Name: Robin E. Valenzuela	**Date Performed:**
Course/Section:CPE31S24	**Date Submitted:**
Instructor: Engr. Jonathan Taylar	**Semester and SY:**

Activity 1: Configure Network using Virtual Machines

1. **Objectives:**

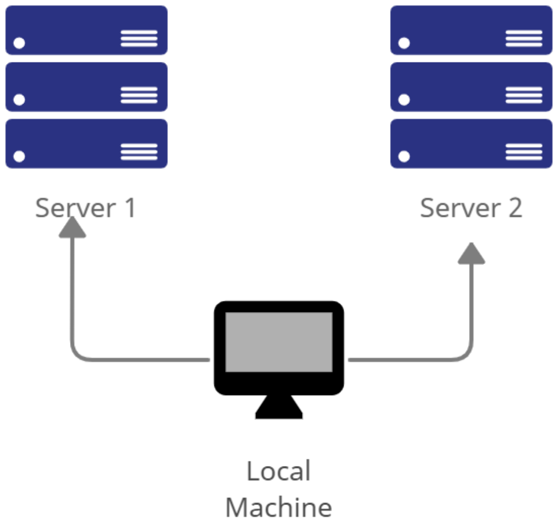
1.1. Create and configure Virtual Machines in Microsoft Azure or VirtualBox

1.2. Set-up a Virtual Network and Test Connectivity of VMs

2. **Discussion:**

Network Topology:

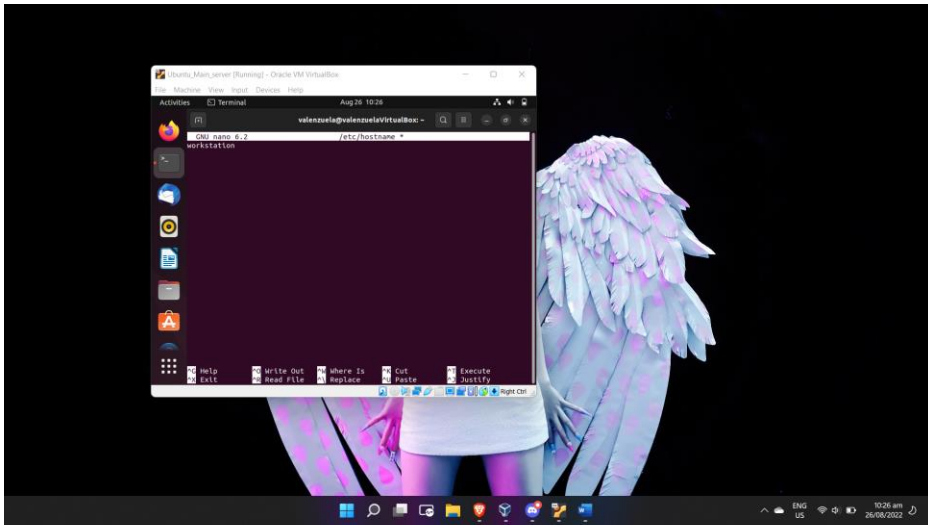
Assume that you have created the following network topology in Virtual Machines, *provide screenshots for each task*. (Note: *it is assumed that you have the prior knowledge of cloning and creating snapshots in a virtual machine*).



Task 1: Do the following on Server 1, Server 2, and Local Machine. In editing the file using nano command, press control + O to write out (save the file). Press enter when asked for the name of the file. Press control + X to end.

1. Change the hostname using the command *sudo nano /etc/hostname*
   - 1.1 Use server1 for Server 1
   - 1.2 Use server2 for Server 2
   - 1.3 Use workstation for the Local Machine
2. Edit the hosts using the command *sudo nano /etc/hosts.* Edit the second line.
   - 2.1 Type 127.0.0.1 server 1 for Server 1
   - 2.2 Type 127.0.0.1 server 2 for Server 2
   - 2.3 Type 127.0.0.1 workstation for the Local Machine

