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 u=rw-,g=---,o=--- /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 u=rw-,g=---,o=--- /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 u=rw-,g=r--,o=r-- /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 u=rw-,g=r--,o=r-- /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 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 install lynis
```

2. Command to view documentation and instructions:

```
Man lynis
```

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:

```
# Lynis Report
report_version_major=1
report_version_minor=0
report_datetime_start=2022-10-20 01:52:49
auditor=[Not Specified]
lynis_version=3.0.7
os=Linux
os_name=Ubuntu
os_fullname=Ubuntu 18.04.3 LTS
os_version=18.04
linux_version=Ubuntu
os_kernel_version=5.0.0
os_kernel_version_full=5.0.0-23-generic
hostname=UbuntuDesktop
test_category=all
test_group=all
plugin_directory=/usr/share/lynis/plugins
suggestion[]=LYNIS|Version of Lynis outdated, consider upgrading to the latest version|-|-|
lynis_update_available=1
binaries_count=2463
binaries_suid_count=/bin/fusermount /bin/mount /bin/ping /bin/ping4 /bin/ping6 /bin/su /bin/umount /sbin/mount.cifs /usr/bin/arping /usr/bin/chfn /usr/bin/chsh /usr/bin/gpa$
binaries_sgid_count=/sbin/pam_extrausers_chkpwd /sbin/unix_chkpwd /usr/bin/bsd-write /usr/bin/chage /usr/bin/crontab /usr/bin/dotlockfile /usr/bin/expiry /usr/bin/locate /u$
binary_paths=/snap/bin,/usr/local/games,/usr/games,/bin,/sbin,/usr/bin,/usr/sbin,/usr/local/bin,/usr/local/sbin
vm=1
vmtype=virtualbox
container=0
notebook=0
systemd=1
plugins_enabled=0
hostid=7050b1906953cd7be84dc8330c56cd4e6a49c2e3
hostid2=b9066583dbab7ebd0e1c79f0ac1e0e2ef35a80e04550b80c74ad68f0d41c45cc
suggestion[]=BOOT-5122|Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password)|-|-|
running_service_tool=systemctl
running_service[]=accounts-daemon
running_service[]=acpid
running_service[]=avahi-daemon
running_service[]=bolt
running_service[]=colord
running_service[]=containerd
running_service[]=cron
running_service[]=cups-browsed
running_service[]=cups
running_service[]=dbus
running_service[]=docker
running_service[]=dovecot
running_service[]=firewalld
running_service[]=fwupd
running_service[]=gdm
running_service[]=irqbalance
running_service[]=kerneloops
running_service[]=ModemManager
running_service[]=networkd-dispatcher
running_service[]=NetworkManager
running_service[]=nginx
running_service[]=nmbd
running_service[]=packagekit
running_service[]=polkit
running_service[]=postfix@-
running_service[]=rsyslog
running_service[]=rtkit-daemon
running_service[]=smbd
running_service[]=snapd
```

Bonus

1. Command to install chkrootkit:

```
Sudo apt install chkrootkit
```

2. Command to view documentation and instructions:

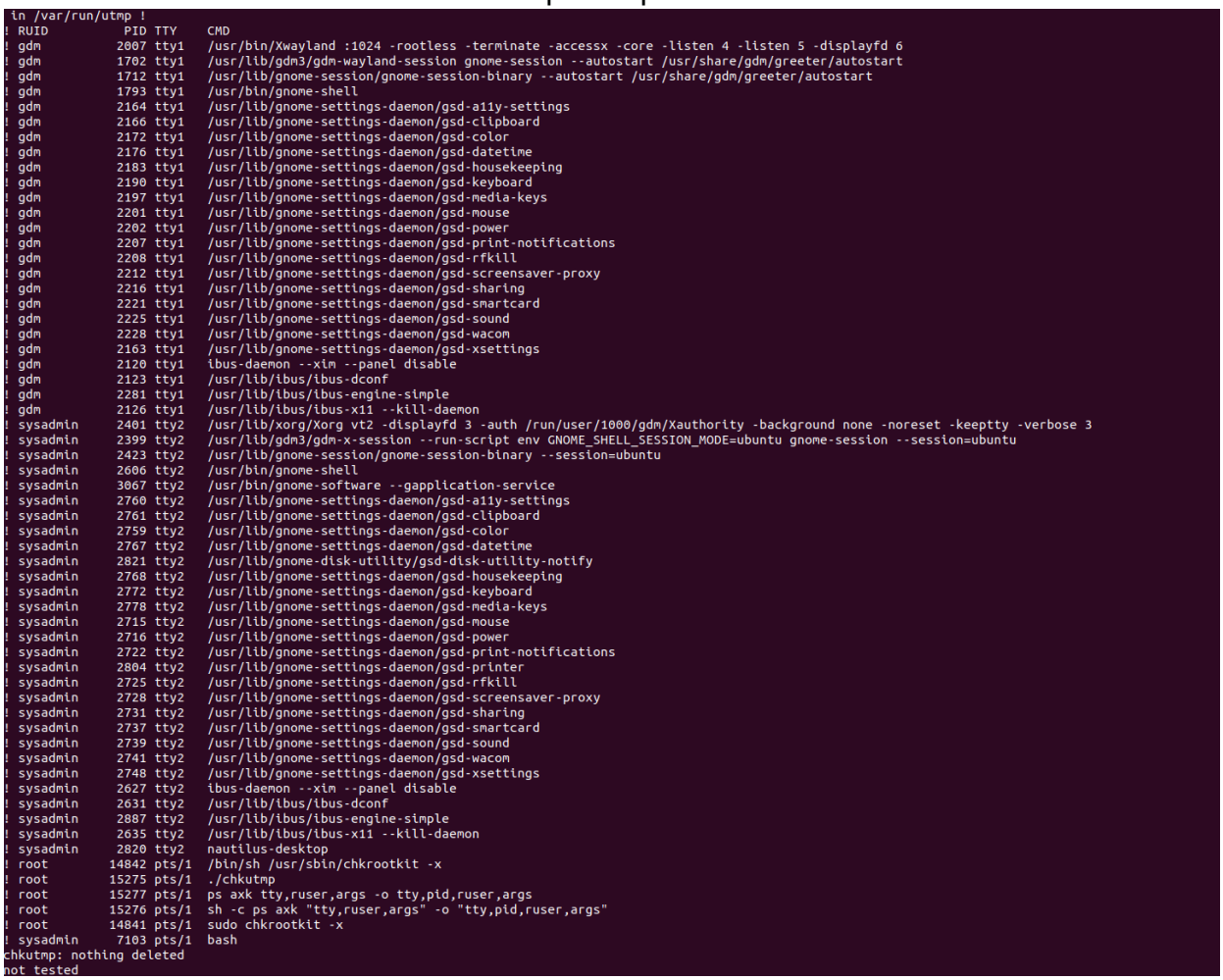
```
Man chkrootkit
```

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:



```
in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          2007 tty1   /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -listen 4 -listen 5 -displayfd 6
! gdm          1702 tty1   /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          1712 tty1   /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/gdm/greeter/autostart
! gdm          1793 tty1   /usr/bin/gnome-shell
! gdm          2164 tty1   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! gdm          2166 tty1   /usr/lib/gnome-settings-daemon/gsd-clipboard
! gdm          2172 tty1   /usr/lib/gnome-settings-daemon/gsd-color
! gdm          2176 tty1   /usr/lib/gnome-settings-daemon/gsd-datetime
! gdm          2183 tty1   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! gdm          2190 tty1   /usr/lib/gnome-settings-daemon/gsd-keyboard
! gdm          2197 tty1   /usr/lib/gnome-settings-daemon/gsd-media-keys
! gdm          2201 tty1   /usr/lib/gnome-settings-daemon/gsd-mouse
! gdm          2202 tty1   /usr/lib/gnome-settings-daemon/gsd-power
! gdm          2207 tty1   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm          2208 tty1   /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm          2212 tty1   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm          2216 tty1   /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm          2221 tty1   /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm          2225 tty1   /usr/lib/gnome-settings-daemon/gsd-sound
! gdm          2228 tty1   /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm          2163 tty1   /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm          2120 tty1   ibus-daemon --xim --panel disable
! gdm          2123 tty1   /usr/lib/ibus/ibus-dconf
! gdm          2281 tty1   /usr/lib/ibus/ibus-engine-simple
! gdm          2126 tty1   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2401 tty2   /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! sysadmin     2399 tty2   /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin     2423 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin     2606 tty2   /usr/bin/gnome-shell
! sysadmin     3067 tty2   /usr/bin/gnome-software --gapplication-service
! sysadmin     2760 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin     2761 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin     2759 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     2767 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     2821 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     2768 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     2772 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     2778 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     2715 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     2716 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     2722 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     2804 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     2725 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     2728 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     2731 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     2737 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     2739 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     2741 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     2748 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     2627 tty2   ibus-daemon --xim --panel disable
! sysadmin     2631 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     2887 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     2635 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2820 tty2   nautilus-desktop
! root        14842 pts/1  /bin/sh /usr/sbin/chkrootkit -x
! root        15275 pts/1  ./chkutmp
! root        15277 pts/1  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        15276 pts/1  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        14841 pts/1  sudo chkrootkit -x
! sysadmin     7103 pts/1  bash
chkutmp: nothing deleted
not tested
```