Practical 4:- SSH Server: Password Authentication. Configure SSH Server to manage a server from the remote computer, SSH Client: (Ubuntu and Windows)

Solution:-

Step1:- Installing Openssh-server

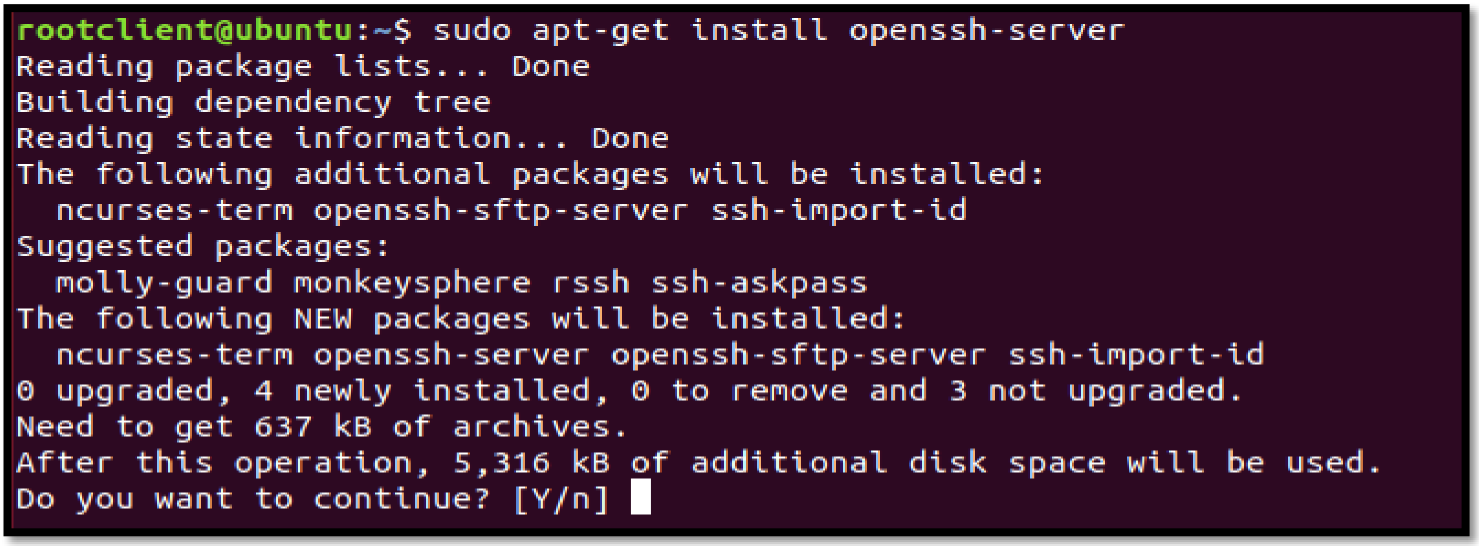
To install and enable SSH on your Ubuntu system complete the following steps:

Open your terminal either by using the Ctrl+Alt+T keyboard shortcut or by clicking on the terminal icon and install the openssh-server package by typing:

# sudo apt update

# sudo apt install openssh-server

Enter the password when prompted and enter Y to continue with the installation.

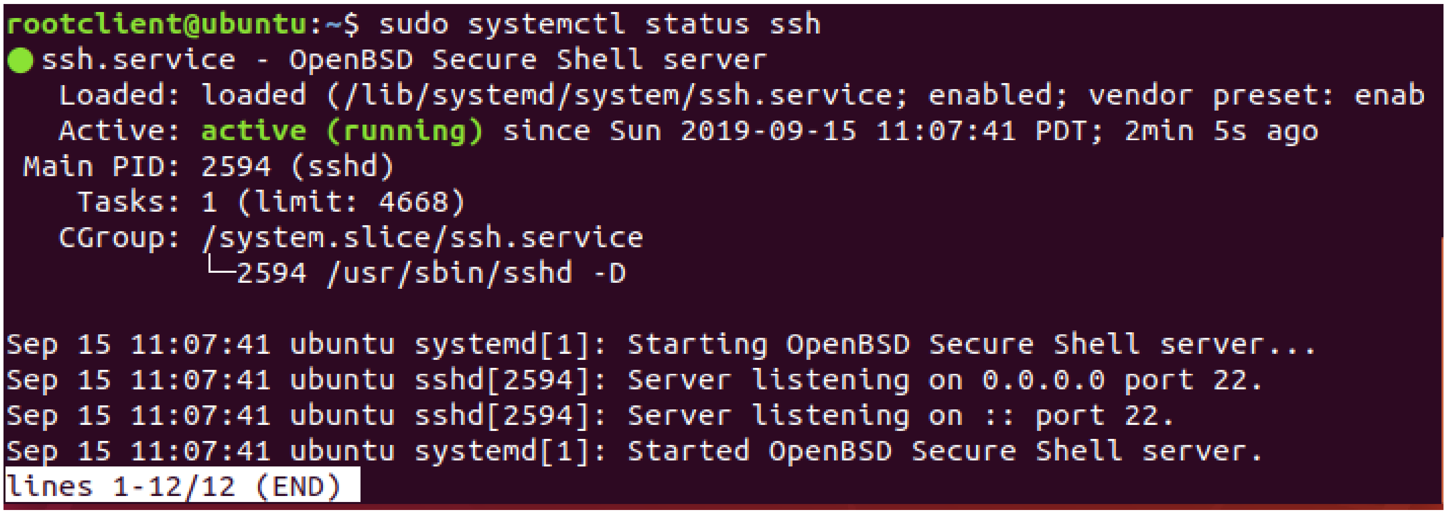


```
rootclient@ubuntu:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere rssh ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 3 not upgraded.
Need to get 637 kB of archives.
After this operation, 5,316 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Once the installation is completed, the SSH service will start automatically. To verify that the installation was successful and SSH service is running type the following command which will print the SSH server status:

# sudo systemctl status ssh

You should see something like Active: active (running):



