EN4720: Security in Cyber-Physical Systems
Exercise — Authorization

Name: Thalagala B. P.
Index No: 180631J

May 19, 2023

This is an individual exercise!
Due Date: 19 May 2023 by 11.59 PM

This exercise has to be carried out using a Linux-based PC/virtual machine. Read all the instructions and questions before attempting the exercise. Add answers under each question in the Questions section and submit the resulting PDF.

Instructions

1. Understand how linux users and groups work.
2. Understand how linux file ownership and permissions work.
3. Answer the questions given below.

Questions

1. View the currently logged in user.

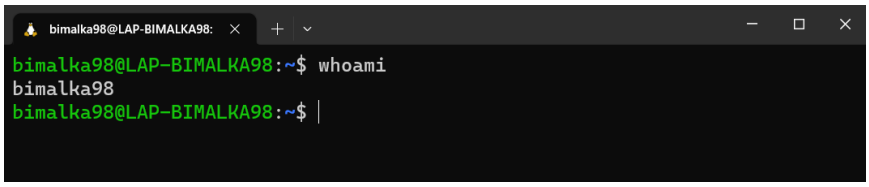

Figure 1: Currently logged in user

2. Create a sub directory as excercise4. Create a text file resolutions.txt with "Hello World" text in the file and store the file in the newly created directory as exercise4/resolutions.txt. Dump the file to the terminal using the `cat` command.

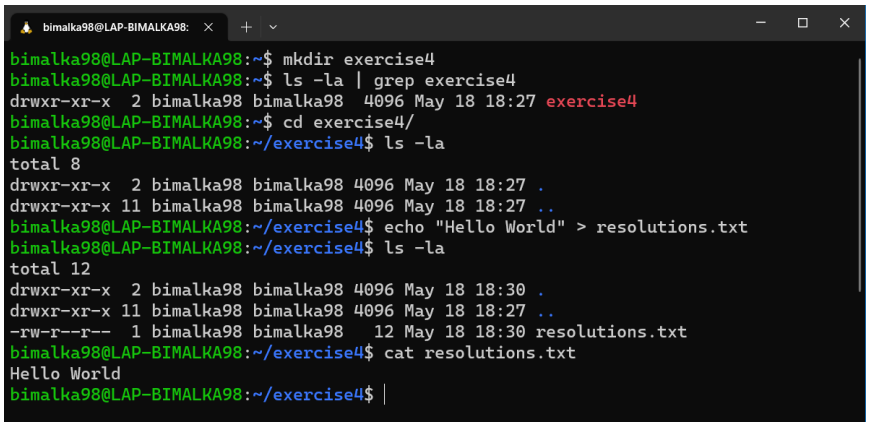

Figure 2: Creating a sub-directory, creating a file with the required text and dump its content to the terminal

