# Cybersecurity Incident Report

|  |
| --- |
| **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: If the web server takes too long to respond, the gateway server will send a timeout error  message to the requesting browser.  The logs show that: rows, the log begins to reflect the struggle the web server is having to keep up  with the abnormal number of SYN requests coming in at a rapid pace. The attacker is sending  several SYN requests every second.  This event could be:  A form of passive sniffing because the threat actor does not inject any traffic into the network |
|

|  |
| --- |
| **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:  Three-Way Handshake in TCP  When a website visitor tries to establish a connection with a web server, a three-way handshake occurs using the TCP (Transmission Control Protocol) protocol. This handshake ensures a reliable connection is established between the client and server. Here are the three steps of the handshake:  1. SYN (Synchronize) Packet  The client (website visitor) sends a SYN packet to the server to initiate the connection. This packet includes the client's initial sequence number, which is used to keep track of the data being sent.  2. SYN-ACK (Synchronize-Acknowledgment) Packet  The server responds with a SYN-ACK packet, which acknowledges the client's SYN packet and sends its own SYN packet. This packet includes the server's initial sequence number and an acknowledgment of the client's sequence number.  3. ACK (Acknowledgment) Packet  The client responds with an ACK packet, which completes the handshake and establishes the connection. This packet acknowledges the server's SYN packet and confirms the connection is established.  Explain what happens when a malicious actor sends a large number of SYN packets all at once: When an actor sends a large number of syn all at once pretending to initiate a TCP connection but does not respond and so the receiver then waits until it can no longer respond causing a slow down in the response time.  Explain what the logs indicate and how that affects the server: The logs indicate that the threat actor sends an overwhelming number of SYN every second causing an unresponsive server |