SSH and SCP Implementation

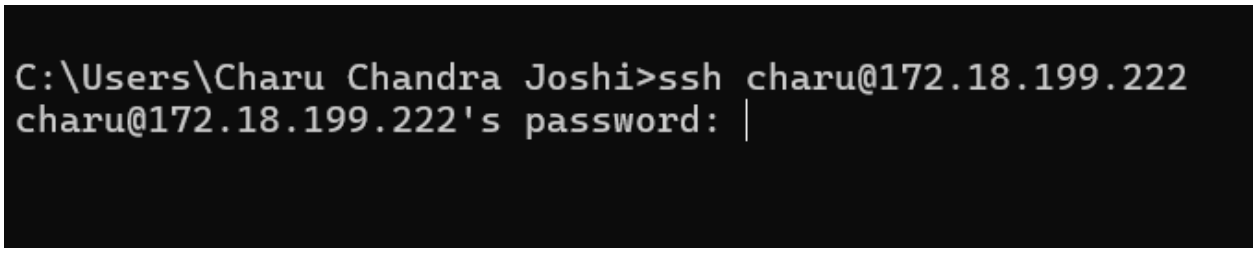
Group No. 7
202111001: Abhay Mishra
202111019: Charu Chandra Joshi
202111028: Falgun Soni
202111067: Prakhar Shukla
202111075: Sahil Sonkar

I. SSH connection using password.

Server IP: `inet 172.18.199.222/20`

Host Name: `charu`

Command: ssh charu@172.18.199.222



Successfully connected to the remote server using ssh.

```
C:\Users\Charu Chandra Joshi>ssh charu@172.18.199.222
charu@172.18.199.222's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.10.16.3-microsoft-standard-WSL2 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Sat Apr  6 19:14:37 IST 2024

  System load:  0.0               Processes:             15
  Usage of /:   4.2% of 250.98GB   Users logged in:       0
  Memory usage: 3%                IPv4 address for eth0: 172.18.199.222
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

5 updates can be applied immediately.
5 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sat Apr  6 19:05:22 2024 from 172.18.192.1
charu@LAPTOP-2REOVJ5L:~$
```

II. SSH connection using RSA keys.

Step-1: Generate the SSH Keys (ssh-keygen)

```
C:\Users\Charu Chandra Joshi>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\Charu Chandra Joshi/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\Charu Chandra Joshi/.ssh/id_rsa
Your public key has been saved in C:\Users\Charu Chandra Joshi/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Tse+KabpYYIy2vFGPpEpFmHgtAT0rO12oOO20Gua9dM charu chandra joshi@LAPTOP-2REOVJ5L
The key's randomart image is:
+---[RSA 3072]----+
|==               |
|+ *              |
| + +             |
|  +      .       |
| . + o  S o      |
| .=.*  o o       |
|++=*.+o . .      |
|+B+=*oEoo  o     |
|==+.o++o .o      |
+----[SHA256]-----+
```

Step-2: Copy the public key to server

cmd: ssh-copy-id charu@172.18.199.222

```
Charu Chandra Joshi@LAPTOP-2REOVJ5L MINGW64 ~ (master)
$ ssh-copy-id charu@172.18.199.222
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/c/Users/Charu Chandra Joshi/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
charu@172.18.199.222's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'charu@172.18.199.222'"
and check to make sure that only the key(s) you wanted were added.
```

As a result, there is no need to verify using any password. The command **ssh charu@172.18.199.222** directly establishes the connection without the need to enter a password.

```
C:\Users\Charu Chandra Joshi>ssh charu@172.18.199.222
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.10.16.3-microsoft-standard-WSL2 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Sat Apr  6 19:31:17 IST 2024

  System load:  0.0                Processes:             18
  Usage of /:   4.2% of 250.98GB   Users logged in:       0
  Memory usage: 3%                 IPv4 address for eth0: 172.18.199.222
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

5 updates can be applied immediately.
5 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sat Apr  6 19:30:58 2024 from 172.18.192.1
charu@LAPTOP-2REOVJ5L:~$
```

III. SCP

1. Uploading a file to the server.

Moving the file move.txt to the server.
cmd: **scp source_path charu@172.18.199.222:destination_path**

move.txt

```
This is a file that has to be moved to the server.
```

```
C:\Users\Charu Chandra Joshi>scp ./move.txt charu@172.18.199.222:~/Desktop
move.txt
```

Verifying if the file moved correctly:

```
Last login: Sat Apr  6 19:43:57 2024 from 172.18.192.1
charu@LAPTOP-2REOVJ5L:~$ cd Desktop
charu@LAPTOP-2REOVJ5L:~/Desktop$ cat move.txt
This is a file that has to be moved to the server.charu@LAPTO
```

We can see the file has moved correctly to ~/Desktop.

2. Downloading a file from the server.

We'll download the file down.txt to our local system. The file is located in server directory ~/Desktop/down.txt.

down.txt

```
charu@LAPTOP-2REOVJ5L:~/Desktop$ cat down.txt
Hi, this is the file in server which we want to download.
```

cmd: **scp username@remote_host:/path/to/remote/file.txt /path/to/local/directory**

```
C:\Users\Charu Chandra Joshi>scp charu@172.18.199.222:~/Desktop/down.txt .
down.txt
```

We downloaded the file to the home directory of the local machine. Let's verify if it is downloaded correctly.
Verification:

```
C:\Users\Charu Chandra Joshi>type down.txt
Hi, this is the file in server which we want to download.
```

As shown, the file down.txt downloaded correctly with correct content using scp.

IV. Conclusion

We first used ssh to connect to a server with the use of the password. Afterwards we used the public key of the local host to authenticate the server. This is done by generating the keys on a local machine and then saving it to the server.
We also saw the use of scp to first upload a file to the server and then download a file to the local machine.