# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| Employees are currently unable to access the website and are getting a timeout error message. Using Wireshark network analyzer to examine the traffic coming to the web server, we see many SYN packets being sent from an unfamiliar IP address. This is a denial of service (DoS) attack on our web server, specifically a SYN Flood attack. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| The DoS attack is causing the website to be unresponsive to web traffic. The threat actor is sending many SYN packets to the web server. Normally, the web server would try to establish a connection to the client by using the TCP/IP handshake. The server sents a SYN/ACK packet back to the client and maintains an open connection so the client can respond back with an ACK packet to finalize creation of the connection. In this case, the web server is appropriately sending the SYN/ACK packet back and keeping a connection open for the client to repond back to finalize the handshake. The client is not responding back with ACK packets but is flooding the server with SYN packets, forcing the web server to maintain open connections. This causes the server to become unresponsive to normal web traffic due to running out of available connections. |