Name: John Renzo L. Mendoza	**Date Performed:** August 22, 2023
Course/Section: CPE31S5	**Date Submitted:** August 23, 2023
Instructor: Engr. Roman Richard	**Semester and SY:** First Semester, 2023- 2024

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*.

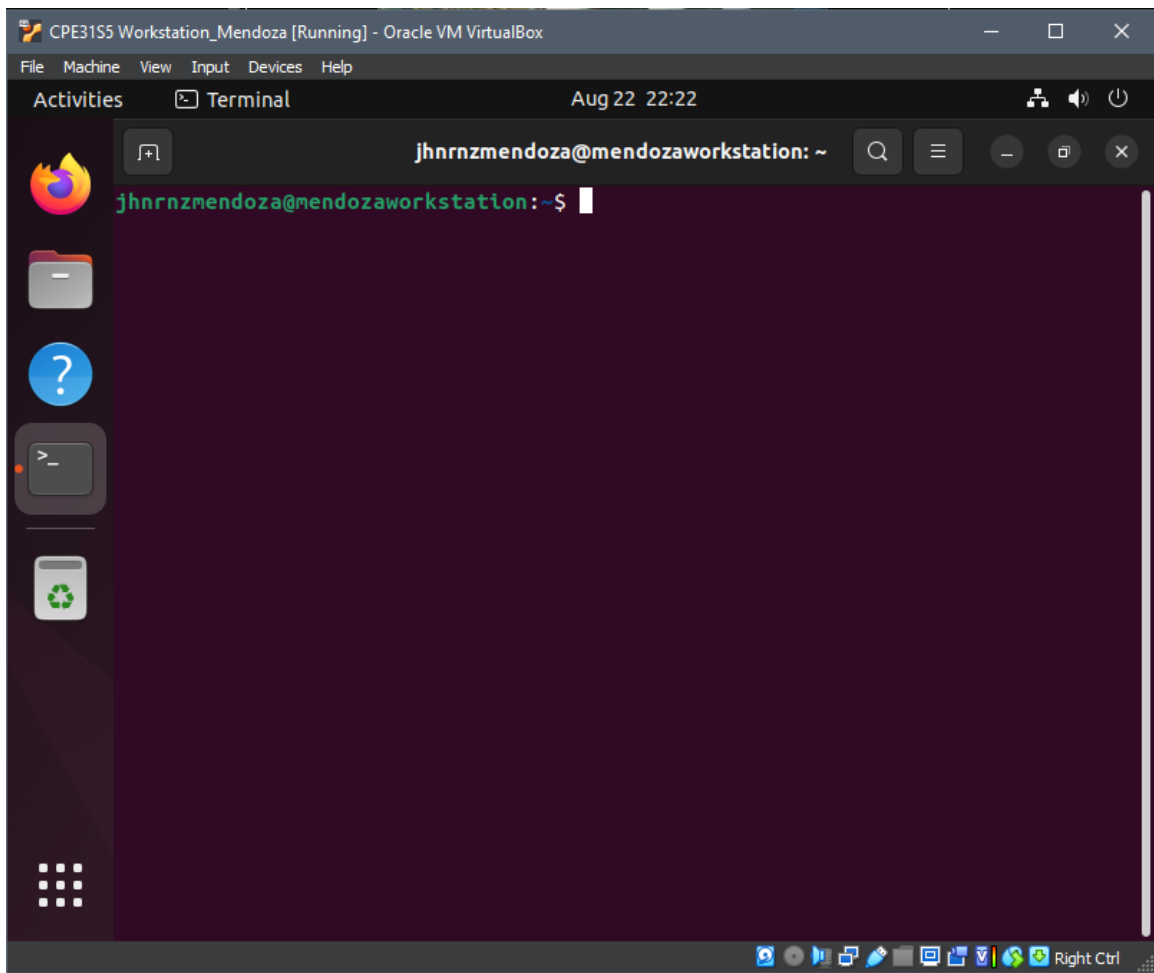(Note: *it is assumed that you have prior knowledge of cloning and creating snapshots in a virtual machine*).

Image 1.1.1. Screenshot of the Installation
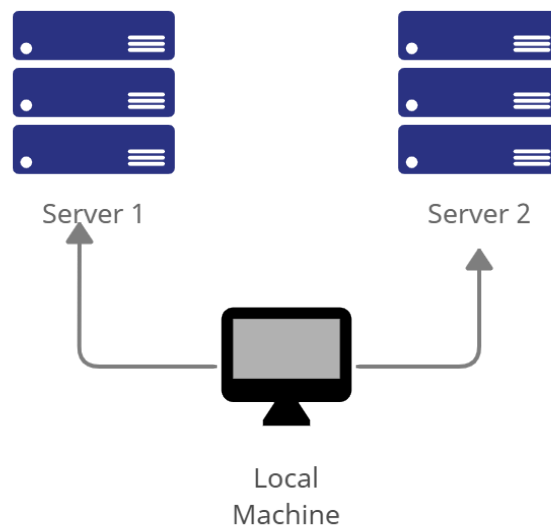
Image 1.1.2. Screenshot of the Installed of the Workstation

