

## Week 4 Task T4.1PA

Answer the below questions

1. Question 1:

- a. What is a Docker? How it is different from a Virtual Machine?
  - With the help of Docker, programs and their dependencies can be packaged into lightweight, portable containers that share that operating system of the host system. Containers are resource-efficient and start up rapidly. In contrast, virtual machines (VMs) are more resource-intensive, heavier, and require a longer startup time because they come with an entire operating system installed. Because they come with an entire operating system installed. Because each virtual machine runs independently with its own operating system, they offer strong isolation. Docker containers ensure constant performance by being easier to migrate between environments.
- b. Include a screenshot confirming that you have managed to create the docker image, build it and get an “alice” shell (by following the readme file in Access Control folder).

```
(kali@kali)-[~/Downloads/LAB2_access_control]
$ sudo docker build -t labsec2 .
[+] Building 185.7s (24/24) FINISHED                                docker:default
=> [internal] load build definition from Dockerfile                0.0s
=> => transferring dockerfile: 2.51kB                             0.0s
=> [internal] load metadata for docker.io/library/ubuntu:18.04    6.4s
=> [internal] load .dockerignore                                  0.0s
=> => transferring context: 2B                                       0.0s
=> [ 1/19] FROM docker.io/library/ubuntu:18.04@sha256:152dc042452c496007f07ca9127571cb9c29697f42acbfad72324 72.4s
=> => resolve docker.io/library/ubuntu:18.04@sha256:152dc042452c496007f07ca9127571cb9c29697f42acbfad72324b2b 0.0s
=> => sha256:152dc042452c496007f07ca9127571cb9c29697f42acbfad72324b2b2e43c98 1.33kB / 1.33kB      0.0s
=> => sha256:dca176c9663a7ba4c1f0e710986f5a25e672842963d95b960191e2d9f7185ebe 424B / 424B      0.0s
=> => sha256:f9a80a55f492e823bf5d51f1bd5f87ea3eed1cb31788686aa99a2fb61a27af6a 2.30kB / 2.30kB      0.0s
=> => sha256:7c457f213c7634afb95a0fb2410a74b7b5bc0ba527033362c240c7a11bef4331 25.69MB / 25.69MB 70.7s
=> => extracting sha256:7c457f213c7634afb95a0fb2410a74b7b5bc0ba527033362c240c7a11bef4331 1.5s
=> [internal] load build context                                  0.0s
=> => transferring context: 12.72kB                                0.0s
=> [ 2/19] RUN apt update                                         94.7s
=> [ 3/19] COPY etc/skel/bashrc /etc/skel/.bashrc               0.1s
=> [ 4/19] RUN echo "root:root" | chpasswd                       0.4s
=> [ 5/19] RUN apt install -y iputils-ping libc-bin acl          5.7s
=> [ 6/19] RUN adduser --disabled-password alice; adduser --disab 0.8s
=> [ 7/19] RUN echo "bob:bob" | chpasswd; echo "carol:carol" | c 0.4s
=> [ 8/19] RUN addgroup student                                  0.4s
=> [ 9/19] RUN usermod -a -G student alice                       0.4s
=> [10/19] RUN usermod -a -G student bob                         0.4s
=> [11/19] RUN echo "This file is readable by student group" > / 0.4s
=> [12/19] RUN echo "dsaffs" > /tmp/file1; echo "dsaf33" > /tmp/ 0.4s
=> [13/19] RUN chmod 171 /tmp/file1; chmod 262 /tmp/file2; chmo 0.4s
=> [14/19] RUN chgrp student /tmp/file5; chgrp student /tmp/file 0.4s
=> [15/19] COPY hello /home/alice/alice_shell                   0.1s
=> [16/19] RUN chown alice:alice /home/alice/alice_shell; chmo 0.3s
=> [17/19] RUN echo "This file should be readable/writable by ca 0.4s
=> [18/19] COPY acl.conf /etc/init.d/                           0.1s
=> [19/19] RUN chmod 755 /etc/init.d/acl.conf                   0.3s
=> exporting to image                                             0.6s
=> => exporting layers                                             0.6s
=> => writing image sha256:4a06fbfe6e13c5030cc3cdf8a2a9e245aa93dfbf6c73733a4c6a1e24eb698ed6 0.0s
=> => naming to docker.io/library/labsec2                        0.0s

(kali@kali)-[~/Downloads/LAB2_access_control]
$ sudo docker run -it labsec2 bash
alice:~$
```

