Cybersecurity Incident Report 2

Scenario Summary

As a security analyst for a travel agency, I received an automated alert indicating a problem with the company's web server. Attempts to access the website resulted in a connection timeout. Using a Wireshark TCP/HTTP log provided in spreadsheet format, I identified a surge of SYN requests from an unfamiliar IP address, suggesting a potential denial-of-service attack. I temporarily took the server offline to stabilize it and blocked the suspicious IP via the firewall. This report analyzes the incident and outlines the impact, response, and recommendations for preventing future attacks.

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

One potential explanation for the website's connection timeout error message is:

- The web server is overwhelmed by a high volume of incomplete connection requests, preventing it from responding to legitimate traffic and stopping employees from logging in and continuing regular business.

- The logs show a large number of incoming TCP SYN requests from an unfamiliar IP address, which do not complete the TCP handshake process.

This event could be:

- A **TCP SYN Flood Attack**, which is a type of **Denial of Service (DoS)** attack.

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

When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake:

1. **SYN:** The client sends a **SYN** (synchronize) message to the server to initiate a connection.

2. **SYN-ACK:** The server responds with a **SYN-ACK** (synchronize-acknowledge) message to acknowledge the request.

3. **ACK:** The client replies with an **ACK** (acknowledge) message, and the connection is established.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:

- The attacker sends many SYN requests but does **not respond** to the SYN-ACK messages from the server. This causes the server to **hold the half-open connections** in memory, waiting for completion. As these pile up, the server **runs out of resources** and becomes unable to respond to new, legitimate connection requests.

Explain what the logs indicate and how that affects the server:

- The logs show **a surge of SYN packets** from a single IP address without the expected follow-up ACK responses. This pattern suggests that the server is being **flooded with connection attempts** that are never completed, leading to **resource exhaustion**, connection timeouts, and ultimately **website unavailability** for users and employees.