

# Lab Assignment



Cybersecurity Professional Program

Linux Security

## Services and Hardening

**LNK-05-L1**

**Install and Configure SSH**

## Lab Objective

Understand how to configure a new virtual machine in VirtualBox and how to transfer a file via Secure Copy Protocol (SCP).

## Lab Mission

Install the SSH service for remote connection, use Secure Copy Protocol (SCP) to transfer files, and work with the Ubuntu Linux distribution.

## Lab Duration

40–50 minutes

## Requirements

- Practical experience with the APT package manager
- Knowledge of networking configuration
- Knowledge of SSH commands

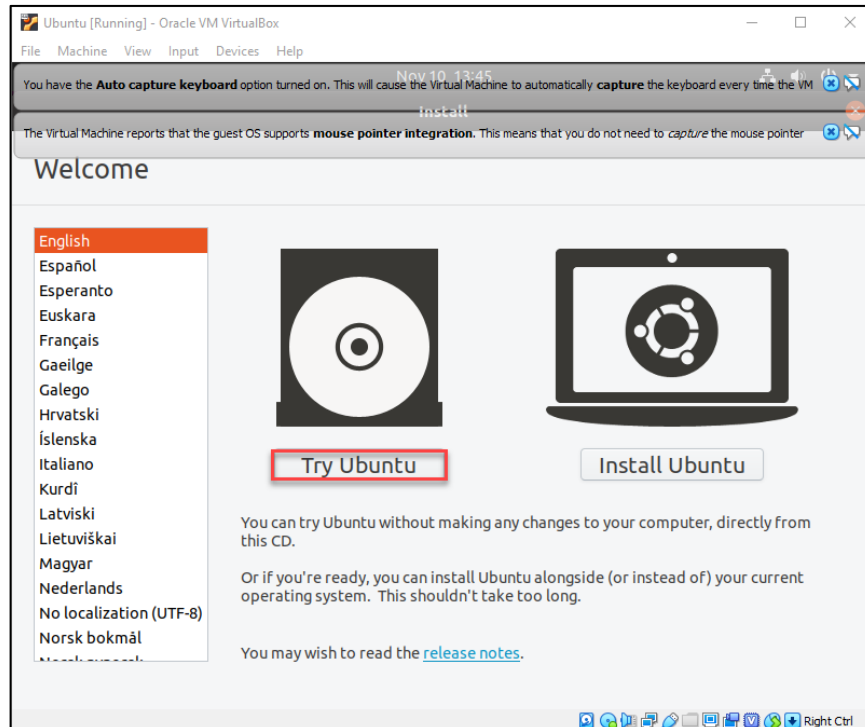
## Resources

- Environment & Tools
  - VirtualBox
    - Debian
    - Ubuntu 20.04
  - SSH

## Lab Task 1: Ubuntu CD Disc Startup

Use the Ubuntu 20.04 installation guide to create a new Ubuntu machine for use throughout the course.

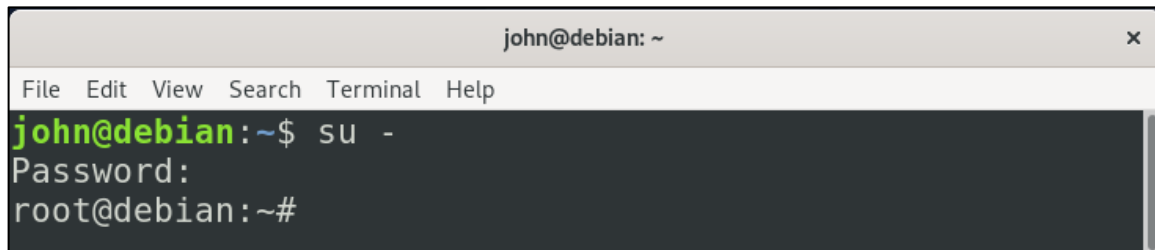
**Note:** When you reach step 15 in the installation guide, click ***Try Ubuntu*** instead of ***Install Ubuntu***.



