CS2107 Self-Exploration Activity 8: Wireshark and Nmap

Notes:

In this Activity 8 about **Wireshark** and **Nmap**, which have been discussed and shown in the lecture, you will perform the following:

1. To use **Wireshark** to inspect captured network packets;
2. To use **Nmap** to find out open ports of a host.

Task 1: Using Wireshark to Inspect Captured Packets

Let's try using **Wireshark**. First, download and install Wireshark (and its necessary dependencies) from https://www.wireshark.org. Then, download a sample PCAP file named `DNS-query-response.pcapng` which has been uploaded to LumiNUS. From the Wireshark's main menu, select "`File` → `Open`", and then select your downloaded file. The captured packet will be displayed in Wireshark's three panes.

You can select a packet of interest shown in Wireshark's ***Packet List*** pane, and then inspect this selected packet's details by clicking on its Frame 1, Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System in Wireshark's ***Packet Details pane***. Explore the packets, and answer these queries:

- What is the IP address of the host that issued a DNS query?
- What is the IP address of the contacted DNS server?
- What domain name was tried to be resolved?
- What is the IP address of the enquired domain name?

Task 2: Using Nmap to Inspect Open Ports of a Host

In our lecture, we have also discussed **Nmap (Network Mapper)**, and you have seen its demo. Now, it is time for you to try using Nmap.

Note that, as per NUS's Accepted Use Policy (AUP) which you've signed, you ***must not*** run a port mapper like Nmap on our University's network! Hence, you can run it on **your *own home network***, and do **scan *your own machine*** only.

On your Ubuntu machine, install Nmap by running:

```
$ sudo apt-get install nmap
```

Then, verify your installation by running Nmap to show its version:

```
$ nmap --version
```

To have your Ubuntu run a network service, you can install Apache web server by invoking the following command:

```
$ sudo apt install apache2
```

Then, start the Apache's web-server service (if it has not been started) by running:

```
$ sudo systemcl start apache2
```

Now, run Nmap to find out the **open ports** on your Ubuntu machine as follows:

```
$ nmap localhost
```

You should see that port 80 (HTTP) is open on your machine. Note that port 443 (HTTPS) is *not* open by default by Apache, since you will need to first obtain a certificate for the server as described in our Self-Exploration Activity 6, and then install and configure your issued certificate on Apache as described in: https://www.digicert.com/kb/csr-ssl-installation/ubuntu-server-with-apache2-openssl.htm, https://httpd.apache.org/docs/current/ssl/ssl_howto.html.

To additionally ask Nmap to perform a (server) **version detection**, do run:

```
$ nmap -sV localhost
```

Lastly, you can ask Nmap to identify **the OS** of your machine by running:

```
$ nmap -O localhost
```