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):

```
Not needed
```

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):

```
Not needed
```

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):

```
adduser sam
adduser joe
adduser amy
adduser sara
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:

```
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:engineers /home/engineers
```

Step 4: Lynis Auditing

1. Command to install Lynis:

```
sudo apt install lynis
```

2. Command to view documentation and instructions:

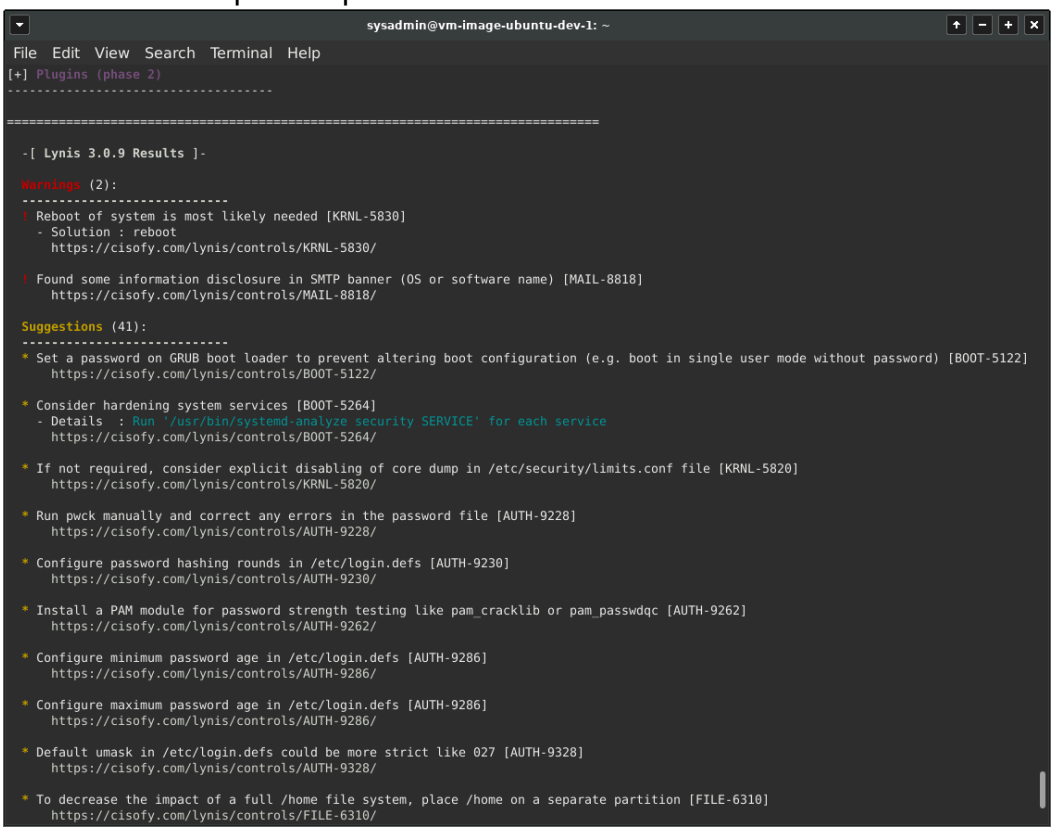
```
man lynis
```

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:



```
sysadmin@vm-image-ubuntu-dev-1: ~
File  Edit  View  Search  Terminal  Help
[+] Plugins (phase 2)
------------------------------------

================================================================================

  -[ Lynis 3.0.9 Results ]-

  Warnings (2):
  ----------------------------
  ! Reboot of system is most likely needed [KRNL-5830]
    - Solution : reboot
      https://cisofy.com/lynis/controls/KRNL-5830/

  ! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
      https://cisofy.com/lynis/controls/MAIL-8818/

  Suggestions (41):
  ----------------------------
  * 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/

  * 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/

  * 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/
```

sysadmin@vm-image-ubuntu-dev-1: ~

File Edit View Search Terminal Help

```
      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 (4 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/

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

  * Install a package audit tool to determine vulnerable packages [PKGS-7398]
      https://cisofy.com/lynis/controls/PKGS-7398/

  * 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 fi
le (/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/
```

```
sysadmin@vm-image-ubuntu-dev-1: ~
File  Edit  View  Search  Terminal  Help

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

 * 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/

 * Enable auditd to collect audit information [ACCT-9628]
     https://cisofy.com/lynis/controls/ACCT-9628/

