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 DoS attack. As per the data logs we capture using a packet sniffer in transit to and from the web server. a large number of TCP SYN requests coming from an unfamiliar IP address. This could be a SYN Flood attack which is a DoS attack that stimulates a TCP connection and floods with SYN packets.

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.When visitors try to establish a connection (initial request), the source sends a SYN packet to the destination, requesting to establish a connection.

2. The (SYN, ACK) packet is the response from the web server you get for the initial request agreeing to the connection. Server will reserve the system resources for the final step of the handshake.

3. The (ACK) packet is sent from the visitor's machine acknowledging the permission to connect. Final step required to make the successful TCP connection.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:
As happened in this incident, sending a large number of SYN packets as the first part of the handshake can overwhelm the server. If the number of SYN requests are higher than the server resources to handle the requests, the server will be unable to respond to requests. This is a DoS attack called a SYN flood attack that stimulates a TCP connection flooding server with SYN packets.

Explain what the logs indicate and how that affects the server: When investigating logs we can see the IP address 203.0.113.0 sending SYN packets in the beginning with no issues. There are legitimate TCP connection establishments in the first few requests, but then the server notices that there are an abnormal number of SYN requests from the visitor bearing 203.0.113.0 IP address coming at a rapid pace. Log indicates some legitimate visitor requests also get fail trying to communicate with the server.