1.1

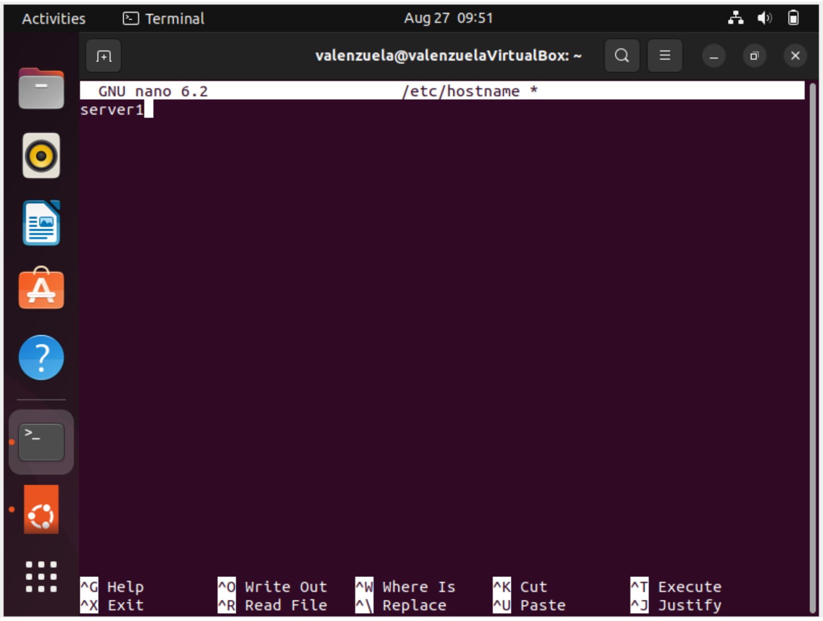


Ubuntu_Main_server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Aug 26 10:26
valenzuela@valenzuelaVirtualBox: ~
Right Ctrl
ENG US
10:26 am 26/08/2022

```
  GNU nano 6.2                     /etc/hostname *
workstation

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```

-For workstation

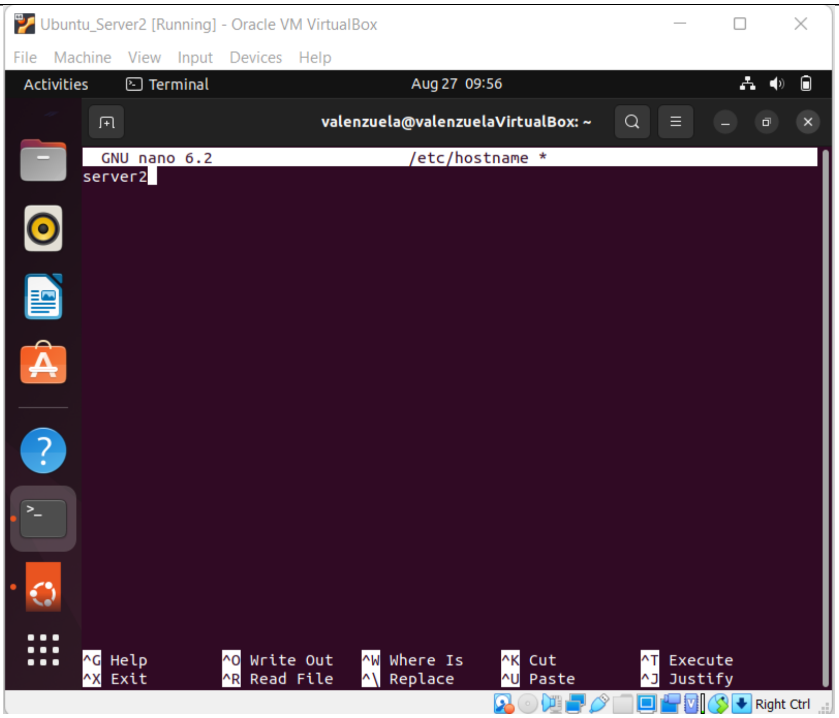
1.2



```
  GNU nano 6.2                     /etc/hostname *
server1

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```

-For server1

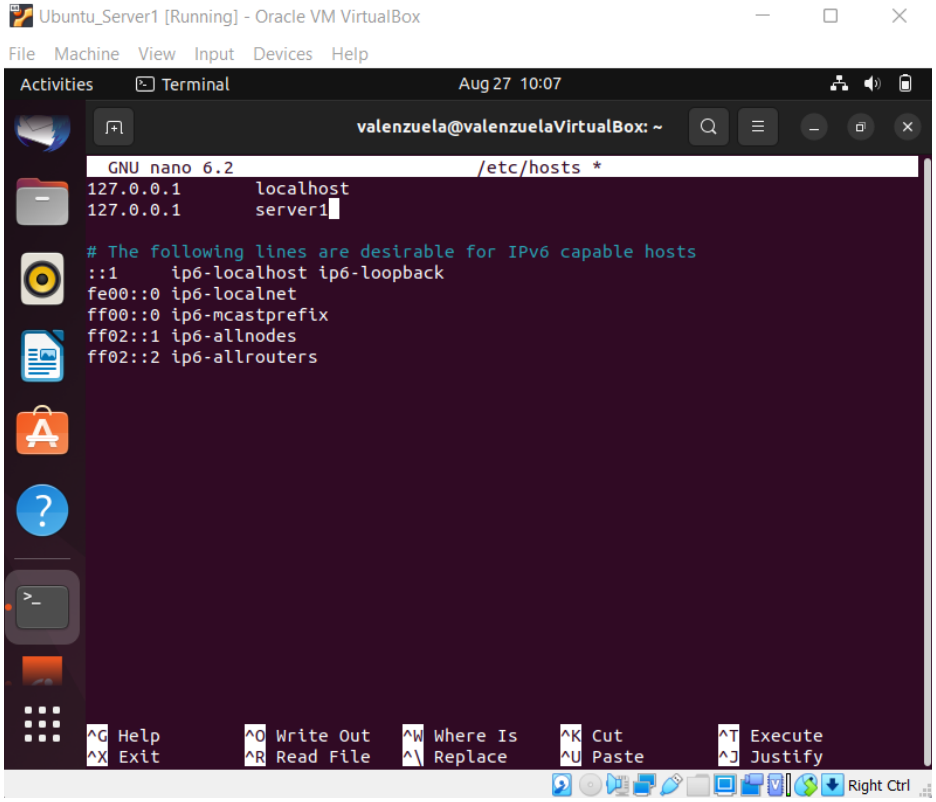
1.3



Ubuntu_Server2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 27 09:56
valenzuela@valenzuelaVirtualBox: ~
Right Ctrl

```
  GNU nano 6.2                     /etc/hostname *
server2

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify
```

