# 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 webserver received a type of DoS attack, called SYN flood attack.  The logs show that: The logs show multiple SYN packet request is greater that the server resource available.  This event could be: the cause of the webserver not responding. The webserver become overwhelmed because of the great number of SYN packet request. |
|

|  |
| --- |
| **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 the initial request from an employee visitor trying to connect on a web page hosted on the webserver. 2. The SYN ACK packet is the web servers’ response to the visitor’s request agreeing to the connection. 3. The ACK packet is the visitor’s machine acknowledging the permission to connect.   Explain what happens when a malicious actor sends a large number of SYN packets all at once: It will overwhelm the web server, resulting on it becoming non responsive.  Explain what the logs indicate and how that affects the server: The logs indicated that a great amount of SYN packet is sent to the webserver, resulting for it to become non responsive. Resulting on the webpage being down. |
|  |