Image 1.1.3. Screenshot of the Installed of the Server 1

Image 1.1.4. Screenshot of the Installed of the Server 2
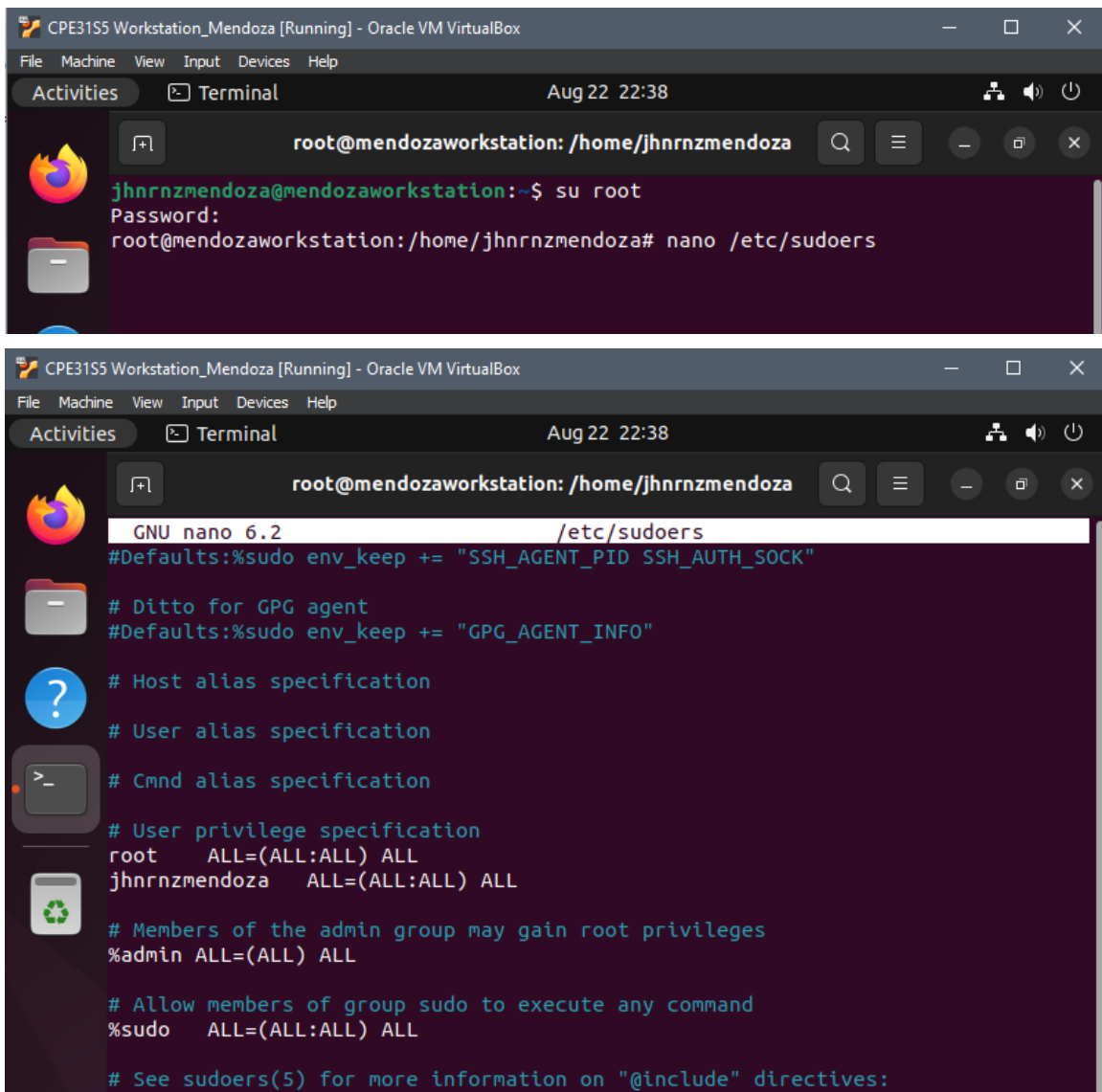
Image 1.1.5. Adding user as a sudoer (sudoer file)

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

```
jhnrnzmendoza@mendozaserver2:~$ sudo nano /etc/hostname
```

CPE31S5 Server 2_Mendoza [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
Ubuntu 22.04.1 LTS server2 tty1

server2 login: jhnrnzmendoza
Password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-79-generic x86_64)

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

  System information as of Tue Aug 22 03:19:02 PM UTC 2023

  System load:  0.1474609375      Processes:               119
  Usage of /:   44.2% of 11.21GB  Users logged in:         0
  Memory usage: 5%                IPv4 address for enp0s3: 10.0.2.15
  Swap usage:   0%


91 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


Last login: Tue Aug 22 15:14:53 UTC 2023 on tty1
jhnrnzmendoza@server2:~$
```
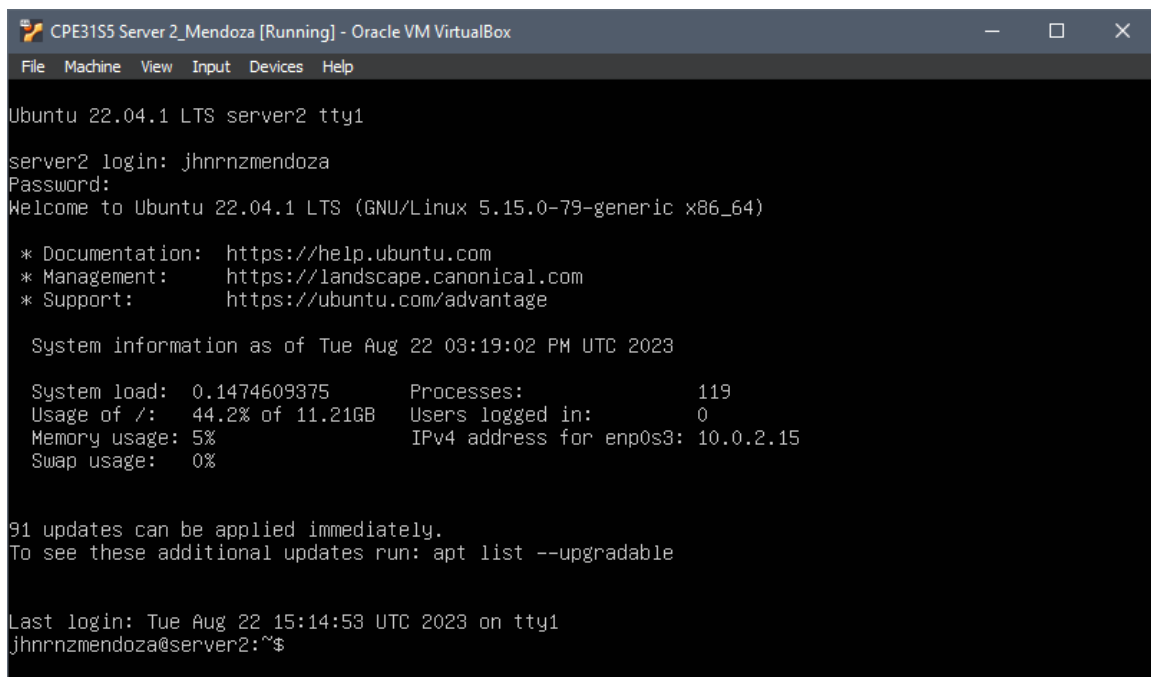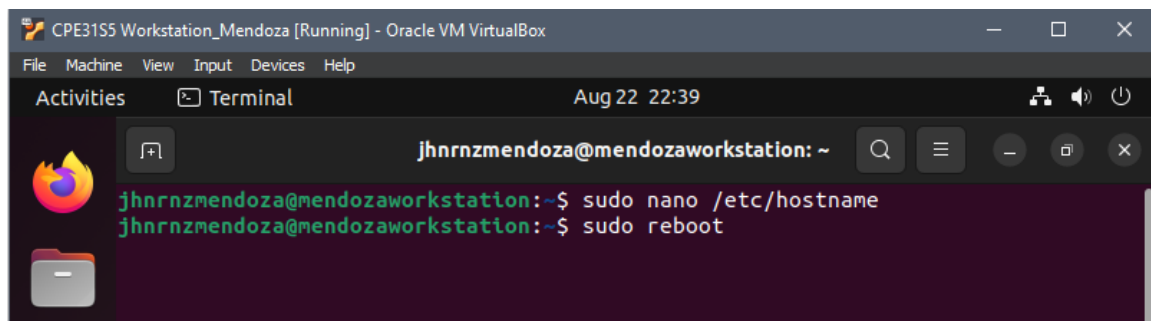
1.3 Use workstation for the Local Machine

CPE31S5 Workstation_Mendoza [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities   Terminal   Aug 22 22:39
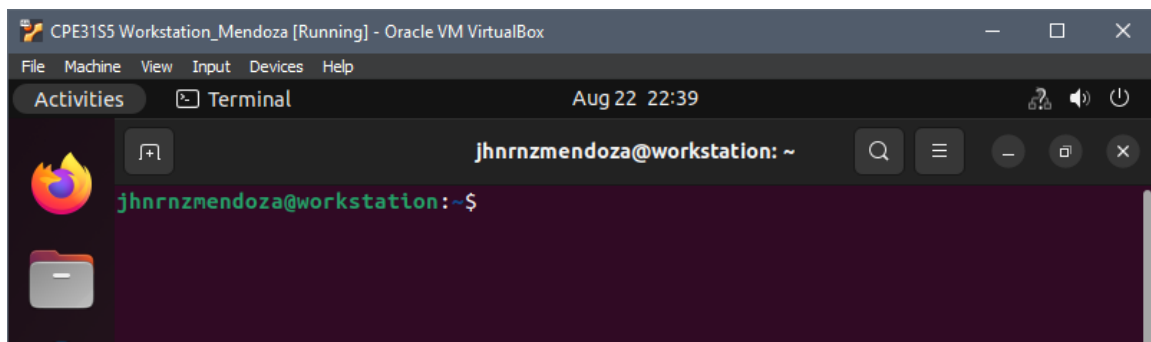
jhnrnzmendoza@mendozaworkstation: ~

