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:

```
[sudo ls -l /etc/shadow]
```

    b. Command to set permissions (if needed):

```
[sudo chmod /etc/gshadow xxx]
```

2. Permissions on `/etc/gshadow` should allow only `root` read and write access.

    a. Command to inspect permissions:

```
[sudo ls -l /etc/gshadow]
```

    b. Command to set permissions (if needed):

```
[sudo chmod /etc/gshadow xxx]
```

3. Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else read access only.

a. Command to inspect permissions:

```
[sudo ls -l /etc/group]
```

b. Command to set permissions (if needed):

```
[sudo chmod /etc/group xxx]
```

4. Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else read access only.

a. Command to inspect permissions:

```
[sudo ls -l /etc/passwd]
```

b. Command to set permissions (if needed):

```
[sudo chmod ls -l /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):

```
[adduser --system sam]
[adduser --system joe]
[adduser --system amy]
[adduser --system sara]
[adduser --system 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 -R admin engineers]
```

## Step 4: Lynis Auditing

1. Command to install Lynis:

```
[sudo apt install lynis]
```

2. Command to view documentation and instructions:

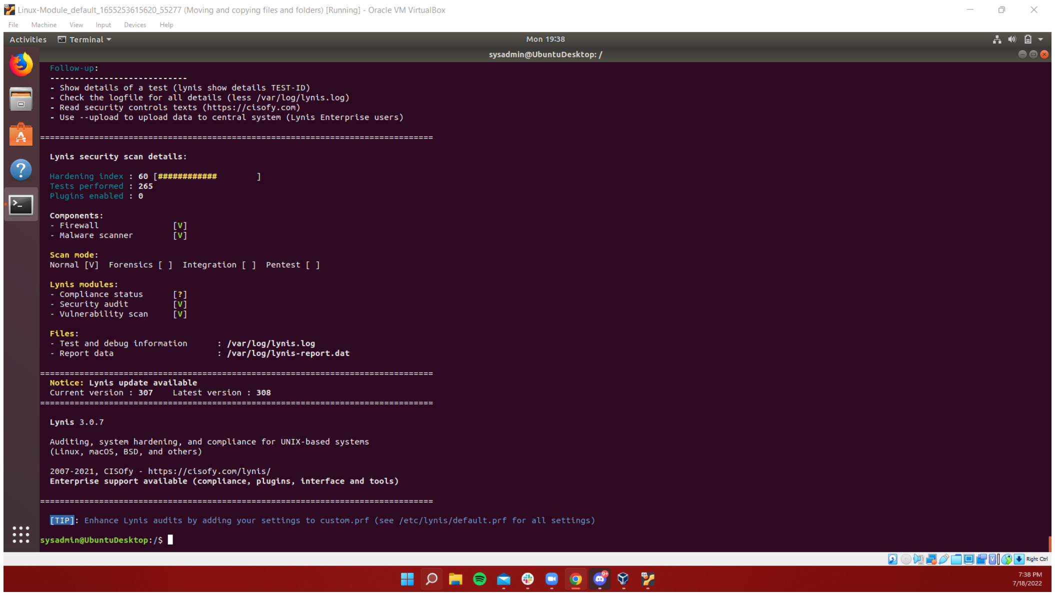
```
[man lynis]
```

3. Command to run an audit:

```
[sudo lynis audit system]
```

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

    a. Screenshot of report output:


Linux-Module_default_1655253615620_55277 (Moving and copying files and folders) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Activities
Terminal
Mon 19:38
sysadmin@UbuntuDesktop: /
7:38 PM
7/18/2022

```
  Follow-up:
  ----------------------------
  - Show details of a test (lynis show details TEST-ID)
  - Check the logfile for all details (less /var/log/lynis.log)
  - Read security controls texts (https://cisofy.com)
  - Use --upload to upload data to central system (Lynis Enterprise users)

================================================================================

  Lynis security scan details:

  Hardening index : 60 [############        ]
  Tests performed : 265
  Plugins enabled : 0

  Components:
  - Firewall               [V]
  - Malware scanner        [V]

  Scan mode:
  Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================
  Notice: Lynis update available
  Current version : 307    Latest version : 308
================================================================================

  Lynis 3.0.7

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

sysadmin@UbuntuDesktop:/$ 
```

## Bonus

1. Command to install chkrootkit:

```
[sudo apt install chkrootkit]
```

2. Command to view documentation and instructions:

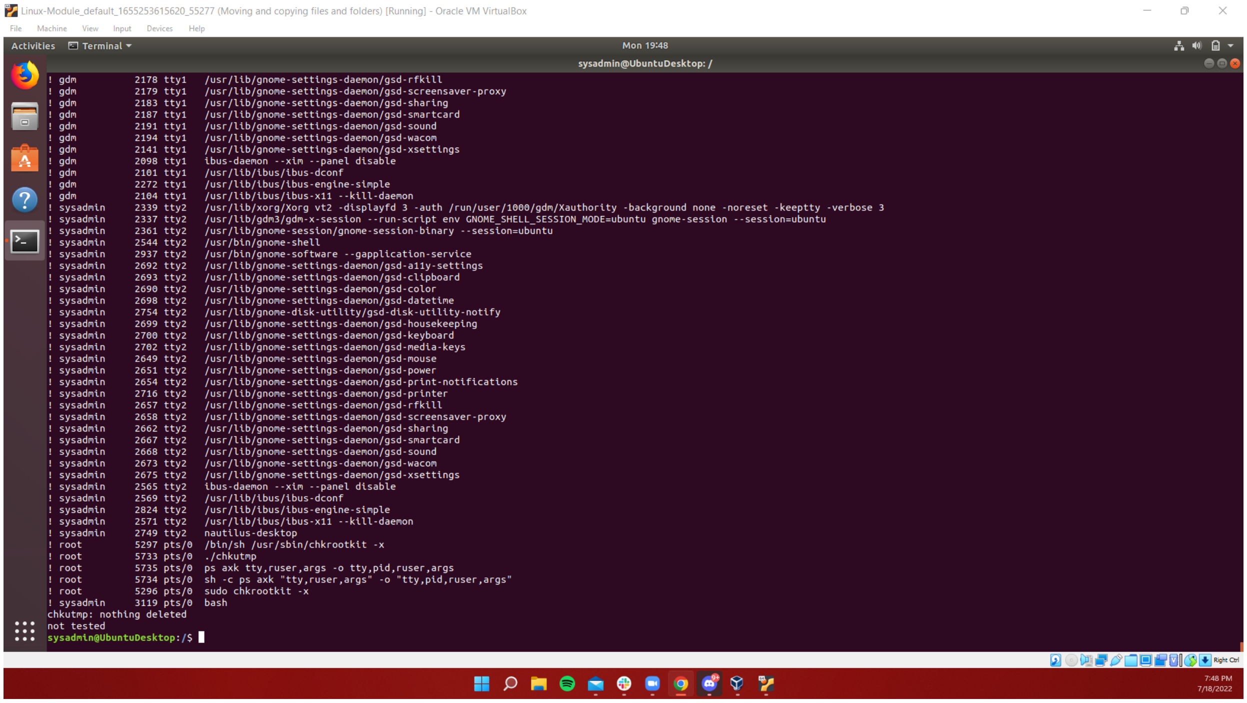
```
[man chkrootkit]
```

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:



Linux-Module_default_1655253615620_55277 (Moving and copying files and folders) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Activities
Terminal
Mon 19:48
sysadmin@UbuntuDesktop: /
7:48 PM
7/18/2022

```
! gdm          2178 tty1   /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm          2179 tty1   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm          2183 tty1   /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm          2187 tty1   /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm          2191 tty1   /usr/lib/gnome-settings-daemon/gsd-sound
! gdm          2194 tty1   /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm          2141 tty1   /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm          2098 tty1   ibus-daemon --xim --panel disable
! gdm          2101 tty1   /usr/lib/ibus/ibus-dconf
! gdm          2272 tty1   /usr/lib/ibus/ibus-engine-simple
! gdm          2104 tty1   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2339 tty2   /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! sysadmin     2337 tty2   /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin     2361 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin     2544 tty2   /usr/bin/gnome-shell
! sysadmin     2937 tty2   /usr/bin/gnome-software --gapplication-service
! sysadmin     2692 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin     2693 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin     2690 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     2698 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     2754 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     2699 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     2700 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     2702 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     2649 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     2651 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     2654 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     2716 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     2657 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     2658 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     2662 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     2667 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     2668 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     2673 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     2675 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     2565 tty2   ibus-daemon --xim --panel disable
! sysadmin     2569 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     2824 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     2571 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2749 tty2   nautilus-desktop
! root         5297 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root         5733 pts/0  ./chkutmp
! root         5735 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root         5734 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root         5296 pts/0  sudo chkrootkit -x
! sysadmin     3119 pts/0  bash
chkutmp: nothing deleted
not tested
sysadmin@UbuntuDesktop:/$ 
```