SSH (Secure Shell)

What is SSH?

SSH is a network protocol. It is used to login to another computer and executes commands in it. Secure Shell provides a secure way to connect to a remote computer over an unsecured network. Unlike Telnet, SSH uses cryptographic techniques to ensure that all communication happens in an encrypted format.

Working:

SSH runs on port number 22 by default. The client begins the SSH session by TCP handshake with the server. The client verifies the server identity matches the previously recorded information and provides the credentials to authenticate. First, both systems agree upon some encryption standard and then the user must authenticate himself. If the credentials match then access to the server is granted.

SSH uses three different types of encryption technologies

1. Symmetric encryption
2. Asymmetric encryption
3. Hashing

Symmetric encryption:

In symmetrical encryption, only one key is used to encrypt the entire communication in an SSH session. Or a pair of keys are used where one can be easily calculated using the other. Initially, some public information is exchanged between the sender and the receiver and the key is calculated (using key exchange algorithms) based on this information independently on both sender and the receiver side. The key is never transmitted in the network. This key generation is done before the client authentication.

Asymmetric encryption:

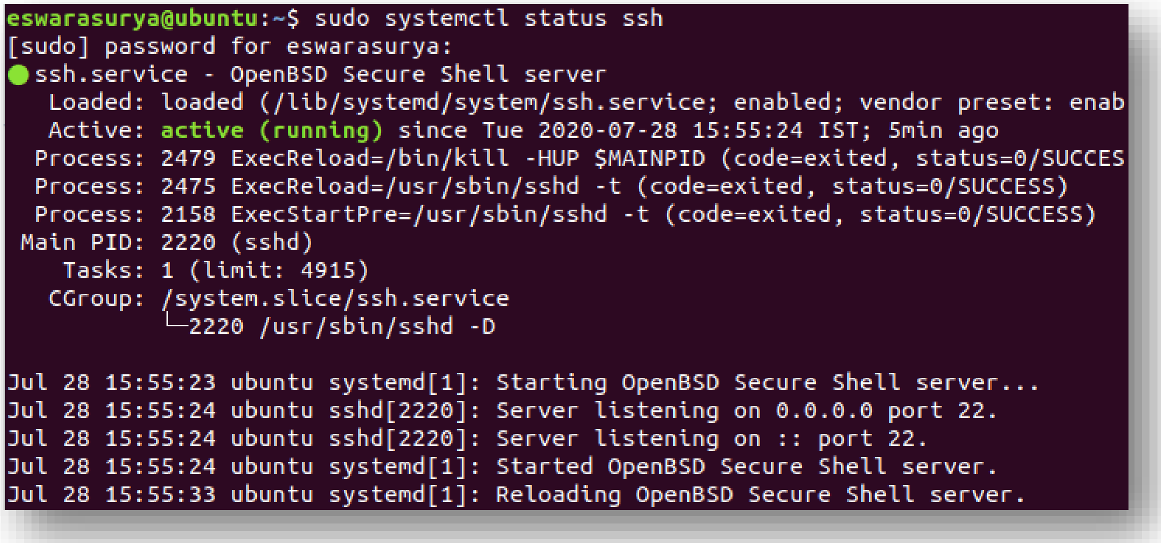
This uses two keys for encryption and description. These two keys are called public key and private key. The public key is distributed freely with all parties and the private key remains private. The private key cannot be computed using the public key. And the relation is as follows, a message that is encrypted by a public key can only be decrypted using the private key. I.e., the public key cannot decrypt its own messages.
Asymmetric encryption is used in the encryption of the key exchange algorithms of the symmetric ssh session.

Hashing:

Hashes are irreversible functions i.e., they can’t be decrypted. SSH uses hashes to verify the authenticity of the messages.

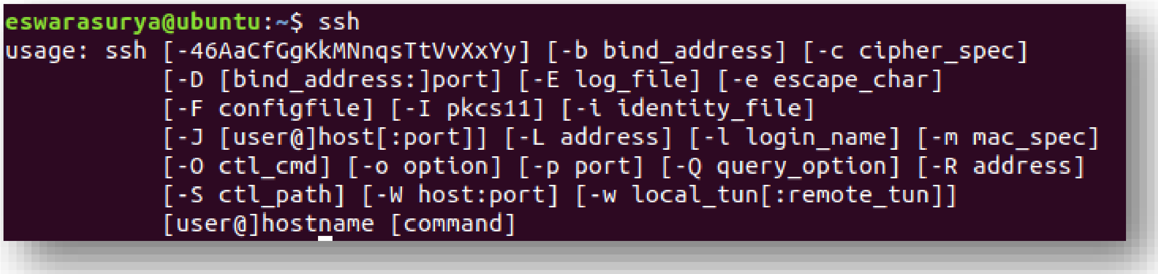
In practice:

SSH server is not installed by default in Ubuntu but can be installed by the command
sudo apt install openssh-server



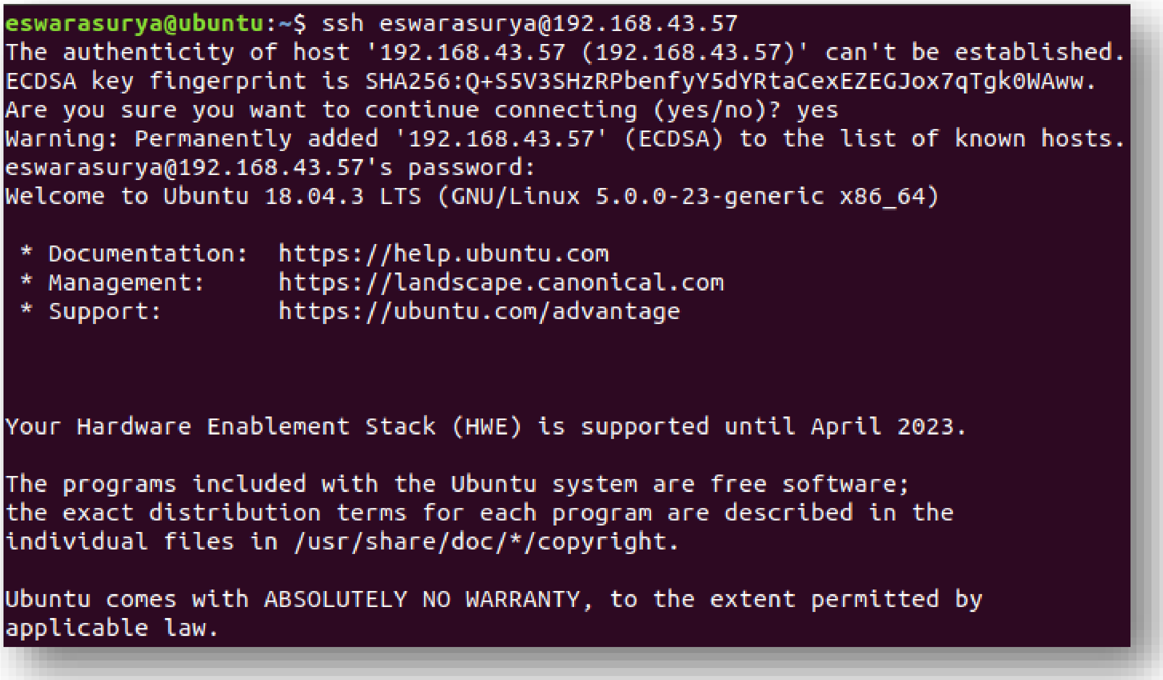
```
eswarasurya@ubuntu:~$ sudo systemctl status ssh
[sudo] password for eswarasurya:
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Tue 2020-07-28 15:55:24 IST; 5min ago
  Process: 2479 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCES
  Process: 2475 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Process: 2158 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 2220 (sshd)
    Tasks: 1 (limit: 4915)
   CGroup: /system.slice/ssh.service
           └─2220 /usr/sbin/sshd -D

Jul 28 15:55:23 ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
Jul 28 15:55:24 ubuntu sshd[2220]: Server listening on 0.0.0.0 port 22.
Jul 28 15:55:24 ubuntu sshd[2220]: Server listening on :: port 22.
Jul 28 15:55:24 ubuntu systemd[1]: Started OpenBSD Secure Shell server.
Jul 28 15:55:33 ubuntu systemd[1]: Reloading OpenBSD Secure Shell server.
```

The client-side of the ssh can be accessed by typing **SSH**



```
eswarasurya@ubuntu:~$ ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
           [-D [bind_address:]port] [-E log_file] [-e escape_char]
           [-F configfile] [-I pkcs11] [-i identity_file]
           [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec]
           [-O ctl_cmd] [-o option] [-p port] [-Q query_option] [-R address]
           [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
           [user@]hostname [command]
```

To connect to the server running we can type s**sh username@ip_address**
In this case, we type ssh eswarasurya@192.168.43.57



```
eswarasurya@ubuntu:~$ ssh eswarasurya@192.168.43.57
The authenticity of host '192.168.43.57 (192.168.43.57)' can't be established.
ECDSA key fingerprint is SHA256:Q+S5V3SHzRPbenfyY5dYRtaCexEZEGJox7qTgk0WAww.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.43.57' (ECDSA) to the list of known hosts.
eswarasurya@192.168.43.57's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.0.0-23-generic x86_64)

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



Your Hardware Enablement Stack (HWE) is supported until April 2023.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

To stop the running of the ssh server we can type the command **sudo systemctl stop ssh** and start again the command is **sudo systemctl start ssh**