```
jhnrnzmendoza@mendozaworkstation:~$ sudo nano /etc/hostname
jhnrnzmendoza@mendozaworkstation:~$ sudo reboot
```

After Reboot:

CPE31S5 Workstation_Mendoza [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities   Terminal   Aug 22 22:39

jhnrnzmendoza@workstation: ~
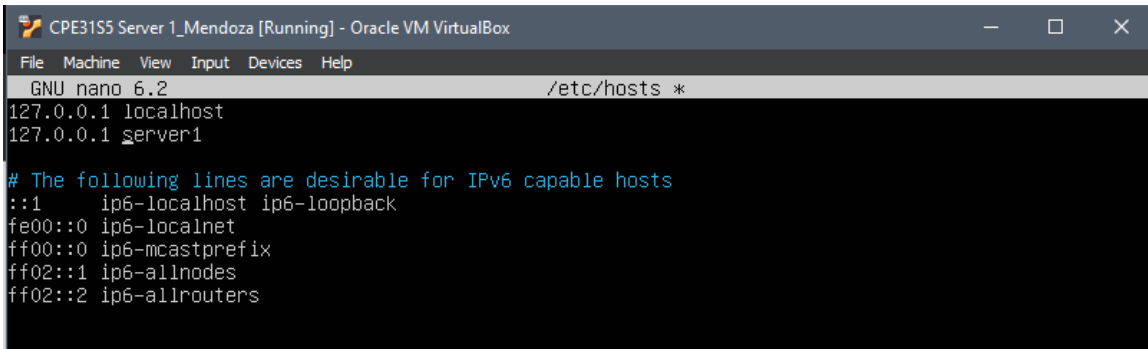
```
jhnrnzmendoza@workstation:~$
```

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

```
jhnrnzmendoza@server1:~$ sudo nano /etc/hosts_
```

```
CPE31S5 Server 1_Mendoza [Running] - Oracle VM VirtualBox       —   □   ×
File  Machine  View  Input  Devices  Help
  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
```

    2.2 Type 127.0.0.1 server 2 for Server 2

