1. **Review Question 7.9** Define a reflection attack.

   A relfection attack is where an attacker sends packets with a spoofed source address to a service running on a network server. The server will respond to the packet sending it to the spoofed source address (which is the actual target). Since the server is just responding to the packets, it is known as the reflector.

2. **Review Question 7.10** Define an amplification attack.

   A variant of reflector attack but differs by generating multiple response packets for each original packet sent. This is achieved by directing the original request to the boradcast address for some network. As a result, all host on that network could potentially respond to the request which would create a flood of responses.

3. **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?

   On a system that will retry 5 times at 30 seconds per request, each of the 256 connections will live in the table for (initial 30s + (5 * 30s)) = 3 minutes. To keep the table full, the attacker will have to send 256 / 3 = about 86 TCP connection requests per minute. The bandwidth = 86 * 40 * 8 / 60 = 459 bits per second.

4. **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?

Answer

5. **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?

   Answer

6. **Question Not in the Book:**Consider the SNORT rule:

```
alert tcp $HOME_NET any <> $EXTERNAL_NET 6666:7000
(msg:"CHAT IRC message"; flow:established;
content:"PRIVMSG "; nocase; classtype:policy-violation;
sid:1463; rev:6;)
```

   Explain what the snort rule does by answering:

   (a) What type of connections would the rule apply to?

   (b) What type of traffic is being monitored?

(c) Is there any additional requirement on the traffic?

Answer

7. **Review Question 8.4** Describe the three logical components of an IDS.

   Answer

8. **Review Question 8.8** Explain the base-rate fallacy.

   Answer

9. **Review Question 8.2** In the context of an IDS, we define a false positive to be an alarm generated by an IDS in which the IDS alerts to a condition that is actually benign. A false negative occurs when an IDS fails to generate an alarm when an alert-worthy condition is in effect. Using the following diagram, depict two curves that roughly indicate false positives and false negatives, respectively:

   Answer

10. **Review Question 8.4** One of the non-payload options in Snort is flow. This option distinguishes between clients and servers. This option can be used to specify a match only for packets flowing in one direction (client to server or visa-versa) and can specify a match only on established TCP connections. Consider the following Snort rule:

```
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS $ORACLE_PORTS\
(msg: ‘‘ORACLE create database attempt:;\
flow: to_server, established; content: ‘‘create database";
nocase;\
classtype: protocol-command-decode;)
```

(a) What does this rule do?

Answer

(b) Comment on the significance of this rule if the Snort devices is placed inside or outside of the external firewall.

Answer