M5 Lab: Ownership and Permissions (Part 2)

CITA 171: OPERATING SYSTEM USE & ADMIN

Gonzalez, Marco A.
SUNY CANTON | 34 CORNELL DRIVE, CANTON, NEW YORK 13617

TABLE OF CONTENTS

1 TABLE OF FIGURES

2 TABLE OF TABLES

3 PERMISSIONS

Permissions are the operating system's security features to protect its resources, such as files and directories. In this lab, permissions applied to files and directories (**file permission and directory permissions)** are explored. Permissions can be applied to three entities:

- **Owner**
- **Group** (the members of a group)
- **Other** (who is not the owner or a group member)

A user ID (UID) is used to specify the owner, and a grou ID (GID) is used to specify the group. There are also three permission types:

- **Read (r)**
- **Write (w)**
- **Execute (x)**

Permission can be either **granted** (r, w, or x) or **denied** (-).

4 FILE PERMISSIONS

The **ls** command is used with the **-l option** to display the current permission state on a file. From the second character to the tenth character of the output are the permissions. See .

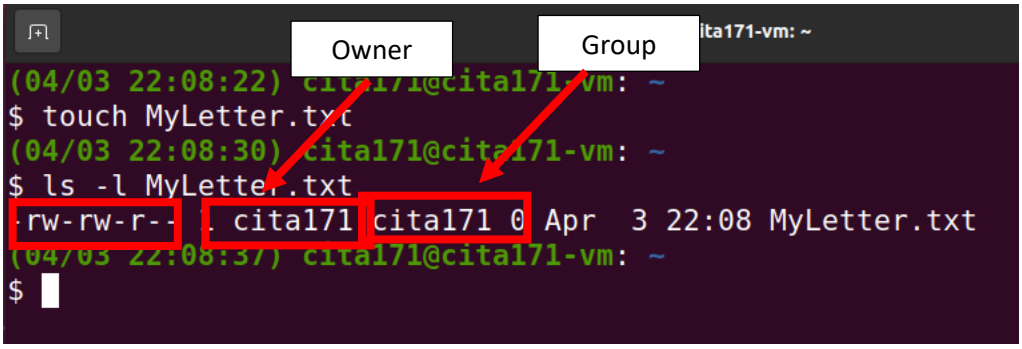

Figure 1. Displaying File Permissions

The permission rw-rw-r—are represented as follows:

Table 1. Permissions Representation Structured of rw-rw-r—

Owner	Owner	Owner	Group	Group	Group	Other	Other	Other
Read (r)	Write (w)	Execute (x)	Read (r)	Write (w)	Execute (x)	Read (r)	Write (w)	Execute (x)
Granted	Granted	Denied	Granted	Granted	Denied	Granted	Denied	Denied

4.1 READ PERMISSION

The file read permission grants the entity (the owner, the group members, or the other) to view the file contents. See Figure 2. File Read Permission Test. In this example, the owner read permission is manipulated using the **chmod** command. Note that only the owner and system administrators can change permissions.

