Cybersecurity

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.

    a. Command to inspect permissions:

```
After navigating to the /etc, you need to use sudo ls -l shadow. You need
sudo to escalate your privileges for 1 command.
```

    b. Command to set permissions (if needed):

```
There are a few, but I decided to use the octal notation method. You would
use sudo chmod (600), or whatever permissions you want to set.
```

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

    a. Command to inspect permissions:

```
You would use ls -l gshadow.
```

    b. Command to set permissions (if needed):

```
Again, use sudo chmod (600), that way, only the owner has read and write
access to the file.
```

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

a. Command to inspect permissions:

```
The command is ls -l group. Unlike the other two files (shadow and gshadow)
the file group has the permissions specified in the question.
```

b. Command to set permissions (if needed):

```
Here you would use sudo chmod (644).
```

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

   a. Command to inspect permissions:

```
Command is ls -l passwd.
```

   b. Command to set permissions (if needed):

```
The permissions are as stated in the question (644), but you could use sudo
chmod if you wanted to change it.
```

Step 2: Create User Accounts

1. Add user accounts for `sam`, `joe`, `amy`, `sara`, and `admin` with the `useradd` command.

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

```
The system prompted me to add them separately. But I used adduser sam, then
adduser joe etc.
```

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

   a. Command to add `admin` to the sudo group:

```
Command is usermod -aG sudo admin. Must be in root for this to work.
```

Step 3: Create User Group and Collaborative Folder

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

```
Command is addgroup engineers.
```

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

```
Again, I could only add each user separately. But it was adduser sam
engineers. I proceeded to add them all this way.
```

3. Create a shared folder for this group at `/home/engineers`.
    a. Command to create the shared folder:

```
While in /home it's mkdir engineers. Note, since I did this in root the id
gives a uid,gid and groups =0.
```

4. Change ownership on the new engineers' shared folder to the `engineers` group.
    a. Command to change ownership of engineers' shared folder to `engineers` group:

```
To change ownership of a folder it is chown engineers:engineers
```

Step 4: Lynis Auditing

1. Command to install Lynis:

```
First I had to run: sudo apt update. Once system was updated, used wget -O
- https://packages.cisofy.com/keys/cisofy-software-public.key |
sudo apt-key add -. After this, used echo "deb
https://packages.cisofy.com/community/lynis/deb/ stable main" |
sudo tee /etc/apt/sources.list.d/cisofy-lynis.list

After this, I updated the system again with sudo apt update.

Finally, I could run sudo apt install Lynis.
```

```
Note*: Normally you could just run sudo apt Lynis, but my VM didn't
have this package installed, so I had to go through the above
steps.

Source
https://linoxide.com/how-to-install-and-run-lynis-on-ubuntu-linux/
```

2. Command to view documentation and instructions:

```
  1) Enter lynis show commands
  2) Enter lynis show settings
  3) There are various other commands you could run after the "lynis show
     commands" that can show you more detail about the package

https://linoxide.com/how-to-install-and-run-lynis-on-ubuntu-linux/
```

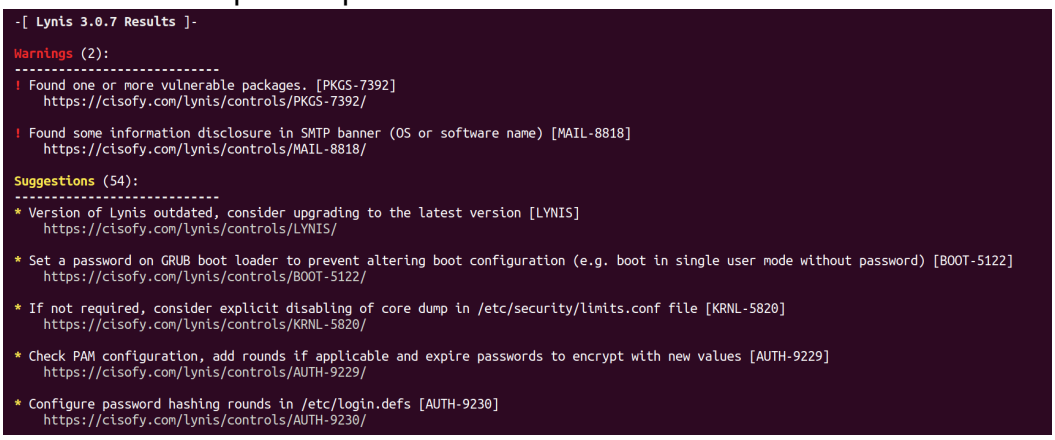
3. Command to run an audit:

```
If not in root, use sudo lynis audit system

https://linoxide.com/how-to-install-and-run-lynis-on-ubuntu-linux/
```

