# 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 malicious or threat actor may be flooding the network or server, so that crashes and not be able to respond to legitimate users<br><br>The logs show that: There is a large number of TCP SYN requests coming from an unknown IP address. The server appears to be overwhelmed by the amount of traffic that's incoming and it is losing its ability to respond to the abnormally large number of SYN requests<br><br>This event could be: It could be SYN (synchronized) flood attack (DoS - Denial of Service attack), where the actor stimulates a TCP connection and floods a server with SYN Packets |

| **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:<br>1. The request goes from the users device to the server to initiate a network handshake<br>2. The request reaches the server and the server reviews it<br>3. The server sends a confirmation to the users device confirming and successfully establishing a handshake<br><br>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 all at once, The server gets overwhelmed by the amount of traffic that's incoming and it is losing its ability to respond to the abnormally large number of SYN requests<br><br>Explain what the logs indicate and how that affects the server: The logs indicate that the case would be a security attack on the servers, falling into the category of DoS attack |