Patrick Austin

12/7/2017

CS 450 Homework 4

1. To flood a 0.5 Mbps link with 500 byte packets, (.5 x 106) / (500 x 8) = 500,000 / 4000 = 125 packets per second must be sent. To request 125 packets per second from the intermediary, where each request is 60 bytes long, the attacker needs a bandwidth of 125 \* 60 \* 8 = 60,000 bits per second = 60Kbps.

Likewise, to flood a 2 Mbps link, (2 x 106) / (500 x 8) = 2,000,000 / 4000 = 500 packets per second must be sent. To request 500 packets per second from the intermediary, the attacker needs a bandwidth of 500 \* 60 \* 8 = 240,000 bits per second = 240 Kbps.

Likewise, to flood a 10 Mbps link, (10 x 106) / (500 x 8) = 10,000,000 / 4000 = 2500 packets per second must be sent. To request 2500 packets per second from the intermediary, the attacker needs a bandwidth of 2500 \* 60 \* 8 = 1,200,000 bits per second = 1.2 Mbps.

2. There are 16 combinations of threat levels given 2 nodes with 4 possible values where repetition is allowed. To find probability of threat level medium given one node generates P3, we want P(1P3,1P4|1P3). Note order does not matter in this scenario, so P(1P3,1P4) = P(1P4,1P3).

Since P(A|B) = P(A,B) / P(B), P(1P3,1P4|1P3) = P(1P3,1P4) / P(1P3).

P(1P3,1P4) = 2/16, since there are 2/16 cases where P3 and P4 are selected.

P(1P3) = 7/16, since there are 7/16 cases where at least one value selected is P3.

Therefore the probability is (2/16) / (7/16) = 2/7.

3. a. The first rule has the effect of allowing inbound SMTP traffic from an external source to the TCP server via port 25. In other words, the TCP server can receive incoming email from outside.

The second rule has the effect of allowing outbound SMTP traffic from the TCP server to an external destination via a port > 1023. In other words, the outside can receive incoming email from the TCP server.

The third rule has the effect of allowing outbound SMTP traffic from the TCP server to an external destination via port 25. In other words, the outside can transmit email to the TCP server.

The fourth rule has the effect of allowing inbound SMTP traffic from an external source to the TCP server via a port > 1023. In other words, the TCP server can transmit email to the outside.

The fifth rule has the effect of blocking all traffic whatsoever- whether inbound or outbound, no matter the address or protocol or port, the communication is blocked.

B. The first packet is allowed because it matches rule A.

The second packet is allowed because it matches rule B.

The third packet is allowed because it matches rule C.

The fourth packet is allowed because it matches rule D.