## 2. Question 2:

- a. What does the “sudo” or “su” command do?
  - While the `su` command requires the password of the current user to convert to a different user account typically the root user the `sudo` command enables you run specified commands with superuser (admin) capabilities using your own password. `su` grants complete access to another user’s environment, but `sudo` is more secure and logs every command.
- b. Include the screenshots of all commands that you have used to complete the Challenge 1. List the password that you obtained in Challenge 1.

```

alice:~$ cd /tmp
alice:/tmp$ ls
file1  file11  file13  file15  file17  file19  file20
file10  file12  file14  file16  file18  file2    file3
alice:/tmp$ ls -l
total 112
-rwxrwx--x+ 1 root root    7 Jun  3 10:08 file1
--wxrw----- 1 root root    7 Jun  3 10:08 file10
-r--rwx-w-+ 1 root root    7 Jun  3 10:08 file11
-r-xr-----wx 1 root root    7 Jun  3 10:08 file12
-rw--wx-----+ 1 root student 7 Jun  3 10:08 file13
-rwx-wx-w-+ 1 root student 7 Jun  3 10:08 file14
--x--x----- 1 root student 7 Jun  3 10:08 file15
--w----- 1 root student 7 Jun  3 10:08 file16
--wxrwx-w- 1 root root    7 Jun  3 10:08 file17
-r--rw--wx 1 root root    7 Jun  3 10:08 file18
-r-xr-x----- 1 root root    7 Jun  3 10:08 file19
--w-rw--w- 1 root root    7 Jun  3 10:08 file2
-rw-r-----w- 1 root root    7 Jun  3 10:08 file20
--wxrwx-wx+ 1 root root    7 Jun  3 10:08 file3
-r--r----- 1 root root    7 Jun  3 10:08 file4
-r-xrwx--x 1 root student 7 Jun  3 10:08 file5
-rw--w--w-+ 1 root student 7 Jun  3 10:08 file6
-rwx-wx-wx+ 1 root student 7 Jun  3 10:08 file7
--xrw--w-+ 1 root student 7 Jun  3 10:08 file8
--w-rwx-wx 1 root root    7 Jun  3 10:08 file9
alice:/tmp$ cat file5
4411c3
alice:/tmp$ █

```

## 3. Question 3

- a. What does the command “ls -l” do?
  - The command is `ls -l` provides a full list of all the files and folders in the current directory, including information on their size, modification date, owner, group, permissions, and filename.
- b. What is the command to set `-rwxr-xr-x` permissions to myfile? (Make sure to include the exact command including any spaces).
  - In Unix/Linux, the `chmod` command is used to modify a file or directory's permissions. It adjusts permission levels for the owner, group, and others, changing who may read, write, or execute the file.
- c. What is the command to set `-rwxr-xr-x` permissions to myfile? (Make sure to include the exact command including any spaces).
  - `chmod 755 myfile`

## 4. Question 4

- a. Look for a file in /tmp/ that is accessible by carol. It contains the password. Include the screenshots of all commands that you have used to complete the Challenge 3. List the password that you obtained in Challenge 3.

```

alice:/tmp$ su carol
Password:
carol:/tmp$ ls
file1  file12  file15  file18  file20  file5  file8
file10  file13  file16  file19  file3  file6  file9
file11  file14  file17  file2  file4  file7
carol:/tmp$ ls -l
total 112
-rwx--x+ 1 root root 7 Jun 3 10:08 file1
--wxrw--- 1 root root 7 Jun 3 10:08 file10
-r--rwx-w-+ 1 root root 7 Jun 3 10:08 file11
-r-xr---wx 1 root root 7 Jun 3 10:08 file12
-rw--wx---+ 1 root student 7 Jun 3 10:08 file13
-rwx-wx-w-+ 1 root student 7 Jun 3 10:08 file14
--x--x--- 1 root student 7 Jun 3 10:08 file15
--w----- 1 root student 7 Jun 3 10:08 file16
--wxrwx-w- 1 root root 7 Jun 3 10:08 file17
-r--rw--wx 1 root root 7 Jun 3 10:08 file18
-r-xr-x--- 1 root root 7 Jun 3 10:08 file19
--w-rw--w- 1 root root 7 Jun 3 10:08 file2
-rw-r---w- 1 root root 7 Jun 3 10:08 file20
--wxrwx-wx+ 1 root root 7 Jun 3 10:08 file3
-r--r----- 1 root root 7 Jun 3 10:08 file4
-r-xrwx--x 1 root student 7 Jun 3 10:08 file5
-rw--w--w-+ 1 root student 7 Jun 3 10:08 file6
-rwx-wx-wx+ 1 root student 7 Jun 3 10:08 file7
--xrw--w-+ 1 root student 7 Jun 3 10:08 file8
--w-rwx-wx 1 root root 7 Jun 3 10:08 file9
carol:/tmp$ getfacl file8
# file: file8
# owner: root
# group: student
user::--x
user:carol:rw-
group::--
mask::rw-
other::-w-

carol:/tmp$ cat file8
ac1lol
carol:/tmp$ █

