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

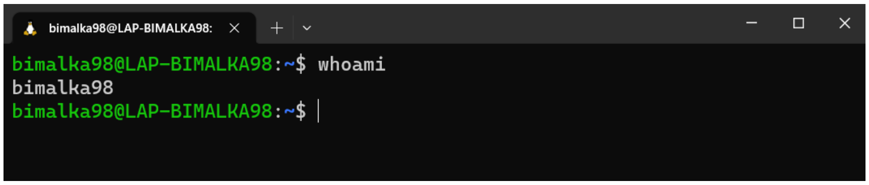
This exercise has to be carried out using a Linux-based PC/virtual machine. Read all the instructions and questions before attempting the exercise. Add answers under each question in the Questions section and submit the resulting PDF.

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

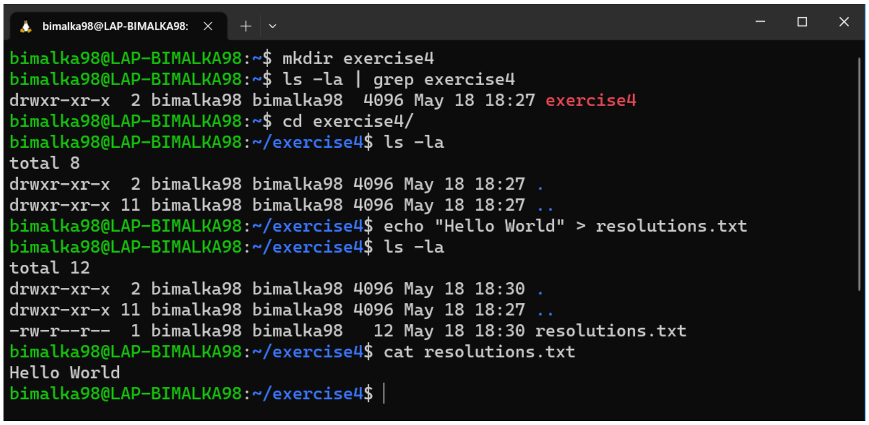
1. View the currently logged in user.



```
bimalka98@LAP-BIMALKA98:~$ whoami
bimalka98
bimalka98@LAP-BIMALKA98:~$ 
```

Figure 1: Currently logged in user

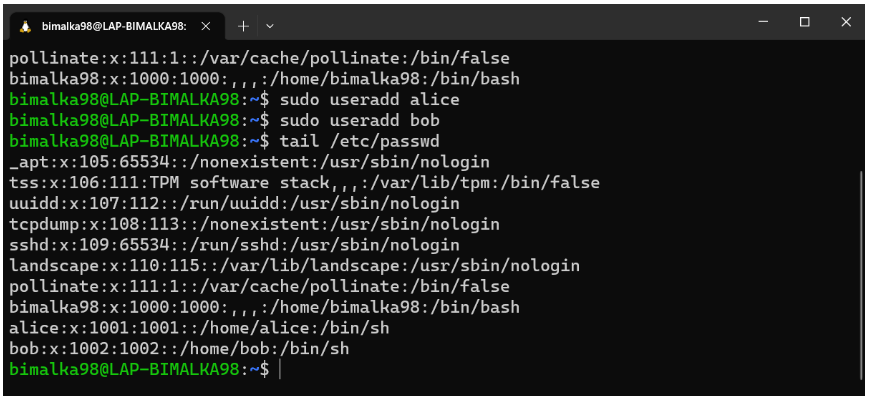
2. Create a sub directory as excercise4. Create a text file resolutions.txt with “Hello World” text in the file and store the file in the newly created directory as exercise4/resolutions.txt. Dump the file to the terminal using the `cat` command.



```
bimalka98@LAP-BIMALKA98:~$ mkdir exercise4
bimalka98@LAP-BIMALKA98:~$ ls -la | grep exercise4
drwxr-xr-x  2 bimalka98 bimalka98  4096 May 18 18:27 exercise4
bimalka98@LAP-BIMALKA98:~$ cd exercise4/
bimalka98@LAP-BIMALKA98:~/exercise4$ ls -la
total 8
drwxr-xr-x  2 bimalka98 bimalka98 4096 May 18 18:27 .
drwxr-xr-x 11 bimalka98 bimalka98 4096 May 18 18:27 ..
bimalka98@LAP-BIMALKA98:~/exercise4$ echo "Hello World" > resolutions.txt
bimalka98@LAP-BIMALKA98:~/exercise4$ ls -la
total 12
drwxr-xr-x  2 bimalka98 bimalka98 4096 May 18 18:30 .
drwxr-xr-x 11 bimalka98 bimalka98 4096 May 18 18:27 ..
-rw-r--r--  1 bimalka98 bimalka98   12 May 18 18:30 resolutions.txt
bimalka98@LAP-BIMALKA98:~/exercise4$ cat resolutions.txt
Hello World
bimalka98@LAP-BIMALKA98:~/exercise4$ 
```

