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 u=rw-,g=---,o=--- /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 u=rw-,g=---,o=--- /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 u=rw-,g=r--,o=r-- /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/group
```

b. Command to set permissions (if needed):

```
sudo chmod u=rw-,g=r--,o=r-- /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 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:

```
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:

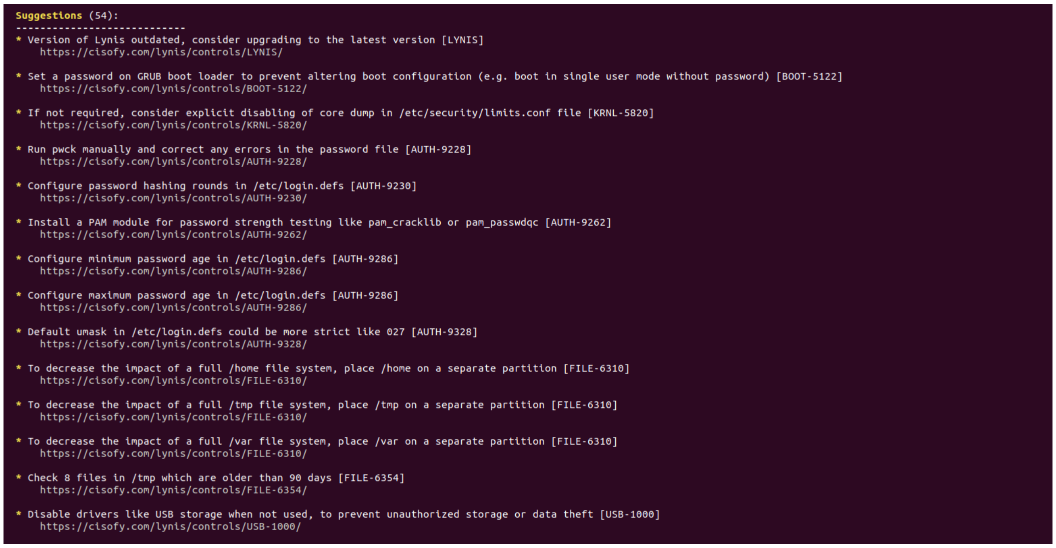
```
man Lynis
```

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:



```
Suggestions (54):
----------------------------
* Version of Lynis outdated, consider upgrading to the latest version [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/limits.conf file [KRNL-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/

* 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-9262]
    https://cisofy.com/lynis/controls/AUTH-9262/

* 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-6310]
    https://cisofy.com/lynis/controls/FILE-6310/

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

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

* Check 8 files in /tmp which are older than 90 days [FILE-6354]
    https://cisofy.com/lynis/controls/FILE-6354/

* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
    https://cisofy.com/lynis/controls/USB-1000/
```

Bonus

1. Command to install chkrootkit:

```
sudo apt install chkrootkit
```

2. Command to view documentation and instructions:

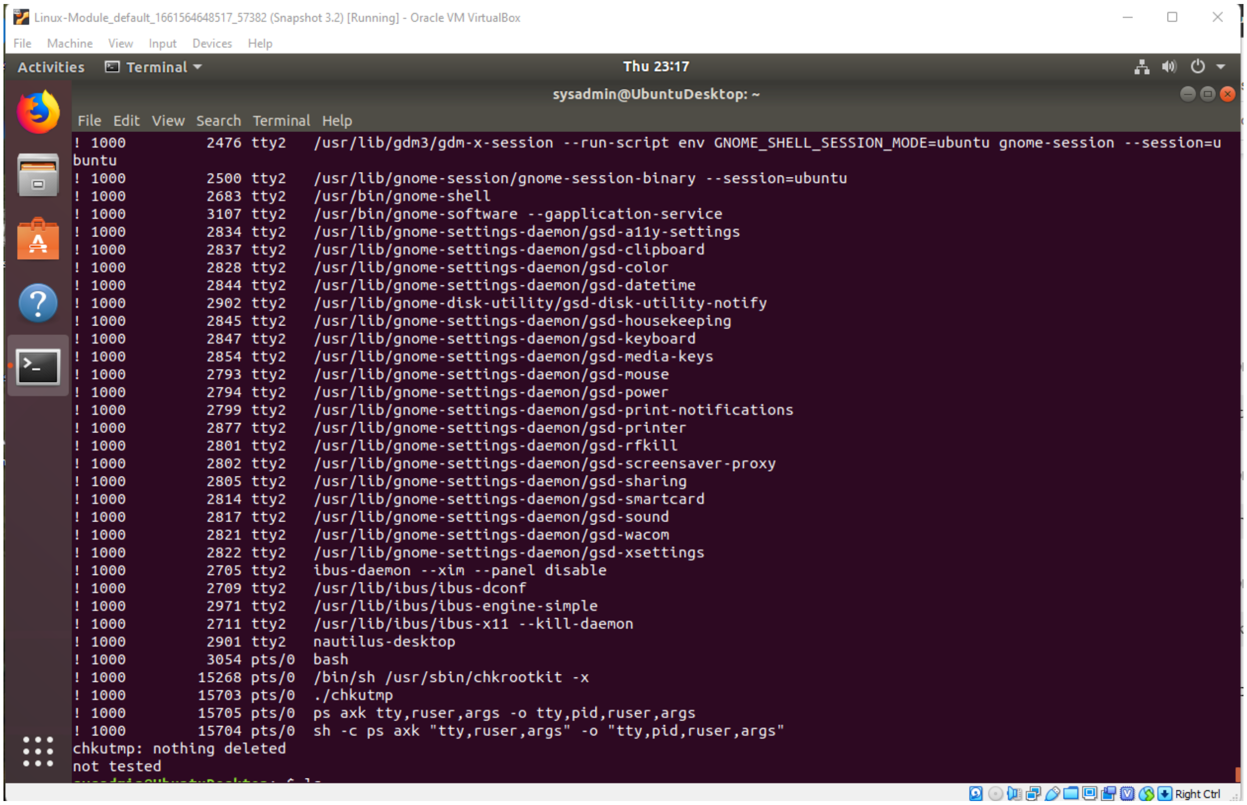
```
man chkrootkit
```

3. Command to run expert mode:

```
chkrootkit -x
```

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

    a. Screenshot of end of sample output:


Linux-Module_default_1661564648517_57382 (Snapshot 3.2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal ▾
Thu 23:17
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Right Ctrl

```
! 1000         2476 tty2   /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=u
buntu
! 1000         2500 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! 1000         2683 tty2   /usr/bin/gnome-shell
! 1000         3107 tty2   /usr/bin/gnome-software --gapplication-service
! 1000         2834 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! 1000         2837 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! 1000         2828 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! 1000         2844 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! 1000         2902 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! 1000         2845 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! 1000         2847 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! 1000         2854 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! 1000         2793 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! 1000         2794 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! 1000         2799 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! 1000         2877 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! 1000         2801 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! 1000         2802 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! 1000         2805 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! 1000         2814 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! 1000         2817 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! 1000         2821 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! 1000         2822 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! 1000         2705 tty2   ibus-daemon --xim --panel disable
! 1000         2709 tty2   /usr/lib/ibus/ibus-dconf
! 1000         2971 tty2   /usr/lib/ibus/ibus-engine-simple
! 1000         2711 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! 1000         2901 tty2   nautilus-desktop
! 1000         3054 pts/0  bash
! 1000        15268 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! 1000        15703 pts/0  ./chkutmp
! 1000        15705 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! 1000        15704 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
chkutmp: nothing deleted
not tested
```