Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on /etc/shadow should allow only root read and write access.

    - Command to inspect permissions: **cd /etc/shadow ls-l**

    - Command to set permissions (if needed): **sudo chmod 600 /etc/shadow**

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

    - Command to inspect permissions: **cd /etc/gshadow ls-l**

    - 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.

    - Command to inspect permissions: **cd /etc/group ls-l**

    - 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.

    - Command to inspect permissions: **cd /etc/passwd ls-l**

    - 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.

    - 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.

    - 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.

    - Command to add group:
    - **sudo addgroup engineers**
2. Add users sam, joe, amy, and sara to the managed group.

  - Command to add users to engineers group (include all four users):
  - **sudo usermod -a -G engineers sam joe amy sara admin**

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

    - Command to create the shared folder:
    - **Mkdir /home/engineers**

4. Change ownership on the new engineers' shared folder to the engineers group.

    - Command to change ownership of engineer's shared folder to engineer group:
    - **sudo chown admin:engineers /home/engineers**

Step 4: Lynis Auditing

1. Command to install Lynis:**sudo apt-get install lynis**

2. Command to see documentation and instructions: **man lynis**

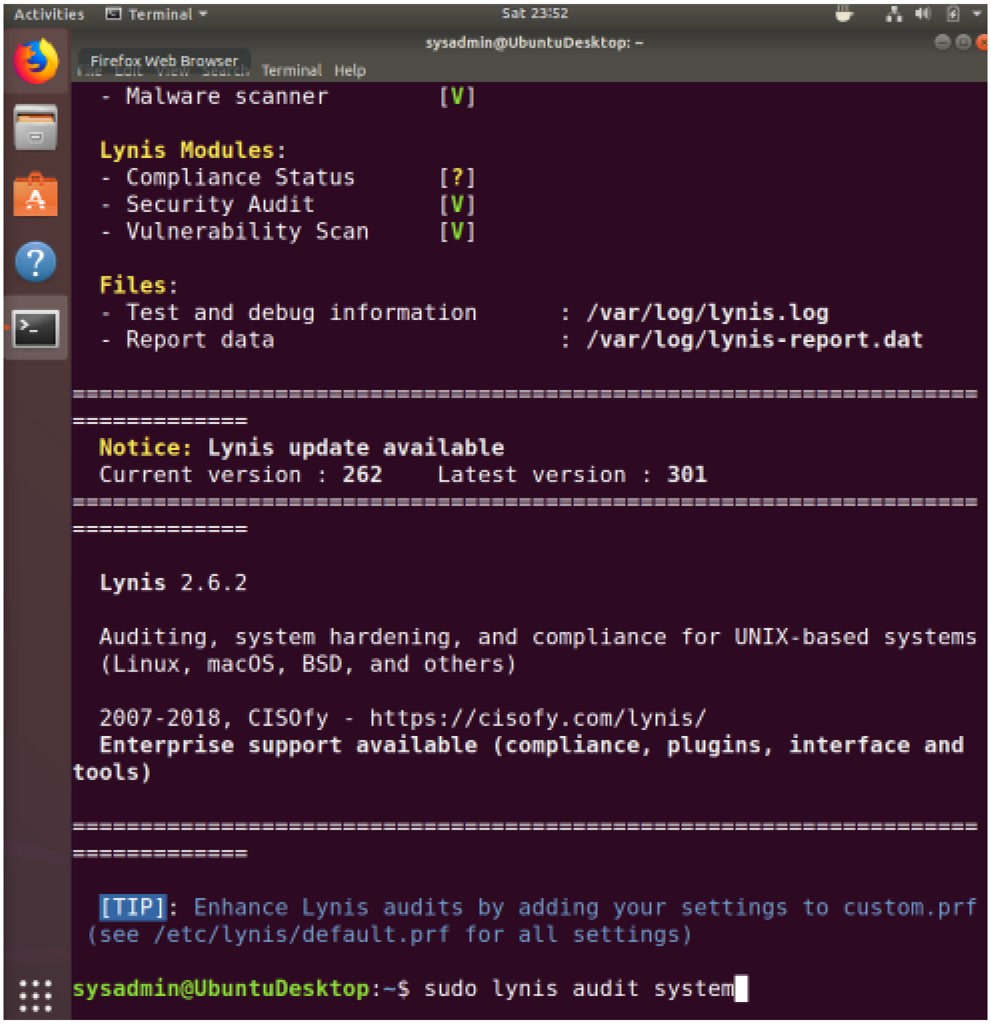
3. Command to run an audit: **sudo audit lynis system**

