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 shadow
```

    b. Command to set permissions (if needed):

```
sudo chmod 600 shadow
```

2. Permissions on `/etc/gshadow` should allow only `root` read and write access.

    a. Command to inspect permissions:

```
ls -l gshadow
```

    b. Command to set permissions (if needed):

```
Sudo chmod 600 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 group
```

    b. Command to set permissions (if needed):

```
sudo chmod 644 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 passwd
```

    b. Command to set permissions (if needed):

```
sudo chmod 644 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 adduser sam
sudo adduser joe
sudo adduser amy
sudo adduser sara
sudo adduser 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 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:

```
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:

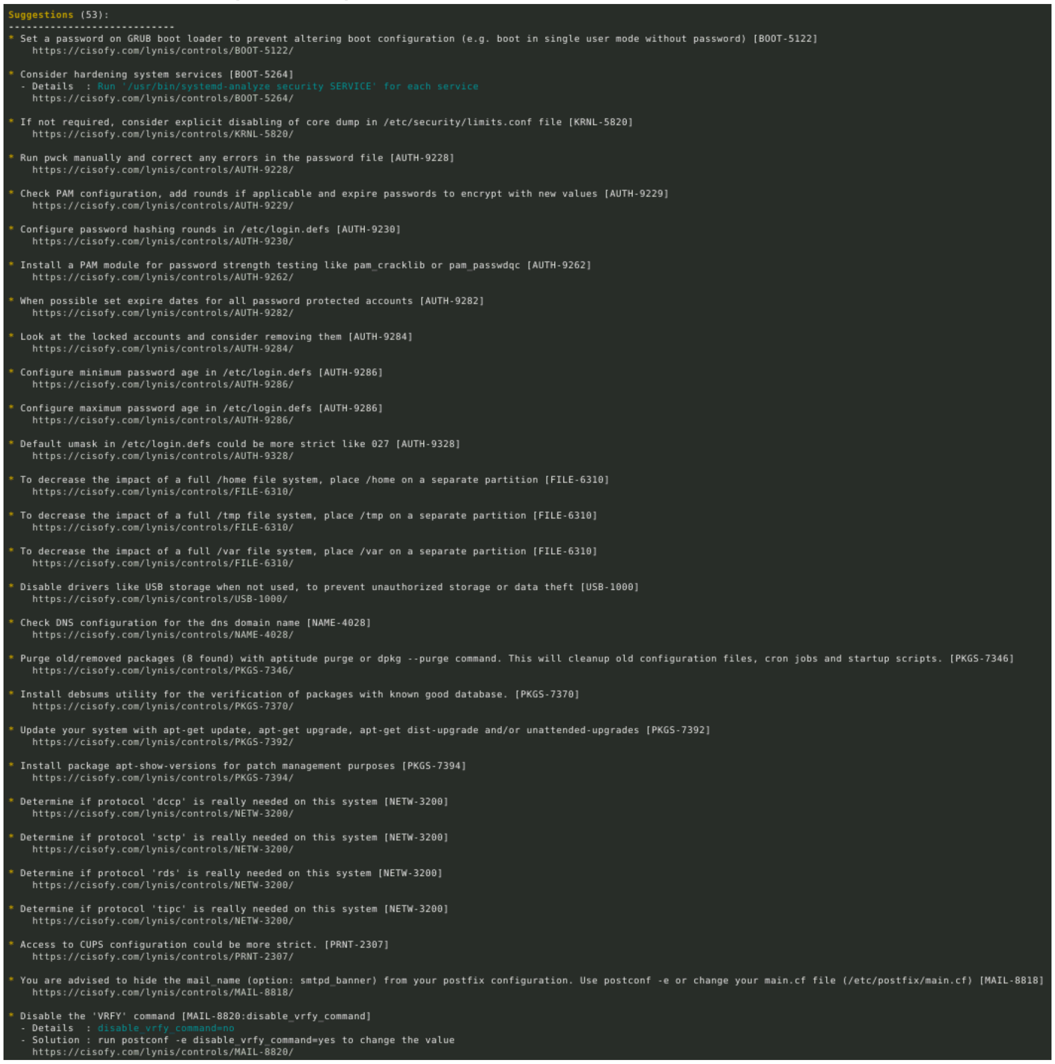
```
sudo lynis --help
```

3. Command to run an audit:

