St. JOSEPH'S
GROUP OF INSTITUTIONS
OMR, CHENNAI - 119

Placement Empowerment Program

Cloud Computing and DevOps Centre

Set Up SSH Key-Based Authentication LocallyGenerate an SSH key pair and configure it for passwordless login between two local machines or VMs.

Name: Monisha J R **Department : CSE**

St. JOSEPH'S COLLEGE OF ENGINEERING | St. JOSEPH'S INSTITUTE OF TECHNOLOGY
AUTONOMOUS INSTITUTIONS, AFFILIATED TO ANNA UNIVERSITY

Introduction :

SSH (Secure Shell) key-based authentication is a secure method of accessing remote machines without using passwords. By generating an SSH key pair, users can log in seamlessly to another machine while improving security and reducing the risks associated with password-based authentication.

Overview :

This task involves setting up SSH key-based authentication between two local machines or virtual machines (VMs). The process includes generating an SSH key pair, copying the public key to the target machine, and verifying passwordless login. Optionally, we can further secure SSH by disabling password authentication on the remote machine.

Objectives :

1. Understand the concept of SSH key-based authentication.
2. Generate an SSH key pair on the client machine.
3. Transfer the public key to the remote machine.
4. Establish a secure, passwordless SSH connection.
5. (Optional) Enhance security by disabling password-based authentication.

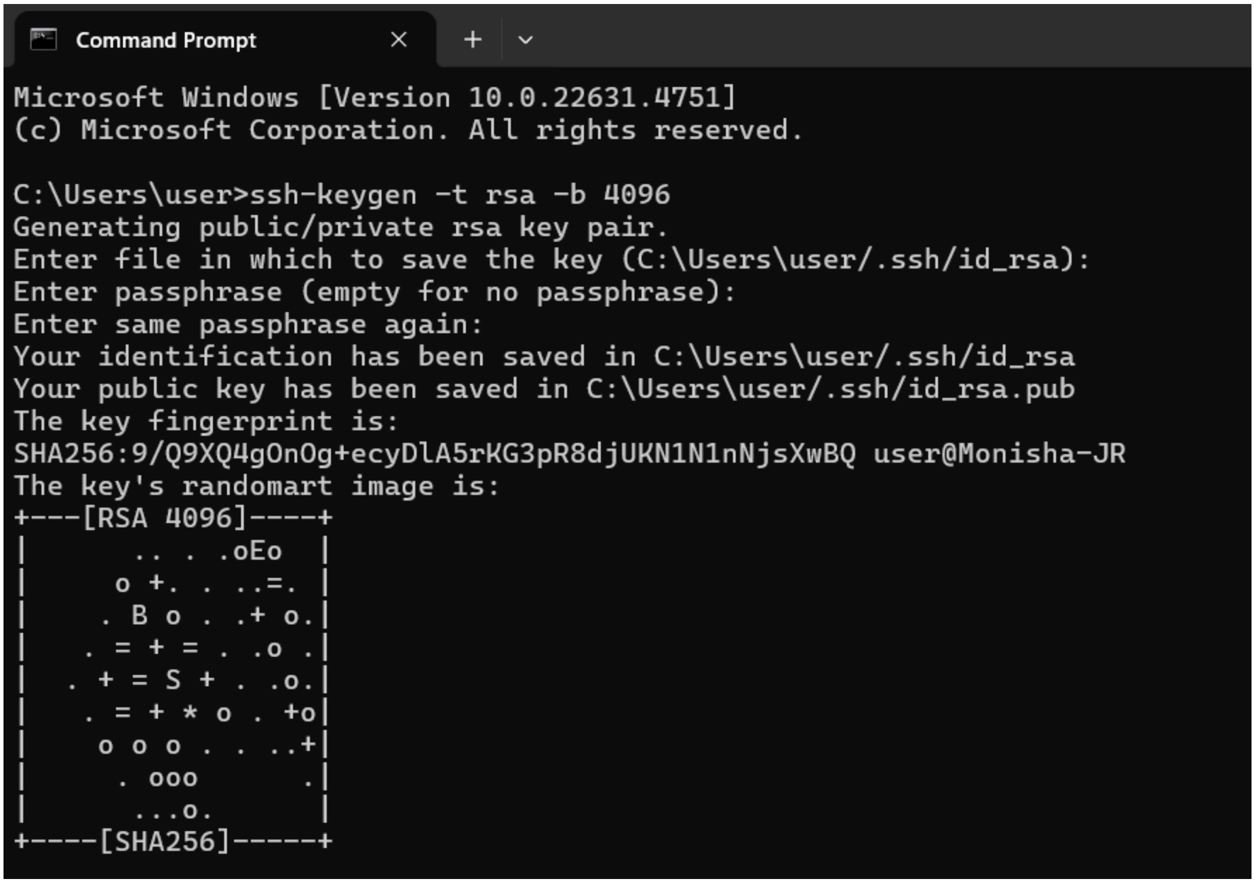
Step by Step Overview :

Step 1: Generate an SSH Key Pair

1. Open a terminal on the **client machine** (the machine you will use to connect to the remote system).
2. Run the following command to generate an SSH key pair:

```
ssh-keygen -t rsa -b 4096
```

