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 /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 `admin1` with the `useradd` command.

   a. Command to add each user account (include all five users):

```
sudo useradd sam
sudo useradd joe
sudo useradd amy
sudo useradd sara
sudo useradd admin1
```

2. Ensure that only the `admin1` has general sudo access.

   a. Command to add `admin1` to the sudo group:

```
sudo usermod -aG sudo admin1
```

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
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`.

   a. Command to create the shared folder:

```
sudo mkdir /home/engineers
sudo chmod -R 777 /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 update
sudo apt-get install lynis
```

2. Command to view documentation and instructions:

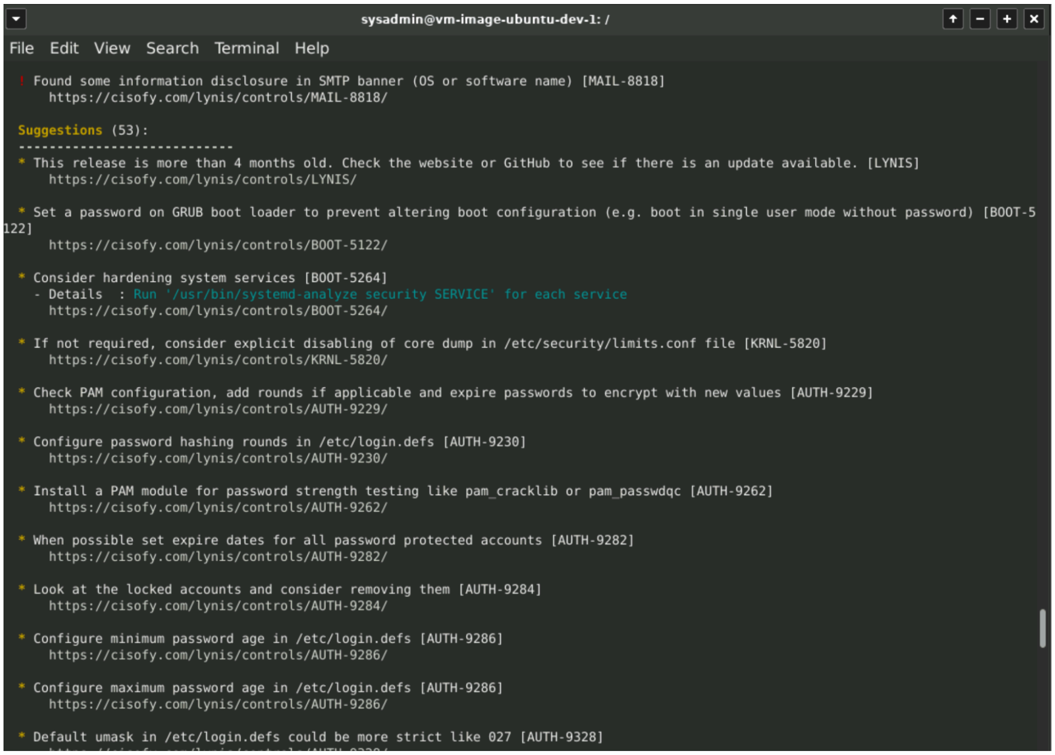
```
lynis show commands
lynis audit system --help
```

3. Command to run an audit:

```
lynis audit system
```

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

    a. Screenshot of report output


sysadmin@vm-image-ubuntu-dev-1: /
File Edit View Search Terminal Help

```
 ! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
     https://cisofy.com/lynis/controls/MAIL-8818/

 Suggestions (53):
 ----------------------------
 * 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/

 * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5
122]
     https://cisofy.com/lynis/controls/BOOT-5122/

 * Consider hardening system services [BOOT-5264]
   - Details  : Run '/usr/bin/systemd-analyze security SERVICE' for each service
     https://cisofy.com/lynis/controls/BOOT-5264/

 * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
     https://cisofy.com/lynis/controls/KRNL-5820/

 * Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
     https://cisofy.com/lynis/controls/AUTH-9229/

 * Configure password hashing rounds in /etc/login.defs [AUTH-9230]
     https://cisofy.com/lynis/controls/AUTH-9230/

 * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
     https://cisofy.com/lynis/controls/AUTH-9262/

 * When possible set expire dates for all password protected accounts [AUTH-9282]
     https://cisofy.com/lynis/controls/AUTH-9282/

 * Look at the locked accounts and consider removing them [AUTH-9284]
     https://cisofy.com/lynis/controls/AUTH-9284/

 * Configure minimum password age in /etc/login.defs [AUTH-9286]
     https://cisofy.com/lynis/controls/AUTH-9286/

 * Configure maximum password age in /etc/login.defs [AUTH-9286]
     https://cisofy.com/lynis/controls/AUTH-9286/

 * Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
```