```
sudo lynis audit
```

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

    a. Screenshot of report output:



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

* 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]
    https://cisofy.com/lynis/controls/AUTH-9328/

* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]
    https://cisofy.com/lynis/controls/FILE-6310/

* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]
    https://cisofy.com/lynis/controls/FILE-6310/

* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]
    https://cisofy.com/lynis/controls/FILE-6310/

* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
    https://cisofy.com/lynis/controls/USB-1000/

* Check DNS configuration for the dns domain name [NAME-4028]
    https://cisofy.com/lynis/controls/NAME-4028/

* Purge old/removed packages (8 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]
    https://cisofy.com/lynis/controls/PKGS-7346/

* Install debsums utility for the verification of packages with known good database. [PKGS-7370]
    https://cisofy.com/lynis/controls/PKGS-7370/

* Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades [PKGS-7392]
    https://cisofy.com/lynis/controls/PKGS-7392/

* Install package apt-show-versions for patch management purposes [PKGS-7394]
    https://cisofy.com/lynis/controls/PKGS-7394/

* Determine if protocol 'dccp' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'sctp' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'rds' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'tipc' is really needed on this system [NETW-3200]
    https://cisofy.com/lynis/controls/NETW-3200/

* Access to CUPS configuration could be more strict. [PRNT-2307]
    https://cisofy.com/lynis/controls/PRNT-2307/

* You are advised to hide the mail_name (option: smtpd_banner) from your postfix configuration. Use postconf -e or change your main.cf file (/etc/postfix/main.cf) [MAIL-8818]
    https://cisofy.com/lynis/controls/MAIL-8818/

* Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]
  - Details  : disable_vrfy_command=no
  - Solution : run postconf -e disable_vrfy_command=yes to change the value
    https://cisofy.com/lynis/controls/MAIL-8820/
```

