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 SYN flood attack, which is a form of Denial-of-Service (DoS).

The logs show that:
A single IP address (203.0.113.0) sent a large number of TCP [SYN] packets to the web server (192.0.2.1). These requests initiated many incomplete three-way handshakes, leaving the server waiting for final acknowledgment (ACK) responses that never came.

This event could be:
A Direct SYN Flood DoS attack. The attack comes from one source IP and overwhelms the server's available resources, preventing legitimate users from completing connections.

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. SYN – The client (visitor's browser) sends a SYN packet to the server to request a connection.

2. SYN-ACK – The server responds with a SYN-ACK to acknowledge and accept the request.

3. ACK – The client sends back an ACK packet, completing the handshake and allowing data transfer.

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

The attacker sends repeated SYN requests but does not respond with the final ACK step. This leaves the server with many "half-open" connections, consuming memory and system resources. Eventually, the server runs out of capacity and can't respond to legitimate users.

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

The logs show a continuous stream of SYN packets from IP 203.0.113.0 with minimal or no follow-up responses. Meanwhile, legitimate traffic starts failing. We see RST, ACK

packets and 504 Gateway Timeout errors, showing that the web server can no longer keep up. This confirms that the SYN flood attack is overloading the server and preventing normal website functionality.