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 SYN flood attack. The logs show an abnormal and overwhelming number of TCP SYN requests originating from an unfamiliar IP address (203.0.113.0). This event could be indicative of a direct Denial of Service (DoS) attack on the company's web server. The primary objective of a SYN flood attack is to saturate the target server with a high volume of incoming SYN requests, rendering it unable to respond to legitimate connection attempts.

Section 2: Explain how the attack is causing the website to malfunction
In a normal web server interaction, a three-way handshake is established between a client (e.g., an employee's computer) and the server. This handshake typically consists of the following steps: 1. The client sends a SYN (synchronize) packet to initiate a connection request. 2. The server responds with a SYN, ACK (synchronize acknowledge) packet, indicating it is ready to establish the connection. 3. The client acknowledges with an ACK (acknowledge) packet, completing the handshake. In the case of a SYN flood attack: ● The malicious actor sends a large number of SYN packets (step 1) to initiate connections at an extremely rapid rate. This artificially increases the number of half-open connections and consumes server resources. ● As observed in the logs, the attacker (IP address 203.0.113.0) sends continuous SYN requests (rows 119 and onwards) without proceeding to complete the handshake. This behavior causes a backlog of half-open connections, eventually overwhelming the server. The logs indicate that the company's web server starts responding to the attacker's SYN requests (rows 52-54) but becomes progressively less responsive to legitimate client requests (highlighted in green). This situation leads to network congestion and results in connection timeouts for genuine website visitors (highlighted in yellow). The consequences of this attack are significant: ● The website experiences slow loading times, ultimately leading to connection timeouts for legitimate users.

- Normal user requests are lost or not processed due to server overload.
- The organization may suffer revenue loss as customers cannot access the website to make bookings or purchases.
- The brand's reputation may be damaged, as users experience poor website performance.

To mitigate this attack, the organization can implement various security measures, including the use of rate limiting, Intrusion Prevention Systems (IPS), Web Application Firewalls (WAFs), and employing anti-DDoS solutions. Ongoing monitoring and a well-defined incident response plan should also be established to ensure timely detection and response to such attacks in the future. Additionally, cloud-based content delivery networks (CDNs) and load balancing can help distribute and absorb incoming traffic to prevent server overload.