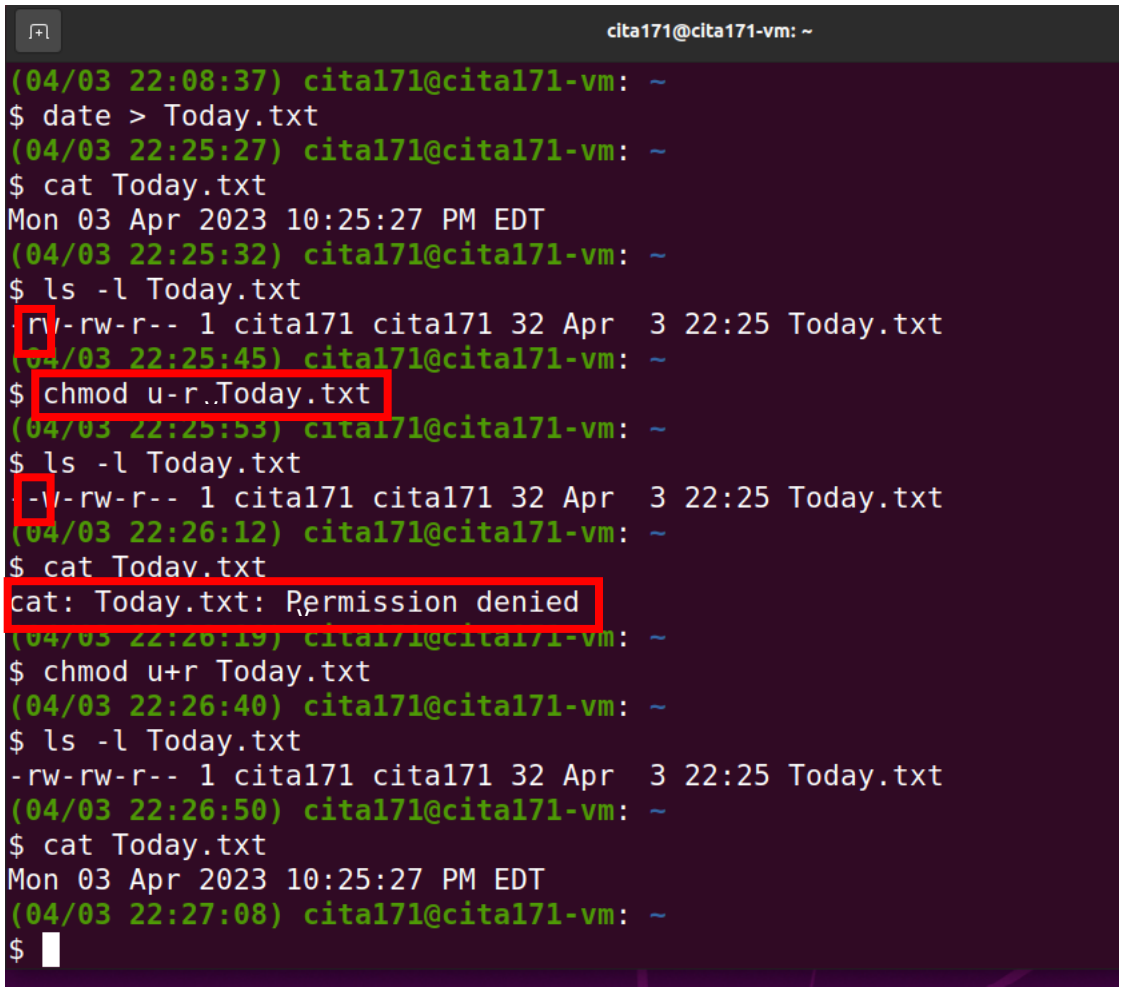

Figure 2. File Read Permission Test

The chmod command controls the owner, group, and other permissions by

Table 2. The chmod Command Entity Specifications

u	Owner
g	Group
o	Other

The command then uses the **plus sign** (+) to grant and the **minus sign** (-) to deny the read (r), write (w), and execute (x) permissions.

4.2 Write Permission

The file write permission grants the entity to modify the contents of the file. See Figure 3.

