Week 4 Homework Submission File: Linux Systems Administration

**Note – all commands to run are light blue in sequence
# are explanations of the commands used

Step 1: Ensure Permissions on Sensitive Files

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

   ○ Command to inspect permissions:

     Open Terminal login into sysadmin from ~ navigate to /etc

     Run the command:

     ```
     ls -al /etc/shadow
     ```

     # -l list files in long format -a shows hidden files

   ○ Command to set permissions (if needed):

     ```
     sudo chmod 600 /etc/shadow
     ```

     #chmod sets file permissions

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

   ○ Command to inspect permissions:

     ```
     ls -al /etc/gshadow
     ```

   ○ Command to set permissions (if needed):

     ```
     sudo chmod 600 /etc/gshadow
     ```

     #chmod sets file permissions

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

   ○ Command to inspect permissions:

```
ls -al /etc/group
```

- ○ Command to set permissions (if needed):

```
sudo chmod 644 /etc/group

#chmod sets file permissions
```

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

- ○ Command to inspect permissions:

```
ls -al /etc/passwd
```

- ○ Command to set permissions (if needed):

```
sudo chmod 644 /etc/passwd

#chmod sets file permissions
```

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):

Move to the /home directory and run the following command:

```
for u in sam joe amy sara admin; do sudo useradd -m $u; echo "$u:Password" | sudo chpasswd $u; done
```

Check users are created, run: sudo tail -n5 /etc/shadow /etc/passwd

```
#for u – creates multiple users with u being the variable

#useradd -m adds a home directory

#echo $u:Password – creates a default user password as “Password”

#chpasswd – command reads a list of user name and password pairs from

 standard input and uses this information to update a group of existing

 users. Each line is of the format: user_name:password
```

2. **Force users to create 16-character passwords incorporating numbers and symbols.**

   From /home directory and run the following command:

   ```
   for u in sam joe amy sara admin; do sudo chage -d 0 $u; done
   ```

   - Command to edit pwquality.conf file:

     Move to /etc/security run:

     ```
     sudo nano /etc/security/pwquality.conf
     ```

     ```
     #navigate down the list to make required changes to pwquality
     ```

   - Updates to configuration file:

     ```
     minclass = 4
     ```

     ```
     minlen = 16
     ```

3. **Force passwords to expire every 90 days**.

   - Command to set each new user's password to expire in 90 days (include all five users):

     From /etc/security run:

     ```
     for u in sam joe amy sara admin; do sudo chage -M 90 $u; done
     ```

4. **Ensure that only the admin has general sudo access.**

   #Check: sudo visudo for admin 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):

      ```
      for u in sam joe amy sara; do sudo usermod -G engineers $u; done


      #check: grep 'engineers' /etc/group
      ```

3. **Create a shared folder for this group at /home/engineers.**
    - Command to create the shared folder:

      ```
      sudo 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 root:engineers engineers
      ```

5. **Add the SGID bit and the sticky bit to allow collaboration between engineers in this directory**.

    - Command to set SGID and sticky bit to shared folder:

      ```
      sudo chmod g+s,o+t /home/engineers
      ```

Step 4: Lynis Auditing

1. Command to install Lynis:

    ```
    sudo apt -y install lynis
    ```

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

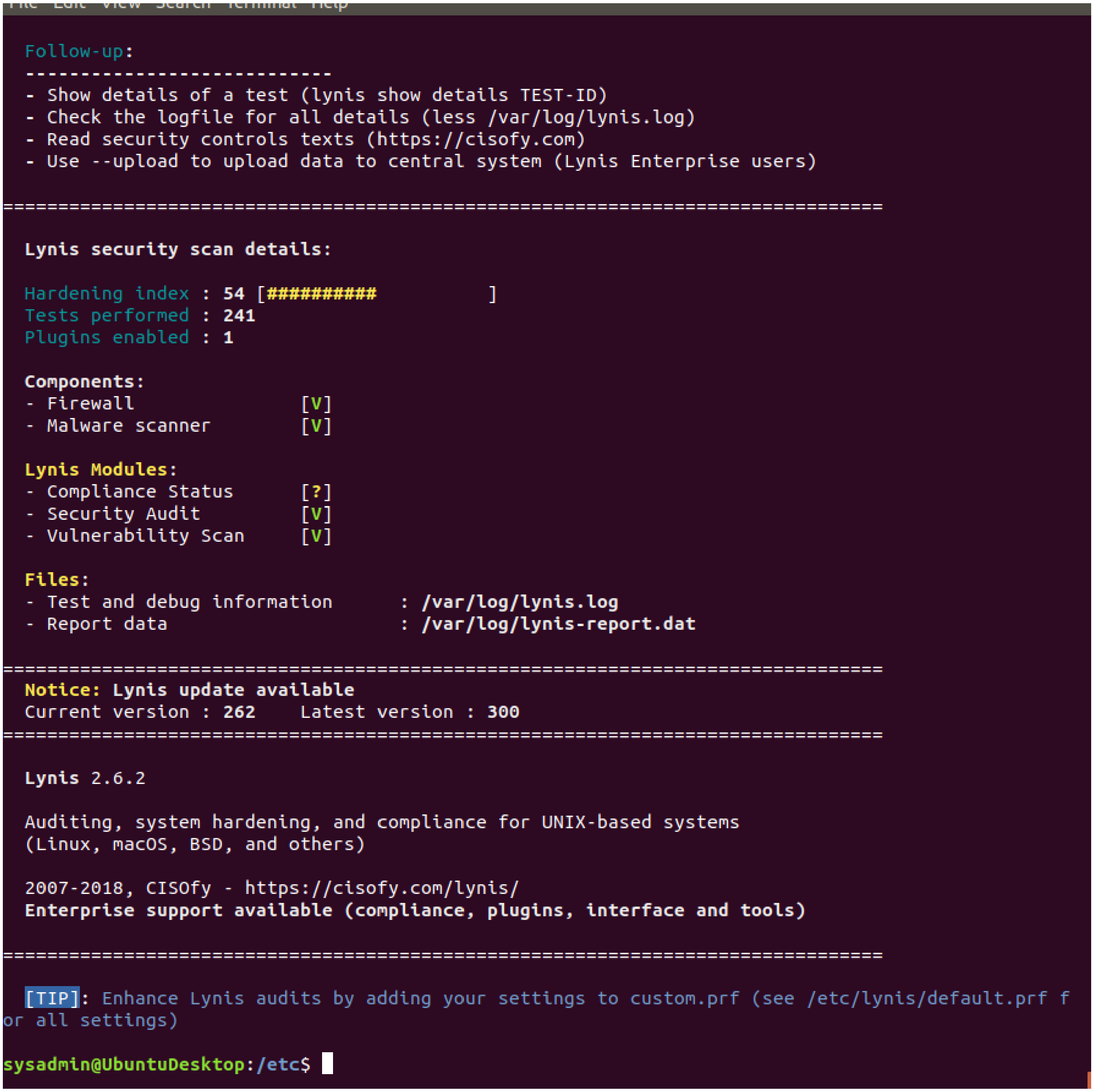
3. Command to run an audit: `sudo lynis audit system`