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

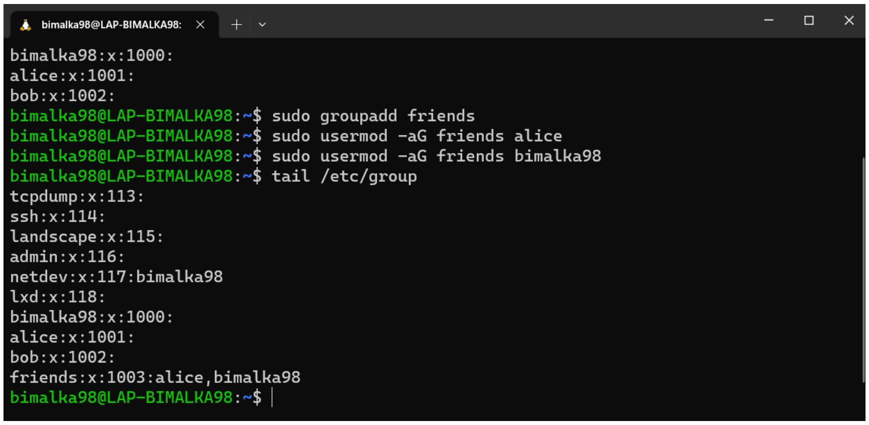
3. Create two new user accounts as alice and bob.



```
pollinate:x:111:1::/var/cache/pollinate:/bin/false
bimalka98:x:1000:1000:,,,:/home/bimalka98:/bin/bash
bimalka98@LAP-BIMALKA98:~$ sudo useradd alice
bimalka98@LAP-BIMALKA98:~$ sudo useradd bob
bimalka98@LAP-BIMALKA98:~$ tail /etc/passwd
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
landscape:x:110:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
bimalka98:x:1000:1000:,,,:/home/bimalka98:/bin/bash
alice:x:1001:1001::/home/alice:/bin/sh
bob:x:1002:1002::/home/bob:/bin/sh
bimalka98@LAP-BIMALKA98:~$ 
```

Figure 3: Creating two new user accounts

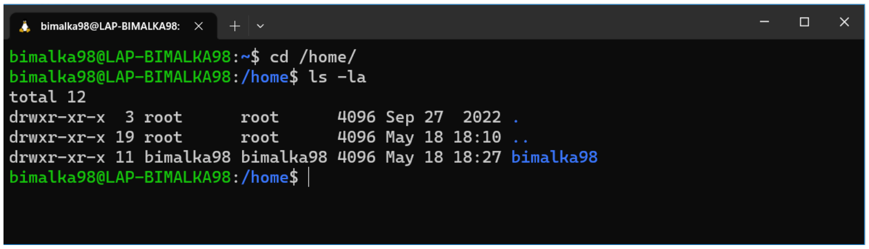
4. Create a group as friends and add alice and yourself (currently logged in user) to the group friends



```
bimalka98:x:1000:
alice:x:1001:
bob:x:1002:
bimalka98@LAP-BIMALKA98:~$ sudo groupadd friends
bimalka98@LAP-BIMALKA98:~$ sudo usermod -aG friends alice
bimalka98@LAP-BIMALKA98:~$ sudo usermod -aG friends bimalka98
bimalka98@LAP-BIMALKA98:~$ tail /etc/group
tcpdump:x:113:
ssh:x:114:
landscape:x:115:
admin:x:116:
netdev:x:117:bimalka98
lxd:x:118:
bimalka98:x:1000:
alice:x:1001:
bob:x:1002:
friends:x:1003:alice,bimalka98
bimalka98@LAP-BIMALKA98:~$
```