3. Create two new user accounts as alice and bob.

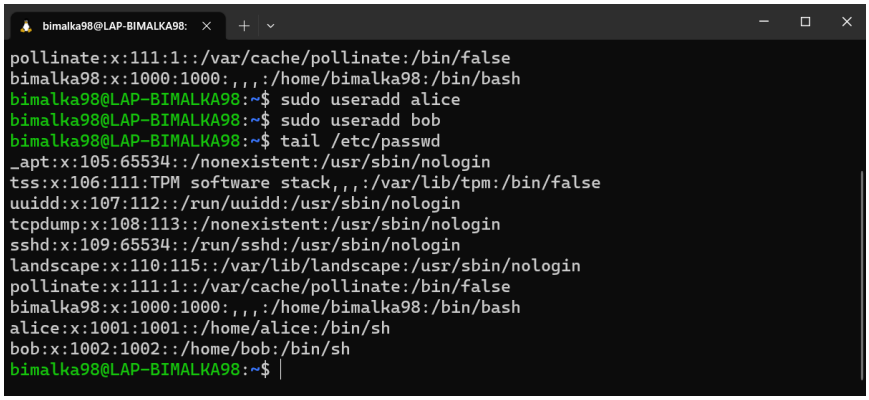

Figure 3: Creating two new user accounts

4. Create a group as friends and add alice and yourself (currently logged in user) to the group friends

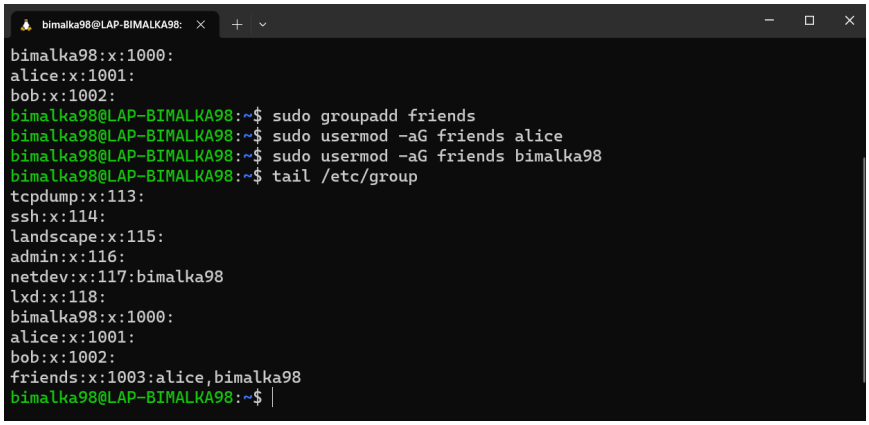

Figure 4: Creating a group and add members

5. Make sure your (currently logged in user's) home directory has execute permissions for all the users.

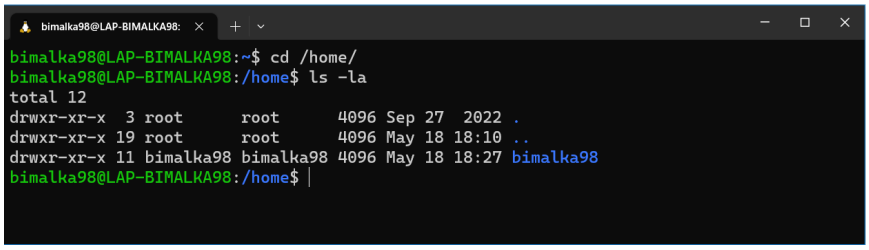

Figure 5: Execution permission to the current user's home directory

6. Become (log in as) one of your new user accounts (alice or bob). You can simply `su -` to the alternate user.

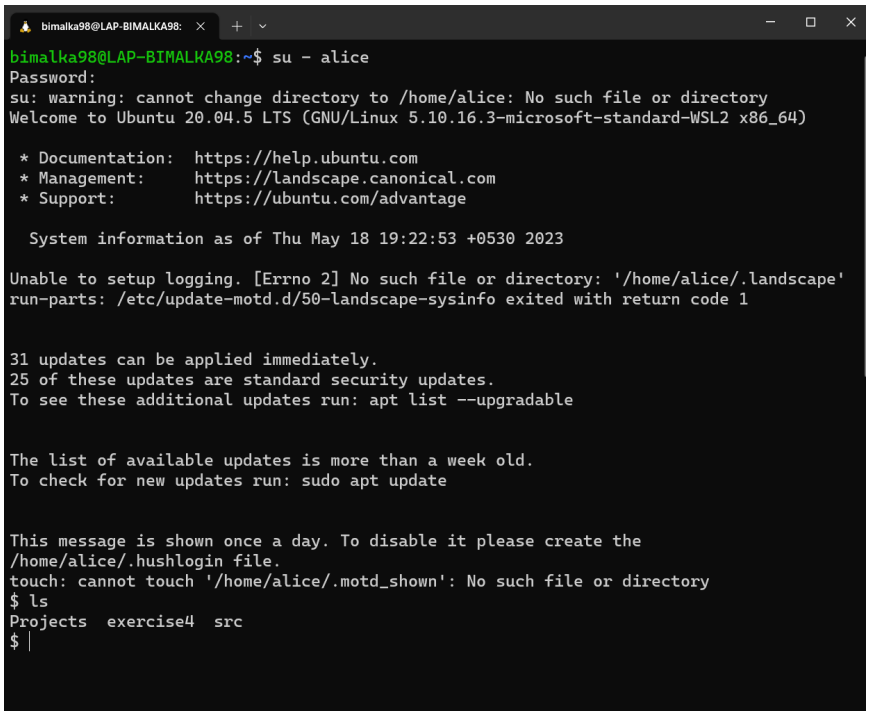

Figure 6: Log-in as the user `alice`

7. As the new user, confirm that you can view the file by dumping the content to the terminal. Try adding a new item to the resolutions.txt file. Why can't you modify the file as the new user?