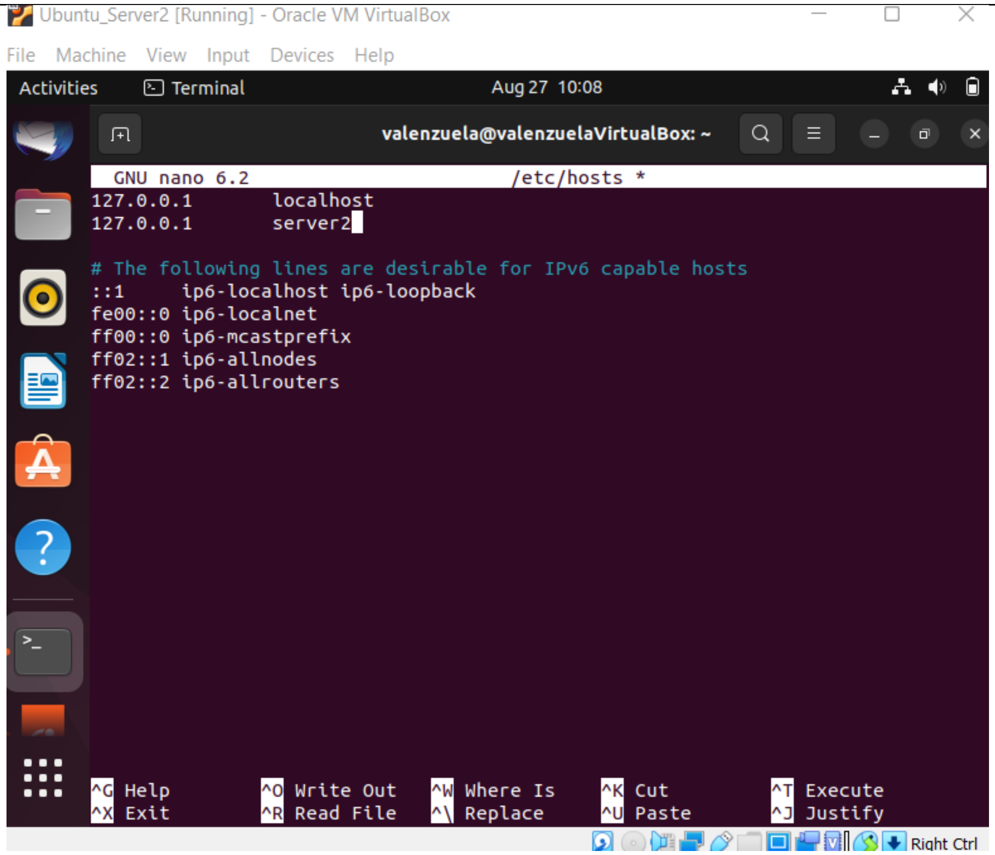
-For server2



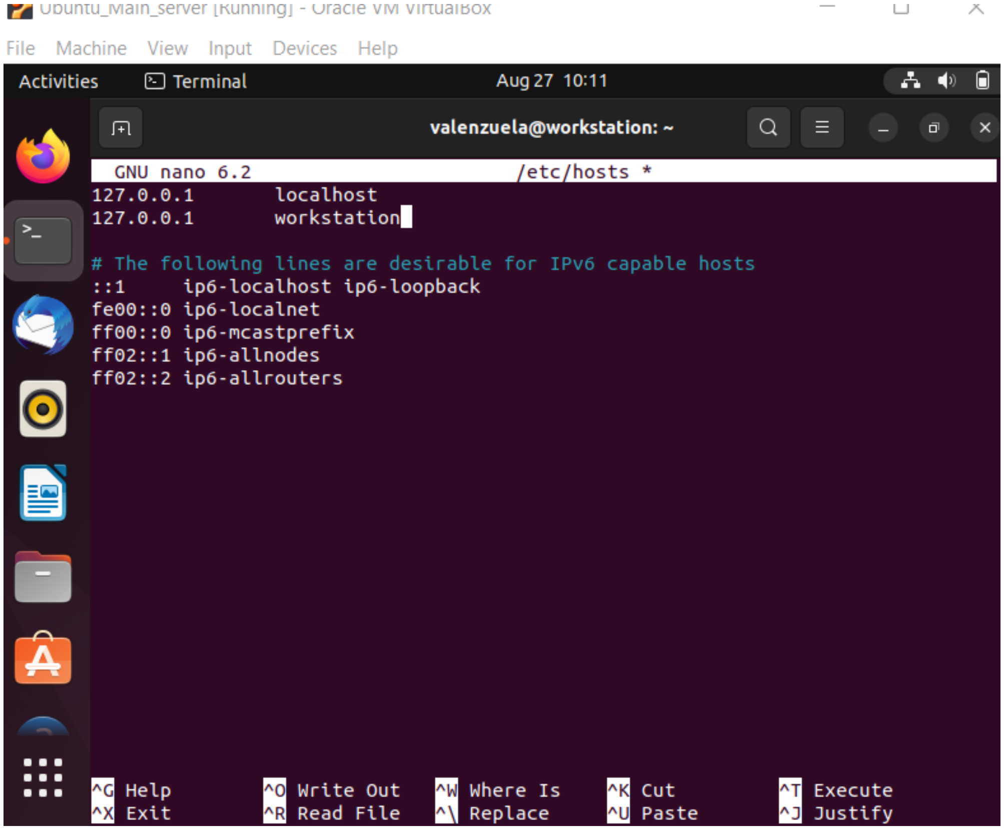
Ubuntu_Server1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Aug 27 10:07
valenzuela@valenzuelaVirtualBox: ~
Right Ctrl

```
  GNU nano 6.2                      /etc/hosts *
127.0.0.1       localhost
127.0.0.1       server1

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify
```

2.1.