```
jhnrnzmendoza@server2:~$ sudo nano /etc/hosts
```

```
CPE31S5 Server 2_Mendoza [Running] - Oracle VM VirtualBox       —   □   ×
File  Machine  View  Input  Devices  Help
  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
```

    2.3 Type 127.0.0.1 workstation for the Local Machine
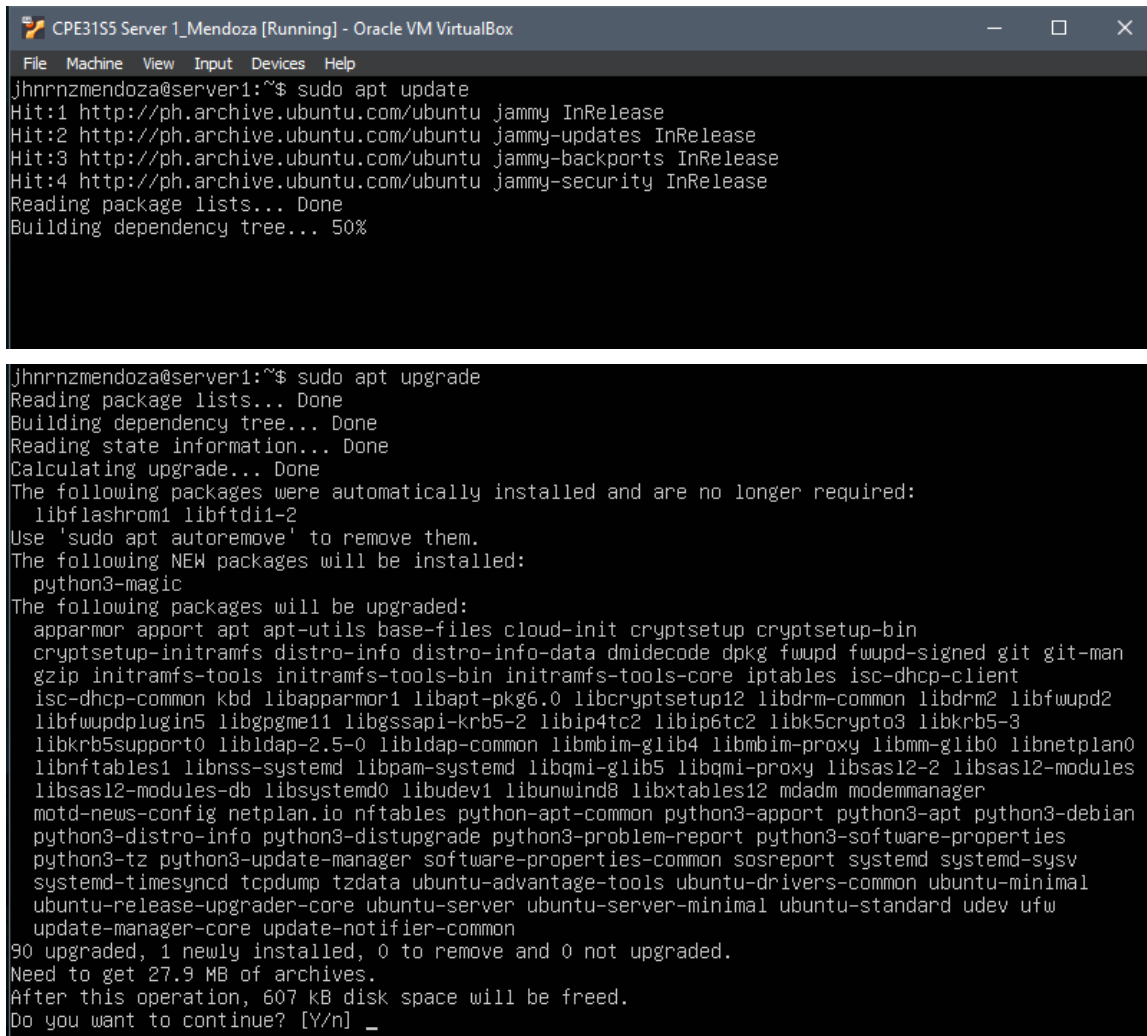
```
CPE31S5 Workstation_Mendoza [Running] - Oracle VM VirtualBox       —   □   ×
File  Machine  View  Input  Devices  Help
Activities      Terminal              Aug 22 22:40
                        jhnrnzmendoza@workstation: ~
  GNU nano 6.2                          /etc/hosts *
127.0.0.1        localhost
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
```

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.

Server 1


```
CPE31S5 Server 1_Mendoza [Running] - Oracle VM VirtualBox

File  Machine  View  Input  Devices  Help
jhnrnzmendoza@server1:~$ sudo apt update
Hit:1 http://ph.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://ph.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://ph.archive.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... 50%
```

```
jhnrnzmendoza@server1:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  python3-magic
The following packages will be upgraded:
  apparmor apport apt apt-utils base-files cloud-init cryptsetup cryptsetup-bin
  cryptsetup-initramfs distro-info distro-info-data dmidecode dpkg fwupd fwupd-signed git git-man
  gzip initramfs-tools initramfs-tools-bin initramfs-tools-core iptables isc-dhcp-client
  isc-dhcp-common kbd libapparmor1 libapt-pkg6.0 libcryptsetup12 libdrm-common libdrm2 libfwupd2
  libfwupdplugin5 libgpgme11 libgssapi-krb5-2 libip4tc2 libip6tc2 libk5crypto3 libkrb5-3
  libkrb5support0 libldap-2.5-0 libldap-common libmbim-glib4 libmbim-proxy libmm-glib0 libnetplan0
  libnftables1 libnss-systemd libpam-systemd libqmi-glib5 libqmi-proxy libsas12-2 libsas12-modules
  libsas12-modules-db libsystemd0 libudev1 libunwind8 libxtables12 mdadm modemmanager
  motd-news-config netplan.io nftables python-apt-common python3-apport python3-apt python3-debian
  python3-distro-info python3-distupgrade python3-problem-report python3-software-properties
  python3-tz python3-update-manager software-properties-common sosreport systemd systemd-sysv
  systemd-timesyncd tcpdump tzdata ubuntu-advantage-tools ubuntu-drivers-common ubuntu-minimal
  ubuntu-release-upgrader-core ubuntu-server ubuntu-server-minimal ubuntu-standard udev ufw
  update-manager-core update-notifier-common
90 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 27.9 MB of archives.
After this operation, 607 kB disk space will be freed.
Do you want to continue? [Y/n] _
```
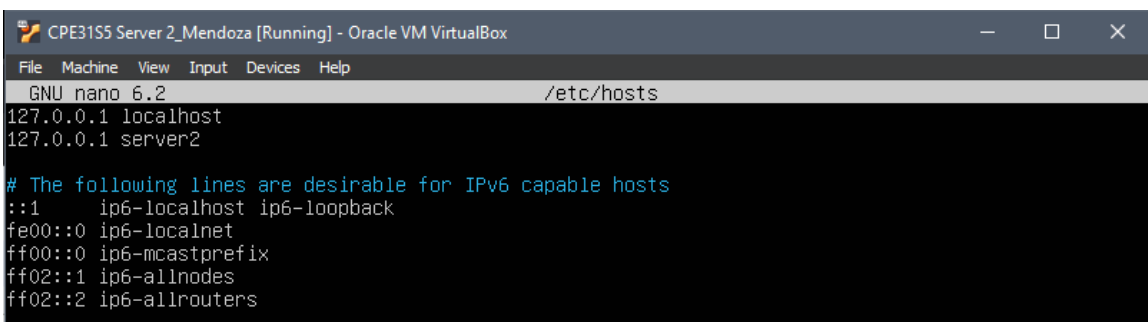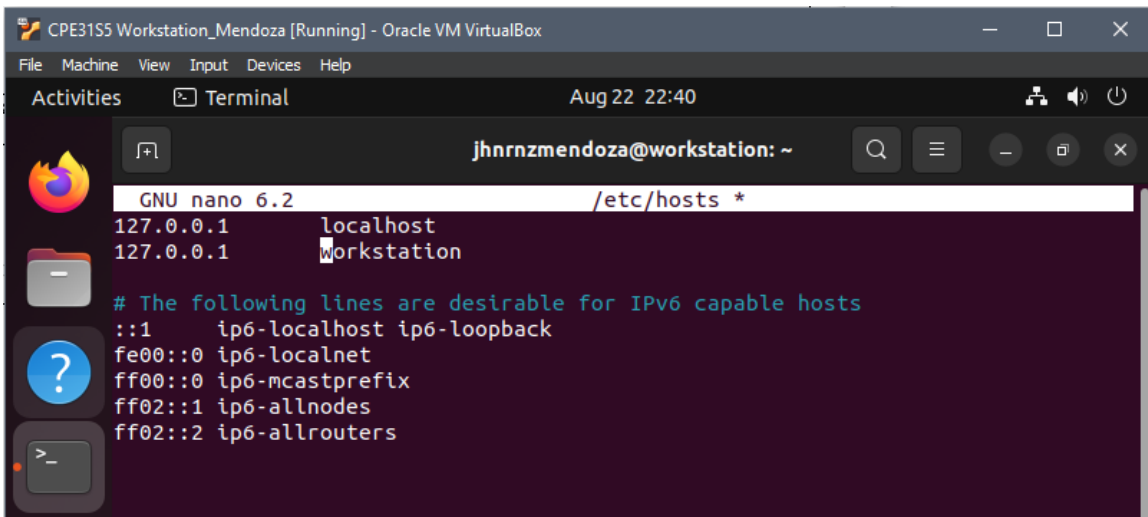
Server 2

File   Machine   View   Input   Devices   Help

