# 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: Looking at Wireshark TCP/HTTP logs, its clear to see that the web server is receiving a lot of traffic from certain IP that is sending a lot of SYN packets for first part of the three part handshake. Early on it’s looking like a DoS attack that is flooding the server.  Logs show that source IP “203.0.113.0” has sent over 10 SYN requests over a period of 2 seconds. First request coming in at row 52 at 3.390692 seconds and row 72 at 6.229638 seconds that starts to cause issues for internal traffic resulting in HTTP/1.1 504 Gateway Time-out (text/html) error messages being given to employees. | |
|

| **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] packet is the initial request from an employee visitor trying to connect to a web page hosted on the web server. SYN stands for “synchronize.”   2. [SYN, ACK] packet is the web server’s response to the visitor’s request agreeing to the connection. The server will reserve system resources for the final step of the handshake. SYN, ACK stands for “synchronize acknowledge.”  3. [ACK] packet is the visitor’s machine acknowledging the permission to connect. This is the final step required to make a successful TCP connection. ACK stands for “acknowledge.”  If a server receives a lot of SYN request packets in a short period that is over the resources available to process these requests it causes the server to become overwhelmed and not able to respond to genuine requests.  Logs clearly show that high requests of SYN acknowledgements are received and puts due stress on the server resulting in an [RST, ACK] packet being sent if the [SYN, ACK] packet is not received. RST stands for reset, acknowledge and visitor will receive error message in browser as connection attempt will be dropped. Visitors can then attempt to refresh the browser for a new SYN request. |