Week 4 Task T4.1PA

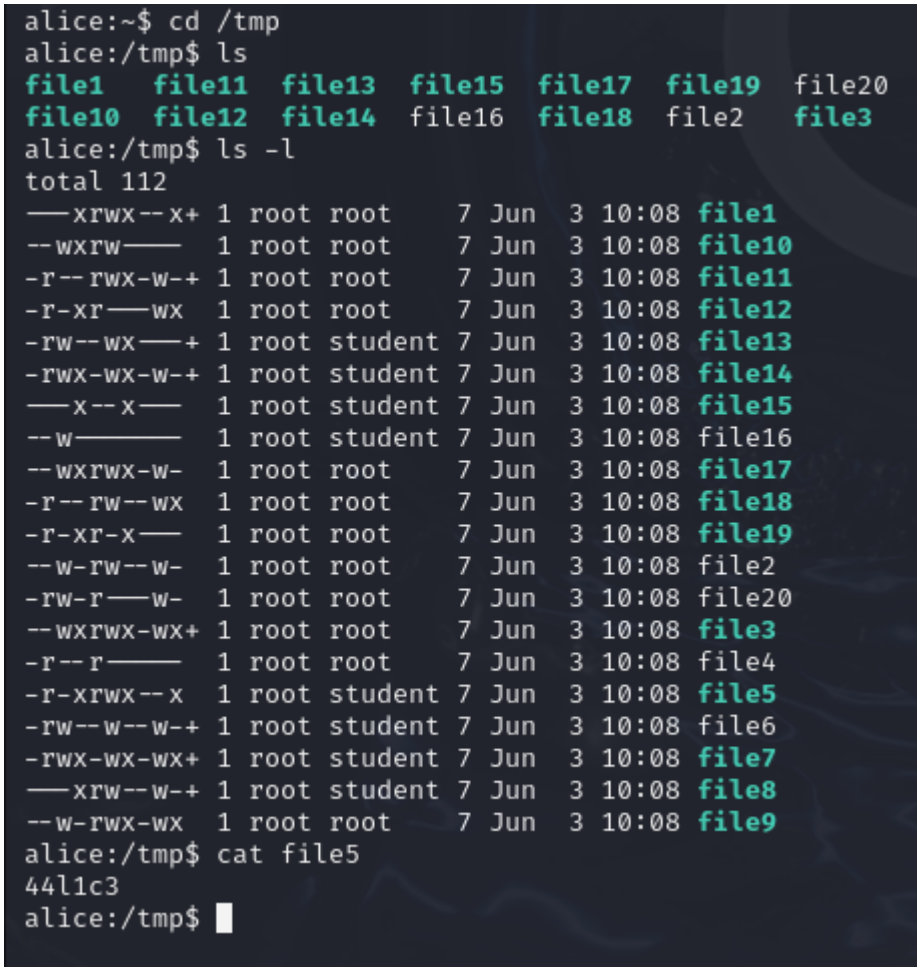
Answer the below questions

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).

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.

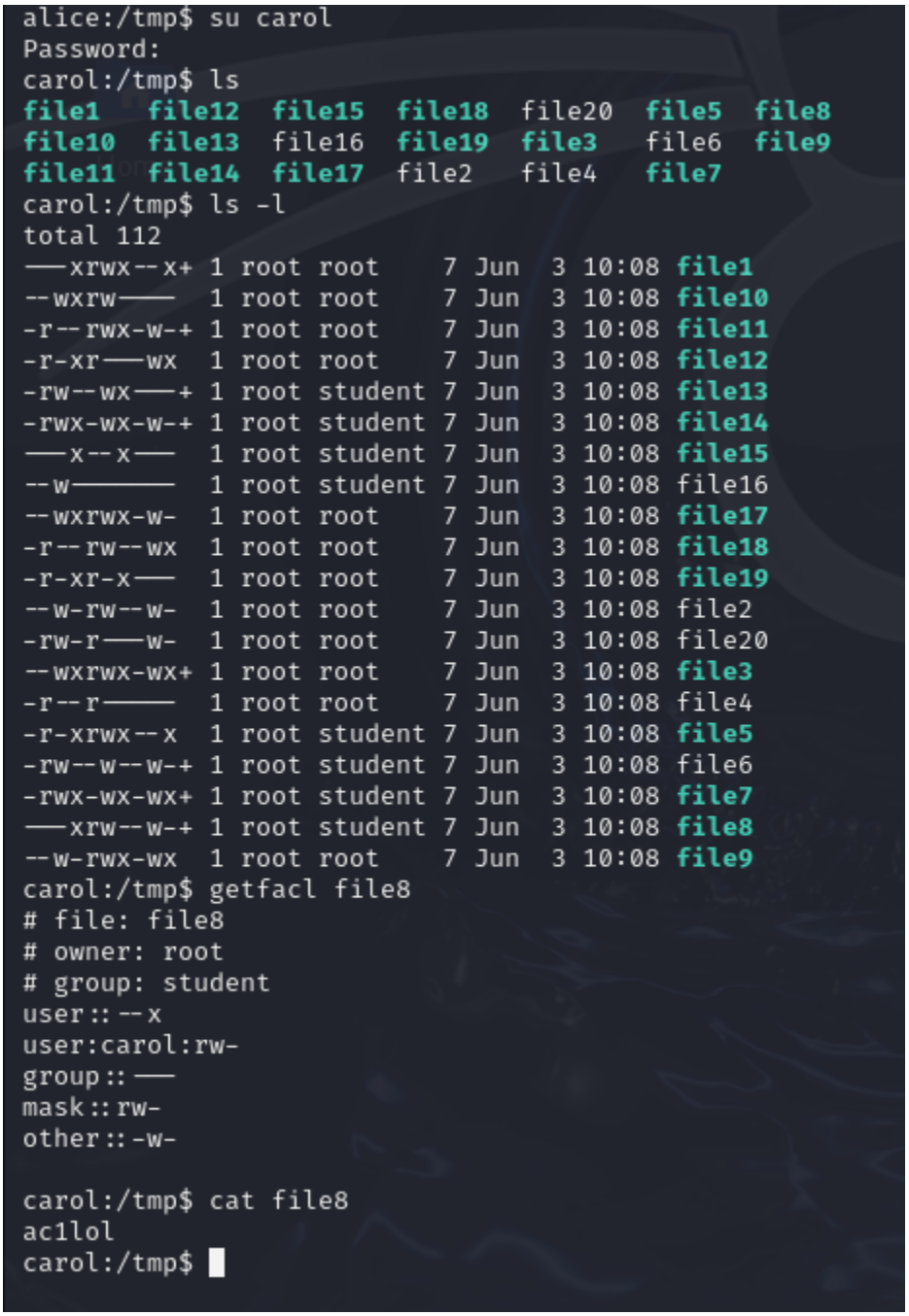


3. Question 3
    a. What does the command “ls -l” do?
        - The command is –l provides a full list of all the files and folders in the current directory, including information on their size, modification date, owner, group, permissions, and filename.

    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.



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 hedo 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.