**SSH Commands**

**STEP 1: Ensure Both Systems Have SSH Tools Installed**

**On Fedora (my computer):**

Check if the SSH client is installed:

ssh -V

Output should be like: OpenSSH\_9.x

If not installed, run:

sudo dnf install openssh-clients

**On the Remote Computer (Target):**

Install and enable SSH server:

sudo dnf install openssh-server

sudo systemctl enable sshd

sudo systemctl start sshd

Verify it's running:

sudo systemctl status sshd

**STEP 2: Open SSH Port on the Remote Computer**

Enable SSH through the firewall:

sudo firewall-cmd --permanent --add-service=ssh

sudo firewall-cmd --reload

**STEP 3: Create a New User on the Remote Computer (if needed)**

If the user account you want to SSH into **doesn't exist**, create it:

sudo adduser yourusername

sudo passwd yourusername

Replace yourusername with the name you want (e.g., john).

**STEP 4: Find the Remote Computer’s IP Address**

On the remote system:

ip a

Look for inet under a network adapter (like eth0 or wlan0). It should look like 192.168.1.x.

**STEP 5: Generate SSH Key Pair on Your Fedora System**

On **your Fedora computer** (client):

ssh-keygen -t rsa -b 4096

* When asked for a location, press Enter to use default: ~/.ssh/id\_rsa
* You can press Enter again for no passphrase, or enter one if you want additional protection

This creates:

* ~/.ssh/id\_rsa (private key)
* ~/.ssh/id\_rsa.pub (public key)

**STEP 6: Set Proper Permissions for SSH Keys**

Still on Fedora:

chmod 700 ~/.ssh

chmod 600 ~/.ssh/id\_rsa

chmod 644 ~/.ssh/id\_rsa.pub

**STEP 7: Copy Public Key to the Remote Machine**

**Option A (Easy Way): Using**

**ssh-copy-id**

ssh-copy-id yourusername@remote\_ip

Example:

ssh-copy-id john@192.168.1.5

You'll be prompted for the remote user’s password once.

This adds your public key to /home/yourusername/.ssh/authorized\_keys on the remote system.

**Option B (Manual Way)**

1. View your public key on Fedora:

cat ~/.ssh/id\_rsa.pub

1. On the remote system (login using password):

ssh yourusername@remote\_ip

1. On the remote system, create .ssh directory:

mkdir -p ~/.ssh

chmod 700 ~/.ssh

1. Add your key:

nano ~/.ssh/authorized\_keys

Paste the public key content here, save and close.

1. Set permissions:

chmod 600 ~/.ssh/authorized\_keys

Make sure the ownership is correct:

chown -R yourusername:yourusername ~/.ssh

**STEP 8: Test Passwordless SSH Login**

On your Fedora system, run:

ssh yourusername@remote\_ip

You should now log in **without entering a password**!

**STEP 9: Disable Password Login on Remote System (For Security)**

Edit SSH config on the remote system:

sudo nano /etc/ssh/sshd\_config

Find and modify/add these lines:

PasswordAuthentication no

PubkeyAuthentication yes

Then restart SSH service:

sudo systemctl restart sshd

⚠️ **Make sure your SSH key login works first**, or you’ll be locked out.

**Final Test**

Back on your Fedora system:

ssh yourusername@remote\_ip

* Should log in directly with no password.
* You can now run remote commands or even copy files using scp.