*All questions in the task instruction sheet must be answered.*

Question #1.a What is a Docker? How it is different from a virtual Machine?

Answer:

Docker is a platform designed to develop, ship, and run applications inside lightweight, portable containers, which reduces the impact of hardware differences on program operation.

Docker’s architecture is lightweight, its containers share the host OS’s kernel and use isolated user spaces to run applications. They do not require a full OS installation per application. While VM machines run a full operation system.

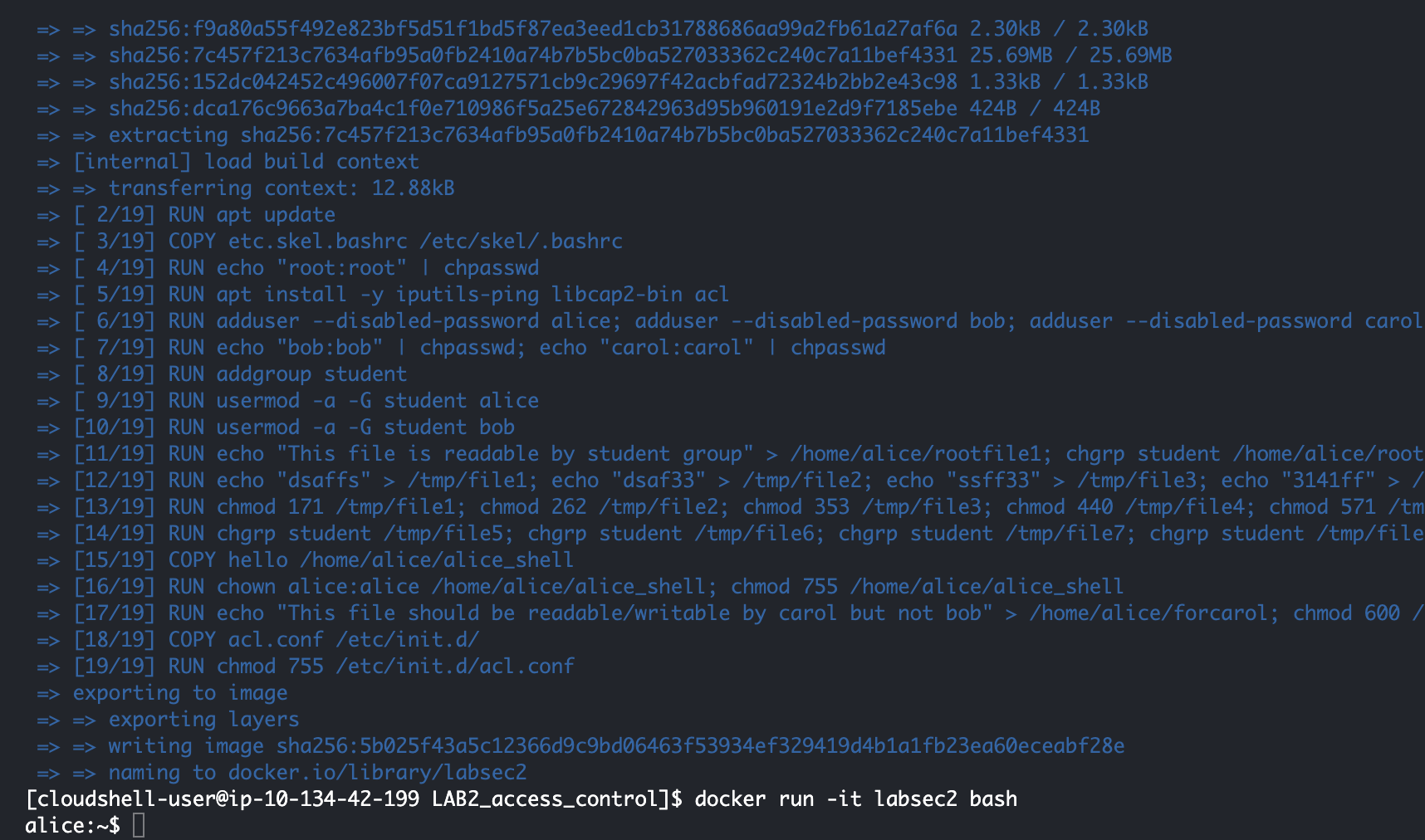
Because Docker containers share the host OS kernel, they start up almost instantly and use less disk space and memory. While WMs run a full OS, they are more resource-intensive (booting up a VM takes longer because the entire OS must start).

