Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
A connection timeout error message was shown in the browser. After using a packet sniffer to capture the packets it was found out that a large number of TCP SYN requests were coming from an unknown IP address. In the Wireshark TCP/HTTP logs, it was found out that there were huge requests of TCP SYN packets, for which the web server was not able to answer as the request exited its limit for response.This event could be a SYN flood Attack and as the IP is constant hence it is a DoS 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. The three steps of the handshake are as follows: 1. The [SYN] packet is the initial request from the employee visitor trying 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”. When the attacker was initially sending the SYN packets, the web server was able to answer, but when the attacker started sending huge amounts of SYN packets, the web server stopped responding to legitimate employee visitor traffic. From the TCP/HTTP logs, we could find out that initially there was a normal transaction between the website visitor and the web server, the normal handshake process takes a few milliseconds to complete. Then we can see the employee's browser requesting the sales.html webpage using the HTTP protocol at the application level of the TCP/IP model. Followed by the web server responding to the request(log items: 47-51). Log items (52-54) shows that the attacker’s initial request was answered normally. However, the attacker keeps sending more SYN requests, but still at this point the web server was able to respond to the normal visitors traffic and the employee’s browser requests for the sales.html webpage with a GET command and the web server responds (log items 55-62). Log items(63-83) the log begins to reflect the struggle of the web server to keep up with the abnormal SYN requests coming in at a rapid pace. The rows highlighted and labeled yellow of the logs are failed

communications between legitimate employee website visitors and the web server. Even after this, the web server was trying to answer the attacker's SYN requests, but ultimately stopped (log items: 125-214), resulting in a web server failure.