Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
A large number of TCP SYN requests are flooding the web server from an unfamiliar IP address. Which was likely caused by a SYN flood attack, a type of denial-of-service (DoS) attack that overwhelms a server with incomplete TCP connection requests. This is evidenced by the large number of TCP SYN requests from an unfamiliar IP address, leading to the server's inability to respond and the resulting connection timeout error.

Section 2: Explain how the attack is causing the website to malfunction
The SYN flood attack disrupts the website's functionality by exhausting the server's resources with a barrage of incomplete TCP connection requests. This prevents the server from processing legitimate user requests, causing connection timeouts and rendering the website inaccessible. This can lead to significant consequences for the travel agency, including lost revenue, reputational damage, and customer dissatisfaction.