2.2. 
Ubuntu_Server2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Aug 27 10:08
valenzuela@valenzuelaVirtualBox: ~
Right Ctrl

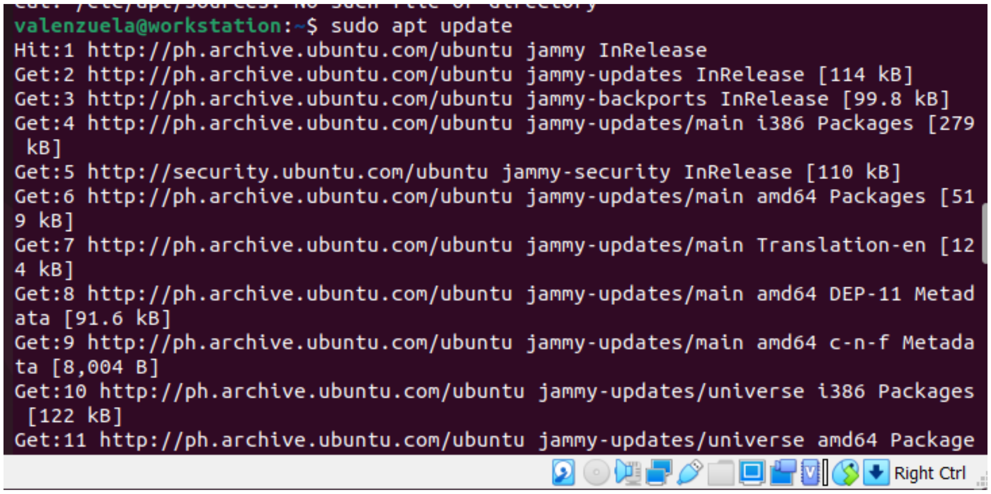
```
  GNU nano 6.2                          /etc/hosts *
127.0.0.1       localhost
127.0.0.1       server2

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters










^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify
```

2.3. 
Ubuntu_Main_server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Aug 27 10:11
valenzuela@workstation: ~

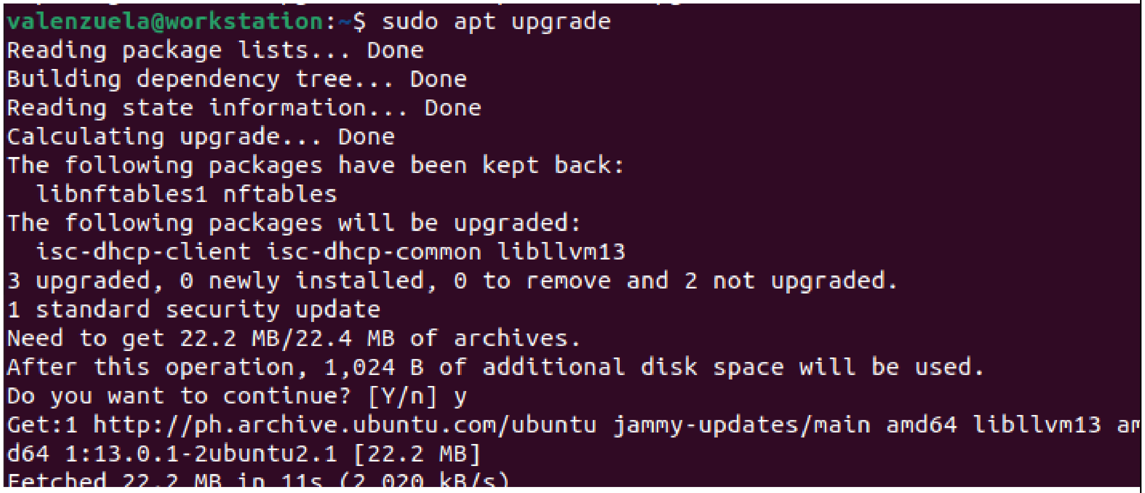
```
  GNU nano 6.2                          /etc/hosts *
127.0.0.1       localhost
127.0.0.1       workstation

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters










^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify
```

Task 2: Configure SSH on Server 1, Server 2, and Local Machine. Do the following:

1. Upgrade the packages by issuing the command *sudo apt update* and *sudo apt upgrade* respectively.

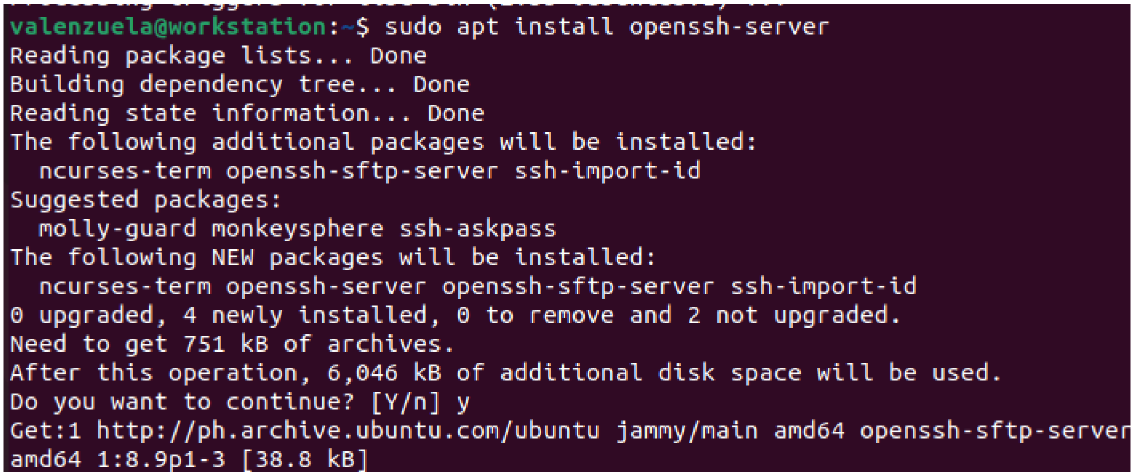


```
valenzuela@workstation:~$ sudo apt update
Hit:1 http://ph.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://ph.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Get:3 http://ph.archive.ubuntu.com/ubuntu jammy-backports InRelease [99.8 kB]
Get:4 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [279
 kB]
Get:5 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:6 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [51
9 kB]
Get:7 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [12
4 kB]
Get:8 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metad
ata [91.6 kB]
Get:9 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metada
ta [8,004 B]
Get:10 http://ph.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages
 [122 kB]
Get:11 http://ph.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Package
```



```
valenzuela@workstation:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
  libnftables1 nftables
The following packages will be upgraded:
  isc-dhcp-client isc-dhcp-common libllvm13
3 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
1 standard security update
Need to get 22.2 MB/22.4 MB of archives.
After this operation, 1,024 B of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libllvm13 am
d64 1:13.0.1-2ubuntu2.1 [22.2 MB]
Fetched 22.2 MB in 11s (2,020 kB/s)
```