3. When prompted, press Enter to save the key in the default location (~/.ssh/id_rsa).
4. If asked for a passphrase, you can leave it empty for passwordless authentication or set a passphrase for added security.



```
Microsoft Windows [Version 10.0.22631.4751]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\user/.ssh/id_rsa
Your public key has been saved in C:\Users\user/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:9/Q9XQ4gOnOg+ecyDlA5rKG3pR8djUKN1N1nNjsXwBQ user@Monisha-JR
The key's randomart image is:
+---[RSA 4096]----+
|      .. . .oEo  |
|     o +. . ..=. |
|    . B o . .+ o.|
|   . = + = . .o .|
|  . + = S + . .o.|
|   . = + * o . +o|
|    o o o . . ..+|
|     . ooo      .|
|      ...o.      |
+----[SHA256]-----+
```

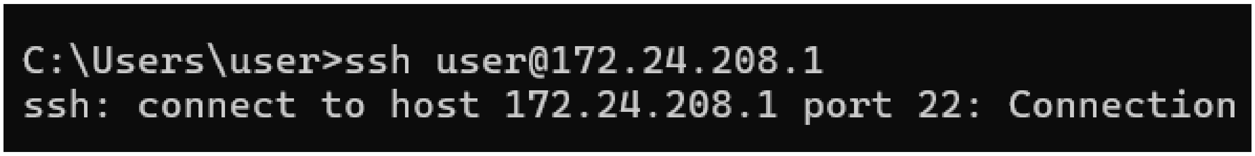
Step 2: Copy the Public Key to the Remote Machine

1. Use the following command to copy the public key to the remote machine (or second local machine/VM):

ssh-copy-id username@remote_machine_ip

Replace username with the actual username on the remote machine and remote_machine_ip with its IP address.

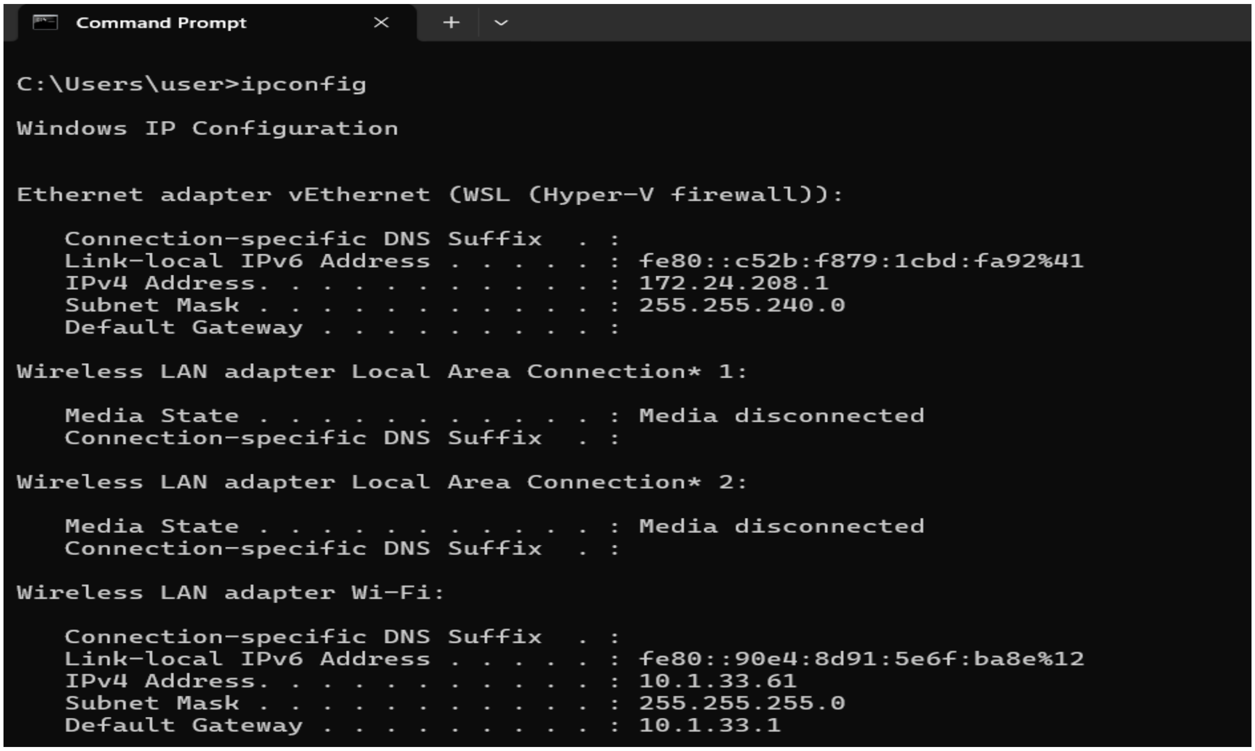
2. If prompted, enter the password of the remote machine’s user.



```
C:\Users\user>ssh user@172.24.208.1
ssh: connect to host 172.24.208.1 port 22: Connection
```

3. To check the ip address run :

ipconfig



```
C:\Users\user>ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (WSL (Hyper-V firewall)):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c52b:f879:1cbd:fa92%41
   IPv4 Address. . . . . . . . . . . : 172.24.208.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::90e4:8d91:5e6f:ba8e%12
   IPv4 Address. . . . . . . . . . . : 10.1.33.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.33.1
```

Step 3: Test SSH Login

1. Try logging in to the remote machine without entering a password:

```
ssh username@remote_machine_ip
```

2. If successful, SSH will log in without asking for a password.

Outcome :

✅ Successfully log in to the remote machine without entering a password.

✅ Improve security by eliminating the risk of password compromise.

✅ Gain a deeper understanding of SSH authentication mechanisms.

✅ Be able to securely manage remote systems with key-based authentication.