```

## 5. Question 5

- a. In a paragraph (up to 200 words) summarize what you understood about SUID permission and capabilities as covered in Challenge 4. This need so be in your own words. (i.e., no direct quotes).
  - Programs that have SUID (Set User ID) permission can operate with their owner's privileges instead of the person carrying it out. This is required for some system utilities that demand elevated privileges. An executable belonging to user "alice" with SUID set, for instance can be used by user "bob" and continue to function with "Alice" benefits. To accomplish this, use the command "chmod 4755 filename" to set the SUID bit. This modifies the file's permissions such that an "s" appears where the owner's executable bit should be. However, because of certain weaknesses, SUID can dangerous, especially when applied to root. Privilege drop is a strategy used to reduce this, Privilege drop is strategy used to reduce this, where the software runs with elevated privileges for only the essential actions before dropping them. Furthermore, Linux Capabilities provide a more precise permission system that lets programs be given particular rights without giving them complete, the "cap\_net\_raw\_" capability can be provided to allow raw network activities instead to setting SUID root for the "ping" command, restricting the scope of elevated privileges and improving security

## 6. Question 6

- a. Is the following statement True or False? `Sticky bit is a special permission that can be assigned to a file'.
  - False
- b. Is the following statement True or False? `An executable file has SUID permission set. When the file is executed on the system, the user who runs the file becomes the file's temporary owner'.
  - False
- c. You just created a new script file named myapp.sh. However, when you try to run it from the command prompt, the bash shell generates an error that says -bash: ./myapp.sh: Permission denied. Which command will fix this problem?
  - `chmod +x myapp.sh`
- d. A file named sit182.txt has a mode of rw-r--r--. If arash is not the file's owner and is not a member of the group that owns this file, what can he do with it?
  - He can read the file but cannot write to it or execute it. Since others have only permission to read
- e. A file named Google Class Room.ppt has a mode of rw-r--r--. If chang-tsun is the file's owner, what can he do with it?
  - He can read and write the file

## 7. Question 7

- a. If you wanted to have a data file that you could read or write, but don't want anyone else to see, the permission would be.....(answer using the 9-bit e.g. -r--r--r--)
  - -rw-----
- b. If the file is owned by the user, the.....permission determine the access. (fill the blank either with OWNER/GROUP/OTHER)
  - OWNER
- c. If the group of the file is the same as the user's group, the..... Determine the access. (fill the blank either with OWNER/GROUP/OTHER)
  - Group
- d. If the user is not the file owner, and is not in the group, then the ..... is used. (fill the blank either with OWNER/GROUP/OTHER)
  - Other

## 8. Question 8

a. Reflection point – What did you learn that was new to you? How did you manage to learn about UNIX permissions to complete this task? Did you primarily use the Help Video and textbook provided or used your own resources?

- I gained knowledge about the complexities of UNIX file permission – including the application of unique permission like SUID, SGID, and the sticky bit – by finishing this work. I was unfamiliar with these ideas, so seeing how they were used in various contexts strengthened my understanding of Unix/Linux access control techniques. I mostly used my resources, practice in the terminal, and the challenges to learn about UNIX permission. Understanding how to utilize permissions in practical situations was made easier by the examples' practical and visual presentation of topics. I then used what I had learned, practiced using the terminal, and did more research by consulting the Linux handbook. This method guaranteed a thorough comprehension and the capacity to do the associated responsibilities efficiently. Together, these resources improved my educational experience by increasing the accessibility and usefulness of the process of comprehending and utilizing Unix permissions.