2. Install the SSH server using the command *sudo apt install openssh-server*.

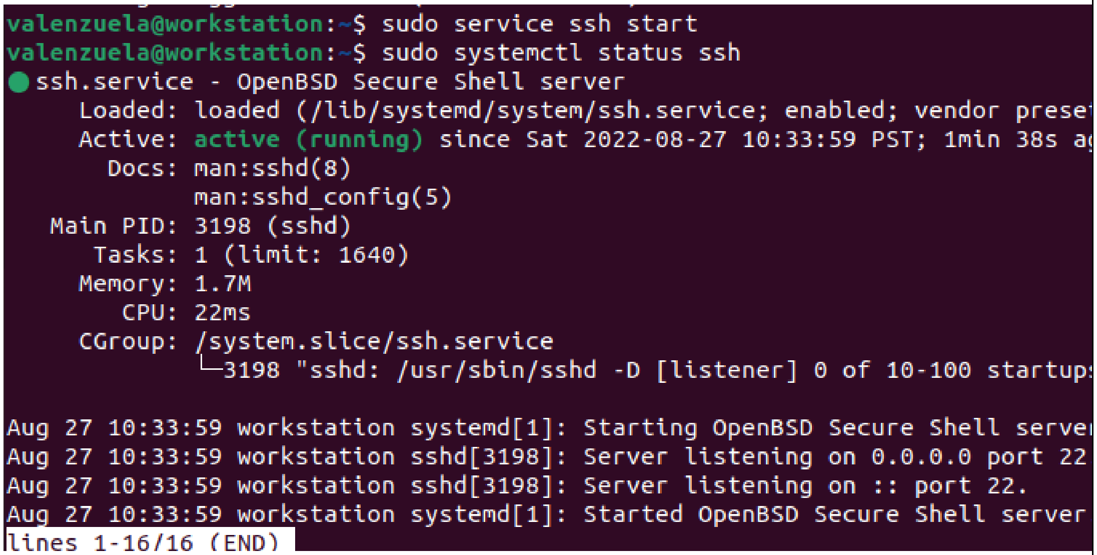


```
valenzuela@workstation:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere 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 2 not upgraded.
Need to get 751 kB of archives.
After this operation, 6,046 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ph.archive.ubuntu.com/ubuntu jammy/main amd64 openssh-sftp-server
amd64 1:8.9p1-3 [38.8 kB]
```

3. Verify if the SSH service has started by issuing the following commands:

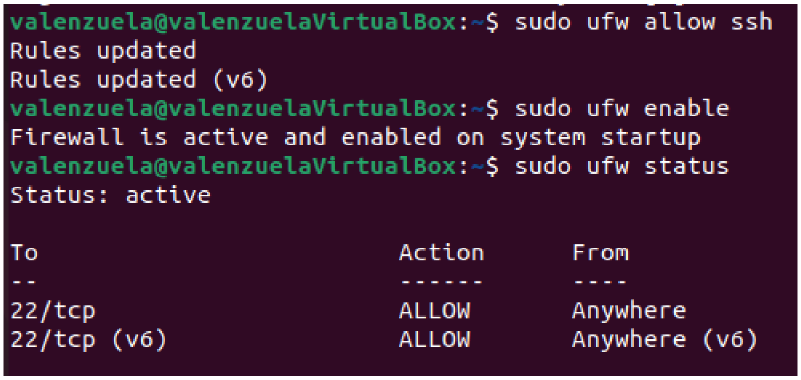
   3.1 *sudo service ssh start*

3.2 *sudo systemctl status ssh*



```
valenzuela@workstation:~$ sudo service ssh start
valenzuela@workstation:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor prese
     Active: active (running) since Sat 2022-08-27 10:33:59 PST; 1min 38s ag
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 3198 (sshd)
      Tasks: 1 (limit: 1640)
     Memory: 1.7M
        CPU: 22ms
     CGroup: /system.slice/ssh.service
             └─3198 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Aug 27 10:33:59 workstation systemd[1]: Starting OpenBSD Secure Shell server
Aug 27 10:33:59 workstation sshd[3198]: Server listening on 0.0.0.0 port 22
Aug 27 10:33:59 workstation sshd[3198]: Server listening on :: port 22.
Aug 27 10:33:59 workstation systemd[1]: Started OpenBSD Secure Shell server
lines 1-16/16 (END)
```

