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:

The logs show that:
One possible explanation for the website's connection timeout error is a **SYN flood attack**.

The logs indicate that the server was overwhelmed with a large number of SYN packets, which resulted in repeated HTTPS errors. Since all of the traffic originated from a single IP address, this points to a **Denial-of-Service (DoS) attack** rather than a Distributed Denial-of-Service (DDoS) attack.

The logs show that the server was flooded with a large number of SYN packets, which caused two key errors:

- **Gateway timeout**
- **SYN-ACK packet not received by the web server, leading to RST responses**

This event could be: This event can therefore be classified as a **SYN flood / DoS attack**.

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, requesting to start a connection.
2. **SYN-ACK:** The server replies with a synchronization acknowledgment (SYN-ACK) packet, confirming receipt and readiness to connect.
3. **ACK:** The client responds with an acknowledgment (ACK) packet, completing the handshake and establishing the connection.

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

- The server allocates resources for each incoming SYN request but never receives the final ACK.
- This overwhelms the server's connection table, consuming memory and processing

power.

- Legitimate users cannot complete their handshakes, resulting in failed or delayed connections.

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

- **Red (SYN Flood Attack):** Repeated SYN packets from the same IP address overwhelming the server.
- **Yellow (Errors):** Connection failures such as **gateway timeout** and **SYN-ACK packets not received → RST responses**.
- **Green (Successful Handshake):** Normal TCP three-way handshakes where SYN → SYN-ACK → ACK completed without issue.

- The logs show a flood of SYN packets from a single IP address.
- Errors observed include **gateway timeouts** and **SYN-ACK packets not being received by the web server, leading to RST (reset) responses**.
- This behavior confirms a **SYN flood Denial-of-Service (DoS) attack**, where the server is overloaded and unable to handle legitimate traffic.