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 high volume of abnormal TCP connection attempts, which led to server resource exhaustion and disrupted normal traffic.

The logs show that:

- A large number of TCP SYN packets were sent to the web server, primarily from source IP 203.0.113.0, with 140 connection attempts.
- The server attempted to respond with SYN-ACK packets, but many of these connections were followed by RST (Reset) packets, instead of completing the handshake.
- This behavior suggests that either:
    - A malicious actor was attempting a SYN Flood Attack, overwhelming the server with connection requests.
    - A misconfigured or overloaded system was failing to handle legitimate TCP connection attempts properly.

This event could be:
A potential SYN Flood Attack originating from IP 203.0.113.0, or an issue with the server's TCP connection handling, leading to service disruption. Further investigation is needed to determine whether this was an intentional attack or a server-side issue.

Section 2: Explain how the attack is causing the website to malfunction

The Three-Way Handshake Process in TCP

When website visitors try to establish a connection with the web server, a **three-way handshake** occurs using the TCP protocol:

1. **SYN (Synchronize)** – The client sends a **SYN** packet to the server to request a connection.
2. **SYN-ACK (Synchronize-Acknowledge)** – The server responds with a **SYN-ACK** packet, acknowledging the request and signaling its readiness to establish a

connection.
3. **ACK (Acknowledge)** – The client sends a final **ACK** packet, completing the handshake, and the connection is established successfully.

Impact of a Large Number of SYN Packets Sent by a Malicious Actor

- In a **SYN Flood Attack**, a malicious actor sends a massive number of **SYN packets** to the server but does not complete the handshake.
- The server **reserves system resources** for each half-open connection, waiting for the final **ACK** packet that never arrives.
- Since the server can only handle a limited number of simultaneous connections, it eventually **runs out of resources**, making it unable to process new requests from legitimate users.
- This results in website visitors experiencing **slow responses or complete connection failures (timeouts)**.

What the Logs Indicate and How It Affects the Server

- The logs show that **IP 203.0.113.0 sent 140 SYN requests** in a short period.
- The server responded with SYN-ACK packets but received very few ACK responses, meaning **many connections remained half-open**.
- Additionally, the presence of **RST (Reset) packets** in the logs suggests that the server was overwhelmed and forcefully closing connections.
- As a result, the server's resources were exhausted, **preventing legitimate users from accessing the website**.