**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:
   * Command to set permissions (if needed):

﻿sysadmin@UbuntuDesktop:~$ ls -l /etc/shadow

-rw------- 1 root shadow 3477 Dec 15 14:18 /etc/shadow

sysadmin@UbuntuDesktop:~$

1. Permissions on /etc/gshadow should allow only root read and write access.
   * Command to inspect permissions:
   * Command to set permissions (if needed):

﻿sysadmin@UbuntuDesktop:~$ ls -l /etc/gshadow

-rw------- 1 root shadow 1135 Dec 15 14:21 /etc/gshadow

1. Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.
   * Command to inspect permissions:
   * Command to set permissions (if needed):

﻿sysadmin@UbuntuDesktop:~$ ls -l /etc/group

-rw----r-- 1 root root 1380 Dec 15 14:21 /etc/group

sysadmin@UbuntuDesktop:~$ sudo chmod 644 /etc/group

sysadmin@UbuntuDesktop:~$ ls -l /etc/group

-rw-r--r-- 1 root root 1380 Dec 15 14:21 /etc/group

1. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.
   * Command to inspect permissions:
   * Command to set permissions (if needed):

﻿﻿sysadmin@UbuntuDesktop:~$ sudo chmod 644 /etc/passwd

sysadmin@UbuntuDesktop:~$ ls -l /etc/passwd

-rw-r--r-- 1 root root 3358 Dec 15 14:18 /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):

sysadmin@UbuntuDesktop:/home$ sudo adduser sam

Adding user `sam' ...

Adding new group `sam' (1014) ...

Adding new user `sam' (1007) with group `sam' ...

Creating home directory `/home/sam' ...

Copying files from `/etc/skel' ...

Enter new UNIX password:

Retype new UNIX password:

Sorry, passwords do not match

passwd: Authentication token manipulation error

passwd: password unchanged

Try again? [y/N] y

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

Changing the user information for sam

Enter the new value, or press ENTER for the default

Full Name []: Sam

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n] y

sysadmin@UbuntuDesktop:/home$ sudo adduser joe

Adding user `joe' ...

Adding new group `joe' (1015) ...

Adding new user `joe' (1013) with group `joe' ...

Creating home directory `/home/joe' ...

Copying files from `/etc/skel' ...

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

Changing the user information for joe

Enter the new value, or press ENTER for the default

Full Name []: Joe

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n] Y

sysadmin@UbuntuDesktop:/home$ sudo adduser amy

Adding user `amy' ...

Adding new group `amy' (1016) ...

Adding new user `amy' (1014) with group `amy' ...

Creating home directory `/home/amy' ...

Copying files from `/etc/skel' ...

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

Changing the user information for amy

Enter the new value, or press ENTER for the default

Full Name []: Amy

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n] Y

sysadmin@UbuntuDesktop:/home$ sudo adduser sara

Adding user `sara' ...

Adding new group `sara' (1017) ...

Adding new user `sara' (1015) with group `sara' ...

Creating home directory `/home/sara' ...

Copying files from `/etc/skel' ...

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

Changing the user information for sara

Enter the new value, or press ENTER for the default

Full Name []: Sara

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n] Y

sysadmin@UbuntuDesktop:/home$ sudo adduser admin

Adding user `admin' ...

Adding new group `admin' (1018) ...

Adding new user `admin' (1016) with group `admin' ...

Creating home directory `/home/admin' ...

Copying files from `/etc/skel' ...

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

Changing the user information for admin

Enter the new value, or press ENTER for the default

Full Name []: admin

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n] Y

1. Ensure that only the admin has general sudo access.
   * Command to add admin to the sudo group:

sysadmin@UbuntuDesktop:/home$ sudo usermod -aG sudo admin

﻿sysadmin@UbuntuDesktop:~$ sudo groups admin

admin : admin sudo

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

1. Add an engineers group to the system.
   * Command to add group:
2. Add users sam, joe, amy, and sara to the managed group.
   * Command to add users to engineers group (include all four users):
3. Create a shared folder for this group at /home/engineers.
   * Command to create the shared folder:
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:

sysadmin@UbuntuDesktop:/home$ sudo addgroup engineers

Adding group `engineers' (GID 1019) ...

Done.

sysadmin@UbuntuDesktop:/home$ sudo usermod -aG engineers sam

sysadmin@UbuntuDesktop:/home$ sudo usermod -aG engineers joe

sysadmin@UbuntuDesktop:/home$ sudo usermod -aG engineers amy

sysadmin@UbuntuDesktop:/home$ sudo usermod -aG engineers sara

sysadmin@UbuntuDesktop:/home$ sudo usermod -aG sudo admin

sysadmin@UbuntuDesktop:/home$ groups sam

sam : sam engineers

sysadmin@UbuntuDesktop:/home$ groups joe

joe : joe engineers

sysadmin@UbuntuDesktop:/home$ groups amy

amy : amy engineers

sysadmin@UbuntuDesktop:/home$ groups sara

sara : sara engineers

sysadmin@UbuntuDesktop:/home$ groups admin

admin : admin sudo

sysadmin@UbuntuDesktop:/home$ sudo mkdir engineers

sysadmin@UbuntuDesktop:/home$ sudo chmod 777 engineers

﻿sysadmin@UbuntuDesktop:/home/engineers$ ls -la

drwxrwxrwx 2 root root 4096 Dec 15 14:26

﻿grep -i "sam\|joe\|amy\|sara\|admin" /etc/passwd

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

sysadmin:x:1000:1000:sysadmin,,,:/home/sysadmin:/bin/bash

sam:x:1007:1014:Sam,,,:/home/sam:/bin/bash

joe:x:1013:1015:Joe,,,:/home/joe:/bin/bash

amy:x:1014:1016:Amy,,,:/home/amy:/bin/bash

sara:x:1015:1017:Sara,,,:/home/sara:/bin/bash

admin:x:1016:1018:admin,,,:/home/admin:/bin/bash

**Step 4: Lynis Auditing**

1. Command to install Lynis:

**sudo apt install lynis**

1. Command to see documentation and instructions:

* man lynis
* DOCUMENTATION :Supporting documentation can be found via https://cisofy.com/support/

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:

﻿﻿root@UbuntuDesktop:/# sudo apt 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:

﻿Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Bonus**

1. Command to install chkrootkit:

root@UbuntuDesktop:/# sudo apt install chkrootkit

Reading package lists... Done

Building dependency tree

Reading state information... Done

chkrootkit is already the newest version (0.52-1ubuntu0.1).

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

1. Command to see documentation and instructions:

* ﻿man chkrootkit
* Chkrootkit.org
* The Manual Documentation exists on the Home Page of chkrootkit.org

1. Command to run expert mode:

sudo chkrootkit -x > /usr/sbin/chkrootkit2.txt

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

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated