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: This could be a (DDos) attack since is seems a number of unwanted traffic is coming through, specifically a SYN flood attack or a TCP flood attack The logs show that: There is a large amount of TCP/SYN requests coming in from an unfamiliar IP address. This event could be: This could be an attempt from a malicious actor to overwhelm the web server with excessive SYN requests.

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 client sends a SYN packet to the server to initiate a connection 2. The server then acknowledges the request by sending back a SYN-ACK packet to the client 3. The client responds with an ACK packet and the connection is established Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a flood of SYN packets are sent to the server by a malicious actor, the server begins to find room for each SYN request, expecting an ACK that never comes. The flood of SYN packets causes the server to exhaust its resources, preventing it from handling legitimate request, leading to a DOS (Denial of service) Explain what the logs indicate and how that affects the server: The log indicated an abnormally high number of SYN requests from a single IP address, which is an obvious clue that a SYN flood DDoS attack is in place. This overwhelms the server and causes it to become unresponsive. Legitimate users then receive a timeout error and cant access the website. 4. How can this affect the organization: This can affect the organization by drumming up a

feeling of distrust by the user. They may be wondering if my information is safe on this company's website. Another reason is if a user can't access a site then the client may visit another site and never return to yours.