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 DoS attack.

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

This event could be: a type of DoS attack called a 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. The SYN packet is the initial request from a visitor to the destination requesting to connect.

2. The Destination replies to the visitor’s source IP with a SYN-ACK packet to accept the connection request. The destination will reserve resources for the source to connect.

3. The ACK packet is the visitor’s machine to the destination acknowledging the permission to connect.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: The system slows down or stops functioning due to the high request from the TCP SYN requests.

Explain what the logs indicate and how that affects the server: the logs indicate that the server can not be accessed due to the amount of information being requested.