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 a denial of service attack (DOS). The logs show that an unknown IP is sending an extreme amount of TCP SYN packet requests to the web server to cause it to stop responding. As a result legitimate traffic cannot connect to the web server and gets an error message. This event could be a SYN flooding denial of service 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. The three steps of the handshake are: 1.The source IP sends a request to connect in the form of a SYN packet to the web server. 2. The web server responds with a SYN-ACK packet back to the source IP which accepts the request to connect and prepares for it. 3. The source IP confirms the connection by sending another ACK packet back to web server. When a malicious actor sends a large number of SYN packets all at once this is called a SYN flooding attack, which overloads a server's capacity to process connection requests because the server must allocate resources for each connection attempt. As a result the server is left with no resources to process an actual connection request that is not from this malicious actor. The logs indicate the server has stopped processing legitimate traffic and is completely bombarded with SYN requests from the unknown IP. As a result there is no way to access the server as a regular user and any new people who visit get a connection timeout message which is just the connection attempt being canceled because the server didn’t respond in time.