# 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 server crash. The logs indicate that a single source port has sent multiple [SYN] requests, without waiting for the next steps of the handshake to occur. This event could be the cause of a malicious actor performing a 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. In step 1 the source device sends a [SYN] message. This is used to establish a connection. 2. The second step is when the destination device sends a [SYN, ACK] message. This sends a [SYN] message to the source device and acknowledges the previous step. 3. Finally the source device send an [ACK] message which is just used to acknowledge the [SYN] message from step 2   Explain what happens when a malicious actor sends a large number of SYN packets all at once:  When a malicious actor sends a large number of SYN packets the server will be overwhelmed, this means that the website that is hosted in the server will become unreachable.  Explain what the logs indicate and how that affects the server: The logs indicate that a malicious actor has sent multiple SYN packets from a single source, this caused the server to be unavailable to legitimate employee website visitors. |