Course: Computer Network for Communication
Cours code: CSA0735

faculty: Dr. Rajaram
Dr. Anand

Submitted by:

Name: MOHAMMAD ALEYAS

Reg no: 192521220

Department: B. Tech Information Technology

Semester: Ist

College: SIMATS

project 5

Submitted to:

Name: Dr. Rajaram
Dr. Anand

Depart of IT

SIMATS Engineering

Assignment 5

SYN flood Attack Analysis and Mitigation on financial Web portals.

Scenario:

A financial web portal experiences SYN flood attack during peak hours, severely affecting availability. The attacker generates 10,000 SYN packet per second on a 1Gbps link.

a) Explanation of SYN flooding and its Impact.

SYN flooding is a type of Denial of service (DOS) attack where an attacker sends a rapid Succession of Tcp SYN (Synchronization) requests to target system without completing the Tcp Three way handshake.

How it works:

- Normally, when a client initiates a Tcp Connection, it sends a SYN packet.
- The server responds with SYN-Ack.
- The client then replies with an Ack, Completing the handshake.
- In SYN flooding, the attacker never sends the final Ack, leaving the server with open connections.

Impact:

- Exhausts server resources (memory, CPU)
- Prevents legitimate users from establishing connections.
- Causes service unavailability especially dangerous for critical systems like financial web portals.
- May lead to downtime, revenue loss, and customer dissatifaction.

b) Estimate Data Rate from SYN flood attack.

Given

- 10,000 SYN packets per second
- Assume standard SYN packet size = 60 bytes (480 bits)

Data rate = packets/sec × packet size (in bits)

= 10,000 × 480 bits

= 4,800,000 bits/sec

= 4.8 Mbps

Conclusion.

The SYN flood attack is consuming approximately 4.8 Mbps of bandwidth, while this is a small portion of a 1 Gbps link, the real damage comes from server resource exhaustion, not bandwidth consumption.

c) Recommended firewall Rule sets to counteract SYN floods.

To mitigate SYN flood attack, the flowing firewall rules and configurations can be applied:

1. Rate limiting

bash

```
Iptables -A INPUT -p tcp --syn -m limit --limmut/10
     second -j Accept
```

This limit incoming SYN packets to 10 per Second, protecting the server from being overwhelmed.

2. SYN cookies

- enable SYN cookies in the operating system to prevent Tcp state table exhaustion.

Bash

```
sysctl -w net.Ipv4.tcp_symcookies=1
```

3. connection limits per Ip

bash

```
Iptables -A INPUT -p tcp --sym -m connlimit --
connlimit -above 5 -j Drop
```

- This drops new connections if a single IP ones more than 5 connections simultanely

4. Drop Invalid packets.

bash

```
Iptables -A INPUT -m state --state INVALID -j Drop
```

1) Suggested Anomaly Detection Techniques

To detect SYN flood or similar anomalies, the following techniques are recommended.

1. Threshold -Based Detection

- Monitor SYN packet rate
- Trigger alerts if packet rate exceeds pre-defined threshold (e.g >1000 SYN/sec)

2. Statistical Analysis

- Analyze average and standard deviation of connection request over time.
- Detect abnormal spikes

3. Machine Learning Models.

- Train model (e.g SVM, Random forest) on network traffic patterns to identify unusual behavior.

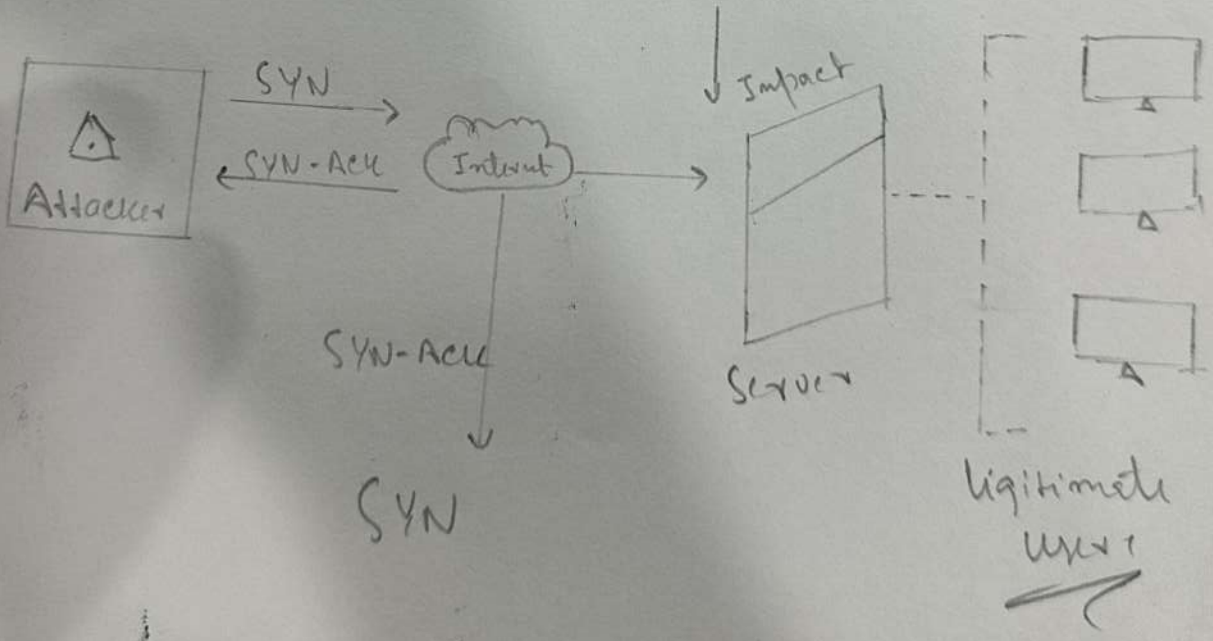
4. Behavioral profiling:

- Establish baseline behavior of users.
- Detect deviations indicating malicious activity.

5. use of Intrusion Detection System (IDS),
. Tools used Snort, Suricata and Bro/Zeek can detect alert on SYN flood patterns.

Conclusion

SYN flooding is a critical threat to high value- systems such as financial portals. Although it may not always consume high bandwidth, the real damage lies in its ability to deplete server resources. Proper firewall rules, system tuning, and intelligent anomaly detection can prevent or minimize the damage caused by such attacks. A layered security approach ensures better resillience and availability of services.


SYN
SYN-ACK
Attacker
Internet
SYN-ACK
SYN
Impact
Server
ligitimate users