COMPSCI 314 S2C Assignment 1

Department of Computer Science
The University of Auckland

Due: 11:59 p.m., Friday, 20 August, 2010
(NO LATE SUBMISSIONS)

Carefully review the tutorial document before starting the assignment. This assignment contributes to 5% of your overall course mark. Submit your assignment in ***PDF*** *format to* ***Assignment Drop Box****. Include all* ***workings*** *and* ***explanations****.* You must also carry out experiments using *windump*/*Wireshark* and include your results, e.g., output screen-shots. *Marks will be deducted for ambiguous solutions. Zero marks are awarded if the answers contain no explanation. Also, refer to the Departmental Policy on Cheating on Assignments.*

It is recommended that you perform the work in one of the Computer Science labs. Some people may prefer to install Wireshark on their own computer and work at home, but the results may be different and we cannot help if you have problems.

Assignment Drop Box *(https://adb.ec.auckland.ac.nz/adb/).*
Departmental Policy on Cheating on Assignments
*(*http://www.cs.auckland.ac.nz/administration/policies/CheatingPolicy.php*)*

[Total: 50 marks]

Q1. Packet capturing [10 marks]

a) Go to **Capture Options** in Wireshark and briefly explain ***Capture Packets in promiscuous mode*** option. Why aren't you able to capture packets which are destined to other computers in the lab even if you enable this option?
b) In **Edit** menu, explain functionality of ***Set Time Reference*** item.
c) What is the difference between ***display filter*** and ***capture filter***?
d) In **Analyze** menu, explain functionality of ***Follow TCP Stream*** item**.**

Q2. DNS packet observation [10 marks]

You need to use the web browser to visit a HTTP web page, e.g., www.altavista.com. Capture the full packets that are travelling between you and the web page. You only need to visit once to capture all the packets. Make sure to avoid HTTP status code *304*; this is most likely to happen if you are refreshing the web page. You should save the captured packets to files so as to analyze them later.

a) What filter string would you use to filter out ***DNS query*** packets? Note: If you don't see any DNS request packets for www.altavista.com in the trace, try other web sites until you do and then use the address of that web site in sections (b) and (d) instead of www.altavista.com.

b) How many DNS query packets for www.altavista.com have you observed? Explain why, if you have observed more than one.
c) What are the IP address and Ethernet address of DNS? Explain how you could find them.
d) Browse another web site (e.g. www.yahoo.com). Then try to browse www.altavista.com again and capture the packets. How many DNS queries for www.altavista.com have you observed this time? Explain why, if different from last time.

Q3. ICMP packet observation [15 marks]

a) tracert is a utility which helps network users to find the routing path between two hosts in the Internet. Run the following command and capture traveling packets. Look into the packets and try to explain how this utility works.
Windows: tracert google.ca Linux: traceroute google.ca
b) Run the following command and capture the packets. Is there any ICMP echo request for this address among the captured packets? If not, explain why.
Ping 127.0.0.1
c) Ping two different web sites (e.g. mail.yahoo.com and www.google.com) and capture ICMP echo request packets. Why are the destination Ethernet addresses the same in request packets while destination IP addresses are different?
d) Next, ping www.auckland.ac.nz and then www.cs.auckland.ac.nz, capturing ICMP echo request packets. What differences do you see in the captured packets? (Note: this particular test should certainly be made in the CS labs.)

Q4. Packet trace file [15 marks]

Download **test.pcap** from the 314 webpage Assignment section and open it by Wireshark and answer the following questions:

a) Is there any fragmented packet in the trace file? Explain how you investigated this.
b) What are the minimum and maximum packet sizes?
c) A file named ***2-important-dates.pdf*** (380 KB) has been download from a web site. Look into the captured packets and calculate the file download speed (payload Byte/s)? Explain how you calculated that. (hint: filter out HTTP GET packets and look for the file name in **Info** column to find the start of download and http response code 200 shows the end of download).
d) There are some packets which have been detected by Wireshark as SMB packets. SMB is the native network file sharing protocol in Microsoft Windows environments. Choose a response packet to QUERY_PATH_INFO at random. QUERY_PATH_INFO command is used by the client to retrieve attributes of a specified file which is resided on the server. How many protocols do you observe in the packet? List protocol names and header sizes. What percentage of the total packet is useful data? Don't forget to illustrate your answer with a screen shot.
e) What TCP ports have been used by HTTP server/client and SMB server/client?

End of Assignment-1