Agenda: SSH

Configuring Server for SSH

1. Identify one server machine. Install openssh-server.

   sudo apt-get install openssh-server

   If error occurs do the following:

   sudo rm /var/lib/apt/lists/lock

   sudo rm /var/cache/apt/archives/lock

   sudo rm /var/lib/dpkg/lock

2. Check whether the service is on.

   sudo service ssh status

   (if it is off, sudo service ssh start, else do nothing)

3. Identify the ip address of the server machine. Write it down.

   Ifconfig | grep "inet addr"

4. Create a file named one.txt in the server with some contents

   cat > one.txt

5. Display the contents of the file

6. Set the date and time as 10-03-2018 9:00 AM in the server

   sudo date - -set 10 Mar 2018 09:00:00 AM

7. Display the date and check

Configure Client and establish Remote Connection with password

1. In your client machine, install openssh-client.

   sudo apt-get install openssh-client

2. To connect to the server remotely

   ssh usename@server-ip

3. It asks for password

4. Give password to connect

5. Once connected you can access the server files at your machine

6. Execute the following basic commands

   Cat one.txt

   Date

   Cal

   Who

   Echo $HOME

7. Try copying the file one.txt to your home directory

   Scp student@server-ip:/home/student/one.txt   student@client-ip: /home/student

8. What difficulty you face?

9. Was the file copied?

10. Try installing some package from your remote machine into the server.

11. Was it done? Check in the server.

Create SSH keys?

1. Check for the ssh-keys

2. Ls /home/student/.ssh/
3. Check whether ssh keys are present
4. If present you can directly do copying of key into the server by going to step 11
5. If not, generate the keys [follow steps 6 to 9]
6. **ssh-keygen**
7. Enter file in which to save the key (/home/demo/.ssh/id_rsa): <press enter>

   [It will store the file in .ssh hidden directory]
8. Enter passphrase (empty for no passphrase):   <it is optional. Give a string or just press enter>
9. Enter same passphrase again:

   [If you want to Generate ssh keys with larger number of bits

   ssh-keygen -b 4096

   Overwrite (y/n)? y]
10. Copy the client's public key into the server
11. Check the generated keys – **ls /home/student/.ssh**
12. **ssh-copy-id -i /home/student/.ssh/id_rsa.pub <Server-ip>**
13. exit

Remote Connection without password

1. Copy the client public key into the server
2. Now connect to the server
3. It will not ask password.
4. Check with some commands that you have done already
5. Check with copying of a file with scp.
6. Install the openssh-server in the client machine also
7. Now try copying the file from client to server with scp command
8. Can you able to copy now?
9. Check whether the file is copied?