## Lab Task 2: Install SSH and Work with SSH and SCP

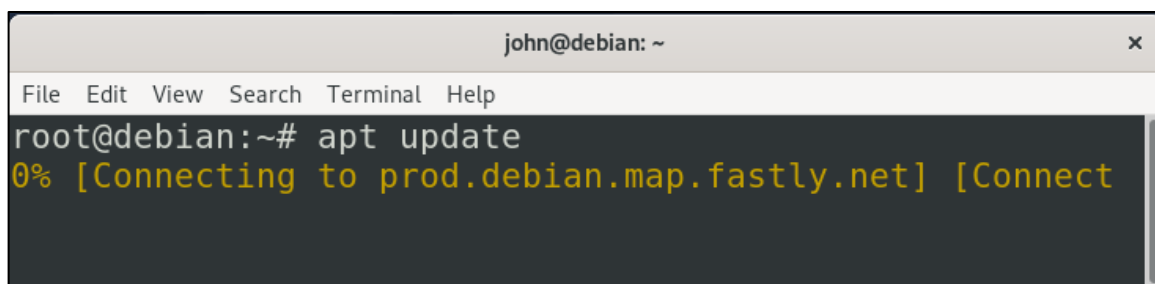
Facilitate communication between two Linux clients using Secure Shell (SSH).

- 1 Open the terminal and use the command ***su -*** to switch to the root user.



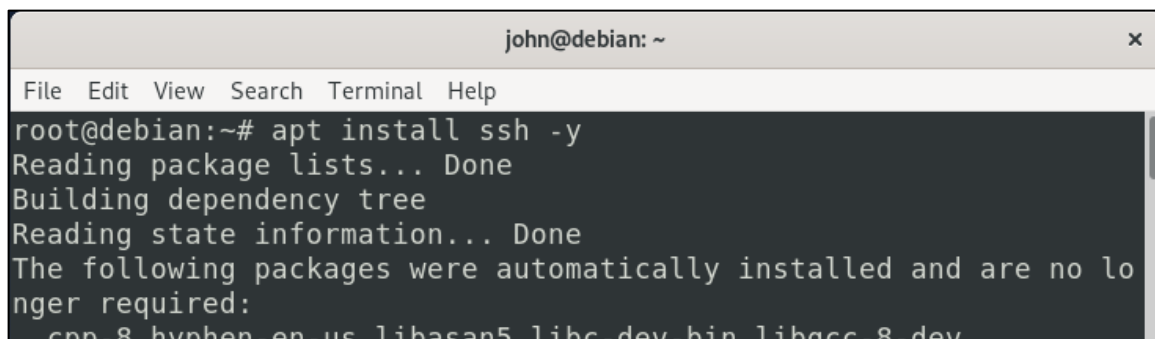
```
john@debian: ~  
File Edit View Search Terminal Help  
john@debian:~$ su -  
Password:  
root@debian:~#
```

- 2 Use the ***apt update*** command.



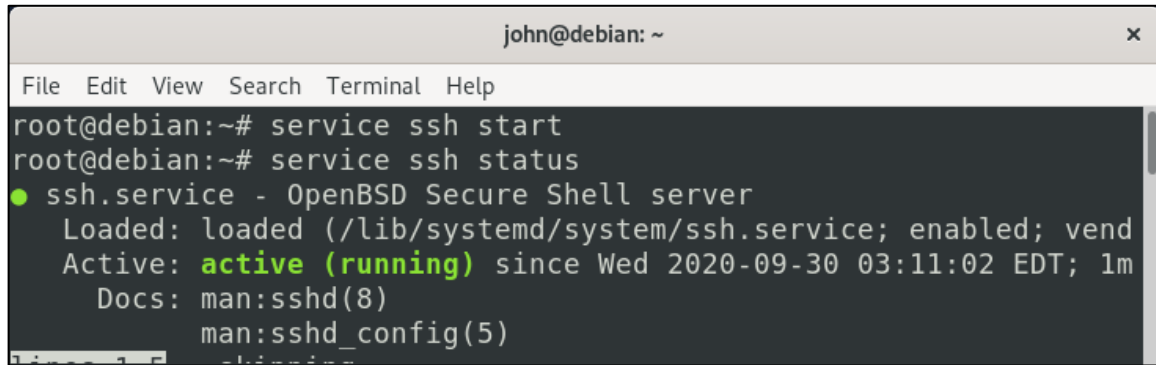
```
john@debian: ~  
File Edit View Search Terminal Help  
root@debian:~# apt update  
0% [Connecting to prod.debian.map.fastly.net] [Connect
```

