# 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 web server has potentially fallen victim to a DoS attack  The logs show that:  Approximately 47 messaged were sent and received by the web server in approximately 3.1 seconds.  This event could be:  A threat actor performing 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 device sends out a SYN packet, requesting a connection to the server 2. If authorized, the server sends back a SYN-ACK packet, acknowledging the request and providing a port to connect to 3. The device creates a connection to the server on the provided port via a sent ACK packet   Explain what happens when a malicious actor sends a large number of SYN packets all at once:  The server attempts to read each SYN packet sent, and additionally send back a SYN-ACK packet to the threat actor. If the number of SYN requests is greater than the available resources the server has to handle requests, the server will become overwhelmed and unable to respond to the requests.  Explain what the logs indicate and how that affects the server:  The logs indicate the server initially responds to the threat actors SYN request. Eventually however, the gateway server responds with a timeout error to the web server due to the request taking too long. This then prompts the web server to close the connection attempt and send a RST-ACK packet, which gives the visitor a timeout error message. The web server will stop responding to legitimate visitor traffic, with the logs showing only SYN requests being sent, and nothing returning. From log item 125 onwards, the web server stops responding. As there is one IP address sending SYN packets, it can be assumed this is a direct DoS SYN flood attack. |