Figure 4: Creating a group and add members

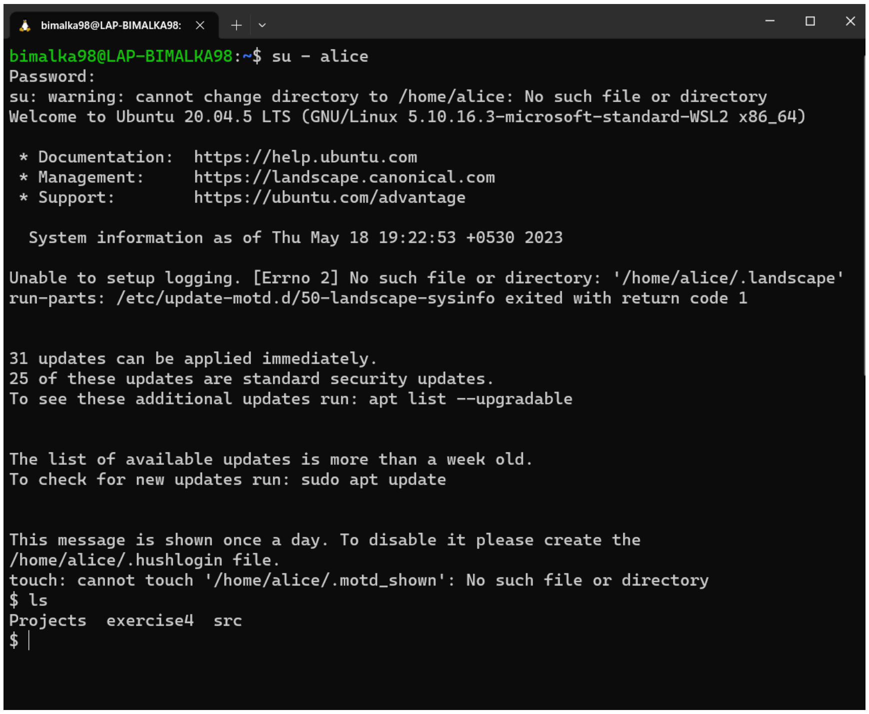
5. Make sure your (currently logged in user's) home directory has execute permissions for all the users.



```
bimalka98@LAP-BIMALKA98:~$ cd /home/
bimalka98@LAP-BIMALKA98:/home$ ls -la
total 12
drwxr-xr-x  3 root      root      4096 Sep 27  2022 .
drwxr-xr-x 19 root      root      4096 May 18 18:10 ..
drwxr-xr-x 11 bimalka98 bimalka98 4096 May 18 18:27 bimalka98
bimalka98@LAP-BIMALKA98:/home$
```

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

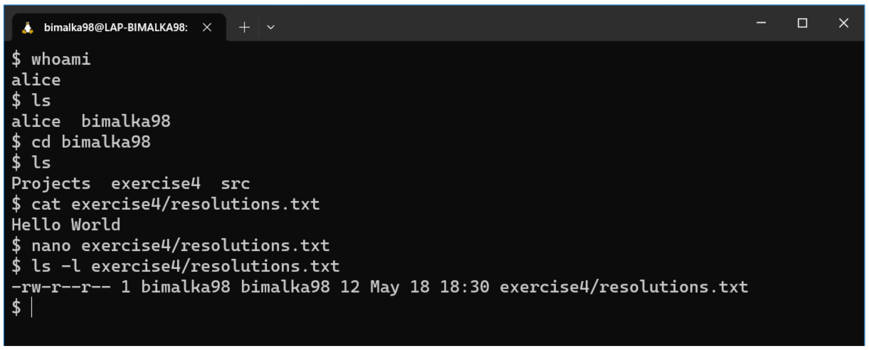
6. Become (log in as) one of your new user accounts (alice or bob). You can simply `su -` to the alternate user.



```
bimalka98@LAP-BIMALKA98:~$ su - alice
Password:
su: warning: cannot change directory to /home/alice: No such file or directory
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.10.16.3-microsoft-standard-WSL2 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu May 18 19:22:53 +0530 2023

Unable to setup logging. [Errno 2] No such file or directory: '/home/alice/.landscape'
run-parts: /etc/update-motd.d/50-landscape-sysinfo exited with return code 1


31 updates can be applied immediately.
25 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


This message is shown once a day. To disable it please create the
/home/alice/.hushlogin file.
touch: cannot touch '/home/alice/.motd_shown': No such file or directory
$ ls
Projects  exercise4  src
$ |
```

