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 DOS attack. The logs show that there are multiple SYN requests being made by an unknown IP address. There is a large volume of traffic coming in. This event could be a SYN flooding 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.
1.The syn packet is the initial request from an employee visitor requesting access to a web page
2. The SYN Ack is web response agreeing to the connection requested by the visitor
3.The ACK packet is the visitor's machine acknowledging permission to the connection.

When a malicious actor floods a network with SYN packets, he usually sends a large number of SYN packets. Which then overwhelms the server for connection. When this happens, there are no resources available for legitimate connections.

The log indicates that the web server became overwhelmed and is unable to process visitors' SYN requests