```
jhnrnzmendoza@server2:~$ sudo apt update
Hit:1 http://ph.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://ph.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://ph.archive.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... 71%
```
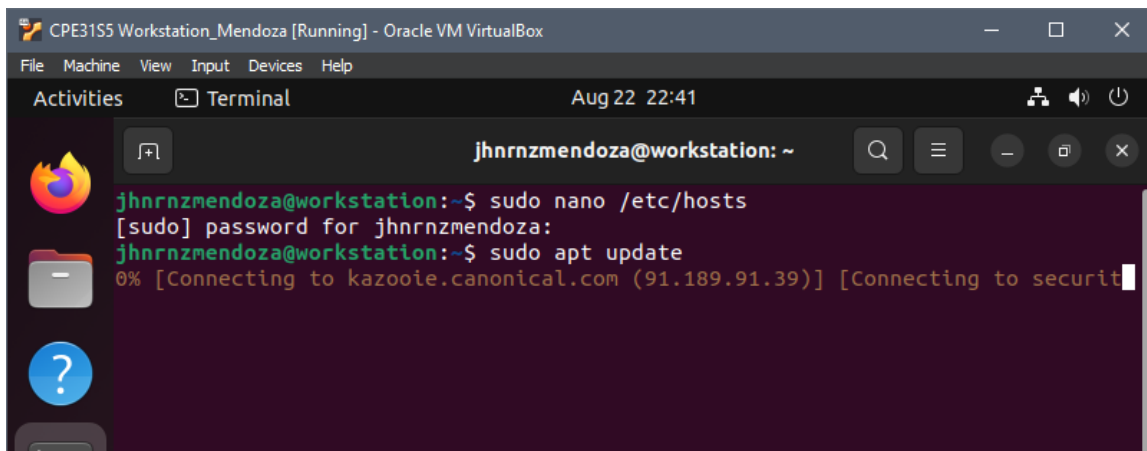
```
jhnrnzmendoza@server2:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  python3-magic
The following packages will be upgraded:
  apparmor apport apt apt-utils base-files cloud-init cryptsetup cryptsetup-bin
  cryptsetup-initramfs distro-info distro-info-data dmidecode dpkg fwupd fwupd-signed git git-man
  gzip initramfs-tools initramfs-tools-bin initramfs-tools-core iptables isc-dhcp-client
  isc-dhcp-common kbd libapparmor1 libapt-pkg6.0 libcryptsetup12 libdrm-common libdrm2 libfwupd2
  libfwupdplugin5 libgpgme11 libgssapi-krb5-2 libip4tc2 libip6tc2 libk5crypto3 libkrb5-3
  libkrb5support0 libldap-2.5-0 libldap-common libmbim-glib4 libmbim-proxy libmm-glib0 libnetplan0
  libnftables1 libnss-systemd libpam-systemd libqmi-glib5 libqmi-proxy libsasl2-2 libsasl2-modules
  libsasl2-modules-db libsystemd0 libudev1 libunwind8 libxtables12 mdadm modemmanager
  motd-news-config netplan.io nftables python-apt-common python3-apport python3-apt python3-debian
  python3-distro-info python3-distupgrade python3-problem-report python3-software-properties
  python3-tz python3-update-manager software-properties-common sosreport systemd systemd-sysv
  systemd-timesyncd tcpdump tzdata ubuntu-advantage-tools ubuntu-drivers-common ubuntu-minimal
  ubuntu-release-upgrader-core ubuntu-server ubuntu-server-minimal ubuntu-standard udev ufw
  update-manager-core update-notifier-common
90 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 27.9 MB of archives.
After this operation, 607 kB disk space will be freed.
Do you want to continue? [Y/n]
```

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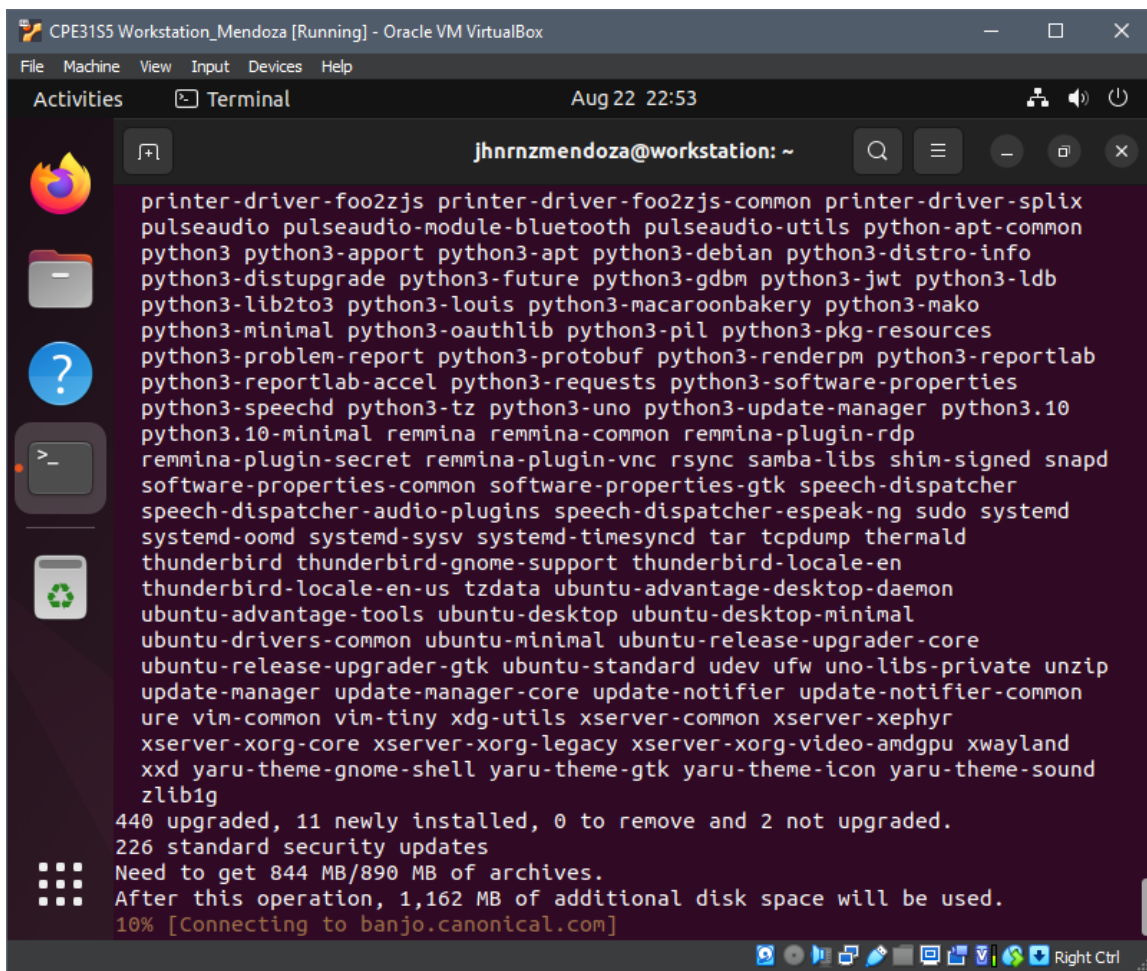
2. Install the SSH server using the command *sudo apt install openssh-server*.

Server 1

Server 2

Local Machine

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*

Server 1

