1. ***SSH is a cryptographic network protocol used for secure connection between a client and a server and supports various authentication mechanisms.***
2. ***The two most popular mechanisms are passwords based authentication and public key based authentication.***
3. ***Now, we will see how to setup an SSH key-based authentication as well how to connect to our Linux server without entering a password***

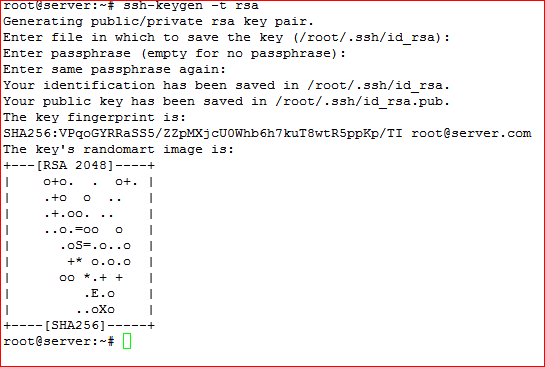
*192.168.72.80 : Address of client.*

*192.168.92.81 : Address of remote side.*

***Now Create Authentication SSH-Kegen Keys on Address of client...;;;;;***

*ssh-keygen -t rsa {for generating ssh key}*

*enter 3 times will show output like below.*

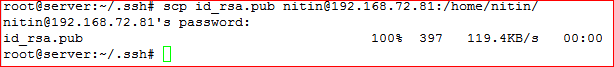


*Then show the hidden file by the Command """"(ls -a)""""*

*cd .shh*

*Shown a file* ***id\_rsa.pub , now send file to the remote side by below command...***

*scp id\_rsa.pub nitin@192.168.72.81:/home/nitin/*



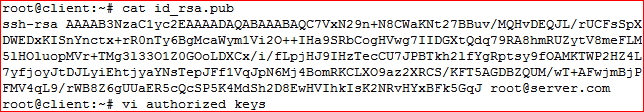
***Now at client side....;;;***

***Move file at home directory and make a file named authorized\_ke ys***

*mv /home/nitin/id\_rsa.pub /root*

*ls -ltr*

cat id\_rsa.pub



***Copy key and paste in authorized\_keys***

*ls -ltr*

***Create .ssh file manually....,,,***

*mkdir .ssh*

*cd .ssh*

*vi authorized\_keys*

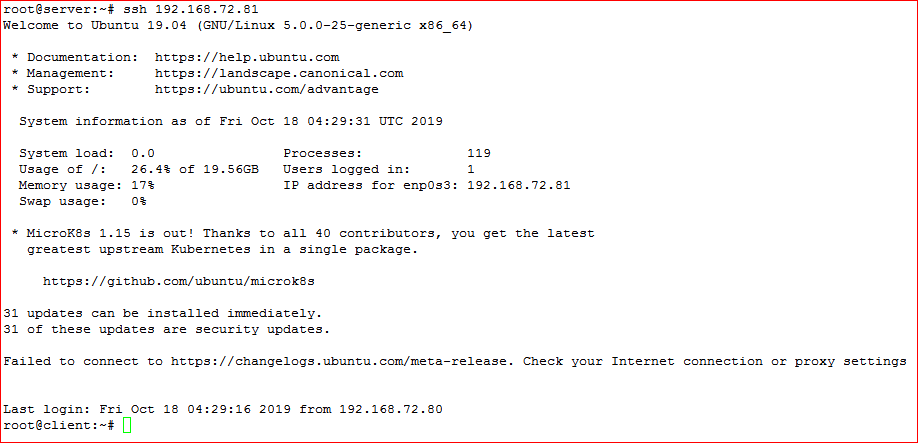
***paste the key and save file....,,,,,,***

*chmod 640 authorized\_keys*

***Now check....,,,***

*ssh 192.168.72.81*

*you will log in with entering the password for first time then after no need of password...*

**