## **Steps to Configure SSH Key-Based Authentication**

Step 1:- Logged in to Server A and created ssh key

```
Toot@ServerA:-# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.
Your passphrase again:
Your p
```

Step 2:- We need to copy the Public Key from server A



Step 3 :- We need to create /.ssh file in server B and need to give 700 file permission to the same file

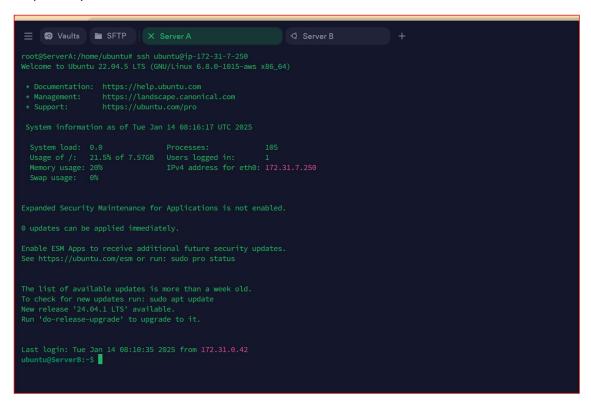


## Step 4:-Take Server B access and write below commands

echo "(paste\_the Server A\_public\_key\_here)" >> ~/.ssh/authorized\_keys and give below permission to file :- /.ssh/authorized\_Keys

chmod 600 ~/.ssh/authorized\_keys

Step 5:- Try to access ServerB from ServerA



Note:-1)We can access Server B from Server A, but not vice versa

2) We need to copy the Public keys for connection not an Private