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: Somebody with malicious intent successfully completed a DoS attack and is flooding the website with SYN packets to cause the website to be overwhelmed. The logs show that: there are connection attempts from users to access the website, but are beginning to fail due to the overload of syn packets. This event could be: caused due to syn flooding, coming from an attacker who is trying to prevent the website from working by overwhelming it with traffic.

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. Explain the three steps of the handshake: 1. First, the user asks the server for a connection, sending a syn, which means synchronize. 2. Next, the website sends a receipt of this and says, “okay you’re good” with an ACK. So the response will look like [Syn, Ack] acknowledging the visitor's request to connect to the server. The destination will reserve resources for the source to connect. 3. Finally, the website sends a port for the visitor to connect and the source will say [ACK] for acknowledging the permission to connect and then they can access the website, which transitions the TCP connection to an HTML. Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious attacker sends a large number of SYN packets to a website, it causes it to be overwhelmed and not able to function correctly or allow other users to access it. Explain what the logs indicate and how that affects the server: The logs indicate a normal connection, then it shows an attacker syn flooding the website with a large number of syn packets. Since the website is overwhelmed with syn packets, it doesn’t have enough resources for the sources to connect.