

Name: Flores, Marc Oliver U.	Date Performed: 15/08/2023
Course/Section: CPE 232-CPE31S4	Date Submitted: 15/08/2023
Instructor: Dr. Jonathan V. Taylar	Semester and SY: First Semester 2023-2024

Activity 1: Configure Network using Virtual Machines

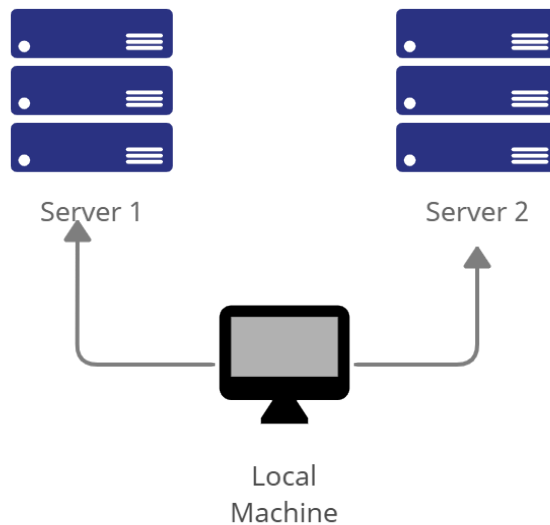
1. Objectives:

- 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 the prior knowledge of cloning and creating snapshots in a virtual machine).



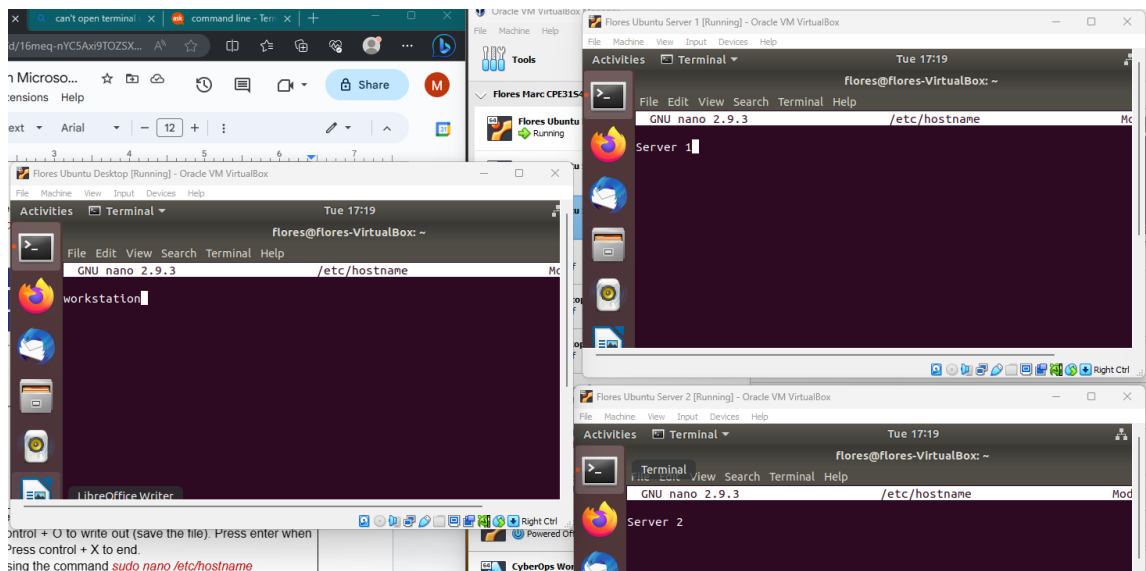
Task 1: Do the following on Server 1, Server 2, and Local Machine. In editing the file using nano command, press control + O to write out (save the file). Press enter when asked for the name of the file. Press control + X to end.

