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:

$ ls -al /etc/shadow

-rw-r—r— 1 root shadow 3165 oct 18 01:28 /etc/shadow

- Command to set permissions (if needed):

$ sudo chmod 600 /etc/shadow (Ask root password)

$ ls -al /etc/shadow

-rw------- 1 root shadow 3165 oct 18 01:28 /etc/shadow

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

- Command to inspect permissions:

$ ls -al /etc/gshadow

-rw-r—r— 1 root shadow 1129 Oct 17 22:48 /etc/gshadow

- Command to set permissions (if needed):

$ sudo chmod 600 /etc/gshadow

--rw------- 1 root shadow 1129 Oct 17 22:48 /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:

$ ls -al /etc/group

-rw-rw-r—1 root root 1372 Oct 17 22:48 /etc/group

- Command to set permissions (if needed):

$ sudo chmod 644 /etc/group

-rw-r—r—1 root root 1372 Oct 17 22:48 /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:

$ ls -al /etc/passwd

-rw-rw-r—1 root root 3384 Oct 18 01:28 /etc/passwd

- Command to set permissions (if needed):

$sudo chmod 644 /etc/passwd

-rw-r—r—1 root root 3384 Oct 18 01:28 /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):

$ sudo adduser sam (Ask Unix password)

$ sudo adduser joe

$ sudo adduser amy

$ sudo adduser sara

$ sudo adduser admin

$ tail /etc/passwd (verify user in system)

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

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

$ groups admin

admin : admin

$ sudo -lU admin

User admin is not allowed to run sudo on UbuntuDesktop.

$ sudo usermod -aG sudo admin

$ groups admin

Admin : admin sudo

#$ sudo nano /etc/sudoers

#Edit & add: admin All=(ALL: ALL) All

#$ sudo -lU admin

#(ALL : ALL) ALL

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

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

- Command to add group:

$ sudo addgroup engineers

Verify: $ tail /etc/group

Engineers:x:1023:

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

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

$ sudo usermod -aG engineers sam

$ sudo usermod -aG engineers joe

$ sudo usermod -aG engineers amy

$ sudo usermod -aG engineers sara

Verify: groups <username> ( like - sara: sara engineers)

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

- Command to create the shared folder:

Verify users & groups: $tail /etc/group (engineers:x:1023:sam,joe,amy,sara)

$ sudo mkdir -p /home/engineers/

Change the permission for share folder “engineers”

$ sudo chmod -R 774 /home/engineers/

Change group ownership to engineers

$ sudo chgrp -R engineers /home/engineers

Now Sara, Amy, Joe and Sam can share a folder “engineer” only. Other can read it only.

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:

Right now, engineers group and root have permission to changes

drwxrwxr-- 2 root engineers 4096 Oct 20 18:48 engineers

$ sudo chgrp -R engineers /home/engineers

($sudo chown :engineers /home/engineers)

### Step 4: Lynis Auditing

1. Command to install Lynis:

It is already installed in system (for installation: $ sudo apt-get install lynis)

