Passwordless SSH Connections Between Linux machines

Full Name: Klajdi Cami

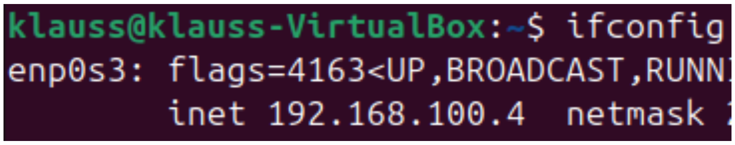
Procedure before the activity:

First, we open the two virtual machines and run the command

ifconfig

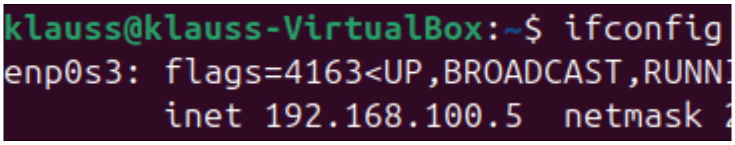
in the terminal of both to see the different IP addresses.

Client:



```
klauss@klauss-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNN
        inet 192.168.100.4  netmask
```

Server:

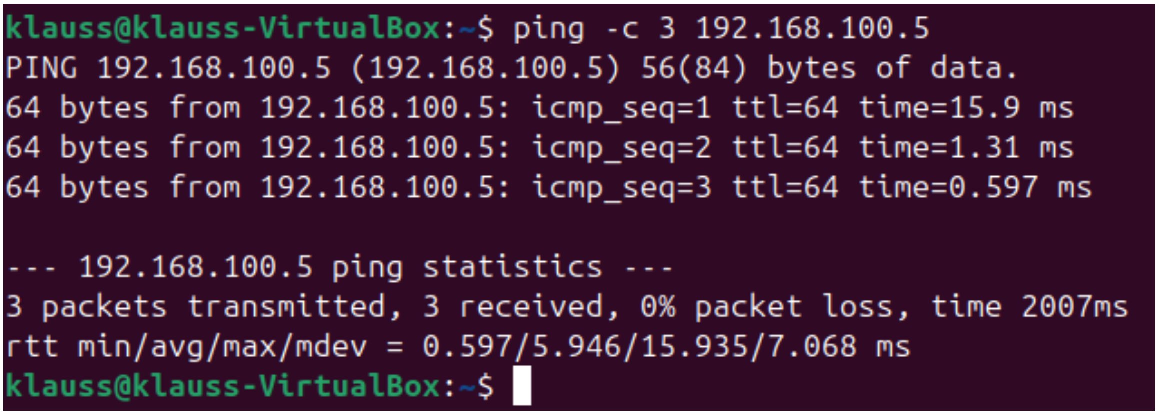


```
klauss@klauss-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNN
        inet 192.168.100.5  netmask
```

