Assignment 2

The aim of this assignment is to make you familiar with a basic TCP/IP packet capturing (sniffing) tool called *tcpdump*.

Read the man pages of tcpdump thoroughly to understand the different options/filters and work out the following laboratory experiments. Prepare a report to give a summary of your findings:

(a) Check the version of the tcpdump and the libpcap utilities. Also find the number of interfaces available with your computer. Switch the network of eth0/eth1 (or the ethernet interface name as appeared) to promiscuous mode.

(b) Write the tcpdump command to capture 20 packets by listening to the promiscuous mode interface of your host and save the result as *.pcap file (both with and without -n option).

(c) Read the above file and identify the different fields present in TCP/IP packets captured by tcpdump.

(d) Extract packet arrival time, source IP address, destination IP address and port.

(e) Extract source MAC address and destination MAC addresses.

(f) Get the inter-arrival times while capturing packets.

(g) Use tcpdump to capture HTTP/HTTPS request and reply from www.google.com. Also print the packet content in ASCII format.

(h) For each command below, use tcpdump to capture the associated packets, and explain the different fields of each request and reply: (i) ping (ii) wget (iii) traceroute.

(i) Write the tcpdump command that captures packets containing TCP packets with a specific IP address as (i) both source and destination, (ii) only source, and (iii) only destination.

(j) Write the tcpdump command that captures packets containing ICMP packets between two hosts with different IP addresses.

(k) Write the tcpdump command to capture packets containing SSH request and reply between two specific IP addresses (hint: use port number 22 for SSH)