Step 1: Create Authentication SSH-Kegen Keys on – (192.168.0.12)

First login into server 192.168.0.12 with user tecmint and generate a pair of public keys using following command.

**[tecmint@tecmint.com ~]$ ssh-keygen -t rsa**

Generating public/private rsa key pair.

Enter file in which to save the key (/home/tecmint/.ssh/id\_rsa): [Press enter key]

Created directory '/home/tecmint/.ssh'.

Enter passphrase (empty for no passphrase): [Press enter key]

Enter same passphrase again: [Press enter key]

Your identification has been saved in /home/tecmint/.ssh/id\_rsa.

Your public key has been saved in /home/tecmint/.ssh/id\_rsa.pub.

The key fingerprint is:

5f:ad:40:00:8a:d1:9b:99:b3:b0:f8:08:99:c3:ed:d3 tecmint@tecmint.com

The key's randomart image is:

+--[ RSA 2048]----+

| ..oooE.++|

| o. o.o |

| .. . |

| o . . o|

| S . . + |

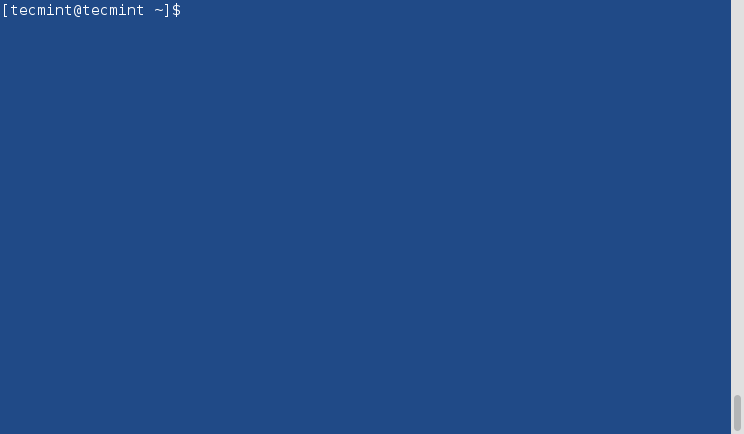
| . . . o|

| . o o ..|

| + + |

| +. |

+-----------------+

[](https://www.tecmint.com/wp-content/uploads/2012/10/Create-SSH-RSA-Key.gif)

*Create SSH RSA Key*

Step 2: Create .ssh Directory on – 192.168.0.11

Use SSH from server 192.168.0.12 to connect server 192.168.0.11 using sheena as user and create .sshdirectory under it, using following command.

**[tecmint@tecmint ~]$ ssh sheena@192.168.0.11 mkdir -p .ssh**

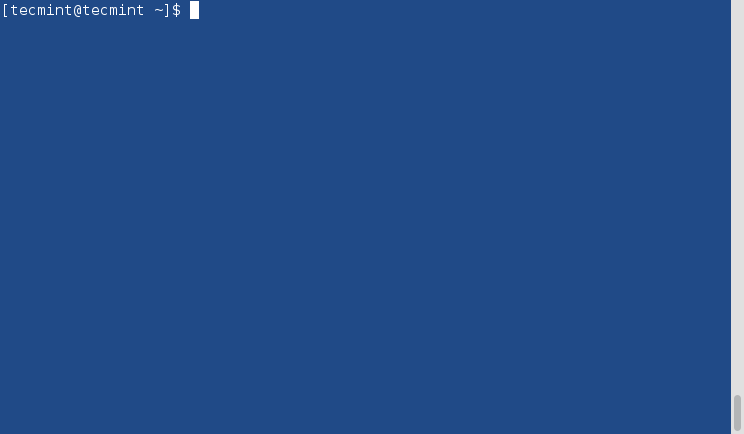
The authenticity of host '192.168.0.11 (192.168.0.11)' can't be established.

RSA key fingerprint is 45:0e:28:11:d6:81:62:16:04:3f:db:38:02:la:22:4e.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '192.168.0.11' (ECDSA) to the list of known hosts.

