This file is created for those users who want to login to a remote server. This file applies to both Linux and Windows operating systems. First, you should know about the basic terms like SSH, bashrc file, configuration file, keys, and for Windows, Putty. I hope this guide helps you and save your time.

Terms and Their Definations:

1. **SSH** (Secure Shell) is a cryptographic network protocol used for secure communication, remote command-line login, and remote command execution between computers.

2. The **.bashrc** file is a script that is executed whenever a new terminal session is started in interactive mode in the Bash shell. It is used to configure the shell environment, including setting environment variables, defining aliases and functions, and running initialization commands.

3. **A configuration file**, often shortened to config file, is a plain text file used to store parameters and settings for software applications. It allows users and developers to easily modify and customize how a program operates without changing the actual code. Configuration files typically contain key-value pairs or structured data that the software reads upon startup to configure its behavior according to the user's preferences or operational requirements.

4. In Linux, public and private keys are used in cryptography to secure data and authenticate users.

Public Key: A cryptographic key that can be shared openly. It is used to encrypt data or verify a digital signature. Anyone can use the public key to encrypt a message intended for the key's owner.
Private Key: A cryptographic key that is kept secret by the owner. It is used to decrypt data or create a digital signature. Only the owner can use the private key to decrypt messages encrypted with their public key or to sign documents.
Together, they form a key pair used in various security protocols, such as SSH for secure remote access and SSL/TLS for secure web browsing.

5. **PuTTY** is a free, open-source terminal emulator, serial console, and network file transfer application. It supports several network protocols, including SSH (Secure Shell), Telnet, rlogin, and raw socket connection.
Terminal Emulator: Software that emulates a terminal within a window on your computer, allowing you to interact with a remote system as if you were physically present at the machine's terminal.

Method 1 How to login Linux(Rocky-linux):

Step1:
Go to terminal in your system by pressing (Keyboard Shortcut: Press Ctrl + Alt + T)

Step2:
Use any txt editor like (vi, vim, nano,....)
first check if you have editor installed with command it shows the version, otherwise first install it.

Step3: Check if vi is installed: // its easy to use
Open a terminal and type the following command:
vi --version
vim --version

Step4: install the editor if you donot have:

sudo dnf install vim //For Rocky Linux:

sudo apt update // For Ubuntu
sudo apt install vim // For Ubuntu:

Step5:
Now type the below command in terminal and open the .ssh/config file.

----------code block----------
just paste this code with your credentials in your .ssh/config file
vi ~/.ssh/config

Add Your Host Configuration:

```
Host MyHPCLab              //Host is a nickname you give to the configuration.
   HostName IP address     //HostName is the IP address or domain of your server.
   User XXXXXXX            //User is your username on the server.
```

SET PASWORD:

Step6: Now you could login on server just type the nickname you want to use or set:
Connect Using the Nickname:
Now, you can connect to your server using the nickname you defined:

ssh MyHPCLab
after this you add your server pasword and you entered in the HPCNEXUS-Server`s world:

Step7: you can save your pasword too
Step 1: Generate SSH Keys
Open Terminal.
Generate SSH Key Pair: Run the following command and follow the prompts. Press Enter to accept the default file location and enter a passphrase if you want to add an extra layer of security (you can leave it empty for no passphrase).

ssh-keygen -t rsa -b 4096 -C "username@gmail.com"

Enter this file: // in my case i did not use the default file so i set my own file or location for keys:

/path/to folder/.ssh/my_server_key

Set a Passphrase (optional but recommended):
You will then be prompted to enter a passphrase. You can either enter a passphrase for added security or leave it empty for no passphrase.

00000000 // here you should set a pasword in numeric values any one yo want.

Step 2: Copy the SSH Key to Your Server
Copy the SSH Key: Use the ssh-copy-id command to copy your public key to the server. Replace username@x.x.x.x with your username and server IP address.

ssh-copy-id -i /home/user/.ssh/my_server_key.pub username@x.x.x.x

Step 3: Update Your SSH Config File
Edit SSH Config File:

vi ~/.ssh/config

Add Your Host Configuration:

Host MyHPCLab
HostName IP address
User username
IdentityFile /home/user/.ssh/my_server_key

Step 4: Connect to Your Server
Now, you can connect to your server without entering the password:

ssh MyHPCLab

when it requires a password to unlok key enter:
00000 // enter that pasword you set when you genrated the keys.

its successfully working:
just type

ssh MyHPCLab

hurrrrryyyyyy

Method2:

Step 1:
OPen the terminal and open the file .bashrc with the help of below command
vi ~/.bashrc

Step 2:
now set your alias like as shown in below command.

alias MyHPCLab='ssh username@x.x.x.x'

Step 3:
just paste this command at the end of file.
then press ESC button, then press [:wq] for save and quit.

Step 4:
reload the changes type below command in terminal.
source ~/.bashrc

Step 5:
Connect Using the Alias:
Now you can connect using the alias:

MyHPCLab

End of settings for Linux

How to Login on server if you are Window user

Step 1: Installing PuTTY on Linux (Ubuntu).

Update the package list:
sudo apt update
Install PuTTY:

Step 2:
sudo apt install putty
putty //Verify installation by running

---------- If you are used the Rocky Linux then use these below commands:
Rocky Linux uses yum or dnf for package management. PuTTY might not be available in the default repositories, so you might need to enable the EPEL repository.

Step 1:
Installing PuTTY on Rocky Linux Using dnf
Enable the EPEL (Extra Packages for Enterprise Linux) repository mentioned in step 2.

Step 2:
sudo dnf install epel-release // Update the package list

Step 3:
sudo dnf update

Step 4: Install PuTTY:
sudo dnf install putty

Step 5:
Verify the installation:

putty

---------- Putty installed ----------

Time to login on server with putty ----------

Once you have PuTTY installed on your Windows machine, you can use it to connect to a remote server via SSH. Here's a step-by-step guide on how to connect to a server using PuTTY.

1. Open PuTTY
Locate and open PuTTY from your Start menu or desktop shortcut.

2. Configure the Connection
Host Name (or IP address): Enter the IP address or hostname of the server you want to connect to. For example, if your server's IP is 192.168.1.1, you would enter 192.168.1.1.
Port: Enter the port number for the SSH connection. By default, this is 22, but it could be different if your server is configured to use a different port.
Connection Type: Ensure that "SSH" is selected. This is typically the default. Here's an example of the settings:

Host Name (or IP address): 192.168.1.1
Port: 22
Connection Type: SSH
---

3. Save the Session (Optional)
You can save your settings for future use by entering a name in the "Saved Sessions" box and clicking "Save". This way, you won't need to re-enter the details every time you connect.

4. Connect to the Server
Click the "Open" button at the bottom of the PuTTY window. This will start the connection process.

5. Login
A terminal window will open. If this is your first time connecting to this server, you might see a security alert asking if you trust the host. Click "Yes" to proceed.

You will be prompted to enter your username. Type your username and press Enter.

Next, you will be prompted to enter your password. Type your password and press Enter. Note that you won't see the password characters as you type them for security reasons.

---------- **Finished** ----------