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):

```
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):

```
chmod 600 /etc/shadow
```

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):

```
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):

```
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/shared
```

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/shared
```

Step 4: Lynis Auditing

1. Command to install Lynis:

```
sudo wget https://downloads.cisofy.com/lynis/lynis-3.0.8.tar.gz
```

2. Command to view documentation and instructions:

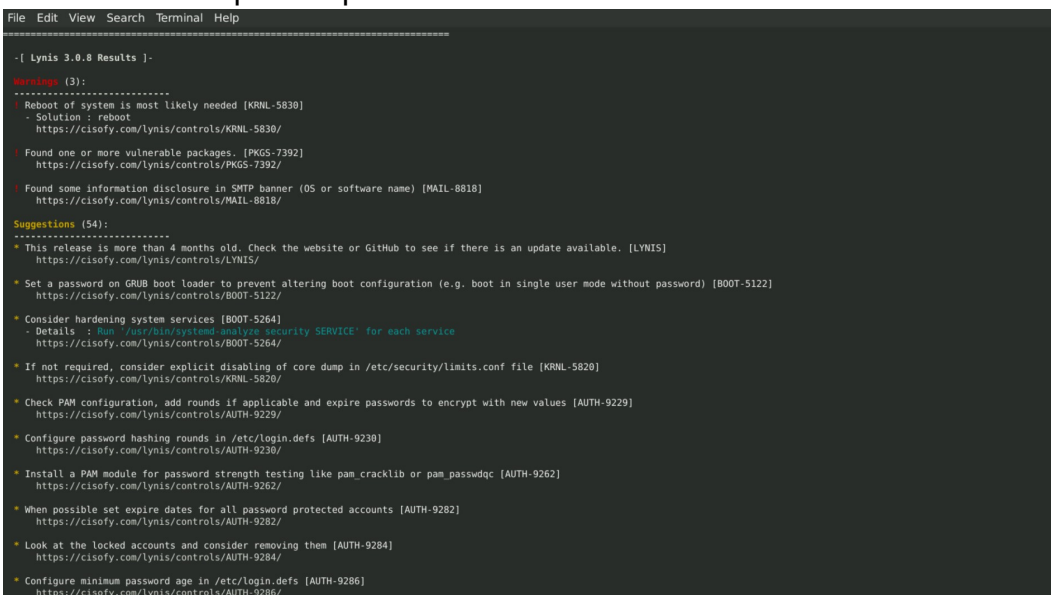
```
sudo lynis show help
```

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:



```
File  Edit  View  Search  Terminal  Help
================================================================================

  -[ Lynis 3.0.8 Results ]-

  Warnings (3):
  ----------------------------
  ! Reboot of system is most likely needed [KRNL-5830]
    - Solution : reboot
      https://cisofy.com/lynis/controls/KRNL-5830/

  ! Found one or more vulnerable packages. [PKGS-7392]
      https://cisofy.com/lynis/controls/PKGS-7392/

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

  Suggestions (54):
  ----------------------------
  * 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-5122]
      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/
```

Optional Additional Challenge

1. Command to install chkrootkit:

```
$ 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:

```
! gdm          2371 tty1   /usr/libexec/gsd-a11y-settings
! gdm          2328 tty1   /usr/libexec/gsd-color
! gdm          2348 tty1   /usr/libexec/gsd-datetime
! gdm          2372 tty1   /usr/libexec/gsd-housekeeping
! gdm          2331 tty1   /usr/libexec/gsd-keyboard
! gdm          2356 tty1   /usr/libexec/gsd-media-keys
! gdm          2382 tty1   /usr/libexec/gsd-power
! gdm          2335 tty1   /usr/libexec/gsd-print-notifications
! gdm          2495 tty1   /usr/libexec/gsd-printer
! gdm          2337 tty1   /usr/libexec/gsd-rfkill
! gdm          2361 tty1   /usr/libexec/gsd-screensaver-proxy
! gdm          2317 tty1   /usr/libexec/gsd-sharing
! gdm          2347 tty1   /usr/libexec/gsd-smartcard
! gdm          2363 tty1   /usr/libexec/gsd-sound
! gdm          2323 tty1   /usr/libexec/gsd-wacom
! gdm          2512 tty1   ibus-daemon --panel disable -r --xim
! gdm          2881 tty1   /usr/libexec/ibus-engine-simple
! gdm          2519 tty1   /usr/libexec/ibus-memconf
! gdm          2530 tty1   /usr/libexec/ibus-portal
! gdm          2521 tty1   /usr/libexec/ibus-x11 --kill-daemon
! max        401288 pts/0  bash
! max        401402 pts/0  bash
! max        401313 pts/0  su sysadmin
! max        401409 pts/0  su sysadmin
! root       396595 pts/0  bash
! root       540716 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root       541161 pts/0  ./chkutmp
! root       541163 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root       541162 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root       396594 pts/0  su
! root       396609 pts/0  su sysadmin
! root       396914 pts/0  su sysadmin
! root       396593 pts/0  sudo su
! root       396913 pts/0  sudo su sysadmin
! root       540715 pts/0  sudo chkrootkit -x
! sally      401277 pts/0  bash
! sally      401286 pts/0  su max
! sysadmin   396554 pts/0  bash
! sysadmin   396610 pts/0  bash
! sysadmin   396915 pts/0  bash
! sysadmin   401316 pts/0  bash
! sysadmin   401411 pts/0  bash
! sysadmin   401276 pts/0  su sally
! sysadmin   401401 pts/0  su max
chkutmp: nothing deleted
not tested
sysadmin@vm-image-ubuntu-dev-1:/$
```