4. Provide a report from the Lynis output on what can be done to harden the system.
   In the report from lynis, parts of the message displayed this:

```
Warnings (4):

  ! Version of Lynis is very old and should be updated [LYNIS]

      https://cisofy.com/controls/LYNIS/

  ! No password set for single mode [AUTH-9308]

      https://cisofy.com/controls/AUTH-9308/

  ! Found one or more vulnerable packages. [PKGS-7392]

      https://cisofy.com/controls/PKGS-7392/

  ! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]

      https://cisofy.com/controls/MAIL-8818/

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

  Notice: Lynis update available

  Current version : 262    Latest version : 301

=======================================================================
```

Lynis needs to be updated to the most recent version. And passwords set properly for single mode. Removing vulnerable packages to fortify the system and be more secure.

  - Screenshot of report output:



```
  - Malware scanner         [V]

  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 : 262    Latest version : 301
=====================================================================
=============

  Lynis 2.6.2

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

  2007-2018, 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:~$ sudo lynis audit system
```

Bonus

1. Command to install chkrootkit: **sudo apt-get install chkrootkit**

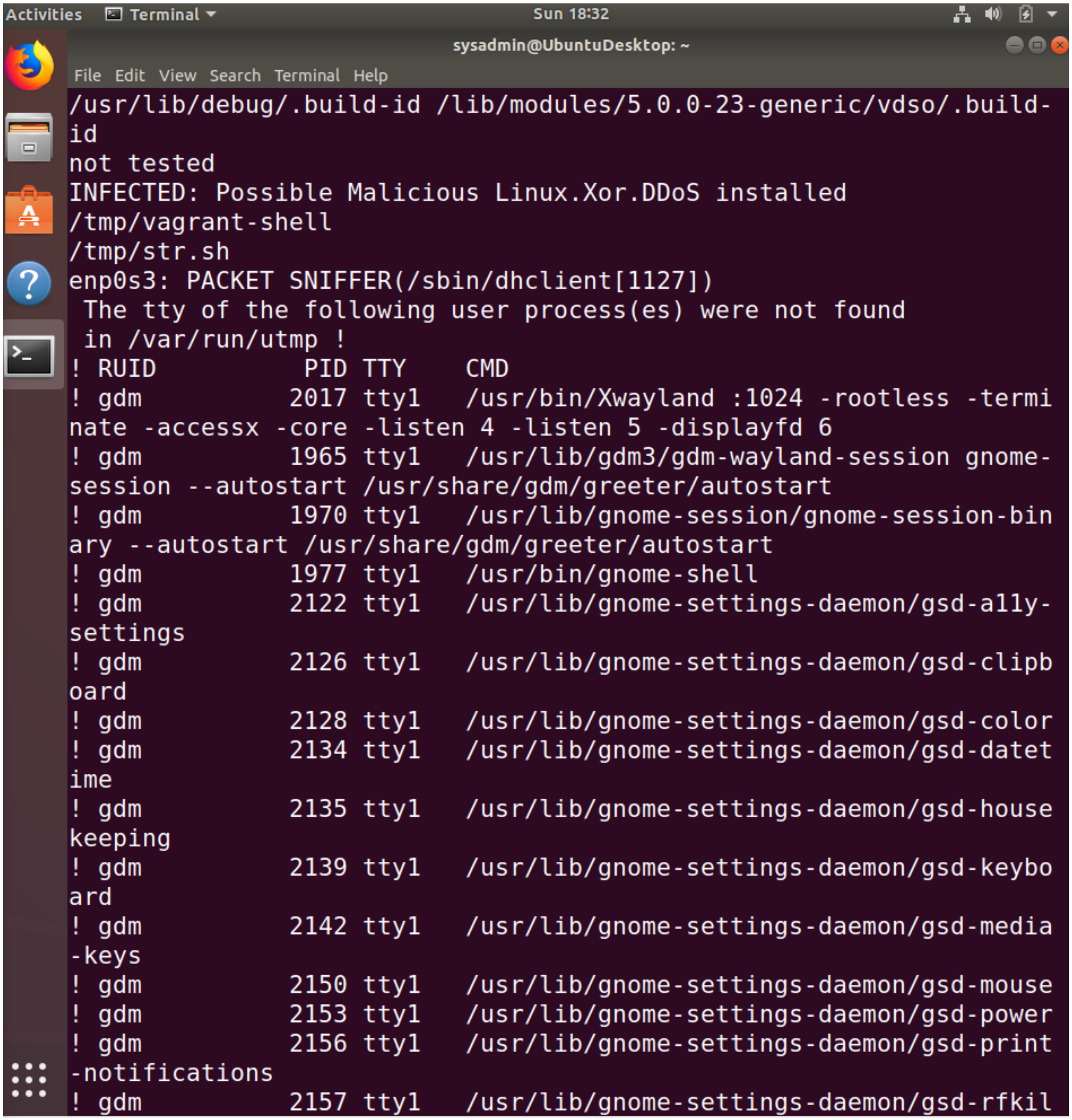
2. Command to see documentation and instructions: **man chkrootkit**