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

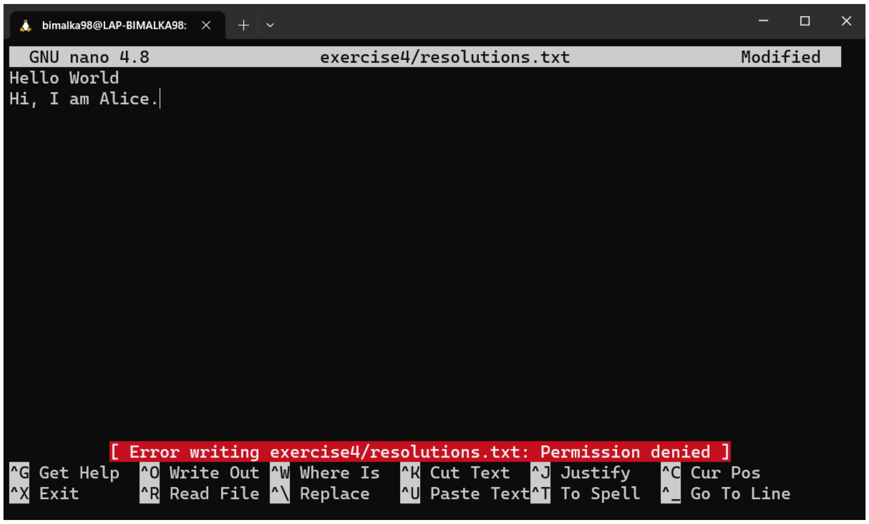
7. As the new user, confirm that you can view the file by dumping the content to the terminal. Try adding a new item to the resolutions.txt file. Why can't you modify the file as the new user?



```
$ whoami
alice
$ ls
alice  bimalka98
$ cd bimalka98
$ ls
Projects  exercise4  src
$ cat exercise4/resolutions.txt
Hello World
$ nano exercise4/resolutions.txt
$ ls -l exercise4/resolutions.txt
-rw-r--r-- 1 bimalka98 bimalka98 12 May 18 18:30 exercise4/resolutions.txt
$ |
```

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

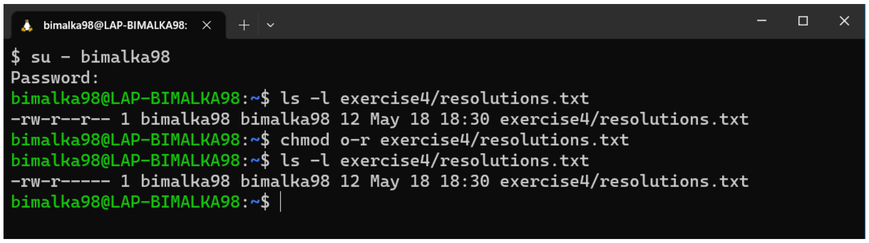
As the Figure 8 illustrates, altering the content of the `resolutions.txt` *file, is denied. Because, the* `other` *users in the Linux host machine has only the* `read` *permission for that file, and no write permission is given to them. This fact is verified by the output of the last command in the 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–).*



```
  GNU nano 4.8                exercise4/resolutions.txt                  Modified
Hello World
Hi, I am Alice.




               [ Error writing exercise4/resolutions.txt: Permission denied ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text^T To Spell  ^_ Go To Line
```

