CENG489 HW3-C: A Simple Packet Sniffer

1 Overview

Packet sniffing is an important concept in network security; it is a major threat in network communication. Being able to understand this threat is essential for understanding security measures in networking. There are many packet sniffing tools, such as `Wireshark`, `Tcpdump`, `Netwox`, etc. Some of these tools are widely used by security experts, as well as by attackers. Being able to use these tools is important, but what is more important is to understand how these tools work, i.e., how packet sniffing is implemented in software. The objective of this assignment is to master the technologies underlying most of the sniffing tools.

2 Tasks

2.1 Task 1: Writing a Packet Sniffing Program

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. Tim Carstens has written a tutorial on how to use the `pcap` library to write a sniffer program. The tutorial is available at `http://www.tcpdump.org/pcap.htm`.

Please write a packet sniffer program that prints out the source and destination IP addresses of each captured packet. You can check out sniffex.c in the linked tutorial to understand how to write a packet sniffer.

2.2 Task 2: Writing Filters.

Please write filter expressions for your sniffer program to capture each of the followings.

- Capture the ICMP packets between two specific hosts (i.e. given IP addresses).
- Capture the TCP packets that have a destination port range from 10 to 100.

2.3 Task 3: Sniffing Passwords.

Please show how you can use your sniffer to capture the password when somebody is using `telnet` on the network that you are monitoring. You may need to modify your sniffer code to print out the data part of a captured TCP packet (telnet uses TCP). You also need to start the `telnetd` server on your VM. If

you are using the pre-built VM, the `telnetd` server is already installed; just type the following command to start it.

```
% sudo service openbsd-inetd start
```