Module 4 Challenge: Linux Systems Administration

In this module's class activities, you acted as a system administrator in order to troubleshoot a malfunctioning Linux server.

The senior administrator was quite pleased with your work. Now, they would like you to prepare another server to replace the malfunctioning server. To do so, complete the steps detailed in the Instructions section.

Lab Environment

You will continue to use your web lab this week.

Instructions

For each of the following steps, you will need to run the correct command and confirm the results. Take notes of those results as you will be using it for the quiz.

Step 1: Ensure Permissions on Sensitive Files

The `/etc/` directory is where system configuration files exist. Start by navigating to this directory with `cd /etc/`.

Inspect the file permissions of each of the following files. You should have already done this during an in-class activity, but double check them now. If any file's permissions do not match the descriptions listed here, update the file's permissions.

1. Permissions on `/etc/shadow` should allow only `root` read and write access.
2. Permissions on `/etc/gshadow` should allow only `root` read and write access.
3. Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else read access only.
4. Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else read access only.

   Hint:

   Run the following command to view the file permissions: `ls -l <file>`.

   If permissions need changing or modifying, use the `chmod` command.

cd /etc/
ls -l /etc/shadow
ls -l /etc/gshadow
ls -l /etc/group
ls -l /etc/passwd

```
sysadmin@vm-image-ubuntu-dev-1:/etc$ ls -l /etc/shadow
-rw------- 1 root shadow 3188 Mar 21 09:48 /etc/shadow
sysadmin@vm-image-ubuntu-dev-1:/etc$ ls -l /etc/gshadow
-rw------- 1 root shadow 1401 Mar 21 09:47 /etc/gshadow
sysadmin@vm-image-ubuntu-dev-1:/etc$ ls -l /etc/group
-rw-r--r-- 1 root root 1674 Mar 21 09:47 /etc/group
sysadmin@vm-image-ubuntu-dev-1:/etc$ ls -l /etc/passwd
-rw-r--r-- 1 root root 3778 Mar 21 09:48 /etc/passwd
sysadmin@vm-image-ubuntu-dev-1:/etc$
```

Step 2: Create User Accounts

In this step, you'll set up various users in the system. For this exercise, use the `useradd` command. Research this command to determine how to best use this tool to create the user accounts. The necessary commands do not require that you work from a specific directory.

1. Add user accounts for `sam`, `joe`, `amy`, `sara`, and `admin1`.

   Hint: In order to add users to the system, you need to run the command with `sudo`.

   sudo useradd sam (same for joe, amy, sara & admin1)
   sudo passwd sam (same for joe, amy, sara & admin1)

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo useradd sam
[sudo] password for sysadmin:
sysadmin@vm-image-ubuntu-dev-1:~$ sudo useradd joe
sysadmin@vm-image-ubuntu-dev-1:~$ sudo useradd amy
sysadmin@vm-image-ubuntu-dev-1:~$ sudo useradd sara
sysadmin@vm-image-ubuntu-dev-1:~$ sudo useradd admin1
sysadmin@vm-image-ubuntu-dev-1:~$ sudo useradd admin1
useradd: user 'admin1' already exists
sysadmin@vm-image-ubuntu-dev-1:~$ sudo passwd sam
New password:
Retype new password:
passwd: password updated successfully
sysadmin@vm-image-ubuntu-dev-1:~$ sudo password joe
sudo: password: command not found
sysadmin@vm-image-ubuntu-dev-1:~$ sudo passwd joe
New password:
Retype new password:
passwd: password updated successfully
sysadmin@vm-image-ubuntu-dev-1:~$ sudo passwd amy
New password:
Retype new password:
passwd: password updated successfully
sysadmin@vm-image-ubuntu-dev-1:~$ sudo passwd sara
New password:
Retype new password:
passwd: password updated successfully
sysadmin@vm-image-ubuntu-dev-1:~$ sudo passwd admin1
New password:
Retype new password:
passwd: password updated successfully
```

2. Make sure that only the `admin1` user has general `sudo` group access. This requires a command that will allow user modifications.

sudo usermod -a -G sudo admin1
sudo -lU admin1

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo -lU admin1
Matching Defaults entries for admin1 on vm-image-ubuntu-dev-1:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User admin1 may run the following commands on vm-image-ubuntu-dev-1:
    (ALL : ALL) ALL
sysadmin@vm-image-ubuntu-dev-1:~$
```

Step 3: Create User Group and Collaborative Folder

Now, you'll run the commands to fully set up a group on your system.

This requires you to create a group, add users to it, create a shared group folder, and set the group folder owners for this shared folder.

1. Add the group `engineers` to the system.
   sudo groupadd engineers
   sudo tail /etc/group

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo groupadd engineers
sysadmin@vm-image-ubuntu-dev-1:~$ sudo tail /etc/group
developers:x:1015:adam,billy,sally,max,jane
mike:x:1016:
general:x:1017:mike
splunk:x:142:
sam:x:1018:
joe:x:1019:
amy:x:1020:
sara:x:1021:
admin1:x:1022:
engineers:x:1023:
sysadmin@vm-image-ubuntu-dev-1:~$
```

2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group. The process is similar to the one you used to add `admin1` to the `sudo` group in the previous step.
   sudo usermod -a -G engineers joe
   sudo usermod -a -G engineers amy
   sudo usermod -a -G engineers sara

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo usermod -a -G engineers sam
sysadmin@vm-image-ubuntu-dev-1:~$ sudo usermod -a -G engineers joe
sysadmin@vm-image-ubuntu-dev-1:~$ sudo usermod -a -G engineers amy
sysadmin@vm-image-ubuntu-dev-1:~$ sudo usermod -a -G engineers sara
sysadmin@vm-image-ubuntu-dev-1:~$ id sam
uid=1014(sam) gid=1018(sam) groups=1018(sam),1023(engineers)
sysadmin@vm-image-ubuntu-dev-1:~$ id joe
uid=1015(joe) gid=1019(joe) groups=1019(joe),1023(engineers)
sysadmin@vm-image-ubuntu-dev-1:~$ id amy
uid=1016(amy) gid=1020(amy) groups=1020(amy),1023(engineers)
sysadmin@vm-image-ubuntu-dev-1:~$ id sara
uid=1017(sara) gid=1021(sara) groups=1021(sara),1023(engineers)
sysadmin@vm-image-ubuntu-dev-1:~$
```