```
rootclient@ubuntu:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Sun 2019-09-15 11:07:41 PDT; 2min 5s ago
 Main PID: 2594 (sshd)
    Tasks: 1 (limit: 4668)
   CGroup: /system.slice/ssh.service
           └─2594 /usr/sbin/sshd -D

Sep 15 11:07:41 ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
Sep 15 11:07:41 ubuntu sshd[2594]: Server listening on 0.0.0.0 port 22.
Sep 15 11:07:41 ubuntu sshd[2594]: Server listening on :: port 22.
Sep 15 11:07:41 ubuntu systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

Press **q** to get back to the command line prompt.

Now that SSH is installed and running on your Ubuntu system you can connect to it via SSH from any remote machine. Linux and macOS systems have SSH clients installed by default.

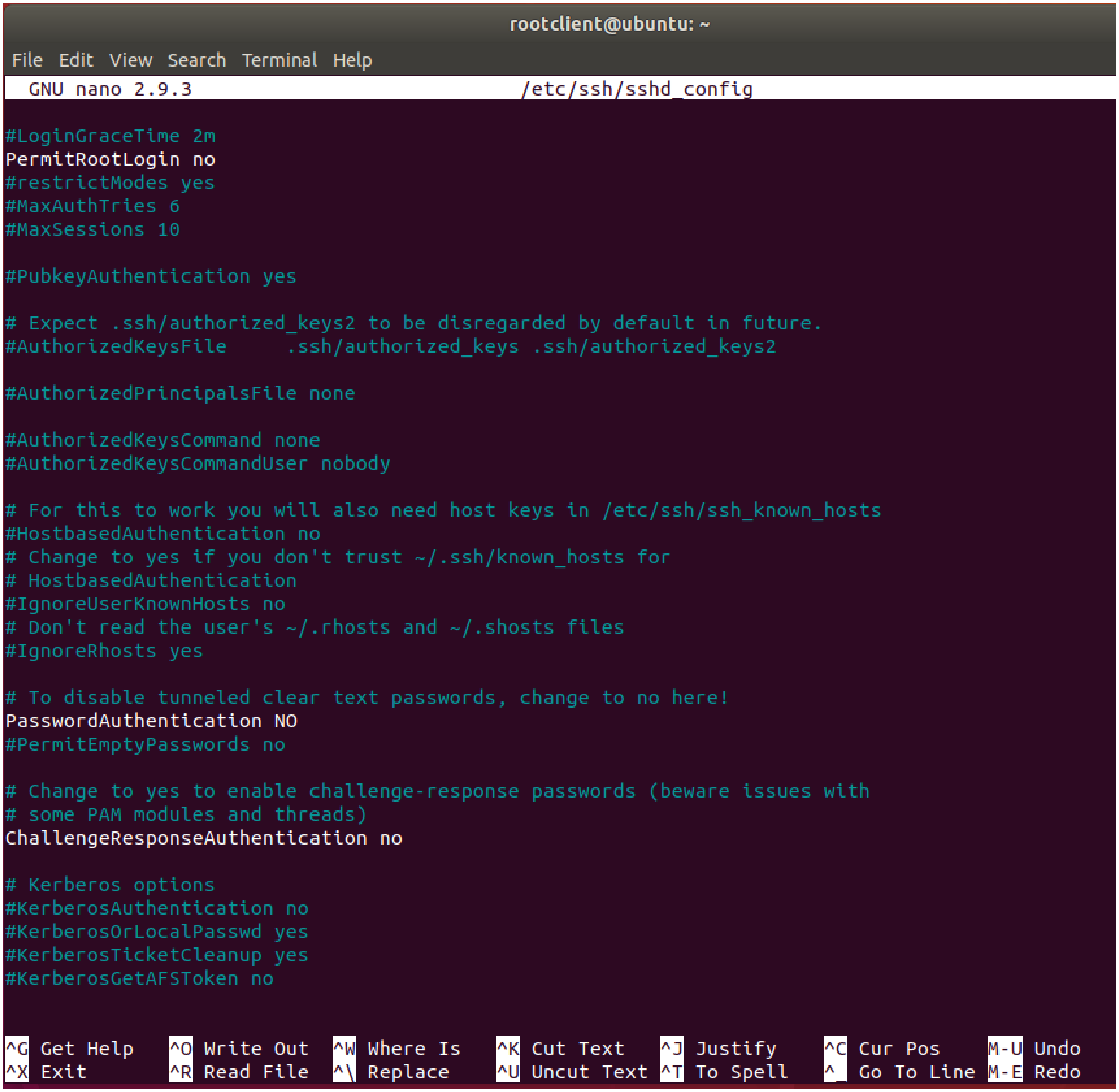
Step 2:- Configure Openssh-server

Now that the server is installed, its default configuration file can be found at the location below:-

/etc/ssh/sshd_config

Open the configuration file to make changes, you run the following command.

# Sudo nano /etc/ssh/sshd_config



```
  GNU nano 2.9.3                          /etc/ssh/sshd_config

#LoginGraceTime 2m
PermitRootLogin no
#restrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication NO
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no


^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line M-E Redo
```

Step3:- Making Basic changes /etc/ssh/sshd_config file

OpenSSH default setting allow password authentication. To disable, changes the line to

PasswordAuthenication NO

To fully disable the root user, change the line to:

PermitRootLogin No

Save the File.

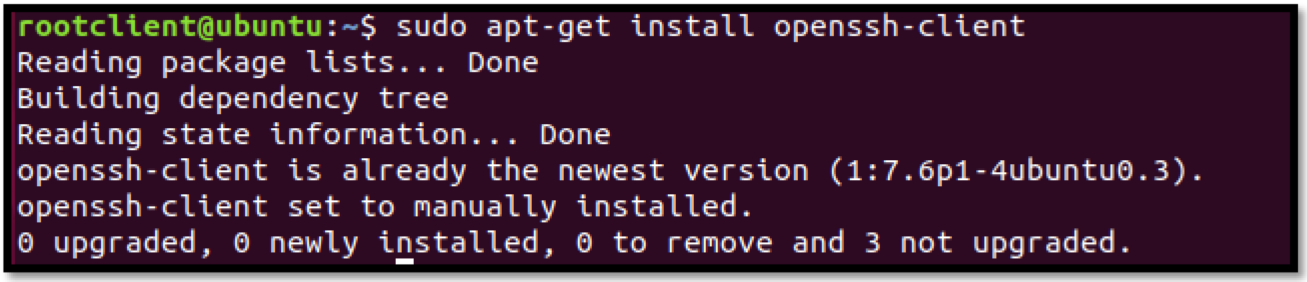
To apply the changes you made, run the commands below to restart the OpenSSH server.

# sudo systemctl restart ssh

Step 4:- Install SSH-client over Ubuntu

You must have SSH client program installed on the computer from which you want to connect to your remote computer using SSH. It should be installed by default on most Linux operating systems these days.TO Install SSH-client run the following command:

# sudo apt-get install Openssh-client



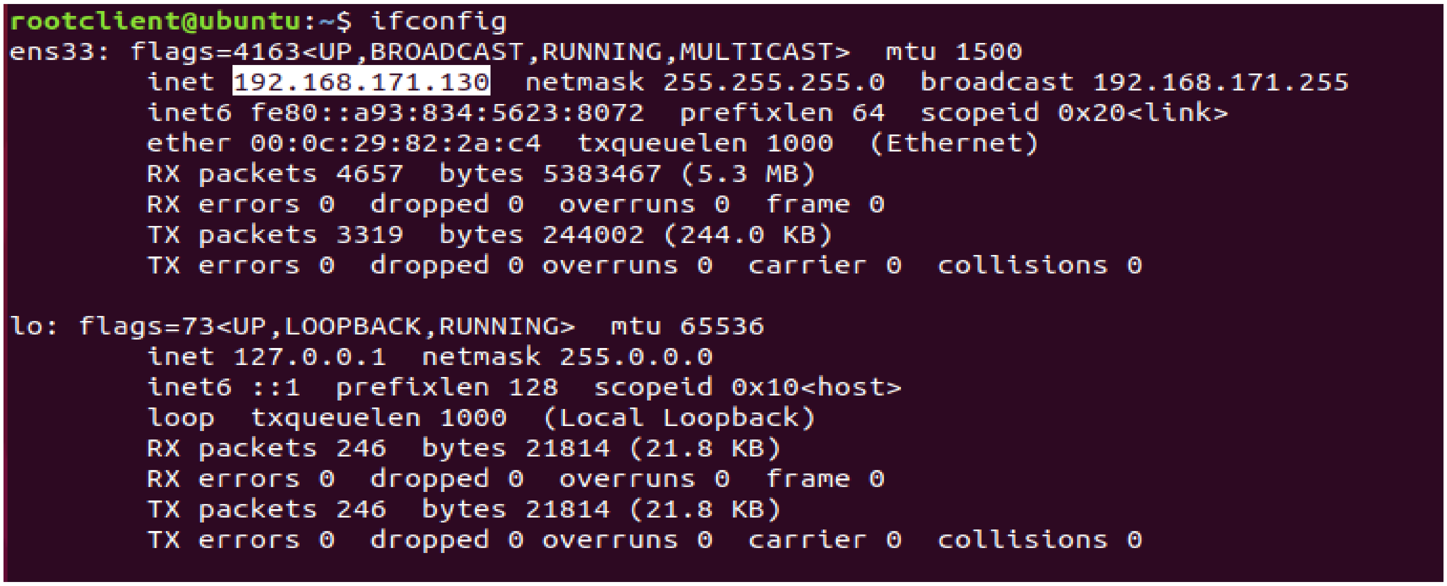
```
rootclient@ubuntu:~$ sudo apt-get install openssh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-client is already the newest version (1:7.6p1-4ubuntu0.3).
openssh-client set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```

To connect to your Ubuntu machine over LAN you only need to enter the following command:

#ssh rootclient@192.168.171.130

- Change the username with the **actual user name** and ip_address with the **IP Address of the Ubuntu machine where you installed SSH.**
- If you don't know your IP address you can easily find it using the ifconfig command:

# ifconfig



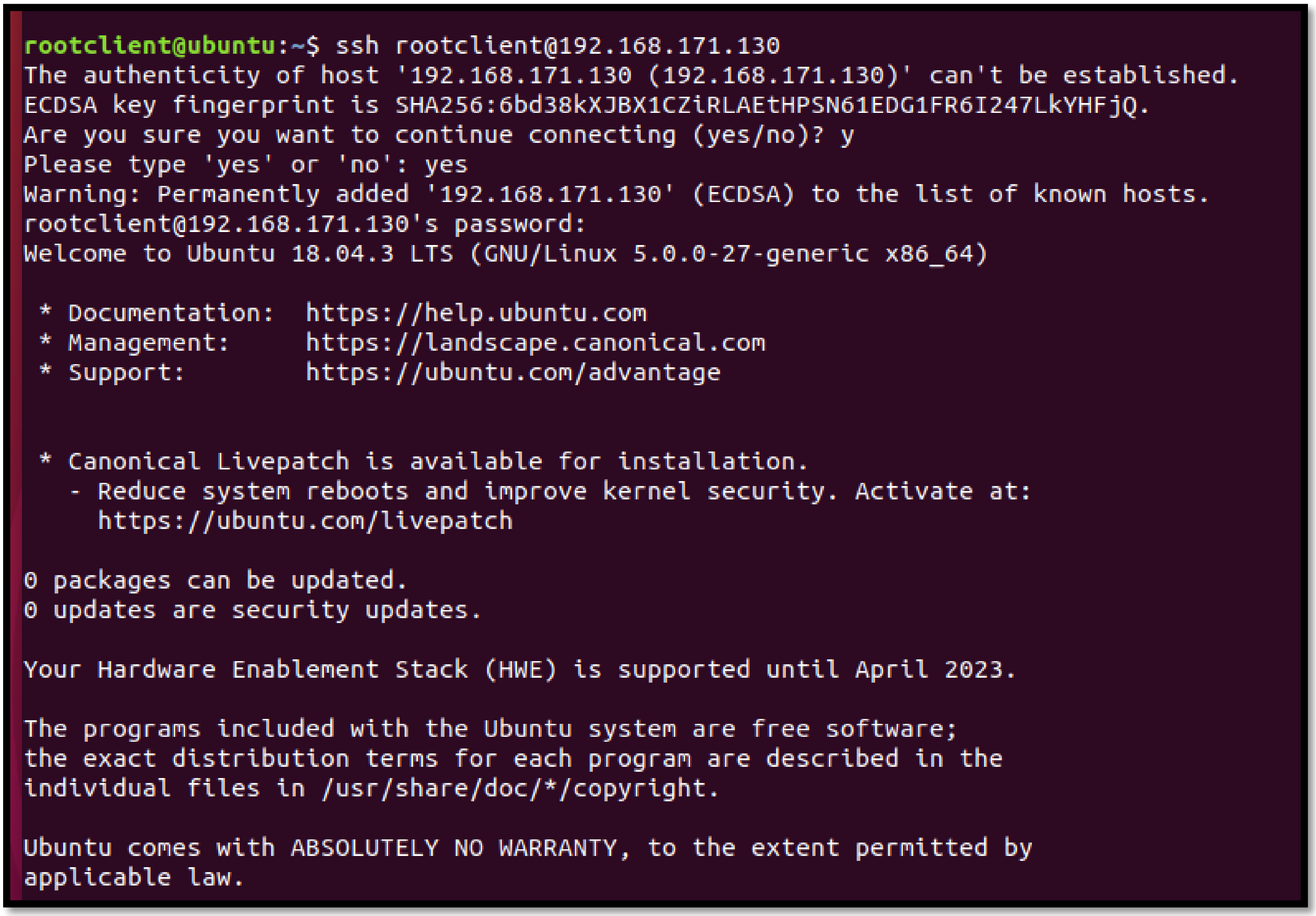
```
rootclient@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.171.130  netmask 255.255.255.0  broadcast 192.168.171.255
        inet6 fe80::a93:834:5623:8072  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:82:2a:c4  txqueuelen 1000  (Ethernet)
        RX packets 4657  bytes 5383467 (5.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3319  bytes 244002 (244.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 246  bytes 21814 (21.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 246  bytes 21814 (21.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