Then, we run the command

Ping -c 192.168.100.5

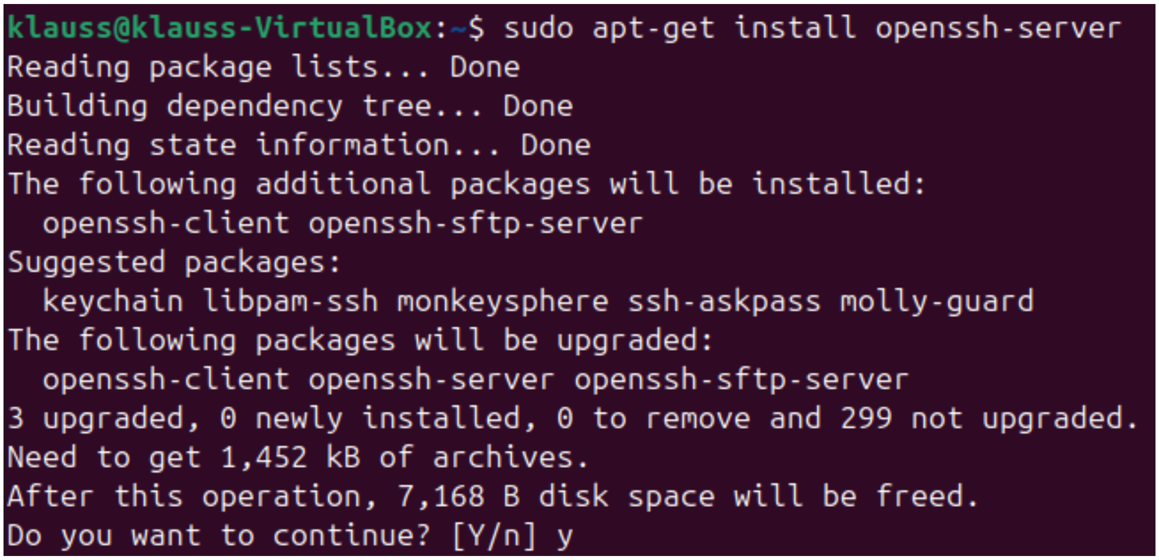
on the client to confirm the connectivity between the two machines.



```
klauss@klauss-VirtualBox:~$ ping -c 3 192.168.100.5
PING 192.168.100.5 (192.168.100.5) 56(84) bytes of data.
64 bytes from 192.168.100.5: icmp_seq=1 ttl=64 time=15.9 ms
64 bytes from 192.168.100.5: icmp_seq=2 ttl=64 time=1.31 ms
64 bytes from 192.168.100.5: icmp_seq=3 ttl=64 time=0.597 ms

--- 192.168.100.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 0.597/5.946/15.935/7.068 ms
klauss@klauss-VirtualBox:~$
```

We install and update the **openssh** application on the Linux virtual machine that acts as the server with the command

sudo apt-get install openssh-server



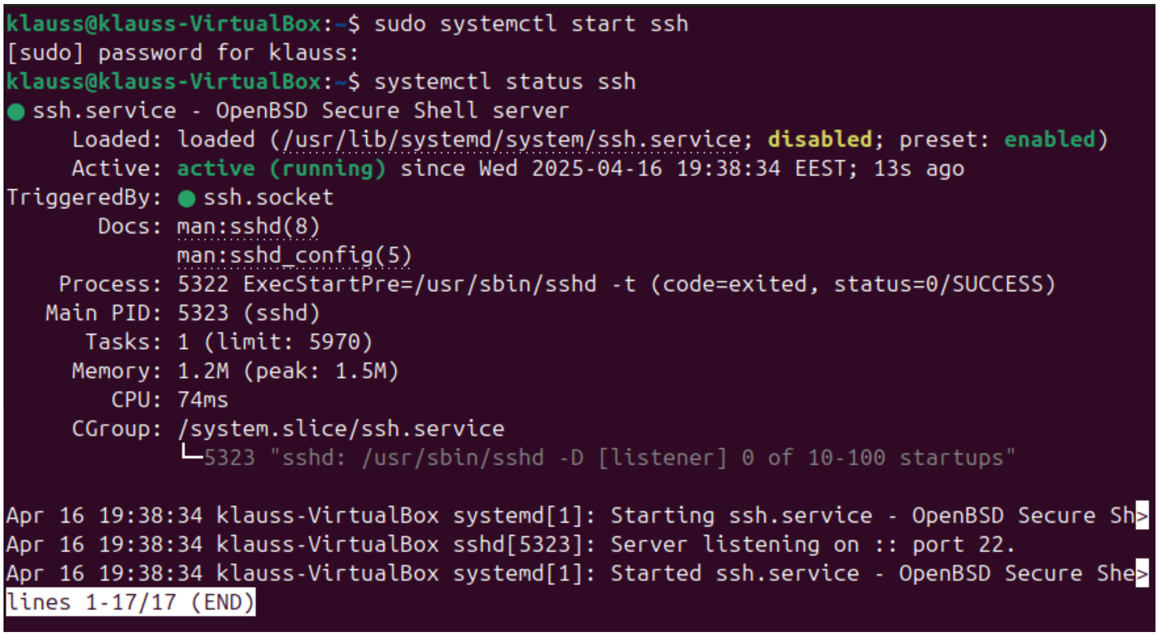
```
klauss@klauss-VirtualBox:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  openssh-client openssh-sftp-server
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following packages will be upgraded:
  openssh-client openssh-server openssh-sftp-server
3 upgraded, 0 newly installed, 0 to remove and 299 not upgraded.
Need to get 1,452 kB of archives.
After this operation, 7,168 B disk space will be freed.
Do you want to continue? [Y/n] y
```

