Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
One possible explanation for the website connection timeout error message is a DoS attack. The logs show that the web server stops responding after it is overloaded with SYN packet requests. This event could be a type of DoS attack called synchronized flooding (SYN).

Section 2: Explain how the attack is causing the website to malfunction
When website visitors try to establish a connection with the server, a 3-way handshake occurs using the TCP protocol. The linking process consists of three steps: 1. A SYN packet is sent from source to destination, requesting the connection. 2. The destination responds to the source with a SYN-ACK packet to accept the connection request. The destination will reserve resources for the source to connect. 3. The source sends an ACK packet to the destination to confirm connection permission. In the case of a synchronized flooding attack, a threat agent will send a large number of SYN packets at once, which will saturate the available server resources to be reserved for the connection. When this happens, there are no server resources left for legitimate TCP connection requests. The logs indicate that the web server has become overwhelmed and is unable to process SYN requests from visitors. The server cannot open a new connection to new visitors, who receive a connection timeout message