# 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 logs show that: web server isn’t responding since its being loaded with SYN packets  This event could be: due to a DoS attack called SYN flooding |
|

|  |
| --- |
| **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 packet is sent from the source to the destination, which signifies SYNCHRONISATION i.e. a request to connect 2. The source is then acknowledged using a SYN-ACK packet in return. The destination will reserve resources for the source 3. After all the packets are sent, a last ACK packet is sent from the source to the destination.   Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a large amount of SYN packets are sent at the same time, the server starts to become unresponsive, it’s called SYN Flood Attack. When this happens, the server doesn’t have any resources left for legitimate TCP connections  Explain what the logs indicate and how that affects the server: The logs show that the server became unresponsive due to the large amount of SYN requests. The server is unable to open new requests/connections. |
|  |