Cyber Security Incident Report Travel Agency

Part 1: Identification of the Type of Attack Causing the Network Interruption

Based on the available information, the connection timeout error message experienced by the website suggests a possible Denial of Service (DoS) attack. Analysis of the logs reveals that the web server ceases to respond when it is overwhelmed with an excessive number of SYN packet requests. This specific incident aligns with a type of DoS attack known as SYN flooding.

Part 2: Explanation of How the Attack Leads to Website Malfunction

When visitors attempt to establish a connection with the web server, the TCP protocol initiates a three-way handshake process. This process consists of the following steps:

1. The source sends a SYN packet to the destination, indicating a request to establish a connection.
2. The destination responds with a SYN-ACK packet, acknowledging the connection request and allocating resources to accommodate the connection.
3. The source then sends an ACK packet, confirming the permission to establish the connection.

In the case of a SYN flood attack, a malicious actor deliberately floods the web server with an overwhelming volume of SYN packets simultaneously. This flood of SYN packets consumes the server's available resources that are meant to be allocated for establishing connections. As a result, there are no server resources remaining to handle legitimate TCP connection requests.

The logs indicate that the web server has been inundated and is unable to process the SYN requests from visitors effectively. Consequently, the server is incapable of opening new connections for legitimate visitors, who in turn receive a connection timeout message.