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: Server being flooded with SYN packets The logs show that: there are a lot of SYN requests happening. The web server is having trouble keeping up with the abnormal number of SYN requests which is sent almost every second. It shows errors such as web servers taking too long to respond and timeout errors in browsers. Multiple source IP addresses are found from the requests. This event could be: SYN flood attack **When we review the Wireshark logs, we could see that there are SYN requests from one IP address almost every second which is abnormal. The web server is having trouble keeping up with the SYN requests which is causing timeout errors in browsers and taking a long time to respond. This would most likely 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.Device sends a SYN packet which is the initial request from an employee visitor to connect to a web page hosted on the web server. 2. The server responds with a SYN/ACK packet to acknowledge the receipt of the device's request and leaves a port open for the final step of the handshake. It is a packet where the web server’s response to the visitor’s request agrees to the connection. 3.Server receives the final ACK packet from the device. TCP connection is established. It is the visitor’s machine acknowledging the permission to connect. Explain what happens when a malicious actor sends a large number of SYN packets all at once: Server will be overwhelmed and would be unable to function. Explain what the logs indicate and how that affects the server: Logs indicate that the web server is trying to keep up with the abnormal number of SYN requests coming in a rapid

pace. There are many errors showing up. Then, it stops responding to legitimate employee visitor traffic. The visitor receives more error messages which blocks them from establishing or maintaining a connection to the web server. Eventually, web server stops responding.

This attack is the DoS SYN flood attack since there are multiple attemtps of SYN requests happening every second from one IP address. It is causing problems with responding to legitimate employee visitor traffic, maintaining or establishing connection to the web server, and stopped the web server from responding properly.