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

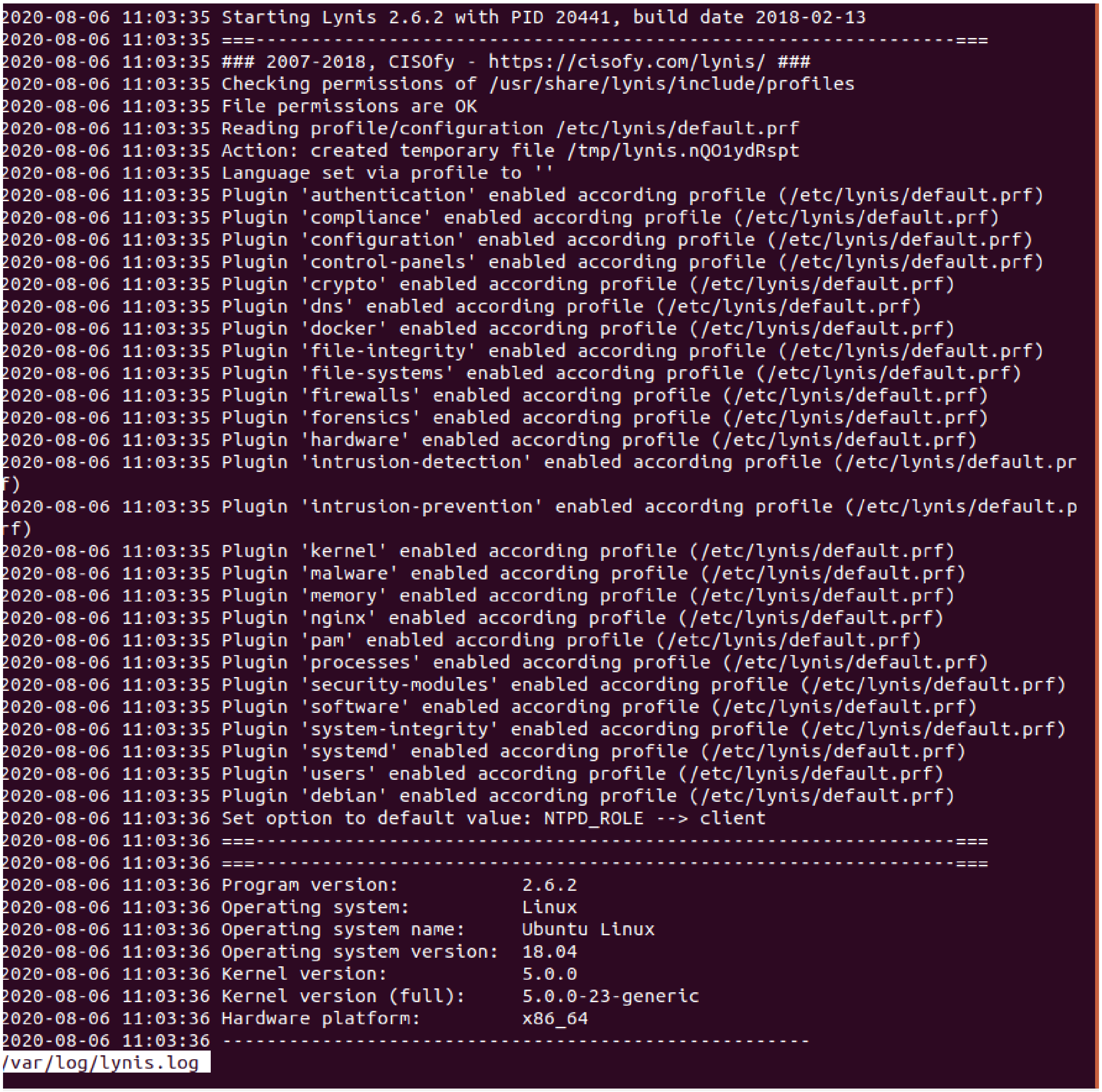
    - Screenshot of report output:

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


  -[ Lynis 2.6.2 Results ]-
```

Warnings (5):



```
  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 : 54 [##########          ]
  Tests performed : 241
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - 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 : 300
================================================================================

  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 f
or all settings)

