SSH-KEYGEN

What is SSH?

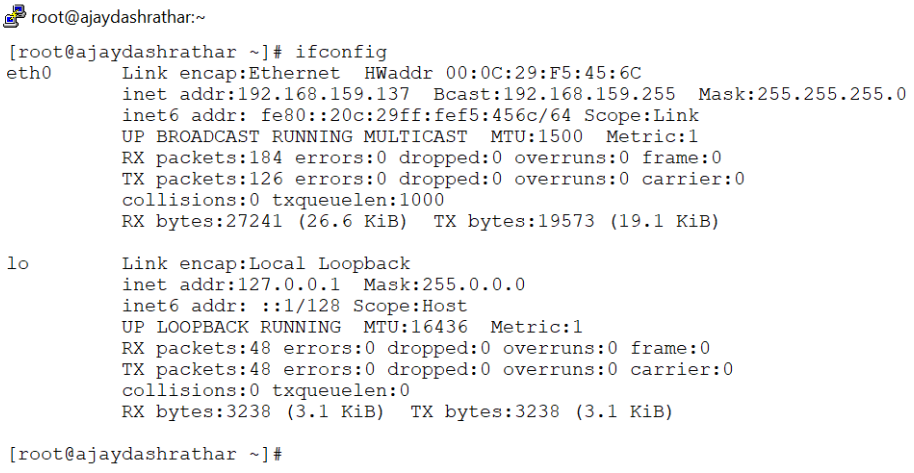
- SSH stands for Secure Shell or Secure Socket Shell. It's a network protocol that allows two computers to communicate and share data securely, even over unsecured networks.

Introduction To the Project

Connecting one server to another server without password using SSH and IP Address.

SERVER-1

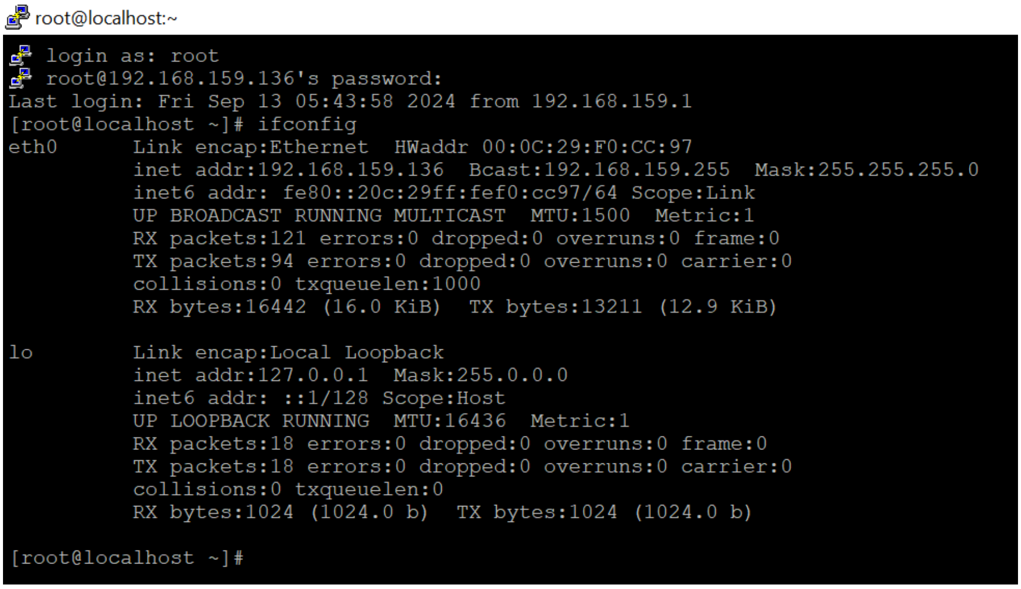
- Lets us know the ip of server 1 and server 2



root@ajaydashrathar:~

```
[root@ajaydashrathar ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F5:45:6C
          inet addr:192.168.159.137  Bcast:192.168.159.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef5:456c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:184 errors:0 dropped:0 overruns:0 frame:0
          TX packets:126 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:27241 (26.6 KiB)  TX bytes:19573 (19.1 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3238 (3.1 KiB)  TX bytes:3238 (3.1 KiB)

[root@ajaydashrathar ~]#
```

SERVER-2



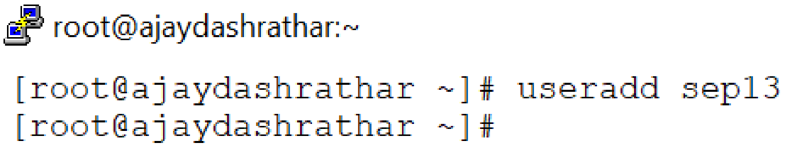
root@localhost:~

```
login as: root
root@192.168.159.136's password:
Last login: Fri Sep 13 05:43:58 2024 from 192.168.159.1
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F0:CC:97
          inet addr:192.168.159.136  Bcast:192.168.159.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef0:cc97/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16442 (16.0 KiB)  TX bytes:13211 (12.9 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1024 (1024.0 b)  TX bytes:1024 (1024.0 b)

[root@localhost ~]#
```

