Cybersecurity Incident Report – SYN Flood Denial of Service (DoS) Attack

Objective

The goal of this report is to analyze an incident in which a company web server became unresponsive due to abnormal inbound traffic. Using packet analysis and network monitoring tools, the objective was to determine the type of network attack, understand how it caused the outage, and propose mitigation steps to prevent future occurrences.

Scenario Overview

As a Security Analyst for a travel agency, I received an automated alert indicating a web server performance issue. Employees reported being unable to access the company's sales webpage. Attempting to visit the website resulted in a connection timeout error. Upon inspecting network traffic with a packet sniffer, I observed a massive volume of TCP SYN requests coming from a single external IP address. The server began dropping legitimate connections and became unreachable due to the overload of half-open TCP connections. This pattern indicated a SYN flood denial of service (DoS) attack in progress.

Step 1: Identify the Type of Attack

Attack Type: SYN Flood Denial of Service (DoS)

Indicators Observed:
• Large number of incoming TCP SYN requests without corresponding ACK responses. • Source IP: unfamiliar and repeatedly sending SYN packets in quick succession. • Server unable to complete the TCP three-way handshake due to backlog exhaustion. • Employees unable to connect to the web service (HTTP/HTTPS).

Attack Explanation:
A SYN flood is a form of Denial of Service (DoS) attack in which an attacker exploits the TCP handshake process. Each SYN request consumes server resources by initiating a half-open connection, awaiting a client acknowledgment that never arrives. When thousands of SYN requests are sent simultaneously, the server's connection queue fills up, preventing new legitimate sessions from being established.

Step 2: Explain How the Attack Caused the Website to Malfunction

Symptoms and Characteristics:

• Excessive TCP SYN traffic overwhelms the web server.

• The backlog of half-open connections leads to resource exhaustion (memory/CPU).

• The server stops responding to legitimate TCP requests, resulting in connection timeouts.

Impact on the Organization:

• The web server became unavailable, disrupting both employee operations and customer access.

• Revenue loss occurred due to downtime during active sales promotions.

• Customer trust was negatively impacted as users experienced consistent failures.

• Employees were unable to access internal tools dependent on the web infrastructure.

Network Devices Involved:

• Web Server (Target): hosted internally, overwhelmed by SYN requests.

• Firewall: initially configured to allow all inbound traffic, later updated to block the attacker IP. •

Attacker Host: remote system sending spoofed SYN packets at a high rate.

Step 3: Response and Mitigation Actions Taken

Action	Description
Immediate Containment	Took the web server offline temporarily to allow recovery and restore normal operation
Blocking	Implemented a firewall rule to block incoming traffic from the attacker's IP address.
Monitoring	Increased network monitoring thresholds to detect further abnormal SYN activity.
Communication	Alerted IT management and the incident response team of the ongoing DoS event.

Step 4: Recommended Preventive Measures

To minimize the risk of recurrence and increase resilience against SYN flood and DoS attacks, the following mitigations are recommended:

1. Deploy SYN Cookies – Configure the TCP/IP stack to handle large numbers of half-open connections efficiently.
2. Enable Rate Limiting on Firewalls or Load Balancers – Throttles SYN packets from a single IP to prevent flooding.
3. Use Intrusion Detection and Prevention Systems (IDS/IPS) – Detects and blocks abnormal connection patterns automatically.
4. Implement Redundant DNS and Load Balancing – Distributes traffic across multiple servers.
5. Consider a DDoS Mitigation Service – Use cloud-based defenses such as Cloudflare or AWS Shield.

Step 5: Conclusion

The incident was a SYN Flood Denial of Service (DoS) attack targeting the company's web server. The attacker exploited the TCP handshake process to overwhelm the server with half-open connections, preventing legitimate users from accessing the site. This investigation demonstrated effective packet analysis, incident identification, and network protection response. By implementing proactive measures such as SYN cookies, rate limiting, and firewall filtering, the company can enhance resilience against future attacks.

Cybersecurity Relevance

This lab enhanced my understanding of TCP/IP communication flow and vulnerabilities, practical DoS detection through Wireshark/tcpdump packet analysis, real-world incident handling procedures, and layered network defense strategies used in SOC environments.