Week 4 Homework: Linux Systems Administration

Scenario

In the previous class activities, you acted as system administrator in order to troubleshoot a malfunctioning server.

The senior administrator was quite pleased with your work. Now, they would like you to prepare another server to replace this server. You are tasked with completing the steps below to prepare a new server.

Lab Environment

Log into your local virtual machine. Use the following credentials:

- **Username: sysadmin**
- **Password: cybersecurity**

In order to get started with your tasks, you will need to open the Terminal within your Ubuntu VM. If you are unsure how to do it, within your Ubuntu VM, do the following:

- **Open the Linux terminal by pressing Ctrl+Alt+T for Windows users or Ctrl+Options+T for Mac users.**

- **Alternatively, press Windows+A or Command+A for Mac users, then type "Terminal" in the search bar and select the Terminal icon (not the Xfce Terminal icon).**

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:~$ ll /etc/shadow
-rw-r----- 1 root shadow 2990 Oct  9 15:22 /etc/shadow
```

- Command to set permissions (if needed):

```
sysadmin@UbuntuDesktop:~$ sudo chmod 600 /etc/shadow
```

-

```
sysadmin@UbuntuDesktop:~$ ll /etc/shadow
-rw------- 1 root shadow 2990 Oct  9 15:22 /etc/shadow
```

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

   - Command to inspect permissions:

```
sysadmin@UbuntuDesktop:~$ ll /etc/gshadow
-rw-r----- 1 root shadow 1081 Oct  9 15:21 /etc/gshadow
```

   - Command to set permissions (if needed):

```
sysadmin@UbuntuDesktop:~$ sudo chmod 600 /etc/gshadow
```

   -

```
sysadmin@UbuntuDesktop:~$ ll /etc/gshadow
-rw------- 1 root shadow 1081 Oct  9 15:21 /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:

```
sysadmin@UbuntuDesktop:~$ ll /etc/group
-rw-r--r-- 1 root root 1309 Oct  9 15:21 /etc/group
```

   - Command to set permissions (if needed):
     No changes as this is correct as is

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:~$ ll /etc/passwd
-rw-r--r-- 1 root root 3206 Oct  9 15:21 /etc/passwd
```

   - Command to set permissions (if needed):
     No changes as this is correct as is

Step 2: Create User Accounts

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

```
sysadmin@UbuntuDesktop:~$ ls /home
adam   amy    http        jack  joe   max    sam   student   tripwire     vagrant
admin  billy  instructor  jane  john  sally  sara  sysadmin  user.hashes
```

   - Command to add each user account (include all five users):

```
sysadmin@UbuntuDesktop:~$ sudo adduser joe
Adding user `joe' ...
Adding new group `joe' (1016) ...
Adding new user `joe' (1014) 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]
```

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

```
sysadmin@UbuntuDesktop:~$ grep sudo /etc/group
sudo:x:27:sysadmin,instructor,student,jack,admin
```

   - Command to add admin to the sudo group:
   - `sysadmin@UbuntuDesktop:~$ 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:

```
sysadmin@UbuntuDesktop:/home$ sudo addgroup engineers
Adding group `engineers' (GID 1020) ...
Done.
```

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

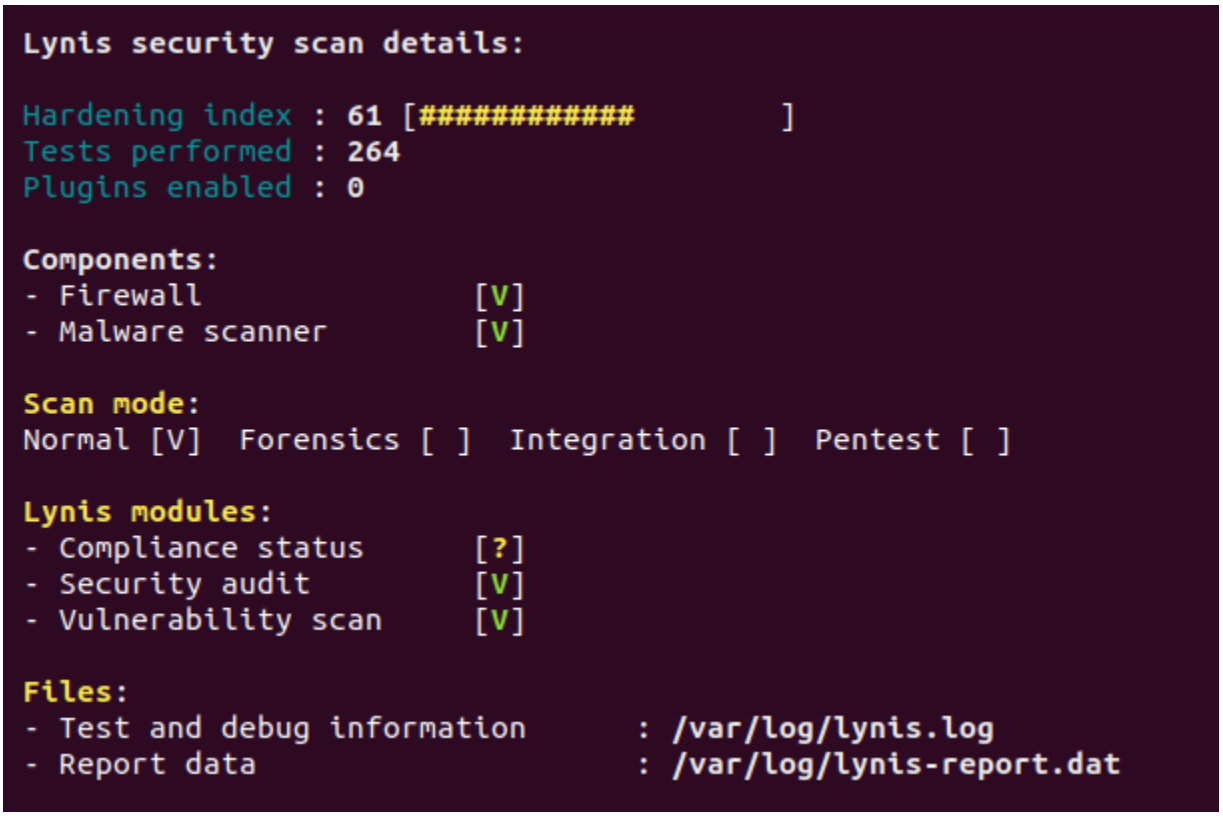
```
sysadmin@UbuntuDesktop:/home$ grep engineers /etc/group
engineers:x:1020:
sysadmin@UbuntuDesktop:/home$ sudo usermod -aG engineers sam
sysadmin@UbuntuDesktop:/home$ grep engineers /etc/group
engineers:x:1020:sam
sysadmin@UbuntuDesktop:/home$ sudo usermod -aG engineers joe
sysadmin@UbuntuDesktop:/home$ sudo usermod -aG engineers amy
sysadmin@UbuntuDesktop:/home$ sudo usermod -aG engineers sara
sysadmin@UbuntuDesktop:/home$ grep engineers /etc/group
engineers:x:1020:sam,joe,amy,sara
```

3. Create a shared folder for this group at /home/engineers.
    - Command to create the shared folder:
    -
```
sysadmin@UbuntuDesktop:/home$ sudo mkdir engineers
sysadmin@UbuntuDesktop:/home$ ls
adam   amy    engineers  instructor  jane  john  sally  sara     sysadmin  user.hashes
admin  billy  http       jack        joe   max   sam    student  tripwire  vagrant
```
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 chgrp -R engineers /home/engineers/
sysadmin@UbuntuDesktop:/home$ ll
total 88
drwxr-xr-x 21 root       root       4096 Oct 14 15:23 ./
drwxr-xr-x 31 root       root       4096 Oct  4 22:19 ../
drwxr-xr-x  8 adam       adam       4096 May 14 16:29 adam/
drwxr-xr-x  8 admin      admin      4096 Oct 14 15:08 admin/
drwxr-xr-x  8 amy        amy        4096 Oct 14 15:07 amy/
drwxr-xr-x  8 billy      billy      4096 May 14 16:29 billy/
drwxr-xr-x  2 root       engineers  4096 Oct 14 15:23 engineers/
drwxr-xr-x  8 http       http       4096 May 14 16:29 http/
drwxr-xr-x  9 instructor instructor 4096 May 14 16:36 instructor/
drwxr-xr-x  8 jack       jack       4096 May 14 16:29 jack/
drwxr-xr-x  9 jane       jane       4096 Oct 12 00:48 jane/
drwxr-xr-x  8 joe        joe        4096 Oct 14 15:06 joe/
drwxr-xr-x  8 john       john       4096 May 14 16:29 john/
drwxr-xr-x  9 max        max        4096 Oct  6 23:08 max/
drwxr-xr-x  8 sally      sally      4096 May 14 16:29 sally/
drwxr-xr-x  8 sam        sam        4096 Oct 14 15:05 sam/
drwxr-xr-x  8 sara       sara       4096 Oct 14 15:07 sara/
drwxr-xr-x  8 student    student    4096 May 14 16:24 student/
drwxr-xr-x 20 sysadmin   sysadmin   4096 Oct 14 15:00 sysadmin/
```

