Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
One potential explanation for the website's connection timeout error message is: overloading the network with SYN requests The logs show that: several requests came from one IP address, which is the attacker and other from a regular customer This event could be: a SYN flood attack

Section 2: Explain how the attack is causing the website to malfunction
When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake: 1.The SYN packet is the initial request from an employee visitor trying to connect to a web page hosted on the web server. 2. The SYN, ACK packet is the response from the web server to the request agreeing the connection. 3.The ACK packet is the visitor’s machine acknlowledging the permission to connect. Explain what happens when a malicious actor sends a large number of SYN packets all at once: the network slows down because of the large number of packets that are sended to it. Explain what the logs indicate and how that affects the server: there are many requests in a very short time and this leads to the server to shut down or slow down.