STEPS TO PERFORM THE SSH-KEYGEN

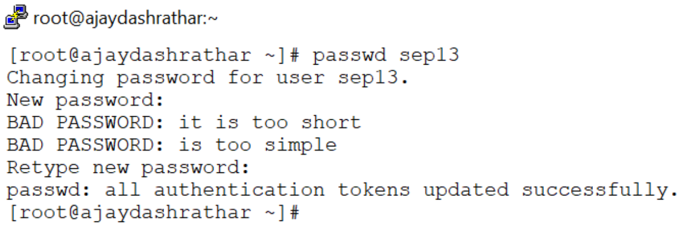
SERVER -1

- Let’s create a new user in server1
- Type the Command in server 1 **useradd sep13**



```
[root@ajaydashrathar ~]# useradd sep13
[root@ajaydashrathar ~]#
```

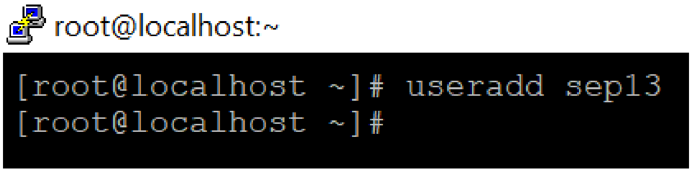
- setting the passwd for the user of sep13
- Type the Command in server 1 **passwd sep13**



```
[root@ajaydashrathar ~]# passwd sep13
Changing password for user sep13.
New password:
BAD PASSWORD: it is too short
BAD PASSWORD: is too simple
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ajaydashrathar ~]#
```

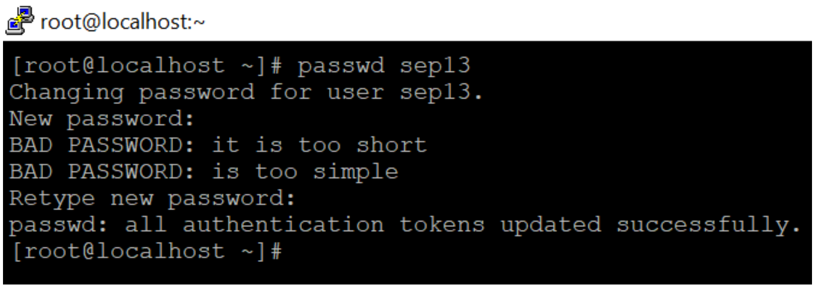
SERVER -2

- Let’s create a new user in server 2
- Type the Command in server 1 **useradd sep13**



```
[root@localhost ~]# useradd sep13
[root@localhost ~]#
```

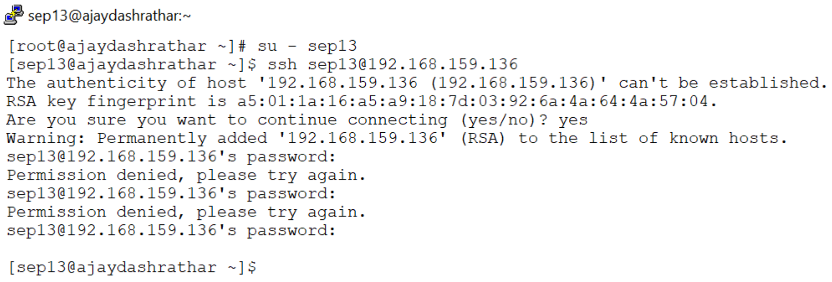
- Setting the passwd for the user of sep13
- Type the Command in server 2 **passwd sep13**



```
[root@localhost ~]# passwd sep13
Changing password for user sep13.
New password:
BAD PASSWORD: it is too short
BAD PASSWORD: is too simple
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
```

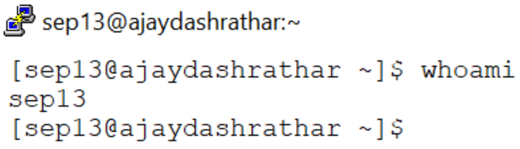
Server 1

- Let's login as a user called **sep13**
- Type the command **su - sep13**



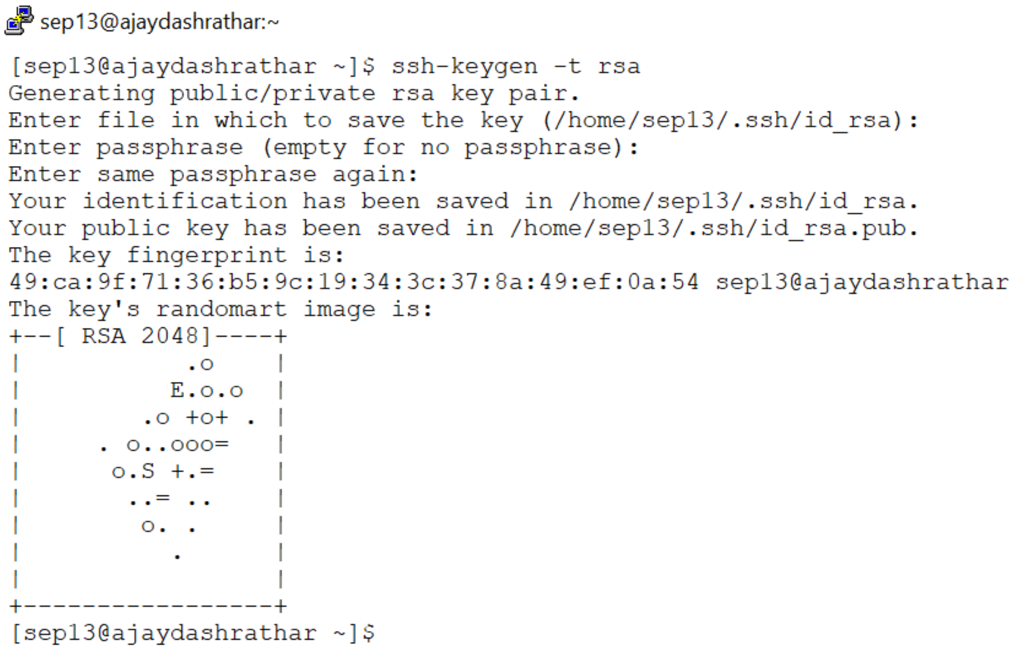
```
[root@ajaydashrathar ~]# su - sep13
[sep13@ajaydashrathar ~]$ ssh sep13@192.168.159.136
The authenticity of host '192.168.159.136 (192.168.159.136)' can't be established.
RSA key fingerprint is a5:01:1a:16:a5:a9:18:7d:03:92:6a:4a:64:4a:57:04.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.159.136' (RSA) to the list of known hosts.
sep13@192.168.159.136's password:
Permission denied, please try again.
sep13@192.168.159.136's password:
Permission denied, please try again.
sep13@192.168.159.136's password:

[sep13@ajaydashrathar ~]$
```