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

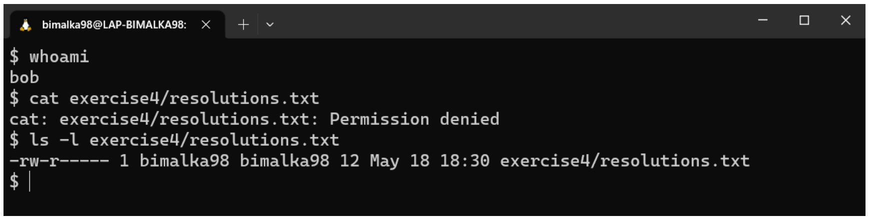
8. Note that the permissions on a newly created file allow all users on the system to read the file. Assume that you want to keep resolutions.txt file private. Modify the file's permissions, such that read access for others is removed.



```
$ su - bimalka98
Password:
bimalka98@LAP-BIMALKA98:~$ ls -l exercise4/resolutions.txt
-rw-r--r-- 1 bimalka98 bimalka98 12 May 18 18:30 exercise4/resolutions.txt
bimalka98@LAP-BIMALKA98:~$ chmod o-r exercise4/resolutions.txt
bimalka98@LAP-BIMALKA98:~$ ls -l exercise4/resolutions.txt
-rw-r----- 1 bimalka98 bimalka98 12 May 18 18:30 exercise4/resolutions.txt
bimalka98@LAP-BIMALKA98:~$
```

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

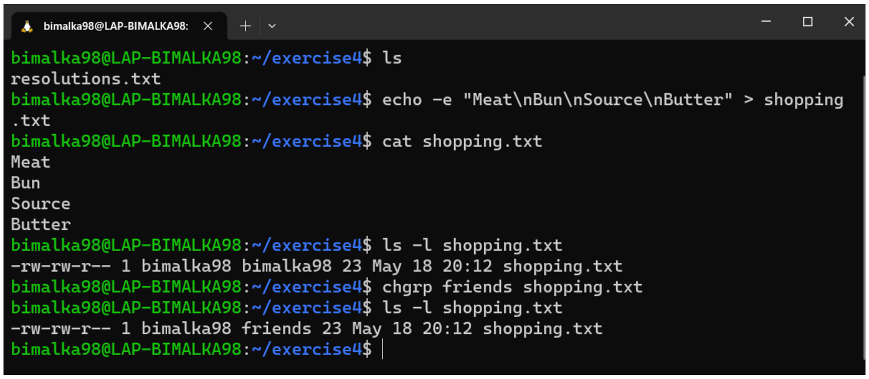
9. Using the other new account (if you used alice before, now use bob), confirm that other users on the system are not able to read your resolutions.txt file by trying to dump the file to the terminal.



```
$ whoami
bob
$ cat exercise4/resolutions.txt
cat: exercise4/resolutions.txt: Permission denied
$ ls -l exercise4/resolutions.txt
-rw-r----- 1 bimalka98 bimalka98 12 May 18 18:30 exercise4/resolutions.txt
$
```

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

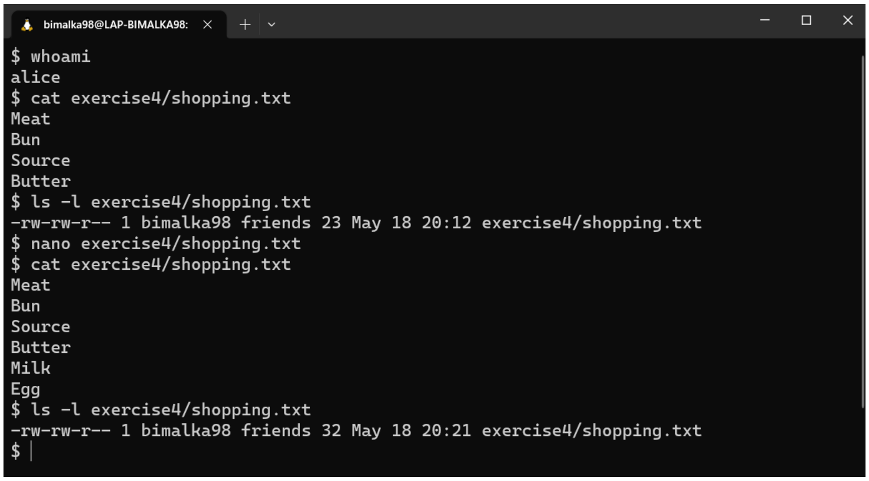
10. Compose a short shopping list in your preferred text editor, or using the command line. Store the file as exercise4/shopping.txt. Change the group owner of the file to friends.



```
bimalka98@LAP-BIMALKA98:~/exercise4$ ls
resolutions.txt
bimalka98@LAP-BIMALKA98:~/exercise4$ echo -e "Meat\nBun\nSource\nButter" > shopping
.txt
bimalka98@LAP-BIMALKA98:~/exercise4$ cat shopping.txt
Meat
Bun
Source
Butter
bimalka98@LAP-BIMALKA98:~/exercise4$ ls -l shopping.txt
-rw-rw-r-- 1 bimalka98 bimalka98 23 May 18 20:12 shopping.txt
bimalka98@LAP-BIMALKA98:~/exercise4$ chgrp friends shopping.txt
bimalka98@LAP-BIMALKA98:~/exercise4$ ls -l shopping.txt
-rw-rw-r-- 1 bimalka98 friends 23 May 18 20:12 shopping.txt
bimalka98@LAP-BIMALKA98:~/exercise4$ 
```

