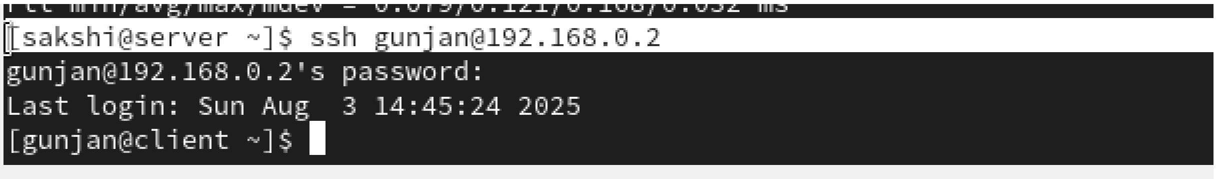
Secure Socket Shell

This task is performed under local user

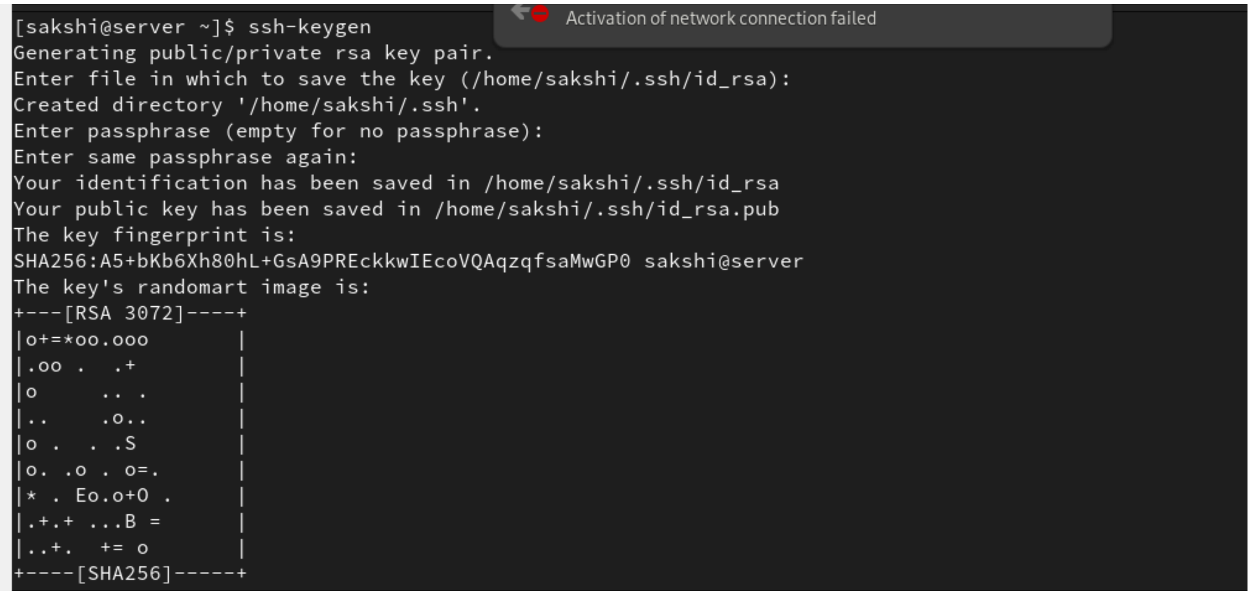
Server Machine:

Password based authentication



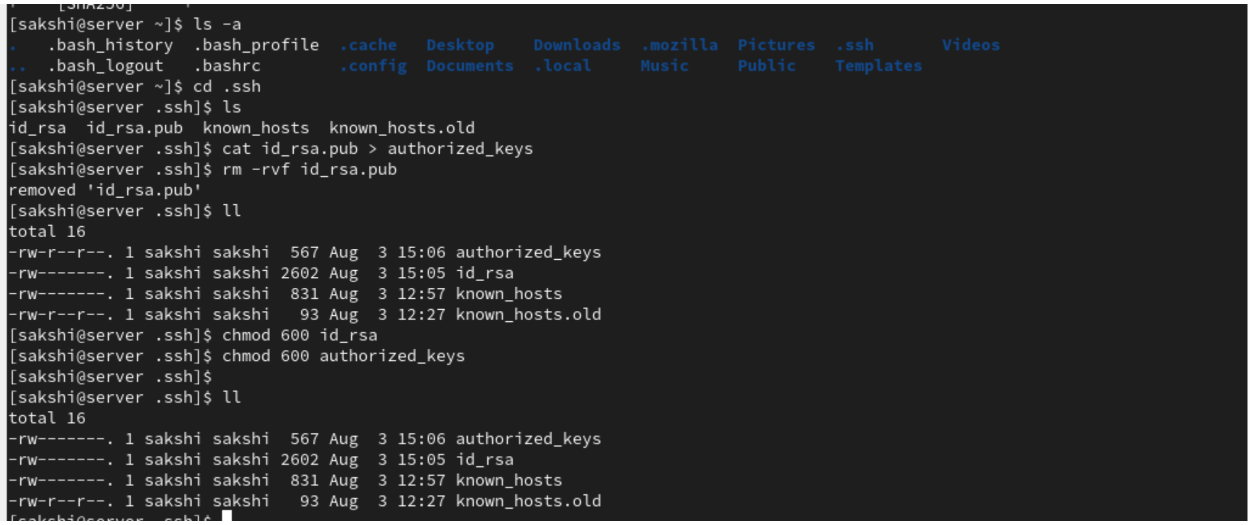
```
rtt min/avg/max/mdev = 0.079/0.121/0.168/0.032 ms
[sakshi@server ~]$ ssh gunjan@192.168.0.2
gunjan@192.168.0.2's password:
Last login: Sun Aug  3 14:45:24 2025
[gunjan@client ~]$ 
```

Key based authentication



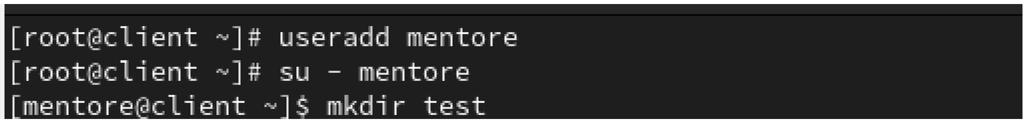
Activation of network connection failed

```
[sakshi@server ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/sakshi/.ssh/id_rsa):
Created directory '/home/sakshi/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/sakshi/.ssh/id_rsa
Your public key has been saved in /home/sakshi/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:A5+bKb6Xh80hL+GsA9PREckkwIEcoVQAqzqfsaMwGP0 sakshi@server
The key's randomart image is:
+---[RSA 3072]----+
|o+=*oo.ooo       |
|.oo .   .+       |
|o      .. .      |
|..     .o..      |
|o .   . .S       |
|o. .o . o=.      |
|* . Eo.o+O .     |
|.+.+ ...B =      |
|..+.   += o      |
+----[SHA256]-----+
```

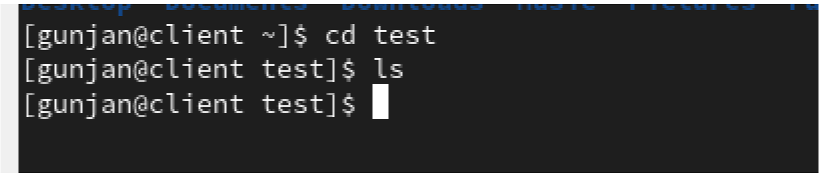


```
[sakshi@server ~]$ ls -a
.   .bash_history  .bash_profile  .cache   Desktop    Downloads  .mozilla  Pictures  .ssh       Videos
..  .bash_logout   .bashrc        .config  Documents  .local     Music     Public    Templates
[sakshi@server ~]$ cd .ssh
[sakshi@server .ssh]$ ls
id_rsa  id_rsa.pub  known_hosts  known_hosts.old
[sakshi@server .ssh]$ cat id_rsa.pub > authorized_keys
[sakshi@server .ssh]$ rm -rvf id_rsa.pub
removed 'id_rsa.pub'
[sakshi@server .ssh]$ ll
total 16
-rw-r--r--. 1 sakshi sakshi  567 Aug  3 15:06 authorized_keys
-rw-------. 1 sakshi sakshi 2602 Aug  3 15:05 id_rsa
-rw-------. 1 sakshi sakshi  831 Aug  3 12:57 known_hosts
-rw-r--r--. 1 sakshi sakshi   93 Aug  3 12:27 known_hosts.old
[sakshi@server .ssh]$ chmod 600 id_rsa
[sakshi@server .ssh]$ chmod 600 authorized_keys
[sakshi@server .ssh]$
[sakshi@server .ssh]$ ll
total 16
-rw-------. 1 sakshi sakshi  567 Aug  3 15:06 authorized_keys
-rw-------. 1 sakshi sakshi 2602 Aug  3 15:05 id_rsa
-rw-------. 1 sakshi sakshi  831 Aug  3 12:57 known_hosts
-rw-r--r--. 1 sakshi sakshi   93 Aug  3 12:27 known_hosts.old
[sakshi@server .ssh]$ 
```