- Type the command **whoami**



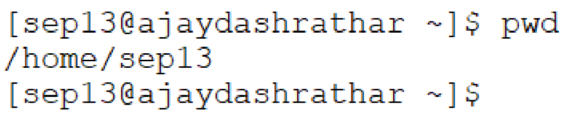
```
[sep13@ajaydashrathar ~]$ whoami
sep13
[sep13@ajaydashrathar ~]$
```

- Type the command **ssh-keygen -t rsa**



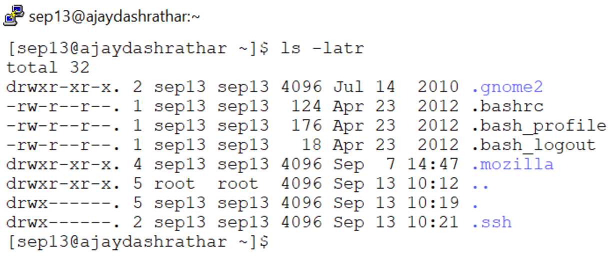
```
[sep13@ajaydashrathar ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/sep13/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/sep13/.ssh/id_rsa.
Your public key has been saved in /home/sep13/.ssh/id_rsa.pub.
The key fingerprint is:
49:ca:9f:71:36:b5:9c:19:34:3c:37:8a:49:ef:0a:54 sep13@ajaydashrathar
The key's randomart image is:
+--[ RSA 2048]----+
|           .o    |
|          E.o.o  |
|        .o +o+ . |
|     . o..ooo=   |
|      o.S +.=    |
|       ..= ..    |
|        o. .     |
|          .      |
|                 |
+-----------------+
[sep13@ajaydashrathar ~]$
```

- Type the command **pwd**



```
[sep13@ajaydashrathar ~]$ pwd
/home/sep13
[sep13@ajaydashrathar ~]$
```

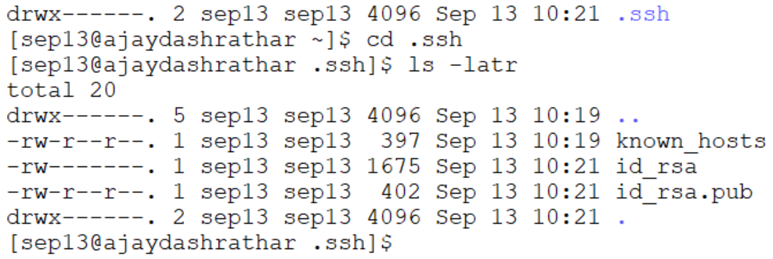
- Type the command **<u>ls -latr</u>**



sep13@ajaydashrathar:~

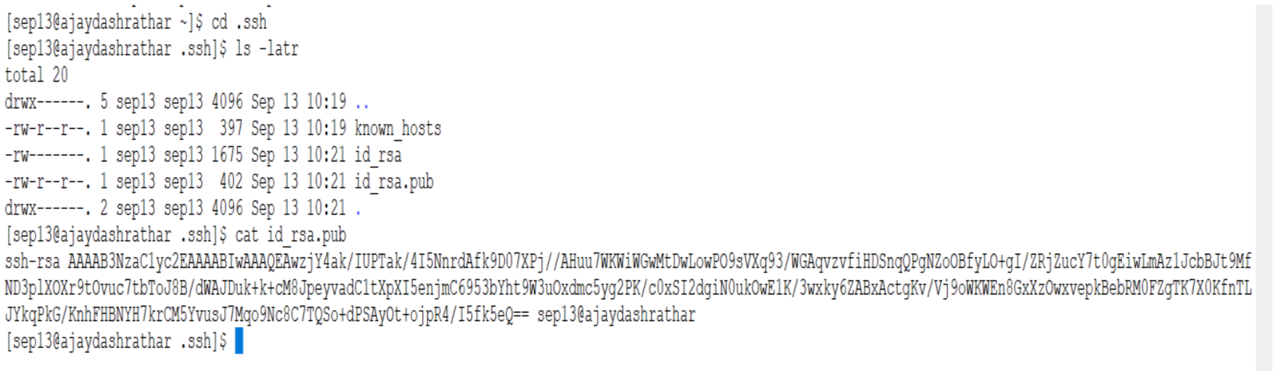
```
[sep13@ajaydashrathar ~]$ ls -latr
total 32
drwxr-xr-x. 2 sep13 sep13 4096 Jul 14  2010 .gnome2
-rw-r--r--. 1 sep13 sep13  124 Apr 23  2012 .bashrc
-rw-r--r--. 1 sep13 sep13  176 Apr 23  2012 .bash_profile
-rw-r--r--. 1 sep13 sep13   18 Apr 23  2012 .bash_logout
drwxr-xr-x. 4 sep13 sep13 4096 Sep  7 14:47 .mozilla
drwxr-xr-x. 5 root  root  4096 Sep 13 10:12 ..
drwx------. 5 sep13 sep13 4096 Sep 13 10:19 .
drwx------. 2 sep13 sep13 4096 Sep 13 10:21 .ssh
[sep13@ajaydashrathar ~]$
```

