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:

   View access level for the file: Shadow

   ls -l /etc/shadow

   -rw------- 1 root shadow 3561 Sep 29 00:00 /etc/shadow

   Command to set permissions (if needed):

   Change shadow to allow root to read and write only

   sudo chmod 600 /etc/shadow

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

   Command to inspect permissions:

   View access level for the file:gshadow

   ls -l /etc/gshadow

   -rw------- 1 root shadow 1188 Sep 28 23:39 /etc/gshadow

   Command to set permissions (if needed):

   Change gshadow to allow root to read and write only

   sudo chmod 600 /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:

View access level for the file:group

ls -l /etc/group

-rw-r--r-- 1 root root 1447 Sep 28 23:39 /etc/group

Command to set permissions (if needed):

Change group to allow root to read and write only

sudo chmod 644 /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:

View access level for the file:passwd

ls -l /etc/passw

-rw-r--r-- 1 root root 3514 Sep 29 00:00 /etc/passwd

Command to set permissions (if needed):

Change passwd to allow root to read and write only

sudo chmod 644 /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):

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

   1.A: sudo adduser sam

   1.B: sudo adduser joe

   1.C: sudo adduser amy

   1.D: sudo adduser sara

   1.E: sudo adduser admin

*once we created user account, a UID, and GIU were created:

	Pass:	**UID:**	**GroupID:**
1.A: sudo adduser sam	sam	1016	1007
1.B: sudo adduser joe	joe	1017	1012
1.C: sudo adduser amy	amy	1018	1013
1.D: sudo adduser sara	sara	1019	1014
1.E: sudo adduser admin	admin	1020	1015

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

Command to add admin to the sudo group:

2.A: 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):

2.A: sudo addgroup engineers sam

2.B: sudo addgroup engineers joe

2.C: sudo addgroup engineers amy

2.D: sudo addgroup engineers sara

2.E: sudo addgroup engineers admin

3. **Create a shared folder for this group at /home/engineers.**

Command to create the shared folder:

Cat /etc/group: Engineers:x:1021:sam, joe, amy, sara, admin

Sudo mkdir /home/engineers

4. **Change ownership on the new engineers' shared folder to the engineers group:**

   Command to change ownership of engineer's shared folder to engineer group:

   sudo chown engineers /home/engineers

Step 4: Lynis Auditing

1. Command to install Lynis:

   sudo apt install lynis

   Or, apt instal lynis (from root)

2. Command to see documentation and instructions:

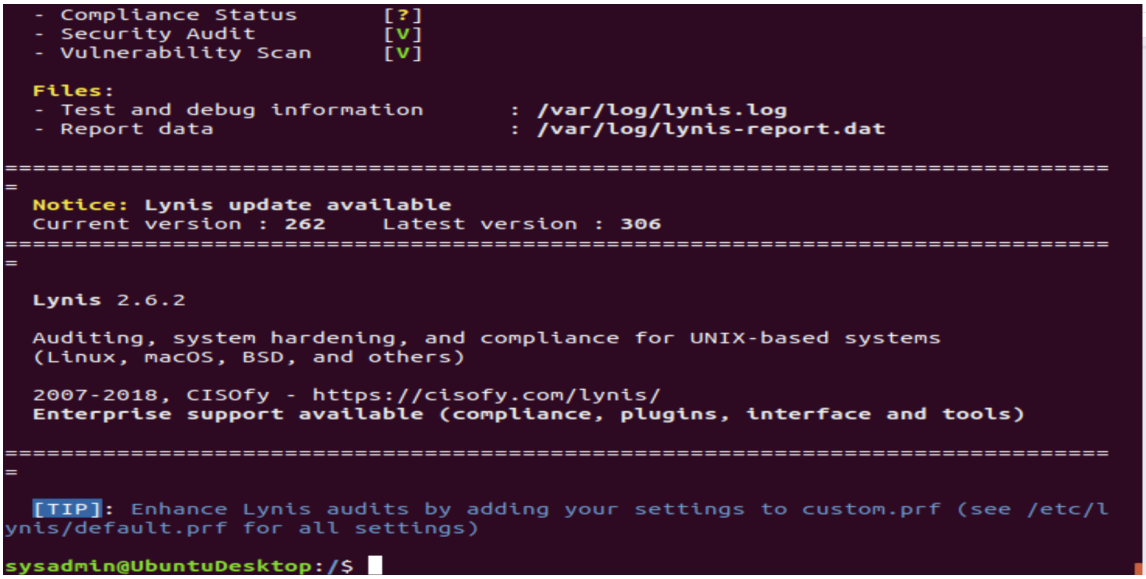
   Run lynis man for manuals/ instructions for complete guide of commands

3. Command to run an audit:

   lynis audit system (from root), Or 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:



```
  - Compliance Status      [?]
  - Security Audit         [V]
  - Vulnerability Scan     [V]

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

================================================================================
=
  Notice: Lynis update available
  Current version : 262    Latest version : 306
================================================================================
=

  Lynis 2.6.2

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

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

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/l
ynis/default.prf for all settings)

sysadmin@UbuntuDesktop:/$
```

Bonus:

1. Command to install chkrootkit:

   sudo apt-get install chkrootkit, Or apt-get instal chkrootkit (from root)

2. Command to see documentation and instructions:

   chkrootkit man

   OPTIONS:

```
      files whether they have been tampered with. Some tools which chk-
      rootkit 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  sepa-
             rated.

      -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
```

-h Print a short help message and exit.

-V Print version information and exit.

-l Print available test s.

-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

3. Command to run expert mode:

sudo chkrootkit -x , Or chkrootkit -x (from root)

4. Provide a report from the chrootkit output on what can be done to harden the system.

Screenshot of end of sample output:

```
! sysadmin      3368 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin      3370 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin      3317 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin      3319 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin      3324 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notificatio
ns
! sysadmin      3394 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin      3325 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin      3327 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin      3331 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin      3332 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin      3338 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin      3340 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin      3347 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin      3229 tty2   ibus-daemon --xim --panel disable
! sysadmin      3241 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin      3465 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin      3245 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin      3429 tty2   nautilus-desktop
! sysadmin      3146 tty2   [notify-send] <defunct>
! root         12496 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root         12931 pts/0  ./chkutmp
! root         12933 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root         12932 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args
"
! root         12493 pts/0  sudo chkrootkit -x
! sysadmin      4274 pts/0  bash
chkutmp: nothing deleted
not tested
sysadmin@UbuntuDesktop:/$
```

VAGRANT UPDATE:

1. Pull the latest vagrant virtual machine build.

1.A: sudo apt install Vagrant

"The following packages will be upgraded:
  libarchive13 librados2
2 upgraded, 119 newly installed, 0 to remove and 481 not upgraded." Run twice....
0 upgraded, 0 newly installed, 0 to remove and 481 not upgraded.

The install went through successfully.