**sheena**@192.168.0.11's password: [**Enter Your Password Here**]

[](https://www.tecmint.com/wp-content/uploads/2012/10/Create-SSH-Directory.gif)

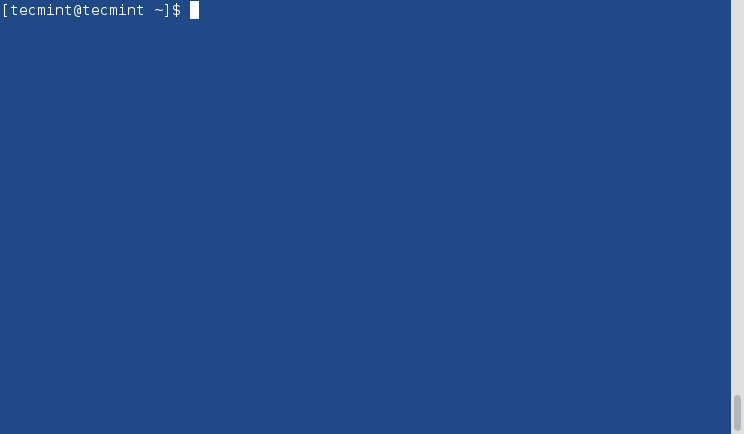
*Create SSH Directory Under User Home*

Step 3: Upload Generated Public Keys to – 192.168.0.11

Use SSH from server 192.168.0.12 and upload new generated public key (id\_rsa.pub) on server 192.168.0.11under sheena‘s .ssh directory as a file name authorized\_keys.

**[tecmint@tecmint ~]$ cat .ssh/id\_rsa.pub | ssh sheena@192.168.0.11 'cat >> .ssh/authorized\_keys'**

**sheena**@192.168.1.2's password: [**Enter Your Password Here**]

[](https://www.tecmint.com/wp-content/uploads/2012/10/Upload-RSA-Key.gif)

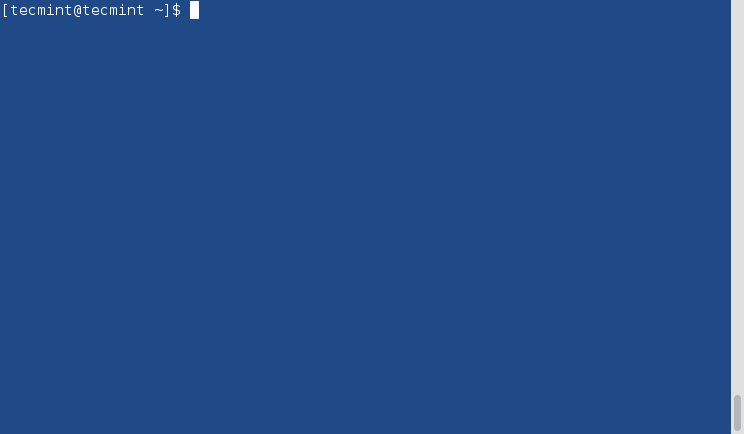
*Upload RSA Key*

Step 4: Set Permissions on – 192.168.0.11

Due to different SSH versions on servers, we need to set permissions on .ssh directory and authorized\_keys file.

**[tecmint@tecmint ~]$ ssh sheena@192.168.0.11 "chmod 700 .ssh; chmod 640 .ssh/authorized\_keys"**

**sheena**@192.168.0.11's password: [**Enter Your Password Here**]

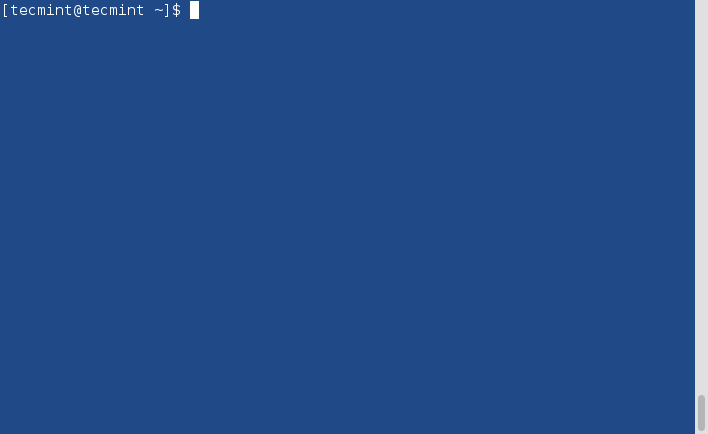
[](https://www.tecmint.com/wp-content/uploads/2012/10/Set-Permission-on-SSH-Key.gif)

*Set Permission on SSH Key*

Step 5: Login from 192.168.0.12 to 192.168.0.11 Server without Password

From now onwards you can log into 192.168.0.11 as sheena user from server 192.168.0.12 as tecmint user without password.

**[tecmint@tecmint ~]$ ssh sheena@192.168.0.11**

[](https://www.tecmint.com/wp-content/uploads/2012/10/SSH-Remote-Passwordless-Login.gif)

*SSH Remote Passwordless Login*