Name: Christian Aaron C. Buduan	Date Performed: 8/25/2024
Course/Section: CPE 212 - CPE 31S2	Date Submitted: 8/25/2024
Instructor: Engr Robin Valenzuela	Semester and SY: 1st sem - 3rd year

Activity 1: Configure Network using Virtual Machines

1. **Objectives:**

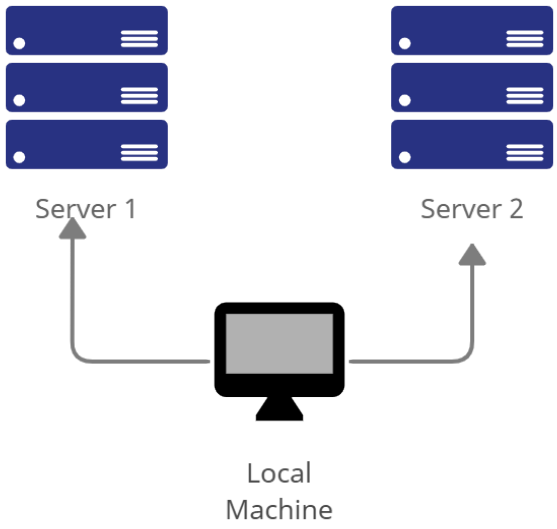
1.1. Create and configure Virtual Machines in Microsoft Azure or VirtualBox

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

```
qcacbuduan@BuduanDesktop:~$ sudo nano /etc/hostname
[sudo] password for qcacbuduan:
```

```
  GNU nano 6.2
server1
```

1.2 Use server2 for Server 2

```
qcacbuduan@BuduanDesktop:~$ sudo nano /etc/hostname
[sudo] password for qcacbuduan:
```

```
  GNU nano 6.2
server2
```

1.3 Use workstation for the Local Machine

```
qcacbuduan@BuduanDesktop:~$ sudo nano /etc/hostname
qcacbuduan@BuduanDesktop:~$
```

```
  GNU nano 6.2
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

```
qcacbuduan@BuduanDesktop:~$ sudo nano /etc/hosts
```

```
  GNU nano 6.2                                    /etc/h
127.0.0.1       localhost
127.0.0.1       BuduanDesktop.myguest.virtualbox.org
```

2.2 Type 127.0.0.1 server 2 for Server 2

```
qcacbuduan@BuduanDesktop:~$ sudo nano /etc/hosts
```

```
  GNU nano 6.2                                    /etc/ho
127.0.0.1       localhost
127.0.0.1       BuduanDesktop.myguest.virtualbox.org
```

2.3 Type 127.0.0.1 workstation for the Local Machine

```
qcacbuduan@BuduanDesktop:~$ sudo nano /etc/hosts
```

```
  GNU nano 6.2                                    /etc/hosts
127.0.0.1       localhost
127.0.0.1       BuduanDesktop.myguest.virtualbox.org
```

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

Workstation

```
qcacbuduan@BuduanDesktop:~$ sudo apt update && sudo apt upgrade
[sudo] password for qcacbuduan:
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://security.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
259 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
  ubuntu-pro-client ubuntu-pro-client-l10n
The following packages have been kept back:
  linux-generic-hwe-22.04 linux-headers-generic-hwe-22.04 linux-image-generic-hwe-22.04
  python3-update-manager update-manager update-manager-core
The following packages will be upgraded:
  alsa-ucm-conf apparmor apport apport-gtk apt apt-utils base-files bind9-dnsutils bind9-host
  bind9-libs bluez bluez-cups bluez-obexd busybox-initramfs busybox-static coreutils cpio cups
```

Server 1

```
qcacbuduan@BuduanDesktop:~$ sudo apt update
[sudo] password for qcacbuduan:
Hit:1 http://ph.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://ph.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:4 http://ph.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:5 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [690 kB]
Get:6 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1,987 kB]
Get:7 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [349 kB]
Get:8 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [103 kB]
Get:9 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main DEP-11 48x48 Icons [37.5 kB]
Get:10 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main DEP-11 64x64 Icons [56.8 kB]
Get:11 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [17.8 kB]
Get:12 http://ph.archive.ubuntu.com/ubuntu jammy-updates/restricted i386 Packages [38.9 kB]
Get:13 http://ph.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [2,384 kB]
35% [6 Packages store 0 B] [13 Packages 1,293 kB/2,384 kB 54%]
```

