

Week 4 Homework Submission File: Linux Systems Administration

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): **`sudo chmod 600 /etc/shadow`**

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): **`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: **`ls -l /etc/group`**

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: **`ls -l /etc/passwd`**

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`**

2. Ensure that only the admin has general sudo access. **`sudo -IU admin`**

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 -G engineers sam`**
(joe,amy,sara)

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

Command to create the shared folder: **`mkdir engineers`**
ensam

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: **`chgrp engineers engineers/`**

Step 4: Lynis Auditing

1. Command to install Lynis: **`sudo apt install Lynis`**

2. Command to see documentation and instructions: **sudo lynis audit info**
 3. Command to run an audit: **Q 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:

```

File Edit View Search Terminal Help
https://cisofy.com/controls/CONT-8104/

* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
https://cisofy.com/controls/KRNL-6000/

* Harden compilers like restricting access to root user only [HROD-7222]
https://cisofy.com/controls/HROD-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 tests (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

=====
Lynis security scan details:

Hardening Index : 56 [#####]
Tests performed : 240
Plugins enabled : 1

Components:
- Firewall [V]
- Hardware 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 : 303

=====
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:~$

```

Bonus

1. Command to install chkrootkit: **sudo apt install chkrootkit**
 2. Command to see documentation and instructions: **sudo chkrootkit -h**
 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.
- Screenshot of end of sample output:

```

File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$

! gdm 2160 tty1 /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm 2164 tty1 /usr/lib/gnome-settings-daemon/gsd-sound
! gdm 2170 tty1 /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm 2118 tty1 /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm 2084 tty1 dbus-daemon --xln --panel disable
! gdm 2087 tty1 /usr/lib/ibus/ibus-dconf
! gdm 2181 tty1 /usr/lib/ibus/ibus-engine-simple
! gdm 2090 tty1 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 3409 tty2 /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! sysadmin 3407 tty2 /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin 3429 tty2 /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin 3606 tty2 /usr/bin/gnome-shell
! sysadmin 4077 tty2 /usr/bin/gnome-software --gapplication-service
! sysadmin 3751 tty2 /usr/lib/gnome-settings-daemon/gsd-ally-settings
! sysadmin 3753 tty2 /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin 3748 tty2 /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin 3759 tty2 /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin 3837 tty2 /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin 3761 tty2 /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin 3762 tty2 /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin 3764 tty2 /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin 3711 tty2 /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin 3712 tty2 /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin 3716 tty2 /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin 3800 tty2 /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin 3719 tty2 /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin 3720 tty2 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin 3723 tty2 /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin 3724 tty2 /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin 3730 tty2 /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin 3736 tty2 /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin 3738 tty2 /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin 3625 tty2 dbus-daemon --xln --panel disable
! sysadmin 3629 tty2 /usr/lib/ibus/ibus-dconf
! sysadmin 3968 tty2 /usr/lib/ibus/ibus-engine-simple
! sysadmin 3632 tty2 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 3831 tty2 nautilus-desktop
! root 26626 pts/0 /bin/sh /usr/sbin/chkrootkit -x
! root 27059 pts/0 ./chkutmp
! root 27061 pts/0 ps axk tty,ruser,args -o tty,pid,ruser,args
! root 27060 pts/0 sh -c ps axk 'tty,ruser,args' -o 'tty,pid,ruser,args'
! root 26625 pts/0 sudo chkrootkit -x
! sysadmin 12883 pts/0 bash
! jane 11665 pts/1 bash
! root 11652 pts/1 su jane
! root 11651 pts/1 sudo su jane
! sysadmin 11188 pts/1 bash
chkutmp: nothing deleted
not tested
sysadmin@UbuntuDesktop:~$

```