Aim: SSH Server: Password Authentication Configure SSh Server to manage a server from the remote computer, SSH Client :(Ubuntu and Windows)

SSH (Secure Socket Shell):

Secure Socket Shell, is a protocol which allow to connect securely to a remote computer or a server by using a text-based interface.

When a secure SSH connection is established, a shell session will be started, and we will be able to manipulate the server by typing commands within the client on your local computer.

System and network administrators use this protocol the most, as well as anyone who needs to manage a computer remotely in a highly secure manner.

1] To enable SSH password authentication, we must SSH in as root to edit this file:

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

2] Then, change the line

PasswordAuthentication no to PasswordAuthentication yes

3] After making that change, restart the SSH service by running the following command as root:

**sudo service ssh restart**

# To check if the client is available on your Linux-based system: Type ssh in terminal

**username@host:~$ ssh**

Run the following command to install the OpenSSH client on your computer:

**sudo apt-get install openssh-client**

Type in your superuser password when asked.Hit Enter to complete the installation.

you will need to install the OpenSSH server. Leave the terminal open and:

1] To install the SSH server:

**sudo apt-get install openssh-server ii**.

2] Enter and Y to allow the installation to continue after the disk space prompt.

The required support files will be installed, and then you can check if the SSH server is running on the machine by typing this command:

**sudo service ssh status**

3] Now edit the SSH daemon configuration file, for example, you can change the default port for SSH connections.

**sudo nano /etc/ssh/sshd\_config**

3] The configuration file will open in the editor of your choice. In this case, we used Nano.

If you need to install Nano, run this command:

**sudo apt-get install nano**

4] We need to restart SSH service every time we make any changes to the sshd\_config file:

**sudo service ssh restart**

Establish a secure remote connection with your servers. To do so:

1. Open the SSH terminal on your machine and run the following command

**ssh your\_username@host\_ip\_address**

If the username on machine matches the one on the server type:

1. **ssh host\_ip\_address**