```
qcacbuduan@BuduanDesktop:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
  linux-generic-hwe-22.04 linux-headers-generic-hwe-22.04 linux-image-generic-hwe-22.04
  python3-update-manager ubuntu-advantage-tools update-manager update-manager-core
The following packages will be upgraded:
  alsa-ucm-conf apparmor apport apport-gtk apt apt-utils base-files bind9-dnsutils bind9-host
  bind9-libs bluez-obexd busybox-initramfs busybox-static coreutils cpio cups cups-bsd cups-client
  cups-common cups-core-drivers cups-daemon cups-ipp-utils cups-ppdc cups-server-common distro-info
```

Server 2

```
qcacbuduan@BuduanDesktop:~$ sudo apt update
[sudo] password for qcacbuduan:
0% [Connecting to ph.archive.ubuntu.com] [Waiting for headers]
```

```
qcacbuduan@BuduanDesktop:~$ sudo apt-get 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:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  linux-generic-hwe-22.04 linux-headers-generic-hwe-22.04 linux-image-generic-hwe-22.04
  python3-update-manager ubuntu-advantage-tools update-manager update-manager-core
The following packages will be upgraded:
  accountsservice alsa-ucm-conf apparmor apport apport-gtk apt apt-utils avahi-autoipd base-
  bash bluez-obexd bsdextrautils bsdutils busybox-initramfs coreutils cups-ppdc distro-info
  distro-info-data dns-root-data dnsmasq-base dpkg dpkg-dev e2fsprogs eject ethtool evince
  evince-common fdisk firmware-sof-signed fonts-noto-color-emoji fonts-opensymbol gdb gdm3
```

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

Workstation

```
qcacbuduan@BuduanDesktop:~$ sudo apt install openssh-server
[sudo] password for qcacbuduan:
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 6 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]
```

Server 1

```
qcacbuduan@BuduanDesktop:~$ sudo apt install openssh-server
[sudo] password for qcacbuduan:
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 7 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]
```

Server 2

```
qcacbuduan@BuduanDesktop:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
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 7 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]
```

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

Workstation

```
qcacbuduan@BuduanDesktop:~$ sudo service ssh start
[sudo] password for qcacbuduan:
qcacbuduan@BuduanDesktop:~$ 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 Sun 2024-08-25 20:06:10 +08; 25min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 88040 (sshd)
      Tasks: 1 (limit: 9430)
     Memory: 1.7M
        CPU: 43ms
     CGroup: /system.slice/ssh.service
             └─88040 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 25 20:06:10 BuduanDesktop systemd[1]: Starting OpenBSD Secure Shell server...
Aug 25 20:06:10 BuduanDesktop sshd[88040]: Server listening on 0.0.0.0 port 22.
Aug 25 20:06:10 BuduanDesktop sshd[88040]: Server listening on :: port 22.
Aug 25 20:06:10 BuduanDesktop systemd[1]: Started OpenBSD Secure Shell server.
```

Server 1

```
qcacbuduan@BuduanDesktop:~$ 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 Sun 2024-08-25 20:16:48 +08; 16min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 87956 (sshd)
      Tasks: 1 (limit: 9430)
     Memory: 1.7M
        CPU: 73ms
     CGroup: /system.slice/ssh.service
             └─87956 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 25 20:16:48 BuduanDesktop systemd[1]: Starting OpenBSD Secure Shell server...
Aug 25 20:16:48 BuduanDesktop sshd[87956]: Server listening on 0.0.0.0 port 22.
Aug 25 20:16:48 BuduanDesktop sshd[87956]: Server listening on :: port 22.
Aug 25 20:16:48 BuduanDesktop systemd[1]: Started OpenBSD Secure Shell server.
```

Server 2

```
qcacbuduan@BuduanDesktop:~$ 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 Sun 2024-08-25 20:34:42 +08; 47s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 79461 (sshd)
      Tasks: 1 (limit: 9430)
     Memory: 1.7M
        CPU: 50ms
     CGroup: /system.slice/ssh.service
             └─79461 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

ug 25 20:34:42 BuduanDesktop systemd[1]: Starting OpenBSD Secure Shell server...
ug 25 20:34:42 BuduanDesktop sshd[79461]: Server listening on 0.0.0.0 port 22.
ug 25 20:34:42 BuduanDesktop sshd[79461]: Server listening on :: port 22.
ug 25 20:34:42 BuduanDesktop systemd[1]: Started OpenBSD Secure Shell server.
```

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

Workstation

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

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

Server 1

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

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

Server 2

