Week 4 Homework Submission File: Linux Systems Administration

Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on /etc/shadow should allow only root read and write access.

    - Command to inspect permissions: **ls -l /etc/shadow**

    - Command to set permissions (if needed): **sudo chmod 600 shadow**

```
sysadmin@UbuntuDesktop:/etc$ ls -l shadow
-rw------- 1 root shadow 3374 Dec 15 15:48 shadow
```

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

    - Command to inspect permissions: **ls -l /etc/gshadow**

    - Command to set permissions (if needed): **sudo chmod 600 /etc/gshadow**

```
sysadmin@UbuntuDesktop:/$ ls -l /etc/gshadow
-rw------- 1 root shadow 1126 Dec 15 15:53 /etc/gshadow
```

3. Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.

    - Command to inspect permissions: **ls -l /etc/group**
    - Command to set permissions (if needed): **sudo chmod 644 /etc/group**

```
sysadmin@UbuntuDesktop:/$ ls -l /etc/group
-rw-r--r-- 1 root root 1367 Dec 15 15:53 /etc/group
```

4. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.

    - Command to inspect permissions: **ls -l /etc/passwd**

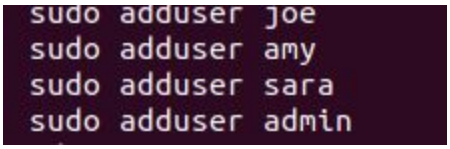
    - Command to set permissions (if needed): **sudo chmod 644 /etc/passwd**

```
sysadmin@UbuntuDesktop:/$ ls -l /etc/passwd
-rw-r--r-- 1 root root 3496 Dec 15 15:48 /etc/passwd
```

Step 2: Create User Accounts

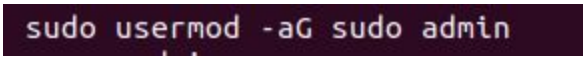
1. Add user accounts for sam, joe, amy, sara, and admin.

    - Command to add each user account (include all five users):
        i. **sudo adduser sam**
        ii. **sudo adduser joe**
        iii. **sudo adduser amy**
        iv. **sudo adduser sara**
        v. **sudo adduser admin**



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

    - 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.

    - Command to add group: **sudo addgroup engineers**

2. Add users sam, joe, amy, and sara to the managed group.

    - Command to add users to engineers group (include all four users):
        i. **sudo usermod -aG engineers sam**
        ii. **sudo usermod -aG engineers joe**
        iii. **sudo usermod -aG engineers amy**
        iv. **sudo usermod -aG engineers sara**

```
sudo usermod -aG engineers amy
sudo usermod -aG engineers joe
sudo usermod -aG engineers sara
sudo usermod -aG engineers sam
```

```
sysadmin@UbuntuDesktop:/$ sudo cat /etc/group | grep engineers
[sudo] password for sysadmin:
engineers:x:1018:amy,joe,sara,sam
```

3. Create a shared folder for this group at /home/engineers.
    - Command to create the shared folder:
        i. **sudo mkdir /home/engineers**

```
drwxrwxr--  2 root       engineers     4096 Dec 15 16:05 engineers
drwxr-xr-x  8 instructor instructor    4096 Oct 27 16:24 instructor
```

4. Change ownership of the new engineers' shared folder to the engineers group.
    - Command to change ownership of engineer's shared folder to engineer group: **sudo chgrp -R engineers /home/engineers**

```
sudo chgrp -R engineers /home/engineers
```

```
drwxrwxr--  2 root       engineers     4096 Dec 15 16:05 engineers
drwxr-xr-x  8 instructor instructor    4096 Oct 27 16:24 instructor
```

