Cybersecurity Incident Report:
TCP SYN Flood Analysis

1. Executive Summary

Network traffic analysis identified a TCP SYN flood denial-of-service (DoS) attack targeting the organization's web server (192.0.2.1) over HTTPS (port 443). The attack originated from a single external IP address (203.0.113.0) and resulted in exhaustion of server-side connection resources. As a consequence, legitimate users experienced connection resets, slow response times, and HTTP 504 Gateway Time-out errors.

2. Incident Description and Timeline

During the initial seconds of the packet capture, normal TCP communication was observed between employee workstations (198.51.100.x) and the web server, including successful TCP handshakes and HTTP 200 OK responses. Shortly thereafter, a high volume of TCP SYN packets originating from 203.0.113.0 began appearing at a rapid and sustained rate.

As the attack progressed, the web server intermittently responded to legitimate traffic but increasingly issued RST/ACK packets. In the later stages of the incident, gateway devices generated HTTP 504 Gateway Time-out errors, indicating that the server was no longer able to process incoming requests. Eventually, legitimate traffic ceased almost entirely, while the logs became dominated by attacker-generated SYN packets.

3. Technical Analysis

Under normal conditions, TCP connections are established through a three-way handshake consisting of a SYN request from the client, a SYN/ACK response from the server, and a final ACK from the client. This behavior was clearly observed in the early log entries, where employee systems successfully accessed the sales.html webpage.

During the attack, the malicious host repeatedly sent SYN packets without completing the handshake. The server allocated resources for each pending connection, resulting in a growing number of half-open sessions. As these accumulated, the server's connection table and processing capacity were exhausted, preventing new legitimate TCP connections from being established.

4. Impact Assessment

The SYN flood attack rendered the organization’s website partially and eventually fully unavailable. Employees and customers were unable to access web resources required for normal operations, resulting in service disruption, potential revenue loss, and reputational risk. The incident demonstrates how a relatively simple network-level attack can have significant operational consequences.

5. Response and Mitigation

As an immediate containment measure, the web server was temporarily taken offline to allow recovery. Firewall rules were applied to block the attacking IP address, and traffic monitoring was intensified to verify service stability following restoration.

6. Conclusions and Recommendations

This incident was classified as a direct SYN flood DoS attack, based on the single-source nature of the traffic and the observed TCP handshake abuse. To reduce the likelihood of similar incidents in the future, it is recommended to enable SYN cookies, implement rate limiting for incoming TCP connection attempts, deploy intrusion prevention mechanisms capable of detecting DoS patterns, and establish automated alerts for abnormal TCP behavior.