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: Connection timeout error message which refers to a DoS attack.

The logs show that: Web server stops responding after it is overloaded with SYN packet requests.

This event could be: DoS attack or SYN flooding

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 packet is sent from the source to the destination.
2. The Destination replies to the source (SYN-ACK) packet to accept the connection request. It will reserve resources for the source to connect.
3. Final ACK packet is sent from the source to the destination acknowledging the permission.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: Overwhelms the servers available resources to reserve the ACK connection.

Explain what the logs indicate and how that affects the server: Log indicates the web server has become overwhelmed and is unable to process the visitors SYN request. Unable to open a connection