# 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 Threat Actor attacking the website with a DoS or DDoS attack.**  The logs show that: **A single IP address is flooding the network with SYN requests.**  This event could be: **A DoS Attack** | |
|

| **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. **The visitor sends a SYN request. This requests Synchronization or the establishment of a path of communication.**  2. **The server responds with SYN, ACK. This acknowledges the synchronization request, establishes a path of communication and sends an acknowledgement key so that the designated computer can access this path of communication.**  3. **The visitor responds with ACK. This is the acknowledgement from the visitor and cements this path as the route the server and visitor will use to communicate.**  Explain what happens when a malicious actor sends a large number of SYN packets all at once: **When a malicious actor initiates a SYN flood attack they send a large number of SYN requests with no intention of following up with an ACK when the server tries to respond. This can overwhelm the server as the server keeps attempting to create paths of communication. This interferes with other devices communicating with the server as the server begins to slow and can no longer respond to other visitors in a timely manner causing timeouts.**  Explain what the logs indicate and how that affects the server: **The logs indicate that a single IP address repeatedly sent SYN requests to the server and did not respond to the Server sending back a SYN, ACK. The server attempted to stop the visitor by sending a RES, ACK which would normally cause a visitor to have to reset their connection to a server. Instead this IP address continued to send SYN requests until the server was overwhelmed.** |