```
jhnrrnzmendoza@server1:~$ sudo service ssh start
jhnrrnzmendoza@server1:~$ sudo systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2023-08-22 15:27:49 UTC; 3min 28s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 16170 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 16174 (sshd)
      Tasks: 1 (limit: 4557)
     Memory: 1.7M
        CPU: 20ms
     CGroup: /system.slice/ssh.service
             └─16174 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 22 15:27:48 server1 systemd[1]: ssh.service: Deactivated successfully.
Aug 22 15:27:48 server1 systemd[1]: Stopped OpenBSD Secure Shell server.
Aug 22 15:27:48 server1 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 22 15:27:49 server1 sshd[16174]: Server listening on 0.0.0.0 port 22.
Aug 22 15:27:49 server1 systemd[1]: Started OpenBSD Secure Shell server.
Aug 22 15:27:49 server1 sshd[16174]: Server listening on :: port 22.
```

Server 2

```
jhnrrnzmendoza@server2:~$ sudo service ssh start
jhnrrnzmendoza@server2:~$ sudo systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2023-08-22 15:28:06 UTC; 2min 14s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 16168 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 16172 (sshd)
      Tasks: 1 (limit: 4557)
     Memory: 1.7M
        CPU: 19ms
     CGroup: /system.slice/ssh.service
             └─16172 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 22 15:28:06 server2 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 22 15:28:06 server2 sshd[16172]: Server listening on 0.0.0.0 port 22.
Aug 22 15:28:06 server2 sshd[16172]: Server listening on :: port 22.
Aug 22 15:28:06 server2 systemd[1]: Started OpenBSD Secure Shell server.
```

Local Machine

```
jhnrnzmendoza@workstation:~$ sudo service ssh start
jhnrnzmendoza@workstation:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: >
     Active: active (running) since Tue 2023-08-22 23:32:48 +08; 30s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 41649 (sshd)
      Tasks: 1 (limit: 4629)
     Memory: 1.7M
        CPU: 18ms
     CGroup: /system.slice/ssh.service
             └─41649 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 22 23:32:48 workstation systemd[1]: Starting OpenBSD Secure Shell server...
Aug 22 23:32:48 workstation sshd[41649]: Server listening on 0.0.0.0 port 22.
Aug 22 23:32:48 workstation sshd[41649]: Server listening on :: port 22.
Aug 22 23:32:48 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*