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

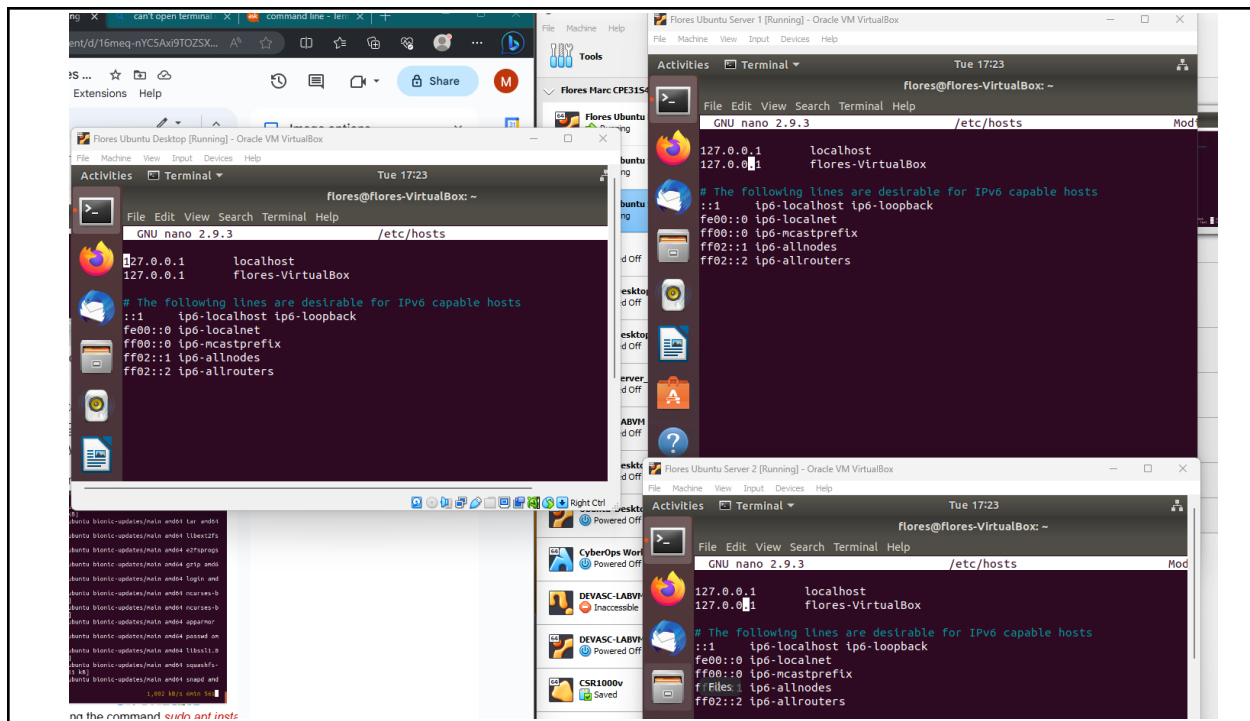


2. Edit the hosts using the command *sudo nano /etc/hosts*. Edit the second line.

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



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.

I did this by doing the command: `sudo apt update | sudo apt upgrade -y`

```

File Edit View Search Terminal Help
64 2.7.6-2ubuntu1.1 [102 kB]
Get:152 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libpam0g
amd64 1.1.8-3.6ubuntu2.18.04.6 [54.3 kB]
Get:153 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 tar amd64
1.29b-2ubuntu0.4 [234 kB]
Get:154 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libx2f5
2 amd64 1.44.1-1ubuntu1.4 [156 kB]
Get:155 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 e2fsprogs
amd64 1.44.1-1ubuntu1.4 [390 kB]
Get:156 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 gzip amd6
4 1.6-5ubuntu1.2 [90.3 kB]
Get:157 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 login amd
64 1:4.5-1ubuntu2.5 [307 kB]
Get:158 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ncurses-b
in amd64 6.1-1ubuntu1.18.04.1 [163 kB]
Get:159 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ncurses-b
ase all 6.1-1ubuntu1.18.04.1 [18.3 kB]
Get:160 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 apparmor
amd64 2.12-4ubuntu5.3 [488 kB]
Get:161 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 passwd am
d64 1:4.5-1ubuntu2.5 [818 kB]
Get:162 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libssl1.0
.0 amd64 1.0.2n-1ubuntu5.13 [1,089 kB]
Get:163 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 squashfs-
tools amd64 1:4.3-6ubuntu0.18.04.4 [111 kB]
Get:164 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 snapd amd
64 2.58+18.04.1 [37.9 MB]
36% [164 snapd 11.1 MB/37.9 MB 29%] 1,092 kB/s 6min 56s

