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 malicious attacker is repeatedly sending SYN requests despite the server already approving his initial SYN request. This overload in traffic causes the web server to be unable to function normally, causing the web server's request to never reach the gateway server. This then throws a time-out error message to the requesting browser.

The logs show that:

A user from the source IP 203.0.113.0 caused repeated SYN requests to the web server, causing the web server's approval time to skyrocket to 30 seconds and become unresponsive.

This event could be:

A DoS attack from the source IP 203.0.113.0.

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.

A visitor requests access to a web page, which creates a SYN packet that gets delivered to the web server.

2.

The web server responds to the visitor's source IP address with a SYN and an ACK packet, alongside reserving resources to complete the handshake, which gives approval to the visitor.

3.

The visitor's web browser receives the ACK packet, which the browser acknowledges the permission to connect to the web page.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:

The malicious actor makes a SYN request to the web server, the web server then responds with a SYN and an ACK packet alongside reserving the resources to complete the handshake. However, because the malicious actor continues to send SYN packets without completing the handshake, the server's resources continue to overload until it cannot handle any more incoming requests.

Explain what the logs indicate and how that affects the server:

A user from the source IP 203.0.113.0 begins requesting access to the web server by sending a SYN packet at 3.39 seconds. The web server responds to the user's request with a SYN,ACK packet, the user's browser acknowledges the request and is granted permission to access the web server. After the acknowledgement, the user continues to send more SYN packets to the web server in quick succession. The web server attempts to send a SYN,ACK packet in response but the incoming traffic from the user overloads the web server's ability to respond with SYN,ACK. This causes any incoming requests to the web server to time-out, and makes accessing the web server impossible.