4. Provide a report from the Lynis output with recommendations for hardening the system.

    a. Screenshot of report output:



```
-[ Lynis 3.0.7 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 (54):
----------------------------
* Version of Lynis outdated, consider upgrading to the latest version [LYNIS]
    https://cisofy.com/lynis/controls/LYNIS/

* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single 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 values [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/
```

The report is extensive, but the main 2 warnings include: "one or more vulnerable packages" and information disclosure in SMTP banner.

See below for security scan details:

```
Lynis security scan details:

Hardening index : 61 [############        ]
Tests performed : 267
Plugins enabled : 0

Components:
- Firewall               [V]
- Malware scanner        [V]

Scan mode:
Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

Lynis modules:
- Compliance status      [?]
- Security audit         [V]
- Vulnerability scan     [V]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat
```

Bonus

1. Command to install chkrootkit:

```
**While in root** apt install -y chkrootkit

Source
https://lindevs.com/install-chkrootkit-on-ubuntu/
```

2. Command to view documentation and instructions:

```
Again, I'm root: chkrootkit. Otherwise, add sudo
```

3. Command to run expert mode:

```
./chkrootkit -x. Quite verbose. This mode allows you to find clues that
trojans may be in your programs. Very clever considering the only known
vulnerabilities pertaining to chkrootkit is with regards to trojans.

Source
http://chkrootkit.org/faq/
```

4. Provide a report from the chrootkit output with recommendations for hardening the system.

    a. Screenshot of end of sample output:

I ran chkrootkit -q, which was the closest thing I could find to recommendations from the tool. The output is below, and it says that vagrant could possibly be malicious.

```
root@UbuntuDesktop:/home# chkrootkit -q

/usr/lib/debug/.build-id /usr/lib/python2.7/dist-packages/ansible/galaxy/data/container/files/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/d
ata/container/.travis.yml /usr/lib/python2.7/dist-packages/ansible/galaxy/data/container/templates/.git_keep /usr/lib/python2.7/dist-packages/ansible/gal
axy/data/default/collection/roles/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/collection/docs/.git_keep /usr/lib/python2.7/dis
t-packages/ansible/galaxy/data/default/role/files/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/default/role/.travis.yml /usr/lib/python
2.7/dist-packages/ansible/galaxy/data/default/role/templates/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/apb/files/.git_keep /usr/lib/
python2.7/dist-packages/ansible/galaxy/data/apb/.travis.yml /usr/lib/python2.7/dist-packages/ansible/galaxy/data/apb/templates/.git_keep /usr/lib/python2
.7/dist-packages/ansible/galaxy/data/network/files/.git_keep /usr/lib/python2.7/dist-packages/ansible/galaxy/data/network/.travis.yml /usr/lib/python2.7/
dist-packages/ansible/galaxy/data/network/templates/.git_keep /lib/modules/5.0.0-23-generic/vdso/.build-id
/usr/lib/debug/.build-id /lib/modules/5.0.0-23-generic/vdso/.build-id
not tested
INFECTED: Possible Malicious Linux.Xor.DDoS installed
/tmp/vagrant-shell
/tmp/response.varfile
/tmp/str.sh
/tmp/burpsuite_community_linux_v2022_1_1.sh
enp0s3: PACKET SNIFFER(/sbin/dhclient[1043])
1 deletion(s) between Sun Oct  2 10:32:41 2022 and Sun Oct  2 10:34:38 2022
 The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          2084 tty1   /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -listen 4 -listen 5 -displayfd 6
```