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 server is facing a DoS attack(SYN flood)

The logs show that: The server stops answering the client after receiving many SYN requests.

This Event could be a DoS attack (SYN flood)

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 packet to establish a connection with the server

2. Then the server replies to the client with a SYN-ACK packet telling the client that the connection request is accepted

3. Last, the client will send an ACK packet to acknowledge the permission to connect.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a DoS attack (such as a SYN flood) occurs, the server allocates a certain amount of resources for incomplete connection requests. Once these resources are exhausted, the server is unable to handle new connection requests and begins denying them.
Explain what the logs indicate and how that affects the server:
The logs from No.124 to the rest indicate that the server does not have any available resources for the upcoming connection request. The server is unable to accept new visitor’s connection request.