## 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:

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

-rw-r----- 1 root shadow 2864 Jul 8 23:20 /etc/shadow

- Command to set permissions (if needed):

sysadmin@UbuntuDesktop:/etc$ sudo chmod 600 shadow

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

-rw------- 1 root shadow 2864 Jul 8 23:20 /etc/shadow

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

- Command to inspect permissions:

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

-rw-r----- 1 root shadow 1056 Jul 8 23:20 /etc/gshadow

- Command to set permissions (if needed):

sysadmin@UbuntuDesktop:/etc$ sudo chmod 600 gshadow

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

-rw------- 1 root shadow 1056 Jul 8 23:20 /etc/gshado

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

- Command to inspect permissions:

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

-rw-r--r-- 1 root root 1277 Jul 8 23:20 /etc/group

- Command to set permissions (if needed):

sysadmin@UbuntuDesktop:/etc$ sudo chmod 644 group

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

-rw-r--r-- 1 root root 1277 Jul 8 23:20 /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:

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

-rw-r--r-- 1 root root 3131 Jul 8 23:20 /etc/passwd

- Command to set permissions (if needed):

sysadmin@UbuntuDesktop:/etc$ sudo chmod 644 passwd

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

-rw-r--r-- 1 root root 3131 Jul 8 23:20 /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:/$ sudo su

root@UbuntuDesktop:/# 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:

passwd: password updated successfully

Changing the user information for sam

Enter the new value, or press ENTER for the default

Full Name []:

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n] y

You have new mail in /var/mail/root

root@UbuntuDesktop:/# adduser joe

Adding user `joe' ...

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

Adding new user `joe' (1012) 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 []:

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n] y

root@UbuntuDesktop:/# adduser amy

Adding user `amy' ...

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

Adding new user `amy' (1013) 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 []:

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n] y

root@UbuntuDesktop:/# adduser sara

Adding user `sara' ...

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

Adding new user `sara' (1014) 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 []:

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n] y

root@UbuntuDesktop:/#

root@UbuntuDesktop:/# adduser admin

Adding user `admin' ...

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

Adding new user `admin' (1015) 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 []:

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n] y

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

- Command to add `admin` to the `sudo` group:

sudo usermod -a -G sudo admin

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

1. Add an `engineers` group to the system.

- Command to add group:

sysadmin@UbuntuDesktop:/etc$ sudo su

root@UbuntuDesktop:/etc# addgroup engineers

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

Done.

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

- Command to add users to `engineers` group (include all four users):

root@UbuntuDesktop:/etc# sudo usermod -a -G engineers sam

root@UbuntuDesktop:/etc# sudo usermod -a -G engineers joe

root@UbuntuDesktop:/etc# sudo usermod -a -G engineers amy

root@UbuntuDesktop:/etc# sudo usermod -a -G engineers sara

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

- Command to create the shared folder:

sysadmin@UbuntuDesktop:/home$ sudo mkdir -p /bigproject/sharedFolder

sysadmin@UbuntuDesktop:/home$ sudo chgrp -R engineers /bigproject/sharedFolder

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 root:engineers sharedFolder

(at least I think the original group owner was root, I came back to edit after the fact)  
Checking with ls -l, output: drwxr-xr-x 2 root engineers 4096 Jul 11 00:40 sharedFolder

### Step 4: Lynis Auditing

1. Command to install Lynis:

sysadmin@UbuntuDesktop:/usr/local$ sudo git clone https://github.com/CISOfy/lynis

Cloning into 'lynis'...

remote: Enumerating objects: 14082, done.

remote: Counting objects: 100% (237/237), done.

remote: Compressing objects: 100% (143/143), done.

remote: Total 14082 (delta 143), reused 171 (delta 94), pack-reused 13845

Receiving objects: 100% (14082/14082), 7.53 MiB | 8.26 MiB/s, done.

Resolving deltas: 100% (10377/10377), done.