- 3 Use the command ***apt install ssh -y*** to install the SSH service.



```
john@debian: ~  
File Edit View Search Terminal Help  
root@debian:~# apt install ssh -y  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  cpp-8 g++-8 libasan5 libc-dev-bin libc6-dev
```

- 4 Use the command ***service ssh start*** to start the SSH service. Verify that SSH is running and active using the ***service ssh status*** command.

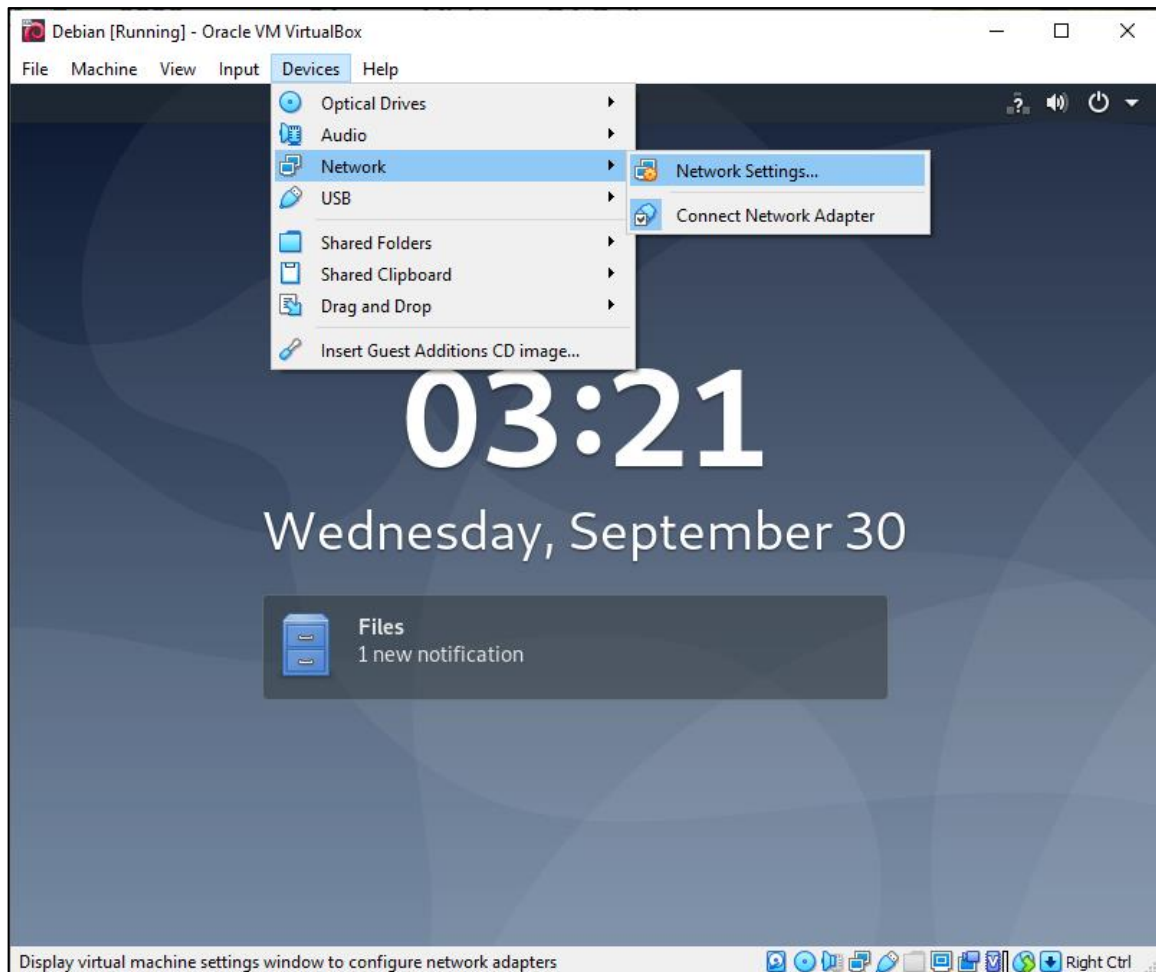
A terminal window titled 'john@debian: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
root@debian:~# service ssh start
root@debian:~# service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vend