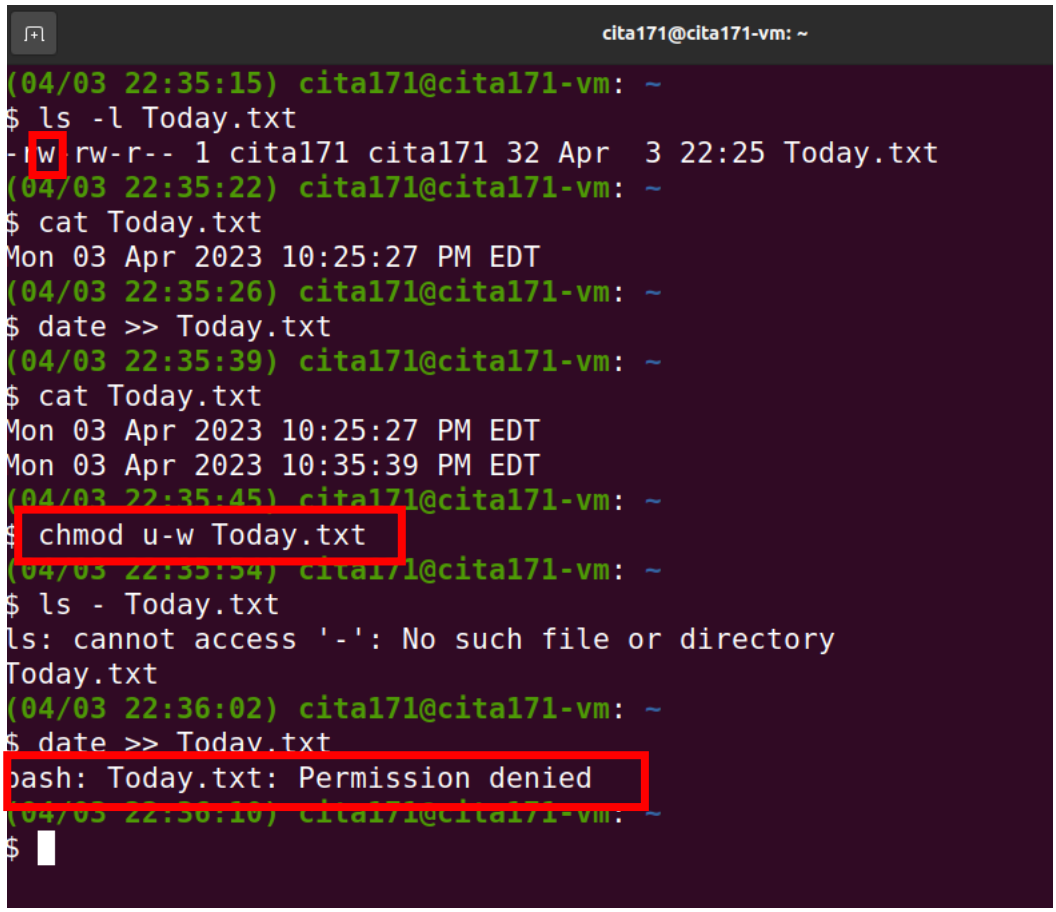

Figure 3. File Write Permission Test

4.3 Execute Permission

The file execute permission is primarily for executables files (programs). However, it is strongly recommended to deny this permission on all user document files for security reasons. This permission grants the entity to run the file to create computer processes. See Figure 4. In this example, the date command (executable file) is disabled for other users. Note that the owner of the file is root, and the group is the root group of which the cita171 is not a member. Therefore, the cita171 user is also controlled by the other permission. Because the cita171 user is not the owner, sudo command must ne used to change the permission.