And Docker containers are highly portable. They can run on any system that supports Docker, regardless of the underlying hardware. But VMs are less portable due to their larger size and dependency on hypervisor technology.

Question #1.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).

Answer:

Todo: XXXXX



Question #2.a What does the “sudo” or “su” command do?

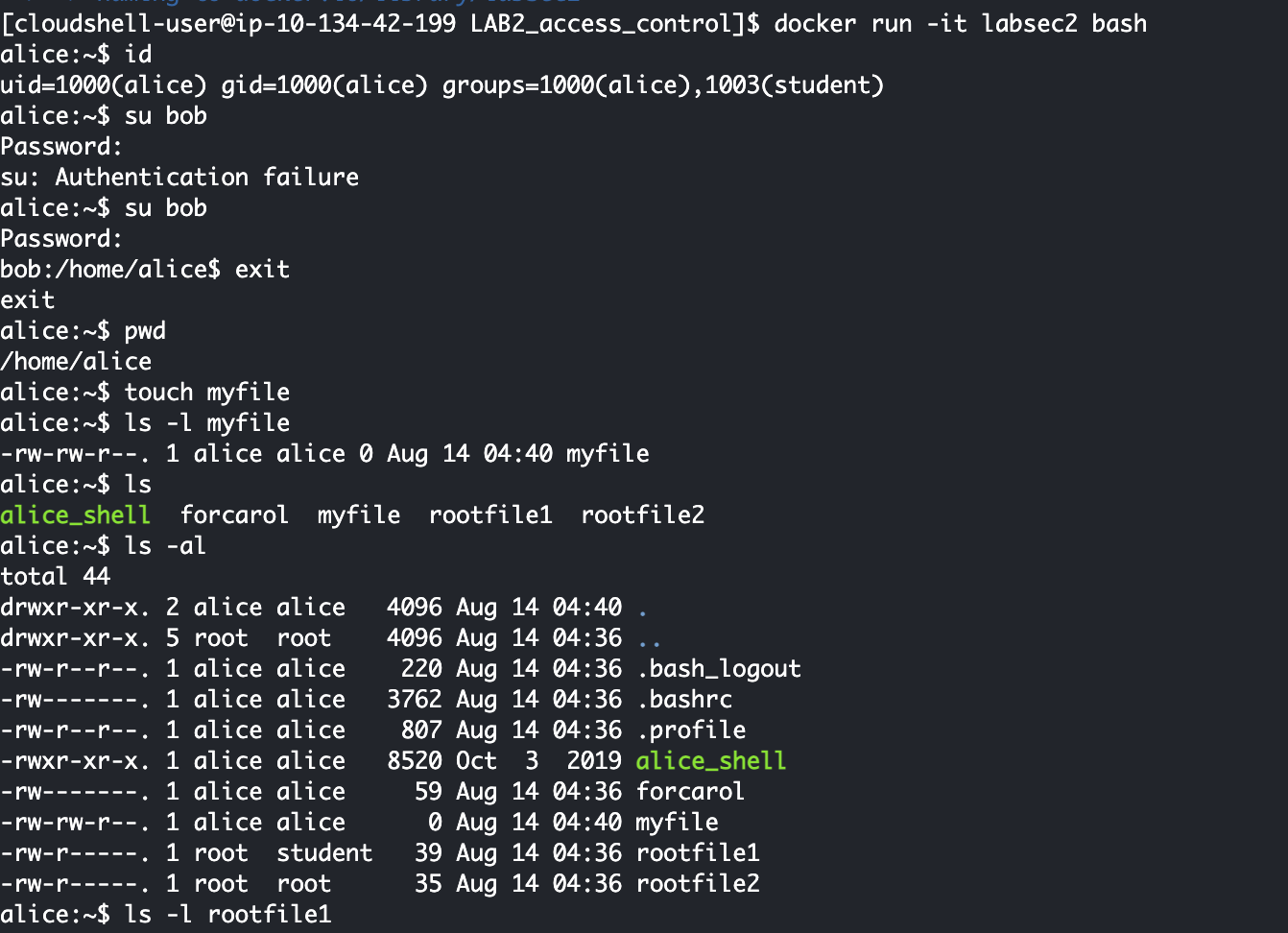
Answer:

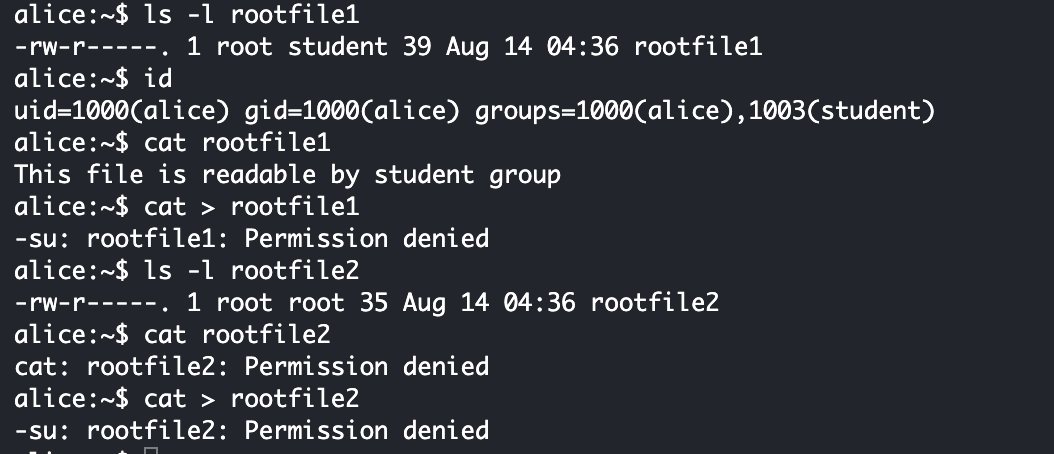
“sudo” allows a permitted user to execute a command as the superuser or other user, as specified by the security policy.

“su” allows us to switch the current user to another user, typically the root user.

Question #2.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.

Answer:





Question #3.a What does the command “ls -l” do?

Answer:

This command is to list the files and directories in a directory in a long listing format

Question #3.b In your own words (i.e., no direct quotes), what does `Chmod’ command do in Unix/Linux?

Answer:

This command help us protect the file/directory security, which only allows users with permission to operate files/directories.

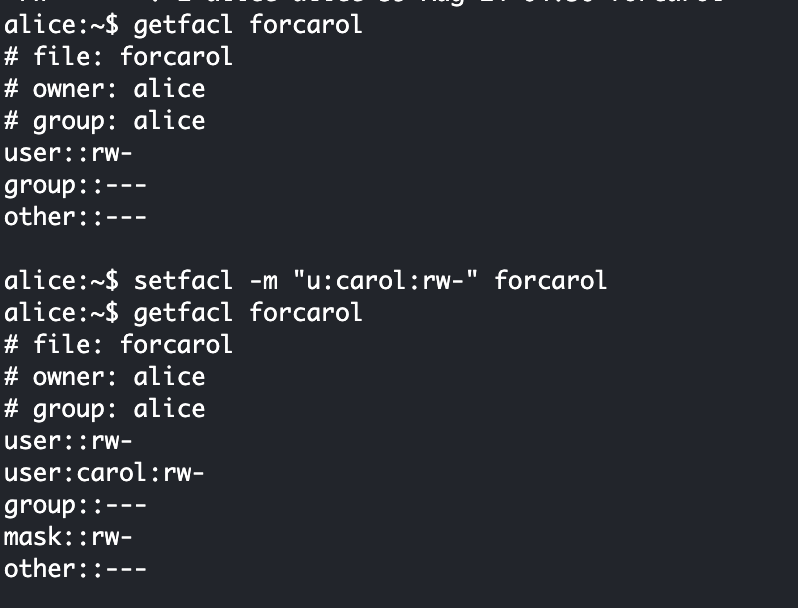
Question #3.c What is the command to set -rwxr-xr-x permissions to myfile? (make sure to include the exact command including any spaces)

