**Cybersecurity Incident Report**

**Google Cybersecurity Professional Certification Program**

**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 Denial-of-Service (DoS) attack, specifically a Distributed Denial-of-Service (DDoS) attack

The logs show that:

A large number of TCP SYN requests are coming from an unfamiliar IP address.

This event could be:

An attacker overwhelming the web server with a flood of connection requests, preventing legitimate users from accessing the website. This aligns with the characteristics of a DDoS attack.

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

Three Steps of the TCP Three-Way Handshake:

SYN (Synchronize): The client (visitor's browser) sends a packet with the SYN flag set. This packet includes a sequence number that the client will use to sequence the data it sends.

SYN-ACK (Synchronize-Acknowledge): The server responds with a packet that has both the SYN and ACK (Acknowledge) flags set. This acknowledges the client's SYN packet and includes its own sequence number.

ACK (Acknowledge): The client sends a final packet with the ACK flag set, acknowledging the server's SYN-ACK packet. This completes the handshake and establishes the connection.

How a Large Number of SYN Packets Affects the Server:

When a malicious actor sends a large number of SYN packets all at once, it disrupts the normal flow of the three-way handshake:

Overwhelmed Server: The server receives a massive number of connection requests (SYN packets) but doesn't receive the final ACK from any of them. This creates a backlog of half-opened connections on the server.

Resource Depletion: The server allocates resources (memory, processing power) to manage these half-opened connections. With a large number of them, the server becomes overloaded and struggles to respond to legitimate connection requests.

Connection Timeout: Legitimate clients attempting to connect experience timeouts because the server is busy processing the backlog of incomplete connections. This explains the connection timeout error message on the website.

What the Logs Indicate:

The logs showing a large number of SYN requests from an unfamiliar IP address are a strong indicator of a DDoS attack. This abnormal traffic pattern is overwhelming the server's capacity to establish legitimate connections.