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 direct DoS attack from source external IP address 203.0.113.0. The logs show that the web server was struggling handling multiple requests and stops responding after it is overloaded with SYN packet requests, with 151 SYN packets logged and only 5 SYN-ACK responses. This event could be a type of DoS attack called SYN flooding, where the server is flooded with incomplete connection requests, exhausting resources. A breakdown of the network traffic from the log: 1. TCP Handshakes (Normal Connections) - Packets 47, 48, and 49: Represent a normal TCP handshake between `198.51.100.23` and `192.0.2.1` for port 443 (SYN → SYN-ACK → ACK), establishing a secure connection over HTTPS. - Packets 52 and 53: Another handshake attempt from a different IP (`203.0.113.0`) towards the same destination (`192.0.2.1`). -The 1st attempt of the attack from an unfamiliar IP address 2. HTTP Traffic: - Packet 50: The client at `198.51.100.23` issues an HTTP GET request for the file `/sales.html`. - Packet 51: The server at `192.0.2.1` responds with an HTTP 200 OK, serving the requested file. - Similar traffic follows for requests from different source IPs, such as `198.51.100.14` and `198.51.100.5`. 3. Anomalies (Possible Attacks or Connection Resets): - Packets 73, 80, 83, 85, 89: These contain `RST` (Reset) flags, indicating that the server at `192.0.2.1` is forcefully closing connections with multiple sources (e.g., `198.51.100.16`, `203.0.113.0`). This could either be a reaction to network issues or part of a DoS (Denial of Service) attempt.

Section 2: Explain how the attack is causing the website to malfunction
When the website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The handshake consists of three steps: 1. **SYN (Synchronize):** The client sends a SYN packet to the server to initiate a connection. 2. **SYN-ACK (Synchronize-Acknowledge):** The server responds with a SYN-ACK packet to acknowledge the request and signal readiness to establish a connection. 3. **ACK (Acknowledge):** The client sends an ACK packet, confirming the connection, allowing data transmission to begin. When a malicious actor sends a large number of SYN packets without completing the handshake, the server allocates resources for each request and waits for the final ACK. However, the ACK never arrives, causing the server to leave these connections in a half-open state. As more SYN packets flood the server, it runs out of available resources to process legitimate requests, leading to delays or complete failure in responding to real users. The logs indicate a large disparity between the number of SYN packets (151) and SYN-ACK responses (5). This means the server is being overwhelmed by SYN requests but is unable to respond to all of them. This results in the server's connection queue becoming full, leading to connection timeouts, slow loading times, and the inability for legitimate users to connect, ultimately causing the website to malfunction