2. Command to see documentation and instructions:

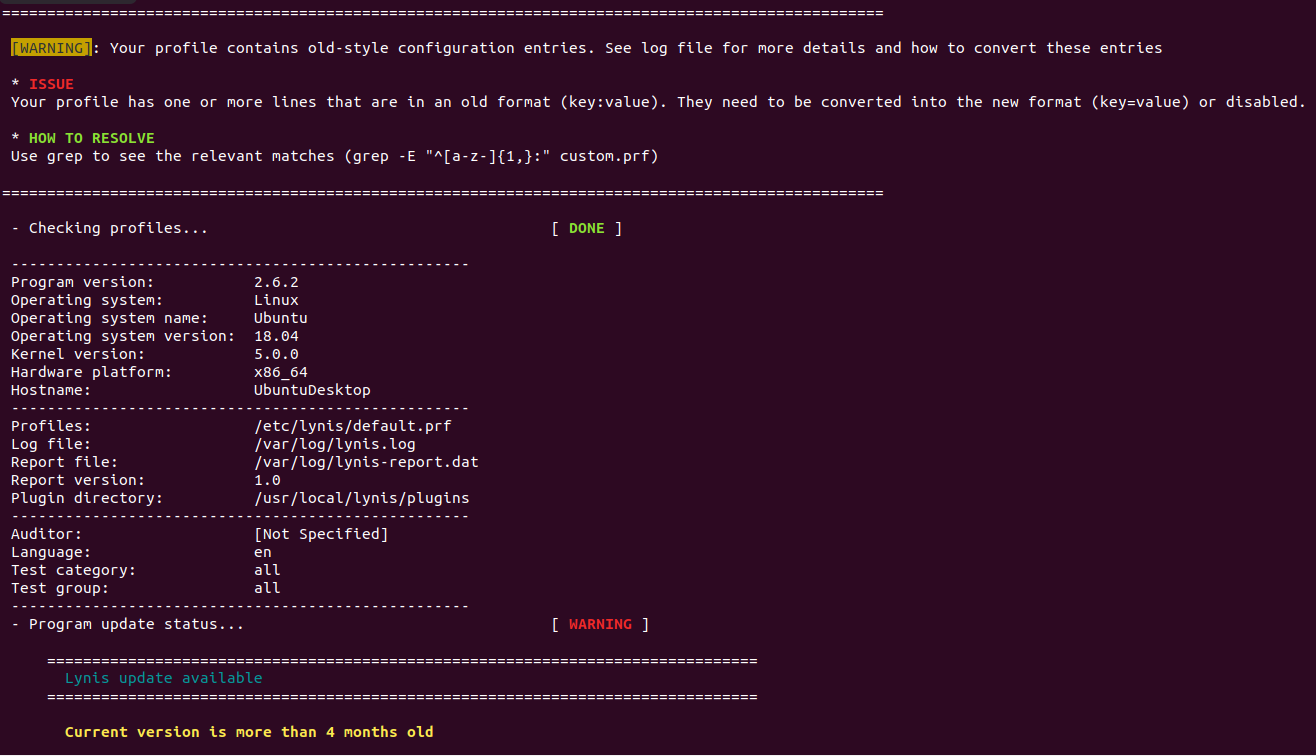
sysadmin@UbuntuDesktop:/usr/local/lynis$ man lynis

3. Command to run an audit:

sysadmin@UbuntuDesktop:/usr/local/lynis$ sudo lynis audit system --quick

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

- Screenshot of report output:



### Bonus

1. Command to install chkrootkit:

apt install chkrootkit -y

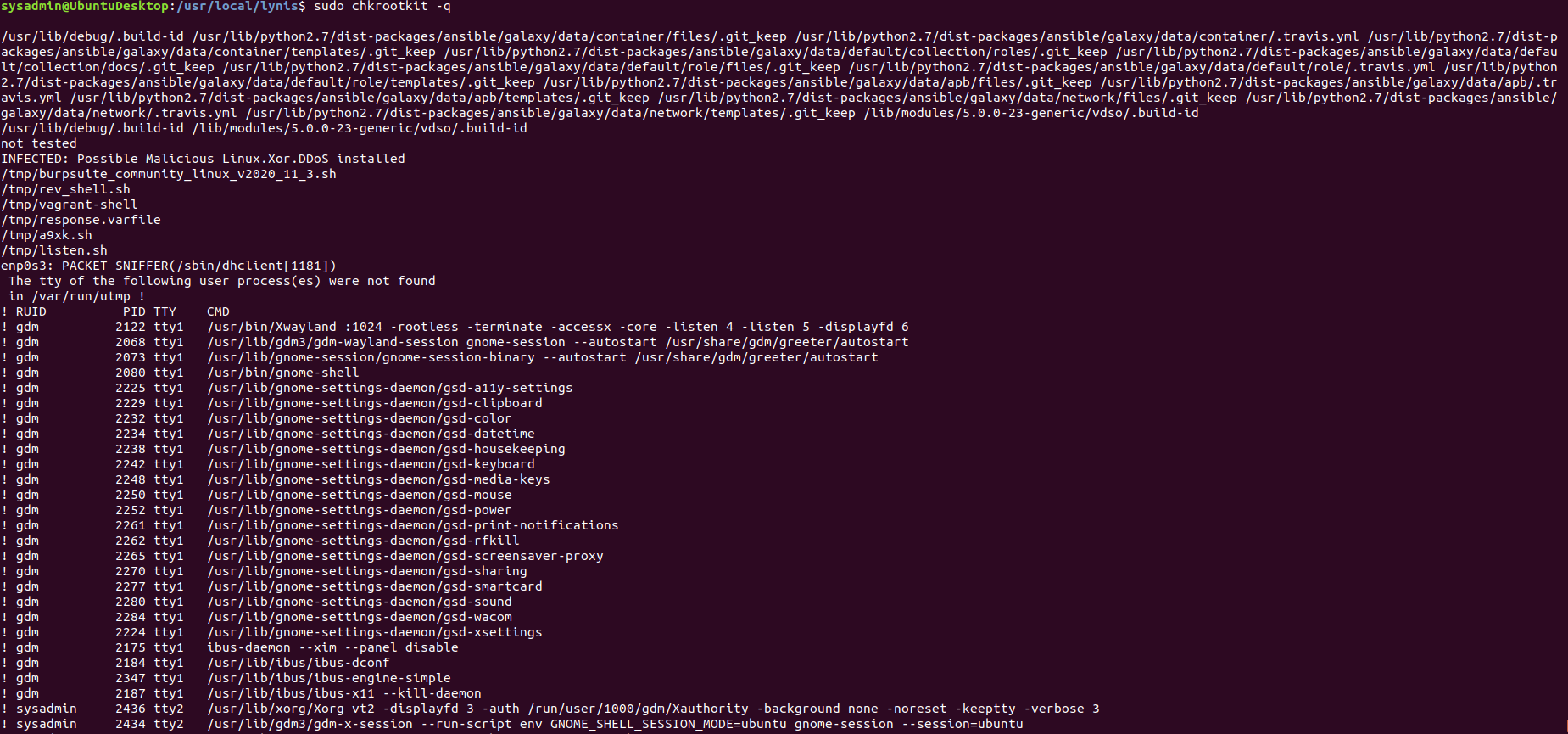
2. Command to see documentation and instructions:

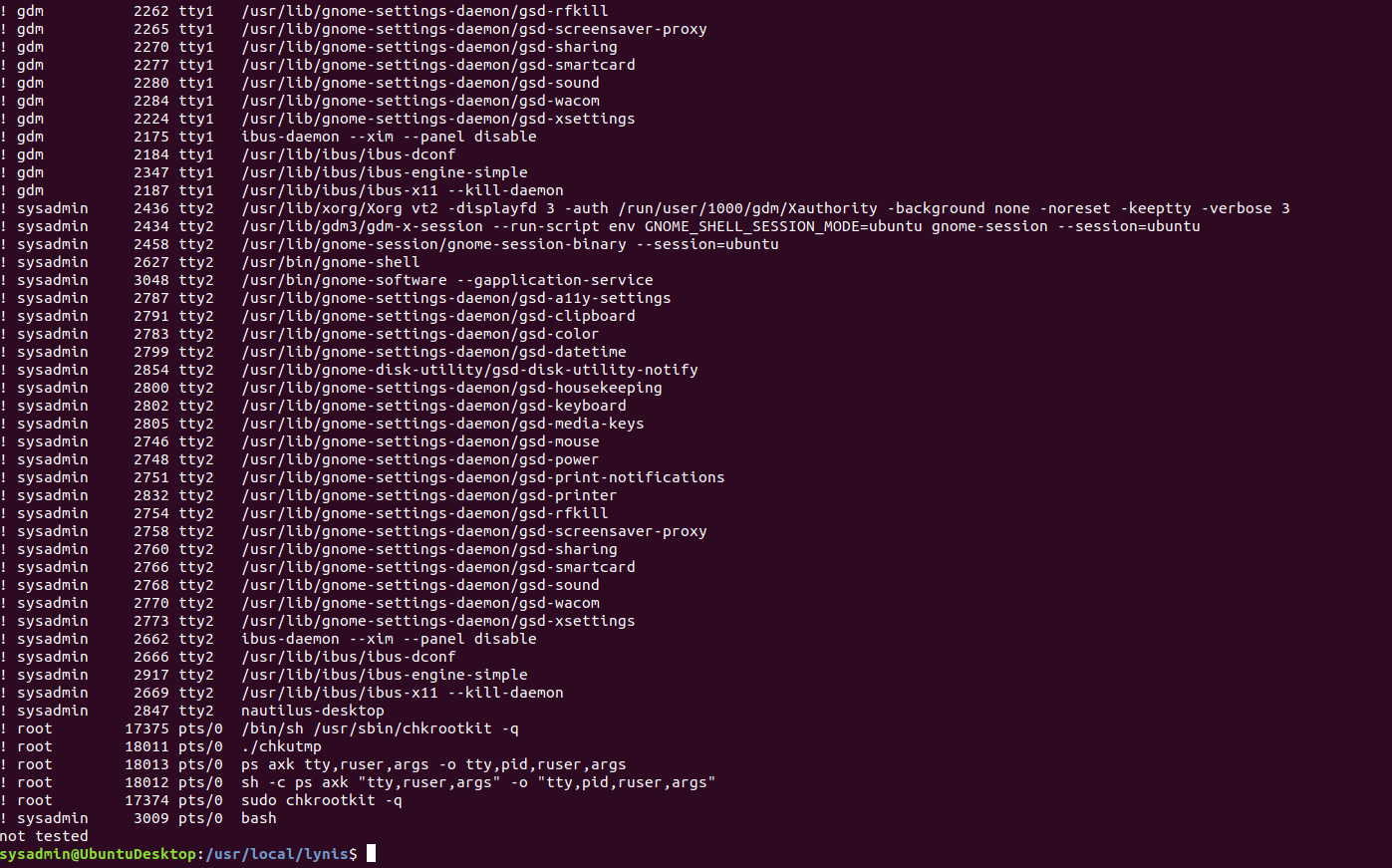
man chkrootkit

3. Command to run expert mode:

sudo chkrootkit -x

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

- Screenshot of end of sample output:



---

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.