National University of Singapore
School of Computing

CS2105 **DIY Exercise 4** Semester 2 12/13

HAVE FUN, AND BE CURIOUS

1. This question assumes that you have gone through Problem 2 of Problem Set 7 and understand what a root certificate is. Go look for the root certificates installed on your computer.

   - On Mac OS X, launch the application "Keychain Access"
   - On Microsoft Windows, launch "Certificate Manager" by clicking on the Start button, typing "certmgr.msc" into the Search box, and pressing Enter.
   - On Linux, AFAIK, there is no nice GUI tool to view the certificates. The command line tool "openssl" allows you to view installed certificates, usually under /etc/pki/tls/.

   Are these root certificates unsigned or self-signed? Who issued the root certificates?

2. This questions assume that you have the School of Computing Virtual Private Network (SoC VPN) setup on your computer. For documentation on SoC VPN and setup instructions, see `https://docs.comp.nus.edu.sg/node/1553`. For help with setup, please approach the Technical Help Desk at COM1 Level 1.

   We also assume that you are comfortable with running Wireshark, capturing packets, and filtering the display of packets.

   You can follow this exercise even if you are connected to the Internet from within NUS.

   (a) First, pick one of the IP addresses of www.google.com by running `dig`. Suppose the IP address you pick is 123.45.67.89.

   (b) Leave the SoC VPN off. Run Wireshark and start capturing packets. Run the following command:

   ```
   curl -I 123.45.67.89
   ```

   Use Wireshark to filter out the packets you sent and received from this IP address with the filter `ip.addr == 123.45.67.89`. Take a good look at the packets.

   (c) Now, turn on SoC VPN. Run Wireshark and restart your packet capture. Run the same `curl` command again, and using the same filter to filter the packets capture. What do you see (or not see)?

   (d) Stop capturing, remove the filters, and observes all the TCP traffic captured. Where has all the TCP traffic gone to?

3. In this question, you will learn to setup a pair of private key and public key for communication between your sunfire account and your cs2105-z account. With these setup, you no longer have to key in your password everytime you ssh into cs2105-z from sunfire!

   - On sunfire, type the command:

     ```
     ssh-keygen -t rsa
     ```

     This command generates a pair of keys, a public key and private key. When asked, you can save the keys at the suggested location (under $HOME/.ssh) with the default names (id_rsa for private key and id_rsa.pub for public key). You can enter an empty string for passphrase if you like[1].
   - Since id_rsa is your private key, make sure you set the permission correctly (chmod 600 /.ssh/id_rsa if you are not sure) so that noone else can read your private key.
   - Now, make a copy of your public key and put it under $HOME/.ssh directory on your cs2105-z account under the name `authorized_keys`. Run the following command on sunfire:

[1] A passphrase is like a password. It provides additional protection to the private key

`scp ~/.ssh/id_rsa.pub cs2105-z.comp.nus.edu.sg:~/.ssh/authorized_keys`

This command assumes that the file `authorized_keys` does not already exist. If it does, I assume that you already know what you are doing and know how to add a new public key to the file.

- After this step, try ssh into cs2105-z from sunfire. You should now be able to login directly without password!

(a) What is the purpose of copying the public key to cs2105-z? Why not the private key?

(b) What does using these pair of public/private key ensure? Confidentiality? Authentication? Or message integrity?

(c) If you ssh from cs2105-z back to sunfire, do you still need to enter a password? Why?

THE END