 * Check output of aa-status [MACF-6208]
   - Details  : /sys/kernel/security/apparmor/profiles
   - Solution : Run aa-status
     https://cisofy.com/lynis/controls/MACF-6208/

 * Determine if automation tools are present for system management [TOOL-5002]
     https://cisofy.com/lynis/controls/TOOL-5002/

 * 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/
```

```
sysadmin@vm-image-ubuntu-dev-1: ~
File  Edit  View  Search  Terminal  Help

 * 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/

 Follow-up:
 ----------------------------
 - Show details of a test (lynis show details TEST-ID)
 - Check the logfile for all details (less /home/sysadmin/lynis.log)
 - Read security controls texts (https://cisofy.com)
 - Use --upload to upload data to central system (Lynis Enterprise users)

================================================================================

  Lynis security scan details:

  Hardening index : 68 [#############       ]
  Tests performed : 248
  Plugins enabled : 0

  Components:
  - Firewall               [V]
  - Malware scanner        [V]

  Scan mode:
  Normal [ ]  Forensics [ ]  Integration [ ]  Pentest [V] (running non-privileged)

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Files:
  - Test and debug information      : /home/sysadmin/lynis.log
  - Report data                     : /home/sysadmin/lynis-report.dat

================================================================================
```

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:

```
sysadmin@vm-image-ubuntu-dev-1: ~
File  Edit  View  Search  Terminal  Help
sysadmin@vm-image-ubuntu-dev-1:~$ sudo chkrootkit -q

/usr/lib/debug/.build-id /usr/lib/modules/5.15.0-1047-azure/vdso/.build-id /usr/lib/modules/5.15.0-1042-azure/vdso/.build-id /usr/lib/llvm-
9/build/utils/lit/tests/.coveragerc
/usr/lib/debug/.build-id /usr/lib/modules/5.15.0-1047-azure/vdso/.build-id /usr/lib/modules/5.15.0-1042-azure/vdso/.build-id
INFECTED: Possible Malicious Linux.Xor.DDoS installed
/tmp/response.varfile
/tmp/burpsuite_community_linux_v2022_1_1.sh
/tmp/str.sh
You have     1 process hidden for readdir command
You have     1 process hidden for ps command
chkproc: Warning: Possible LKM Trojan installed
eth0: PACKET SNIFFER(/usr/lib/systemd/systemd-networkd[702])
 The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          2185 tty1   /usr/bin/Xwayland :1024 -rootless -noreset -accessx -core -auth /run/user/129/.mutter-Xwaylandauth.ZO7NA2 -liste
n 4 -listen 5 -displayfd 6 -listen 7
! gdm          2173 tty1   /usr/libexec/at-spi-bus-launcher
! gdm          2489 tty1   /usr/libexec/at-spi2-registryd --use-gnome-session
! gdm          1399 tty1   dbus-daemon --nofork --print-address 4 --session
! gdm          2178 tty1   /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
! gdm          1398 tty1   dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          1501 tty1   /usr/libexec/dconf-service
! gdm          1303 tty1   /usr/lib/gdm3/gdm-wayland-session dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          2490 tty1   /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
! gdm          1402 tty1   /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
! gdm          1524 tty1   /usr/bin/gnome-shell
! gdm          2536 tty1   /usr/libexec/gsd-a11y-settings
! gdm          2499 tty1   /usr/libexec/gsd-color
! gdm          2520 tty1   /usr/libexec/gsd-datetime
! gdm          2541 tty1   /usr/libexec/gsd-housekeeping
! gdm          2504 tty1   /usr/libexec/gsd-keyboard
! gdm          2521 tty1   /usr/libexec/gsd-media-keys
! gdm          2542 tty1   /usr/libexec/gsd-power
! gdm          2508 tty1   /usr/libexec/gsd-print-notifications
! gdm          2567 tty1   /usr/libexec/gsd-printer
! gdm          2516 tty1   /usr/libexec/gsd-rfkill
! gdm          2524 tty1   /usr/libexec/gsd-screensaver-proxy
! gdm          2496 tty1   /usr/libexec/gsd-sharing
! gdm          2519 tty1   /usr/libexec/gsd-smartcard
! gdm          2532 tty1   /usr/libexec/gsd-sound
! gdm          2497 tty1   /usr/libexec/gsd-wacom
! gdm          2636 tty1   ibus-daemon --panel disable -r --xim
! gdm          2998 tty1   /usr/libexec/ibus-engine-simple
! gdm          2685 tty1   /usr/libexec/ibus-memconf
! gdm          2726 tty1   /usr/libexec/ibus-portal
! gdm          2688 tty1   /usr/libexec/ibus-x11 --kill-daemon
```