As you can see from the output, the system IP address is **192.168.171.130.**

Once you’ve found the IP address, go back to the remote machine you’re trying to log in with and enter the following command:

#ssh rootclient@192.168.171.130

When you connect through SSH for the first time, you will see a message looking something like this:



```
rootclient@ubuntu:~$ ssh rootclient@192.168.171.130
The authenticity of host '192.168.171.130 (192.168.171.130)' can't be established.
ECDSA key fingerprint is SHA256:6bd38kXJBX1CZiRLAEtHPSN61EDG1FR6I247LkYHFjQ.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.171.130' (ECDSA) to the list of known hosts.
rootclient@192.168.171.130's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.0.0-27-generic x86_64)

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


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

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.
```

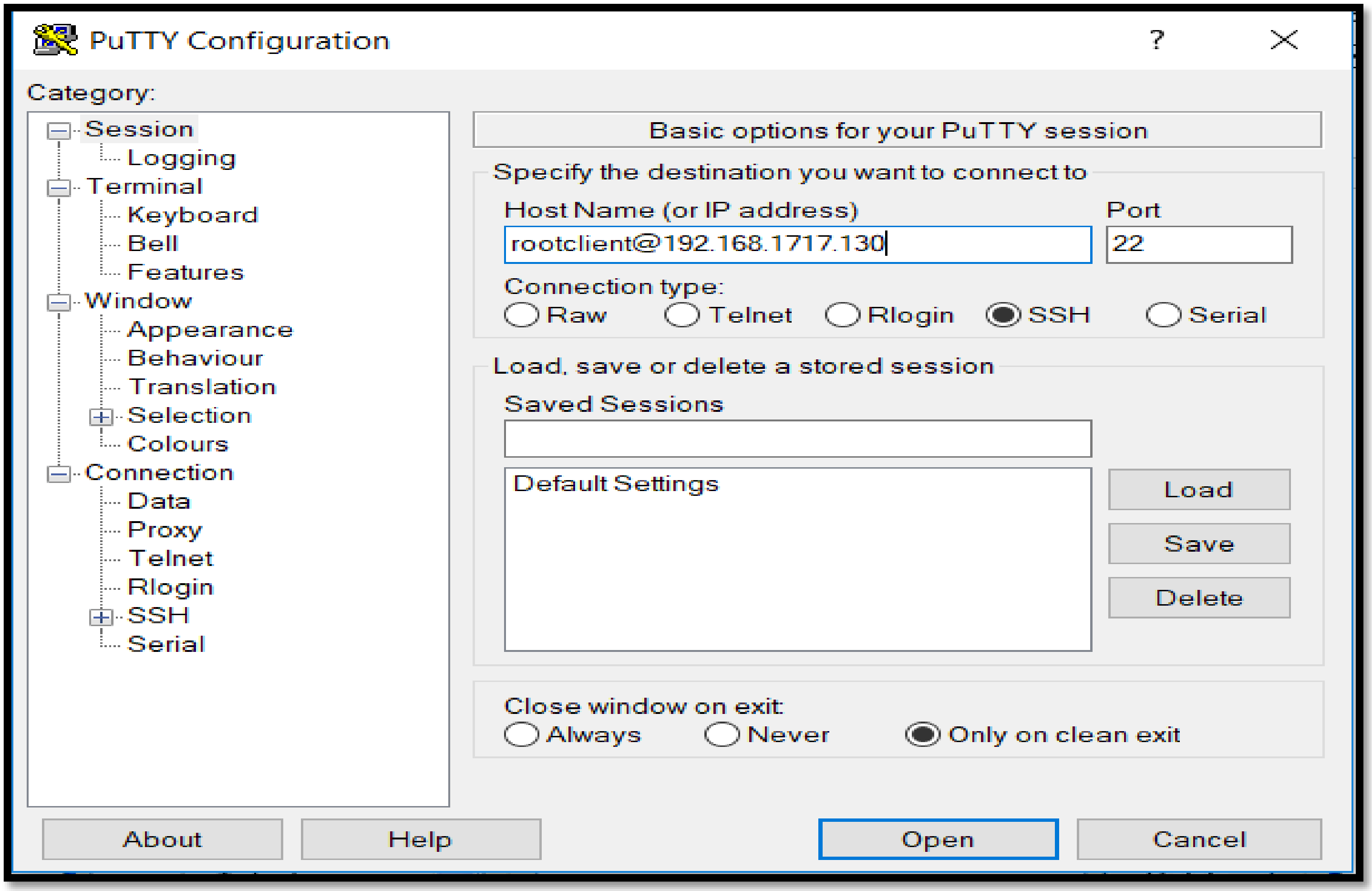
You are now logged in to your Ubuntu machine.

