**Module 4:**

**Linux server - Manage user and Groups and working with file systems**

1. The default User ID (UID) for the root user, also known as the superuser, is typically 0 (zero).

2. The default User ID (UID) for system users varies depending on the distribution and configuration of the Linux system. However, system users are typically assigned UIDs in a reserved range that starts from 1 and goes up to a certain value (often 999 or 9999) or even higher.

3. The User ID (UID) for normal users, also known as regular users or non-system users, typically starts from a value greater than 1000. This range is reserved for regular user accounts to distinguish them from system users and services.

4. . Here's how you can add comments to the /etc/passwd file:

Open the /etc/passwd file in a text editor with root privileges.

Navigate to the line where you want to add a comment.

Add your comment at the beginning of the line, prefixed with a hash symbol #.

Save the changes and exit the text editor.

5. The /etc/passwd file in Linux contains essential information about user accounts configured on the system.

6. The /etc/shadow file in Linux stores encrypted password information for user accounts on the system.

7. The /etc/group file in Linux stores information about user groups on the system.

8. The /etc/gshadow file in Linux stores encrypted password information for user groups on the system. It is similar to the /etc/shadow file for user accounts but specifically for groups.

9. In Linux file permissions, the symbols "+" and "-" are used to modify the permissions of a file or directory relative to its current permissions.

Here's what they mean:

"+" (Plus Symbol):

When used with the chmod command, the plus symbol (+) is used to grant additional permissions to a file or directory.

"-" (Minus Symbol):

Similarly, when used with the chmod command, the minus symbol (**-**) is used to remove permissions from a file or directory.

10. The "r" character represents the read permission.

The "w" character represents the write permission.

The "x" character represents the execute permission.

11. To delete a user along with their home directory in Linux, you can use the userdel command with the -r or --remove option.

12. To add a new user without creating a home directory in Linux, you can use the useradd command with the -M or --no-create-home option. This option prevents the creation of a home directory for the new user.

13. To assign an account expiry date to a user in Linux, you can use the chage command, which stands for "change age" or "change expiration.

14. To add a new group in Linux, you can use the groupadd command.

15. the default permissions for files owned by the root user (superuser) typically vary depending on the specific distribution and system configuration. However, the most common default permissions for files created by the root user are:

**Readable** (r): The root user typically has read permission on files they own, allowing them to view the contents of the file.

**Writable** (w): The root user typically has write permission on files they own, allowing them to modify the contents of the file.

**Executable** (x): The root user typically does not have execute permission on regular files by default, although they can explicitly grant execute permission if needed.

16. The command used to set user ownership of a file or directory in Linux is chown.

17. To remove the password of a user in Linux, you can use the passwd command with the -d or --delete option.

18. The gpasswd command in Linux is used to administer the /etc/group file and group memberships. It allows you to manage group memberships, add or remove users from groups, and set group administrators.

19. The chage command is used to view and change user password expiry information and other password-related settings. You can use chage to set various password policy parameters.

20. The sudo command in Linux stands for "superuser do." It allows users to execute commands with the privileges of another user, typically the superuser (root), after providing their own password for authentication.