Then we start the service using the command

sudo systemctl start ssh

and check if it is up and running using

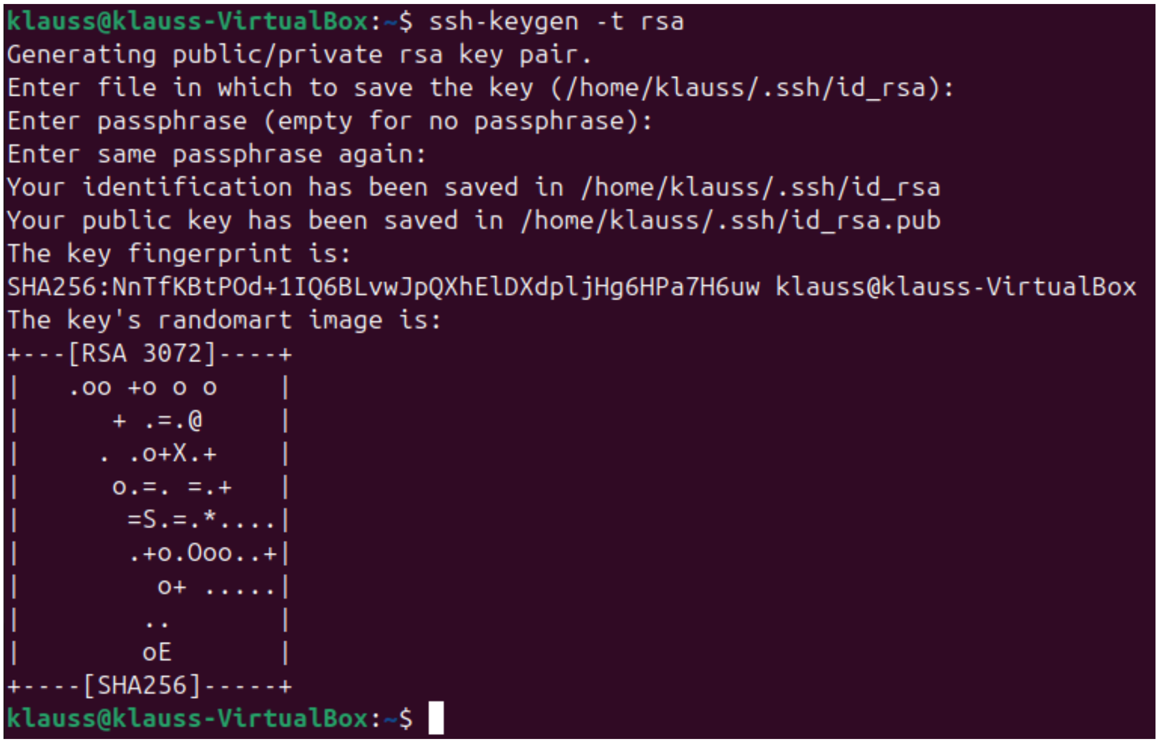
systemctl status ssh



```
klauss@klauss-VirtualBox:~$ sudo systemctl start ssh
[sudo] password for klauss:
klauss@klauss-VirtualBox:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
     Active: active (running) since Wed 2025-04-16 19:38:34 EEST; 13s ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 5322 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 5323 (sshd)
      Tasks: 1 (limit: 5970)
     Memory: 1.2M (peak: 1.5M)
        CPU: 74ms
     CGroup: /system.slice/ssh.service
             └─5323 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Apr 16 19:38:34 klauss-VirtualBox systemd[1]: Starting ssh.service - OpenBSD Secure Sh>
Apr 16 19:38:34 klauss-VirtualBox sshd[5323]: Server listening on :: port 22.
Apr 16 19:38:34 klauss-VirtualBox systemd[1]: Started ssh.service - OpenBSD Secure She>
lines 1-17/17 (END)
```

On the client side, we generate a key pair (public key cryptography) using the command

