**Week 4 Homework: 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/gshadow**
* **﻿-rw------- 1 root shadow 2888 Dec 7 13:58 /etc/shadowls** 
  + **Command to set permissions (if needed)**:
    - ﻿**Permissions were correct**
    - To change permissions you would be:
      1. chmod +rwx filename to add permissions
      2. chmod -rwx directoryname to remove permissions
      3. chmod +x filename to allow executable permissions
      4. chmod -wx filename to take out write an executable permissions

1. Permissions on /etc/gshadow should allow only root read and write access.
   * Command to inspect permissions:
     + **ls -l /etc/gshadow**

* **﻿-rw------- 1 root shadow 3016 Dec 21 15:29 shadow**
  + **Command to set permissions (if needed)**:
    - ﻿**Permissions were correct**
    - To change permissions you would be:
      1. chmod +rwx filename to add permissions
      2. chmod -rwx directoryname to remove permissions
      3. chmod +x filename to allow executable permissions
      4. chmod -wx filename to take out write an executable permissions

1. 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**
     + **﻿-rw-r--r-- 1 root root 1406 Dec 21 15:38 group**
   * **Command to set permissions (if needed)**:
     + ﻿**Permissions were correct**
     + To change permissions you would:
       1. chmod +rwx filename to add permissions
       2. chmod -rwx directoryname to remove permissions
       3. chmod +x filename to allow executable permissions
       4. chmod -wx filename to take out write an executable permissions
2. 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**
* **﻿-rw-r--r-- 1 root root 3395 Dec 21 15:29 passwd**
  + **Command to set permissions (if needed)**:
    - ﻿**Permissions were correct**
    - To change permissions you would:
      1. chmod +rwx filename to add permissions
      2. chmod -rwx directoryname to remove permissions
      3. chmod +x filename to allow executable permissions
      4. chmod -wx filename to take out write an executable permissions

**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):
     + **﻿sudo useradd sam**
     + **sudo useradd joe**
     + **sudo useradd amy**
     + **sudo useradd sara**
     + **sudo useradd admin**
     + **cat passwd**
2. Ensure that only the admin has general sudo access.
   * Command to add admin to the sudo group:

* ﻿**sudo usermod -G sudo admin**
* **cat group**

**Step 3: Create User Group and Collaborative Folder**

1. Add an engineers group to the system.
   * Command to add group:

* ﻿**sudo addgroup engineers**
* **cat group**

1. Add users sam, joe, amy, and sara to the managed group.
   * Command to add users to engineers group (include all four users):

* ﻿**sudo usermod -G engineers sam**
* **sudo usermod -G engineers joe**
* **sudo usermod -G engineers amy**
* **sudo usermod -G engineers sara**
* **cat group**

1. Create a shared folder for this group at /home/engineers.
   * Command to create the shared folder:
     + ﻿**sudo mkdir /home/engineers**
     + **cd /home**
     + **﻿ls -l**
2. 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 engineers**
     + **ls -l**

**Step 4: Lynis Auditing**

1. Command to install Lynis:

**sudo apt-get install lynis**

Reading package lists... Done

Building dependency tree

Reading state information... Done

**\*\*lynis is already the newest version (2.6.2-1).**

The following packages were automatically installed and are no longer required:

fonts-liberation2 fonts-opensymbol gir1.2-dbusmenu-glib-0.4 gir1.2-dee-1.0

gir1.2-geocodeglib-1.0 gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0

gir1.2-gudev-1.0 gir1.2-udisks-2.0 gir1.2-unity-5.0 grilo-plugins-0.3-base

gstreamer1.0-gtk3 libboost-date-time1.65.1 libboost-locale1.65.1 libcdr-0.1-1

libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5 libcolamd2

libdazzle-1.0-0 libe-book-0.1-1 libedataserverui-1.2-2 libeot0 libepubgen-0.1-1

libetonyek-0.1-1 libevent-2.1-6 libexiv2-14 libfreerdp-client2-2 libfreerdp2-2

libgee-0.8-2 libgexiv2-2 libgom-1.0-0 libgpgmepp6 libgpod-common libgpod4

liblangtag-common liblangtag1 liblirc-client0 libmediaart-2.0-0 libmspub-0.1-1

libodfgen-0.1-1 libqqwing2v5 libraw16 librevenge-0.0-0 libsgutils2-2 libssh-4

libsuitesparseconfig5 libvncclient1 libwinpr2-2 libxmlsec1 libxmlsec1-nss

lp-solve media-player-info python3-debconf python3-debian python3-mako

python3-markupsafe syslinux syslinux-common syslinux-legacy

update-notifier-common usb-creator-common

Use 'sudo apt autoremove' to remove them.

* + 1. upgraded, 0 newly installed, 0 to remove and 352 not upgraded.

1. Command to see documentation and instructions:

* **sudo lynis --help**
* **man lynis**
* **sudo lynis show commands**

﻿

Commands:

* lynis audit
* lynis configure
* lynis show
* lynis update
* lynis upload-only

1. Command to run an audit:

* **sudo lynis audit system**

1. Provide a report from the Lynis output on what can be done to harden the system.
   * Screenshot of report output:
   * Text

     Description automatically generated

**Bonus**

1. Command to install chkrootkit:

* **sudo apt install chkrootkit**

1. Command to see documentation and instructions:

* **sudo chkrootkit --help**

1. Command to run expert mode:

* **sudo chkrootkit -x**

1. Provide a report from the chrootkit output on what can be done to harden the system.
   * Screenshot of end of sample output:

Text

Description automatically generated