Step 5:- Install SSH-client over Windows

Step 5.1:- Install PuTTY

PuTTY is a free and open source SSH client for Windows and UNIX systems. It provides easy connectivity to any server running an SSH daemon, so you can work as if you were logged into a console session on the remote system.

- Download and run the PuTTY installer on Windows.
- When you open PuTTY, you’ll be shown the configuration menu. Enter the hostname or IP address of your Server. PuTTY’s default TCP port is 22, the IANA assigned port for for SSH traffic. Change it if your server is listening on a different port. Name the session in the Saved Sessions text bar if you choose, and click Save:



Specify the destination you want to connect to

Host Name (or IP address): rootclient@192.168.1717.130

Port: 22

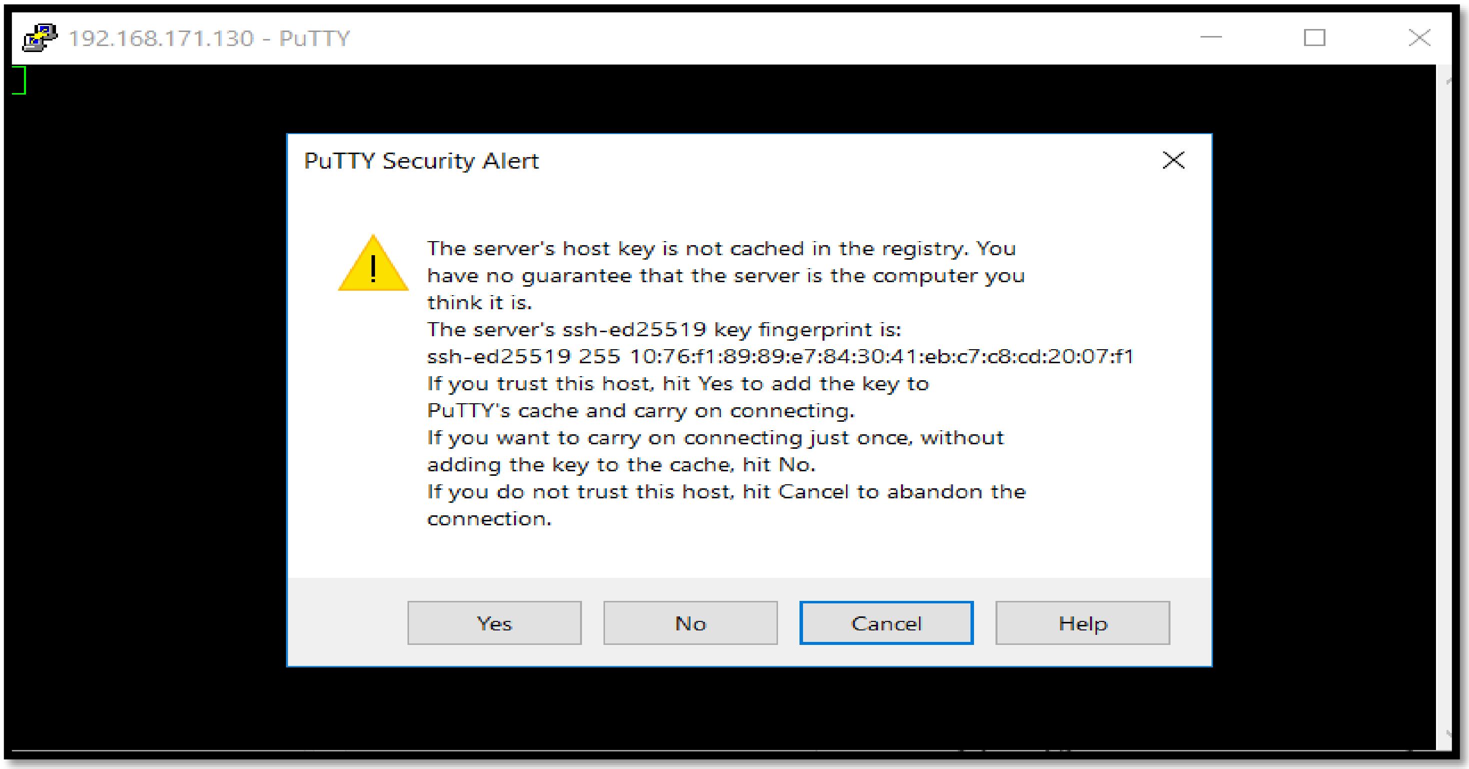
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

