Cybersecurity Incident Report

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
Websites connection timeout error message might be due to DoS attack. Web server is overloaded with SYN packet requests.

Part 2: Explain your analysis of the data and provide one solution to implement
When clients attempt to establish a connection with a web server, a three-way handshake occurs with TCP protocol. In a SYN flood attack a malicious actor will send a large number of SYN packets at one time. This attack will overwhelm the server. Server is unable to open new connections for legitimate users.