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 chomod u+rw /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 chomod u+rw /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 -m
sudo useradd joe -m
sudo useradd amy -m
sudo useradd sara -m
sudo useradd admin -m
```

2. Ensure that only the `admin` has general sudo access.

    a. Command to add `admin` to the sudo group:

```
Sudo gpasswd -a admin sudocat
```

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 gpasswd -a sam engineers
sudo gpasswd -a joe engineers
sudo gpasswd -a amy engineers
sudo gpasswd -a sara engineers
```

3. Create a shared folder for this group at `/home/engineers`.
    a. Command to create the shared folder:

```
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 1019 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 system audit
```

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

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:

Lynis System Audit Report

Suggestions for hardening the system are listed below (55):
---
* 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/

* 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/

* 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/

* /etc/exports has no exported file systems, while NFS daemon is running. Check if NFS needs to run on this system [STRG-1928]
https://cisofy.com/lynis/controls/STRG-1928/

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

* Purge old/removed packages (1 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/

* Check iptables rules to see which rules are currently not used [FIRE-4513]
https://cisofy.com/lynis/controls/FIRE-4513/

* Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
https://cisofy.com/lynis/controls/HTTP-6640/

* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
https://cisofy.com/lynis/controls/HTTP-6643/

* Add HTTPS to nginx virtual hosts for enhanced protection of sensitive data and privacy [HTTP-6710]
https://cisofy.com/lynis/controls/HTTP-6710/

* Consider hardening SSH configuration [SSH-7408]
- Details : AllowTcpForwarding (set YES to NO)
https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : ClientAliveCountMax (set 3 to 2)
https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : Compression (set YES to NO)
https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]

- Details : LogLevel (set INFO to VERBOSE)
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : MaxAuthTries (set 6 to 3)
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : MaxSessions (set 10 to 2)
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : Port (set 22 to)
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : TCPKeepAlive (set YES to NO)
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : X11Forwarding (set YES to NO)
  https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : AllowAgentForwarding (set YES to NO)
  https://cisofy.com/lynis/controls/SSH-7408/

* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
  https://cisofy.com/lynis/controls/LOGG-2154/

* Check what deleted files are still in use and why. [LOGG-2190]
  https://cisofy.com/lynis/controls/LOGG-2190/

* If there are no xinetd services required, it is recommended that the daemon be removed [INSE-8100]
  https://cisofy.com/lynis/controls/INSE-8100/

* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
  https://cisofy.com/lynis/controls/BANN-7126/

* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
  https://cisofy.com/lynis/controls/BANN-7130/

* Enable process accounting [ACCT-9622]
  https://cisofy.com/lynis/controls/ACCT-9622/

* Enable sysstat to collect accounting (no results) [ACCT-9626]
  https://cisofy.com/lynis/controls/ACCT-9626/

* Audit daemon is enabled with an empty ruleset. Disable the daemon or define rules [ACCT-9630]
  https://cisofy.com/lynis/controls/ACCT-9630/

* Run 'docker info' to see warnings applicable to Docker daemon [CONT-8104]
  https://cisofy.com/lynis/controls/CONT-8104/

* Consider restricting file permissions [FILE-7524]
  - Details : See screen output or log file
  - Solution : Use chmod to change file permissions
    https://cisofy.com/lynis/controls/FILE-7524/

* Double check the permissions of home directories as some might be not strict enough. [HOME-9304]
    https://cisofy.com/lynis/controls/HOME-9304/

* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
  - Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
    https://cisofy.com/lynis/controls/KRNL-6000/

* Harden compilers like restricting access to root user only [HRDN-7222]
    https://cisofy.com/lynis/controls/HRDN-7222/

Chkrootkit Report

```
###
### Output of: ./ifpromisc
###
lo: not promisc and no packet sniffer sockets
enp0s3: PACKET SNIFFER(/sbin/dhclient[1509])
docker0: not promisc and no packet sniffer sockets
not infected
###
### Output of: ./chkwtmp -f /var/log/wtmp
###
not infected
not infected
###
### Output of: ./chklastlog  -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          2404 tty1   /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -listen 4 -listen 5 -displayfd 6
! gdm          2358 tty1   /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          2363 tty1   /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/gdm/greeter/autostart
! gdm          2370 tty1   /usr/bin/gnome-shell
! gdm          2516 tty1   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! gdm          2521 tty1   /usr/lib/gnome-settings-daemon/gsd-clipboard
! gdm          2528 tty1   /usr/lib/gnome-settings-daemon/gsd-color
! gdm          2541 tty1   /usr/lib/gnome-settings-daemon/gsd-datetime
! gdm          2543 tty1   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! gdm          2544 tty1   /usr/lib/gnome-settings-daemon/gsd-keyboard
! gdm          2557 tty1   /usr/lib/gnome-settings-daemon/gsd-media-keys
! gdm          2561 tty1   /usr/lib/gnome-settings-daemon/gsd-mouse
! gdm          2564 tty1   /usr/lib/gnome-settings-daemon/gsd-power
! gdm          2567 tty1   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm          2569 tty1   /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm          2573 tty1   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm          2574 tty1   /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm          2578 tty1   /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm          2584 tty1   /usr/lib/gnome-settings-daemon/gsd-sound
! gdm          2585 tty1   /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm          2506 tty1   /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm          2464 tty1   ibus-daemon --xim --panel disable
! gdm          2467 tty1   /usr/lib/ibus/ibus-dconf
! gdm          2654 tty1   /usr/lib/ibus/ibus-engine-simple
! gdm          2470 tty1   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2813 tty2   /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! sysadmin     2811 tty2   /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin     2835 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin     3005 tty2   /usr/bin/gnome-shell
! sysadmin     3525 tty2   /usr/bin/gnome-software --gapplication-service
! sysadmin     3173 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin     3174 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin     3167 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     3178 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     3268 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     3179 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     3180 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     3183 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     3128 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     3129 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     3135 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     3220 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     3138 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     3139 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     3141 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     3144 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     3152 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     3153 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     3158 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     3041 tty2   ibus-daemon --xim --panel disable
! sysadmin     3045 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     3331 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     3052 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     3258 tty2   nautilus-desktop
! root        17326 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root        17762 pts/0  ./chkutmp
! root        17764 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        17763 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        17325 pts/0  sudo chkrootkit -x
! sysadmin     3459 pts/0  bash
chkutmp: nothing deleted
not tested
```