3. Command to run expert mode: **sudo chkrootkit -x**

4. Provide a report from the chrootkit output on what can be done to harden the system.

   Remove possible malicious linux.xor.ddos vagrant shell from tmp folder, or set a crontab to cleanup or remove anything from the tmp folder at the end of every work shift

   - Screenshot of end of sample output:



```
/usr/lib/debug/.build-id /lib/modules/5.0.0-23-generic/vdso/.build-
id
not tested
INFECTED: Possible Malicious Linux.Xor.DDoS installed
/tmp/vagrant-shell
/tmp/str.sh
enp0s3: PACKET SNIFFER(/sbin/dhclient[1127])
 The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          2017 tty1   /usr/bin/Xwayland :1024 -rootless -termi
nate -accessx -core -listen 4 -listen 5 -displayfd 6
! gdm          1965 tty1   /usr/lib/gdm3/gdm-wayland-session gnome-
session --autostart /usr/share/gdm/greeter/autostart
! gdm          1970 tty1   /usr/lib/gnome-session/gnome-session-bin
ary --autostart /usr/share/gdm/greeter/autostart
! gdm          1977 tty1   /usr/bin/gnome-shell
! gdm          2122 tty1   /usr/lib/gnome-settings-daemon/gsd-a11y-
settings
! gdm          2126 tty1   /usr/lib/gnome-settings-daemon/gsd-clipb
oard
! gdm          2128 tty1   /usr/lib/gnome-settings-daemon/gsd-color
! gdm          2134 tty1   /usr/lib/gnome-settings-daemon/gsd-datet
ime
! gdm          2135 tty1   /usr/lib/gnome-settings-daemon/gsd-house
keeping
! gdm          2139 tty1   /usr/lib/gnome-settings-daemon/gsd-keybo
ard
! gdm          2142 tty1   /usr/lib/gnome-settings-daemon/gsd-media
-keys
! gdm          2150 tty1   /usr/lib/gnome-settings-daemon/gsd-mouse
! gdm          2153 tty1   /usr/lib/gnome-settings-daemon/gsd-power
! gdm          2156 tty1   /usr/lib/gnome-settings-daemon/gsd-print
-notifications
! gdm          2157 tty1   /usr/lib/gnome-settings-daemon/gsd-rfkil
```