sysadmin@UbuntuDesktop:/etc$ 
```



```
2020-08-06 11:03:35 Starting Lynis 2.6.2 with PID 20441, build date 2018-02-13
2020-08-06 11:03:35 ===---------------------------------------------------------------===
2020-08-06 11:03:35 ### 2007-2018, CISOfy - https://cisofy.com/lynis/ ###
2020-08-06 11:03:35 Checking permissions of /usr/share/lynis/include/profiles
2020-08-06 11:03:35 File permissions are OK
2020-08-06 11:03:35 Reading profile/configuration /etc/lynis/default.prf
2020-08-06 11:03:35 Action: created temporary file /tmp/lynis.nQO1ydRspt
2020-08-06 11:03:35 Language set via profile to ''
2020-08-06 11:03:35 Plugin 'authentication' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'compliance' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'configuration' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'control-panels' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'crypto' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'dns' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'docker' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'file-integrity' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'file-systems' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'firewalls' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'forensics' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'hardware' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'intrusion-detection' enabled according profile (/etc/lynis/default.pr
f)
2020-08-06 11:03:35 Plugin 'intrusion-prevention' enabled according profile (/etc/lynis/default.p
rf)
2020-08-06 11:03:35 Plugin 'kernel' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'malware' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'memory' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'nginx' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'pam' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'processes' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'security-modules' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'software' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'system-integrity' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'systemd' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'users' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:35 Plugin 'debian' enabled according profile (/etc/lynis/default.prf)
2020-08-06 11:03:36 Set option to default value: NTPD_ROLE --> client
2020-08-06 11:03:36 ===---------------------------------------------------------------===
2020-08-06 11:03:36 ===---------------------------------------------------------------===
2020-08-06 11:03:36 Program version:           2.6.2
2020-08-06 11:03:36 Operating system:          Linux
2020-08-06 11:03:36 Operating system name:     Ubuntu Linux
2020-08-06 11:03:36 Operating system version:  18.04
2020-08-06 11:03:36 Kernel version:            5.0.0
2020-08-06 11:03:36 Kernel version (full):     5.0.0-23-generic
2020-08-06 11:03:36 Hardware platform:         x86_64
2020-08-06 11:03:36 -----------------------------------------------------
/var/log/lynis.log
```

Bonus

1. Command to install chkrootkit: sudo apt -y install chkrootkit
2. Command to see documentation and instructions: man chkrootkit
3. Command to run expert mode:

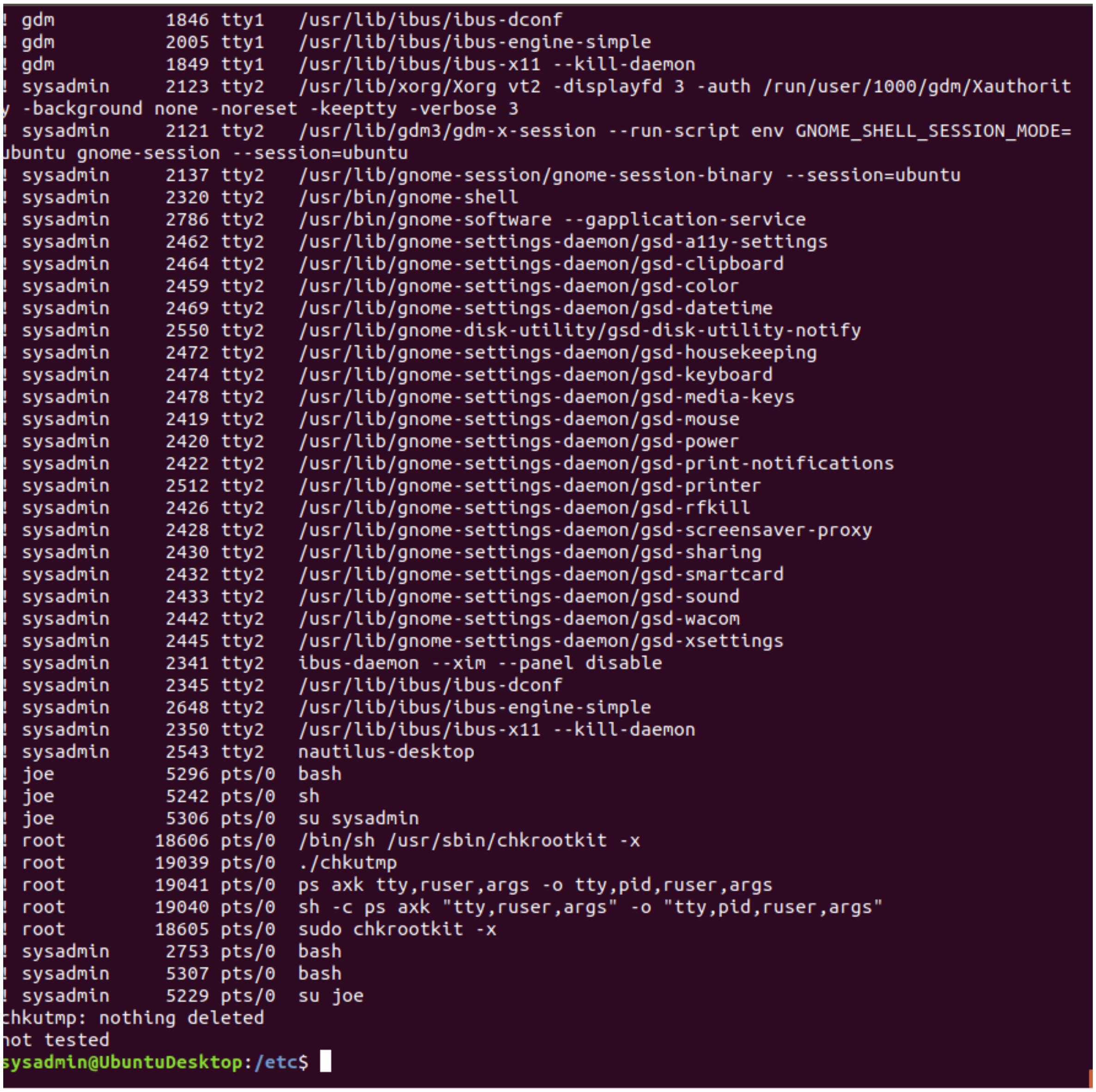
   sudo chkrootkit -x

   sudo chkrootkit -q

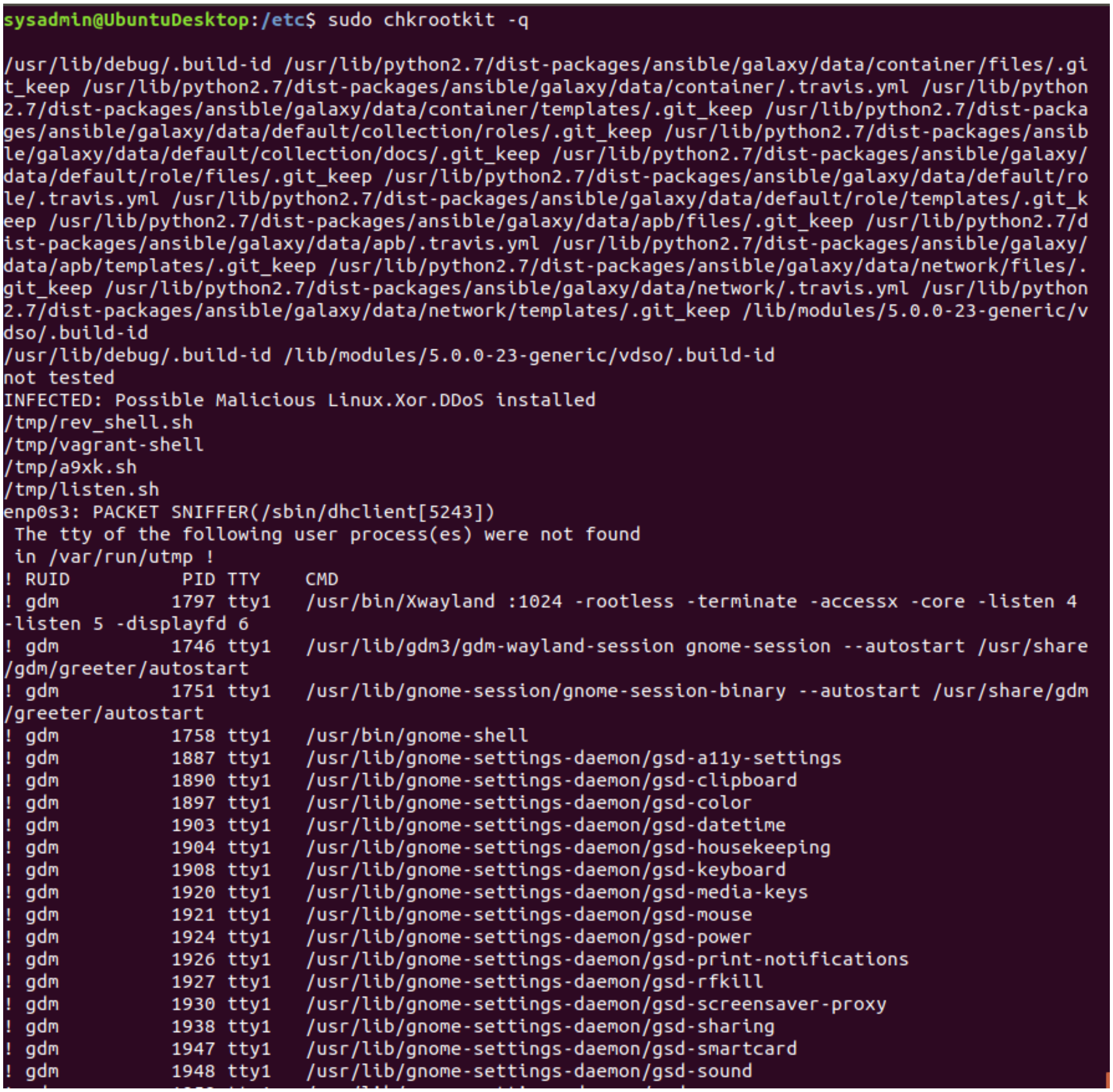
   sudo chkrootkit | grep INFECTED

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

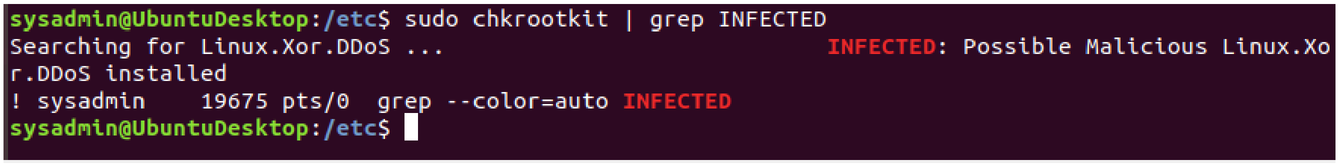
   ○ Screenshot of end of sample output:



