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: That the website is experiencing a Denial of Service attack. This is shown through the following error 504 time-out. The logs show that: On the packet, number 77 shows the following error,, HTTP/1.1 504 Gateway Time-out (text/html) This event could be: A SYN attack because the logs also show a large amount of SYN coming from 203.0.113.0 to destination 192.0.2.1.

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 user sends a SYN packet asking for a handshake. 2. The server responds with a SYN/ACK acknowledging the user. 3. A TCP connection is made between the user and server. Explain what happens when a malicious actor sends a large number of SYN packets all at once: It takes up all the ports on the server making any legitimate requests inaccessible. Explain what the logs indicate and how that affects the server: The logs indicate a SYN flood that takes up all the ports on the server, rendering it useless to any legitimate user trying to access the website. We can block & mitigate the Denial of service attack by blocking the IP in our firewall.