**CSC4200 – Homework 1**

**Initial Setup**

**You are allowed to collaborate with other students on this portion. This portion is ungraded.**

1) Set up a Google Cloud account by visiting here:

https://cloud.google.com/free/

Make sure you receive the $300 credit.

2) Sign in, go to console.

https://console.cloud.google.com/

3) From Menu on the left, go to "Compute Engine", and click on "VM instances"

4) Create an instance. Make sure of the following configurations:

- Machine type: n1-standard-2
- Boot disk – Ubuntu 18.04 LTS
- Disk size – 10 GB

5) Create another VM of same specification.

6) Note the external IP and Internal IP.

7) Configure the firewall.

- Search for “vpc firewall rules” on the console.
- Click on it.
- Delete all the existing rules
- Click on “Create Firewall Rule”

8) Use the following config:

- Name: allowall
- Direction: Ingress
- Action on match: allow
- **Targets: “All instances in the network”**
- Source filter: IP ranges
- Source IP ranges: 0.0.0.0/0
- Protocols and ports: Allow all
- Click on “Create”

9) SSH

a) If using Linux

i) Generate a pair of public/private keys

On Linux, you will run the following command and follow the prompt. For the purpose of this class, a passphrase is unnecessary and can be left blank.

$ ssh-keygen -t rsa

ii) Deploy the key onto google cloud:

(1) Search for "ssh keys" on the console.

(2) Copy and paste the content of the "id_rsa.pub" file into the text field. The location of this file was selected when creating the key earlier.

(3) Save

iii) SSH into your machines – from a terminal, type

$ ssh <your instance's public IP>

b) If using Windows

i) Download and install Putty

(1) Download the 32 bit or 64 bit installer depending on your Operating System with the default settings.

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

(2) Find and open "puttygen"

Hit the generate button while keeping default settings.

(3) Change the " Key comment " to your TNtech username, you will use this as your username in future steps.

(4) Save the private key but do not close the keygen window yet.

(5) Deploy the public key onto google cloud:

(a) Search for “ssh keys” on the Google console.

(b) Copy and paste the content of the “public key” windows from the KeyGen program into the text field

(c) Save

(d) Close the KeyGen window

(6) Find and open “putty”

(a) In the **Category** menu on the left, navigate to **Connection** > **SSH** > **Auth**

(b) In the Private key file for authentication field, browse to the location of the private key saved in the previous step.

(c) In the **Category** menu on the left, navigate back to **Session**

(d) In the Host Name spot insert the external IP of one of the instances.

(e) In the Saved Sessions box, name the server and hit save.

(i) Repeat this for all servers to allow easier ssh access in the future.

(7) When asked for the username, use your TNtech username you entered when creating the SSH key.

**INDIVIDUAL HOMEWORK (Do not collaborate)**

**Please submit a PDF with your work. You might find the "man" command to be very useful.**

SSH into two instances and perform the following tests:

1. Run **ping** between two instances and record the outputs for ***both*** internal and external interfaces. (5pts)

2. Submit the output as a screenshot and a table that briefly explains each field of the output. (20pts)

3. Install traceroute (sudo apt update && sudo apt install traceroute).

4. Run **traceroute** to tntech.edu, record the output (5 pts)

5. Submit the output as a screenshot and a table that briefly explains each field (20 pts)

6. Run **ifconfig** and record the output. (5pts)

7. Submit the output as a screenshot and the following information for an interface that is *not "lo"*: IP address, Ethernet Address, netmask, and MTU (20pts)

8. Run **ip route show** and submit the output as a screenshot (5 pts)

9. Explain the first line of the output (20 pts)