Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
In the Wireshark log, evidence of a Denial of Service (DoS) attack is apparent through a SYN flood. The log reveals that a single IP address is repeatedly sending a high volume of SYN packets to the web server.

Section 2: Explain how the attack is causing the website to malfunction
When visitors try to connect to a web server, it is handled by the TCP protocol which uses a three way handshake. The three way handshake consists of a SYN packet sent from the visitor's source IP to the web server, and the web server sending back an SYN-ACK packet, acknowledging the request. Finally the source IP sends back another ACK packet, acknowledging permission to connect. A SYN flood is a type of DoS attack where an attacker overwhelms a target server by flooding it with a large number of SYN packets, intending to exhaust the server's resources and prevent it from handling legitimate connections. This is causing legitimate traffic to be timed out as the server is not able to respond in time to their requests.