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 chown root: /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 chown root: /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 chown root: /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 chown root: /etc/passwd
```

Step 2: Create User Accounts

1. Add user accounts for `sam`, `joe`, `amy`, `sara`, and `admin1` 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 admin1
```

2. Ensure that only the `admin1` has general sudo access.

    a. Command to add `admin1` to the sudo group:

```
sudo visudo
admin1 ALL=(ALL:ALL) /usr/bin/less
sudo grep less /etc/sudoers
```

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 -G engineers sam
sudo usermod -G engineers joe
sudo usermod -G engineers amy
sudo usermod -G engineers sara
```

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

    a. Command to create the shared folder:

```
sudo mkdir /home/egineers
```

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:

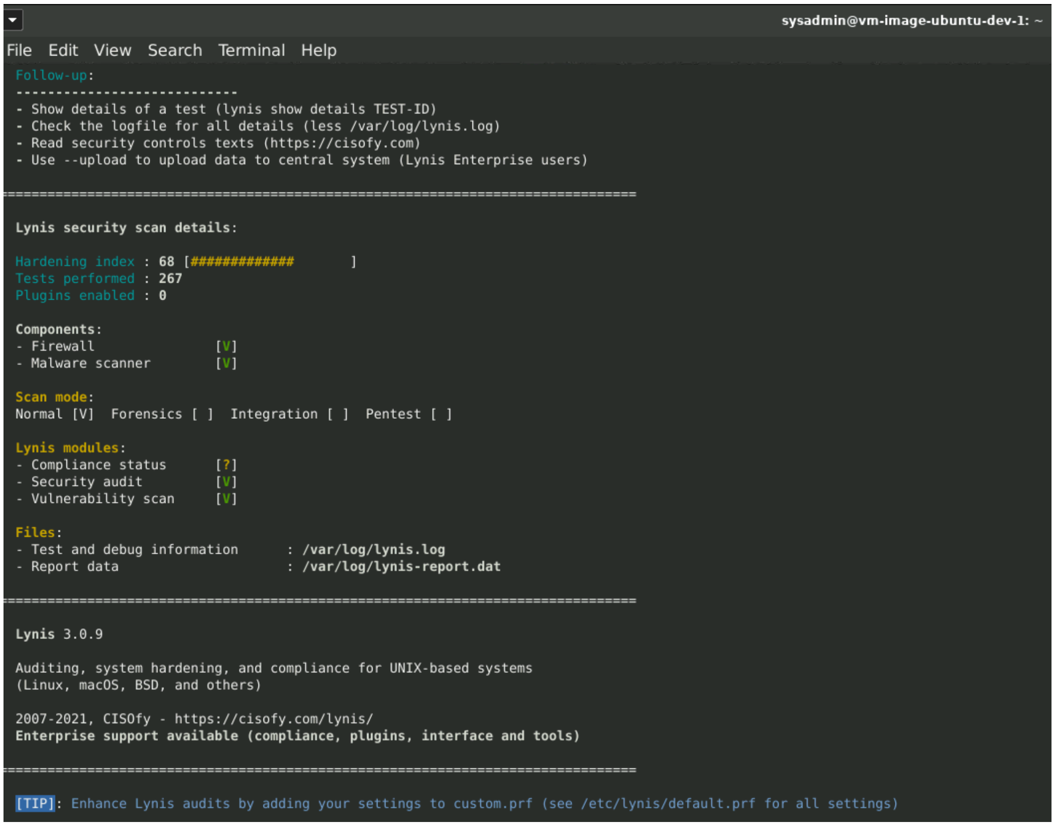
```
man lynis
```

3. Command to run an audit:

```
sudo lynis audit system
```

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

   a. Screenshot of report output:


sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help

```
  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 : 68 [#############       ]
  Tests performed : 267
  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

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

  Lynis 3.0.9

  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)
```

Optional Additional Challenge

1. Command to install chkrootkit:

