



Cybersecurity

Module 4 Challenge Submission File

Linux Systems Administration

Make a copy of this document to work in, and then for each step, add the solution commands below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on `/etc/shadow` should allow only `root` read and write access.
 - a. Command to inspect permissions:

```
[ls -l /etc/shadow]
```

- b. Command to set permissions (if needed):

```
[sudo chmod 600 /etc/shadow]
```

2. Permissions on `/etc/gshadow` should allow only `root` read and write access.
 - a. Command to inspect permissions:

```
[ls -l /etc/gshadow]
```

- b. 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.

- a. Command to inspect permissions:

```
[ls -l /etc/group]
```

- b. 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.

- a. Command to inspect permissions:

```
[ls -l /etc/passwd]
```

- b. 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` with the `useradd` command.

- a. 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.

- a. 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.

a. Command to add group:

```
[sudo groupadd engineers]
```

2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.

a. Command to add users to `engineers` group (include all four users):

```
[sudo usermod -aG engineers sam joe amy sara]
```

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

a. Command to create the shared folder:

```
[sudo mkdir /home/engineers]
```

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

a. Command to change ownership of engineers' shared folder to `engineers` group:

```
[sudo chown :engineers /home/engineers]
```

Step 4: Lynis Auditing

1. Command to install Lynis:

```
[sudo apt-get install lynis]
```

2. Command to view documentation and instructions:

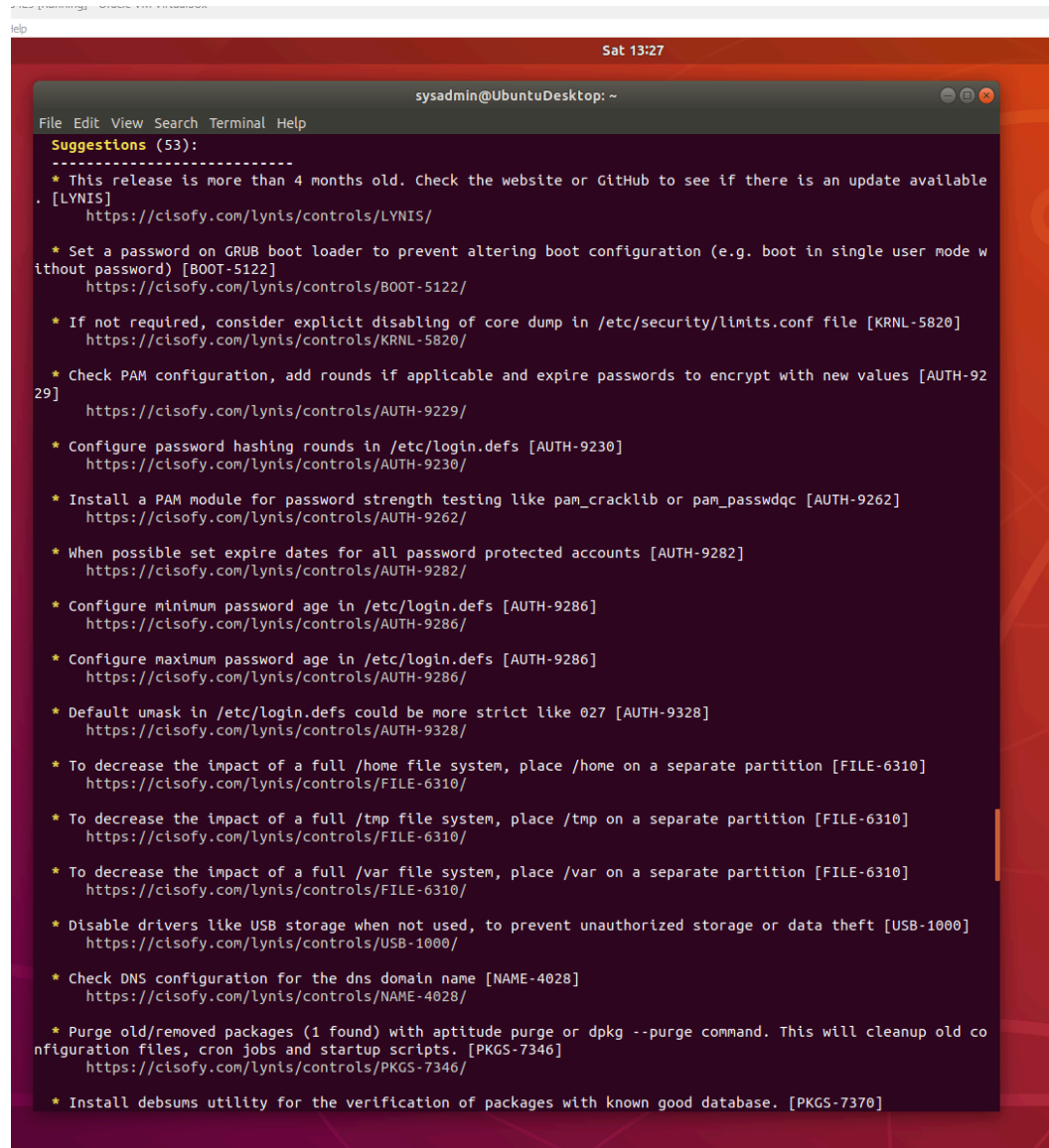
```
[man lynis]
```

3. Command to run an audit:

```
[sudo lynis audit system]
```

4. Provide a report from the Lynis output with recommendations for hardening the system.

- a. Screenshot of report output:

A screenshot of a terminal window titled 'sysadmin@UbuntuDesktop: ~' showing the output of a Lynis scan. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal output is titled 'Suggestions (53):' and lists 20 items, each with a description and a URL. The items are: 1. This release is more than 4 months old. Check the website or GitHub to see if there is an update available [LYNIS] https://cisofy.com/lynis/controls/LYNIS/. 2. Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122] https://cisofy.com/lynis/controls/BOOT-5122/. 3. If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820] https://cisofy.com/lynis/controls/KRNL-5820/. 4. Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229] https://cisofy.com/lynis/controls/AUTH-9229/. 5. Configure password hashing rounds in /etc/login.defs [AUTH-9230] https://cisofy.com/lynis/controls/AUTH-9230/. 6. Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262] https://cisofy.com/lynis/controls/AUTH-9262/. 7. When possible set expire dates for all password protected accounts [AUTH-9282] https://cisofy.com/lynis/controls/AUTH-9282/. 8. Configure minimum password age in /etc/login.defs [AUTH-9286] https://cisofy.com/lynis/controls/AUTH-9286/. 9. Configure maximum password age in /etc/login.defs [AUTH-9286] https://cisofy.com/lynis/controls/AUTH-9286/. 10. Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328] https://cisofy.com/lynis/controls/AUTH-9328/. 11. To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310] https://cisofy.com/lynis/controls/FILE-6310/. 12. To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310] https://cisofy.com/lynis/controls/FILE-6310/. 13. To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310] https://cisofy.com/lynis/controls/FILE-6310/. 14. Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000] https://cisofy.com/lynis/controls/USB-1000/. 15. Check DNS configuration for the dns domain name [NAME-4028] https://cisofy.com/lynis/controls/NAME-4028/. 16. Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346] https://cisofy.com/lynis/controls/PKGS-7346/. 17. Install debsums utility for the verification of packages with known good database. [PKGS-7370]

