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: The website's connection timeout error is likely due to a Denial of Service attack. The logs show that: there is an overwhelming amount of SYN traffic from IP 203.0.113.0 to the server on port 443. This event could be: a SYN flood 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 client sends a SYN packet to the server, requesting a connection. 2. The server responds with a SYN-ACK packet to acknowledge the request. 3. The client replies with an ACK packet to establish a connection. Explain what happens when a malicious actor sends a large number of SYN packets all at once: In a SYN flood, a malicious actor sends numerous SYN packets but does not respond to the server's SYN-ACK replies, leaving the connection half-open. The server waits for the final ACK that never arrives, consuming resources to maintain these half-open connections. Explain what the logs indicate and how that affects the server: Continuous SYN requests without corresponding ACK responses, overloading the server's connection table. The server becomes overwhelmed with incomplete connections, causing it to be unable to handle new legitimate requests, leading to connection timeouts and website unavailability.