**CS6500 - Network Security**

**Tutorial 1 - Packet Sniffing**

Sniffer programs can be easily written using the pcap library. With pcap , the task of sniffers becomes invoking a simple sequence of procedures in the pcap library. At the end of the sequence, packets will be put in buffer for further processing as soon as they are captured. All the details of packet capturing are handled by the pcap library. You are provided with the sample sniffer program named “Sniffex.c” and you are supposed to do the following tasks :

**You should provide screendump evidence in the lab report to show that your program runs successfully and produces expected results.**

1. **Understanding sniffex.c :**
2. You should understand the given program and explain in your own words the sequence of library calls that are essential for the sniffer program. A short summary is expected and not a detailed explanation is required.
3. Why do you need the root privilege to run sniffex ? Where does the program fail if executed without the root privilege?
4. Please turn on and turn off the promiscuous mode in the sniffer program. Can you demonstrate the difference when this mode is on and off? Please describe how you demonstrate this.
5. **Writing Filters :**
6. Please write filter expressions for your sniffer program to capture each of the followings. In your lab reports, you need to include screen dumps to show the results of applying each of these filters.

* Capture the ICMP packets between two specific hosts.
* Capture the TCP packets that have a destination port range from to port 10 - 100

1. **Sniffing Passwords :**

Hello Ms. Sehmat,

Mr. X is a minister working for the government organization of our hostile neighboring country. He will be visiting your house for a discussion with the high-ranking officials in your house - specifically, your father-in-law. It is widely speculated that the minister uses the insecure telnet protocol for communication. Use your terminal to tap into the network traffic and figure out his password. There is just one complication: several low-ranking officials will be attending this meeting !!

[Background: Sehmat is a spy in the hostile neighboring country]