- There will be a directory **<u>.ssh</u>** go Inside the directory. And see the list of files and folders.
- Type the command **<u>cd .ssh</u>**
- Type the command **<u>ls -latr</u>**



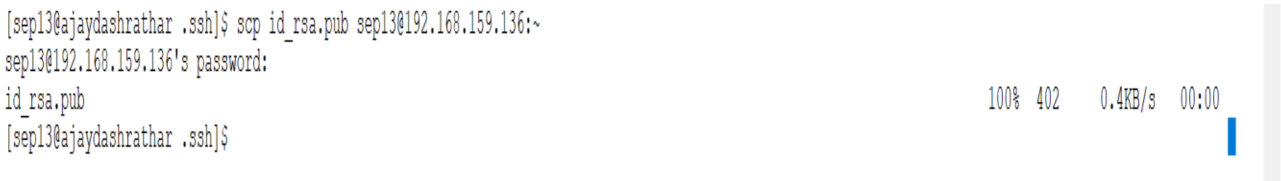
```
drwx------. 2 sep13 sep13 4096 Sep 13 10:21 .ssh
[sep13@ajaydashrathar ~]$ cd .ssh
[sep13@ajaydashrathar .ssh]$ ls -latr
total 20
drwx------. 5 sep13 sep13 4096 Sep 13 10:19 ..
-rw-r--r--. 1 sep13 sep13  397 Sep 13 10:19 known_hosts
-rw-------. 1 sep13 sep13 1675 Sep 13 10:21 id_rsa
-rw-r--r--. 1 sep13 sep13  402 Sep 13 10:21 id_rsa.pub
drwx------. 2 sep13 sep13 4096 Sep 13 10:21 .
[sep13@ajaydashrathar .ssh]$
```

- And see the what the content inside the **id_rsa.pub**
- Type the command **cat id_rsa.pub**



```
[sep13@ajaydashrathar ~]$ cd .ssh
[sep13@ajaydashrathar .ssh]$ ls -latr
total 20
drwx------. 5 sep13 sep13 4096 Sep 13 10:19 ..
-rw-r--r--. 1 sep13 sep13  397 Sep 13 10:19 known_hosts
-rw-------. 1 sep13 sep13 1675 Sep 13 10:21 id_rsa
-rw-r--r--. 1 sep13 sep13  402 Sep 13 10:21 id_rsa.pub
drwx------. 2 sep13 sep13 4096 Sep 13 10:21 .
[sep13@ajaydashrathar .ssh]$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAwzjY4ak/IUPTak/4I5NnrdAfk9D07XPj//AHuu7WKWiWGwMtDwLowPO9sVXq93/WGAqvzvfiHDSnqQPgNZoOBfyLO+gI/ZRjZucY7t0gEiwLmAz1JcbBJt9Mf
ND3plXOXr9tOvuc7tbToJ8B/dWAJDuk+k+cM8JpeyvadC1tXpXI5enjmC6953bYht9W3uOxdmc5yg2PK/c0xSI2dgiN0ukOwE1K/3wxky6ZABxActgKv/Vj9oWKWEn8GxXzOwxvepkBebRM0FZgTK7X0KfnTL
JYkqPkG/KnhFHBNYH7krCM5YvusJ7Mqo9Nc8C7TQSo+dPSAyOt+ojpR4/I5fk5eQ== sep13@ajaydashrathar
[sep13@ajaydashrathar .ssh]$
```

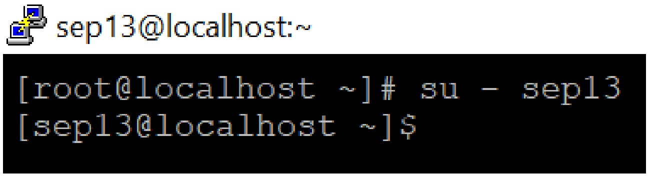
- Transfer the file id_rsa.pub to the second server by using the scp command by mentioning the second server ip address.
- Type the command **scp id_rsa.pub sep13@192.168.159.136**



```
[sep13@ajaydashrathar .ssh]$ scp id_rsa.pub sep13@192.168.159.136:~
sep13@192.168.159.136's password:
id_rsa.pub                                                        100%  402     0.4KB/s   00:00
[sep13@ajaydashrathar .ssh]$
```

