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 likely experienced a SYN flood attack. This type of Denial of Service (DoS) attack overwhelms the server with TCP SYN requests that are never completed, exhausting system resources and causing it to become unresponsive.

The logs show that:

A high number of SYN packets were received from a single IP address (203.0.113.0) without follow-up ACK packets. This indicates that the three-way handshake was never completed, a key characteristic of a SYN flood attack.

This event could be:

A direct DoS attack meant to exhaust the server's resources by leaving many half-open TCP connections, ultimately denying access to legitimate users.

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 (synchronize) packet to the server to begin the connection.

2.

The server responds with a SYN-ACK (synchronize-acknowledge) packet to acknowledge receipt and request confirmation.

3.

The client sends an ACK (acknowledge) packet back to the server, completing the handshake and establishing the connection.

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

The server allocates resources for each SYN request it receives. If the handshake is never completed, these connections stay half-open. Too many half-open connections overwhelm the server, preventing it from handling new legitimate requests.

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

The logs indicate multiple SYN requests from a single IP address without completing the handshake. This results in many half-open connections, which eventually consume all available resources on the server, causing it to time out or crash.