$ which lynis

/usr/sbin/lynis

2. Command to see documentation and instructions:

$sudo lynis show help show

$sudo lynis show help audit

$cat /etc/lynis/default.pdf

$sudo lynis audit system update info

Ver. 2.6.2 outdated latest ver. 301

3. Command to run an audit:

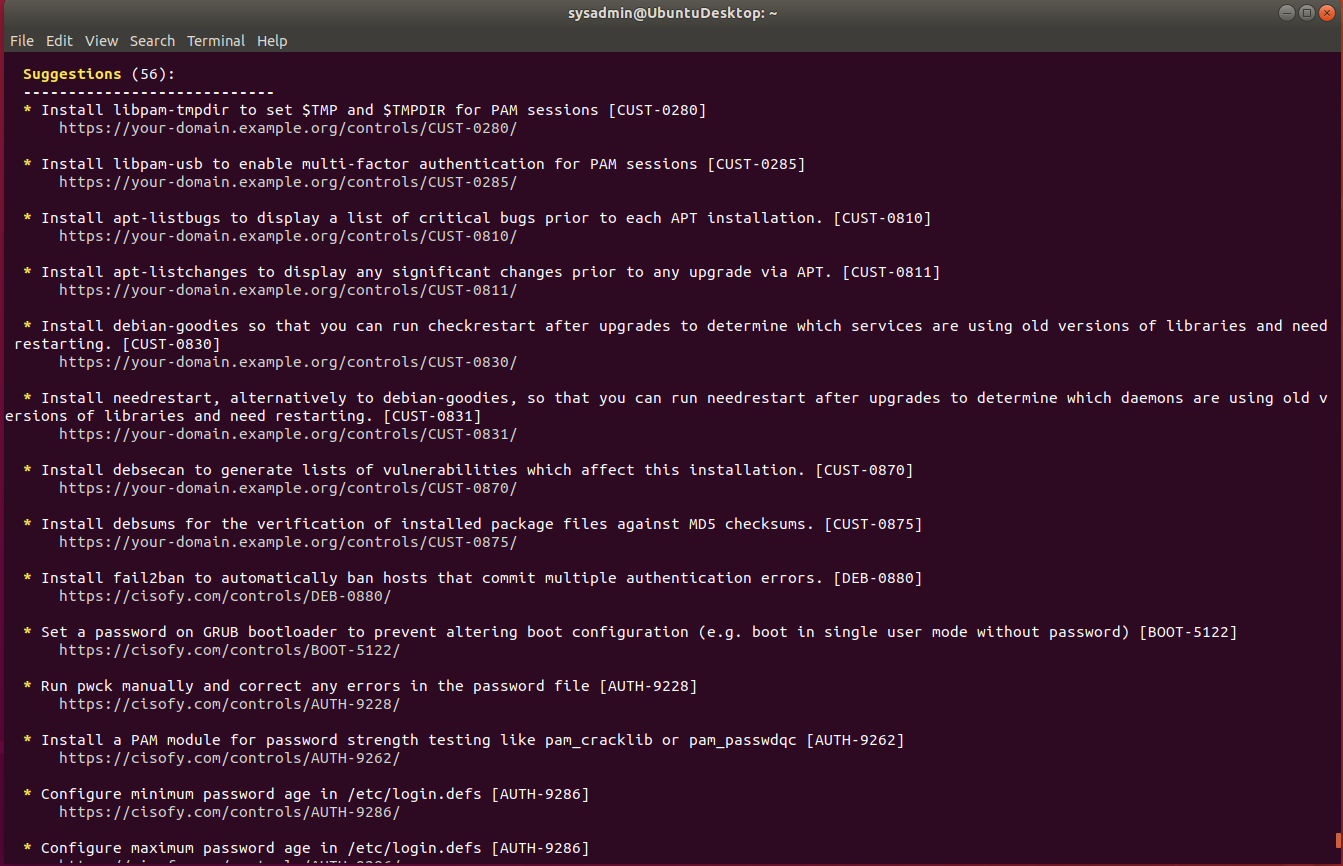
$sudo lynis audit system

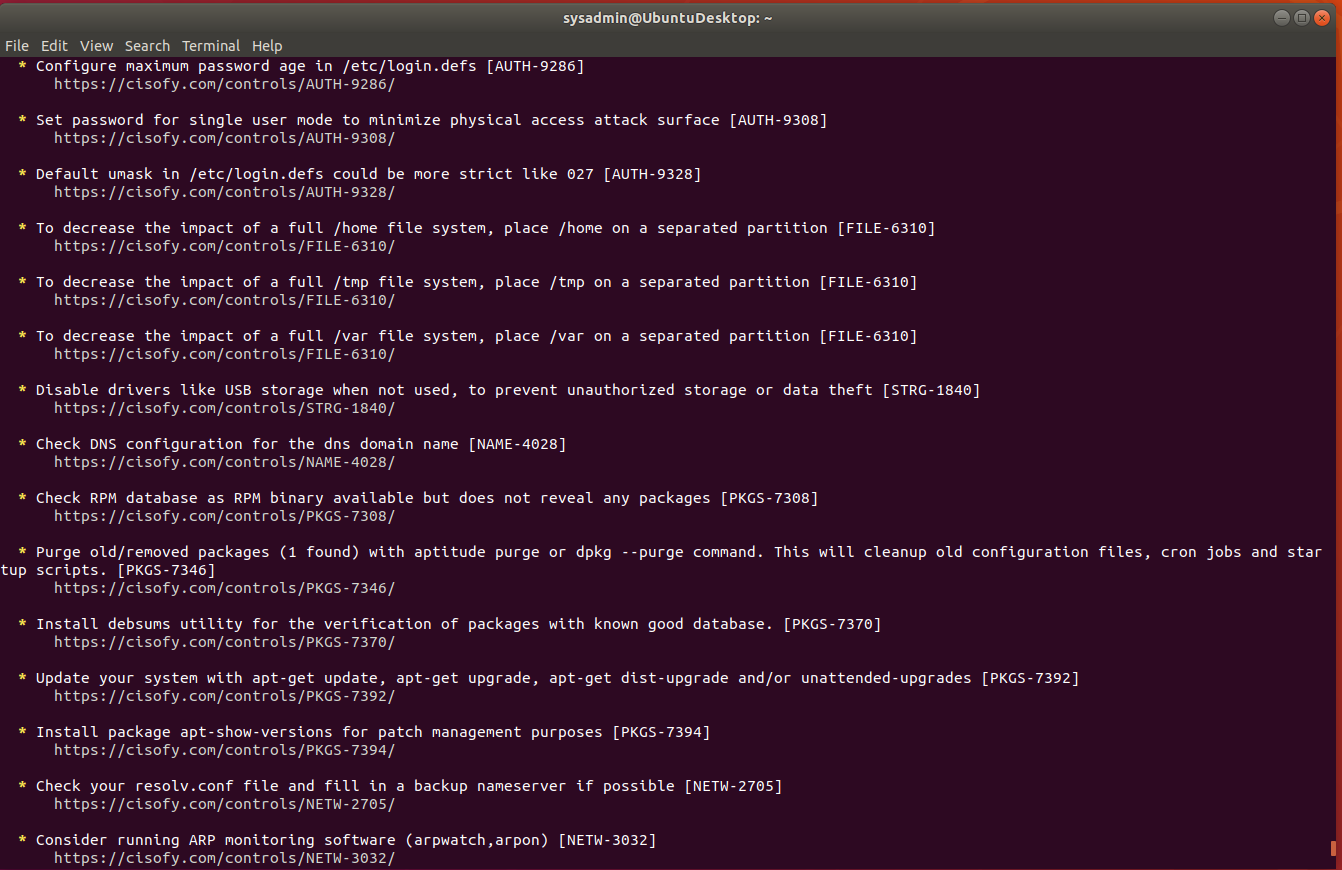
It audits the local pc.

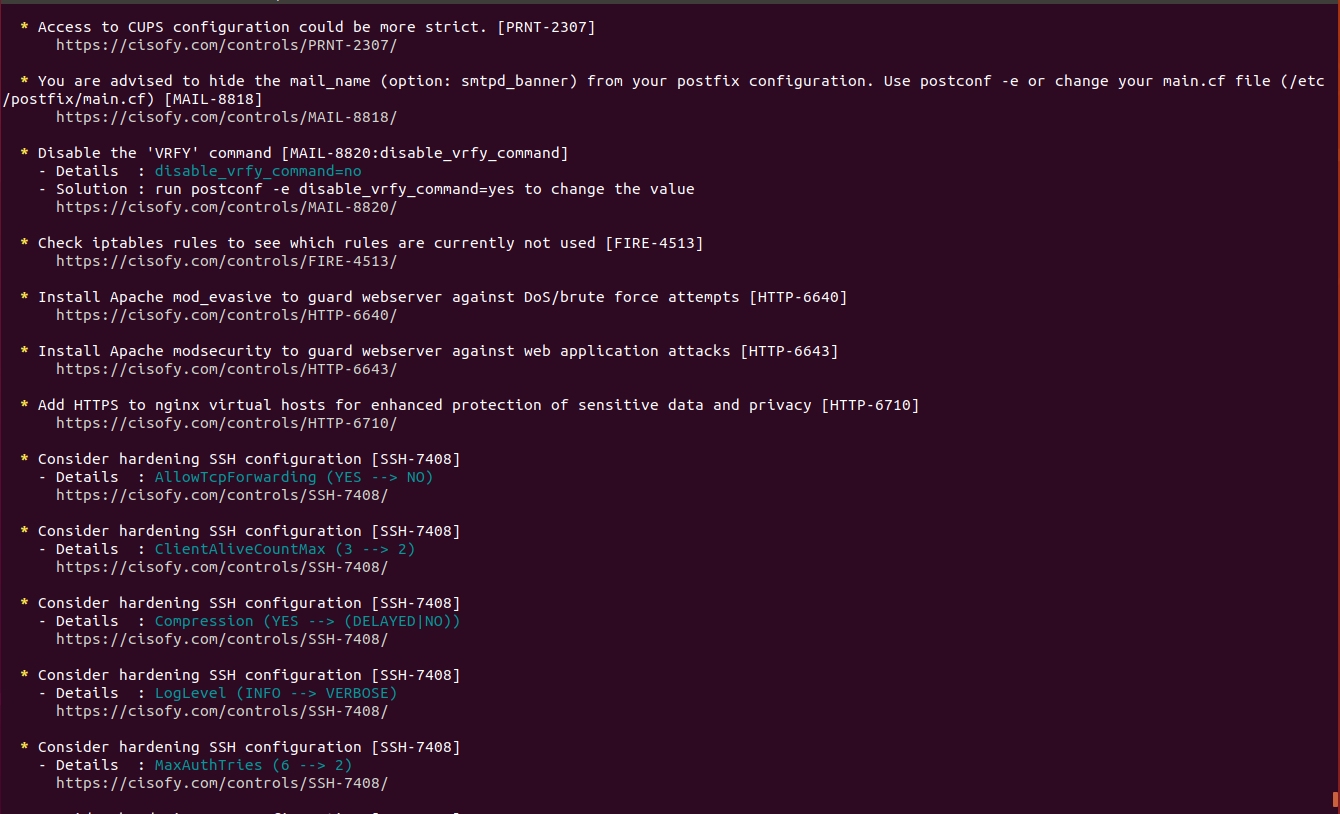
4. Provide a report from the Lynis output on what can be done to harden the system.

