# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| **I received an alert from our monitoring system indicating a problem with the web server. I attempted to visit the company’s website but received a connection timeout error message in my browser. I used the packet sniffer TcpDump to capture the data packet’s transits to and from the web server and noticed a large number of TCP SYN requests coming from an unfamiliar IP address. The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests, and I think the server is under attack of a malicious actor.**  **This event could be a SYN Flood attack, which means that the malicious actor simulates TCP/IP connection and floods our server with SYN packets.** |
|

|  |
| --- |
| **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 visitors try to establish a connection by sending a **SYN** message. 2. The server responds with a **SYN-ACK** message. 3. Finally, the visitors send an **ACK** message, and they are ready to exchange data.   When too many SYN messages are sent to the server, the server crashes, the name of this attack is the SYN Flood Attack.  Explain what the logs indicate and how that affects the server : The logs indicate that there are too many TCP SYN requests, that makes the server overwhelmed by the volume of incoming traffic and it loses its ability to respond. |