```
qcacbuduan@BuduanDesktop:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
qcacbuduan@BuduanDesktop:~$ sudo ufw enable
Firewall is active and enabled on system startup
qcacbuduan@BuduanDesktop:~$ 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.
3. Connectivity test for Local Machine 1 to Server 1:
   ☐ Successful ☐ Not Successful
   2.1 Connectivity test for Local Machine 1 to Server 2:
   ☐ Successful ☐ Not Successful
   2.2 Connectivity test for Server 1 to Server 2:
   ☐ Successful ☐ Not Successful

Documentation:

```
qcacbuduan@Workstation:~$ hostname -I
192.168.56.102
qcacbuduan@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=0.856 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=1.00 ms
^C
--- 192.168.56.103 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 0.856/0.928/1.001/0.072 ms
```

```
qcacbuduan@Workstation:~$ ping 192.168.56.104
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data.
64 bytes from 192.168.56.104: icmp_seq=1 ttl=64 time=2.06 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=64 time=2.19 ms
64 bytes from 192.168.56.104: icmp_seq=3 ttl=64 time=1.45 ms
^C
--- 192.168.56.104 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2422ms
rtt min/avg/max/mdev = 1.445/1.897/2.187/0.324 ms
```

```
qcacbuduan@server1:~$ ping 192.168.56.104
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data.
64 bytes from 192.168.56.104: icmp_seq=1 ttl=64 time=2.43 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=64 time=1.99 ms
64 bytes from 192.168.56.104: icmp_seq=3 ttl=64 time=1.10 ms
^C
--- 192.168.56.104 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.100/1.841/2.432/0.554 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*

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*

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

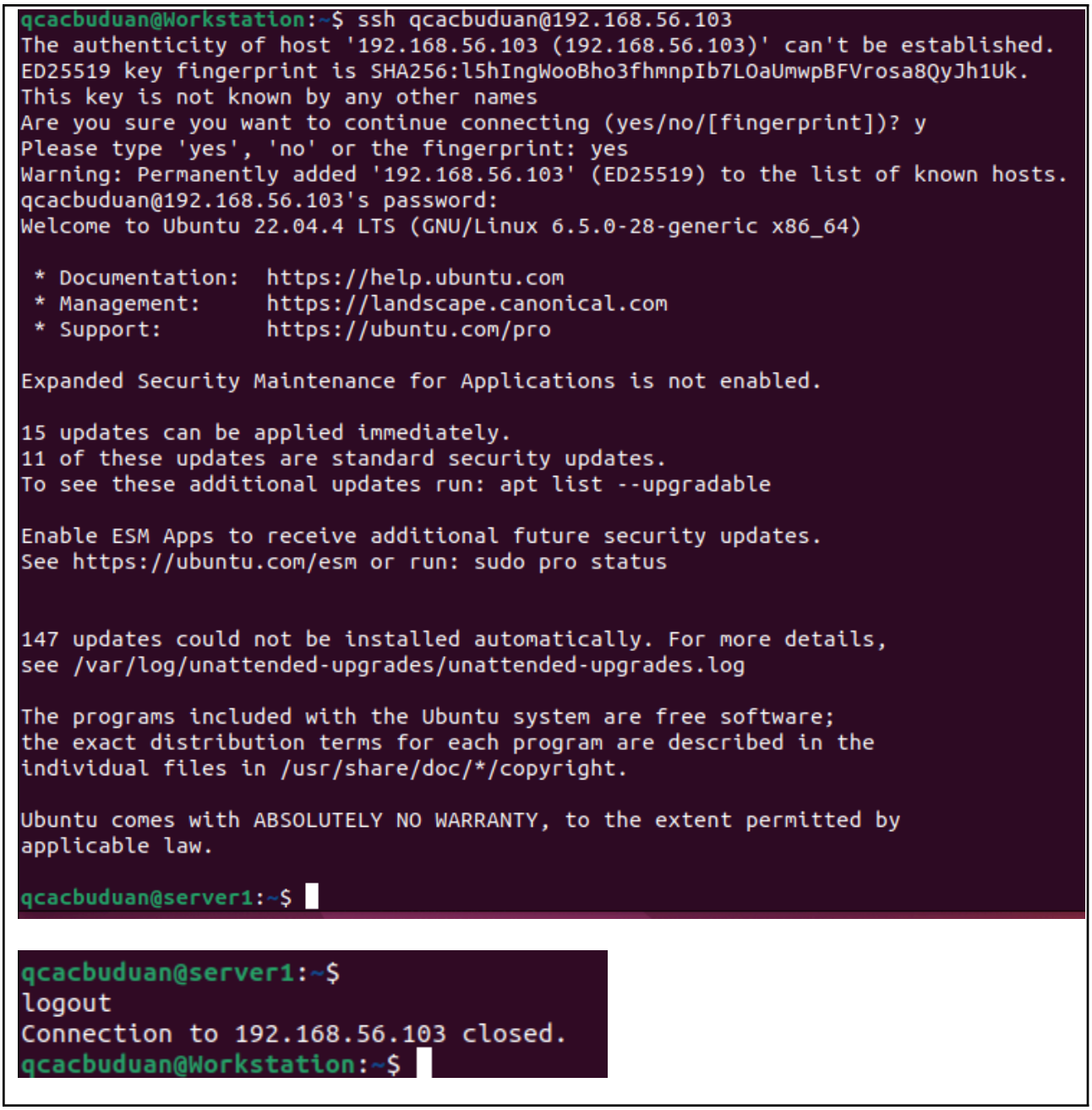
4.1 IP_address server 1 (provide the ip address of server 1 followed by the hostname)

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

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.

Documentation:


qcacbuduan@Workstation:~$ ssh qcacbuduan@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:l5hIngWooBho3fhmnpIb7LOaUmwpBFVrosa8QyJh1Uk.
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 '192.168.56.103' (ED25519) to the list of known hosts.
qcacbuduan@192.168.56.103's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-28-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.
15 updates can be applied immediately.
11 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
147 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
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.
qcacbuduan@server1:~$
qcacbuduan@server1:~$
logout
Connection to 192.168.56.103 closed.
qcacbuduan@Workstation:~$


qcacbuduan@Workstation:~$ ssh qcacbuduan@192.168.56.104
The authenticity of host '192.168.56.104 (192.168.56.104)' can't be established.
ED25519 key fingerprint is SHA256:TPogV7Zbw7IgK8VvS2d4ccDUoFJpHm2tVPvtfga4Woc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.104' (ED25519) to the list of known hosts.
qcacbuduan@192.168.56.104's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-18-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.
15 updates can be applied immediately.
11 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
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.
qcacbuduan@server2:~$
qcacbuduan@server2:~$
logout
Connection to 192.168.56.104 closed.
qcacbuduan@Workstation:~$
qcacbuduan@Workstation:~$ sudo nano /etc/hosts
[sudo] password for qcacbuduan:

```
  GNU nano 6.2                                  /etc/hosts *
127.0.0.1       workstation
127.0.0.1       BuduanDesktop.myguest.virtualbox.org    BuduanDesktop
192.168.56.103  server1
192.168.56.104  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
```

```
qcacbuduan@Workstation:~$ ssh qcacbuduan@server1
The authenticity of host 'server1 (192.168.56.103)' can't be established.
ED25519 key fingerprint is SHA256:l5hIngWooBho3fhmnpIb7LOaUmwpBFVrosa8QyJh1Uk.
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.
qcacbuduan@server1's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-28-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.

15 updates can be applied immediately.
11 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

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


147 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Last login: Sun Aug 25 23:20:22 2024 from 192.168.56.102
qcacbuduan@server1:~$
logout
Connection to server1 closed.
qcacbuduan@Workstation:~$
```

```
qcacbuduan@Workstation:~$ ssh qcacbuduan@server2
The authenticity of host 'server2 (192.168.56.104)' can't be established.
ED25519 key fingerprint is SHA256:TPogV7Zbw7IgK8VvS2d4ccDUoFJpHm2tVPvtfga4Woc.
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.
qcacbuduan@server2's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-18-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.

15 updates can be applied immediately.
1 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

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

Last login: Sun Aug 25 23:23:09 2024 from 192.168.56.102
qcacbuduan@server2:~$
logout
Connection to server2 closed.
qcacbuduan@Workstation:~$
```

Reflections:

Answer the following:

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

   On the text file /etc/hosts, the student appended new information in which inputting the entered hostname right beside the IP address will make it as another way to change or move from server to server due to its difficulties of remembering multiple IP addresses in a set of multiple network topologies. Using this method will make the System Administrator to move another server or computer more efferently, yet if the admin entered an unknown word, or a wrong character because it is case sensitive, IP address and the information inside the /host text file was not listed will result into an error.

2. **How secure is SSH?**

   SSH is a network communication protocol that allow two or more computers to interact with each other mostly between SSH client and server. It secures its data by encrypting its contents to avoid an unauthorized person from interacting with unknown sources.