Quiz0 student name: Kevin Martin

1: (10) list major attacks through Internet and try to analyze about what could be the reasons for the possibilities of these attacks.

Sniffing: as long as an attacker is connected to one of the links that a packet must go through from the original destination to the server. An attacker may use this to observe (steal) the data in a packet.

Injection/spoofing: an attacker may inject their own data into the network. Similar to sniffing, but instead of just passive observation this is active.

Man in the middle: attacker is one of the “middlemen” that a packet must go through on its way to the server. Here the malicious attacker can manipulate the packet.

Denial of Service (DoS): done to bring down a server (generally a major one). This can cost the company who owns the server large amounts of actual money.

2:(20) Describe the packet flow through the Internet in high level picture. What is major function of each connection? how does Network data travel through Internet in detail layers? explain what is in each layer, what's it's function?

First, the application on the local computer generates the data. This is the data that needs to be sent to the final destination (in this case, a remote server). Next the data is transmitted from the local machine onto the network via the Network Interface Card (NIC), which is a physical piece of hardware inside the local machine. The Datalink layer will then help the data reach the local router. After that, the data reaches the router, which will actually send the data to more routers, before reaching the internet. From there, the data continues to be routed through remote serves, until it reaches the router of the destination server. Again, the data is placed back onto the network, and consumed by the server via its own NIC. Finally, a daemon program awaits the data and sends it to the server’s application.

3: (15) what is Datalink layer? What is it’s function (Datalink layer)? What is MAC address? how many bytes can it have ? write an example of Broadcast address for data link layer. In iphone, what is the privacy issue related to the MAC address and why it is an issue? how it is solved

The Datalink layer is the part of the transfer process that sends data from the host computer to the router. Its main function is to send data between two computers that are physically connected. The MAC address is the hardware address that is unique to each NIC card. It can

have 6 bytes.

The broadcast address tells each computer that is connected to the same ethernet whether or not the package is for it (via its NIC card). An example of a broadcast address is FF:FF:FF:FF:FF:FF (which sets the address to all 1's). In this example, all the computers on that ethernet would pick u pand process that data. A real example would be 08:00:27:cf:eb:bd.

The privacy issue related to the MAC address on an iPhone was that every time an iPhone was near a WiFi point, the iPhone would broadcast its own MAC address without the user's consent. To fix this, iPhone began (after iOS 8) to use a software-generated (random) MAC address to simply interface with the WiFi point. If the user actually does want to connect, they can switch to the physical MAC address.

4:(20) what is IP address? what is difference between IP v4 and IP v6? which version are we using in this class? why do we need IP address? how does computer recognize ip address? use an example to describe how IP address works, in a bits wise. How do you know how many hosts you can have? Also how do you know how many net you can have and the reasons? Which part of the ip address the router is looking at and why ?

The IP Address is the scheme in which to identify each device connected to the internet. IP v4 and IP v6 differ in how they are constructed. IP v4 is older and only allowed for 32 bit identification numbers. This meant that only 2^{32} devices could be uniquely identified, which is certainly too small. IP v6 uses a different mechanism which allows for a far greater number of devices. We will be using IP v4 as it is the one most commonly used. We need an IP address to identify each and every device connected to a computer. A computer recognizes the IP address in a three step process: first by idetnfiying the class (class A – E on IP v4), then by idetnfiying the netid (organization/building/etc), and finally the hostid (actual machine). For example, in a class A IP Adress, the first bit will be a zero indicating A. The next 7 bits will be the netid, while the final 24 bits indicate the hostid. You can know the maximum number of hosts by checking which class the address is, which determines the number of bits receserved for the hostid. Then you simply raise 2 to that power. The same is true for the netid: determine the class, look up how many bits are reserved for it, and raise 2 to that power. The router is looking at the netid, because that's how routing was formatted. When a packet comes in, the router will need to quickly split the IP address and determine the netid.

5(20): what is ARP? which layer does it belong to? why do we need ARP?

ARP is the address resolution protocol, and it belongs in Layer 2. We need it to transfer the IP address into the hardware address (from IP ↔ MAC).

6:(15) write a C program to use pointer movement to print an integer byte by byte. Need to be able to compile and print out the bytes.

```
#include <stdio.h>
int main()
{
    int input = 2;
    unsigned char* ptr = (unsigned char*)&input;
    int k = 0;
    while (k < sizeof(input)){
        printf("%x\n", ptr[k]);
        k++;
    }
    return 0;
}
```