Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
The network interruption was caused by a SYN Flood which is a type of DoS attack.

Section 2: Explain how the attack is causing the website to malfunction
The attacker is connecting to the website through a TCP connection many times at once with an attack called a SYN Flood. A TCP connection has a three handshake protocol where the first handshake occurs when a source sends a SYN packet to the destination. From the logs we gather that the service experiencing the attack has many SYN packets being sent to it at once which will overwhelm the network and cause it to crash. It takes a long time for the website to load and report a connection timeout error because the system is backed up with so many TCP requests and still needs to perform a handshake for each request. From the log data it appears to be a DoS attack which means that there's only one device attacking your network at a time. This attack will cause your systems to go offline which can reduce customer retention and will cause financial loss. You can secure your network by implementing stricter firewall configurations to block this IP address as a bandaid, or reduce the amount of TCP requests from an IP address for a specific amount of time. You can also implement a Next Generation Firewall which will monitor your network and secure it against these attacks.