Server 1

```
CPE31S5 Server 1_Mendoza [Running] - Oracle VM VirtualBox          —   □   ×

File  Machine  View  Input  Devices  Help
jhnrnzmendoza@server1:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
jhnrnzmendoza@server1:~$ sudo ufw enable
Firewall is active and enabled on system startup
jhnrnzmendoza@server1:~$ sudo ufw status
Status: active

To                      Action      From
--                      ------      ----
22/tcp                  ALLOW       Anywhere
22/tcp (v6)             ALLOW       Anywhere (v6)
```
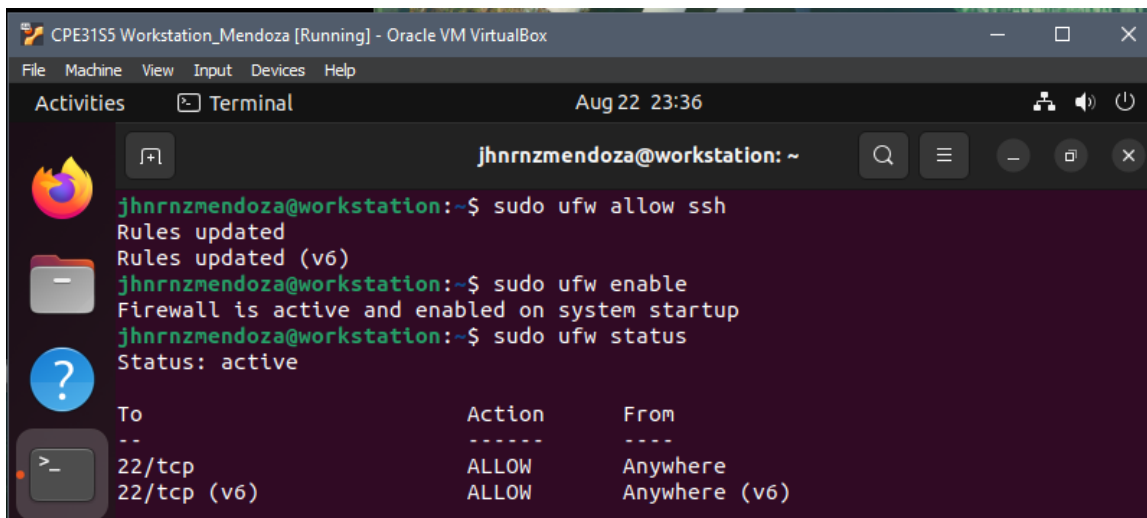
Server 2

```
CPE31S5 Server 2_Mendoza [Running] - Oracle VM VirtualBox          —   □   ×

File  Machine  View  Input  Devices  Help
jhnrnzmendoza@server2:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
jhnrnzmendoza@server2:~$ sudo ufw enable
Firewall is active and enabled on system startup
jhnrnzmendoza@server2:~$ sudo ufw status
Status: active

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

Local Machine
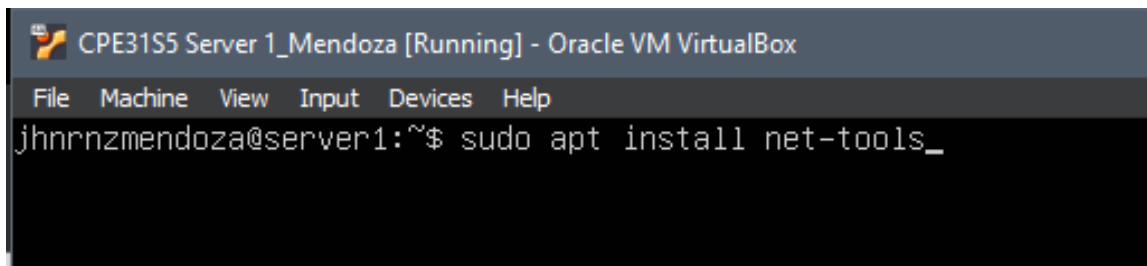
Task 3: Verify network settings on Server 1, Server 2, and Local Machine. On each device, do the following:
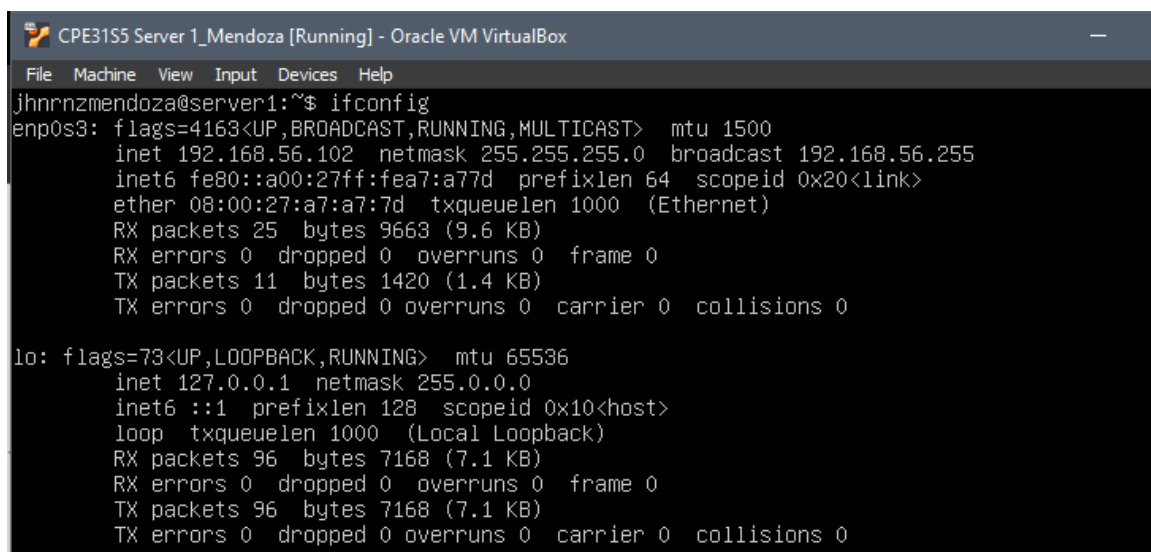
1. Record the ip address of Server 1, Server 2, and Local Machine. Issue the command *ifconfig* and check network settings. Note that the ip addresses of all the machines are in this network 192.168.56.XX.

   In order to use the ifconfig command, the following query is installed on each device for it to be used.

   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

```
jhnrnzmendoza@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=0.530 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.513 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.399 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.420 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.393 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=0.350 ms
64 bytes from 192.168.56.102: icmp_seq=7 ttl=64 time=0.534 ms
64 bytes from 192.168.56.102: icmp_seq=8 ttl=64 time=0.321 ms
64 bytes from 192.168.56.102: icmp_seq=9 ttl=64 time=0.482 ms
64 bytes from 192.168.56.102: icmp_seq=10 ttl=64 time=0.521 ms
```

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

```
⊞                          jhnrnzmendoza@workstation: ~              Q  ≡  —  ▫  ✕

jhnrnzmendoza@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=0.699 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.392 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.576 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.394 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=0.387 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=64 time=0.457 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=64 time=0.353 ms
64 bytes from 192.168.56.103: icmp_seq=8 ttl=64 time=0.289 ms
64 bytes from 192.168.56.103: icmp_seq=9 ttl=64 time=0.355 ms
64 bytes from 192.168.56.103: icmp_seq=10 ttl=64 time=0.307 ms
64 bytes from 192.168.56.103: icmp_seq=11 ttl=64 time=0.508 ms
```

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

```
jhnrnzmendoza@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=0.714 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.541 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.428 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.427 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=0.312 ms
```

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*

```
jhnrnzmendoza@workstation:~$ ssh jhnrnzmendoza@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
ED25519 key fingerprint is SHA256:K7JLZjn/KLSgnUflYhFuaSTT/L+Fndou9GdkLKhYspE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.102' (ED25519) to the list of known hosts.
jhnrnzmendoza@192.168.56.102's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-79-generic x86_64)

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

  System information as of Tue Aug 22 04:05:22 PM UTC 2023

  System load:  0.201171875        Processes:              115
  Usage of /:   44.3% of 11.21GB   Users logged in:        1
  Memory usage: 5%                 IPv4 address for enp0s3: 192.168.56.102
  Swap usage:   0%
```

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*

```
Last login: Tue Aug 22 15:59:14 2023
jhnrnzmendoza@server1:~$
```

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

```
Last login: Tue Aug 22 15:59:14 2023
jhnrnzmendoza@server1:~$
logout
Connection to 192.168.56.102 closed.
jhnrnzmendoza@workstation:~$
```

3. Do the same for Server 2.

