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 DDOS attack from a malicious actor.

The logs show that: A large number of TCP/IP SYN requests from an unfamiliar IP address.

This event could be: A SYN flood.

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- customer server attempts to establish connection with client server

2. SYN-ACK: the client server receives the SYN request

3.ACK- The customer server establishes connection with the client server

Explain what happens when a malicious actor sends a large number of SYN packets all at once: It can overload a server's ability to respond correctly.

Explain what the logs indicate and how that affects the server:The logs show a high volume of SYN requests from an unfamiliar IP address. Due to the high level of traffic the server wouldn’t be able to acknowledge all of the requests at once and wouldn’t be able to function correctly.