CS392/CS682 Lab 2
Understanding Packet Sniffing

Introduction:

A packet sniffer is one of the fundamental tools used for analyzing attacks, diagnosing network problems, and identifying malicious entities in a network. A thorough understanding of a sniffer is a must for any network security specialist.

In this assignment you are given the opportunity to understand how a packet sniffer works; you will also be writing a part of the sniffer that decodes the payload.

Part I: Understanding minisniff:

Study the source code of minisniff, available at http://isis.poly.edu/kulesh/skunk/src/, a raw packet sniffer. The source code is well documented and has enough explanation to walk you through each step of the sniffing process. Your task for this part is to understand minisniff completely and answer the following questions:

1) What library does minisniff use to capture packets? Where in the web can you find more information about this library?
2) Do some research and describe the advantages/disadvantage of using this library? Do not blindly copy and past material from the web. Try to understand the material you find and write what you understood.
3) Are there any alternative libraries available to capture packets? (Open source only)
4) Explain the purpose of the following functions:
    a. *pcap_lookupdev*
    b. *pcap_open_live*
    c. *pcap_lookupnet*
    d. *pcap_compile*
    e. *pcap_setfilter*
    f. *pcap_next*
    g. *pcap_loop*
    h. *pcap_dispatch*
5) Can this library be used to develop an active network fingerprinting tool? Explain.
6) There are five layers in the TCP/IP stack (application, transport, network, link, and physical). Up to what layer can minisniff decode data from the captured packets? Justify your answer using the code.

Part II: Extending minisniff

In this part you will extend minisniff's capabilities:

1) In assignment 0 you explored how to write a small client server program. For this part modify minisniff to capture, decode, and display data from a session of your client server program.
2) Now modify minisniff to capture, decode and display the password from a telnet session.