```

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

```
flores@flores-VirtualBox:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere rssh 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 0 not upgraded.
Need to get 637 kB of archives.
After this operation, 5,320 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ncurses-ter
m all 6.1-1ubuntu1.18.04.1 [248 kB]
Get:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-sft
p-server amd64 1:7.6p1-4ubuntu0.7 [45.5 kB]
Get:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-ser
ver amd64 1:7.6p1-4ubuntu0.7 [332 kB]
Get:4 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ssh-import-
id all 5.7-0ubuntu1.1 [10.9 kB]
Fetched 637 kB in 2s (403 kB/s)
Preconfiguring packages ...
```

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*

```
flores@flores-VirtualBox:~$ sudo service ssh start
flores@flores-VirtualBox:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
   Active: active (running) since Tue 2023-08-15 17:24:45 PST; 1min 41s ago
     Main PID: 2312 (sshd)
        Tasks: 1 (limit: 2318)
       CGroup: /system.slice/ssh.service
              └─2312 /usr/sbin/sshd -D

Aug 15 17:24:45 flores-VirtualBox systemd[1]: Starting OpenBSD Secure Shell ser
Aug 15 17:24:45 flores-VirtualBox sshd[2312]: Server listening on 0.0.0.0 port
Aug 15 17:24:45 flores-VirtualBox sshd[2312]: Server listening on :: port 22
```

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*

```
flores@flores-VirtualBox:~$ sudo ufw allow ssh
```

```
Rules updated
```

```
Rules updated (v6)
```

```
flores@flores-VirtualBox:~$ sudo ufw enable
```

```
Firewall is active and enabled on system startup
```

```
flores@flores-VirtualBox:~$ sudo ufw status
```

```
Status: active
```

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

```
flores@flores-VirtualBox:~$
```

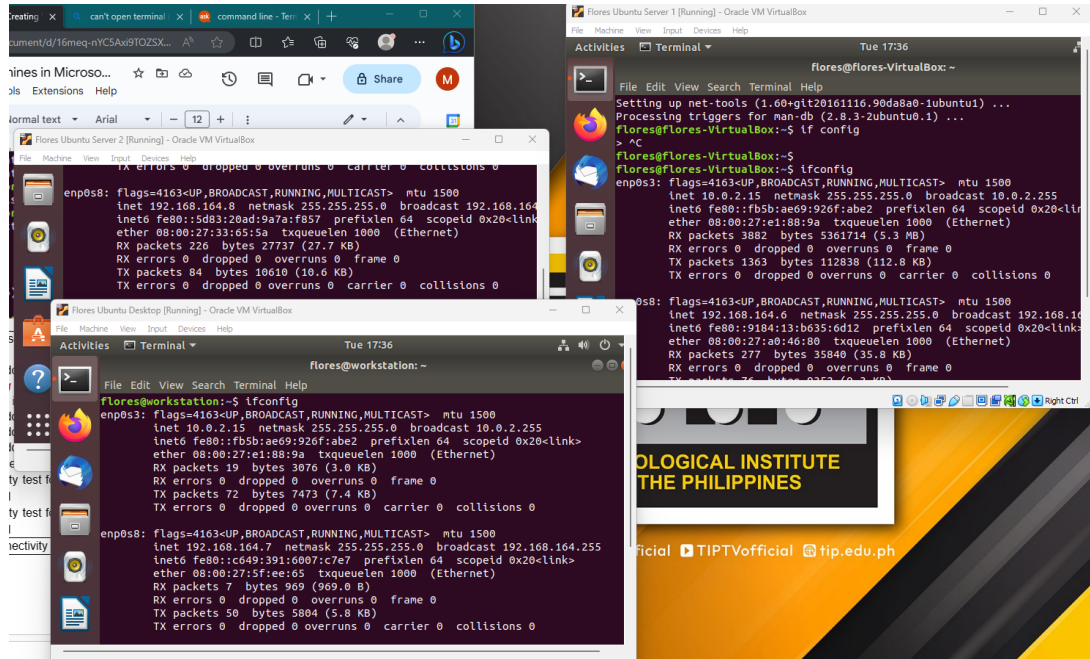
Task 3: Verify network settings on Server 1, Server 2, and Local Machine. On each device, do the following:

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.____

1.2 Server 2 IP address: 192.168.56.____

1.3 Server 3 IP address: 192.168.56.____



2. Make sure that they can ping each other.

2.1 Connectivity test for Local Machine 1 to Server 1: / Successful ☐ Not Successful

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

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

```
flores@workstation:~$ ping 192.168.164.8
PING 192.168.164.8 (192.168.164.8) 56(84) bytes of data.
64 bytes from 192.168.164.8: icmp_seq=1 ttl=64 time=0.948 ms
64 bytes from 192.168.164.8: icmp_seq=2 ttl=64 time=1.10 ms
64 bytes from 192.168.164.8: icmp_seq=3 ttl=64 time=1.32 ms
64 bytes from 192.168.164.8: icmp_seq=4 ttl=64 time=1.43 ms
64 bytes from 192.168.164.8: icmp_seq=5 ttl=64 time=0.472 ms
64 bytes from 192.168.164.8: icmp_seq=6 ttl=64 time=1.03 ms
64 bytes from 192.168.164.8: icmp_seq=7 ttl=64 time=0.443 ms
64 bytes from 192.168.164.8: icmp_seq=8 ttl=64 time=0.648 ms
64 bytes from 192.168.164.8: icmp_seq=9 ttl=64 time=1.78 ms
64 bytes from 192.168.164.8: icmp_seq=10 ttl=64 time=1.34 ms
64 bytes from 192.168.164.8: icmp_seq=11 ttl=64 time=1.60 ms
64 bytes from 192.168.164.8: icmp_seq=12 ttl=64 time=1.16 ms
64 bytes from 192.168.164.8: icmp_seq=13 ttl=64 time=1.66 ms
64 bytes from 192.168.164.8: icmp_seq=14 ttl=64 time=1.26 ms
64 bytes from 192.168.164.8: icmp_seq=15 ttl=64 time=1.84 ms
64 bytes from 192.168.164.8: icmp_seq=16 ttl=64 time=1.48 ms
64 bytes from 192.168.164.8: icmp_seq=17 ttl=64 time=1.26 ms
64 bytes from 192.168.164.8: icmp_seq=18 ttl=64 time=1.21 ms
```

```
flores@flores-VirtualBox:~$ ping 192.168.164.7
PING 192.168.164.7 (192.168.164.7) 56(84) bytes of data.
64 bytes from 192.168.164.7: icmp_seq=1 ttl=64 time=0.948 ms
64 bytes from 192.168.164.7: icmp_seq=2 ttl=64 time=1.10 ms
64 bytes from 192.168.164.7: icmp_seq=3 ttl=64 time=1.32 ms
64 bytes from 192.168.164.7: icmp_seq=4 ttl=64 time=1.43 ms
64 bytes from 192.168.164.7: icmp_seq=5 ttl=64 time=0.472 ms
64 bytes from 192.168.164.7: icmp_seq=6 ttl=64 time=1.03 ms
64 bytes from 192.168.164.7: icmp_seq=7 ttl=64 time=0.443 ms
64 bytes from 192.168.164.7: icmp_seq=8 ttl=64 time=0.648 ms
64 bytes from 192.168.164.7: icmp_seq=9 ttl=64 time=1.78 ms
64 bytes from 192.168.164.7: icmp_seq=10 ttl=64 time=1.34 ms
64 bytes from 192.168.164.7: icmp_seq=11 ttl=64 time=1.60 ms
64 bytes from 192.168.164.7: icmp_seq=12 ttl=64 time=1.16 ms
64 bytes from 192.168.164.7: icmp_seq=13 ttl=64 time=1.66 ms
64 bytes from 192.168.164.7: icmp_seq=14 ttl=64 time=1.26 ms
64 bytes from 192.168.164.7: icmp_seq=15 ttl=64 time=1.84 ms
64 bytes from 192.168.164.7: icmp_seq=16 ttl=64 time=1.48 ms
64 bytes from 192.168.164.7: icmp_seq=17 ttl=64 time=1.26 ms
```

```
[1] + stopped ping 192.168.164.7
flores@flores-VirtualBox:~$ ping 192.168.164.6
PING 192.168.164.6 (192.168.164.6) 56(84) bytes of data.
64 bytes from 192.168.164.6: icmp_seq=1 ttl=64 time=0.948 ms
64 bytes from 192.168.164.6: icmp_seq=2 ttl=64 time=1.10 ms
64 bytes from 192.168.164.6: icmp_seq=3 ttl=64 time=1.32 ms
64 bytes from 192.168.164.6: icmp_seq=4 ttl=64 time=1.43 ms
64 bytes from 192.168.164.6: icmp_seq=5 ttl=64 time=0.472 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 jvtaylor@192.168.56.120`

1.2 Enter the password for server 1 when prompted

