# 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: The web server is too occupied responding to previously received SYN packets, that its resources are utilized to max capacity and the web server is unable to respond to the SYN with an SYN/ACK in time  The logs show that:  This event could be: It appears the webserves is getting overloaded by a suspected ddos attach. Specifically a SYN flood attack. It appears to be a ddos direct 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. STep one is when the user tries to connect to a web page by sending a SYN packet requesting the connection  2. The web server will respond with a SYN/ACK packet confirming and allowing the connection  3.The third step is the connection initing computer sending an ACK packet acknowledging that the connection is approved and starts the connection  Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a large number of SYN packets are received by the webserver, it will allocate resources to respond to every packet, overloading the server and potentially shutting it down. Unable to respond in time and approve connections  Explain what the logs indicate and how that affects the server: multiple SYN request packets are received by the server, causing the server to slow down and becomes unable to respond in time to legitimate SYN requests. Several RST ACK are transferred and eventually the server stops responding to legitimate requests. It continues to log the ddos attackers SYN requests |