REPORT
Network Attack Analysis

v1.0.1

Author:

Eldon Gabriel

June 12, 2025

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	02/15/2025	Eldon G.	Initial draft.
v1.0.1	06/12/2025	Eldon G.	Added section numbering and conclusion.

SECTION 1.0: NETWORK ATTACK ANALYSIS

1.1 Scenario Summary

As a security analyst for a travel agency, I received an automated alert about a potential issue affecting the company's public website, which promotes vacation packages. When I attempted to access the site, I encountered a connection timeout error.

Using a packet sniffer to analyze live traffic, I identified a high volume of TCP SYN requests from an unfamiliar IP address—an indicator of a potential SYN flood attack. This flood of incomplete handshake attempts overwhelmed the web server, causing it to become unresponsive. To mitigate the issue, I took the server offline temporarily and blocked the offending IP address using the firewall.

Recognizing the risk of IP spoofing and recurring attacks, I also provided strategic recommendations to improve the company's defense posture.

1.2 Attack Identification and Analysis

Log analysis revealed that log entry 52, at a timestamp of 3.390692, marked the first instance of abnormal traffic from IP address 203.0.113.0. This pattern matched the signature of a SYN flood—a form of Denial-of-Service (DoS) attack.

By sending a high volume of TCP SYN packets without completing the three-way handshake, the attacker exploited the server's connection resources, leaving half-open connections. Over time, as seen in log entry 98 at timestamp 15.310554, this led to full-service degradation and downtime

.

1.3 Impact of TCP SYN Flood on Website

During a normal TCP handshake:

1. A client sends a SYN packet to the server.
2. The server replies with a SYN-ACK.
3. The client responds with an ACK to complete the connection.

In this case, the attacker didn't send the final ACK, leaving the server with numerous half-open sessions. This consumed system resources and made the server unresponsive to legitimate traffic, causing users to encounter timeout errors when trying to access the website.

SECTION 2.0: CONCLUSION

2.1 Key Takeaways

This incident demonstrated how a basic yet effective DoS tactic, such as a SYN flood, can disrupt business operations when basic network hardening measures are not in place. Although the issue was mitigated by blocking the source IP, this alone is not a sustainable long-term defense.

2.2 Security Implications and Recommendations

To prevent similar attacks in the future, I recommend the following:

- **Enable SYN cookies** on the web server to protect against half-open connections.
- **Rate-limit SYN requests** using firewall rules or an intrusion prevention system (IPS).
- **Implement geo-IP blocking or throttling** for traffic from suspicious or unused regions.
- **Deploy a web application firewall (WAF)** in front of the website to detect and block abnormal patterns.
- **Monitor traffic continuously** with automated alerts for traffic spikes or repeated connection attempts.

Implementing these steps will reduce the risk of DoS-related outages and improve the resilience of the organization's public-facing infrastructure.