<u>Server 2</u>

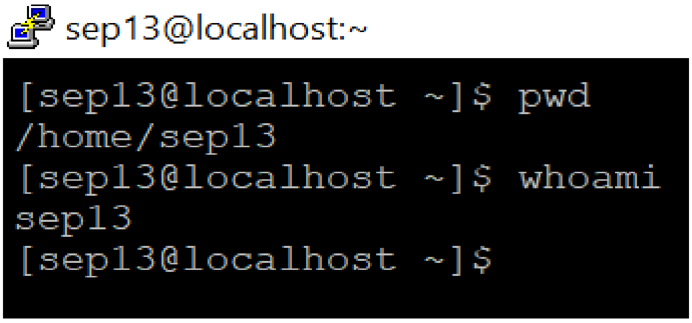
- Login to the second sever as a user called sep13
- Type the command: **<u>su – sep 13</u>**



sep13@localhost:~

```
[root@localhost ~]# su - sep13
[sep13@localhost ~]$
```

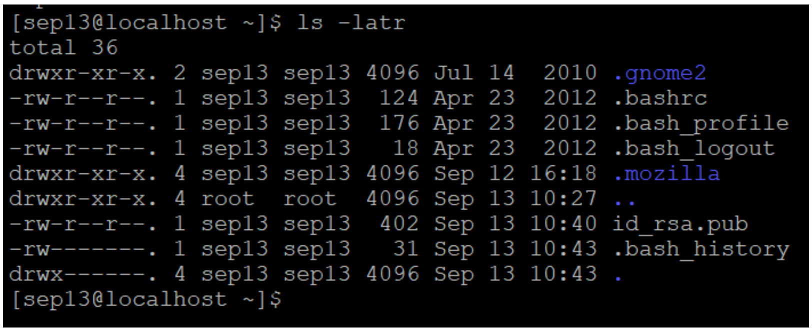
- Type the command **<u>pwd</u>**
- Type the command **<u>whoami</u>**



sep13@localhost:~

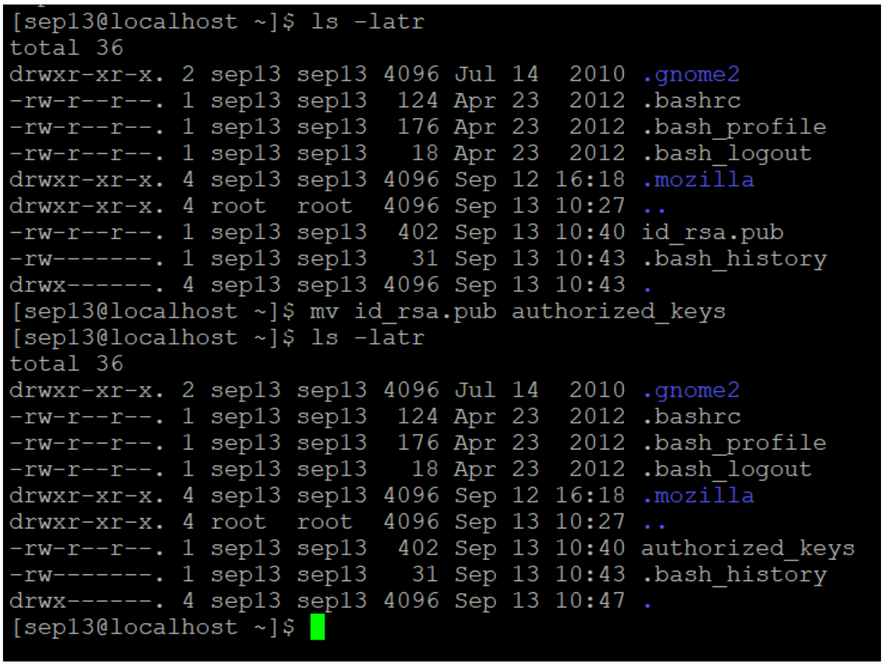
```
[sep13@localhost ~]$ pwd
/home/sep13
[sep13@localhost ~]$ whoami
sep13
[sep13@localhost ~]$
```

- Type the command **<u>ls -latr</u>**
- **id_rsa.pub** file will be present.



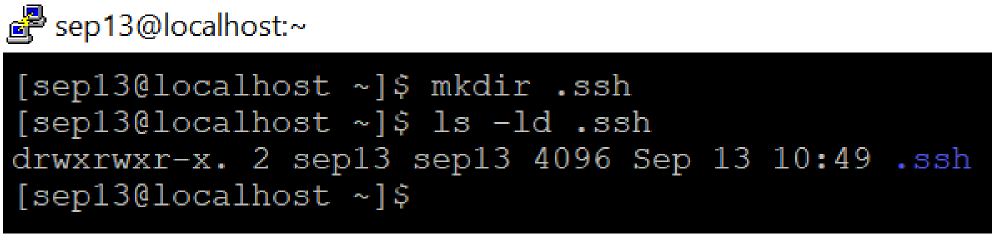
```
[sep13@localhost ~]$ ls -latr
total 36
drwxr-xr-x. 2 sep13 sep13 4096 Jul 14  2010 .gnome2
-rw-r--r--. 1 sep13 sep13  124 Apr 23  2012 .bashrc
-rw-r--r--. 1 sep13 sep13  176 Apr 23  2012 .bash_profile
-rw-r--r--. 1 sep13 sep13   18 Apr 23  2012 .bash_logout
drwxr-xr-x. 4 sep13 sep13 4096 Sep 12 16:18 .mozilla
drwxr-xr-x. 4 root  root  4096 Sep 13 10:27 ..
-rw-r--r--. 1 sep13 sep13  402 Sep 13 10:40 id_rsa.pub
-rw-------. 1 sep13 sep13   31 Sep 13 10:43 .bash_history
drwx------. 4 sep13 sep13 4096 Sep 13 10:43 .
[sep13@localhost ~]$
```

