CIS/CSE644: quizz1a student name: **Evan Smith**

1(10): How to get the address in C language? such as how to get address from normal integer variable?

Int i =10;

Address of i= **&i**

If you want to use a pointer to hold the value of this address, now first try to declare a pointer(what type?) and use it to save the address of i. Then print out the value of (int i ) using this pointer you just declared. (do not need a compiling code, just the major lines.

**int\* i\_ptr = &i;**

**println(i\_ptr);**

2:(10) what does “ (int\*) &a “ mean: ( “a” can be any type except integer type).

**This is casting the pointer to the location of a into a pointer to an integer. This is possible because both sides are simply addresses, we just tell the system what information to expect at that location.**

3: (10)

char **buffer**[LENGTH];

struct ipheader \***ip** = (struct ipheader \*) buffer;

struct udpheader \***udp** = (struct udpheader \*) (buffer + sizeof(struct ipheader);

Char \***data** = buffer + sizeof(struct ipheader) + sizeof(struct udpheader);

explain above code, what they are doing? also what is type casting in C language?

**Here this code is parsing a packet into its component parts, the ip and udp headers as well as the data payload. Type casting in C is essentially telling the system how much memory to look in for the variable, given a starting location (for reference variables).**

3b(5): what is the return of sizeof(); in what unit?

**The return is the number of bytes that the type uses.**

4:(10) steps you need to think about in order to write sniffer? reasons for each step.(briefly)

**Creating a raw socket – passes the full packet including headers, which is useful for snoofing**

**Choosing a protocol – determines which types of packets we want to receive, and later use that decision to help parse the incoming packets.**

**Enable promiscuous mode – allows the network card to gather information from all packets, not just those that are explicitly addressed to your machine.**

**Looped wait statement to receive packets – want to be able to sample packets that are sent on the network.**

4b:(10) what is promiscuous mode? What is normal mode? How do these two modes make difference in sniff tool? What is necessary for sniffing and why?

**Promiscuous mode is when a net card saves all received packets into memory, whereas normal mode is where the card checks each packet to see if the destination header matches that device’s MAC, and only saves the payload to memory if they match. For sniffing, we must use promiscuous mode, because the goal is to gather information that was not necessarily intended to be read by us.**

5:(10) what is raw socket? Why Prof. Du spend time talking about raw socket? What is special about raw socket?

**A raw socket is one that is able to bypass operating system-driven edits to the packets. This allows us to inject spoofed source IP headers that will conceal true identities, and indeed can add any arbitrary values into the headers.**

5b(5): what is critical in the function: send\_raw\_ip\_packet()? (without it, the packet will not be sent), and explain the reason?

**You must provide the pointer to the actual buffer information that should be sent via the raw socket. The function itself still takes care of the checksum, which must be filled out to be sent. The checksum is used to confirm that the received information matches the sent packet.**

6:(10) relationship between raw socket programming and pcap library programming? Why do we need the root privilege to run?

**Raw socket programming allows us to control almost all components of the packet (barring the checksum, which is pure computation), while using the pcap library means that the operating system will automatically fill in the source IP address, which makes it impossible to conceal your identity when spoofing. We must do this with root privilege because only the root user is able to actually create and use raw sockets.**