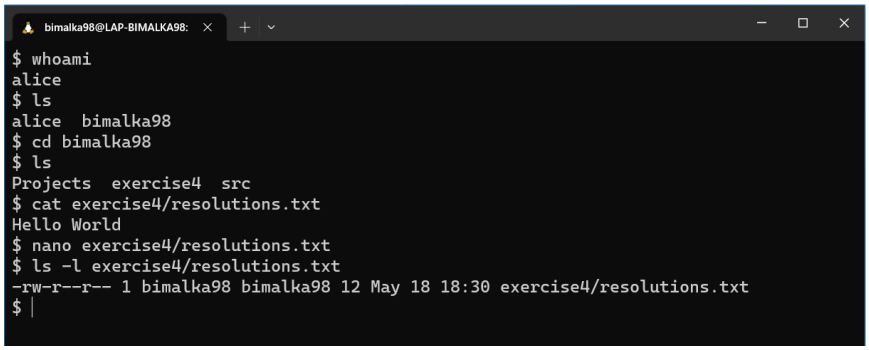

Figure 7: Viewing the content of the `resolutions.txt` file

As the Figure 8 illustrates, altering the content of the `resolutions.txt` *file, is denied. Because, the* `other` *users in the Linux host machine has only the* `read` *permission for that file, and no write permission is given to them. This fact is verified by the output of the last command in the Figure 7, which inspects various permissions to the* `resolutions.txt` *file. The line segment* `-rw-r--r--` *indicates that the User* `bimalka98` *has Read and Write permissions (rw-), the Group* `bimalka98` *has Read permission (r–), and Others have Read permission (r–).*

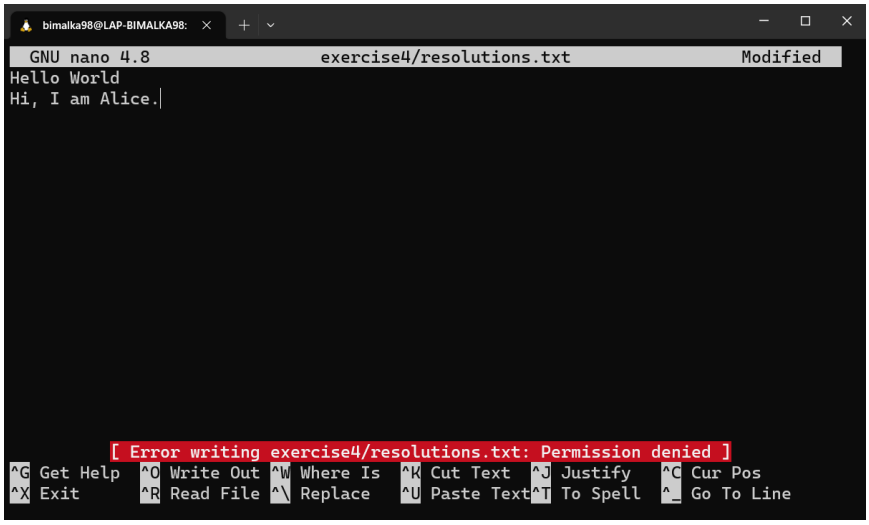

Figure 8: Trying to alter the content of the `resolutions.txt` file: Permission Denied.

8. Note that the permissions on a newly created file allow all users on the system to read the file. Assume that you want to keep resolutions.txt file private. Modify the file's permissions, such that read access for others is removed.

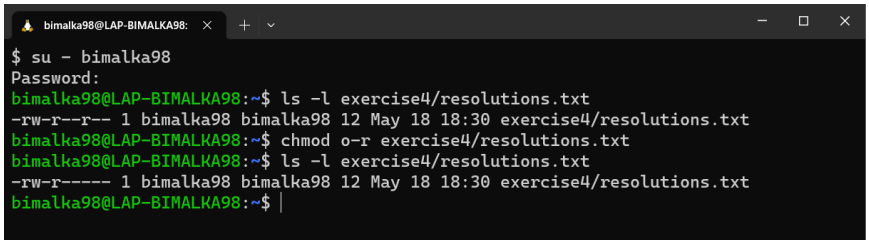

Figure 9: Removing the read access for `other` users

9. Using the other new account (if you used alice before, now use bob), confirm that other users on the system are not able to read your resolutions.txt file by trying to dump the file to the terminal.

