SYED ASAD ZAMAN
p18-0034(B)
p180034@nu.edu.pk

1 SYN Flooding

In order to affect the activity of a server intruder using different types of attacks. In these types of attacks **SYN Flooding** is one of the popular attack. For this purpose the intruder attack the victim server, firewall or other defense system by sending the **SYN** packets at a very high rate that overwhelm the victim by consuming its resources to process these incoming packets. In most cases if a server is protected by a firewall, the firewall will become a victim of the SYN flood itself and begin to flush its state-table, knocking all good connections offline or even worse – reboot. Some firewalls in order to remain up and running, will begin to indiscriminately drop all good and bad traffic to the destination server being flooded. A **SYN-flood DDoS attack** (see the accompanying figure) takes advantage of the **TCP (Transmission Control Protocol)** three-way handshake process by flooding multiple TCP ports on the target system with **SYN (synchronize)** messages to initiate a connection between the source system and the target system.

1.1 HOW TO PROTECT?

The **SmartWall**(a real-time, line-rate, DDoS monitoring System) is capable of mitigating SYN FLOOD attacks all while maintaining full connectivity to avoid disrupting the delivery of legitimate traffic. It is designed to automatically handle floods in real-time.

2 Stream Control Transmission Protocol (SCTP)

TCP has performed immense service as the primary means of reliable data transfer in IP networks. However, an increasing number of recent applications have found TCP too limiting, and have incorporated their own reliable data transfer protocol on top of UDP. The limitations that users have wished to bypass include the following:
1. Lack of reliable transfer without sequence maintenance.
2. Stream-oriented nature of **TCP**.
3. TCP is relatively vulnerable to **denial-of-service attacks(DDoS)**, such as **SYN attacks**.

SCTP stands for Stream Control Transmission Protocol. It is a connection- oriented protocol in computer networks which provides a **full-duplex** association i.e., transmitting multiple streams of data between two end points at the same time that have established a connection in network.

2.1 Characteristics

1. **Unicast with Multiple properties**
2. **Reliable Transmission**
3. **Message Oriented**

2.2 Advantages

1. It is a full- duplex connection.
2. It allows half- closed connections.
3.The message's boundaries are maintained and application doesn't have to split messages.
4. It has properties of both TCP and UDP protocol.

3 TCP Timers

In order to handle the issue of excessive delays and timeout in communications. We use something called **TCP Timer**.

3.1 Types of Timers

1. **Retransmission Timer:**
To retransmit lost segments, TCP uses retransmission timeout (RTO). When TCP sends a segment the timer starts and stops when the acknowledgment is received.
2. **Persistent Timer**
To deal with a zero-window-size deadlock situation, TCP uses a persistence timer.When the sending TCP receives an acknowledgment with a window size of zero, it starts a persistence timer. When the persistence timer goes off, the sending TCP sends a special segment called a probe. This segment contains only 1 byte of new data. It has a sequence number, but its sequence number is never acknowledged; it is even ignored in calculating the sequence number for the rest of the data.
3. **Keep Alive Timer**
A keepalive timer is used to prevent a long idle connection between two TCPs. If a client opens a TCP connection to a server transfers some data and becomes silent the client will crash. In this case, the connection remains open forever. So a keepalive timer is used.
4. **Time Wait Timer**
This timer is used during tcp connection termination. The timer starts after sending the last Ack for 2nd FIN and closing the connection. After a TCP connection is closed, it is possible for datagrams that are still making their way through the network to attempt to access the closed port. The quiet timer is intended to prevent the just-closed port from reopening again quickly and receiving these last datagrams.