

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: **`ll /etc/shadow` or `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: **`ll /etc/gshadow` or `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: **`ll /etc/group` or `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: **`ll /etc/passwd` or `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 useradd sam joe amy sara admin**

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

- Command to add `admin` to the `sudo` group: **sudo usermod -a -G sudo admin**

Step 3: Create User Group and Collaborative Folder

1. Add an `engineers` group to the system.

- Command to add group: **sudo groupadd 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**

sudo usermod -a -G engineers joe, sudo usermod -a -G engineers amy, sudo usermod -a -G engineers sara

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

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

Step 4: Lynis Auditing

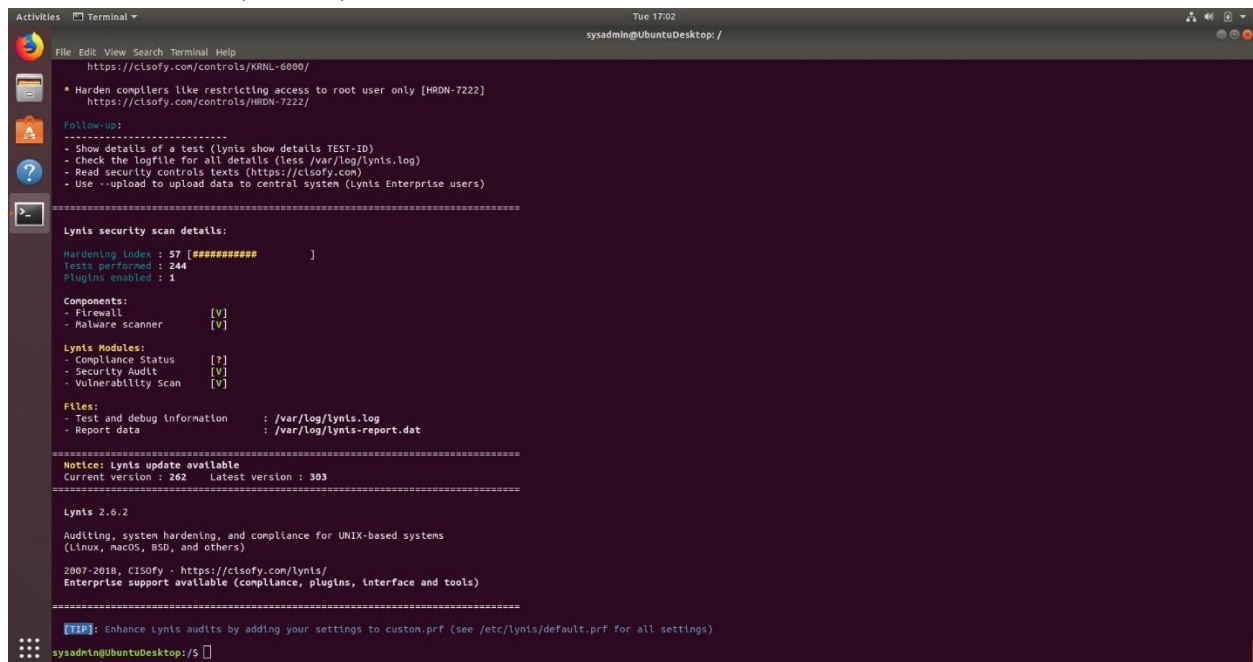
1. Command to install Lynis: **sudo apt install lynis**

2. Command to see documentation and instructions: **./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:



```
Activities Terminal
Tue 17:02
sysadmin@UbuntuDesktop: /

https://cisofy.com/controls/KRNL-6000/
* Harden compilers like restricting access to root user only [HRDN-7222]
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 : 244
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 : 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.prfl (see /etc/lynis/default.prfl for all settings)
sysadmin@UbuntuDesktop: / $
```

Bonus

1. Command to install chkrootkit: `sudo apt-get install chkrootkit`
2. Command to see documentation and instructions: `sudo 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.

- Screenshot of end of sample output:

```

Activities Terminal Tue 17:13
sysadmin@UbuntuDesktop: /

! gdm 2396 tty1 /usr/lib/gnome-settings-daemon/gsd-power
! gdm 2398 tty1 /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm 2401 tty1 /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm 2403 tty1 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm 2405 tty1 /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm 2411 tty1 /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm 2415 tty1 /usr/lib/gnome-settings-daemon/gsd-sound
! gdm 2418 tty1 /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm 2367 tty1 /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm 2325 tty1 dbus-daemon --xln --panel disable
! gdm 2328 tty1 /usr/lib/ibus/ibus-dconf
! gdm 2490 tty1 /usr/lib/ibus/ibus-engine-simple
! gdm 2331 tty1 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 2817 tty2 /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! sysadmin 2815 tty2 /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin 2834 tty2 /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin 3058 tty2 /usr/bin/gnome-shell
! sysadmin 3743 tty2 /usr/bin/gnome-software --application-service
! sysadmin 3260 tty2 /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin 3261 tty2 /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin 3256 tty2 /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin 3267 tty2 /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin 3132 tty2 /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin 3269 tty2 /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin 3272 tty2 /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin 3275 tty2 /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin 3219 tty2 /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin 3220 tty2 /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin 3226 tty2 /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin 3288 tty2 /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin 3229 tty2 /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin 3230 tty2 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin 3234 tty2 /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin 3239 tty2 /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin 3240 tty2 /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin 3244 tty2 /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin 3139 tty2 dbus-daemon --xln --panel disable
! sysadmin 3143 tty2 /usr/lib/ibus/ibus-dconf
! sysadmin 3407 tty2 /usr/lib/ibus/ibus-engine-simple
! sysadmin 3147 tty2 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 3127 tty2 nautilus-desktop
! root 13931 pts/0 /bin/sh /usr/sbin/chkrootkit -x
! root 14364 pts/0 ./chkutap
! root 14365 pts/0 ps aux tty,ruser,args -o tty,pid,ruser,args
! root 14365 pts/0 sh -c ps aux "tty,ruser,args" -o "tty,pid,ruser,args"
! root 13930 pts/0 sudo chkrootkit -x
! sysadmin 3919 pts/0 bash
chkutap: nothing deleted
not tested
sysadmin@UbuntuDesktop:/$

```
