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 server cannot respond to new SYN packets sent by legitimate users.

The logs show that:

An abnormally large number of SYN packets are being received from a single unknown IP address.

This event could be:
This appears to be SYN flood attack

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. To establish a website connection, the client (user) sends a SYN packet to the server.

2. The server returns a SYN/ACK packet to the client.

3. The client returns an ACK packet to the server, completing the

TCP handshake.

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

The server has a finite set of resources that can process the TCP connections. When a larger-than-expected number of SYN packets are received by the server, these resources are depleted, and new, legitimate TCP SYN packets cannot be processed or responded to.

The website can no longer support sessions from legitimate users.

The server logs show the abnormally large number of SYN packets being received by the server, from a single unknown IP address.

Since these SYN packets originate from a single IP address, this appears to be a SYN-flood Denial of Service (DoS) attack.

Were the SYN packets originating from multiple IP addresses this would be considered a Distributed Denial of Service (DdoS) attack.