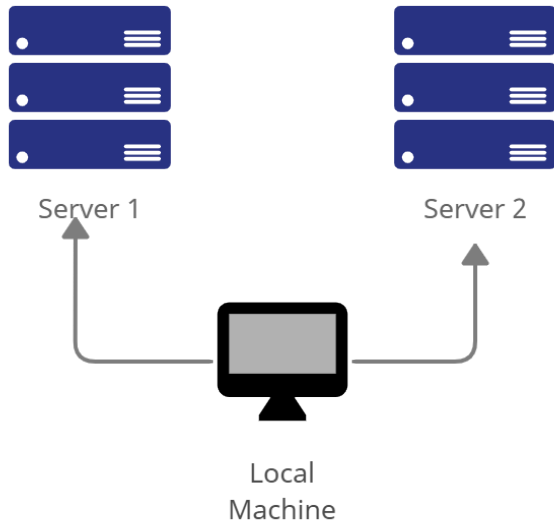
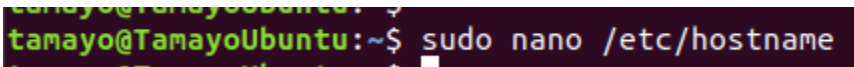


Name: Tamayo, Ray Lan A.	Date Performed: 08/30/2024
Course/Section: CPE212-CPE31S21	Date Submitted: 08/30/2024
Instructor: Engr. Robin Valenzuela	Semester and SY: First Semester 2024-25
Activity 1: Configure Network using Virtual Machines	
1. Objectives: 1.1. Create and configure Virtual Machines in 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, <i>provide screenshots for each task</i> . (Note: <i>it is assumed that you have the prior knowledge of cloning and creating snapshots in a virtual machine</i>).	
 <pre> graph TD LocalMachine[Local Machine] --- Server1[Server 1] LocalMachine --- Server2[Server 2] subgraph Server1_Rack [Server 1] S1_1[] S1_2[] S1_3[] end subgraph Server2_Rack [Server 2] S2_1[] S2_2[] S2_3[] end </pre>	
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 <i>sudo nano /etc/hostname</i>	
	
1.1 Use server1 for Server 1	

```

tamayo@TamayoUbuntu: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/hostname
Server1

```

1.2 Use server2 for Server 2

```

tamayo@TamayoUbuntu: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/hostname
server2

```

1.3 Use workstation for the Local Machine

```

Fri 09:04
tamayo@TamayoUbuntu: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/hostname
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

```

tamayo@TamayoUbuntu: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/hosts
127.0.0.1 server 1
127.0.1.1 TamayoUbuntu.myguest.virtualbox.org TamayoUbuntu

# 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

```

File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/hosts

127.0.0.1      server2
127.0.1.1      TamayoUbuntu.myquest.virtualbox.org    TamayoUbuntu

# 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

```

tamayo@TamayoUbuntu: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/hosts

127.0.0.1      workstation
127.0.1.1      TamayoUbuntu.myquest.virtualbox.org    TamayoUbuntu

# 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.

```

tamayo@TamayoUbuntu:~$ sudo apt update
Hit:1 http://ph.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://ph.archive.ubuntu.com/ubuntu bionic-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu bionic-security InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
676 packages can be upgraded. Run 'apt list --upgradable' to see them.

```



```
tamayo@TamayoUbuntu:~$ sudo service ssh start
tamayo@TamayoUbuntu:~$
```

3.2 *sudo systemctl status ssh*

```
tamayo@TamayoUbuntu:~$ 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 Fri 2024-08-30 10:18:49 +08; 1min 4s ago
   Main PID: 19495 (sshd)
     Tasks: 1 (limit: 2318)
    CGroup: /system.slice/ssh.service
            └─19495 /usr/sbin/sshd -D

Aug 30 10:18:49 TamayoUbuntu systemd[1]: Starting OpenBSD Secure Shell server..
Aug 30 10:18:49 TamayoUbuntu sshd[19495]: Server listening on 0.0.0.0 port 22.
Aug 30 10:18:49 TamayoUbuntu sshd[19495]: Server listening on :: port 22.
Aug 30 10:18:49 TamayoUbuntu systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (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*

```
tamayo@TamayoUbuntu:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
tamayo@TamayoUbuntu:~$ sudo ufw enable
sudoFirewall is active and enabled on system startup
tamayo@TamayoUbuntu:~$ 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: 192.168.56.125

```
inet 192.168.56.125,
```

