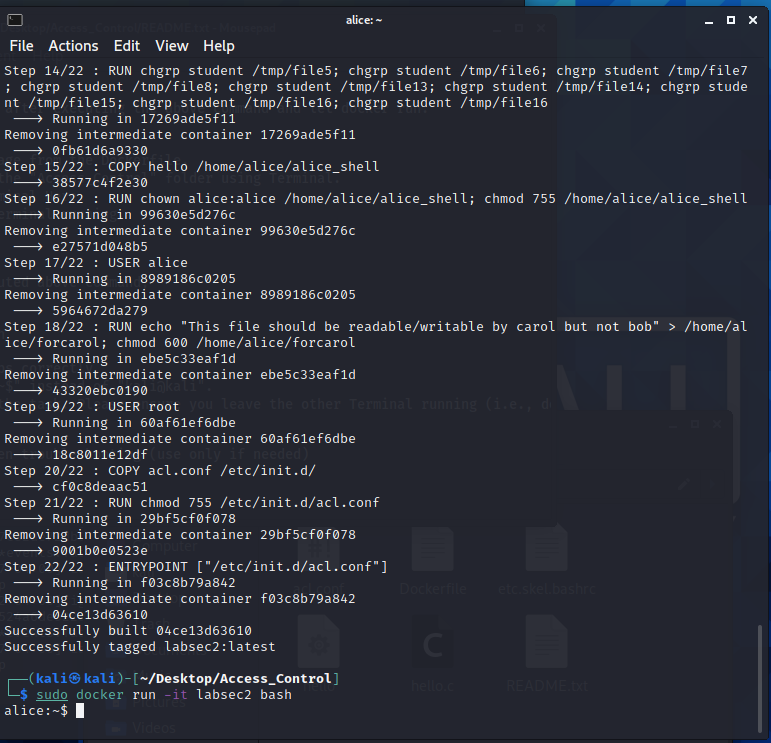
Kali Linux: Task 3.1P

Name of Student

Institutional Affiliation

**Question 1:**

**a) 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).**



**b) List the passwords that you used to access Challenge 2, 3, and 4.**

Password for challenge 2: 99lic4

Password for challenge 3: chmod 755 myfile

Password for challenge 4: aralol

**Question 2:**

**a. What is a Docker? How it is different from a Virtual Machine?**

The container-based technology is Docker, and containers are just operating system user space. The containers running in Docker share the OS kernel of the server. On the other hand, a virtual machine is not container-based. It consists of user space plus operating system kernel space.

**b. What does the “sudo” or “su” command do?**

The sudo command can be used as a different user, by default the root user. The su command is named as root if the user is given the sudo assessment. Running sudo - then type in your user password and the root password will have the same effect that run su.

**c. What does the command “ls -l” do?**

The simple -l command means files and directories to be mentioned. The choice -l lists the content in a long format. You can view the files in the system.

**d. In your own words (i.e., no direct quotes), what does `Chmod’ command do in Unix/Linux?**

You can modify permissions in a file by using a symbolic or numerical mode or a references file by using the Chmod command. Later in this post, we will clarify the modes. The command may take as arguments one or more space-dependent files and/or folders.

**e. In a paragraph (up to 200 words) summarize what you understood about SUID permission and capabilities as covered in Challenge 4. This needs to be in your own words (i.e., no direct quotes).**

SUID is a specific executable file permission which allows other users to execute the file with the file owner's effective permissions. You'll see a s (to mean SUID) special allow for the user instead of the usual x that represents execute permissions. The successful UID becomes that of the file owner, rather than the user running the file, when an SUID bit is set. This is used during execution to have temporarily high permissions. For example, if the executed file belongs with root and the SUID bit has been set, irrespective of who executes the script, permissions (temporarily) will always equal root permissions.

Where filename is the script name or application name. Once the SUID bit is set, it is performed with temporarily high privileges while this application is run. We will use the root command passwd when we try to change our password. You are trying to edit certain configuration files like /etc/passwd, /etc/shadow etc as you try to change your password in this passwd. Some of these files cannot be accessed or displayed with the permissions of the usual root user. If we try to delete SUI Data from this passwd command file and give full permissions, we can not open other files like /etc/shadow to update changes and we will get denied permission.

**Question 3:**

**a. Is the following statement True or False? `sticky bit is a special permission that can be assigned to a file’.**

TRUE

**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’**

TRUE

**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?**

This need one to run the program as the root user. The command used is:

sudo su

**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?**

(rw-r--r--) means that the file owner has read and write permissions (rw-), the group and others have only read permissions (r--). Arash can therefore not read or edit the file since he does not own the fle or belong to the group which owns the file.

**e. A file named ontrack.ppt has a mode of rw-r--r--. If chang-tsun is the file's owner, what can he do with it?**

(rw-r--r--) means that the file owner has read and write permissions (rw-), the group and others have only read permissions (r--). Since chang-tsun owns the file, he has both read and write permissions. This means he can both view and edit the file.

**Question 4:**

**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** -rw------- **(answer using the 9-bit e.g. -r--r--r--)**

**b) If the file is owned by the user, the** OWNER **permission determines the access. (fill the blank either with OWNER/GROUP/OTHER)**

**c) If the group of the file is the same as the user's group, the** OWNER **determines the access. (fill the blank either with OWNER/GROUP/OTHER)**

**d) If the user is not the file owner, and is not in the group, then the** OTHER **is used. (fill the blank either with OWNER/GROUP/OTHER)**

**Question 5: 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 learnt the use of shared operating systems in containers. This implies that in machine resource terms they are much more effective than hypervisors. Containers stay on top of a single Linux instance instead of virtualizing hardware. Each Linux file has its own access licences and is held by a single user and a single community. ls with the long listing option, such as ls-l myfile, is the most popular way to display the permissions in a file. If all files in your present directory are allowed to be viewed, execute the command without an argument. Now I understand how ownership and permissions operate in Linux better.