# 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 that the web server is unable to respond to user requests due to being overwhelmed by requests. The logs show that repeated SYN requests are being sent from a single IP address, progressively reducing and ultimately disabling the server from responding to requests from other users. This event could be a Denial of Service (i.e. DoS) attack, in particular, a SYN flood attack, where a single IP address is used to send SYN requests at a high frequency. |
|

|  |
| --- |
| **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, which are:   1. SYN (client sends a request to synchronise with the server) 2. SYN, ACK (server conveys that it:    1. Has reserved resources for handling the client’s request    2. Gives the client permission to connect 3. ACK (client acknowledges the server’s permission)   When a malicious actor sends a large number of SYN packets all at once, the server is forced to reserve and attempt to respond to each packet, depleting the server’s resources (e.g. ports, processing, memory, etc.).  We see that up to log entry 62, the server was able to respond to users appropriately. However, we see a gateway timeout occur at log entry 77, which means the gateway server did not receive a response from the web server before the timeout; this corresponds to the progressively increasing SYN requests sent from the single IP address.  POTENTIAL FIX: Block requests from the attacking IP address, and configure a firewall (for the future) to limit SYN requests from a single source and/or block IP addresses sending abnormal amounts of SYN requests. |