**Steps to troubleshoot SSH (Secure Shell)**

1. **Verbose Output**

Use the below command to analyse where the fault is in SSH.

*ssh -vvv -l <username> <host\_ip\_address>*

1. **Check logs**

You can use the below command to find some information about the problem.

*cat /var/log/auth.log*

1. **Change SSH access in /etc/hosts.deny file**

You have to keep this empty if you want anyone to connect to your host using ssh or restrict the ip who are allowed to connect to this host using ssh.

*# sshd: ALL*

1. **Allow SSH access in /etc/hosts.allow file**

To allow any user to connect to your host computer using ssh add the below line in the file

*sshd: ALL*

1. **Disable Firewall / Add SSH rule in the Firewall**

Use the below command to disable the Firewall.

*ufw disable*

To add the ssh rule to the Firewall use the below command.

*ufw allow ssh*

1. **Enable PasswordAuthentication**

You have to enable the PasswordAuthentication rule in the /etc/ssh/sshd\_config file to enable the user to enter password to login.

*PasswordAuthentication yes*

1. **Check allowusers & allowgroups rule**

The user should be the owner of his home directory and group owner of his home directory (in case if allowgroups is not commented out)

**Case 1 :** User is both owner and group owner of his directory

*allowusers mohamed-tt0567*

*allowgroups mohamed-tt0567(same as username)*



**Case 2 :** User is owner but not group owner of his directory

*allowusers mohamed-tt0567*

*# allowgroups mohamed-tt0567*