# 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:<br>A SYN flood attack.<br><br>The logs show that:<br>The server was receiving way more connection requests than usual, all from the same weird IP address (192.168.2.75).<br>This event could be:<br>Someone trying to mess up our website on purpose by overloading it with too many 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:<br>1.SYN (Hi, wanna connect?): The visitor's computer sends a SYN message to the website to say "Hey, let's connect!"<br><br>2. SYN-ACK (Sure, let's!): The website sends back a SYN-ACK message to say "Okay, I got your message, let's connect!"<br><br>3.ACK (Cool, we're connected!): The visitor's computer sends an ACK message back to finalize the connection and say "Cool, we're good to go!"<br><br>Explain what happens when a malicious actor sends a large number of SYN packets all at once:<br>In a SYN flood attack, someone sends a ton of SYN messages but never sends the final ACK to complete the handshake.<br>Explain what the logs indicate and how that affects the server: |

The logs show that the server was getting flooded with these fake SYN messages from that one IP address, which caused it to get overwhelmed and stop working.