   Active: active (running) since Wed 2020-09-30 03:11:02 EDT; 1m
   Docs: man:sshd(8)
         man:sshd_config(5)
```

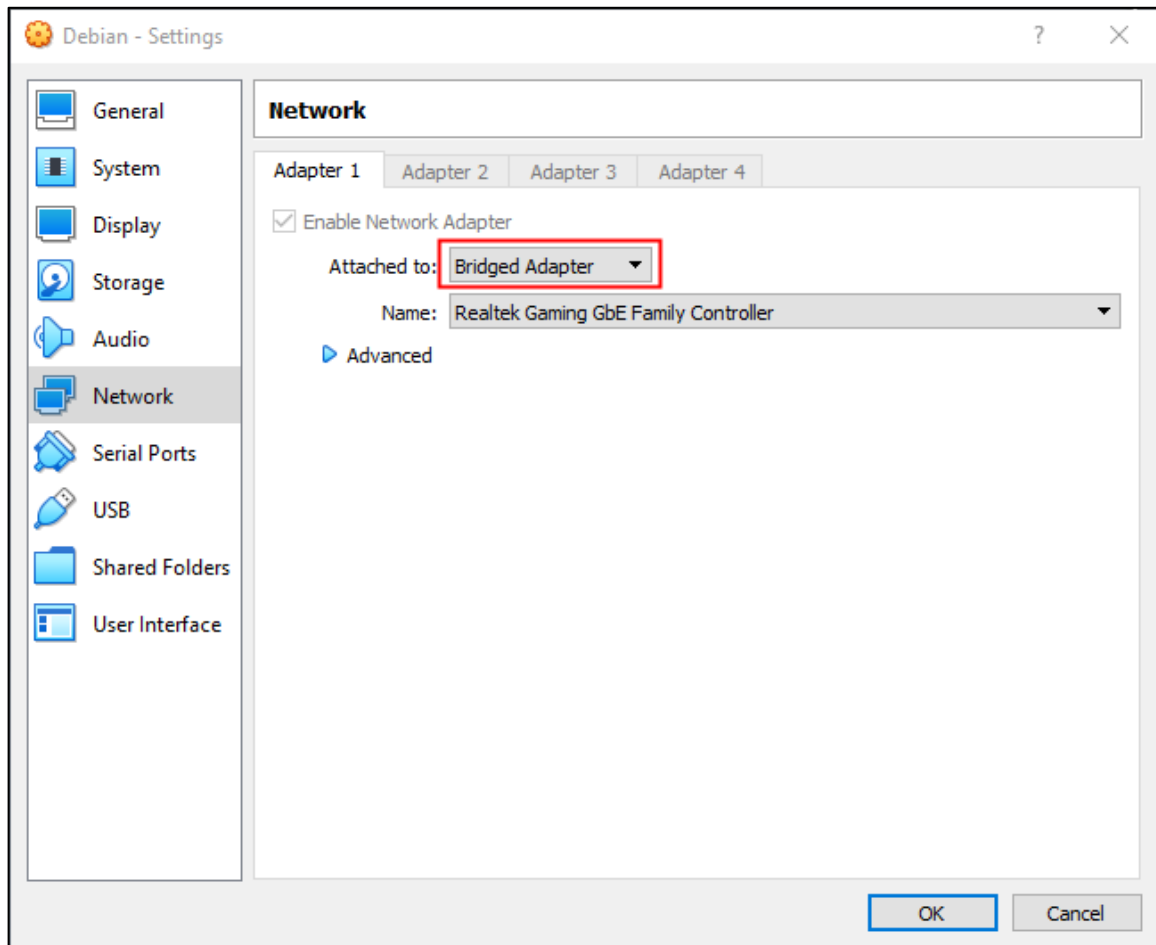
## Lab Task 3: Debian/Ubuntu Network Configuration

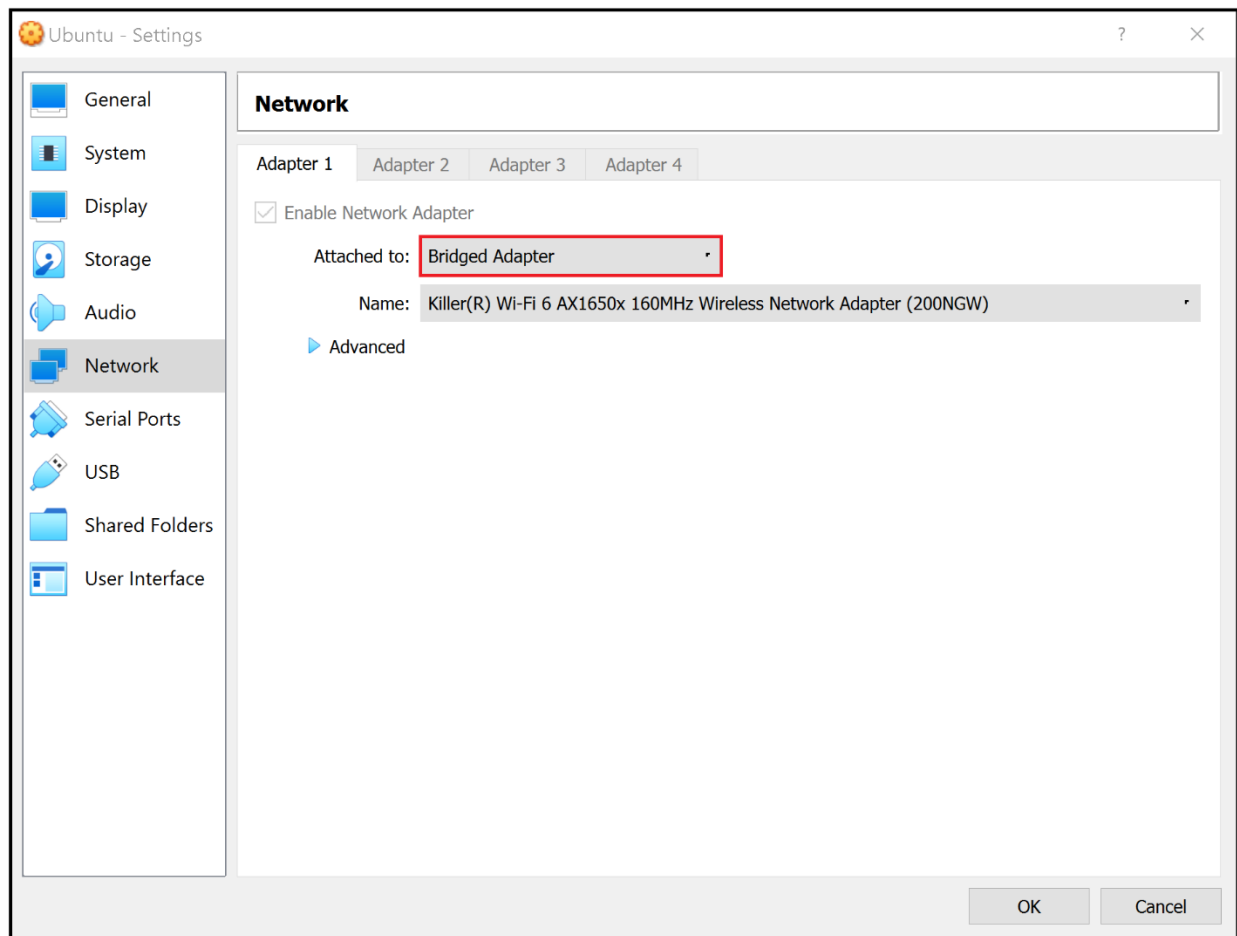
In this task, you will verify that Debian/Ubuntu is in bridged mode and is connected to the internet.

- 1 Click **Devices** in the VM menu, select **Network**, and click **Network Settings...** to open the network configuration window.



- 2 Select the ***Bridged Adapter*** option and click **OK**.  
**Note:** If the ***Bridged Adapter*** causes issues, try NAT.







- 3 Use the command **ip a** to verify the IP address of your local machines. Verify the Debian/Ubuntu machines received an appropriate IP address on the local network.