Optional Additional Challenge

1. Command to install chkrootkit:

```
sudo apt install chkrootkit
```

2. Command to view documentation and instructions:

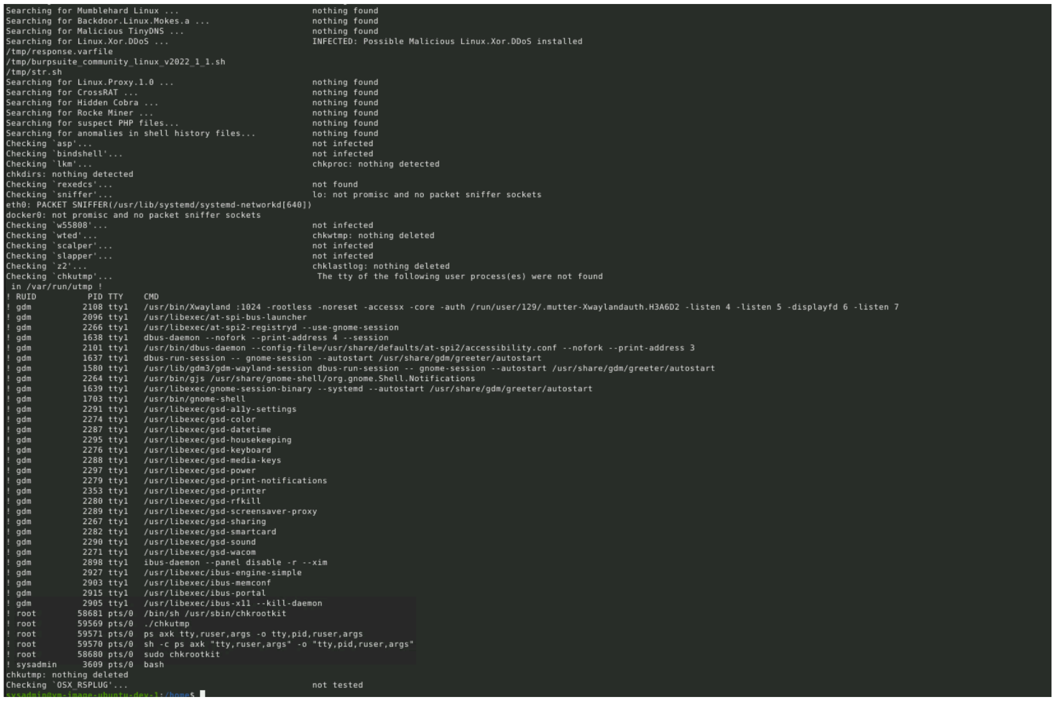
```
sudo chkrootkit --help
```

3. Command to run expert mode:

```
sudo chkrootkit -x
```

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

    a. Screenshot of end of sample output:



```
Searching for Mumblehard Linux ...                          nothing found
Searching for Backdoor.Linux.Mokes.a ...                    nothing found
Searching for Malicious TinyDNS ...                         nothing found
Searching for Linux.Xor.DDoS ...                            INFECTED: Possible Malicious Linux.Xor.DDoS installed
/tmp/response.varfile
/tmp/burpsuite_community_linux_v2022_1_1.sh
/tmp/str.sh
Searching for Linux.Proxy.1.0 ...                           nothing found
Searching for CrossRAT ...                                  nothing found
Searching for Hidden Cobra ...                              nothing found
Searching for Rocke Miner ...                               nothing found
Searching for suspect PHP files...                          nothing found
Searching for anomalies in shell history files...           nothing found
Checking `asp'...                                           not infected
Checking `bindshell'...                                     not infected
Checking `lkm'...                                           chkproc: nothing detected
chkdirs: nothing detected
Checking `rexedcs'...                                       not found
Checking `sniffer'...                                       lo: not promisc and no packet sniffer sockets
eth0: PACKET SNIFFER(/usr/lib/systemd/systemd-networkd[640])
docker0: not promisc and no packet sniffer sockets
Checking `w55808'...                                        not infected
Checking `wted'...                                          chkwtmp: nothing deleted
Checking `scalper'...                                       not infected
Checking `slapper'...                                       not infected
Checking `z2'...                                            chklastlog: nothing deleted
Checking `chkutmp'...                                        The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          2108 tty1   /usr/bin/Xwayland :1024 -rootless -noreset -accessx -core -auth /run/user/129/.mutter-Xwaylandauth.H3A6D2 -listen 4 -listen 5 -displayfd 6 -listen 7
! gdm          2096 tty1   /usr/libexec/at-spi-bus-launcher
! gdm          2266 tty1   /usr/libexec/at-spi2-registryd --use-gnome-session
! gdm          1638 tty1   dbus-daemon --nofork --print-address 4 --session
! gdm          2101 tty1   /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
! gdm          1637 tty1   dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          1580 tty1   /usr/lib/gdm3/gdm-wayland-session dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          2264 tty1   /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
! gdm          1639 tty1   /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
! gdm          1703 tty1   /usr/bin/gnome-shell
! gdm          2291 tty1   /usr/libexec/gsd-a11y-settings
! gdm          2274 tty1   /usr/libexec/gsd-color
! gdm          2287 tty1   /usr/libexec/gsd-datetime
! gdm          2295 tty1   /usr/libexec/gsd-housekeeping
! gdm          2276 tty1   /usr/libexec/gsd-keyboard
! gdm          2288 tty1   /usr/libexec/gsd-media-keys
! gdm          2297 tty1   /usr/libexec/gsd-power
! gdm          2279 tty1   /usr/libexec/gsd-print-notifications
! gdm          2353 tty1   /usr/libexec/gsd-printer
! gdm          2280 tty1   /usr/libexec/gsd-rfkill
! gdm          2289 tty1   /usr/libexec/gsd-screensaver-proxy
! gdm          2267 tty1   /usr/libexec/gsd-sharing
! gdm          2282 tty1   /usr/libexec/gsd-smartcard
! gdm          2290 tty1   /usr/libexec/gsd-sound
! gdm          2271 tty1   /usr/libexec/gsd-wacom
! gdm          2898 tty1   ibus-daemon --panel disable -r --xim
! gdm          2927 tty1   /usr/libexec/ibus-engine-simple
! gdm          2903 tty1   /usr/libexec/ibus-memconf
! gdm          2915 tty1   /usr/libexec/ibus-portal
! gdm          2905 tty1   /usr/libexec/ibus-x11 --kill-daemon
! root        58681 pts/0  /bin/sh /usr/sbin/chkrootkit
! root        59569 pts/0  ./chkutmp
! root        59571 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        59570 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        58680 pts/0  sudo chkrootkit
! sysadmin     3609 pts/0  bash
chkutmp: nothing deleted
Checking `OSX_RSPLUG'...                                    not tested
sysadmin@vm-image-ubuntu-dev-1:/home$
```

    b. chkrootkit provided a list of suspicious directories and notified us of the presence of malicious software (Linux.Xor.DDos).