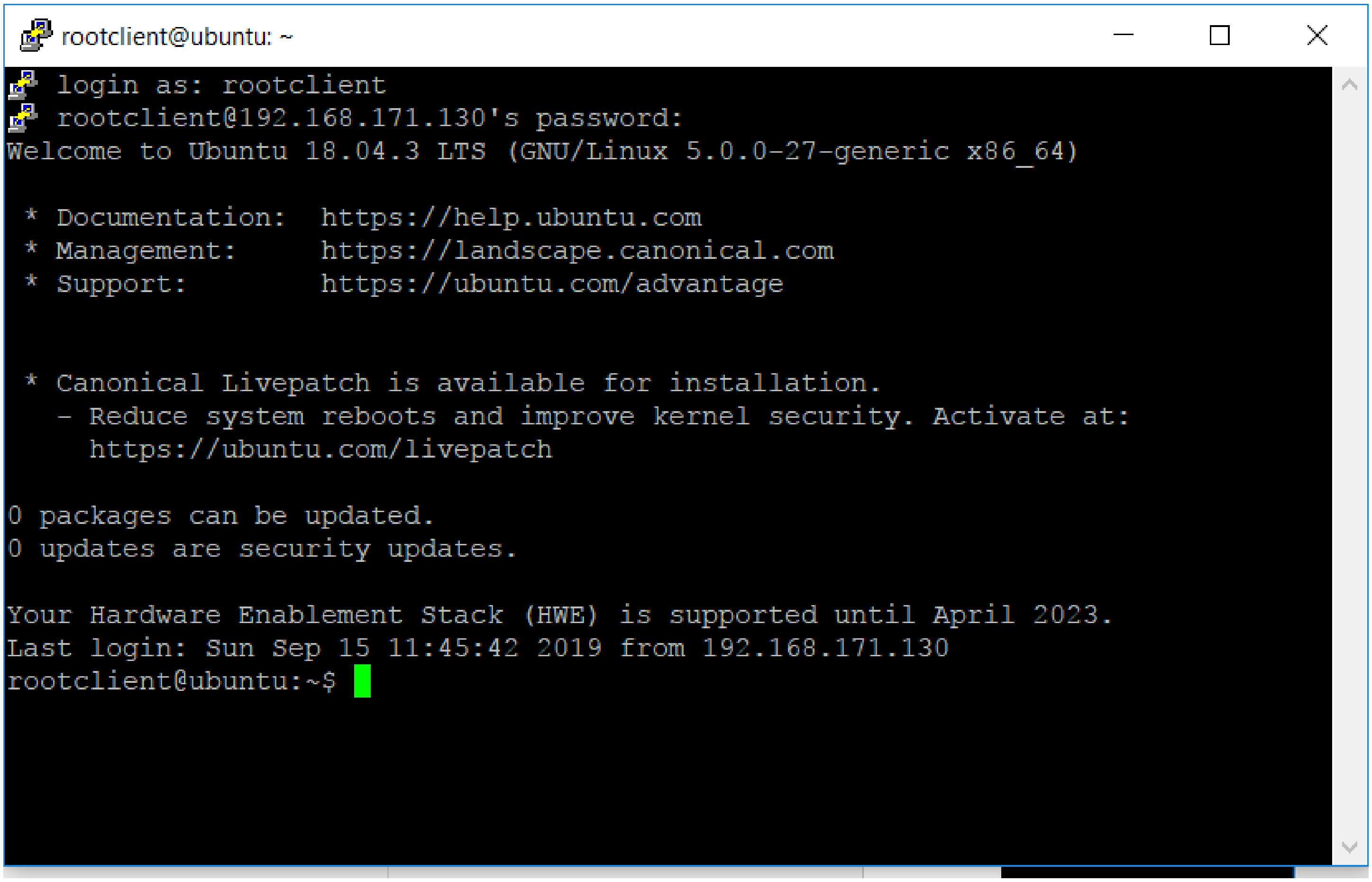
Click Open to start an SSH session. If you have never previously logged into this system with PuTTY, you will see a message alerting you that the server's SSH key fingerprint is new, and asking if you want to proceed.

Do not click anything yet! Verify the fingerprint first.



