

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: **ls -l /etc/shadow**
 - Command to set permissions (if needed):
2. Permissions on /etc/gshadow should allow only root read and write access.
 - Command to inspect permissions: **ls -l /etc/gshadow**
 - Command to set permissions (if needed):
3. Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.
 - Command to inspect permissions: **ls -l /etc/group**
 - Command to set permissions (if needed):
4. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.
 - Command to inspect permissions: **ls -l /etc/passwd**
 - Command to set permissions (if needed):

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 -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.
 - 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

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

- Screenshot of report output:

```
Linux-Module_default_1619239810141_2669 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Sat 20:56
sysadmin@UbuntuDesktop: ~
https://cisofy.com/controls/HRDN-7222/

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 : 57 [#####]
Tests performed : 240
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 : 304
=====

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)

=====

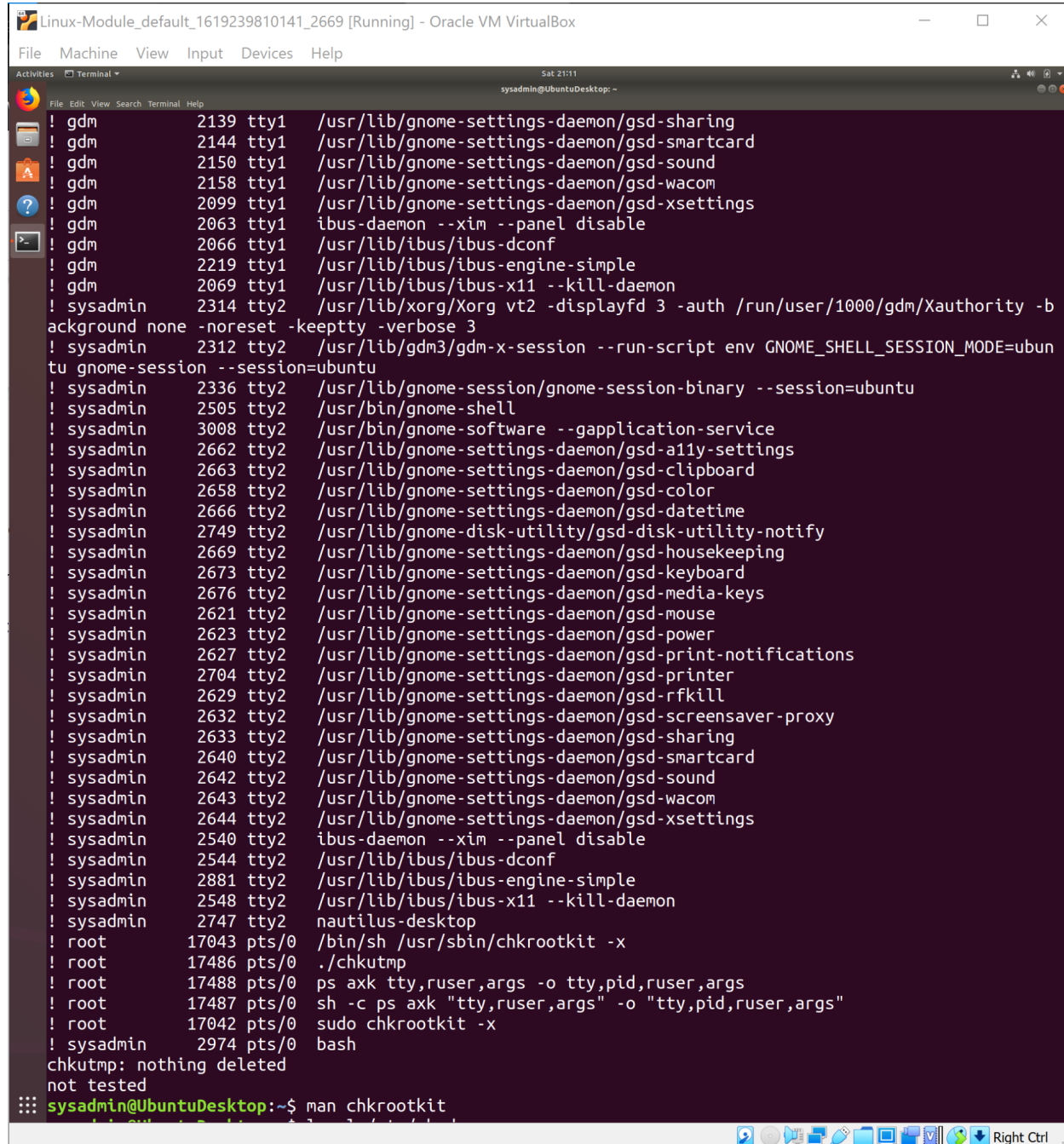
[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for a
ll settings)

sysadmin@UbuntuDesktop:~$
```

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.
 - o Screenshot of end of sample output:



```
Linux-Module_default_1619239810141_2669 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Sysadmin@UbuntuDesktop: ~
! gdm 2139 tty1 /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm 2144 tty1 /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm 2150 tty1 /usr/lib/gnome-settings-daemon/gsd-sound
! gdm 2158 tty1 /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm 2099 tty1 /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm 2063 tty1 ibus-daemon --xim --panel disable
! gdm 2066 tty1 /usr/lib/ibus/ibus-dconf
! gdm 2219 tty1 /usr/lib/ibus/ibus-engine-simple
! gdm 2069 tty1 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 2314 tty2 /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -b
ackground none -noreset -keeptty -verbose 3
! sysadmin 2312 tty2 /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubun
tu gnome-session --session=ubuntu
! sysadmin 2336 tty2 /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin 2505 tty2 /usr/bin/gnome-shell
! sysadmin 3008 tty2 /usr/bin/gnome-software --gapplication-service
! sysadmin 2662 tty2 /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin 2663 tty2 /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin 2658 tty2 /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin 2666 tty2 /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin 2749 tty2 /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin 2669 tty2 /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin 2673 tty2 /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin 2676 tty2 /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin 2621 tty2 /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin 2623 tty2 /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin 2627 tty2 /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin 2704 tty2 /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin 2629 tty2 /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin 2632 tty2 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin 2633 tty2 /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin 2640 tty2 /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin 2642 tty2 /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin 2643 tty2 /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin 2644 tty2 /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin 2540 tty2 ibus-daemon --xim --panel disable
! sysadmin 2544 tty2 /usr/lib/ibus/ibus-dconf
! sysadmin 2881 tty2 /usr/lib/ibus/ibus-engine-simple
! sysadmin 2548 tty2 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 2747 tty2 nautilus-desktop
! root 17043 pts/0 /bin/sh /usr/sbin/chkrootkit -x
! root 17486 pts/0 ./chkutmp
! root 17488 pts/0 ps axk tty,ruser,args -o tty,pid,ruser,args
! root 17487 pts/0 sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root 17042 pts/0 sudo chkrootkit -x
! sysadmin 2974 pts/0 bash
chkutmp: nothing deleted
not tested
Sysadmin@UbuntuDesktop:~$ man chkrootkit
```