# 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 is being overwhelmed by incomplete TCP connection attempts, preventing it from responding to legitimate users.  The logs show that:  There is a large number of incoming **TCP SYN packets** from a single unknown IP address. These packets initiate connections but do not complete the TCP handshake.  This event could be:  A **TCP SYN flood attack**, which is a type of **Denial of Service (DoS)** attack. It targets the TCP protocol by exploiting the connection initiation process, overloading the server's resources with half-open connections. | |
|

| **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.**SYN** – The client sends a TCP SYN packet to the server to initiate a connection.  2. **SYN-ACK** – The server replies with a SYN-ACK packet to acknowledge the request.  3. ACK – The client responds with an ACK packet, completing the handshake and establishing the connection.  Explain what happens when a malicious actor sends a large number of SYN packets all at once:  **The attacker floods the server with SYN packets but never responds with the final ACK. This results in many half-open connections, which consume the server’s memory and connection table slots.**  Explain what the logs indicate and how that affects the server:  The logs show a pattern of excessive SYN requests without corresponding ACK responses, confirming a SYN flood attack. This causes the server to become unresponsive, as it exhausts resources handling fake requests, leading to connection timeouts for real users and website downtime. |