|  |
| --- |
| **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**: DoS Attack  **The logs show that:** the web server stops responding after it is overloaded with SYN packet requests.  **This event could be:** a type of DoS attack called SYN flooding. |
|

# Cybersecurity Incident Report

|  |
| --- |
| **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. SYN (Synchronize): In the first step, the client sends a TCP segment with the SYN (synchronize) flag set to the server. This segment contains a random initial sequence number (ISN) generated by the client. The SYN flag indicates the client's intention to initiate a connection.  2. SYN-ACK (Synchronize-Acknowledge): Upon receiving the initial SYN segment from the client, the server acknowledges the request by sending a TCP segment back to the client. This segment has both the SYN and ACK (acknowledge) flags set. Like the client, the server generates a random ISN for this connection and includes it in the acknowledgment. The ACK flag indicates that the server is willing to establish a connection, and the SYN flag signals its intention to do so.  3. ACK (Acknowledge): In the final step, the client responds to the server's SYN-ACK by sending another TCP segment. This segment has the ACK flag set and acknowledges the receipt of the server's response. The client's acknowledgment includes the server's ISN incremented by 1, indicating that it is ready to start sending data. At this point, the connection is fully established, and both the client and server can begin exchanging data in a reliable and synchronized manner.  **Explain what happens when a malicious actor sends a large number of SYN packets all at once:** When a malicious actor sends a large number of SYN packets all at once, it's referred to as a "SYN flood attack." SYN flood attacks are a common type of Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack that exploits the three-way handshake process in the Transmission Control Protocol (TCP). If the attack is sustained and the server's resources remain overwhelmed, it can lead to a complete denial of service. Legitimate users cannot establish connections with the server, and it effectively disrupts the availability of the targeted service.  **Explain what the logs indicate and how that affects the server:** The logs indicate that the web server has become overwhelmed and is unable to process the visitors’ SYN requests. The server is unable to open a new connection to new visitors who receive a connection timeout message. |