Step 4: Lynis Auditing

1. Command to install Lynis:
```
sysadmin@UbuntuDesktop:~$ apt-key adv --keyserver keyserver.ubuntu.com --recv-keys C80E383C3DE9F
082E01391A0366C67DE91CA5D5F
```
2. Command to see documentation and instructions:
```
sysadmin@UbuntuDesktop:~$ sudo lynis show commands

Commands:
lynis audit
lynis configure
lynis generate
lynis show
lynis update
lynis upload-only
```
3. Command to run an audit:
```
sysadmin@UbuntuDesktop:~$ sudo lynis audit system > report_lynis.txt
```

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

```
  -[ Lynis 3.0.6 Results ]-

  Warnings (2):
  ----------------------------
  ! Found one or more vulnerable packages. [PKGS-7392]
      https://cisofy.com/lynis/controls/PKGS-7392/

  ! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
      https://cisofy.com/lynis/controls/MAIL-8818/

  Suggestions (53):
  ----------------------------
  * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in sing
le user mode without password) [BOOT-5122]
      https://cisofy.com/lynis/controls/BOOT-5122/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file
[KRNL-5820]
      https://cisofy.com/lynis/controls/KRNL-5820/

  * Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new v
alues [AUTH-9229]
      https://cisofy.com/lynis/controls/AUTH-9229/

  * Configure password hashing rounds in /etc/login.defs [AUTH-9230]
      https://cisofy.com/lynis/controls/AUTH-9230/

  * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9
262]
      https://cisofy.com/lynis/controls/AUTH-9262/
```

Bonus

1. Command to install chkrootkit:

```
sysadmin@UbuntuDesktop:~$ apt list --installed | grep chkrootkit

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

chkrootkit/bionic-updates,now 0.52-1ubuntu0.1 amd64 [installed]
```

2. Command to see documentation and instructions:

```
chkrootkit/bionic-updates,now 0.52-1ubuntu0.1 amd64 [installed]
sysadmin@UbuntuDesktop:~$ sudo chkrootkit -h
[sudo] password for sysadmin:
Usage: /usr/sbin/chkrootkit [options] [test ...]
Options:
        -h               show this help and exit
        -V               show version information and exit
        -l               show available tests and exit
        -d               debug
        -q               quiet mode
        -x               expert mode
        -e               exclude known false positive files/dirs, quoted,
                         space separated, READ WARNING IN README
        -r dir           use dir as the root directory
        -p dir1:dir2:dirN path for the external commands used by chkrootkit
        -n               skip NFS mounted dirs
```

3. Command to run expert mode:

```
sysadmin@UbuntuDesktop:~$ sudo chkrootkit -x > /home/sysadmin/report-chkrootkit.txt
```

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

```
sysadmin@UbuntuDesktop:~$ sudo chkrootkit -x > report-chkrootkit.txt
/usr/sbin/chkrootkit: 608: /usr/sbin/chkrootkit: exportmode_output: not found
/usr/sbin/chkrootkit: 609: /usr/sbin/chkrootkit: exportmode_output: not found
```

```
sysadmin@UbuntuDesktop:~$ head report_chkrootkit.tx
ROOTDIR is `/'
not found
###
### Output of: /usr/bin/strings -a /usr/bin/basenam
###
/lib64/ld-linux-x86-64.so.2
libc.so.6
fflush
__printf_chk
setlocale
```

Did not seem to work, but an attempt was made. Oh well!