sudo tail /etc/group

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo tail /etc/group
developers:x:1015:adam,billy,sally,max,jane
mike:x:1016:
general:x:1017:mike
splunk:x:142:
sam:x:1018:
joe:x:1019:
amy:x:1020:
sara:x:1021:
admin1:x:1022:
engineers:x:1023:sam,joe,amy,sara
sysadmin@vm-image-ubuntu-dev-1:~$
```

3. Create a shared folder for this group: `/home/engineers`.
   cd /home
   sudo mkdir engineers

4. Change ownership on the new engineers' shared folder to the `engineers` group.
   sudo chown :engineers /home/engineers

```
sysadmin@vm-image-ubuntu-dev-1:/home$ sudo chown :engineers /home/engineers
sysadmin@vm-image-ubuntu-dev-1:/home$ ls
adam  azadmin  billy  engineers  http  instructor  jane  john  max  mike  packer  sally  student  sysadmin  user.hashes
sysadmin@vm-image-ubuntu-dev-1:/home$ more engineers

*** engineers: directory ***

sysadmin@vm-image-ubuntu-dev-1:/home$
```

Step 4: Lynis Auditing

The final step on your administrator's list involves running an audit against the system in order to harden it. You'll use the system and security auditing tool Lynis to do so.

1. Install the Lynis package to your system if it is not already installed.

2. Check the Lynis documentation for instructions on how to run a system audit.

3. Run a Lynis system audit with `sudo`.

4. Provide a report from the Lynis output with recommendations for how to harden the system.

   Lynis is installed.
   Lynis is checked with sudo lynis show help.
   System audit is run with sudo - sudo lynis audit system --test-from-group sudo

   Report is provided as a text.

```
sysadmin@vm-image-ubuntu-dev-1:/home$ sudo lynis audit system --test-from-group sudo

[ Lynis 3.1.0 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.0
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  20.04
  Kernel version:            5.15.0
  Hardware platform:         x86_64
  Hostname:                  vm-image-ubuntu-dev-1
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /usr/share/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                sudo
  ---------------------------------------------------
```

Or simply just- sudo lynis audit system

```
sysadmin@vm-image-ubuntu-dev-1:/home$ sudo lynis audit system

[ Lynis 3.1.0 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.0
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  20.04
  Kernel version:            5.15.0
  Hardware platform:         x86_64
  Hostname:                  vm-image-ubuntu-dev-1
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /usr/share/lynis/plugins
  ---------------------------------------------------
```

IMPORTANT: Please review your answers carefully before submitting to ensure that they are free of spelling and spacing errors. Incorrect spelling or incorrect spacing syntax will be marked as incorrect answers.

Question 1 12 pts

What is the command used to set permissions on `/etc/shadow` to allow only `root` read and write access?

Group of answer choices

- sudo chmod 600 /etc/shadow
- sudo cd 600 /etc/shadow
- sudo chmod /etc/shadow
- sudo chmod /etc/shadow 600

Question 2 10 pts

What is the octal notation used to set permissions to allow only read/write for root and read for everyone else?

Group of answer choices

- 600
- 644
- 777
- 505

Question 3 10 pts

What is the command to add the user 'sam'?

Group of answer choices

- sudo adduser > sam
- sudo createusr sam
- sudo useradd sam
- sudo useradd = sam

Question 4 12 pts

What is the command used to add the 'admin1' user to the sudoer's group?

Group of answer choices

- sudo grpmod sudo > admin1
- sudo usermod -G sudo admin1
- sudo usermod sudo = admin1
- sudo groupmod sudo admin1

Question 5 10 pts

What is the command used to create the 'engineers' group?

Group of answer choices

- sudo groupadd = engineers
- sudo creategrp = engineers
- sudo addgroup > engineers
- sudo addgroup engineers

Question 6 12 pts

What is the command used to add the 'sam' user to a group without removing them from other groups?

Group of answer choices

- sudo usermod engineers sam
- sudo grpmod > engineers sam
- sudo modgrp sam > engineers
- sudo usermod -aG engineers sam

Question 7 10 pts

What command is used to create a shared folder for the 'engineers' group `/home/engineers`?

Group of answer choices

- sudo mkdir /home/engineers
- sudo mkdir /home = engineers
- sudo mkdir engineers > home
- sudo mkhm /home/engineers

Question 8 12 pts

What is the command to change the ownership of the engineer's folder `/home/engineers` to the engineers group?

Group of answer choices

- sudo chown :engineers /home/engineers
- sudo chowner /home/engineers > engineers
- sudo chown engineers > /home/engineers
- sudo chown /home/engineers = engineers

Question 9 12 pts

What is the command to run a system audit in 'lynis'?

Group of answer choices

- sudo lynis audit -system
- sudo lynis system audit
- sudo lynis -audit system
- sudo lynis audit system