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 an interruption with the system as there is a large amount of packets being sent. The logs show that there is a large amount of TCP SYN requests being sent to the server. This event is most likely a packet sniffing attack known as a SYN 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. First a SYN packet is sent to the server 2. The server sends a SYN/ACK pack back to the device 3. The device then sends the ACK to the server to finish a TCP connection When a malicious actor sends a large number of SYN packets all at once the servers are flooded with multiple packets. The server is unable to react to the large number of packets being sent and therefore, is slowed. When there is a TCP connection that needs to be established is it not possible and the website signals a ‘Timeout error’.