Name : Gangavarapu Abhinay Reddy

course : computer Networks for communication.

course code : CSA0735

Faculty : Dr. Rajaram
Dr. Anand

Regn no : 192525082

submitted by : G. Abhinay Reddy.

Regn no : 192525082.

Department : B. Tech AIML.

semester : Ist semester.

college : SIMATS Engineering

submitted To :

Dr. Rajaram , Dr. Anand

Assignment

unit - V

Scenario : A university server is targeted by a SYN flood attack

a) Descride how a Dos attack overwhelms systems.

A Denial of service (Dos) attack overwhelms a target system by flooding it with excessive requests, consuming its resources (CPU, memory, bandwidth). and making it unavailable to legitimate users. In a SYN flood attack, the attacker sends a large number of TCP SYN packets (used to initiate a connection). but never completes the 3-way handshake. This leaves the server with half-open connections, consuming memory and connection slots, ultimately preventing new legitimate connections

b) Calculate the packet rate needed to exhaust a 1 Gbps link.

Assumption : size of a TCP SYN packet ≈ 60 bytes = 480 bits (including headers)

- Link capacity = 1 Gbps = 1,000,000,000 bit/sec
- Packet size = 480 bits
- Packet rate = Total bits per second / Bits per packet.

Packet rate = $\frac{1000000000}{480} \approx$ 2,083,333 pacs/sec

Answer: Approximately 2.08 million SYN packets per second are needed to saturate a 1 Gbps link.

c) Propose detection techiques using threshold models.

Threshold-based detection involves setting predefined limits for normal network behavior. Some examples include.

-> SYN Rate Threshold: If SYN packets exceed a set rate (eg, 1000 SYN/sec from a single IP) raise an alert.

-> SYN to FIN/RST Ratio: Monitor the ratio of SYN packets to completed TCP sessions. A high SYN-to-FIN ratio indicates half-open connections

- Connection Table Monitoring: Alert when the number of half-open connections exceeds a threshold (e.g., 10000)

- Per-IP Thresholding: Detect unusual activity from specific IPs that exceed typical usage patterns.

d) suggest mitigation strategies include:

1. SYN cookies: server encodes connection state into the SYN-ACK packet and doesn't allocate resources until the handshake is completed.

2. Rate limiting: Throttle SYN requests from individual IPs or regions

3. Firewall Rules: Drop suspicious (or) Malformed SYN packets at the perimeter.

4. Intrusion Detection/Prevention systems (IDS/IPS): Monitor and block known SYN flood patterns.

5. Load Balancers and Reverse Proxies: Offload connection handling and absorb attack traffic.

6. Blacklisting: Block IPs with abnormal SYN rates.