**UNIT- II: The Linux File System, File and Directory management**

**Assignment 2.3**

1. List only text files in your current working directory (Assume text files end with extension txt)

**ls \*.txt**

1. List all subdirectories from your current working directory

**ls -d \*/**

1. List the files sorted by file size in your current working directory

**ls -lS**

1. Display the files in your current working directory with one file name per line.

**ls -1**

1. List the files in your current working directory based on last modified time

**ls -lt**

1. List all the files in your current working directory where the filename ends with a single digit. (For eg: if the file names are abc1 and abc12 then the output should display abc1 only)

**ls -1 \*[0-9]**

1. Display the files in your current working directory in the sorted order of their names (ascending order).

**ls -1**

1. Write a command to display the hidden files in the current working directory.

(Hint: hidden file names start with the symbol ‘.’)

**ls -a**

1. Create a file d1 containing the attributes of all files & directories present in the current working directory, arranged in the descending order of their size.

**ls -lS > d1**

1. Write a command to set the file permission to read-only for all the files in your cwd.

**chmod a+r \*.txt**

1. Write a command to set the file permission to write-only for group users for all the files in your cwd.

**chmod g+w \*.txt**

1. Mask the file permission bits such that all the future files are created as read-only for  
   other and group users.

**umask 007**

1. Display the details of the file /etc/passwd such as inode number, block details, and name length.

**ls-li /etc/passwd**

1. Write a command to enable write permission to group users for all the files in the current working directory. To execute this, initially create a few files without write permission to the group user.

**chmod g+w \*.txt**

1. Set the file permission bits so that all future files are created as
   1. Read-write files
   2. For user give all permission and for group and other user read only permission

**umask 000**