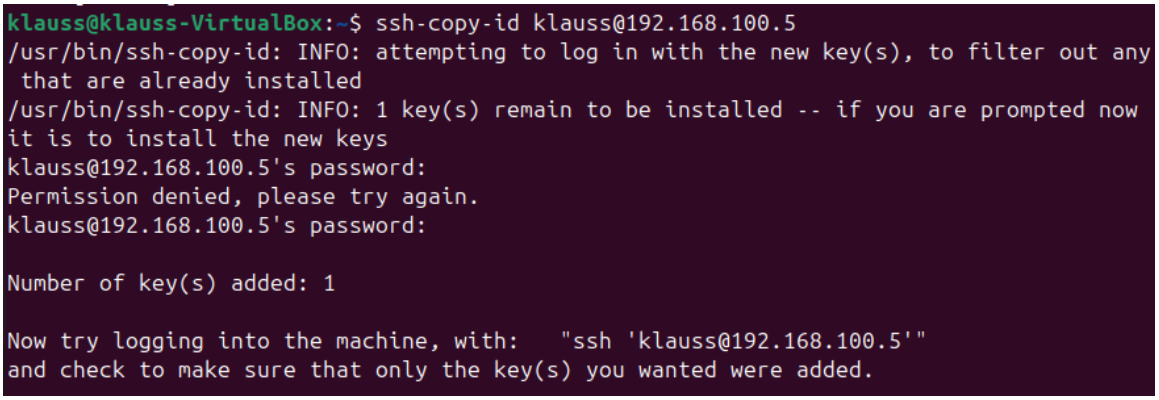
ssh-keygen -t rsa



```
klauss@klauss-VirtualBox:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/klauss/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/klauss/.ssh/id_rsa
Your public key has been saved in /home/klauss/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:NnTfKBtPOd+1IQ6BLvwJpQXhElDXdpljHg6HPa7H6uw klauss@klauss-VirtualBox
The key's randomart image is:
+---[RSA 3072]----+
|   .oo +o o o    |
|      + .=.@     |
|     . .o+X.+    |
|      o.=. =.+   |
|       =S.=.*....|
|       .+o.Ooo..+|
|         o+ .....|
|        ..       |
|        oE       |
+----[SHA256]-----+
klauss@klauss-VirtualBox:~$ 
```

Next, we copy the public key to the server using the command

ssh-copy-id “server’s user name”@”server’s IP address”



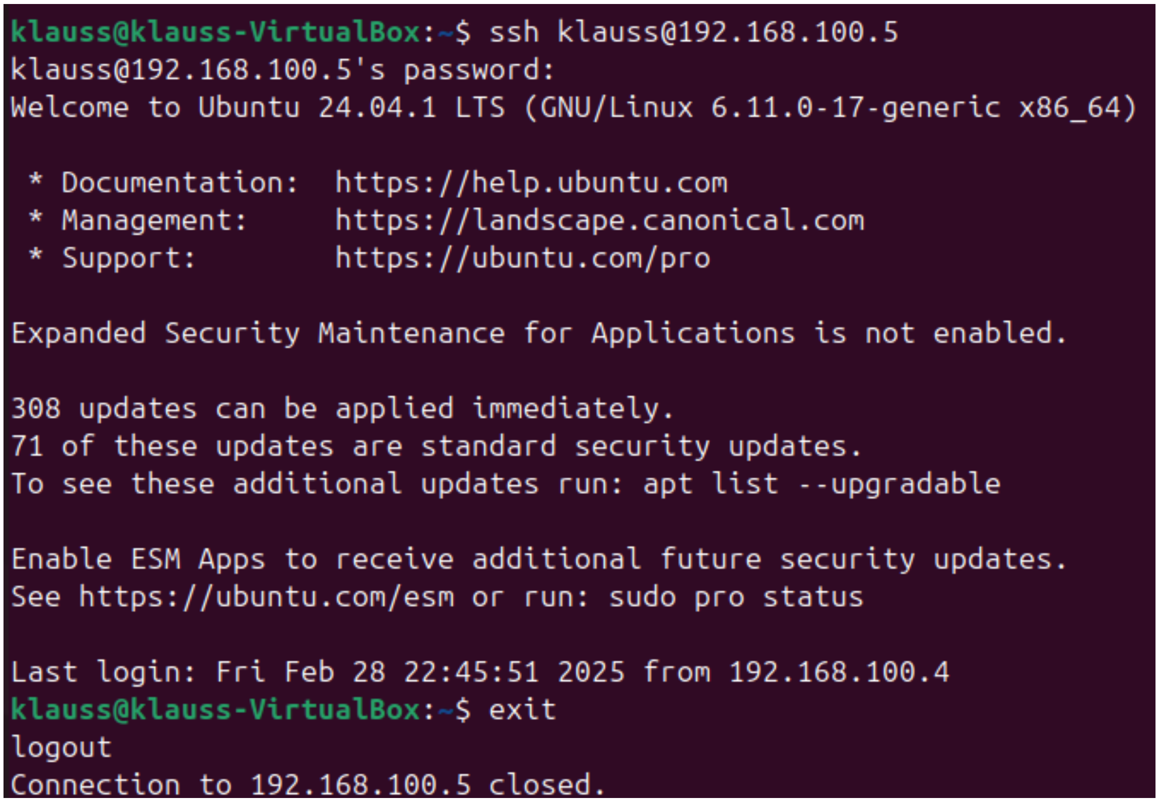
```
klauss@klauss-VirtualBox:~$ ssh-copy-id klauss@192.168.100.5
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any
 that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now
it is to install the new keys
klauss@192.168.100.5's password:
Permission denied, please try again.
klauss@192.168.100.5's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'klauss@192.168.100.5'"
and check to make sure that only the key(s) you wanted were added.
```