- Screenshot of report output:

I created the full report to run the lynis audit system command. Attached the linux file “lynis\_report” too.







### Bonus

1. Command to install chkrootkit:

Sudo apt-get install chkrootkit

Verify:

Which chkrootkit

/usr/sbin/chkrootkit

1. Command to see documentation and instructions:

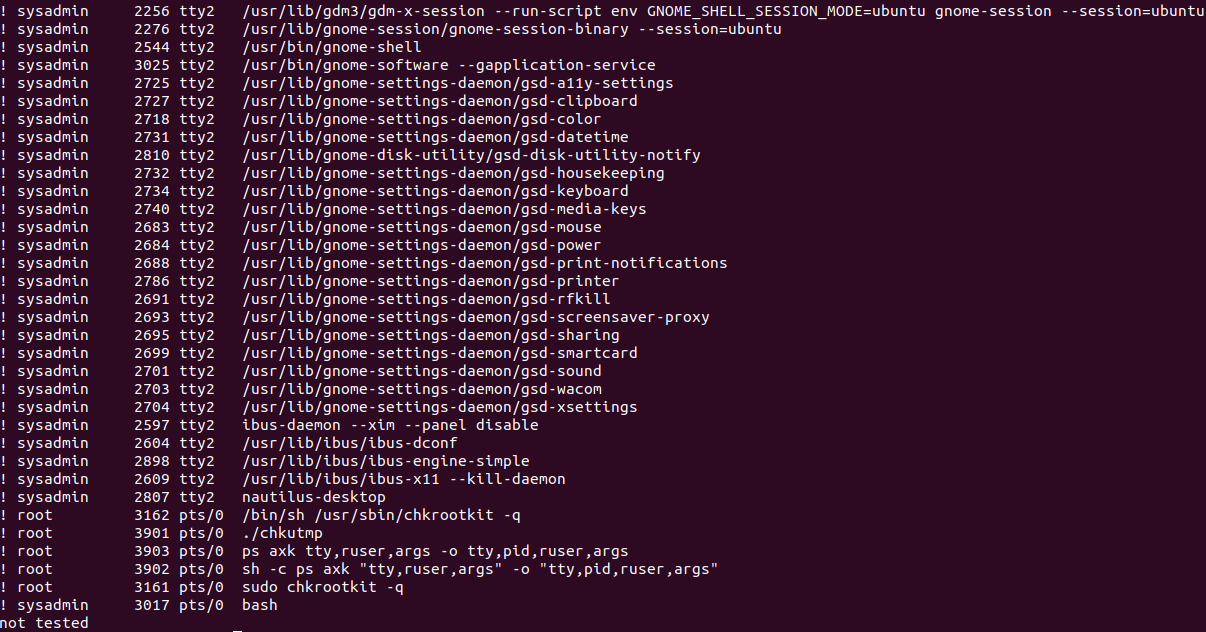
$sudo chkrootkit -h

1. Command to run expert mode:

$sudo chkkroot -x

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

- Screenshot of end of sample output:



---

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