Answer:

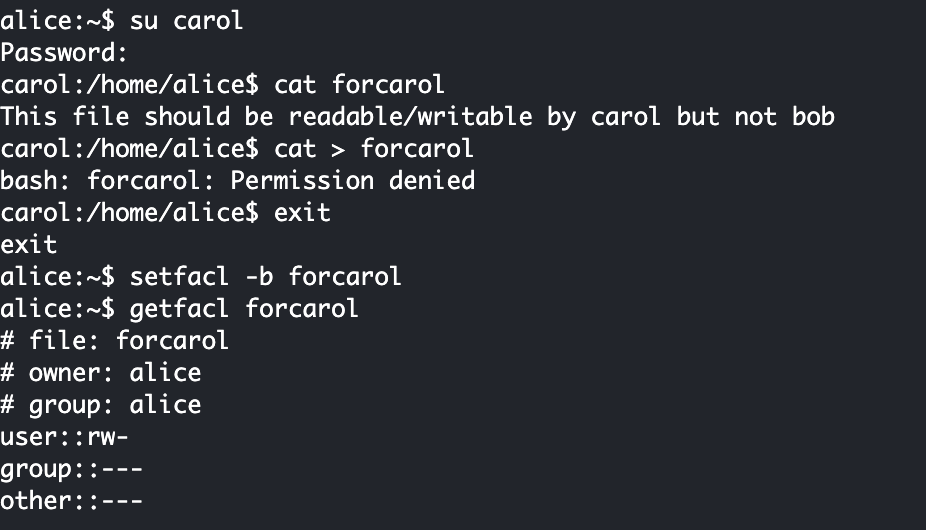
“Chmod 755 myfile”

Question #4

Answer:







Question #5 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).

Answer:

The SUID permission in Unix operating systems allows users to execute a file with the permissions of the file’s owner, rather than with the permissions of the user who is running it. This is particularly useful for tasks that require elevated privileges but shouldn’t require full root access. When a file with SUID is executed, the operating system temporarily grants the user’s process the rights of the file’s owner, often root, allowing the necessary task to be completed securely.

Capabilities, on the other hand, provide a more fine-grained control over privileges, breaking down the all-powerful root access into specific permissions. This allows for safer execution of commands by granting only the necessary privileges to a process without giving it full root access. Capabilities help reduce the risks associated with running processes as root by limiting the scope of what those processes can do, thus enhancing system security.

Question #6

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

False, the sticky bit is a special permission that is assigned to directories, not files.

1. 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, when an executable file has the SUID permission set, the user who runs the file does not become the file’s temporary owner. Instead, the file executes with the privileges of the file’s owner, but the user running the file does not gain ownership or any broader control over the file itself. The SUID bit temporarily elevates the process's permissions to those of the file owner for the duration of the execution, but ownership remains unchanged.

1. 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

1. 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?

Since Arash is neither the owner of the file nor a member of the group that owns the file, he falls under the "Others" category, and he can only read the file.

1. 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?

Read and Write

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

Question #8 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?

Answer: I learned that the SUID bit allows a file to run with the permissions of the file’s owner, but it doesn't automatically grant execute permissions. For a file to be executed, it must have the execute bit set alongside any SUID permissions. And I gained a deeper understanding of how Unix file permissions are represented and managed, specifically how different bits impact file access and execution.

I encountered many problems during the learning process. I found course resources and video resources on Deakin Cloud, and then searched for the corresponding content to match the problem.

*(follow the above format for all questions. Ensure that you include the question number and the answer just below the question number)*