```
sudo apt install chkrootkit
```

2. Command to view documentation and instructions:

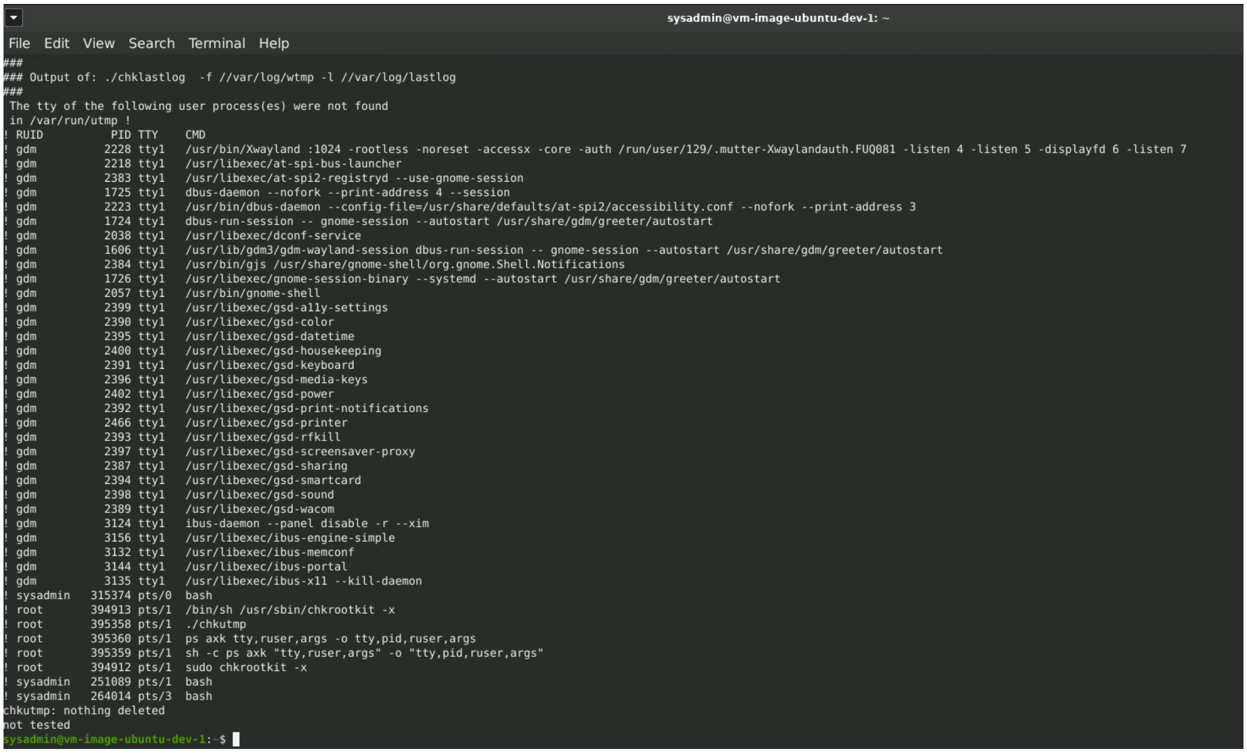
```
Sudo man chkrootkit
```

3. Command to run expert mode:

```
sudo chkroot -x
```

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

   a. Screenshot of end of sample output:



sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help

```
###
### Output of: ./chklastlog  -f //var/log/wtmp -l //var/log/lastlog
###
 The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          2228 tty1   /usr/bin/Xwayland :1024 -rootless -noreset -accessx -core -auth /run/user/129/.mutter-Xwaylandauth.FUQ081 -listen 4 -listen 5 -displayfd 6 -listen 7
! gdm          2218 tty1   /usr/libexec/at-spi-bus-launcher
! gdm          2383 tty1   /usr/libexec/at-spi2-registryd --use-gnome-session
! gdm          1725 tty1   dbus-daemon --nofork --print-address 4 --session
! gdm          2223 tty1   /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
! gdm          1724 tty1   dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          2038 tty1   /usr/libexec/dconf-service
! gdm          1606 tty1   /usr/lib/gdm3/gdm-wayland-session dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          2384 tty1   /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
! gdm          1726 tty1   /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
! gdm          2057 tty1   /usr/bin/gnome-shell
! gdm          2399 tty1   /usr/libexec/gsd-a11y-settings
! gdm          2390 tty1   /usr/libexec/gsd-color
! gdm          2395 tty1   /usr/libexec/gsd-datetime
! gdm          2400 tty1   /usr/libexec/gsd-housekeeping
! gdm          2391 tty1   /usr/libexec/gsd-keyboard
! gdm          2396 tty1   /usr/libexec/gsd-media-keys
! gdm          2402 tty1   /usr/libexec/gsd-power
! gdm          2392 tty1   /usr/libexec/gsd-print-notifications
! gdm          2466 tty1   /usr/libexec/gsd-printer
! gdm          2393 tty1   /usr/libexec/gsd-rfkill
! gdm          2397 tty1   /usr/libexec/gsd-screensaver-proxy
! gdm          2387 tty1   /usr/libexec/gsd-sharing
! gdm          2394 tty1   /usr/libexec/gsd-smartcard
! gdm          2398 tty1   /usr/libexec/gsd-sound
! gdm          2389 tty1   /usr/libexec/gsd-wacom
! gdm          3124 tty1   ibus-daemon --panel disable -r --xim
! gdm          3156 tty1   /usr/libexec/ibus-engine-simple
! gdm          3132 tty1   /usr/libexec/ibus-memconf
! gdm          3144 tty1   /usr/libexec/ibus-portal
! gdm          3135 tty1   /usr/libexec/ibus-x11 --kill-daemon
! sysadmin   315374 pts/0  bash
! root       394913 pts/1  /bin/sh /usr/sbin/chkrootkit -x
! root       395358 pts/1  ./chkutmp
! root       395360 pts/1  ps axk tty,ruser,args -o tty,pid,ruser,args
! root       395359 pts/1  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root       394912 pts/1  sudo chkrootkit -x
! sysadmin   251089 pts/1  bash
! sysadmin   264014 pts/3  bash
chkutmp: nothing deleted
not tested
sysadmin@vm-image-ubuntu-dev-1:~$
```