- We are Renaming the file id_rsa.pub to authorized_keys
- Type the command **mv id_rsa.pub authorized_keys**



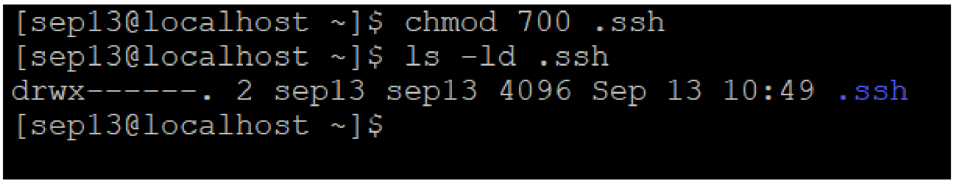
```
[sep13@localhost ~]$ ls -latr
total 36
drwxr-xr-x. 2 sep13 sep13 4096 Jul 14  2010 .gnome2
-rw-r--r--. 1 sep13 sep13  124 Apr 23  2012 .bashrc
-rw-r--r--. 1 sep13 sep13  176 Apr 23  2012 .bash_profile
-rw-r--r--. 1 sep13 sep13   18 Apr 23  2012 .bash_logout
drwxr-xr-x. 4 sep13 sep13 4096 Sep 12 16:18 .mozilla
drwxr-xr-x. 4 root  root  4096 Sep 13 10:27 ..
-rw-r--r--. 1 sep13 sep13  402 Sep 13 10:40 id_rsa.pub
-rw-------. 1 sep13 sep13   31 Sep 13 10:43 .bash_history
drwx------. 4 sep13 sep13 4096 Sep 13 10:43 .
[sep13@localhost ~]$ mv id_rsa.pub authorized_keys
[sep13@localhost ~]$ ls -latr
total 36
drwxr-xr-x. 2 sep13 sep13 4096 Jul 14  2010 .gnome2
-rw-r--r--. 1 sep13 sep13  124 Apr 23  2012 .bashrc
-rw-r--r--. 1 sep13 sep13  176 Apr 23  2012 .bash_profile
-rw-r--r--. 1 sep13 sep13   18 Apr 23  2012 .bash_logout
drwxr-xr-x. 4 sep13 sep13 4096 Sep 12 16:18 .mozilla
drwxr-xr-x. 4 root  root  4096 Sep 13 10:27 ..
-rw-r--r--. 1 sep13 sep13  402 Sep 13 10:40 authorized_keys
-rw-------. 1 sep13 sep13   31 Sep 13 10:43 .bash_history
drwx------. 4 sep13 sep13 4096 Sep 13 10:47 .
[sep13@localhost ~]$ 
```

- Create a directory called as .ssh
- Type the command: **mkdir .ssh**



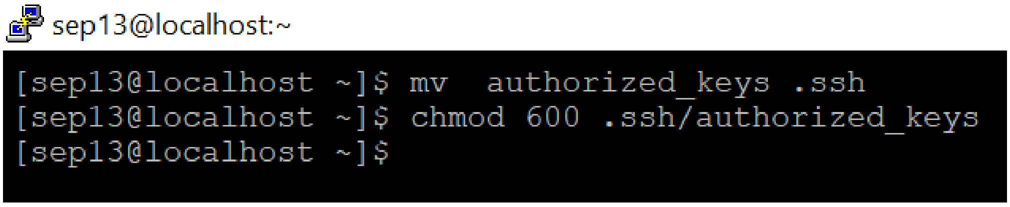
```
[sep13@localhost ~]$ mkdir .ssh
[sep13@localhost ~]$ ls -ld .ssh
drwxrwxr-x. 2 sep13 sep13 4096 Sep 13 10:49 .ssh
[sep13@localhost ~]$
```

- Give the permission for the directory .ssh
- Type the command **chmod 700 .ssh**



```
[sep13@localhost ~]$ chmod 700 .ssh
[sep13@localhost ~]$ ls -ld .ssh
drwx------. 2 sep13 sep13 4096 Sep 13 10:49 .ssh
[sep13@localhost ~]$
```

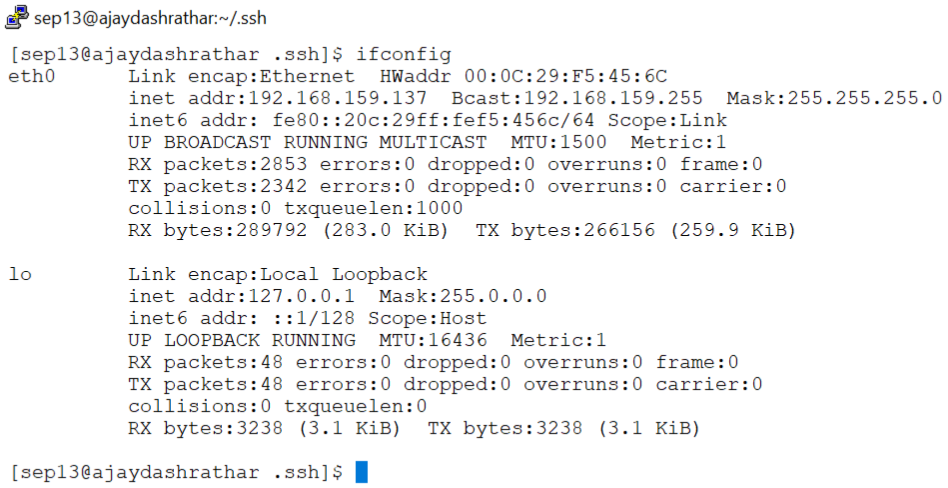
- Move the file authorized_keys to .ssh folder.



```
[sep13@localhost ~]$ mv  authorized_keys .ssh
[sep13@localhost ~]$ chmod 600 .ssh/authorized_keys
[sep13@localhost ~]$
```

