Cybersecurity Incident Report

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:

- A SYN flood attack.

The logs show that:

- Multiple SYN packets are being sent in quick succession to the server without subsequent ACK responses.

This event could be:

- A Denial of Service (DoS) attack, specifically targeting the TCP connection process.
-

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. The client sends a SYN packet to the server to initiate a connection.
2. The server responds with a SYN-ACK packet to acknowledge the connection request.
3. The client sends an ACK packet back to the server to establish the connection.

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

- The server gets overwhelmed with the SYN requests, consumes resources to respond with SYN-ACK, but does not receive the final ACK. This can exhaust server resources and block legitimate connections.

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

- The logs indicate a high volume of SYN requests from a single source, which suggests a SYN flood attack, consuming the server's resources and preventing legitimate connections, leading to a service disruption.

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