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 because the number of SYN requests to the server was greater than the server resources available to handle the requests, resulting in a connection timeout error.

The logs show that a single IP address (203.0.113.0) had started undergoing the three way handshake between itself and the webserver (191.0.2.1), after which it had begun sending an overwhelming number of SYN requests which resulted in the webserver not being able to respond to legitimate network requests from legitimate users.

This event could be a network Level DOS SYN Flood attack, given it was all coming from a single IP address.

Section 2: 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. A user's device (source) wanting to connect to the web server (destination) will send it a SYN (synchronize) packet.

2. The web server then responds with a SYN/ACK packet (synchronize/acknowledge) agreeing to the device's connection request, the web server will reserve some resources for the source to connect.

3. The Source then sends back an ACK packet, acknowledging the permission to connect.

When a malicious actor sends a large number of SYN packets, it overwhelms the web server with these requests, this will eventually leave the web server without enough resources to respond to other, legitimate requests until it eventually becomes unresponsive to any request.

The logs indicate the webserver has been compromised by a DOS SYN flood attack, this is indicated by an abnormal number of SYN requests from a single IP address, resulting in the web server without enough resources to open a new connection to new visitors who receive a connection timeout message.