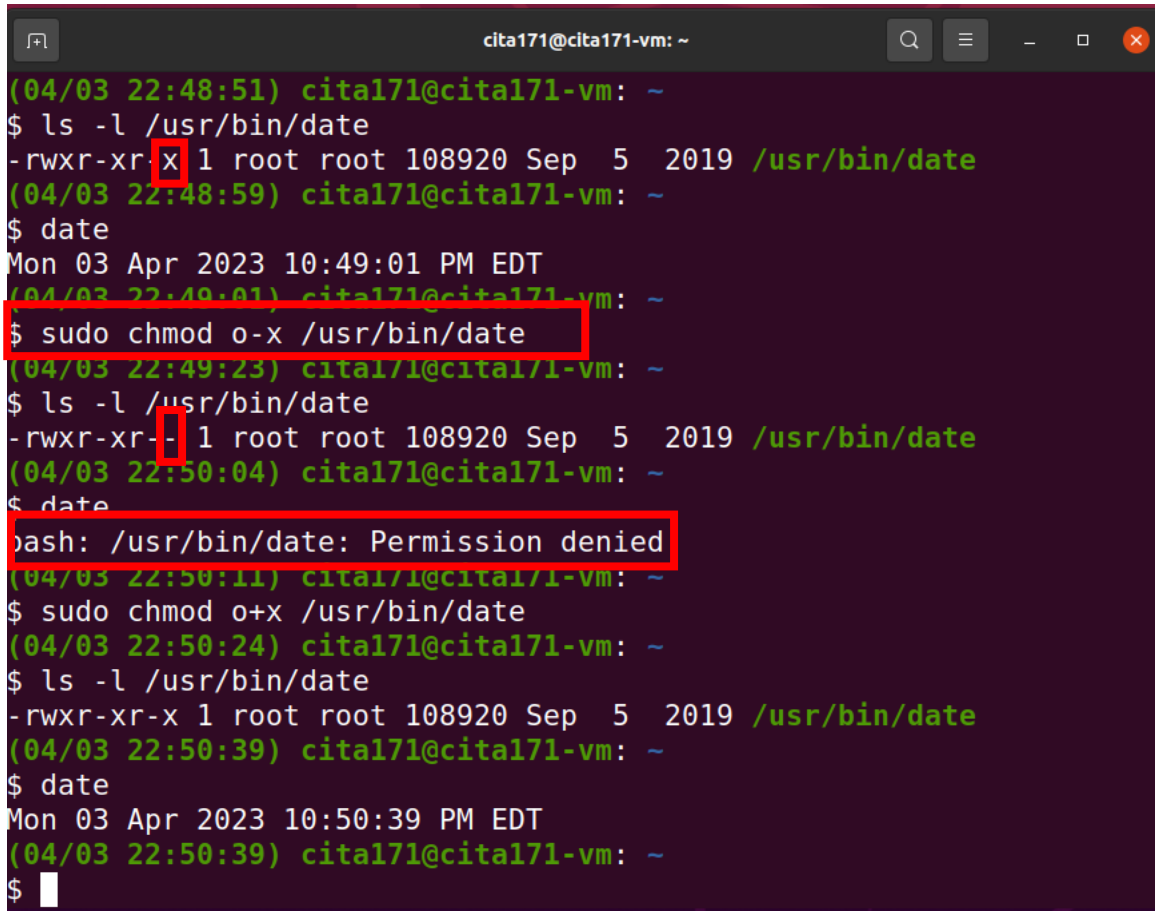

Figure 4. File Execute Permission Test

5 Directory Permissions

The read, write and execute permissions on directories work differently from on files. TO display the directory permissions using the ls command, the -ld options must be used.

5.1 Read Permission

The directory read permission grants the entity to view the directory contents. See Figure 5.