```
sysadmin@vm-image-ubuntu-dev-1: ~
File  Edit  View  Search  Terminal  Help
! RUID          PID TTY    CMD
! gdm          2185 tty1   /usr/bin/Xwayland :1024 -rootless -noreset -accessx -core -auth /run/user/129/.mutter-Xwaylandauth.ZO7NA2 -liste
n 4 -listen 5 -displayfd 6 -listen 7
! gdm          2173 tty1   /usr/libexec/at-spi-bus-launcher
! gdm          2489 tty1   /usr/libexec/at-spi2-registryd --use-gnome-session
! gdm          1399 tty1   dbus-daemon --nofork --print-address 4 --session
! gdm          2178 tty1   /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
! gdm          1398 tty1   dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          1501 tty1   /usr/libexec/dconf-service
! gdm          1303 tty1   /usr/lib/gdm3/gdm-wayland-session dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          2490 tty1   /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
! gdm          1402 tty1   /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
! gdm          1524 tty1   /usr/bin/gnome-shell
! gdm          2536 tty1   /usr/libexec/gsd-a11y-settings
! gdm          2499 tty1   /usr/libexec/gsd-color
! gdm          2520 tty1   /usr/libexec/gsd-datetime
! gdm          2541 tty1   /usr/libexec/gsd-housekeeping
! gdm          2504 tty1   /usr/libexec/gsd-keyboard
! gdm          2521 tty1   /usr/libexec/gsd-media-keys
! gdm          2542 tty1   /usr/libexec/gsd-power
! gdm          2508 tty1   /usr/libexec/gsd-print-notifications
! gdm          2567 tty1   /usr/libexec/gsd-printer
! gdm          2516 tty1   /usr/libexec/gsd-rfkill
! gdm          2524 tty1   /usr/libexec/gsd-screensaver-proxy
! gdm          2496 tty1   /usr/libexec/gsd-sharing
! gdm          2519 tty1   /usr/libexec/gsd-smartcard
! gdm          2532 tty1   /usr/libexec/gsd-sound
! gdm          2497 tty1   /usr/libexec/gsd-wacom
! gdm          2636 tty1   ibus-daemon --panel disable -r --xim
! gdm          2998 tty1   /usr/libexec/ibus-engine-simple
! gdm          2685 tty1   /usr/libexec/ibus-memconf
! gdm          2726 tty1   /usr/libexec/ibus-portal
! gdm          2688 tty1   /usr/libexec/ibus-x11 --kill-daemon
! root       910983 pts/2  /bin/sh /usr/sbin/chkrootkit -q
! root       911632 pts/2  ./chkutmp
! root       911634 pts/2  ps axk tty,ruser,args -o tty,pid,ruser,args
! root       911633 pts/2  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root       910982 pts/2  sudo chkrootkit -q
! sysadmin    77711 pts/2  bash
! sysadmin   686409 pts/2  nano passwd
! root       656916 pts/3  nano roulette_dealer_finder_by_time_and_game.sh
! root       656994 pts/3  nano roulette_dealer_finder_by_time_and_game.sh
! root       656896 pts/3  sudo nano roulette_dealer_finder_by_time_and_game.sh
! root       656993 pts/3  sudo nano roulette_dealer_finder_by_time_and_game.sh
! sysadmin   166669 pts/3  bash
! sysadmin   186828 pts/4  bash
! sysadmin   203609 pts/5  bash
sysadmin@vm-image-ubuntu-dev-1:~$
```

Since chkrootkit doesn’t provide recommendations itself, just identifies suspicious files that are potential indicators of a root kit or malicious software/files, the suspicious items identified through the chkrootkit scan would need to be individually looked into based on what category they come back under.

Sources: For the chkrootkit section, I reviewed the FAQ section on the chkrootkit.org website, as well as https://www.youtube.com/watch?v=_M-S5NiFnSI (How to use the Chkrootkit Command: 2 Minute Linux Tips

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.