Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The website's connection timeout error message when clients try to visit is due to a DDOS attack called the SYN Flood attack. It is evident after reading the tcp logs that the server is failing to respond to legitimate connections due to inadequate resources as the resources are exhausted by the attack.

Section 2: Explain how the attack is causing the website to malfunction
The attack is carried out by exploiting the three way handshake involved in creating a tcp connection. When a user wants to visit a website, a three way handshake between the user and server is performed to establish connection. 1. Client sends a SYN packet to the server 2. Server responds with a SYN ACK message acknowledging the syn packet 3. Client responds with the ACK packet along with some data. The malicious attacker has used several IP addresses to send a huge number of SYN packets to the server. These huge numbers of packets exhaust the server's resources. This causes the server to fail its responsibilities and legitimate connections also fail. Upon inspecting the log, the server treats the SYN requests as legitimate and responded accordingly. However, as the number of SYN requests grew exponentially, the IP addresses have been marked red indicating a threat. The connections that were legitimate but failed are marked in yellow to indicate the failure of the server to respond to connection requests due to the attack.