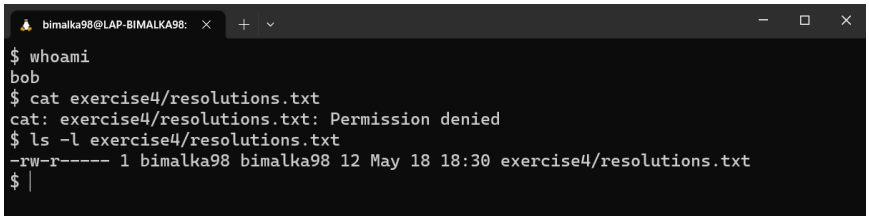

Figure 10: Confirming that other users on the system are not able to read your `resolutions.txt` file, by trying to viewing its content from bob's account

10. Compose a short shopping list in your preferred text editor, or using the command line. Store the file as exercise4/shopping.txt. Change the group owner of the file to friends.

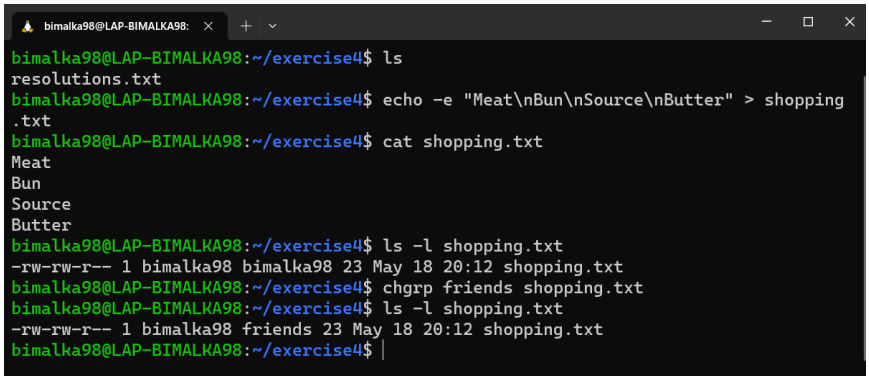

Figure 11: Creating the `shopping.txt` file and change its group owner

11. As the alternate user alice, confirm that you can view the file. Also, note that you can modify the file, by adding an additional item to the shopping list. Dump the file content to the terminal to show that the new item is added.

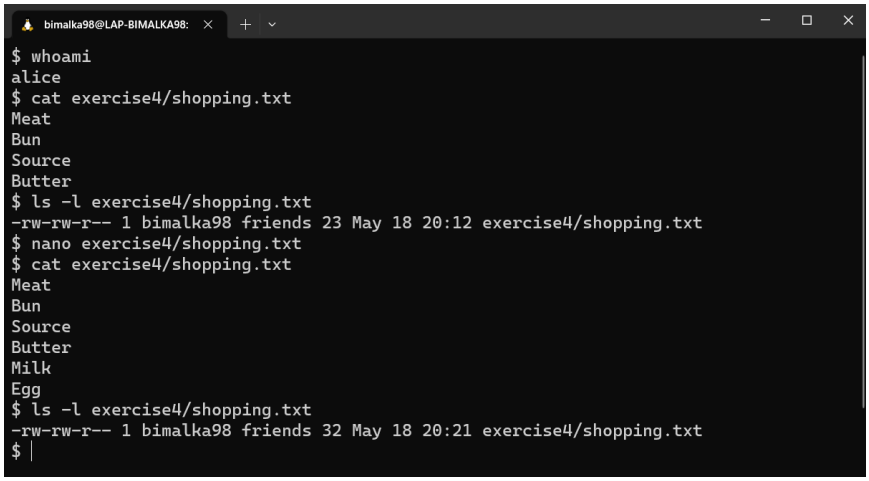

Figure 12: Confirming the read and write permission of the users of the friends group

12. Recall that your other new account (bob) is not a member of the group friends. Try becoming bob and repeat the previous steps. You should be able to view, but not modify, the file.

