# Cybersecurity Incident Report

[**Scenario Description**](https://docs.google.com/document/d/16WvbZs8VIBy8glVtP37FRm-9Lq4W9zPudvYXOgZS8lY/edit?usp=sharing)

[**Wireshark Log**](https://docs.google.com/spreadsheets/d/1jAT2osOEgw0tz3Rbnt7bTFqn5Cqu0CWM7LQd0BgwouY/edit?usp=sharing)

[**Instructions on how to read Wireshark Log**](https://docs.google.com/document/d/1fxq3DCyLQwnJROStcDYfEFKZOUgxs9hwjN26NNN5cmM/edit?usp=sharing)

| **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.  The logs show that there are multiple SYN packet requests than normal which the web server eventually gets overloaded and stops responding to.  This event could be SYN flooding which is a type of DoS attack where the server is overloaded by TCP SYN packets and the server is overwhelmed as a result. In turn, the server is unable to respond to legitimate SYN packet requests. | |
|

| **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. Step 1 consists of the requesting party to send a SYN packet asking to connect to the server. 2. Step 2 is the server replying to this packet with a SYN-ACK (synchronize, acknowledge) packet accepting the connection request. 3. Step 3 is a final ACK (acknowledge) packet that acknowledges the connection.   Explain what happens when a malicious actor sends a large number of SYN packets all at once:  If multiple SYN packets are sent all at once as in the case of a SYN flood attack, the server gets overloaded and the server is unable to respond to the requests. In result, the server is unable to respond to any legitimate SYN packet requests since all the server resources are taken up.  Explain what the logs indicate and how that affects the server:  The logs in this incident show that the web server eventually stops responding to the SYN packet requests. Over some time, the server is unable to start new connections with legitimate requests and some people receive a timeout error as a result. |