Review Question 7.9: *Define a reflection attack.*

The reflection attack is when the attacker sends malicious packages, like a network packet, with spoofed source addresses to service runs on the network server, then the network server responds back to this packet by sending it to the spoofed address that belongs to authentic attack target. The attacker can send several packets with spoofed source address to several servers, causing a flood because there will be several responses that will devastate the target's network link.

Review Question 7.10: *Define an amplification attack.*

This attack is used to transmit a packet with spoofed source addresses to the target system through mediators. This mediators generate MULTIPLE responses after they were transmitted. Therefore, a HUGE number of responses are created for each original packet sent. The attacker can accomplish this by broadcasting the address of the network to respond.

Problem 7.2: *Using a TCP SYN spoofing attack, the attacker aims to flood the table of TCP connection requests on a system so that it is unable to respond to legitimate connection requests. Consider a server system with a table for 256 connection requests. This system will retry sending the SYN-ACK packet five times when it fails to receive an ACK packet in response, at 30 second intervals, before purging the request from its table. Assume no additional countermeasures are used against this attack and the attacker has filled this table with an initial flood of connection requests. At what rate must the attacker continue to send TCP connection requests to this system in order to ensure that the table remains full? Assuming the TCP SYN packet is 40 bytes in size (ignoring framing overhead), how much bandwidth does the attacker consume to continue this attack?*

RATE - first we need to calculate the number of SYN packets = initial + 5 = 6.

Then to calculate the rate we multiply it by the number of seconds = 6*30seconds = 180 seconds which is 3 minutes.
Then 256/3 = 85.3333, therefore = 86 connection request per minute.

BANDWIDTH - 86 * 40 * 8 = 27,520 which needs to be divided by 60 seconds = 458.88 bits per second

Problem 7.3: *Consider a distributed variant of the attack we explore in Problem 7.1. Assume the attacker has compromised a number of broadband-connected residential PCs to use as zombie systems. Also assume each such system has an average uplink capacity of 128 Kbps. What is the maximum number of 500-byte ICMP echo request (ping) packets a single zombie PC can send per second? How many such zombie systems would the attacker need to flood a target organization using a 0.5-Mbps link? A 2-Mbps link? Or a 10-Mbps link? Given reports of botnets composed of many thousands of zombie*

systems, what can you conclude about their controller?s ability to launch DDoS attacks on multiple such organizations simultaneously? Or on a major organization with multiple, much larger network links than we have considered in these problems?

The max number of packets a zombie could send is $128 * 10^3$ / $500 * 8 = 32$

To flood the system we would need $0.5 * 10^6$ / $128 * 10^3 = 3.906$ which is 4 zombies.

The zombies required to flood a target using 2Mbps is $2 * 10^6$ / $128 * 10^3 = 15.625$ which means 16 zombies are required.

Using a 10Mbps $10 * 10^6$ / $128 * 10^3 = 78.125$ which means 78 or 79 (to be more sure) zombies would be required.

We can conclude that DDos attack has the ability to flood any company using bandwidth links and network link capacity of these sizes just by using botnets with thousand of zombies. But for larger than that, it would be more "expensive" to have a successful DDos attack.

Problem 7.4: *In order to implement a DNS amplification attack, the attacker must trigger the creation of a sufficiently large volume of DNS response packets from the intermediary to extend the capacity of the link to the target organization. Consider an attack where the DNS response packets are 500 bytes in size (ignoring framing overhead). How many of these packets per second must the attacker trigger to flood a target organization using a 0.5-Mbps link? A 2-Mbps link? Or a 10-Mbps link? If the DNS request packet to the intermediary is 60 bytes in size, how much bandwidth does the attacker consume to send the necessary rate of DNS request packets for each of these three cases?*

For an organization using 0.5Mbps then $0.5 * 10^6$ / $500 * 8 = 125$, which means 125 packets need to be sent per second.

For an organization with 2Mbps $2 * 10^6$ / $500 * 8 = 500$, therefore 500 packets need to be sent per second.

Lastly for a 10Mbps $10 * 10^6$ / $500 * 8 = 2500$, so 2500 packets need to be sent per second.

Necessary BANDWIDTH for each:
For the .5Mbps = 125 * 60 * 8 = 60000 = 60Kbps
For the 2Mbps = 500 * 60 * 8 = 240,000 = 240Kbps
For the 10Mbps = 2500 * 60 * 8 = 1,200,000 = 1.2Mbps