# 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 an attack is occurring on our web server, causing it to become flooded with other requests.  The logs show that many SYN requests to the web server can't be handled from the following course IP "203.0.113.0".  This event could be an attempt at a SYN flooding attack to stop the web server from working. |
|

|  |
| --- |
| **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:** The client sends a synchronization (SYN) packet to the server to request a new connection.  2. **SYN-ACK:** The server replies with a synchronization-acknowledgment (SYN-ACK) packet to confirm it is ready to communicate.  3. **ACK:** The client sends back an acknowledgment (ACK) packet, completing the three-way handshake and establishing the connection.  Explain what happens when a malicious actor sends a large number of SYN packets all at once:  This is known as a **SYN flood attack**. The attacker sends many SYN requests without completing the handshake, leaving the server waiting for ACKs that never arrive. This consumes server resources and connection slots, slowing down or preventing legitimate users from establishing connections.  Explain what the logs indicate and how that affects the server:  The logs show attacker IP **203.0.113.0** repeatedly sending SYN packets. At first, the server responded normally and still handled legitimate traffic (e.g., from **198.51.100.14**). As the flood continued, the server began failing to respond, producing **HTTP 504 Gateway Timeout** errors and **RST, ACK resets** for valid users. By log entry ~125, the server had stopped responding to legitimate visitors entirely, showing it was overwhelmed by the **direct DoS SYN flood attack**. |