# 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: DNS attack or SYN attack  The logs show that: a lot of SYN requests to the server  This event could be: an attack from malicious attack as doing this will flood the server with too many requests, leading to the server unable to response to other 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. The visitor will send a packet which includes [SYN] to the server 2. The server responds back with a [SYN, ACK], meaning the sender is valid to connect to the website 3. The visitor respond back with a [ACK] => make a successful TCP connection   Explain what happens when a malicious actor sends a large number of SYN packets all at once: depend on the system resource of the server, if the server unable to process all the request, other request will unable to go through  Explain what the logs indicate and how that affects the server: |

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Testing with my own website to compare