Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of TCP SYN requests coming from an unfamiliar IP address. This is a form of SYN flooding as shown on the log and it is an example of DoS 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. First, the visitor's computer will send a SYN packet requesting to connect to the host.
2. The host then responded with SYN-ACK packet agreeing to the connection.
3. The visitor's computer will send an ACK packet acknowledging the permission to connect.

When a malicious actor sends a large number of SYN packets all at once, the web server will be overwhelmed by the volume of incoming traffic and will lose its ability to respond to the abnormally large number of SYN requests.

Based on the logs, the server is under attack by a malicious actor. The attack impacted the website's availability and new visitors get a connection timeout message.