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 10:76:f1:89:89:e7:84:30:41:eb:c7:c8:cd:20:07:f1
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

Login as username and enter password to connect the SSH-server

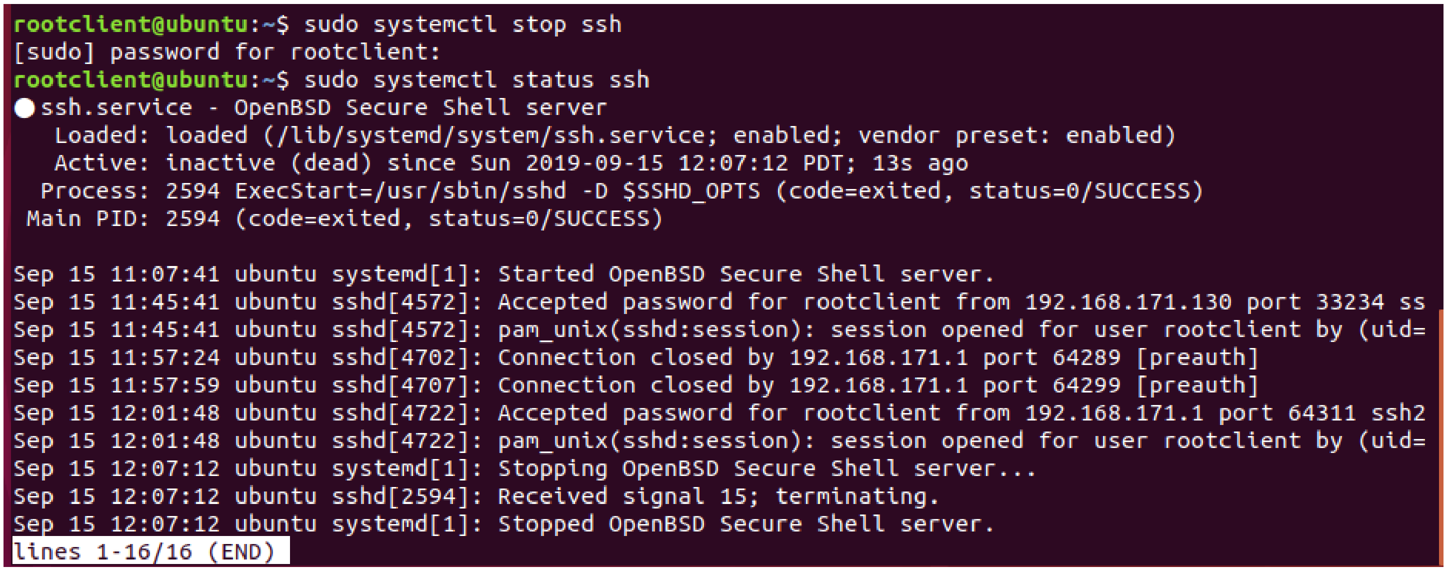


```
login as: rootclient
rootclient@192.168.171.130's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.0.0-27-generic x86_64)

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


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Sun Sep 15 11:45:42 2019 from 192.168.171.130
rootclient@ubuntu:~$
```

Step 6:- Disabling SSH on Ubuntu

If for some reason you want to disable SSH on your Ubuntu machine you can simply stop the SSH service by running:

sudo systemctl stop ssh



```
rootclient@ubuntu:~$ sudo systemctl stop ssh
[sudo] password for rootclient:
rootclient@ubuntu:~$ sudo systemctl status ssh
○ ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Sun 2019-09-15 12:07:12 PDT; 13s ago
  Process: 2594 ExecStart=/usr/sbin/sshd -D $SSHD_OPTS (code=exited, status=0/SUCCESS)
 Main PID: 2594 (code=exited, status=0/SUCCESS)

Sep 15 11:07:41 ubuntu systemd[1]: Started OpenBSD Secure Shell server.
Sep 15 11:45:41 ubuntu sshd[4572]: Accepted password for rootclient from 192.168.171.130 port 33234 ss
Sep 15 11:45:41 ubuntu sshd[4572]: pam_unix(sshd:session): session opened for user rootclient by (uid=
Sep 15 11:57:24 ubuntu sshd[4702]: Connection closed by 192.168.171.1 port 64289 [preauth]
Sep 15 11:57:59 ubuntu sshd[4707]: Connection closed by 192.168.171.1 port 64299 [preauth]
Sep 15 12:01:48 ubuntu sshd[4722]: Accepted password for rootclient from 192.168.171.1 port 64311 ssh2
Sep 15 12:01:48 ubuntu sshd[4722]: pam_unix(sshd:session): session opened for user rootclient by (uid=
Sep 15 12:07:12 ubuntu systemd[1]: Stopping OpenBSD Secure Shell server...
Sep 15 12:07:12 ubuntu sshd[2594]: Received signal 15; terminating.
Sep 15 12:07:12 ubuntu systemd[1]: Stopped OpenBSD Secure Shell server.
lines 1-16/16 (END)
```

To start it again run:

sudo systemctl start ssh