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

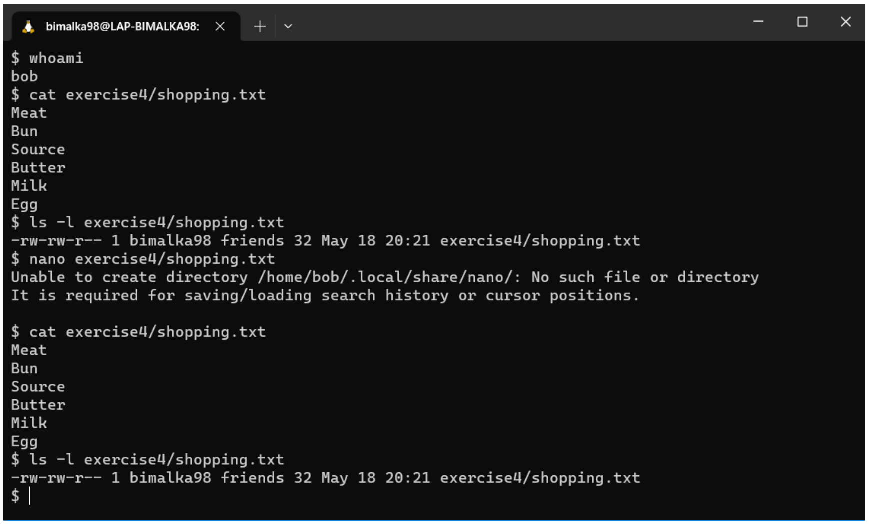
11. As the alternate user alice, confirm that you can view the file. Also, note that you can modify the file, by adding an additional item to the shopping list. Dump the file content to the terminal to show that the new item is added.



```
$ whoami
alice
$ cat exercise4/shopping.txt
Meat
Bun
Source
Butter
$ ls -l exercise4/shopping.txt
-rw-rw-r-- 1 bimalka98 friends 23 May 18 20:12 exercise4/shopping.txt
$ nano exercise4/shopping.txt
$ cat exercise4/shopping.txt
Meat
Bun
Source
Butter
Milk
Egg
$ ls -l exercise4/shopping.txt
-rw-rw-r-- 1 bimalka98 friends 32 May 18 20:21 exercise4/shopping.txt
$ 
```

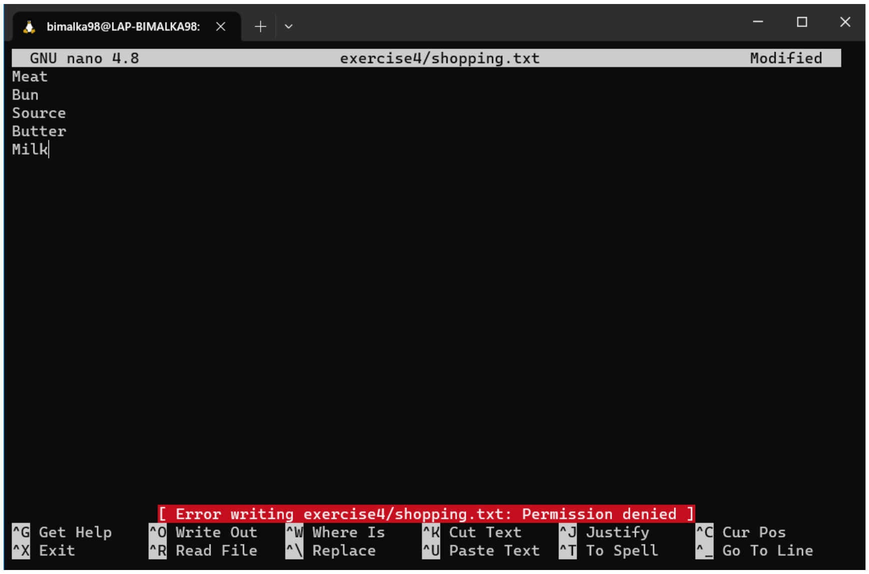
Figure 12: Confirming the read and write permission of the users of the friends group