Step 4: Lynis Auditing

1. Command to install Lynis: **sudo apt-get install lynis**
2. Command to see documentation and instructions: **man lynis**
3. Command to run an audit: **sudo lynis audit system**
4. Provide a report from the Lynis output on what can be done to harden the system.
    - Screenshot of report output: **Provides suggestion on what can be done to harden the system**

```
Suggestions (53):
----------------------------
* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]
    https://your-domain.example.org/controls/CUST-0280/

* Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]
    https://your-domain.example.org/controls/CUST-0285/

* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [CUST-0810]
    https://your-domain.example.org/controls/CUST-0810/

* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CUST-0811]
    https://your-domain.example.org/controls/CUST-0811/

* Install debian-goodies so that you can run checkrestart after upgrades to determine which services are using old versions of libraries and need restarting. [CUST-0830]
    https://your-domain.example.org/controls/CUST-0830/

* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [CUST-0831]
    https://your-domain.example.org/controls/CUST-0831/

* Install debsecan to generate lists of vulnerabilities which affect this installation. [CUST-0870]
    https://your-domain.example.org/controls/CUST-0870/

* Install debsums for the verification of installed package files against MD5 checksums. [CUST-0875]
    https://your-domain.example.org/controls/CUST-0875/

* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
    https://cisofy.com/controls/DEB-0880/

* Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
    https://cisofy.com/controls/BOOT-5122/

* Run pwck manually and correct any errors in the password file [AUTH-9228]
    https://cisofy.com/controls/AUTH-9228/

* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
    https://cisofy.com/controls/AUTH-9262/

* Configure minimum password age in /etc/login.defs [AUTH-9286]
    https://cisofy.com/controls/AUTH-9286/

* Configure maximum password age in /etc/login.defs [AUTH-9286]
    https://cisofy.com/controls/AUTH-9286/

* Set password for single user mode to minimize physical access attack surface [AUTH-9308]
    https://cisofy.com/controls/AUTH-9308/

* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
    https://cisofy.com/controls/AUTH-9328/

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

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

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

* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [STRG-1840]
    https://cisofy.com/controls/STRG-1840/

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

* Check RPM database as RPM binary available but does not reveal any packages [PKGS-7308]
    https://cisofy.com/controls/PKGS-7308/
```

```
* Purge old/removed packages (3 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]
    https://cisofy.com/controls/PKGS-7346/

* Install debsums utility for the verification of packages with known good database. [PKGS-7370]
    https://cisofy.com/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/controls/PKGS-7392/

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

* Consider running ARP monitoring software (arpwatch,arpon) [NETW-3032]
    https://cisofy.com/controls/NETW-3032/

* Access to CUPS configuration could be more strict. [PRNT-2307]
    https://cisofy.com/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/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/controls/MAIL-8820/

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

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

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

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

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

* Consider hardening SSH configuration [SSH-7408]
  - Details  : Compression (YES --> (DELAYED|NO))
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : LogLevel (INFO --> VERBOSE)
    https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details  : MaxAuthTries (6 --> 2)
    https://cisofy.com/controls/SSH-7408/

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

* Consider hardening SSH configuration [SSH-7408]
  - Details  : PermitRootLogin (WITHOUT-PASSWORD --> NO)
    https://cisofy.com/controls/SSH-7408/
```

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

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

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

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

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

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

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

* 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/controls/KRNL-6000/

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

Bonus

1. Command to install chkrootkit: **sudo apt-get install chkrootkit**

2. Command to see documentation and instructions: **man chkrootkit**

```
chkrootkit(1)                                                    General Commands Manual                                                    chkrootkit(1)

NAME
       chkrootkit - Determine whether the system is infected with a rootkit

SYNOPSIS
       chkrootkit [OPTION]... [TESTNAME]...

DESCRIPTION
       chkrootkit  examines  certain  elements  of the target system and determines whether they have been tampered with. Some tools which chkrootkit applies while analyzing binaries and log files can be found at
       /usr/lib/chkrootkit.

OPTIONS
       -h     Print a short help message and exit.

       -V     Print version information and exit.

       -l     Print available tests.

       -d     Enter debug mode.

       -x     Enter expert mode.

       -e     Exclude known false positive files/dirs, quoted, space separated.

       -q     Enter quiet mode.

       -r dir Use dir as the root directory.

       -p dir1:dir2:dirN
              Specify the path for the external commands used by chkrootkit.

       -n     skip NFS mounted dirs

AUTHOR
       Manual page written by Yotam Rubin <yotam@nakif.omer.k12.il> and lantz moore <lmoore@debian.org> for the Debian project. It may be used by others.

SEE ALSO
       strings(1)

                                                                    10 January 2003                                                            chkrootkit(1)
```

3. Command to run expert mode: **sudo chkrootkit -x**

   Sample output running chkrootkit on expert mode

```
 The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          1965 tty1   /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -listen 4 -listen 5 -displayfd 6
! gdm          1919 tty1   /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          1924 tty1   /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/gdm/greeter/autostart
! gdm          1931 tty1   /usr/bin/gnome-shell
! gdm          2064 tty1   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! gdm          2066 tty1   /usr/lib/gnome-settings-daemon/gsd-clipboard
! gdm          2069 tty1   /usr/lib/gnome-settings-daemon/gsd-color
! gdm          2072 tty1   /usr/lib/gnome-settings-daemon/gsd-datetime
! gdm          2073 tty1   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! gdm          2075 tty1   /usr/lib/gnome-settings-daemon/gsd-keyboard
! gdm          2078 tty1   /usr/lib/gnome-settings-daemon/gsd-media-keys
! gdm          2082 tty1   /usr/lib/gnome-settings-daemon/gsd-mouse
! gdm          2083 tty1   /usr/lib/gnome-settings-daemon/gsd-power
! gdm          2092 tty1   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm          2096 tty1   /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm          2097 tty1   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm          2100 tty1   /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm          2108 tty1   /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm          2112 tty1   /usr/lib/gnome-settings-daemon/gsd-sound
! gdm          2117 tty1   /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm          2063 tty1   /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm          2018 tty1   ibus-daemon --xim --panel disable
! gdm          2021 tty1   /usr/lib/ibus/ibus-dconf
! gdm          2180 tty1   /usr/lib/ibus/ibus-engine-simple
! gdm          2024 tty1   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2257 tty2   /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! sysadmin     2255 tty2   /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
! sysadmin     2274 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin     2458 tty2   /usr/bin/gnome-shell
! sysadmin     2853 tty2   /usr/bin/gnome-software --gapplication-service
! sysadmin     2602 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin     2603 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin     2598 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     2609 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     2672 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     2611 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     2612 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     2616 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     2563 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     2564 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     2568 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     2630 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     2571 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     2572 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     2575 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     2579 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     2580 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     2584 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     2585 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     2479 tty2   ibus-daemon --xim --panel disable
! sysadmin     2483 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     2734 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     2485 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     2665 tty2   nautilus-desktop
! root        22784 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root        23222 pts/0  ./chkutmp
! root        23224 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        23223 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        22783 pts/0  sudo chkrootkit -x
! sysadmin     2820 pts/0  bash
chkutmp: nothing deleted
not tested
```

4. Provide a report from the chkrootkit output on what can be done to harden the system.
    - Screenshot of end of sample output:

```
sysadmin@UbuntuDesktop:/$ sudo chkrootkit | grep -i 'infected'
Checking `basename'...                                    not infected
Checking `chfn'...                                        not infected
Checking `chsh'...                                        not infected
Checking `cron'...                                        not infected
Checking `crontab'...                                     not infected
Checking `date'...                                        not infected
Checking `du'...                                          not infected
Checking `dirname'...                                     not infected
Checking `echo'...                                        not infected
Checking `egrep'...                                       not infected
Checking `env'...                                         not infected
Checking `find'...                                        not infected
Checking `grep'...                                        not infected
Checking `hdparm'...                                      not infected
Checking `su'...                                          not infected
Checking `ifconfig'...                                    not infected
Checking `inetd'...                                       not infected
Checking `init'...                                        not infected
Checking `killall'...                                     not infected
Checking `ldsopreload'...                                 not infected
Checking `login'...                                       not infected
Checking `ls'...                                          not infected
Checking `lsof'...                                        not infected
Checking `netstat'...                                     not infected
Checking `passwd'...                                      not infected
Checking `pidof'...                                       not infected
Checking `ps'...                                          not infected
Checking `pstree'...                                      not infected
Checking `slogin'...                                      not infected
Checking `sendmail'...                                    not infected
Checking `sshd'...                                        not infected
Checking `tar'...                                         not infected
Checking `tcpdump'...                                     not infected
Checking `top'...                                         not infected
Checking `traceroute'...                                  not infected
Checking `vdir'...                                        not infected
Checking `w'...                                           not infected
Checking `write'...                                       not infected
Searching for Linux.Xor.DDoS ...                          INFECTED: Possible Malicious Linux.Xor.DDoS installed
Checking `asp'...                                         not infected
Checking `bindshell'...                                   not infected
Checking `w55808'...                                      not infected
Checking `scalper'...                                     not infected
Checking `slapper'...                                     not infected
! sysadmin    22040 pts/0  grep --color=auto -i infected
```