Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

The issue described in the scenario is characteristic of a TCP SYN flood attack, a type of Denial of Service (DoS) attack. In a normal TCP connection, the client and server perform a three-way handshake:

1- Client sends a SYN packet to the server.
2- Server responds with a SYN-ACK.
3- Client replies with an ACK to complete the handshake.

In this case, we observed the following in the packet log:
A successful connection by an employee with IP 198.51.100.23, who completed the TCP handshake (Packets 47–49) and made an HTTP request that received a successful response (HTTP 200 OK).
Other internal IPs, such as 198.51.100.14, also appear to have succeeded, while 198.51.100.16 failed to complete a connection, likely due to the web server being overwhelmed.
A large number of SYN packets were observed coming from a single external IP address: 203.0.113.0, without completing the handshake (no matching ACK or HTTP request packets). This strongly indicates SYN flooding behavior.
The result is that the web server's connection queue fills up, and it cannot process legitimate requests, resulting in timeout errors and service unavailability.
The fact that the server replies with [RST, ACK] (Packet 73) further confirms that it's terminating or rejecting connections, likely due to resource exhaustion or timeouts from incomplete handshakes.
This is likely a SYN spoofing attack to perform a DoS, where the attacker may spoof or hide their true IP address and floods the server with SYN packets, aiming to deplete system resources and deny access to legitimate users.

Section 2: Explain how the attack is causing the website to malfunction

The attack disrupts the website by exploiting the way TCP connections are established.
In a TCP SYN flood attack, the attacker sends a large volume of SYN packets but never completes the handshake (no ACK is sent back). The server, expecting the handshake to complete, allocates resources for each half-open connection and waits for the final ACK. This leads to resource exhaustion on the server, Legitimate users experiencing long load times or connection timeout errors, as their SYN requests are dropped or ignored. The server potentially responds with [RST, ACK] to reject or reset connections, as seen in Packet 73.