Instructor: M. Ahsan

SSH Key-Based Authentication in Linux

You might have questions in your mind such as what is SSH and SSH key-based authentication. In this blog I will try to answer these questions and I will show how we can generate SSH keys for password-less login into remote machines.

What is SSH?

SSH , also know as Secure Shell , is a network protocol that helps transfer data securely between a client and a server over public networks such as the internet. It is based on Asymmetric Cryptography. During data transfers between the client and server, the authenticity plays an important role and SSH provides us with such authentication mechanisms. SSH is used for encrypted data communications between Computers. System Administrators use SSH for managing systems and applications remotely. An SSH server, by default, listens on the standard Transmission Control Protocol (TCP) port 22.

Installing SSH Server:

First of all, make sure you have two machines available. If not, you can use a virtual machine on your host machine. You can find a tutorial on how to install a Virtual Machine by opening this link.

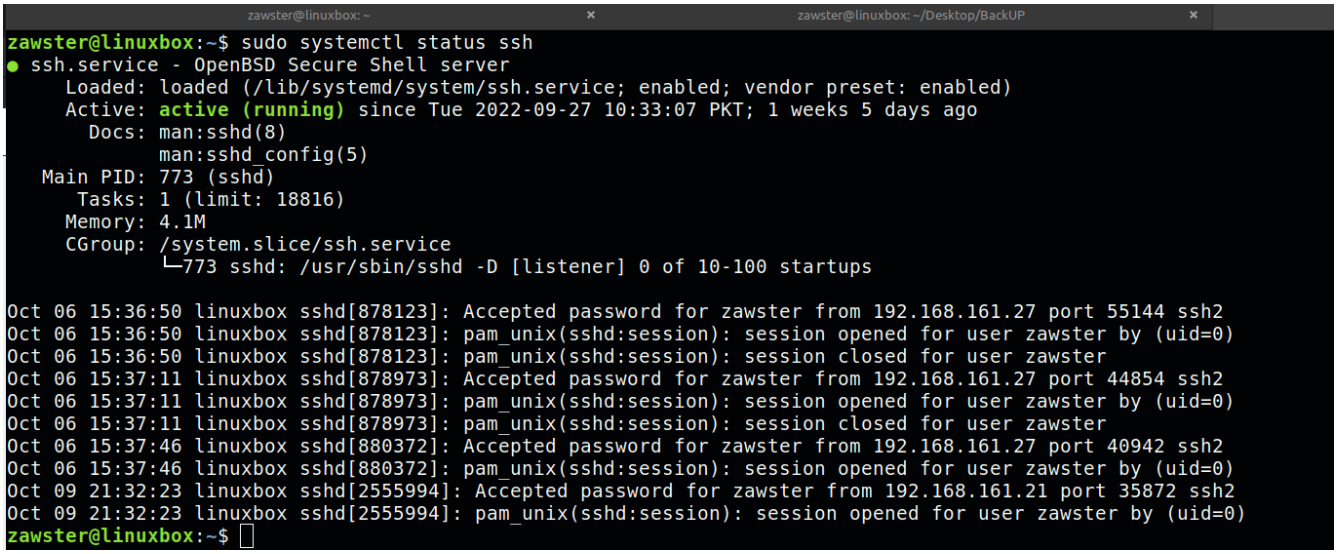
Next, we need to ensure that we have SSH server installed in both our machines. Use the following commands to install an SSH server:

```
sudo apt update
sudo apt install openssh-server
```

Next, check the status of SSH server to make sure that our SSH server is successfully installed and running.

```
sudo systemctl status ssh
```

```
If you see an output like the one below, so you are good to go and move ahead.
```



Checking Network Connection:

Next task is to find the IP addresses of both machines and ping them so as to make sure our connection is successfully established.

For finding IP address:

```
ifconfig
```

Now, ping the IP address of remote machine in the local machine, and vice versa. If both machines are pinging successfully so we can move ahead.

SSH into Remote Machine:

Next, in your local machine give the ssh user@youripaddress command to SSH into the remote machine. This will give us access to the remote machine but it will ask us for a password of the remote machine.

```
ssh zawster@192.168.1.11
```

In the above command zawster is the user name of my remote machine and 192.168.1.11 is the IP address of my remote machine. Next, exit from the machine so as to enter back to your local machine and generate keys for password-less login.
To exit the connect run exit command.

Generating SSH key pair for Password-less Login

To generate keys use the command:

```
ssh-keygen
```

This will generate a pair of keys for you and ask for the location where you want to store the keys. I've used the default location. In order to view the keys, navigate in to the /home/user/.ssh directory and view the files.

```
cd ~/.ssh
ls -la
```

You need to copy your public key to the remote machine using the following command:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub zawster@192.168.1.11
```

The above command will copy the key to the remote machine and you are done with the whole process. Now we can have access to our remote machine without using passwords.

Testing:

In order to test if your password-less login works or not, try to SSH into the remote machine again and this time it won't ask you for a password:

```
ssh zawster@192.168.1.11
```

To view the key that you copied to the remote machine, navigate into the ~/. ssh/authorized_keys directory. Use the command below:

```
cd ~/. ssh/authorized_keys
```

The authorized key directory contains a list all the public keys.