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 a large number of TCP SYN packets without corresponding ACK packets, suggesting a potential SYN flood attack**.** **The logs show that:** Numerous TCP SYN packets are sent from the IP addresses 198.51.100.5 and 198.51.100.7 to the web server's IP 192.0.2.1. There are also RST packets indicating reset connections, which can be a sign of the server being overwhelmed and unable to handle connections properly. **This event could be:** A SYN flood attack, a type of Denial of Service (DoS) attack that overwhelms the web server with a flood of SYN packets, preventing legitimate connections from being established.

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 TCP SYN (synchronize) packet to the server to initiate a connection. 2. **SYN-ACK:** The server responds with a SYN-ACK (synchronize-acknowledge) packet to acknowledge the client's request. 3. **ACK:** The client sends an ACK (acknowledge) packet back to the server, establishing a full-duplex communication channel.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends a large number of SYN packets without completing the handshake (by not sending back the ACK packet), the server allocates resources to wait for the completion of each handshake. This can quickly exhaust the server's available resources, leading to a situation where the server can no longer process legitimate requests, resulting in a denial of service.

Explain what the logs indicate and how that affects the server: The logs indicate a high volume of SYN packets (as seen in the TCP lines with [SYN]) and some RST packets (indicating reset connections). This suggests that the server is being flooded with connection requests it cannot handle, leading to it being unable to respond to legitimate traffic, which causes the connection timeout errors observed by the users.