Yuvika Nibber

Assignment 4

1. Denial of service (DoS) is an attack where the machine or the source of network is made unavailable for the user. It floods the network with traffic which makes browsing websites slower and sometimes unavailable.

Distributed denial of service (DDoS) is an attack where the source of the attack switched IP addresses. It has more than a thousand IP address. DDoS comes from different origins which makes the IP address bounce to several locations.

1. It limits the system to send the packets with caricatured IP addresses. The ISP keeps a track of all the addresses that are allocated with the users and makes sure the valid addresses are used by the user.
2. Control hierarchy approach
3. Slash dotted and flash crowd are the traffic on the system. They stop the traffic requests that are from the users. The relationship between them is that they both restrict the extra bandwidths and scattered servers. They both usually restrict sporting websites.
4. Identify the type of attack-> capturing the packets that flow into the organization and then analyzing it-> design suitable filters to block the flow of attack packets->If a bug is created on the system and not the traffic then it is IDed and recovered using the corrective steps.
5. The ISP are asked to trace the flow of packets back. It is usually difficult and time consuming to trace the packets when the addresses are spoofed. The non-spoofed addressed are usually easy to identify.
6. Number of packets required per second = (Link capacity in bits per second) / (Packet size in bits)

500 Bytes = (500\*8) bits. 1 Mbps = (1\*10^6) bits per second

0.5 Mbps = (0.5\*10^6)/ (500\*8) = 125

2 Mbps = (2\*10^6)/ (500\*8) = 500

10 Mbps= (10\*10^6)/ (500\*8) = 2500

1. Max no. of packets sent by single zombie = (128\*10^3)/ (500\*8) = 32

Required no. of zombie system to flood the target using 0.5mbps = (0.5\*10^6)/ (128\*10^3) = 3.906 = 4.

Required for 2 mbps = (2\*10^6) / (128\*10^3) = 15.625 = 16

Required for 10 mbps = (10\*10^6) / (128\*10^3) = 78.125 = 79

1. Yes, the administrator will need to take the counter measures against DoS. Flash crowd and slash dotted are the types of attacks. The measures taken to reduce their impact when overloaded on the network is predicted. This is mostly done on sporting websites.
2. Required bandwidth for 0.5 Mbps link = 125\*60\*8 = 60\*10^3 = 60Kbps

2 Mbps= 500\*60\*8 = 240\*10^3 = 240 Kbps

10 Mbps = 2500\*60\*8 = 1.2 \*10^6 = 1.2 Mbps

Amplification of three data rates = 500/60 = 8.3 times.