Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

Attack Name: TCP SYN Flood (Denial-of-Service)
Date: 11/08/2025
Analyst: Ukubeyinje Tsegbemi Oghenetega

Summary:
The incident was identified as a TCP SYN Flood attack, a type of Denial-of-Service (DoS) attack. Wireshark analysis of network traffic revealed an abnormally high number of SYN packets being sent to the web server from multiple sources, without completing the TCP three-way handshake.

Evidence from Logs:

- Repeated SYN packets from suspicious IP addresses
- Lack of corresponding ACK responses
- High volume of incomplete connections in the server queue

Impact on Network Performance:
This attack consumes server resources by overloading its connection table, preventing legitimate users from establishing a connection. As a result, the website displayed connection timeout errors and experienced significant performance degradation.

Section 2: Explain how the attack is causing the website to malfunction

1. Description of the Attack

A TCP SYN Flood attack exploits the TCP three-way handshake by sending numerous SYN packets but never completing the handshake with an ACK packet. The server allocates resources for each connection request, quickly exhausting available slots in the connection table.

Main Characteristics:

- Large number of SYN packets from malicious actors
- Incomplete TCP handshakes
- Server resources tied up in half-open connections

---

2. Effect on the Organization's Network

- Web Server Overload: The server's backlog queue filled with half-open connections, preventing new legitimate sessions.
- Network Congestion: Increased packet traffic reduced bandwidth available for normal users.
- Service Disruption: Users experienced long loading times, failed page requests, and connection timeout errors.

---

3. Potential Consequences

- Loss of Service Availability: Critical web services became unreachable for legitimate clients.
- Reputation Damage: Customers may lose trust in the organization's reliability.
- Financial Losses: Downtime may lead to revenue loss for e-commerce or subscription services.
- Increased Security Costs: Resources spent on incident response and mitigation.

---

4. Recommended Mitigation Strategies

- Deploy SYN Cookies: Helps prevent backlog queue exhaustion.
- Rate Limiting: Restrict the number of requests from suspicious IP addresses.
- Firewall Rules: Block malicious IPs identified in the logs.
- Intrusion Detection/Prevention Systems (IDS/IPS): Detect and drop suspicious SYN floods.
- Load Balancers: Distribute traffic across multiple servers to reduce single-point overload.

Note: This analysis is based on a simulated lab scenario and does not involve a real-world breach.