Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
A possible reason for the website's connection timeout error is a Denial-of-Service (DoS) attack. Log data indicates that the web server becomes unresponsive after being overwhelmed by a high volume of SYN packet requests. This pattern suggests a specific type of DoS attack known as SYN flooding.

Section 2: Explain how the attack is causing the website to malfunction
When the website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The handshake consists of three steps: 1. The client sends a SYN packet to initiate the connection. 2. The server responds with a SYN-ACK packet, signaling it's ready to connect and reserves resources. 3. The client replies with an ACK packet, completing the handshake and establishing the connection. In a SYN flood attack, a malicious actor sends a high volume of SYN packets without completing the handshake. This causes the server to allocate resources for each incomplete request, eventually exhausting its capacity. As a result, legitimate users can no longer establish connections, receiving timeout errors instead. The logs show that the server is overwhelmed and unable to respond to incoming SYN requests, preventing new visitors from connecting.