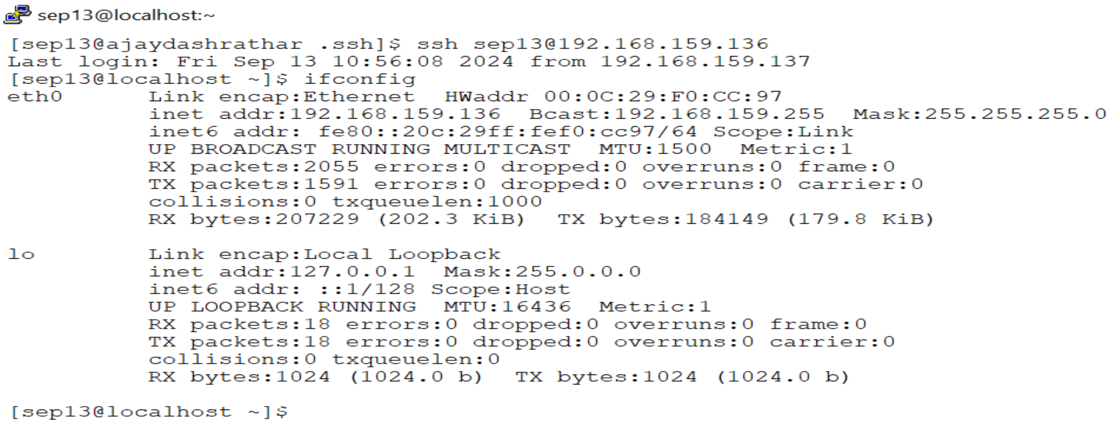
LOGIN TO THE SERVER-1

- See the IP of the Server 1
- Type the command **ifconfig**



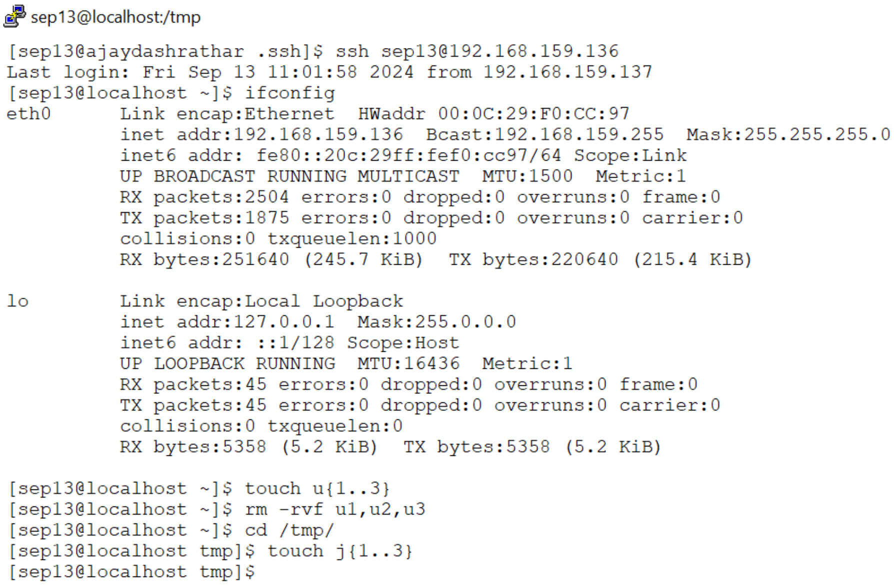
```
[sep13@ajaydashrathar .ssh]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F5:45:6C
          inet addr:192.168.159.137  Bcast:192.168.159.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef5:456c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2853 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2342 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:289792 (283.0 KiB)  TX bytes:266156 (259.9 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3238 (3.1 KiB)  TX bytes:3238 (3.1 KiB)

[sep13@ajaydashrathar .ssh]$
```

- Now we are logged to the server 1 as a user sep13 and we are going to connect to the server 2 without using the password.
- Type the command **ssh sep13@192.168.159.136**



```
[sep13@ajaydashrathar .ssh]$ ssh sep13@192.168.159.136
Last login: Fri Sep 13 10:56:08 2024 from 192.168.159.137
[sep13@localhost ~]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F0:CC:97
          inet addr:192.168.159.136  Bcast:192.168.159.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef0:cc97/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2055 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1591 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:207229 (202.3 KiB)  TX bytes:184149 (179.8 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1024 (1024.0 b)  TX bytes:1024 (1024.0 b)

[sep13@localhost ~]$
```