Optional Additional Challenge

1. Command to install chkrootkit:

```
sudo apt-get install chkrootkit
```

2. Command to view documentation and instructions:

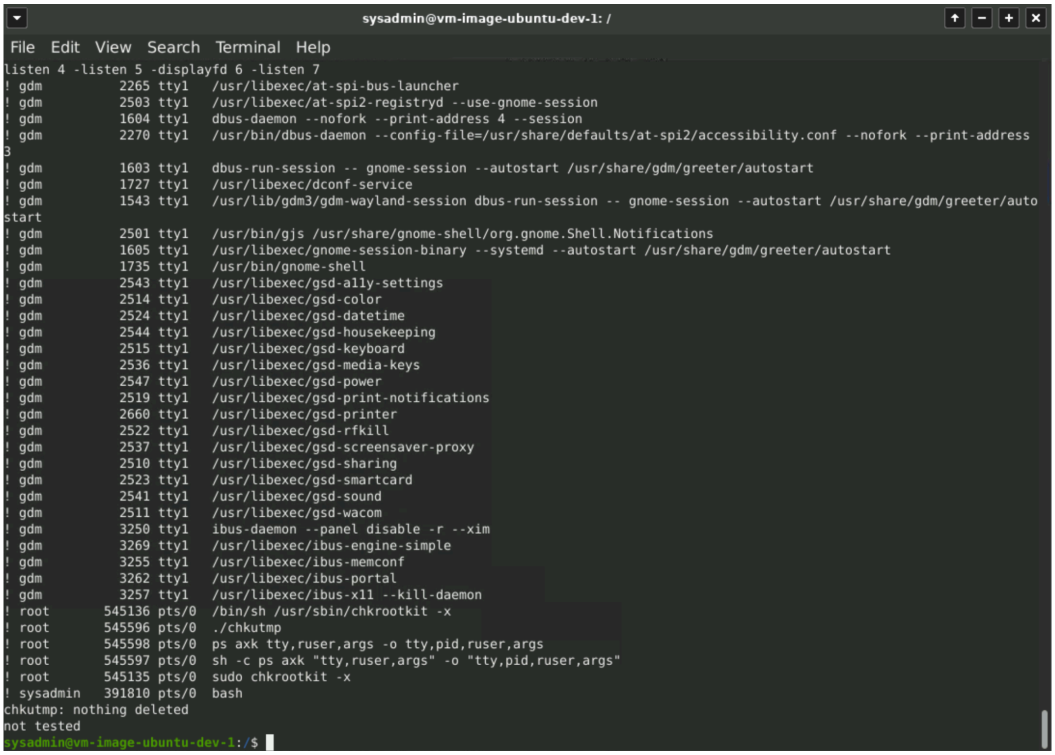
```
chkrootkit man
chkrootkit --help
```

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@vm-image-ubuntu-dev-1: /
File Edit View Search Terminal Help

```
listen 4 -listen 5 -displayfd 6 -listen 7
! gdm          2265 tty1   /usr/libexec/at-spi-bus-launcher
! gdm          2503 tty1   /usr/libexec/at-spi2-registryd --use-gnome-session
! gdm          1604 tty1   dbus-daemon --nofork --print-address 4 --session
! gdm          2270 tty1   /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address
3
! gdm          1603 tty1   dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          1727 tty1   /usr/libexec/dconf-service
! gdm          1543 tty1   /usr/lib/gdm3/gdm-wayland-session dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/auto
start
! gdm          2501 tty1   /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
! gdm          1605 tty1   /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
! gdm          1735 tty1   /usr/bin/gnome-shell
! gdm          2543 tty1   /usr/libexec/gsd-a11y-settings
! gdm          2514 tty1   /usr/libexec/gsd-color
! gdm          2524 tty1   /usr/libexec/gsd-datetime
! gdm          2544 tty1   /usr/libexec/gsd-housekeeping
! gdm          2515 tty1   /usr/libexec/gsd-keyboard
! gdm          2536 tty1   /usr/libexec/gsd-media-keys
! gdm          2547 tty1   /usr/libexec/gsd-power
! gdm          2519 tty1   /usr/libexec/gsd-print-notifications
! gdm          2660 tty1   /usr/libexec/gsd-printer
! gdm          2522 tty1   /usr/libexec/gsd-rfkill
! gdm          2537 tty1   /usr/libexec/gsd-screensaver-proxy
! gdm          2510 tty1   /usr/libexec/gsd-sharing
! gdm          2523 tty1   /usr/libexec/gsd-smartcard
! gdm          2541 tty1   /usr/libexec/gsd-sound
! gdm          2511 tty1   /usr/libexec/gsd-wacom
! gdm          3250 tty1   ibus-daemon --panel disable -r --xim
! gdm          3269 tty1   /usr/libexec/ibus-engine-simple
! gdm          3255 tty1   /usr/libexec/ibus-memconf
! gdm          3262 tty1   /usr/libexec/ibus-portal
! gdm          3257 tty1   /usr/libexec/ibus-x11 --kill-daemon
! root       545136 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root       545596 pts/0  ./chkutmp
! root       545598 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root       545597 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root       545135 pts/0  sudo chkrootkit -x
! sysadmin   391810 pts/0  bash
chkutmp: nothing deleted
not tested
sysadmin@vm-image-ubuntu-dev-1:/$
```