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 flooded SYN Dos attacked causes the timeout The logs show that: The log showed that 203.0.113.0 was the attacker's IP address which was used This event could be: It is a SYN Dos 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. Explain the three steps of the handshake: 1. The [SYN] packet is sent by the user to the web server. 2. The [SYN,ACK] packet is sent by the web server to the user. 3. The [ACK] packet is sent to the web server for acknowledgment. Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends a large number of SYN packets, the server becomes overloaded with the requested eventually crashing. Explain what the logs indicate and how that affects the server: The logs indicate that when the attack was carried out, the server was able to fulfill only a few requests and after some requests, the server crashed and sent the time-out error to a legitimate request.