We can connect via SSH from the client to the server by executing the command

ssh “server’s user name”@”server’s IP address”

And we disconnect from the server using the command

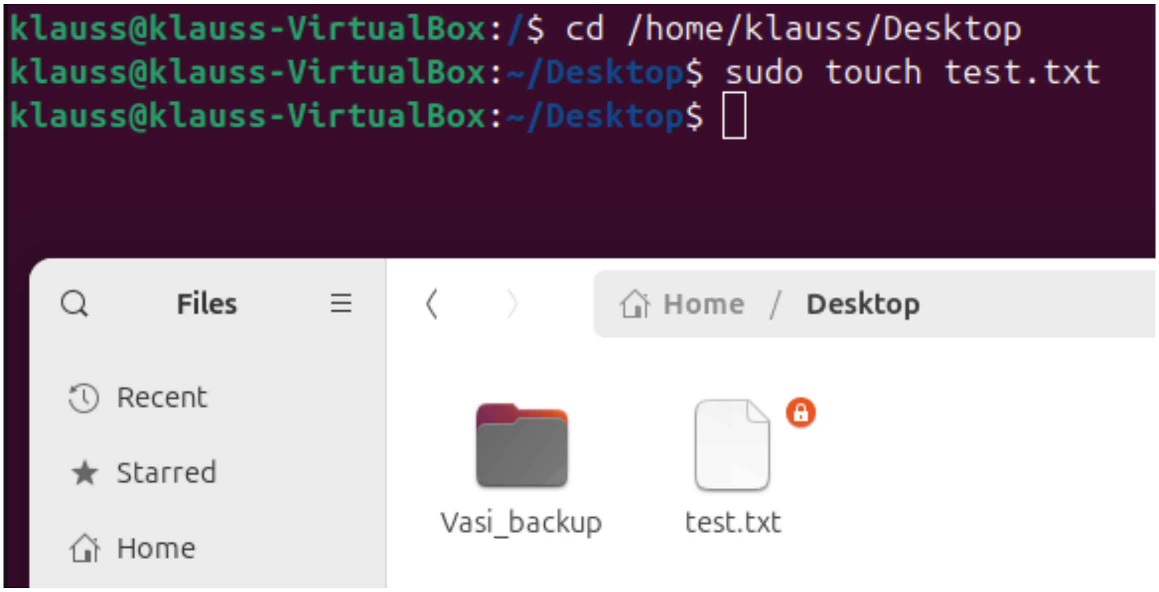
exit



```
klauss@klauss-VirtualBox:~$ ssh klauss@192.168.100.5
klauss@192.168.100.5's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.0-17-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

308 updates can be applied immediately.
71 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

Last login: Fri Feb 28 22:45:51 2025 from 192.168.100.4
klauss@klauss-VirtualBox:~$ exit
logout
Connection to 192.168.100.5 closed.
```

