# 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:  Server can’t handle this amount of traffic.  The logs show that:  There are numerous Syn requests from an attacker  This event could be:  A DoS attack from an attacker who’s ip is 203.0.113.0 | |
|

| **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.In the first step visitor sends a SYN request to the server.  2. Secondly, Web Server checks it and if it’s valid it sends a SYN ACK to the visitor.  3.Finally, Visitor sends a ACK to the server meaning and have granted to the visiting web-site.  Explain what happens when a malicious actor sends a large number of SYN packets all at once: When an attacker sends a large number of SYN packets that makes server slow down because it’s trying to send answer all of the requests which is behind it’s capabilities, it’s bandwidth so it starts malfunctioning.  Explain what the logs indicate and how that affects the server: The logs show that server is trying to answer every SYN request but there are just too many requests. So after some time it’s starting to malfunctioning and as we all see it’s starting to fail at No.73 and from 80 to 214 there is only 1 successful connetion to the server. |