Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

The network interruption which is connection timeout might have occurred due to the DoS attack. According to the log, the web server stopped responding after it was overloaded with SYN packet requests. SYN flooding type of DoS attack can be occured.

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

The visitor made a connection with the web server with the three-way handshake using TCP protocol. The handshake occurs by sending SYN packet from source to destination, then the destination send SYN-ACK to the source and the finally ACK is sent to the destination granting the permission to make a connection.

In this incident of SYN flood attack of DoS, the attacker send many SYN packets to the server at a time which overloads the server capacity. So, there are no server resources remaining for TCP connection request.

According to the log, the server is overwhelmed and it cannot process the SYN request from the visitor. So, new connection is failed to made and connection timeout message displayed.