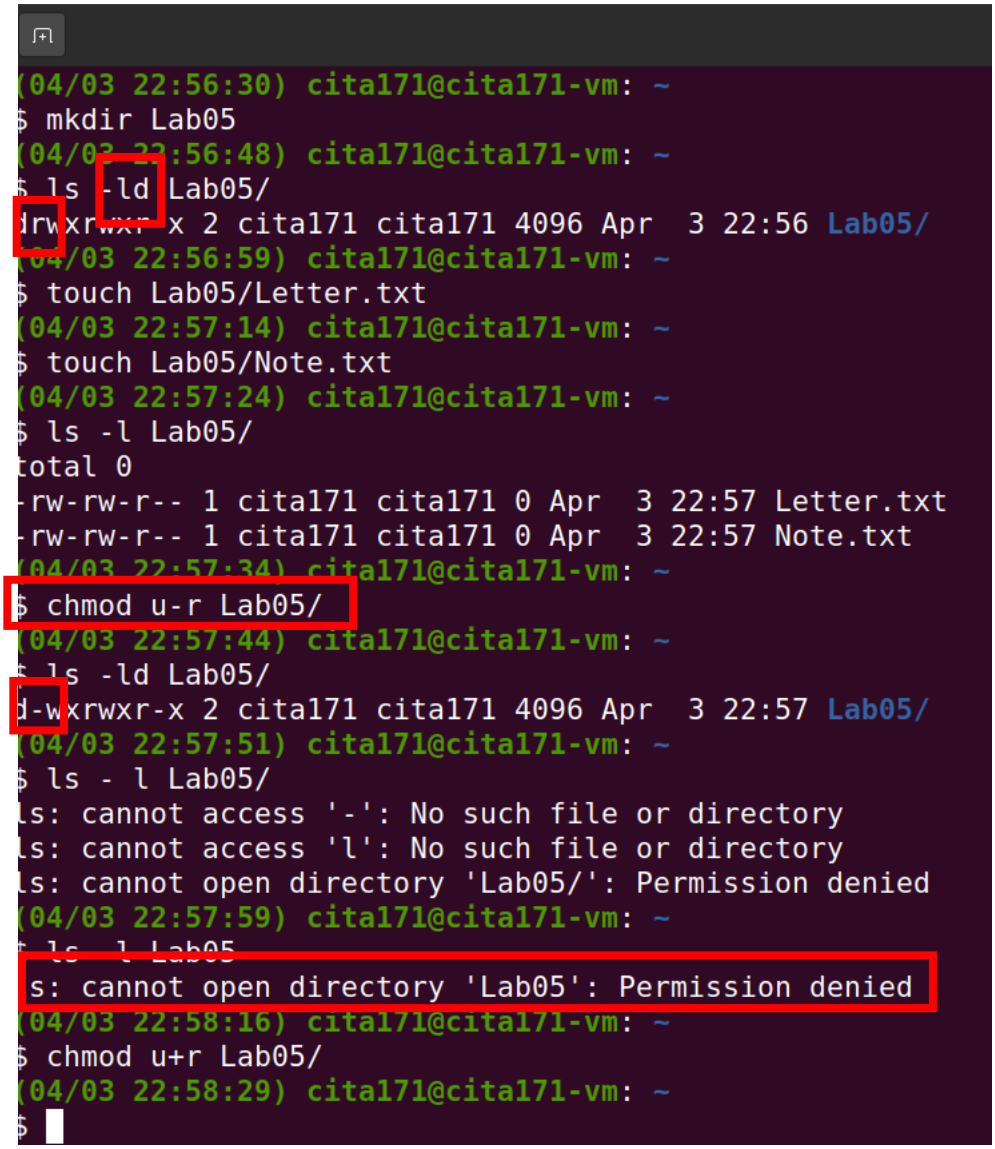

Figure 5. Directory Read Permission Test

5.2 Write Permission

The directory write permission grants the entity to perform file management operations such as creating, renaming, deleting the directory content. See Figure 6. In this example, Note.txt is renamed to Memo.txt. Then the chmod command denies the owner write permission. The owner cannot rename Memo.txt back to Note.txt. The last chmod command restores write permission.

