2.1.a Writing a Packet Sniffing Program

Problem 1

`pcap_lookupdev()` looks up the interface that is being used on the device.

`pcap_open_live()` used for creating a sniffing session

`pcap_datalink()` returns a value indicating the type of link-layer header the device uses

`pcap_compile()` compiles the filter that we will use for sniffing

`pcap_setfilter()` sets the filter for the sniffing session

`pcap_next()` returns a u_char pointer to the packet described by the filter

`pcap_loop()` returns a sniffed packet until it reaches the count of packets wanted by the attacker

Problem 2

You need root privileges to enable promiscuous mode so the host won't know that the attacker is sniffing all traffic on the wire. Having root privileges will allow the attacker to hide that they enabled promiscuous mode.

2.1.b Sniffing Passwords

The sniffer program sniffed out the payload information which was the password. I had to adjust the filter expression and I set the device on the command line.

2.2 Spoofing

Question 4

If the packet length is less than the IP header length, the packet will not send and instead an error is broadcasted that the packet was a bogus length. Basically, as long as the packet length is as large as the IP header length, you can send the packet no matter how big the payload.

Question 5

You do have to calculate the checksum when using C raw socket programming. Scapy calculates the checksum for you.

Question 6

Raw sockets can spoof custom packets that can interfere with incoming traffic which can be bad. Furthermore, root privilege let you break networking rules set in place. The program fails when it tries to create a raw socket for custom packets.