# 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: DDOS attack.  The logs show that: SYN packet requests overloaded the web server causing it to stop responding to requests.  This event could be: a form of SYN flooding which is a type of DOS 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. A [SYN] packet is sent from a visitor/source, trying to connect to the destination.  2. A [SYN, ACK] packet is sent from the destination to the visitor to agree with the connection request. The destination will reserve resources for the source connect.  3. An [ACK] packet is sent from the visitor to the destination acknowledging the permission to connect.  Explain what happens when a malicious actor sends a large number of SYN packets all at once: During a SYN flood attack, an attacker bombards the server with numerous SYN packets simultaneously, exhausting the server’s resources meant for connections.  Explain what the logs indicate and how that affects the server: The logs indicate that the web server is overloaded and can't handle incoming SYN requests. As a result, it can't establish new connections, leading to connection timeout messages for new visitors. |