**CEG4430/6430 Homework 1**

(40 Points)

1. One student has designed a new transport-layer protocol, NTLP, that is completely different from the TCP or UDP. He then creates a packet that has a physical-layer header, a data-link-layer header, and an IP header. This packet contains the NTLP header and the application data payload. The packet is sent to the destination IP address as indicated in the IP header. Will this packet be delivered to the destination IP address indicated in the IP header? Please justify your answer. (5 Points)

Answer Question 1:

Because this protocol is created completely different from the normal TCP and UDP protocols, I do not believe that this protocol will be able to send any packets at all to any designated IP address. In addition to this, according to the Textbook regarding the Transport Layer. The TCP protocol’s purpose is to establish connection with the client and server to allow packets to be sent out and delivered. Now if this new Protocol by-pasted the normal way that TCP and UDP worked and would transfer packets directly through IP Addresses, then I could see this new protocol being able to send the packets to the intended IP address based on the IP header.

1. Please determinate the correctness of the following statements and justify your answers (preferably by examples). (5 Points)
   1. HTTP services have to be offered at port 80.

Answer Question 2a: HTTP is defaulted to offer services at port 80. A reference to this can be fund in the class textbook, Chapter 5 Section 4, page 249 in the second paragraph.

* 1. DNS services are usually offered at port 53 through UDP.

Answer Question 2b: DNS offers its services only from port 53 and no other port. But DNS offers services for not only UDP but also TCP as well.

* 1. An attacker has to use existing transport-layer protocols to make sure the packets are routed through the Internet.

Answer Question 2c: An attacker does not have to know the existing transport-layer protocols because TCP is part of the backbone of internet connection. But in addition, an attacker can connect to the internet without the use of TCP protocol at all. An example of this would be by connecting from IP addresses directly and ignoring TCP all together and this will still accomplish the same task.

* 1. If an attacker uses UDP as the transport-layer protocol, he cannot implement reliable, connection-oriented networking service.

Answer Question 2d: Because UDP is not as secure as TCP, the use of UDP is for fast connection and communication but the connection and transmission of information is not always good. As packets and information can be sent out of order as data ordering and data integrity are not very important as speed is with UDP transport-layer protocol connections. But to get around this an example could be where an Attacker uses UDP for fast tavel and packet sending and then adding on his or her own additional code to give it properties to keep packet order and reliability working more dependably.

1. Three students, A, B, and C, share an apartment. A, B, and C have been assigned 3 IP addresses, respectively. However, there is only one Ethernet cable outlet in the apartment. Therefore, they decide to buy a device to connect three computers to the outlet. (10 Points)
   1. They have decided to buy a hub. If A wants to eavesdrop packets B sends to C, what should A do?

Answer Question 3a: When using a hub, any data sent out is sent out to all users that are connected to the hub. So as long as A is connected to the hub while B and C are online and communicating, A will easily be able to view the information being sent back and forth between B and C by sampling using a tool such as Wireshark to view the packets sent back and forth by spoofing the packets that are being sent between B and C.

* 1. They have decided to buy a switch. What should A do now if he wants to eavesdrop packets sent from B to C?

Answer Question 3b: If the three letters choose to get a switch instead of a hub, the data and frames are only going to be sent between B and C. Since a switch will learn the different IP addresses, and know each person by there IP. For A to be able to see any of the conversation of B and C, A will have to use a technique called Port Mirroring. This technique has the port A uses to mirror the port of B for example and then any communication that is sent from C and is heading to B will also be sent to A as well since his port now mirrors that of B.

1. As we discussed in our lectures, a client can send a DNS request to a recursive DNS server. Then the DNS server will finally issue a DNS request to the authoritative DNS server. An attacker can send fake DNS responses, aiming at poisoning the cache of the target DNS server.
   1. Suppose the source port of the DNS request from the recursive DNS server and the ID field of the request are completely random. What is the probability for the attacker to succeed if the attacker only sends out one fake DNS response whose destination port and ID are randomly selected? (5 Points)

Answer Question 4a: With this specific scenario in mind if this all is taken into account and the birthday paradox is applied to find a percentage on how likely the attacker is to succeed. If the attacker tries one single attempt when the destination port and ID are randomly selected, the percentage rate comes out to be: (1 – n/(2^16)). This is also dealing with the attacker using a DNS Cache Poisoning attack during this attempt. If the attacker is not using this specific method example as shown in the textbook, a general probability of attack success as stated would be as follows: n/(2^32). n = number of attempts.

* 1. It seems that a client can simultaneously issue many DNS requests (say *M* requests) for the same domain (e.g., cash.foo.com) to the recursive DNS server. Then the recursive DNS server will issue *M* DNS requests to the same authoritative DNS server, despite the fact that these requests look for the same domain. The source port and the ID field of these *M* DNS requests (from the recursive DNS server) will be randomly generated by the DNS server. Does this recursive DNS server facilitate the poisoning attack? Please justify your answer by quantifying the probability of success by an attacker and then comparing your result with the answer to question a. (5 Points)

Answer Question 4b: With this new scenario in mind, since there are multiple requests being sent out altogether if the attacker follows the same process then the process would be a similar attack and if the attacker tries for multiple attempts to match the correct IP address and ID, if the attacker is using the birthday paradox method as described in the textbook then the probability would come out as follows: (1-M/(2^16))^M. and M is the number of multiple attack attempts. If the attacker is not using the birthday paradox then I believe that the probability for attack would be as follows: M (the number of attempts) / 2^32. In relation to part a of question 4. The chances of success for an attacker increase as the attacker tries more than a single attempt to attack with a fake DNS IP address and ID.

1. Please read “The Collateral Damage of Internet Censorship by DNS Injection” and answer the following questions.

Link of the Article after searching the title given above: <https://conferences.sigcomm.org/sigcomm/2012/paper/ccr-paper266.pdf>

* 1. How do the collateral damages occur? (5 Points)

Answer Question 5a: Collateral damage is occurred when a DNS query from a recursive resolver enters a censored network, causing the censorship mechanism to react. As stated from the reading of the paper we are instructed to read for the assignment.

* 1. As a DNS request can traverse a number of routers along a path, and each router along the path can inject fake DNS responses. What are the techniques used by the researchers of the paper to identify the router(s) that actually inject fake DNS responses? (5 Points)

Answer Question 5b: From reading the article I have found that in order to find the poisoned DNS injectors, there are two queries being used. The HoneyQuery Probs for non-responsive IPs and any responses were most likely from DNS infections. They were then broken down into different lists to organize what was specifically a DNS injection, what was damaged from the censorship, and finally anything that was part of the response. From here, TraceQueries were used to take these lists and track down the IPs and find exactly where the DNS injections are coming from to remove them and make them extinct from the network.