**User Management and Authentication in Linux**

Proper and secure user management is crucial in any system, especially in environments where multiple users need access to various resources. In Linux, managing individual users can be challenging, so we typically create groups and add users to those groups for easier management of permissions and access control.

**Creating a User**

When a new person joins a project, you need to create a user account for them. This user account allows them to log in and access the necessary resources.

**Command to Create a User**

**useradd <username>**

**Note:** When a user is created in Linux, a group with the same name as the username is also created by default.

**Check User Information**

**id <username>**

**Set User Password**

**passwd <username>**

**Creating a Group**

To manage users effectively, you should create groups that correspond to different teams or roles, such as a DevOps team.

**Command to Create a Group**

**groupadd <groupname>**

**Adding a User to a Group**

Once you have a user and a group, you can add the user to the appropriate group. In Linux, there are two types of groups:

* **Primary Group:** This is the default group associated with a user. Files created by the user will have this group as the group owner.
* **Secondary Group:** These are additional groups to which a user can belong, granting them additional permissions.

**Add a User to a Primary Group**

**usermod -g <groupname> <username>**

**Add a User to a Secondary Group**

**usermod -aG <groupname> <username>**

**Password-Based Authentication**

By default, Linux might disable password-based authentication. To enable it, you need to modify the SSH configuration file.

**Edit SSH Configuration**

SSH configuration is available in /etc/ssh/sshd\_config.

**vim /etc/ssh/sshd\_config**

Ensure the following line is set to yes:

**PasswordAuthentication** **yes**

**Restart SSH Service**

**systemctl restart sshd**

**Key-Based Authentication**

For enhanced security, it’s recommended to use SSH key-based authentication. This method requires users to have an SSH key pair for accessing the system.

**Steps for Key-Based Authentication**

1. **User Generates a Key Pair (On Client Machine)**

**ssh-keygen -f <file-name>**

1. **User Sends Public Key to Admin** The user sends their public key to the system administrator.
2. **Admin Creates the User**

**adduser <username>**

1. **Create a .ssh Directory**
   * Automatically, a new home directory will be created for the user:
   * **/home/<username>**
   * Admin should create a .ssh directory within the user's home directory:
   * **mkdir /home/<username>/.ssh**
   * **chmod 700 /home/<username>/.ssh**
2. **Create authorized\_keys File**
   * Create the authorized\_keys file inside the .ssh directory:
   * **touch /home/<username>/.ssh/authorized\_keys**
   * **chmod 600 /home/<username>/.ssh/authorized\_keys**
   * Open the file and paste the public key inside it.
3. **Update SSH Configuration** Ensure the following lines are present in /etc/ssh/sshd\_config:

**PasswordAuthentication** **no**

**PubkeyAuthentication yes**

1. **Restart SSH Service**

**systemctl restart sshd**

1. **Inform User to Log In** Notify the user that they can now log in to the server using their private key.