1.2 Server 2 IP address: 192.168.56.126

```
inet 192.168.56.126,
```

1.3 Server 3 IP address: 192.168.56.127

```
inet 192.168.56.127
```

2. Make sure that they can ping each other.

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

```
tamayo@workstation:~$ ping 192.168.56.125
PING 192.168.56.125 (192.168.56.125) 56(84) bytes of data.
64 bytes from 192.168.56.125: icmp_seq=1 ttl=64 time=0.318 ms
64 bytes from 192.168.56.125: icmp_seq=2 ttl=64 time=0.210 ms
64 bytes from 192.168.56.125: icmp_seq=3 ttl=64 time=0.284 ms
64 bytes from 192.168.56.125: icmp_seq=4 ttl=64 time=0.221 ms
64 bytes from 192.168.56.125: icmp_seq=5 ttl=64 time=0.194 ms
64 bytes from 192.168.56.125: icmp_seq=6 ttl=64 time=0.200 ms
64 bytes from 192.168.56.125: icmp_seq=7 ttl=64 time=0.180 ms
64 bytes from 192.168.56.125: icmp_seq=8 ttl=64 time=0.193 ms
64 bytes from 192.168.56.125: icmp_seq=9 ttl=64 time=0.207 ms
64 bytes from 192.168.56.125: icmp_seq=10 ttl=64 time=0.187 ms
64 bytes from 192.168.56.125: icmp_seq=11 ttl=64 time=0.194 ms
64 bytes from 192.168.56.125: icmp_seq=12 ttl=64 time=0.191 ms
64 bytes from 192.168.56.125: icmp_seq=13 ttl=64 time=0.185 ms
64 bytes from 192.168.56.125: icmp_seq=14 ttl=64 time=0.196 ms
64 bytes from 192.168.56.125: icmp_seq=15 ttl=64 time=0.240 ms
64 bytes from 192.168.56.125: icmp_seq=16 ttl=64 time=0.208 ms
64 bytes from 192.168.56.125: icmp_seq=17 ttl=64 time=0.196 ms
64 bytes from 192.168.56.125: icmp_seq=18 ttl=64 time=0.217 ms
64 bytes from 192.168.56.125: icmp_seq=19 ttl=64 time=0.199 ms
64 bytes from 192.168.56.125: icmp_seq=20 ttl=64 time=0.262 ms
64 bytes from 192.168.56.125: icmp_seq=21 ttl=64 time=0.249 ms
64 bytes from 192.168.56.125: icmp_seq=22 ttl=64 time=0.259 ms
64 bytes from 192.168.56.125: icmp_seq=23 ttl=64 time=0.320 ms
64 bytes from 192.168.56.125: icmp_seq=24 ttl=64 time=0.262 ms
64 bytes from 192.168.56.125: icmp_seq=25 ttl=64 time=0.267 ms
64 bytes from 192.168.56.125: icmp_seq=26 ttl=64 time=0.267 ms
64 bytes from 192.168.56.125: icmp_seq=27 ttl=64 time=0.214 ms
```

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

```
tamayo@workstation:~$ ping 192.168.56.126
PING 192.168.56.126 (192.168.56.126) 56(84) bytes of data.
64 bytes from 192.168.56.126: icmp_seq=1 ttl=64 time=0.427 ms
64 bytes from 192.168.56.126: icmp_seq=2 ttl=64 time=0.258 ms
64 bytes from 192.168.56.126: icmp_seq=3 ttl=64 time=0.197 ms
64 bytes from 192.168.56.126: icmp_seq=4 ttl=64 time=0.211 ms
64 bytes from 192.168.56.126: icmp_seq=5 ttl=64 time=0.368 ms
64 bytes from 192.168.56.126: icmp_seq=6 ttl=64 time=0.249 ms
64 bytes from 192.168.56.126: icmp_seq=7 ttl=64 time=0.230 ms
64 bytes from 192.168.56.126: icmp_seq=8 ttl=64 time=0.214 ms
64 bytes from 192.168.56.126: icmp_seq=9 ttl=64 time=0.224 ms
64 bytes from 192.168.56.126: icmp_seq=10 ttl=64 time=0.234 ms
```

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


```

tamayo@server1:~$ ping 192.168.56.126
PING 192.168.56.126 (192.168.56.126) 56(84) bytes of data.
64 bytes from 192.168.56.126: icmp_seq=1 ttl=64 time=0.343 ms
64 bytes from 192.168.56.126: icmp_seq=2 ttl=64 time=0.366 ms
64 bytes from 192.168.56.126: icmp_seq=3 ttl=64 time=0.204 ms
64 bytes from 192.168.56.126: icmp_seq=4 ttl=64 time=0.209 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`

```

tamayo@workstation:~$ ssh tamayo@192.168.56.127
The authenticity of host '192.168.56.127 (192.168.56.127)' can't be established
.
ECDSA key fingerprint is SHA256:ZK5SHZiOnhdGMU7/JetkkECT3H7+g4VQU+oUU3ybQ0k.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.56.127' (ECDSA) to the list of known hosts.
tamayo@192.168.56.127'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/pro

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.

```

1.2 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, `jvtaylor@server1`

```
tamayo@workstation:~$ ssh tamayo@192.168.56.127
tamayo@192.168.56.127'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/pro

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

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

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Fri Aug 30 10:55:36 2024 from 192.168.56.127
```

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

```
tamayo@workstation:~$ logout
Connection to 192.168.56.127 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)
 - 4.3 Save the file and exit.

```
tamayo@workstation: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/hosts

192.168.56.125 server1
192.168.56.126 server2
192.168.56.127 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
```

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.

```
tamayo@workstation:~$ ssh tamayo@server1
The authenticity of host 'server1 (192.168.56.125)' can't be established.
ECDSA key fingerprint is SHA256:Yx60zXHARXnzKNlyqXP3QKM0simk8Cte/dd/ikuWmus.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server1,192.168.56.125' (ECDSA) to the list of known hosts.
tamayo@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/pro

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

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

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Fri Aug 30 10:59:51 2024 from 192.168.56.125
```

Reflections:

Answer the following:

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

In the command we are able to use the hostname instead of IP address in SSH commands is that we change the IP address or we add the IP address in the command.

2. How secured is SSH?

The SSH is very secure since the SHH is encrypted and also the authentication of the ssh since it has a strong authentication and public key authentication.

Conclusion

I conclude that I was able to do all the objectives in the activity that I am able to create and configure the virtualbox and also I was able to set-up a virtual network and test the connectivity of the VMs. The activity is very easy since there are step by step procedures on how we can create, configure and set-up in the network. I was able to configure SSH on Server 1, Server 2, and Local

Machine, edit the hosts using the command `sudo nano /etc/hosts`. and also verify SSH connectivity on Server 1, Server 2, and Local Machine. So there are many error that I encounter during the activity and I was able to solve the problems that I encountered during the activity.