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 network interruption may have been caused by a SYN flood attack, which is a typo of Denial of Service (DoS) attack, which causes the traffic to be slowed down and crashes the server. The logs show that there is an IP address 203.0.113.0 making multiple SYN requests to IP destination 192.0.2.1. The log begins to reflect the struggle the web server is having to keep up with the abnormal number of SYN requests coming in at a rapid pace, which indicate a possible DoS attack.

Section 2: Explain how the attack is causing the website to malfunction
The TCP protocol has three steps, which are the following: First, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication. Then, the server responds with a SYN-ACK (acknowledgment) signal. Finally, the client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer. If the number of SYN requests is greater than the server resources available to handle the requests, then the server will become overwhelmed and unable to respond to the requests, causing the server to crash. The logs indicate that there were multiple SYN requests from IP 192.0.2.1. That caused the server to throw HTTP/1.1 504 Gateway Time-out (text/html) error messages and [RST, ACK] packets, RST stands for reset, acknowledge .