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 `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 ~/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 root:engineers ~/engineers
```

Step 4: Lynis Auditing

1. Command to install Lynis:

```
Sudo apt install lynis
```

2. Command to view documentation and instructions:

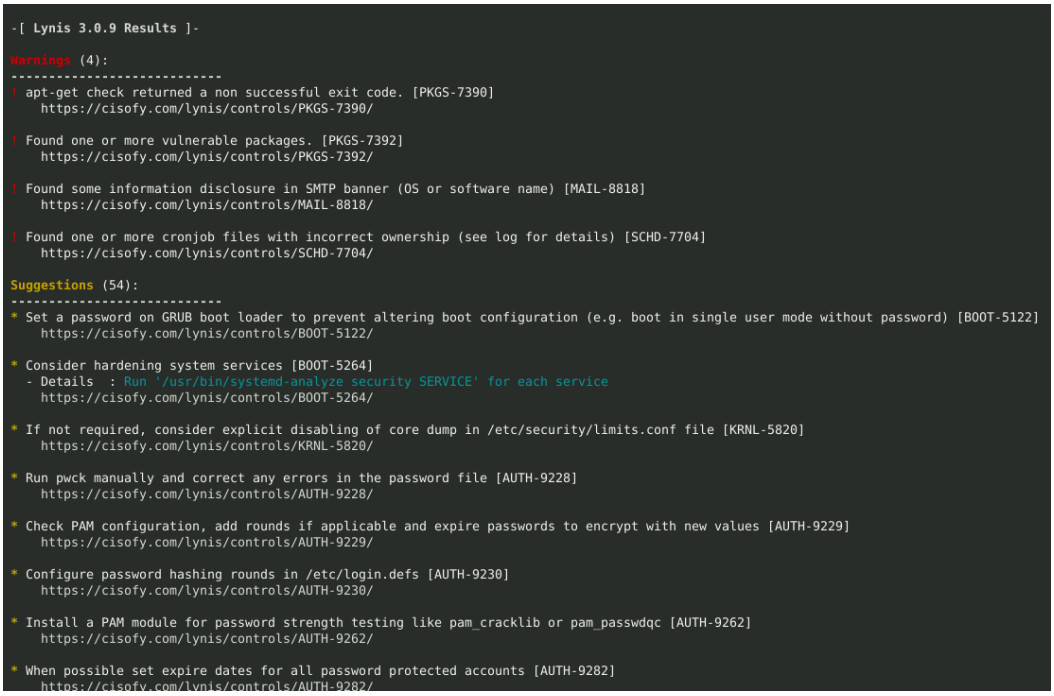
```
Man lynis
```

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:



```
-[ Lynis 3.0.9 Results ]-

Warnings (4):
----------------------------
! apt-get check returned a non successful exit code. [PKGS-7390]
    https://cisofy.com/lynis/controls/PKGS-7390/

! 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/

! Found one or more cronjob files with incorrect ownership (see log for details) [SCHD-7704]
    https://cisofy.com/lynis/controls/SCHD-7704/

Suggestions (54):
----------------------------
* 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/

* Run pwck manually and correct any errors in the password file [AUTH-9228]
    https://cisofy.com/lynis/controls/AUTH-9228/

* 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/
```

Optional Additional Challenge

1. Command to install chkrootkit:

```
Sudo apt 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:

```
### Output of: ./chklastlog -q -f //var/log/wtmp -l //var/log/lastlog
###
 The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          2123 tty1   /usr/bin/Xwayland :1024 -rootless -noreset -accessx -core -auth /run/user/129/.mutter-Xwaylandauth.JM1TC2 -listen 4 -listen 5 -displayfd 6 -listen 7
! gdm          2099 tty1   /usr/libexec/at-spi-bus-launcher
! gdm          2379 tty1   /usr/libexec/at-spi2-registryd --use-gnome-session
! gdm          1195 tty1   dbus-daemon --nofork --print-address 4 --session
! gdm          2104 tty1   /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
! gdm          1194 tty1   dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          1173 tty1   /usr/lib/gdm3/gdm-wayland-session dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          2378 tty1   /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
! gdm          1198 tty1   /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
! gdm          1273 tty1   /usr/bin/gnome-shell
! gdm          2454 tty1   /usr/libexec/gsd-ally-settings
! gdm          2396 tty1   /usr/libexec/gsd-color
! gdm          2421 tty1   /usr/libexec/gsd-datetime
! gdm          2455 tty1   /usr/libexec/gsd-housekeeping
! gdm          2397 tty1   /usr/libexec/gsd-keyboard
! gdm          2433 tty1   /usr/libexec/gsd-media-keys
! gdm          2458 tty1   /usr/libexec/gsd-power
! gdm          2398 tty1   /usr/libexec/gsd-print-notifications
! gdm          2503 tty1   /usr/libexec/gsd-printer
! gdm          2409 tty1   /usr/libexec/gsd-rfkill
! gdm          2434 tty1   /usr/libexec/gsd-screensaver-proxy
! gdm          2385 tty1   /usr/libexec/gsd-sharing
! gdm          2414 tty1   /usr/libexec/gsd-smartcard
! gdm          2443 tty1   /usr/libexec/gsd-sound
! gdm          2389 tty1   /usr/libexec/gsd-wacom
! gdm          2533 tty1   ibus-daemon --panel disable -r --xim
! gdm          2595 tty1   /usr/libexec/ibus-engine-simple
! gdm          2540 tty1   /usr/libexec/ibus-memconf
! gdm          2549 tty1   /usr/libexec/ibus-portal
! gdm          2542 tty1   /usr/libexec/ibus-x11 --kill-daemon
! root        63886 pts/0  /bin/sh /usr/sbin/chkrootkit -x -q
! root        64331 pts/0  ./chkutmp
! root        64333 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        64332 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        63885 pts/0  sudo chkrootkit -x -q
! sysadmin     9952 pts/0  bash
! sysadmin     9988 pts/1  bash
sysadmin@vm-image-ubuntu-dev-1:/etc$
```