Creating and transferring a file with SCP

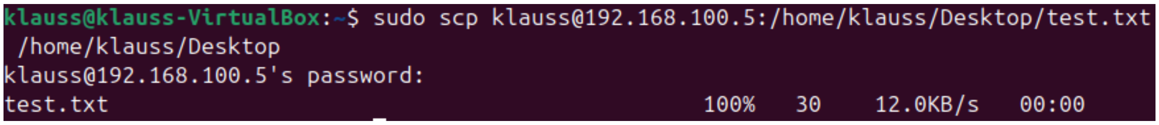
On the server machine, create a .txt file on the Desktop.



```
klauss@klauss-VirtualBox:/$ cd /home/klauss/Desktop
klauss@klauss-VirtualBox:~/Desktop$ sudo touch test.txt
klauss@klauss-VirtualBox:~/Desktop$ 
```

From the client side, we download the file we previously created to its own Desktop by executing the command

scp «client's username»@"Server's IP address":<server's path for .txt file> <client's path for .txt to be stored>



```
klauss@klauss-VirtualBox:~$ sudo scp klauss@192.168.100.5:/home/klauss/Desktop/test.txt
 /home/klauss/Desktop
klauss@192.168.100.5's password:
test.txt                                          100%   30    12.0KB/s   00:00
```

Activity 1:

Download the file "CyberSecurity Economics for Emerging Markets" from elearning on the Client side. Then, transfer this file to the server machine using scp.

<u>Answer:</u>

First, we download the file "CyberSecurity Economics for Emerging Markets" from elearning. Then, having connected to the server via SSH, we execute the following commands on the client:

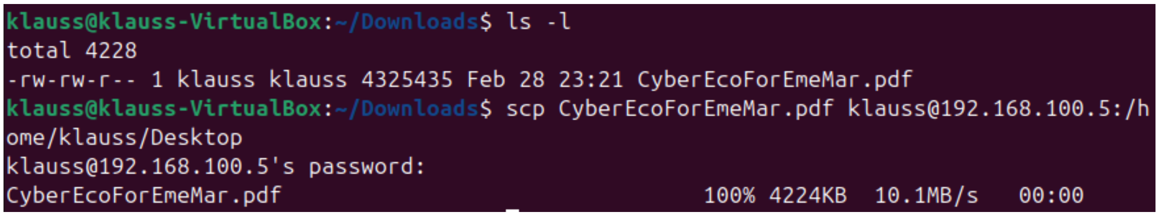
cd /home/klauss/Downloads

ls -l to see the file

and finally

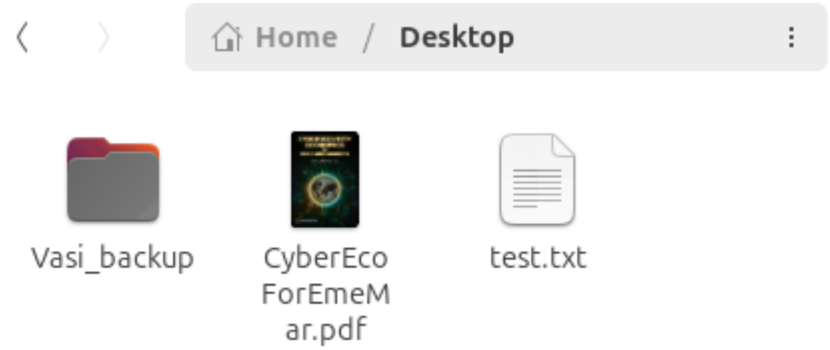
scp CyberEcoForEmeMar.pdf klauss@192.168.100.5:/home/klauss/Desktop

to send the file to the server



```
klauss@klauss-VirtualBox:~/Downloads$ ls -l
total 4228
-rw-rw-r-- 1 klauss klauss 4325435 Feb 28 23:21 CyberEcoForEmeMar.pdf
klauss@klauss-VirtualBox:~/Downloads$ scp CyberEcoForEmeMar.pdf klauss@192.168.100.5:/h
ome/klauss/Desktop
klauss@192.168.100.5's password:
CyberEcoForEmeMar.pdf                                  100% 4224KB  10.1MB/s   00:00
```

We confirm that the file has arrived on the server.


Home / Desktop
Vasi_backup
CyberEcoForEmeMar.pdf
test.txt