# 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 DoS attack due to a SYN flood attack that is flooding the web server with too many SYN packets.  The attack occurred at 3.390692 after establishing a connection after the three way handshake.  A malicious attacker using and interfering a network connection by overwhelming the web server with SYN packets. | |
|

| **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 connection started to send the request a SYN from the device at 3.144521   2. The server responded with a SYN/ACK at 3.195755 to acknowledge the receipt of the request  3. The device sent back ACK at 3.246989 to acknowledge the established TCP connection between the two network connections.  This attack is affecting the traffic connection by the amount of SYN packets that are being sent to the server which are making the web server slow. This could indicate a Distributed Denial of Service (DDos) attack using too many devices to interfere with the network to the web server.  The logs are indicating that a large number of SYN packets were sent to the web server causing it to become unresponsive and unable to process any new connection. |