Activity File: Linux Landmarks

For the activities over the next few days, you will act as a **Junior Linux Systems Administrator** at *Corp X*. A senior administrator has asked you to audit a malfunctioning Linux server. As such, all of the activities over the next week will take place in the same lab environment.

- You will complete several tasks in the next week of class activities and homeworks related to **Linux auditing and hardening**. Everything you do will be second nature for many Linux administrators, and are great skills to talk about during job interviews.

- The first step for troubleshooting any computer issue is gathering information. In this activity, the senior administrator has sent you a list of information to gather about the target system. You will use this information for further analysis.

- You will start with a basic audit of system files, exploring some of the most important locations in the file system to identify evidence of suspicious activity.

Use the following credentials to log into the lab environment:

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

Be sure to ask your instructors and classmates for help if you get stuck.

Instructions:

To set up this activity, run the following command: `sudo bash /home/instructor/Documents/setup_scripts/instructor/landmarks_review.sh`

- Ignore any `rm: cannot remove` errors that appear.

Here is the audit checklist provided by your senior administrator:

1. Create a `research` directory in your home folder to place notes of your findings.

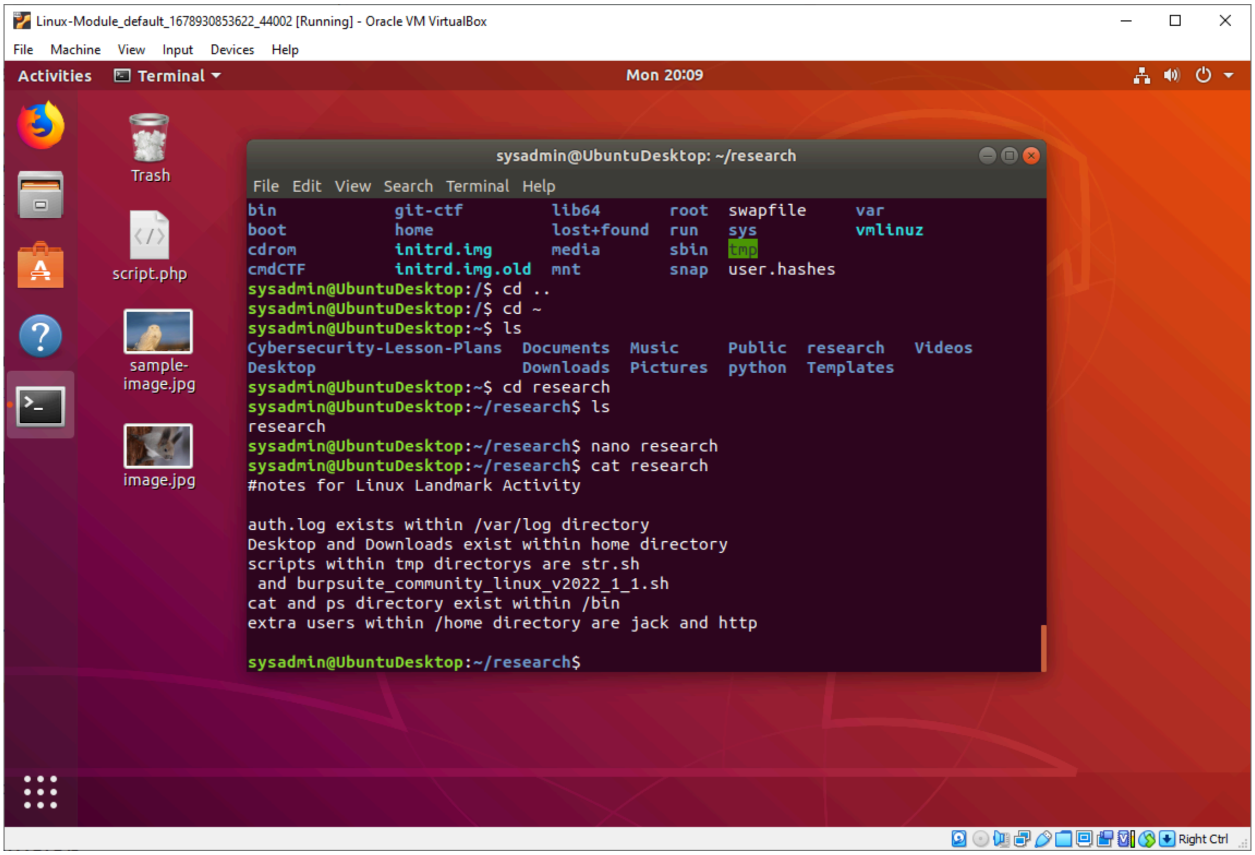
2. Access the /var/log directory and check that the `auth.log` exists. You need this to check for suspicious logins.

3. Access your personal home directory and check if you have a `Desktop` and `Downloads` directory.

4. Access the binary directory and check if you can find `cat` and `ps` binary files.

5. Check if there are any scripts in temporary directories, as those may be suspicious.

6. Check that the only users with accounts in the `/home` directory are `adam`, `billy`, `instructor`, `jane`, `john max`, `sally`, `student`, `sysadmin` and `vagrant`. There should not be additional directories. Note any other users that you find.


Linux-Module_default_1678930853622_44002 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mon 20:09
Trash
script.php
sample-image.jpg
image.jpg
sysadmin@UbuntuDesktop: ~/research
File Edit View Search Terminal Help
Right Ctrl

```
bin                git-ctf          lib64        root   swapfile     var
boot               home             lost+found   run    sys          vmlinuz
cdrom              initrd.img       media        sbin   tmp
cmdCTF             initrd.img.old   mnt          snap   user.hashes
sysadmin@UbuntuDesktop:/$ cd ..
sysadmin@UbuntuDesktop:/$ cd ~
sysadmin@UbuntuDesktop:~$ ls
Cybersecurity-Lesson-Plans  Documents  Music     Public  research   Videos
Desktop                     Downloads  Pictures  python  Templates
sysadmin@UbuntuDesktop:~$ cd research
sysadmin@UbuntuDesktop:~/research$ ls
research
sysadmin@UbuntuDesktop:~/research$ nano research
sysadmin@UbuntuDesktop:~/research$ cat research
#notes for Linux Landmark Activity

auth.log exists within /var/log directory
Desktop and Downloads exist within home directory
scripts within tmp directorys are str.sh
 and burpsuite_community_linux_v2022_1_1.sh
cat and ps directory exist within /bin
extra users within /home directory are jack and http

sysadmin@UbuntuDesktop:~/research$
```