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 website seems to be experiencing a SYN flood attack.

The logs show that:
A single IP address (203.0.113.0) is repeatedly sending SYN packets to the server's port 443 without completing the three-way handshake.

This event could be:
A targeted Denial-of-Service (DoS) attack aimed at exhausting the server's resources, making it unresponsive to legitimate requests.

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 sends a SYN packet to the server requesting a connection.

2. The server responds with a SYN, ACK packet acknowledging the connection request

3.The client sends an ACK packet back to the server to finalize the connection setup.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:
The malicious actor floods the target with SYN packets without sending the final ACK. This behavior causes the server to allocate resources waiting for the final ACKs that never arrive. Over time, the server can become overwhelmed, consuming all available resources, and leaving no room for legitimate requests. This can result in the server becoming unresponsive or, in some cases, crashing.

Explain what the logs indicate and how that affects the server:
The logs show repeated SYN packets from IP address 203.0.113.0 to the server's port 443. However, these packets do not progress to complete the three-way handshake. As the server waits for the corresponding ACK responses, its resources are consumed.

The repeated SYN packets without corresponding ACKs indicate a SYN flood attack. Eventually, as seen in the logs, legitimate requests receive "504 Gateway Time-out" errors, highlighting the server's inability to handle the flood of requests and serve legitimate traffic simultaneously.