Client Machine:

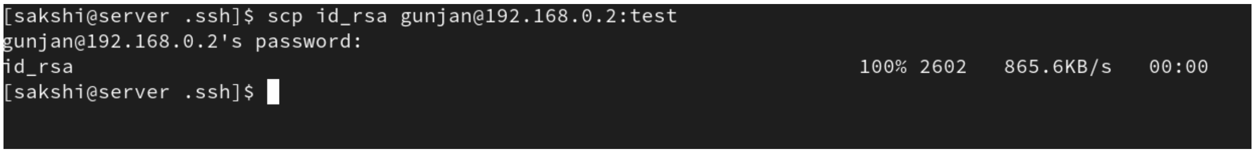


```
[root@client ~]# useradd mentore
[root@client ~]# su - mentore
[mentore@client ~]$ mkdir test
```



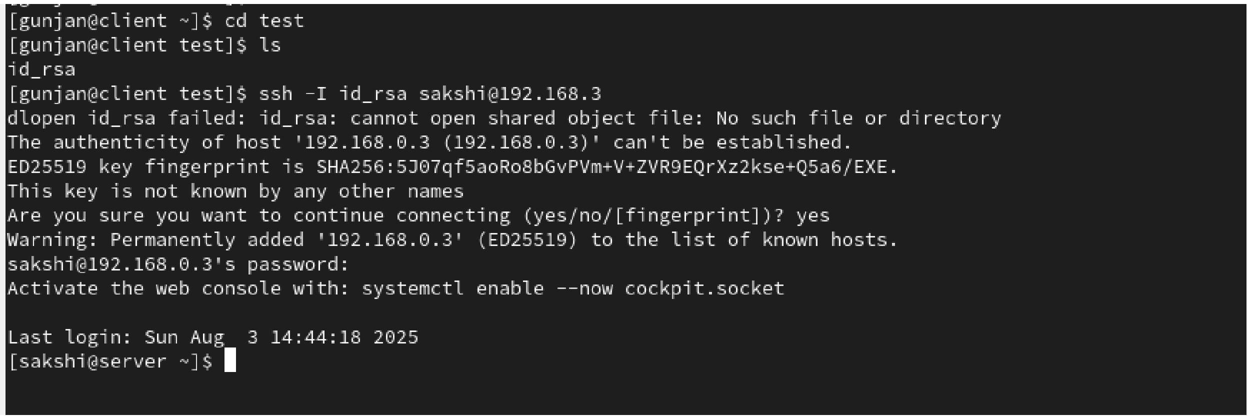
```
[gunjan@client ~]$ cd test
[gunjan@client test]$ ls
[gunjan@client test]$ 
```

Server Machine: share encryption key



```
[sakshi@server .ssh]$ scp id_rsa gunjan@192.168.0.2:test
gunjan@192.168.0.2's password:
id_rsa                                                              100% 2602   865.6KB/s   00:00
[sakshi@server .ssh]$ 
```

Client Machine:



```
[gunjan@client ~]$ cd test
[gunjan@client test]$ ls
id_rsa
[gunjan@client test]$ ssh -I id_rsa sakshi@192.168.3
dlopen id_rsa failed: id_rsa: cannot open shared object file: No such file or directory
The authenticity of host '192.168.0.3 (192.168.0.3)' can't be established.
ED25519 key fingerprint is SHA256:5J07qf5aoRo8bGvPVm+V+ZVR9EQrXz2kse+Q5a6/EXE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.3' (ED25519) to the list of known hosts.
sakshi@192.168.0.3's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sun Aug  3 14:44:18 2025
[sakshi@server ~]$ 
```