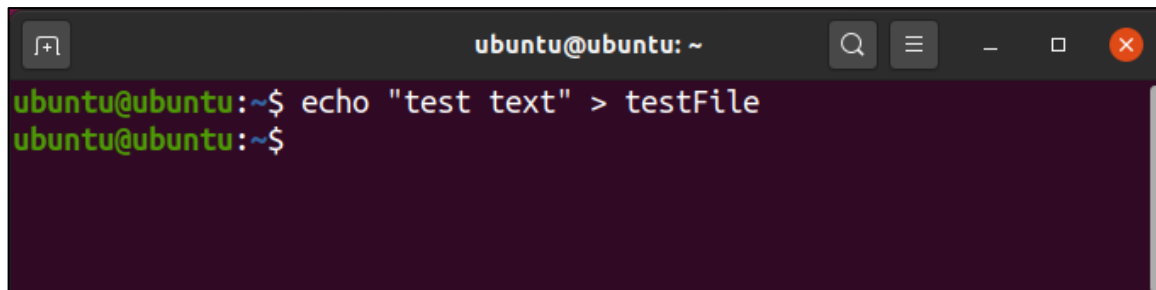
```
john@debian: ~  
File Edit View Search Terminal Help  
root@debian:~# ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
    link/ether 08:00:27:6d:00:ff brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.12/24 brd 192.168.1.255 scope global dynamic enp0s3  
        valid_lft 3598sec preferred_lft 3598sec  
    inet6 2a00:a040:19c:a2e7:a00:27ff:fe6d:ff/64 scope global dynamic mngtmpaddr  
        valid_lft 808166sec preferred_lft 330576sec  
    inet6 fe80::a00:27ff:fe6d:ff/64 scope link  
        valid_lft forever preferred_lft forever  
root@debian:~#
```