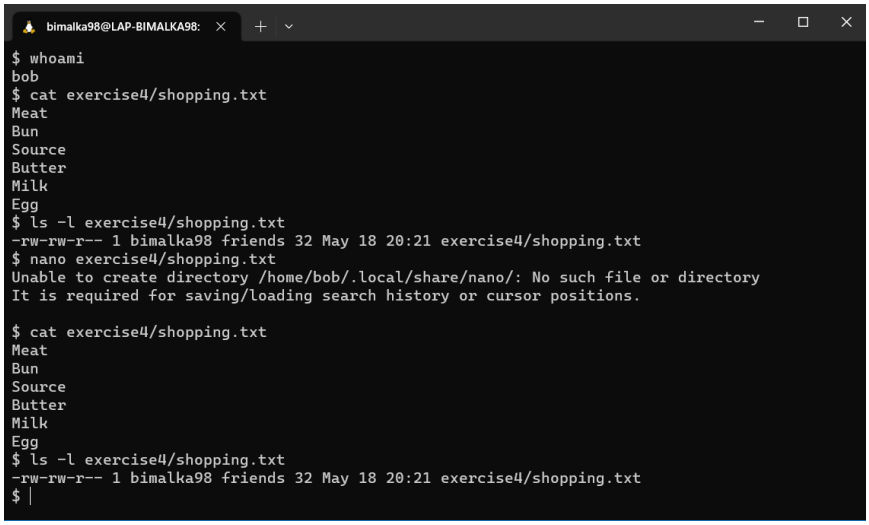

Figure 13: Checking the read and write permission of the user `bob`

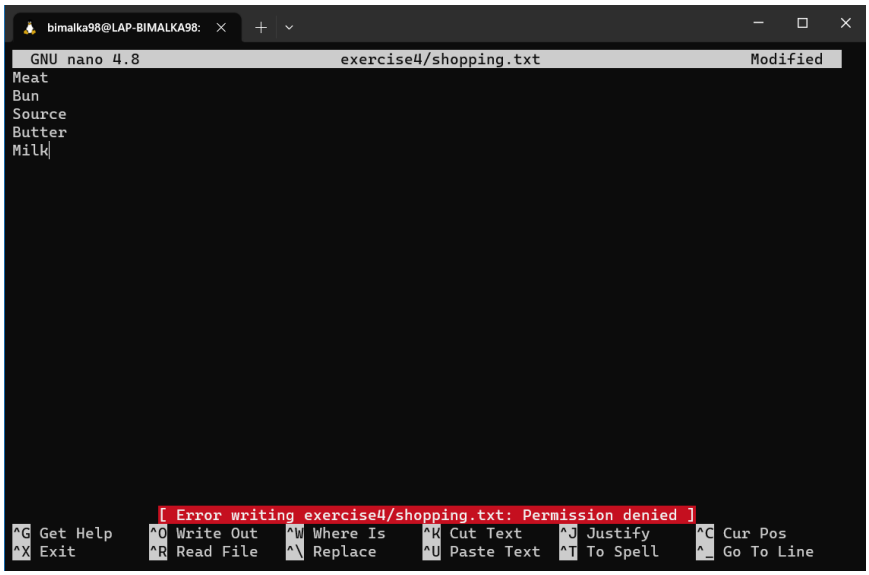

Figure 14: Verifying the user `bob` does not have write permission

Provide analytical answers to the questions below. Screenshots are not required.

13. What are the challenges that organizations face during the cyber security authorization process, and how can they be overcome?

    The following answer was adopted from `https://www.accenture.com/us-en/blogs/security/keys-successful-access-authorization`

    Challenges and ways to overcome them:

    - ***Lack of vendor solutions*** *- Due to inflexibility and performance concerns of the available cyber security authorization processes, most organizations chose to build the authorization systems which best suits for their specific requirement. The growth of the number of vendor specializing in this area is a way to overcome this challenge. So that organization can select the best match for their requirements and adopt the solution accordingly.*
    - ***Complexity of managing policies*** *- When managing authorization processes, organizations need to maintain/ update rules that determine who is allowed to access certain information and resources. This process involve, analyzing the existing complex code to identify already existing rules and reverse engineer the existing decision making (if/ else) algorithms to understand how those rules are enforced. This whole process is super complex to carry out manually.Tools with Artificial Intelligence capabilities have been built by vendors to dynamically generate and manage policies. In addition to that friendly user interfaces that hides the complexity of extensible access control markup language (XACML) has also become a grate relief.*
    - ***Performance and scale*** *- Organizations need to make sure that their systems can handle the ever increasing demands of the authorization process. However, this process involves communication between various system components which essentially can slow down the system. Focusing on modernizing applications and systems that take advantage of cloud technologies is a way to address this issue, as they often have better integration with authorization tools.*

14. How do different cyber security authorization frameworks differ from one another, and what are the key considerations that organizations should take into account when choosing a framework to follow?

    Your answer here

15. What are the most common vulnerabilities that may be identified during the cyber security authorization process, and how can organizations address them?

    Your answer here