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 the server was the target of a **TCP SYN flood attack**.

The logs show that the IP address **203.0.113.0** sent an abnormally high number of SYN packets (139) to the web server, while normal clients only sent a single SYN request each.

This event could be a **Denial of Service (DoS) attack** using SYN flooding.

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. The steps are:

1. The client sends a **SYN** packet to the server to request a connection.
2. The server responds with a **SYN-ACK** packet to acknowledge the request.
3. The client replies with an **ACK** packet to confirm, completing the handshake.

In a SYN flood attack, the malicious actor sends a very large number of SYN packets but never replies with the final ACK.
As a result:

- The server allocates resources and keeps many “half-open” connections waiting for the final ACK.
- Eventually, the server becomes overwhelmed and cannot process legitimate connection requests.
- This causes users to experience slow loading times or complete connection timeouts, as observed in the incident.

The logs confirm this pattern: a massive amount of SYN traffic from one IP address, without the expected ACK replies, exhausted the server’s ability to handle new connections.