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 that: The logs show a *SYN Flood Attack* from the IP address 203.0.133.0 targeting the server on the 192.0.2.1 IP.

This event could be: Denial of Service (DoS) Attack / SYN Flood Attack. This attacks targets the availability of the server / service.

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. The client send a SYN flag requesting a connection to the server.

2. The server responds with SYN/ACK acknowledging the connection.

3. The client responds with ACK acknowledging the server response and gets ready to transmit data.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor overwhelms the system with SYN packets, the server fills up the its connections table with half-open connections attacking the availability of the server / service.

Explain what the logs indicate and how that affects the server: The logs show a large number of SYN packets from 203.0.133.0 [malicious actor / client] to 192.0.2.1 [server] starting ~7 seconds. This is consider a SYN Flood Attack a type of Denial of Service (DoS) Attack preventing legitimate users from connecting.