Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

When using a packet sniffer tool, I have discovered that there were a large number of TCP SYN requests coming from an unfamiliar IP address. In the logs, It indicates that web server fails to respond and gives an error message “connection timeout error”.
This likely shows a type of DoS Attack called 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. A SYN (Synchronize) Packet is sent from a source to establish connection with destination.

2. SYN/ACK (Synchronize Acknowledgement) is responded back by destination to accept the connection request. The destination will then reserve resources for the source to connect

3. ACK (Acknowledgement) will be sent as a final packet from source to destination acknowledging the establishment of connection

When a threat actor initiates a SYN flood attack, the attack itself will send a large number of SYN packets at once which overwhelms the server’s resources. This eventually causes the server to run out of resources for actual connections resulting in a timeout error

The logs indicate that the web server is receiving too many SYN requests from one IP address, in which the server is unable to open new connections to new visitors.