Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The website's connection timeout error is likely caused by a SYN flood attack. In this scenario, the server is overwhelmed with an excessive number of SYN requests from a single IP address, preventing it from responding to legitimate connection attempts. This results in the gateway server issuing timeout error messages. The network logs reveal that the web server becomes unresponsive to incoming requests, supporting the conclusion that a direct DoS (Denial of Service) attack using SYN flooding is the root cause of the issue.

Section 2: Explain how the attack is causing the website to malfunction
When users attempt to connect to the website, the TCP protocol initiates a three-way handshake to establish the connection: 1. The client sends a SYN (synchronize) request to the server to initiate the connection. 2. The server responds with a SYN/ACK (synchronize/acknowledge), indicating readiness to proceed. 3. The client sends an ACK (acknowledge) to confirm the connection, completing the handshake. In a SYN flood attack, the malicious actor sends a massive number of SYN requests without completing the handshake. The server allocates resources for each incoming SYN request but becomes overwhelmed when its capacity is exceeded. This resource exhaustion prevents the server from processing legitimate requests, causing it to fail. The logs further indicate that the server stops responding to legitimate traffic, and users encounter repeated error messages when attempting to connect. This disruption of service confirms that the SYN flood attack effectively incapacitated the server, preventing it from handling normal operations.