```
john@john-VirtualBox:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:bb:76:30 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.0.46/24 brd 192.168.0.255 scope global dynamic noprefixroute enp0s3  
        valid_lft 86206sec preferred_lft 86206sec  
    inet6 fe80::c81c:5495:e80f:d599/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

## Lab Task 4: File Creation and Transfer

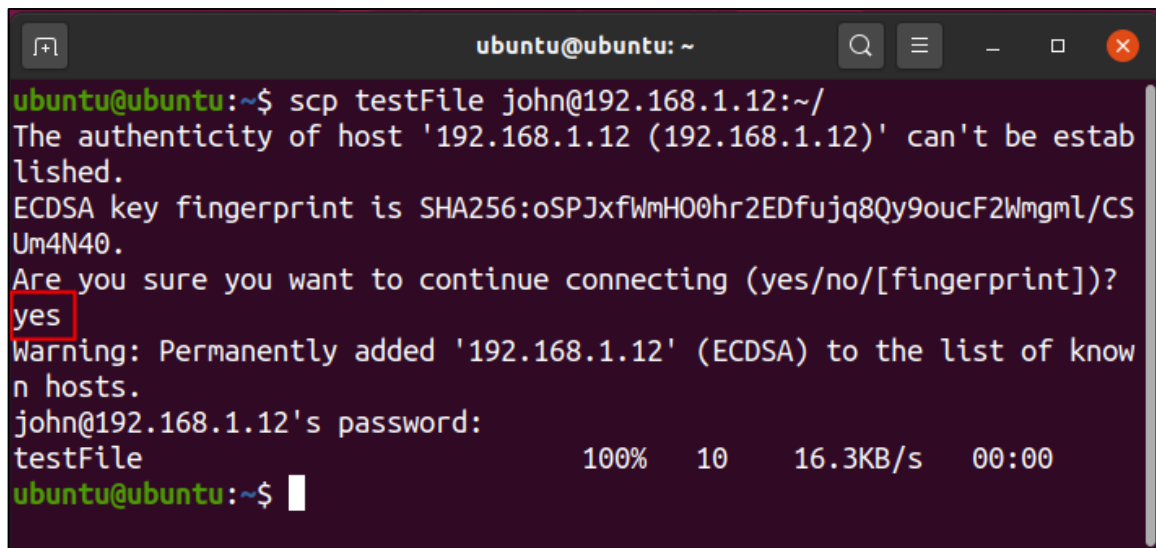
In this task, you will create a file on the Ubuntu machine and transfer it to the Debian machine.

