AUTH-9282]
    https://cisofy.com/lynis/controls/AUTH-9282/

* Look at the locked accounts and consider removing them [AUTH-9284]
    https://cisofy.com/lynis/controls/AUTH-9284/

* Configure minimum password age in /etc/login.defs [AUTH-9286]
    https://cisofy.com/lynis/controls/AUTH-9286/

* Configure maximum password age in /etc/login.defs [AUTH-9286]
    https://cisofy.com/lynis/controls/AUTH-9286/

* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
    https://cisofy.com/lynis/controls/AUTH-9328/

* To decrease the impact of a full /home file system, place /home on a separate partition [FILE
310]
    https://cisofy.com/lynis/controls/FILE-6310/

* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6
0]
```

Bonus

1. Command to install chkrootkit:

```
sudo apt install chkrootkit
```

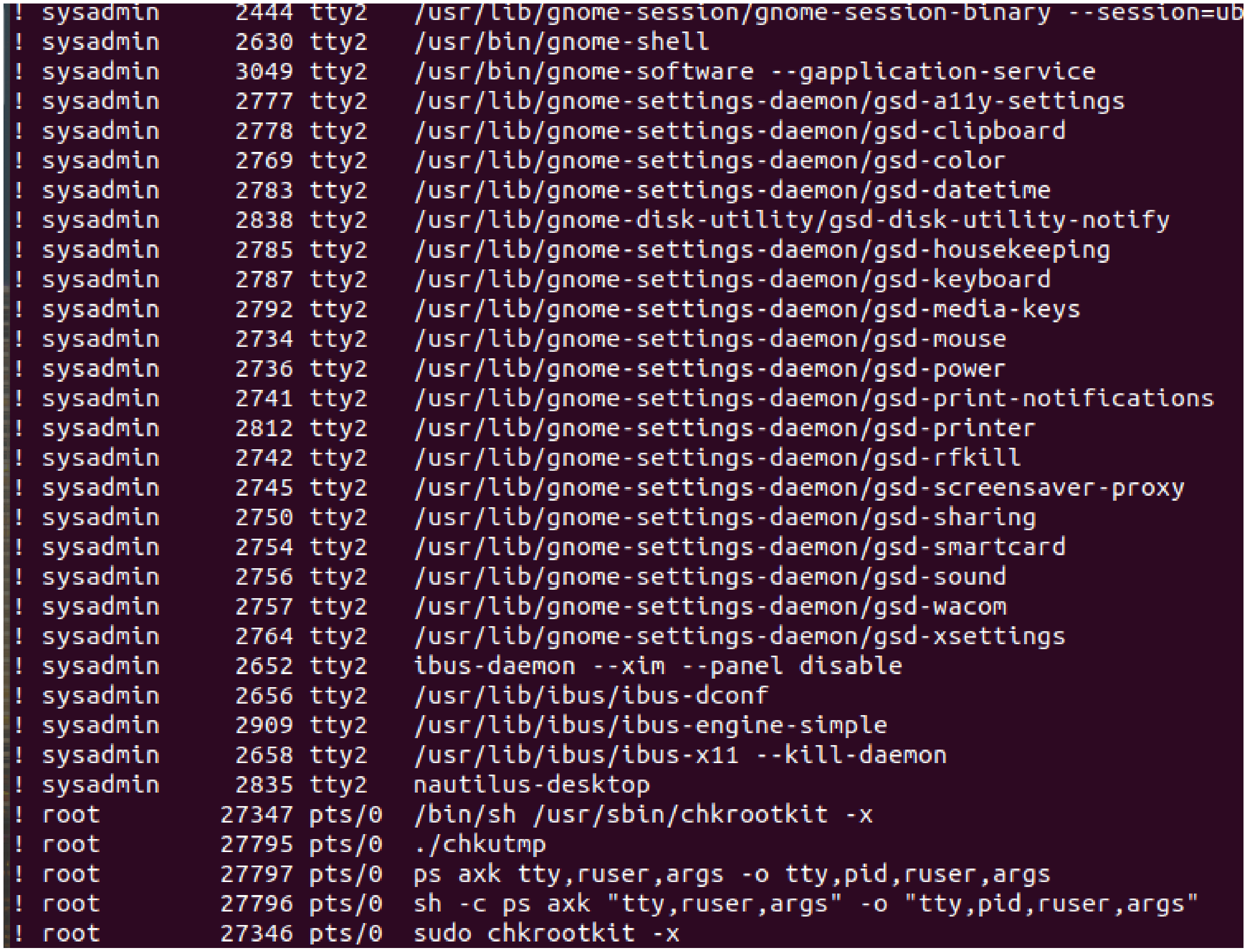
2. Command to view documentation and instructions:

```
chkrootkit —-help
```

3. Command to run expert mode:

```
sudo chkrootkit -x
```

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



```
! sysadmin     2444 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ub
! sysadmin     2630 tty2   /usr/bin/gnome-shell
! sysadmin     3049 tty2   /usr/bin/gnome-software --gapplication-service
! sysadmin     2777 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin     2778 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin     2769 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     2783 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     2838 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     2785 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     2787 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     2792 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     2734 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     2736 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     2741 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     2812 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     2742 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     2745 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     2750 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     2754 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     2756 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     2757 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     2764 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     2652 tty2   ibus-daemon --xim --panel disable
! sysadmin     2656 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     2909 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     2658 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2835 tty2   nautilus-desktop
! root        27347 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root        27795 pts/0  ./chkutmp
! root        27797 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        27796 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        27346 pts/0  sudo chkrootkit -x
```