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 an overwhelming number of requests coming from an unfamiliar IP address. This is probably a type of attack called Denial of Service(DoS) or a Distributed Denial of Service(DDOS), which floods the server with requests that it can no longer process and makes the server no longer work.

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 visitor's server trying to connect sends a SYN packet to synchronize the connection.
2. The server that receives the SYN request, sends back a SYN, ACK packet to acknowledge the synchronization. The destination will reserve resources to connect
3. The visitor's server sends back an ACK packet to finally acknowledge the permission to connect.

When a malicious actor sends a large number of SYN packets all at once the server floods of packets that are trying to establish a fake connection at a fast pace which stops the server from answering to actual visitors

The logs indicate that the web server has become overwhelmed and is unable to process the visitors' SYN requests. The server is unable to open a new connection to new visitors who receive a connection timeout message.