```
flores@workstation:~$ ssh flores@192.168.164.7
The authenticity of host '192.168.164.7 (192.168.164.7)' can't be established.
ECDSA key fingerprint is SHA256:Qv2fASqW0DdrA8UmlkJHW3+RJbSIp8TQaCJkN90eSI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.164.7' (ECDSA) to the list of known hosts.
flores@192.168.164.7's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

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

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

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

Your Hardware Enablement Stack (HWE) is supported until April 2023.

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.
```

1.3 Verify that you are in server 1. The user should be in this format `user@server1`.

For example, `jvtaylor@server1`

```
New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Tue Aug 15 17:44:24 2023 from 192.168.164.7
flores@Server1:~$
```

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

```
Last login: Tue Aug 15 17:44:24 2023 from 192.168.164.7
flores@Server1:~$ logout
Connection to 192.168.164.6 closed.
flores@workstation:~$
```

3. Do the same for Server 2.


```

See https://ubuntu.com/esm or run: sudo pro statu
Your Hardware Enablement Stack (HWE) is supported

The programs included with the Ubuntu system are
the exact distribution terms for each program are
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the
applicable law.

flores@Server2:~$ logout
Connection to 192.168.164.8 closed.
flores@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.

```

GNU nano 2.9.3 /etc/hosts

127.0.0.1    localhost
127.0.0.1    flores-VirtualBox
192.168.164.6 server 1
192.168.164.8 server 2

# 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

```

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 jvtaylor@server1`. Enter the password when prompted. Verify that you have entered Server 1. Do the same for Server 2.

```
flores@workstation:~$ ssh flores@server1
The authenticity of host 'server1 (192.168.164.6)' can't be established.
ECDSA key fingerprint is SHA256:PyDzR4092i+88DbHRMdNNbbRZvNZlkyeWBqqzxKoyOI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server1' (ECDSA) to the list of known hosts.
flores@server1's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

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

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

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

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Tue Aug 15 17:46:35 2023 from 192.168.164.7
flores@Server1:~$
```

```
flores@workstation:~$ ssh flores@server2
The authenticity of host 'server2 (192.168.164.8)' can't be established.
ECDSA key fingerprint is SHA256:EmxL5wZPQ03ae6rvlpKPINbyCnpUa/eiRLGLQrAqWOY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server2' (ECDSA) to the list of known hosts.
flores@server2's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

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

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

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

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Tue Aug 15 17:47:21 2023 from 192.168.164.7
flores@Server2:~$
```

Reflections:

Answer the following:

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

You can use the hostname instead of IP address in SSH commands because of the name resolution. The name resolution is the process of mapping a name to an IP address.

2. How secured is SSH?

SSH or known as Secure Shell is a secure protocol that provides a mechanism for establishing a cryptographically secured connection between two parties, authenticating each side to the other, and passing the commands and output back and forth.

Conclusion:

In this laboratory activity I was able to create and configure a virtual machine in a virtual box and setup a virtual network and test connectivity of the VMs. I was able to perform each of the tasks because of the clear demonstration and guidance of our instructor. I was also encountered a problem where I can't open my terminal and find a solution on the internet to proceed with my activity.