# Assignment #4: Linux File Permissions [3%]

This assignment relates to the following Course Learning Requirements:

CLR 3: Work with GUI and command-line interfaces

Objective of this Assignment:

This assignment covers Linux file permissions and user management.

# Pre-Assignment Instructions:

1. Launch the VMWare Workstation and run the Ubuntu Virtual Machine instance from last week.
2. Launch the Terminal Window.
3. Read the following articles on file permissions and user mask.
   1. <https://www.guru99.com/file-permissions.html>
   2. <https://www.networkworld.com/article/3224897/whats-behind-the-linux-umask.html>

**Assignment Tasks:**

Follow the exercises by entering the commands and recording the results into the word file provided in this assignment. Once completed, upload the Word file to Brightspace.

Note: Whenever you are unsure of a command, you can look up the definition and usage using the keyword **man** (short for **manual page**) and the command name.

**Exercise #1: Testing permissions**

While logged in as a regular user, use the following command to create a directory named top in **your** user’s home directory:

**mkdir -p /home/user/lab4/top**

Follow the instructions below to complete Table #1.

1. Change the permission of the top directory using the **chmod** command. The exact command is given in the second column of the table.
2. Execute the commands listed in the first row (starting with the third column) for that permission level. For each command line document whether the command line executes successfully or not: Use PD for Permission Denied, OK for success, NF for “No such file or directory”

The commands are:

**ls -l top**

**mkdir top/sub**

**rmdir top/sub**

**cd top**

**cd .. (execute this ONLY if your current directory is top!)**

Follow the above procedure for each row of the table (row 1 to 8).

Note: Before you run each **chmod** command in the table below, make sure your current directory is ~/lab4.

**Table #1: Testing directory permissions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Row #** | **Command line to modify permissions** | **ls -l top** | **mkdir top/sub** | **rmdir  top/sub** | **cd top** |
| **1** | **chmod u+r-w+x top** | OK | PD | NF | OK |
| **2** | **chmod u-r+wx top** | PD | OK | OK | OK |
| **3** | **chmod u+rw-x top** | OK | PD | PD | PD |
| **4** | **chmod u-rw+x top** | PD | PD | NF | OK |
| **5** | **chmod u-r+w-x top** | PD | PD | PD | PD |
| **6** | **chmod u+r-wx top** | OK | PD | PD | PD |
| **7** | **chmod u-rwx top** | PD | PD | PD | PD |
| **8** | **chmod u+rwx top** | OK | OK | OK | OK |

**Default permissions**

**Exercise #2: Viewing a user's default permissions**

Login as a regular user.

Type **umask** and record the output of the command: \_0002\_\_\_\_\_\_\_\_\_\_\_\_\_

Based on the umask, what are the default permissions for directories and files in octal mode, based on your umask:

directory: \_\_\_775\_\_\_\_\_\_\_ file: \_\_\_\_664\_\_\_\_\_\_

Verify it by creating a new file with the **touch** command.

Record the default permissions set on the file in symbolic mode:

\_\_\_\_\_\_rw-rw-r--\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the default permissions set on the file in octal mode:

\_\_\_\_\_\_664\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Verify it by creating a new directory with the **mkdir** command.

Record the default permissions set on the directory in symbolic mode:

\_\_\_\_\_\_\_rwxrwxr-x\_\_\_\_\_\_\_\_\_\_\_\_

What is the default permissions set on the directory in octal mode:

\_\_\_\_\_\_\_775\_\_\_\_\_\_\_\_\_\_\_\_

**Exercise #3: Changing default permissions**

Set the **umask** to 044, record the command you use \_\_\_\_\_umask 044\_\_\_\_\_\_\_\_\_\_

Type **umask** and record the output of the command: \_\_\_\_\_0044\_\_\_\_\_\_\_\_\_

Based on the **umask**, what are the default permissions for directories and files in octal mode, based on your **umask**:

directory: \_\_733\_\_\_\_\_\_\_\_ file: \_\_\_\_622\_\_\_\_\_\_

Verify it by creating a new file.

Record the default permissions set on the file in symbolic mode:

\_\_\_\_\_rw - - w - - w -\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the default permissions set on the file in octal mode:

\_\_\_\_\_\_\_622\_\_\_\_\_\_\_\_\_\_\_\_

Verify it by creating a new directory.

Record the default permissions set on the directory in symbolic mode:

\_\_\_\_\_rwx -wx-wx\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the default permissions set on the directory in octal mode:

\_\_\_\_\_\_\_\_733\_\_\_\_\_\_\_\_\_\_\_

**Ownership**

**Exercise #4: Creating new users**

Create the two user accounts with the following commands:

**su - root**

**useradd -d /home/user1 user1 -m**

**useradd -d /home/user2 user2 -m**

**passwd user1**

Type in a password when prompted. If you do not type the username after the passwd command, you are changing the root password!

**passwd user2**

**Exercise #5: Creating shared directory**

Enter the following command

**mkdir /shared**

Who is the owner of the /shared directory? \_\_\_root\_\_\_\_\_\_\_\_\_

What is the group name of the /shared directory? \_\_\_\_root\_\_\_\_\_\_\_\_

Give full access permissions to /shared for everybody

Record the command you use: \_\_\_\_\_\_\_chmod 777 /shared\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Exercise #6: Making changes from user1**

Enter the following commands and note the outputd:

**su - user1**

Has the prompt changed to “$”?\_\_\_\_\_yes\_\_\_\_\_\_\_

**cd /shared**

**cat > plan**

Hint: Input “this is a test” at the blinking cursor. Press ctrl+d when you are done.

Who is the owner of that file? \_\_\_\_\_\_\_\_user1\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the group name of that file? \_\_\_\_\_user1\_\_\_\_\_\_\_

**chmod o-rwx /shared/plan**

Make sure that others have no access permissions. Verify with ls -l that you achieved the desired result.

**Exercise #7: Making changes from user2**

Login as user2 and try to modify the file using the following commands:

**su - user2**

**cat >> /shared/plan**

Record the message: \_\_\_\_\_\_permission denied\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Why? user2 is not a member of the group user1 and therefore has no permissions to the file “plan”

**Exercise #8: Changing file ownership**

Login as root and change the ownership of plan to user2 using the following commands:

**su - root**

**chown user2.user2 /shared/plan**

Verify that user2 is the owner of plan with command: \_\_ls -l /shared/plan\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Login as user2 and try to modify the /shared/plan. Can you do it? \_\_yeah\_\_\_\_\_

Login as user1 and try to modify the /shared/plan. Can you do it? \_\_no\_\_\_\_\_

While you are logged in as user2, try to delete the file. Can you do it (eventually)?

\_\_\_\_\_\_\_yeah\_\_\_\_\_\_\_\_\_\_\_

**Exercise #9: Minimum Permissions**

Circle (or highlight) the minimum permissions required to successfully complete the actions listed below.

To copy a file the user requires

for the source directory: R W X

for the target directory: R W X

for the file: R W X

To move a file the user requires

for the source directory: R W X

for the target directory: R W X

for the file: R W X

To delete a file the user requires

for the directory: R W X

for the file: R W X