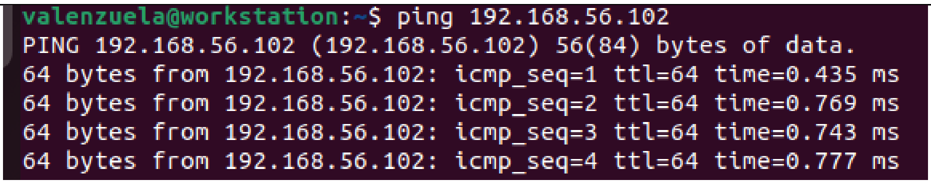
4. Configure the firewall to all port 22 by issuing the following commands:
   4.1 *sudo ufw allow ssh*
   4.2 *sudo ufw enable*
   4.3 *sudo ufw status*



```
valenzuela@valenzuelaVirtualBox:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
valenzuela@valenzuelaVirtualBox:~$ sudo ufw enable
Firewall is active and enabled on system startup
valenzuela@valenzuelaVirtualBox:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
```

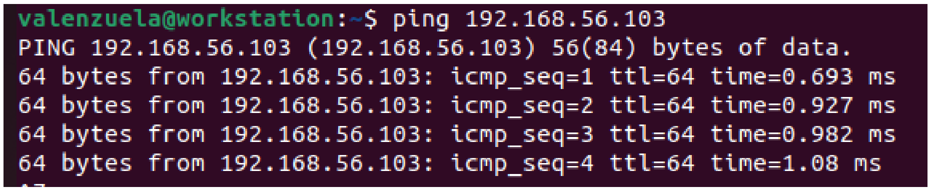
Task 3: Verify network settings on Server 1, Server 2, and Local Machine. On each device, do the following:

1. Record the ip address of Server 1, Server 2, and Local Machine. Issue the command *ifconfig* and check network settings. Note that the ip addresses of all the machines are in this network 192.168.56.XX.
   1.1 Server 1 IP address: 192.168.56.102
   1.2 Server 2 IP address: 192.168.56.103
   1.3 Server 3 IP address: 192.168.56.104
2. Make sure that they can ping each other.
   2.1 Connectivity test for Local Machine 1 to Server 1: ☒ Successful ☐ Not Successful



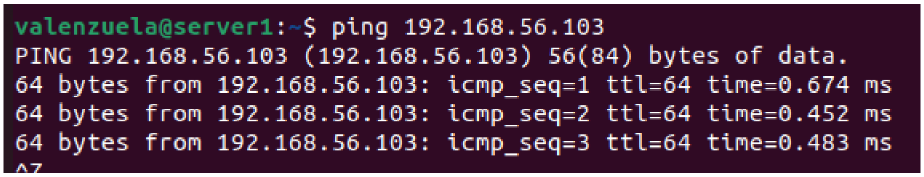
```
valenzuela@workstation:~$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.435 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.769 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.743 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.777 ms
```

2.2 Connectivity test for Local Machine 1 to Server 2: ☒ Successful ☐ Not Successful



```
valenzuela@workstation:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.693 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.927 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.982 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=1.08 ms
^Z
```

2.3 Connectivity test for Server 1 to Server 2: ☒ Successful ☐ Not Successful



```
valenzuela@server1:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.674 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.452 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.483 ms
^Z
```

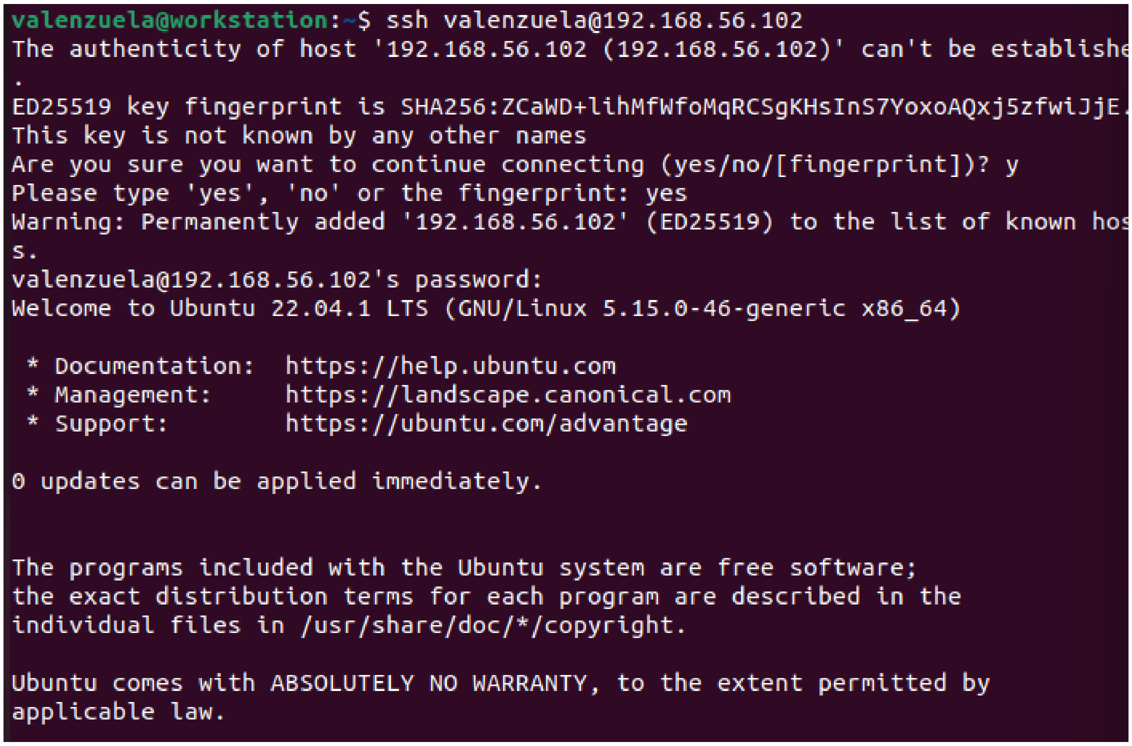
Task 4: Verify SSH connectivity on Server 1, Server 2, and Local Machine.