Bonus

1. Command to install chkrootkit:

```
[sudo apt-get install chkrootkit]
```

2. Command to view documentation and instructions:

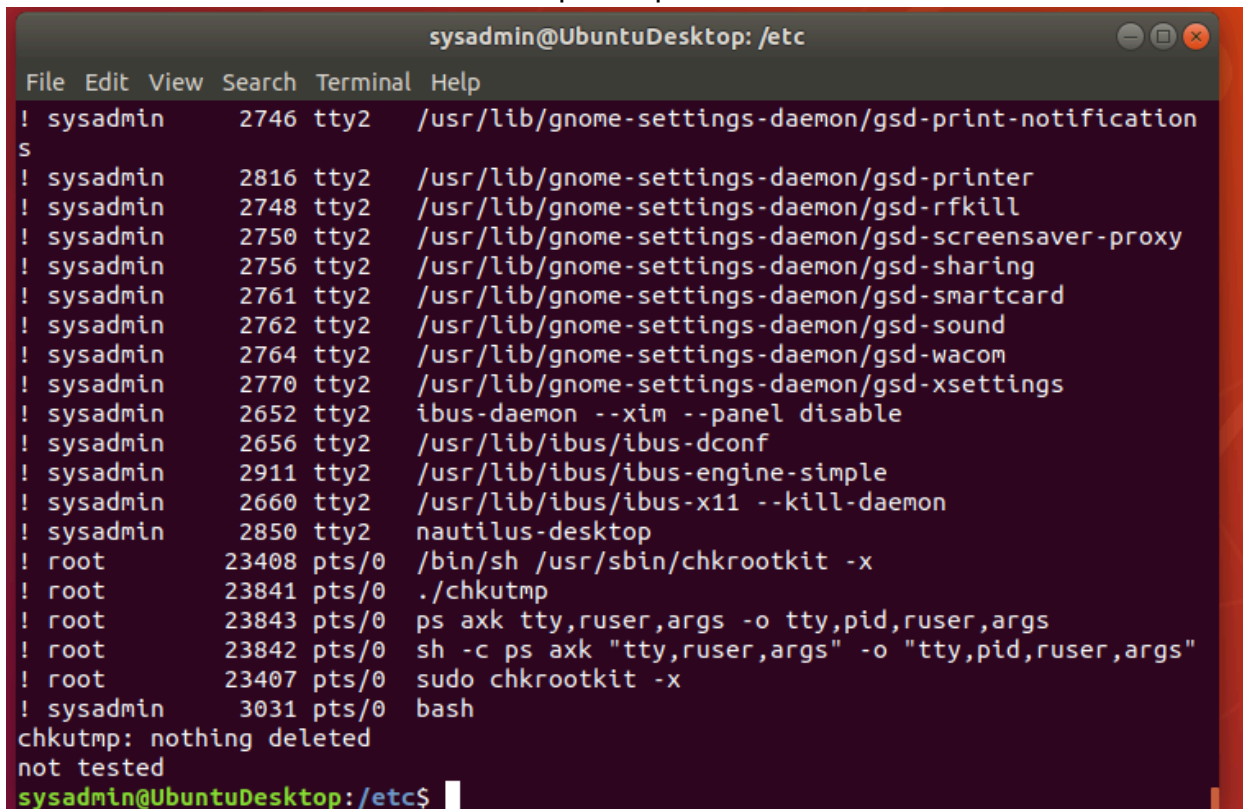
```
[man chkrootkit]
```

3. Command to run expert mode:

```
[sudo chkrootkit -x]
```

4. Provide a report from the chrootkit output with recommendations for hardening the system.

- a. Screenshot of end of sample output:



```
sysadmin@UbuntuDesktop: /etc
File Edit View Search Terminal Help
! sysadmin      2746 tty2    /usr/lib/gnome-settings-daemon/gsd-print-notification
s
! sysadmin      2816 tty2    /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin      2748 tty2    /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin      2750 tty2    /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin      2756 tty2    /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin      2761 tty2    /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin      2762 tty2    /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin      2764 tty2    /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin      2770 tty2    /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin      2652 tty2    ibus-daemon --xim --panel disable
! sysadmin      2656 tty2    /usr/lib/ibus/ibus-dconf
! sysadmin      2911 tty2    /usr/lib/ibus/ibus-engine-simple
! sysadmin      2660 tty2    /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin      2850 tty2    nautilus-desktop
! root          23408 pts/0   /bin/sh /usr/sbin/chkrootkit -x
! root          23841 pts/0   ./chkutmp
! root          23843 pts/0   ps axk tty,ruser,args -o tty,pid,ruser,args
! root          23842 pts/0   sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root          23407 pts/0   sudo chkrootkit -x
! sysadmin      3031 pts/0   bash
chkutmp: nothing deleted
not tested
sysadmin@UbuntuDesktop: /etc$
```