



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 useradd sam  
sudo useradd joe  
sudo useradd amy  
sudo useradd sara  
sudo useradd 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 addgroup 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
```

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 -y
```

2. Command to view documentation and instructions:

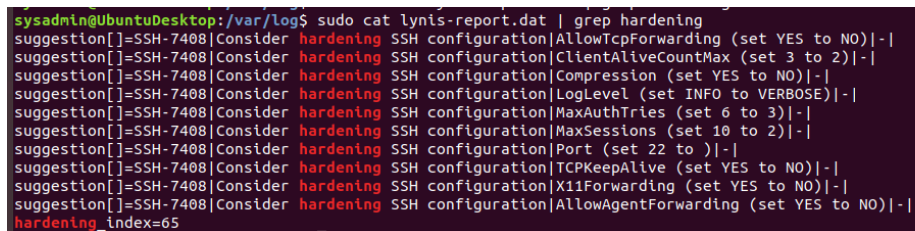
```
sudo lynis --help
```

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:



```
sysadmin@UbuntuDesktop:/var/log$ sudo cat lynis-report.dat | grep hardening
suggestion[]=SSH-7408|Consider hardening SSH configuration|AllowTcpForwarding (set YES to NO)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|ClientAliveCountMax (set 3 to 2)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|Compression (set YES to NO)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|LogLevel (set INFO to VERBOSE)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|MaxAuthTries (set 6 to 3)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|MaxSessions (set 10 to 2)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|Port (set 22 to )|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|TCPKeepAlive (set YES to NO)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|X11Forwarding (set YES to NO)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|AllowAgentForwarding (set YES to NO)|-|
hardening_index=65
```

Bonus

1. Command to install chkrootkit:

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

2. Command to view documentation and instructions:

```
sudo chkrootkit --help
```

3. Command to run expert mode:

```
sudo chkrootkit -x
```

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

- a. Screenshot of end of sample output:

```

! gdm 2206 tty1 /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm 2207 tty1 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm 2212 tty1 /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm 2219 tty1 /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm 2223 tty1 /usr/lib/gnome-settings-daemon/gsd-sound
! gdm 2225 tty1 /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm 2167 tty1 /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm 2126 tty1ibus-daemon --xln --panel disable
! gdm 2129 tty1 /usr/lib/ibus/ibus-dconf
! gdm 2288 tty1 /usr/lib/ibus/ibus-engine-simple
! gdm 2133 tty1 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 19043 tty2 /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! sysadmin 19041 tty2 /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin 19064 tty2 /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin 19250 tty2 /usr/bin/gnome-shell
! sysadmin 19688 tty2 /usr/bin/gnome-software --gapplication-service
! sysadmin 19403 tty2 /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin 19398 tty2 /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin 19401 tty2 /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin 19414 tty2 /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin 19502 tty2 /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin 19407 tty2 /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin 19410 tty2 /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin 19417 tty2 /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin 19416 tty2 /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin 19363 tty2 /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin 19364 tty2 /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin 19445 tty2 /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin 19366 tty2 /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin 19369 tty2 /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin 19372 tty2 /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin 19378 tty2 /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin 19380 tty2 /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin 19388 tty2 /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin 19386 tty2 /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin 19271 tty2ibus-daemon --xln --panel disable
! sysadmin 19275 tty2 /usr/lib/ibus/ibus-dconf
! sysadmin 19561 tty2 /usr/lib/ibus/ibus-engine-simple
! sysadmin 19277 tty2 /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin 19476 tty2 nautilus-desktop
! root 28183 pts/0 /bin/sh /usr/sbin/chkrootkit -x
! root 28637 pts/0 ./chkutmp
! root 28639 pts/0 ps axk tty,ruser,args -o tty,pid,ruser,args
! root 28638 pts/0 sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root 28182 pts/0 sudo chkrootkit -x
! sysadmin 23943 pts/0 bash
chkutmp: nothing deleted
not tested
sysadmin@ubuntuDesktop:/home$

```