```
! gdm          1846 tty1   /usr/lib/ibus/ibus-dconf
! gdm          2005 tty1   /usr/lib/ibus/ibus-engine-simple
! gdm          1849 tty1   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2123 tty2   /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthorit
y -background none -noreset -keeptty -verbose 3
! sysadmin     2121 tty2   /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=
ubuntu gnome-session --session=ubuntu
! sysadmin     2137 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin     2320 tty2   /usr/bin/gnome-shell
! sysadmin     2786 tty2   /usr/bin/gnome-software --gapplication-service
! sysadmin     2462 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin     2464 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin     2459 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     2469 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     2550 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     2472 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     2474 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     2478 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     2419 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     2420 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     2422 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     2512 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     2426 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     2428 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     2430 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     2432 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     2433 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     2442 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     2445 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     2341 tty2   ibus-daemon --xim --panel disable
! sysadmin     2345 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     2648 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     2350 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2543 tty2   nautilus-desktop
! joe          5296 pts/0  bash
! joe          5242 pts/0  sh
! joe          5306 pts/0  su sysadmin
! root        18606 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root        19039 pts/0  ./chkutmp
! root        19041 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        19040 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        18605 pts/0  sudo chkrootkit -x
! sysadmin     2753 pts/0  bash
! sysadmin     5307 pts/0  bash
! sysadmin     5229 pts/0  su joe
hkutmp: nothing deleted
ot tested
sysadmin@UbuntuDesktop:/etc$ 
```



