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 is that the server is receiving an abnormally high number of connection requests, causing it to become unresponsive and resulting in connection timeouts for users. The logs show that the web server is receiving multiple TCP SYN requests originating from a single IP address without the completion of the TCP three-way handshake. This event is consistent with a Denial of Service (DoS) attack, specifically a SYN flood attack, in which a malicious actor sends a large number of SYN packets without responding with the final ACK. This behavior causes the server to maintain a large number of half-open connections, exhausting system resources and preventing legitimate users from establishing connections. To mitigate this issue, defensive measures such as enabling SYN cookies, limiting the number of half-open connections, reducing connection timeouts, and deploying an Intrusion Prevention System (IPS) to detect and block anomalous traffic patterns should be implemented.

Section 2: Explain how the attack is causing the website to malfunction
When a website visitor attempts to establish a connection with a web server, the TCP protocol uses a three-way handshake to initiate the connection. 1. In the first step, the client sends a SYN (synchronize) packet to request a connection. 2. The server responds with a SYN/ACK (synchronize/acknowledge) packet, indicating that it is ready to establish the connection. 3. Finally, the client sends an ACK (acknowledge) packet to confirm the connection, completing the handshake. In a SYN flood attack, a malicious actor sends a large volume of SYN packets but never responds with the final ACK. As a result, the server keeps these connections in a half-open state, consuming available ports, memory, and processing resources. Over time, this resource exhaustion prevents the server from accepting legitimate connection requests. The logs indicate repeated SYN connection attempts from a single IP address without corresponding ACK responses. This pattern confirms that the server is being

overwhelmed by half-open connections, leading to service degradation and the observed website connectivity issues.