# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| The website’s connection timeout error message may be due to the server not responding. The logs indicate an HTTP/1.1/504 Gateway Time-out (text/html) error along with [RST, ACK]. This event could potentially be a malicious SYN Flooding (DoS) 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. The [SYN] packet is the initial request from the visitor going to the web server  2. The [SYN, ACK] packet is the web server’s response to the visitor request agreeing to the connection  3. The [ACK] packet is the visitor’s machine acknowledging the permission to connect.  If the number of SYN request is greater than the server resources available to handle the request, then the server will become overwhelmed and unusable to respond to the request.  Explain what the logs indicate and how that affects the server:  An HTTP/1.1 504 Gateway Time-out (text/html) error message. This message is generated by a gateway server that was waiting for a response from the web server. If the web server takes too long to respond, the gateway server will send a timeout error message to the requesting browser  An [RST, ACK] packet, which could be sent to the requesting visitor if the [SYN, ACK] packet is not receive a timeout error message in their browser and the connection attempt is dropped. The visitor can refresh their browser to attempt to send a new SYN request. |