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: **SYN flood attack**.

The logs show that:
- There are multiple **SYN** packets from **203.0.113.0** to **192.0.2.1**.
- The server is likely unable to process legitimate requests because its connection table is filling up.

This event could be:
A **Denial of Service (DoS) attack**, specifically a **SYN flood**, where an attacker overwhelms the web server by sending a flood of **TCP SYN 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:

1. **SYN (Synchronize)** – The client sends a **SYN packet** to request a connection.

2. **SYN-ACK (Synchronize-Acknowledge)** – The server responds with a **SYN-ACK** to acknowledge the request.

3. **ACK (Acknowledge)** – The client sends an **ACK** to complete the handshake, and data transfer begins.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:

- The attacker sends **a high volume of SYN requests** but does not complete the handshake by sending an ACK.
- This leaves the server waiting for responses, keeping resources occupied.
- The server's connection table fills up with half-open connections.
- Legitimate users cannot establish new connections, leading to **timeouts and service disruption**.

Explain what the logs indicate and how that affects the server:

- The logs show repeated **SYN packets** from a suspicious source IP without corresponding **ACK responses**.
- This suggests the attacker is **exhausting server resources**, making it **unable to process legitimate requests**.

Next Steps:

- **Block the attacking IP** at the firewall (temporary fix).
- **Enable SYN cookies** to prevent half-open connections from overwhelming the server.
- **Use a rate-limiting mechanism** to restrict excessive SYN requests.
- **Monitor for further attacks** to detect IP spoofing or distributed attacks.