Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
Based on the provided TCP log and color-coded information, it seems that there is a series of red-colored lines indicating multiple unsuccessful TCP connection attempts with the [SYN] flag set and accessing sales.html file. This pattern is consistent with a type of network attack known as a "SYN flood" attack. A SYN flood attack is a form of Denial of Service (DoS) attack in which an attacker sends a large number of TCP connection requests with the [SYN] flag set but without completing the full TCP handshake.

Section 2: Explain how the attack is causing the website to malfunction
Based on the provided TCP log, it appears that the website is experiencing a DDoS (Distributed Denial of Service) attack. Here's how the attack is causing the website to malfunction: **Normal TCP Connections (Green Entries):** The log begins with normal TCP connection handshakes. This is the standard process by which a client establishes a connection with a server. In the green entries, you can see the SYN (synchronize) and ACK (acknowledge) flags being exchanged between the client and the server. This is the expected behavior for a healthy website. **Attack Activity (Red Entries):** The red entries indicate attack activity. In these entries, you can see multiple sources (IP addresses) attempting to establish TCP connections with the server by sending SYN packets. However, the ACK packets (acknowledging the connection) are not being received from the server. This is indicative of a SYN flood attack, a type of DDoS attack where the attackers overwhelm the server by sending a large volume of SYN requests

without completing the connection establishment process.

Normal TCP Connections Failing (Yellow Entries): The yellow entries represent normal TCP connections failing due to the ongoing attack. In these entries, you can see that the client sends a SYN packet to initiate a connection, but the server responds with a RST (reset) packet, terminating the connection. This is likely because the server is under heavy load from the attack and cannot handle the incoming connection requests.

HTTP Requests and Responses (Green Entries): Throughout the log, you can also see successful HTTP requests and responses. These entries represent clients attempting to access the website's content. While some of these requests are successful and receive HTTP 200 OK responses, others are affected by the attack and do not receive responses.

In summary, the attack is causing the website to malfunction by overwhelming it with a large number of SYN requests, leading to a situation where the server is unable to handle legitimate connection requests. As a result, normal TCP connections are failing, including HTTP requests, leading to unresponsiveness and a potential downtime of the website. This kind of attack can effectively disrupt the availability of the website's services, making it inaccessible to users.