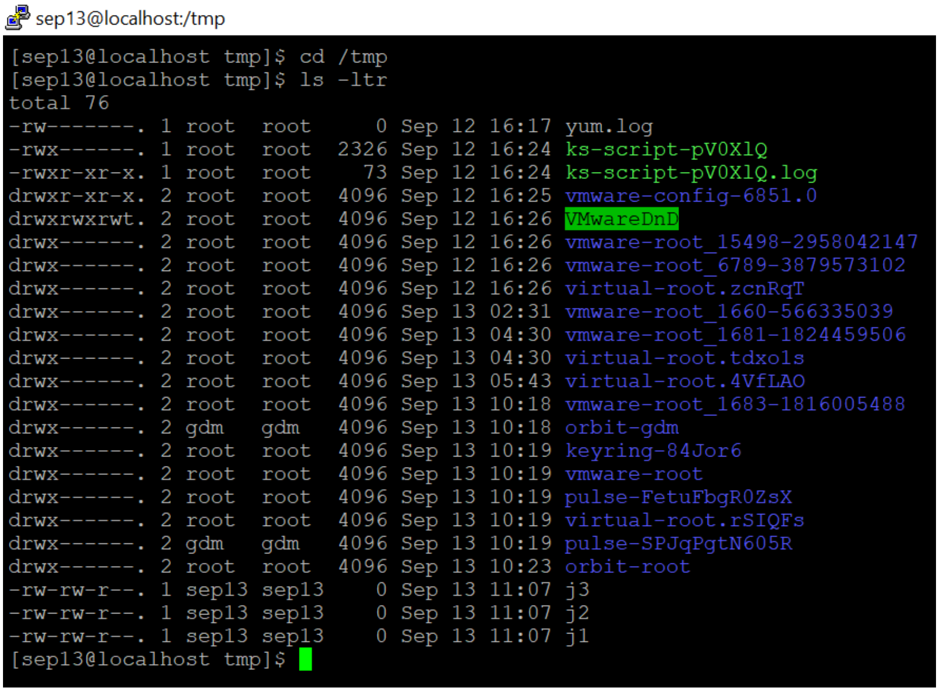
- Create a some files in server 1 it should be present in the server2 .
- Type the command **touch j{1..3}**



```
[sep13@ajaydashrathar .ssh]$ ssh sep13@192.168.159.136
Last login: Fri Sep 13 11:01:58 2024 from 192.168.159.137
[sep13@localhost ~]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F0:CC:97
          inet addr:192.168.159.136  Bcast:192.168.159.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef0:cc97/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2504 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1875 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:251640 (245.7 KiB)  TX bytes:220640 (215.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:45 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5358 (5.2 KiB)  TX bytes:5358 (5.2 KiB)

[sep13@localhost ~]$ touch u{1..3}
[sep13@localhost ~]$ rm -rvf u1,u2,u3
[sep13@localhost ~]$ cd /tmp/
[sep13@localhost tmp]$ touch j{1..3}
[sep13@localhost tmp]$
```

LOGIN TO THE SERVER – 2

- Whatever the files created under the server 1 these files are present in the server 2 you can verify that j1,j2,j3 files are present.



```
[sep13@localhost tmp]$ cd /tmp
[sep13@localhost tmp]$ ls -ltr
total 76
-rw-------. 1 root  root     0 Sep 12 16:17 yum.log
-rwx------. 1 root  root  2326 Sep 12 16:24 ks-script-pV0X1Q
-rwxr-xr-x. 1 root  root    73 Sep 12 16:24 ks-script-pV0X1Q.log
drwxr-xr-x. 2 root  root  4096 Sep 12 16:25 vmware-config-6851.0
drwxrwxrwt. 2 root  root  4096 Sep 12 16:26 VMwareDnD
drwx------. 2 root  root  4096 Sep 12 16:26 vmware-root_15498-2958042147
drwx------. 2 root  root  4096 Sep 12 16:26 vmware-root_6789-3879573102
drwx------. 2 root  root  4096 Sep 12 16:26 virtual-root.zcnRqT
drwx------. 2 root  root  4096 Sep 13 02:31 vmware-root_1660-566335039
drwx------. 2 root  root  4096 Sep 13 04:30 vmware-root_1681-1824459506
drwx------. 2 root  root  4096 Sep 13 04:30 virtual-root.tdxols
drwx------. 2 root  root  4096 Sep 13 05:43 virtual-root.4VfLAO
drwx------. 2 root  root  4096 Sep 13 10:18 vmware-root_1683-1816005488
drwx------. 2 gdm   gdm   4096 Sep 13 10:18 orbit-gdm
drwx------. 2 root  root  4096 Sep 13 10:19 keyring-84Jor6
drwx------. 2 root  root  4096 Sep 13 10:19 vmware-root
drwx------. 2 root  root  4096 Sep 13 10:19 pulse-FetuFbgR0ZsX
drwx------. 2 root  root  4096 Sep 13 10:19 virtual-root.rSIQFs
drwx------. 2 gdm   gdm   4096 Sep 13 10:19 pulse-SPJqPgtN605R
drwx------. 2 root  root  4096 Sep 13 10:23 orbit-root
-rw-rw-r--. 1 sep13 sep13    0 Sep 13 11:07 j3
-rw-rw-r--. 1 sep13 sep13    0 Sep 13 11:07 j2
-rw-rw-r--. 1 sep13 sep13    0 Sep 13 11:07 j1
[sep13@localhost tmp]$
```