1. On the Local Machine, issue the following commands:

1.1 ssh username@ip_address_server1 for example, *ssh jvtaylar@192.168.56.120*

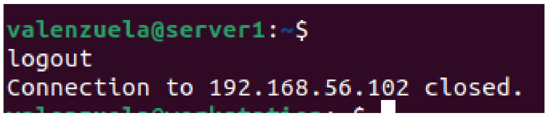
1.2 Enter the password for server 1 when prompted

1.3 Verify that you are in server 1. The user should be in this format user@server1. For example, *jvtaylar@server1*



```
valenzuela@workstation:~$ ssh valenzuela@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be establishe
.
ED25519 key fingerprint is SHA256:ZCaWD+lihMfWfoMqRCSgKHsInS7YoxoAQxj5zfwiJjE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.56.102' (ED25519) to the list of known hos
s.
valenzuela@192.168.56.102's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-46-generic x86_64)

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

0 updates can be applied immediately.


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.
```

2. Logout of Server 1 by issuing the command *control + D.*

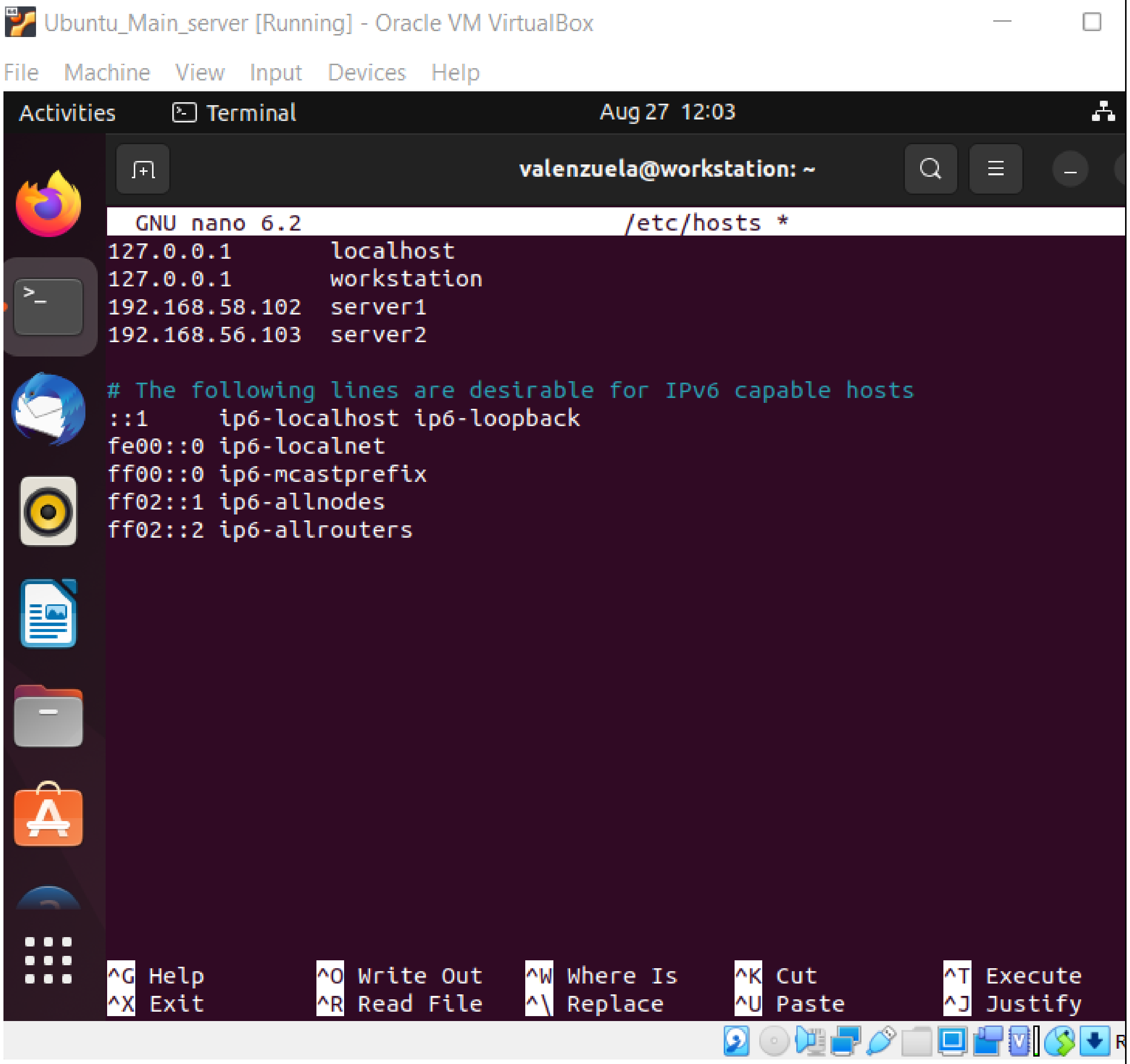


```
valenzuela@server1:~$
logout
Connection to 192.168.56.102 closed.
```

3. Do the same for Server 2.
4. Edit the hosts of the Local Machine by issuing the command *sudo nano /etc/hosts.* Below all texts type the following:

4.1 IP_address server 1 (provide the ip address of server 1 followed by the hostname)

4.2 IP_address server 2 (provide the ip address of server 2 followed by the hostname)

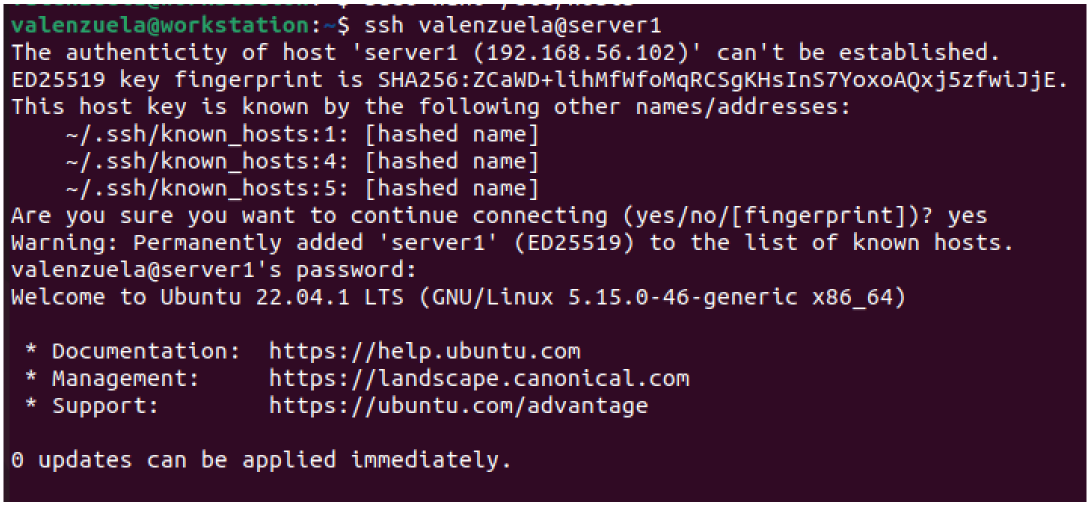

Ubuntu_Main_server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Aug 27 12:03
valenzuela@workstation: ~

```
  GNU nano 6.2                    /etc/hosts *
127.0.0.1       localhost
127.0.0.1       workstation
192.168.58.102  server1
192.168.56.103  server2

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```

4.3 Save the file and exit.

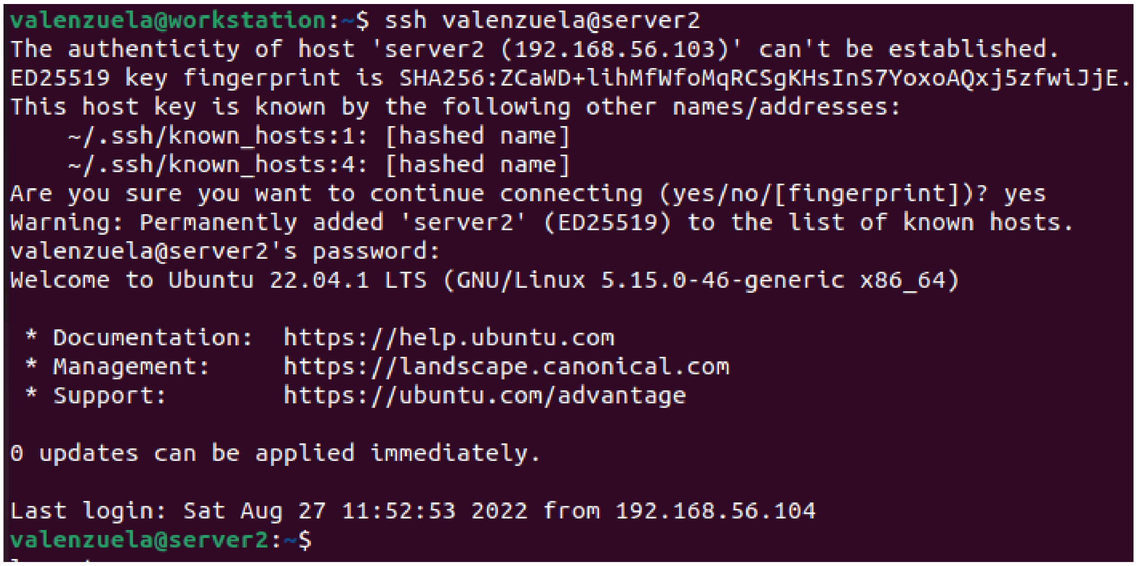
5. On the local machine, verify that you can do the SSH command but this time, use the hostname instead of typing the IP address of the servers. For example,

try to do *ssh jvtaylar@server1*. Enter the password when prompted. Verify that you have entered Server 1. Do the same for Server 2.



```
valenzuela@workstation:~$ ssh valenzuela@server1
The authenticity of host 'server1 (192.168.56.102)' can't be established.
ED25519 key fingerprint is SHA256:ZCaWD+lihMfWfoMqRCSgKHsInS7YoxoAQxj5zfwiJjE.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server1' (ED25519) to the list of known hosts.
valenzuela@server1's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-46-generic x86_64)

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

0 updates can be applied immediately.
```

Server1



```
valenzuela@workstation:~$ ssh valenzuela@server2
The authenticity of host 'server2 (192.168.56.103)' can't be established.
ED25519 key fingerprint is SHA256:ZCaWD+lihMfWfoMqRCSgKHsInS7YoxoAQxj5zfwiJjE.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server2' (ED25519) to the list of known hosts.
valenzuela@server2's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-46-generic x86_64)

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

0 updates can be applied immediately.

Last login: Sat Aug 27 11:52:53 2022 from 192.168.56.104
valenzuela@server2:~$
```

Server2

Reflections:

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?

   -It is because we are able to add the ip and the hostname of both server1 and server2 in the sudo nano /etc/hosts and the workstation is able to read it as the same as the ip address.

2. How secured is SSH?

   -It is secure because it encrypts it during the connection in an unsecure network.

I affirm that I shall not give or receive any unauthorized help on this exam and that all work shall be my own. – Robin Valenzuela