Cybersecurity Incident Report: SYN Flood Denial-of-Service Attack

Date: 4 May 2025
Author: Kashish Patiyal
Incident Type: Denial-of-Service (DoS) Attack
Target: Company Sales Webpage
Target IP: 192.168.120.30
Attacker IP: 192.168.120.100
Tool Used: Wireshark

Incident Summary

A denial-of-service (DoS) attack was detected against the company's internal sales webpage. Upon analysing the network traffic using Wireshark, it was confirmed that the attack was a SYN Flood, which resulted in a Gateway Timeout error when legitimate users attempted to access the site.

Technical Analysis

TCP Three-Way Handshake Recap

Normally, TCP connections are established using the three-way handshake:

1. SYN – Client sends a synchronization (SYN) packet to the server to initiate a connection.
2. SYN-ACK – Server responds with a synchronization-acknowledgment (SYN-ACK).
3. ACK – Client completes the handshake with an acknowledgment (ACK).

Once this handshake is complete, the server and client can communicate.

Attack Behaviour

In the case of a SYN Flood attack:

- The attacker floods the server with a high volume of **SYN packets**.
- The server replies with **SYN-ACK** for each, waiting for the final **ACK**.
- The attacker **never responds with ACK**, leaving connections half-open.
- These half-open connections **exhaust server resources**, preventing it from handling legitimate requests.

57	3.664863	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
58	3.730097	198.51.100.14	192.0.2.1	TCP	14785->443 [ACK] Seq=1 Win-5792 Len=120...
59	3.795332	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win-5792 Len=120...
60	3.860567	198.51.100.14	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
61	3.939499	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win-5792 Len=120...
62	4.018431	192.0.2.1	198.51.100.14	HTTP	HTTP/1.1 200 OK (text/html)
63	4.097363	198.51.100.5	192.0.2.1	TCP	33638->443 [SYN] Seq=0 Win-5792 Len=120...
64	4.176295	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win-5792 Len=1
65	4.255227	192.0.2.1	198.51.100.5	TCP	443->33638 [SYN, ACK] Seq=0 Win-5792 Len=1
66	4.256159	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
67	5.235091	198.51.100.5	192.0.2.1	TCP	33638->443 [ACK] Seq=1 Win-5792 Len=120...
68	5.236023	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
69	5.236955	198.51.100.16	192.0.2.1	TCP	32641->443 [SYN] Seq=0 Win-5792 Len=120...
70	5.237887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

Wireshark Log Interpretation

Based on the attached Wireshark TCP/HTTP logs:

- The attacker at IP 192.168.120.100 sent **repeated SYN packets** to the target server at IP 192.168.120.30.
- The server responded with SYN-ACKs but **never received ACKs**, confirming incomplete handshakes.
- As a result, the server became overwhelmed and failed to respond to legitimate HTTP GET requests from other users.
- A typical log entry showed:

  GET / HTTP/1.1
  Host: 192.168.120.30
  User-Agent: Mozilla/5.0
  [Response: 504 Gateway Timeout]

73	6.230548	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=0 Win-5792 Len=1
74	6.330539	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
75	6.330885	198.51.100.7	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win=5792 Len=0...
76	6.331231	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
77	7.330577	192.0.2.1	198.51.100.5	TCP	HTTP/1.1 504 Gateway Time-out (text/html)
78	7.351323	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
79	7.360768	198.51.100.22	192.0.2.1	TCP	6345->443 [SYN] Seq=0 Win=5792 Len=0...
80	7.380773	192.0.2.1	198.51.100.7	TCP	443->42584 [RST, ACK] Seq=1 Win-5792 Len=1
81	7.380878	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
82	7.383879	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
83	7.482754	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=(
84	7.581629	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
85	7.680504	192.0.2.1	198.51.100.22	TCP	443->6345 [RST, ACK] Seq=1 Win=5792 Len=0.

Impact

- Employees were unable to access the sales webpage, disrupting business operations.

- The network infrastructure faced temporary resource exhaustion.
- Critical HTTP requests could not be fulfilled due to the server's overloaded connection table.

125	21.136783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
126	21.459796	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
127	21.782809	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
128	22.105822	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
129	22.428835	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
130	22.751848	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
131	23.074861	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
132	23.397874	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
133	23.720887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
134	24.0439	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
135	24.366913	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
136	24.689926	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

Recommended Mitigations

To prevent similar attacks in the future:

- **Implement SYN Cookies**: Protects against SYN Floods by not allocating resources until the handshake is complete.
- **Rate Limiting**: Restrict the number of half-open connections from a single IP.
- **Firewalls/IPS**: Configure firewalls and intrusion prevention systems to detect and drop suspicious SYN floods.
- **Traffic Monitoring**: Use tools like Wireshark or Zeek to monitor anomalies in traffic behaviour.
- **Blacklisting**: Temporarily block IPs sending unusually high volumes of SYN packets.

Conclusion

This incident demonstrates the importance of monitoring network traffic and having DoS mitigation strategies in place. A simple SYN Flood can cripple a server if left unchecked. Early detection through packet analysis tools like Wireshark plays a crucial role in rapid response and recovery.
