Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The most likely explanation for the connection timeout error messages is that the web server was subjected to a SYN flood DoS attack. Wireshark logs show multiple incoming SYN packets from one IP address over time, which overwhelmed the server and led to loss of connection for legitimate users

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 the server to request that a connection is established. 2. The server sends a SYN/ACK packet to the client to acknowledge the SYN request. 3. The client sends an ACK packet back to the server and a TCP connection is established. When the web server sends a SYN/ACK packet to a client, a certain amount of system resources are reserved to manage the connection that will be established. When a malicious actor sends a large number of SYN requests to a server but does not send an ACK packet in response to the server's SYN/ACK packets, system resources are continuously allocated for connections that are never properly established. This eventually results in system failure due to lack of resources. Wireshark logs indicate a large volume of SYN requests coming from a single IP address in a short amount of time, likely indicating a SYN flood DoS attack. This impaired the performance of the web server and meant that it was not able to establish connections to legitimate users due to lack of available system resources.