```
jhnrnzmendoza@workstation:~$ ssh jhnrnzmendoza@192.168.56.103
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established.
ED25519 key fingerprint is SHA256:47VO8jD6iQqaqPUAy4gnwBdrKaevsNDZruD/M+Yrjwo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.103' (ED25519) to the list of known hosts.
jhnrnzmendoza@192.168.56.103's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-79-generic x86_64)

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

  System information as of Tue Aug 22 04:06:44 PM UTC 2023

  System load:   0.11181640625    Processes:                115
  Usage of /:    44.3% of 11.21GB  Users logged in:          1
  Memory usage: 6%                 IPv4 address for enp0s3: 192.168.56.103
  Swap usage:    0%
```

```
Last login: Tue Aug 22 16:01:41 2023
jhnrnzmendoza@server2:~$
logout
Connection to 192.168.56.103 closed.
jhnrnzmendoza@workstation:~$
```

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)

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.

Server 1

```
jhnrnzmendoza@workstation:~$ ssh jhnrnzmendoza@server1
The authenticity of host 'server1 (192.168.56.102)' can't be established.
ED25519 key fingerprint is SHA256:K7JLZjn/KLSgnUflYhFuaSTT/L+Fndou9GdkLKhYspE.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [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.
jhnrnzmendoza@server1's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-79-generic x86_64)

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

  System information as of Tue Aug 22 04:10:10 PM UTC 2023

  System load:  0.20361328125      Processes:             114
  Usage of /:   44.3% of 11.21GB   Users logged in:       1
  Memory usage: 6%                 IPv4 address for enp0s3: 192.168.56.102
  Swap usage:   0%
```
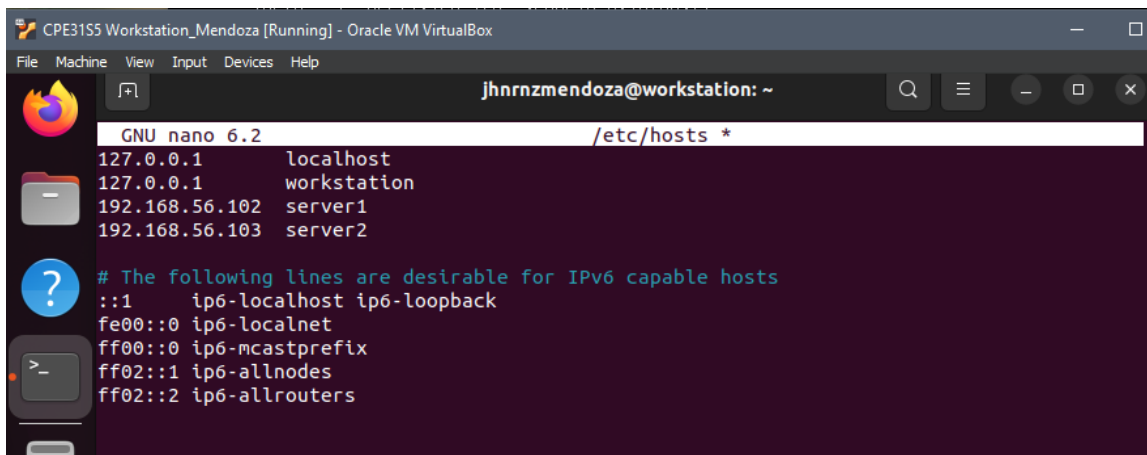
```
Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet
connection or proxy settings


Last login: Tue Aug 22 16:05:22 2023 from 192.168.56.104
jhnrnzmendoza@server1:~$
```

Server 2

```
jhnrnzmendoza@workstation:~$ ssh jhnrnzmendoza@server2
The authenticity of host 'server2 (192.168.56.103)' can't be established.
ED25519 key fingerprint is SHA256:47VO8jD6iQqaqPUAy4gnwBdrKaevsNDZruD/M+Yrjwo.
This host key is known by the following other names/addresses:
    ~/.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.
jhnrnzmendoza@server2's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-79-generic x86_64)

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

  System information as of Tue Aug 22 04:11:39 PM UTC 2023

  System load:  0.0048828125      Processes:               114
  Usage of /:   44.3% of 11.21GB   Users logged in:         1
  Memory usage: 6%                 IPv4 address for enp0s3: 192.168.56.103
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.
```

```
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet
connection or proxy settings


Last login: Tue Aug 22 16:06:44 2023 from 192.168.56.104
jhnrnzmendoza@server2:~$
```

Reflections:

Answer the following:

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

   After physically connecting the desktop to the servers by following the given network topology, we are able to have an ip address generated for each of the servers as well as the local machine (desktop). Using these ip addresses, we input it to the /etc/hostname file in which you may append an ip address with its paired hostname. Then, the user would be able to use the hostname instead of the ip address in order to remotely access the server. Furthermore, by accessing the servers using the local machine, the user is still prompted with an authentication in which it asks the password of the respective server, in this way, only privileged or authorized users can access the remote servers.

2. How secure is SSH?

   Based on this activity, we are able to remotely access the 2 servers using a local machine which is the desktop workstation. Initially, we have given the 2 servers and 1 workstation their own hostname, user, and password. After connecting them using the given network topology, we are able to access each server remotely. We may say that this is secure as the user who is trying to access the remote servers is prompted with an authentication which does not permit random or alien access to the servers. To what extent does secured shell's security? the connection established in ssh connection is encrypted in a way that only the devices connected in an ssh network can access the data, meaning, no other devices outside the network has permissions to the data.