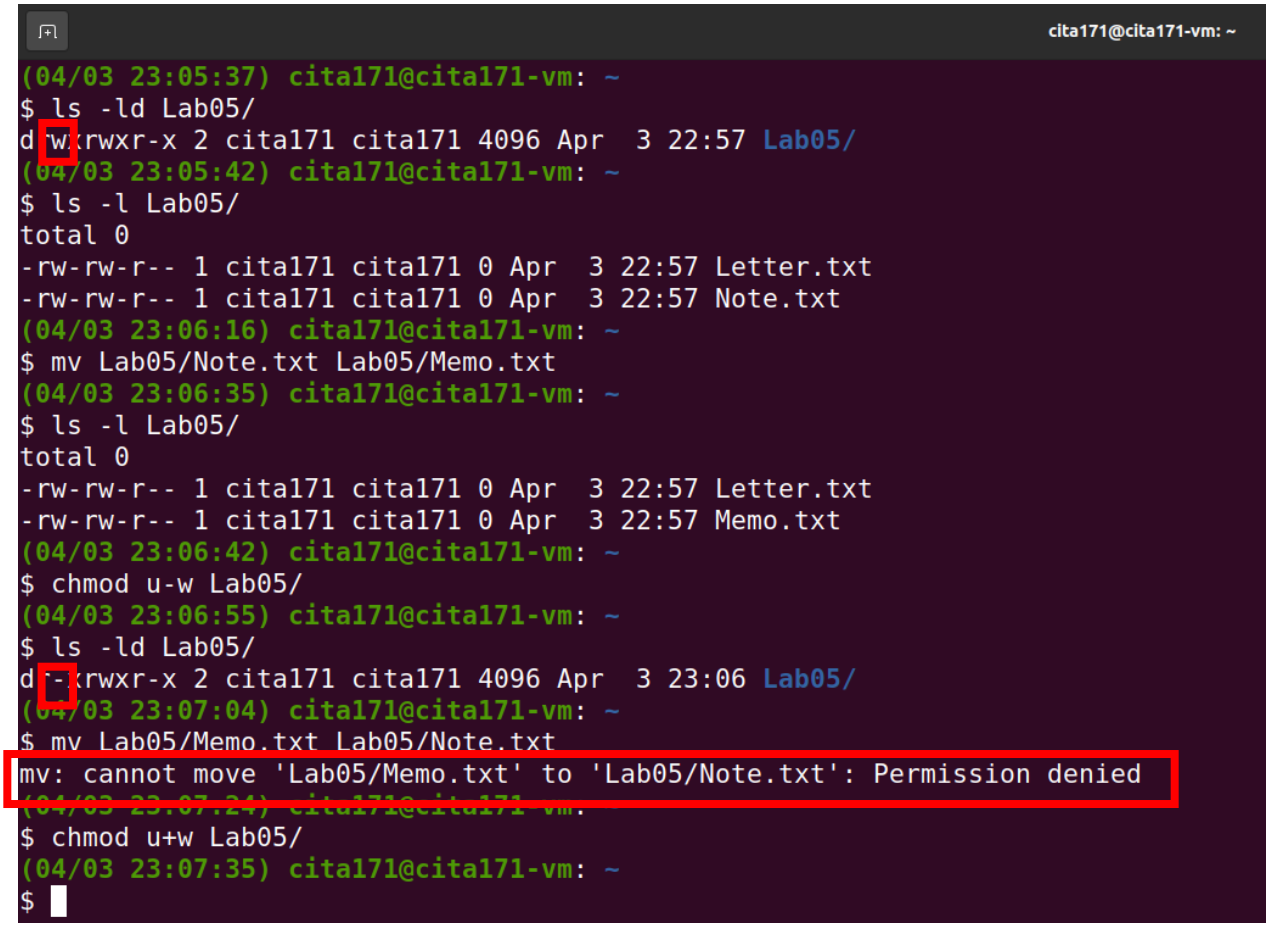

Figure 6. Directory Write Permission Test

5.3 Execute Permission

The directory execute permission grants the entity to **traverse** (walk through) the directory. See Figure 7. In this example, the cita171 user wants to change the current working directory (/home/cita171) to the Lab05 directory (/home/cita171/Lab05). The pwd command is used to check the current working directory, Notice that when the owner-execute permission is denied, the attempt to change the working directory to Lab05 is denied.