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.



```
$ whoami
bob
$ cat exercise4/shopping.txt
Meat
Bun
Source
Butter
Milk
Egg
$ ls -l exercise4/shopping.txt
-rw-rw-r-- 1 bimalka98 friends 32 May 18 20:21 exercise4/shopping.txt
$ nano exercise4/shopping.txt
Unable to create directory /home/bob/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

$ cat exercise4/shopping.txt
Meat
Bun
Source
Butter
Milk
Egg
$ ls -l exercise4/shopping.txt
-rw-rw-r-- 1 bimalka98 friends 32 May 18 20:21 exercise4/shopping.txt
$ |
```

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



```
  GNU nano 4.8                    exercise4/shopping.txt                    Modified
Meat
Bun
Source
Butter
Milk















                [ Error writing exercise4/shopping.txt: Permission denied ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line
```

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` *and 'Bing Chat' feature.*

    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?

    The following answer was adopted from `https://www.knowledgehut.com/blog/security/cyber-security-frameworks` *and 'Bing Chat' feature.*

    Cyber security authorization frameworks differ from one another, depending on the facts that are mentioned below. An organization should take these specifications into account when choosing a framework to follow.

    - ***Industry requirements/ Regulatory compliance*** *- Depending on the specific industry that a particular organization belongs to, the information security measures it should take into account differs. Such as procedures that must be followed by a healthcare provider may be different from that of online retail stores.*
      - *HIPAA (Health Insurance Portability and Accountability Act), sets forth requirements for protecting the privacy and security of patient health information*
      - *PCI DSS (Payment Card Industry Data Security Standard), sets forth requirements for protecting credit card data*
      - *GDPR (General Data Protection Regulation), sets forth requirements for protecting the privacy and security of personal data of EU citizens.*

- ***Operational requirements*** *- The chosen framework should provide guidelines on how to implement and manage information security controls in a way that it supports the organization's day-to-day operations.*
- ***Complexity and scale*** *- Various frameworks support varying degree of complexity and scale. The framework must be selected in a way that it matches the complexity and scale of the organization needs and functionalities.*

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

The following answer was adopted from
1. `https://goteleport.com/blog/authorization-vulnerabilities/` *and 'Bing Chat' feature.*

Common vulnerabilities that may be identified during the cyber security authorization process:

- ***Insecure direct object reference (IDOR)****: This occurs when software allows a user to access resources or perform actions without adequately verifying the resource owner.*
- ***Unprotected resources****: This occurs when resources that should be protected are left accessible without proper authorization.*
- ***Maintaining client-side authorization state****: This occurs when authorization state is maintained on the client-side, allowing attackers to manipulate it.*
- ***Directory traversal****: This occurs when an attacker is able to access restricted directories by manipulating user input.*
- ***Misconfigured access policies****: This occurs when access policies are not properly configured, allowing unauthorized access to resources.*
- ***Bypassable policies****: This occurs when policies (eg: policies based on user location, device type and etc.) can be bypassed by attackers, allowing unauthorized access to resources.*

The mentioned vulnerabilities can be addressed through below actions:

- ***Mature access control mechanisms****: Organizations must incorporate best practices such as "Zero-Trust" and principles such "Least-privilege" to control the access.*
- ***Regular assessments****: Regularly assessing of the system's user accounts and their access levels can mitigate potential risks. In addition, enforcing rules such as "Password Rotation" can be used to identify stale accounts which can become point of failures in the future.*