Cybersecurity Incident Report

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

This is a direct DoS SYN flood attack, as the attack is originating from only one IP address.

Section 2: Explain how the attack is causing the website to malfunction

The attacker is flooding the web server with SYN requests, which ultimately overwhelms it. Legitimate users will experience errors that indicate they cannot establish or maintain a connection and will not be able to access the website.

A firewall can be configured to block the offending IP address, which will temporarily eliminate the traffic and allow the web server to operate normally. A long term solution would be to add and configure an advanced firewall that is capable of identifying such activity and proactively remediating it.