```
sysadmin@UbuntuDesktop:/etc$ sudo chkrootkit -q

/usr/lib/debug/.build-id /usr/lib/python2.7/dist-packages/ansible/galaxy/data/container/files/.gi
t_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/container/.travis.yml /usr/lib/python
2.7/dist-packages/ansible/galaxy/data/container/templates/.git_keep /usr/lib/python2.7/dist-packa
ges/ansible/galaxy/data/default/collection/roles/.git_keep /usr/lib/python2.7/dist-packages/ansib
le/galaxy/data/default/collection/docs/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/
data/default/role/files/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/ro
le/.travis.yml /usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/role/templates/.git_k
eep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/apb/files/.git_keep /usr/lib/python2.7/d
ist-packages/ansible/galaxy/data/apb/.travis.yml /usr/lib/python2.7/dist-packages/ansible/galaxy/
data/apb/templates/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/network/files/.
git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/network/.travis.yml /usr/lib/python
2.7/dist-packages/ansible/galaxy/data/network/templates/.git_keep /lib/modules/5.0.0-23-generic/v
dso/.build-id
/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/rev_shell.sh
/tmp/vagrant-shell
/tmp/a9xk.sh
/tmp/listen.sh
enp0s3: PACKET SNIFFER(/sbin/dhclient[5243])
 The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          1797 tty1   /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -listen 4
-listen 5 -displayfd 6
! gdm          1746 tty1   /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /usr/share
/gdm/greeter/autostart
! gdm          1751 tty1   /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/gdm
/greeter/autostart
! gdm          1758 tty1   /usr/bin/gnome-shell
! gdm          1887 tty1   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! gdm          1890 tty1   /usr/lib/gnome-settings-daemon/gsd-clipboard
! gdm          1897 tty1   /usr/lib/gnome-settings-daemon/gsd-color
! gdm          1903 tty1   /usr/lib/gnome-settings-daemon/gsd-datetime
! gdm          1904 tty1   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! gdm          1908 tty1   /usr/lib/gnome-settings-daemon/gsd-keyboard
! gdm          1920 tty1   /usr/lib/gnome-settings-daemon/gsd-media-keys
! gdm          1921 tty1   /usr/lib/gnome-settings-daemon/gsd-mouse
! gdm          1924 tty1   /usr/lib/gnome-settings-daemon/gsd-power
! gdm          1926 tty1   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm          1927 tty1   /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm          1930 tty1   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm          1938 tty1   /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm          1947 tty1   /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm          1948 tty1   /usr/lib/gnome-settings-daemon/gsd-sound
```



```
sysadmin@UbuntuDesktop:/etc$ sudo chkrootkit | grep INFECTED
Searching for Linux.Xor.DDoS ...                            INFECTED: Possible Malicious Linux.Xo
r.DDoS installed
! sysadmin    19675 pts/0  grep --color=auto INFECTED
sysadmin@UbuntuDesktop:/etc$
```