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: the server not being able to handle the traffic coming in or a malicious actor The logs show that: A specific IP address is sending in a bunch of Syn packets to flood the service This event could be: Is a SYN attack which is leading to a Dos or denial of service

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 to connect to a web page hosted on the web server. SYN stands for “synchronize. 2. The [SYN, ACK] packet is the web server’s response to the visitor’s request agreeing to the connection. The server will reserve system resources for the final step of the handshake. SYN, ACK stands for “synchronize acknowledge 3.The [ACK] packet is the visitor’s machine acknowledging the permission to connect. This is the final step required to make a successful TCP connection. ACK stands for “acknowledge.” Explain what happens when a malicious actor sends a large number of SYN packets all at once: In a SYN flood attack, a malicious actor inundated a server with a barrage of SYN packets, exploiting the TCP handshake process. These packets are crafted to appear legitimate, initiating connection requests but failing to complete the handshake. As the server allocates resources to track each connection attempt, its connection queue becomes overwhelmed with half-open connections. Consequently, the server exhausts its resources, leading to a denial of service (DoS) situation where legitimate users are unable to access the server's services. Explain what the logs indicate and how that affects the server: The logs indicate that the web server has become overwhelmed and is unable to process the visitors’ SYN requests. The server is unable to open a new

connection to new visitors who receive a connection timeout message.