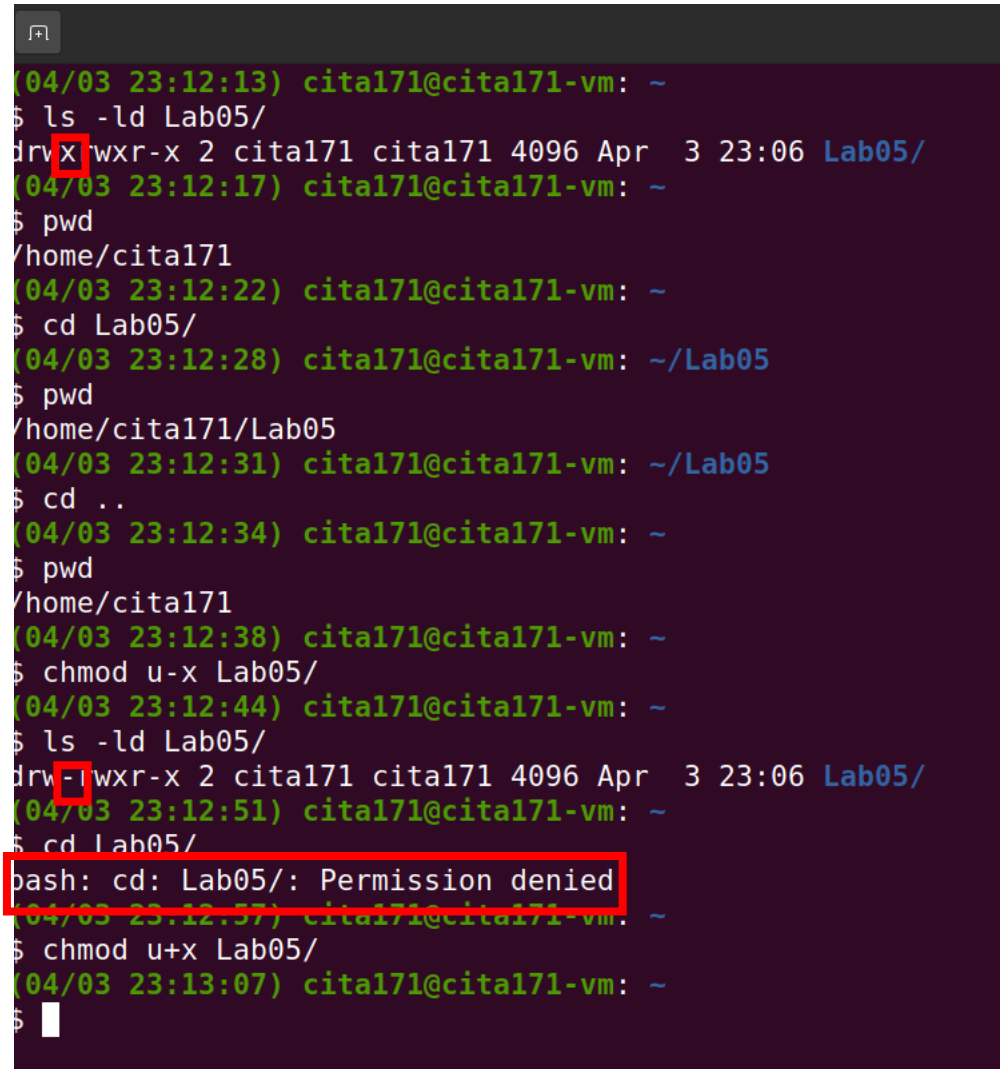

Figure 7. Directory Execute Permission Test

6 SYMBOLIC VS. NUMERIC PERMISSIONS

So far, the **symbolic method** is used to manage permissions. The symbolic method uses the following characters (symbols) such as u, g, o, r, w, x to manage permissions. There is another method called the numeric method. The numeric method uses numbers instead of symbols. See Table 3.

Table 3. Numeric and Symbolic Methods Comparison

Numeric Method	Symbolic Method	Meaning
4	r	Read Granted
2	w	Write Granted
1	x	Execute Granted
0	-	Denied

For example, show how to express rw-rw-r—numerically to 664. See Table 4.

Table 4. Numerical Permission of rw-rw-r--

Permission	Owner	Group	Other
Read	4	4	4
Write	2	2	0
Execute	0	0	0
Total	6	6	4

To allow the owner to read/write and deny all permissions from the group and the other (rw-------) numerically, 600 is used. See Table 5.

Table 5. Numerical Permissions of rw-------

Permission	Owner	Group	Other
Read	4	0	0
Write	2	0	0
Execute	0	0	0
Total	6	0	0

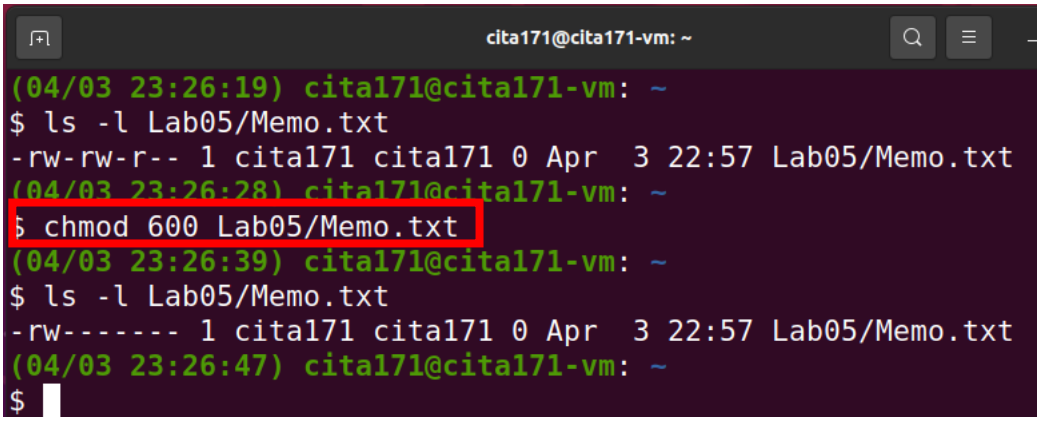

Figure 8. Using the chmod Command Numerically