- 1 Open the terminal in the same way you open it in Debian. Use the command **`echo "test text" > testFile`** to create a new file with the text *test text*.

A terminal window titled 'ubuntu@ubuntu: ~' with search, menu, and window control icons. It shows the command 'echo "test text" > testFile' being executed, followed by a new prompt 'ubuntu@ubuntu:~\$' on the next line.

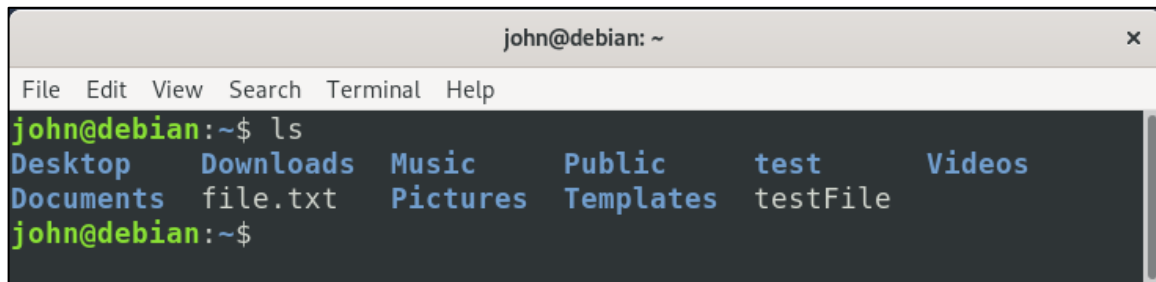
```
ubuntu@ubuntu: ~  
ubuntu@ubuntu:~$ echo "test text" > testFile  
ubuntu@ubuntu:~$
```

- 2 Use the command **`scp testFile <user>@<ip address>:~/`** to transfer the file from Ubuntu to your home directory on the Debian machine via SCP. Type **yes** when asked to connect and provide your password.

A terminal window titled 'ubuntu@ubuntu: ~' showing the execution of 'scp testFile john@192.168.1.12:~/'. It displays a warning about host authenticity, asks for confirmation to continue, and the user responds 'yes'. It then prompts for the password, shows the file transfer progress (100%, 10 files, 16.3KB/s, 00:00), and ends with a new prompt 'ubuntu@ubuntu:~\$'.

```
ubuntu@ubuntu: ~  
ubuntu@ubuntu:~$ scp testFile john@192.168.1.12:~/  
The authenticity of host '192.168.1.12 (192.168.1.12)' can't be established.  
ECDSA key fingerprint is SHA256:oSPJxfWmH00hr2EDfujq8Qy9oucF2Wmgm1/CS  
Um4N40.  
Are you sure you want to continue connecting (yes/no/[fingerprint])?  
yes  
Warning: Permanently added '192.168.1.12' (ECDSA) to the list of know  
n hosts.  
john@192.168.1.12's password:  
testFile                               100%  10   16.3KB/s   00:00  
ubuntu@ubuntu:~$
```

- 3 On the Debian machine, navigate to your home directory and verify the file was transferred using the *ls* command.



```
john@debian: ~  
File Edit View Search Terminal Help  
john@debian:~$ ls  
Desktop    Downloads  Music      Public     test       Videos  
Documents  file.txt   Pictures   Templates  testFile  
john@debian:~$
```