Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
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. The log show that at number 125 the web server stops responding to both legitimate visitors and attacker, The only items logged at that point are from the attack. As there is only one IP address attacking the web server, you can assume this is a direct DoS SYN flood 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 an employee visitor trying to connect to a web page hosted on the web server. SYN stands for “synchronize” 2. The [SYN, ACK] packet is the response from the web server which give an handshake to the employee visitor to connect to the web page hosted on the web server SYN,ACK Stand for “synchronize, acknowledge.” 3. The [ACK] packet is a receipt from an employee visitor telling the Web server that the visitor acknowledge the permission to connect, this is the final step to make sure TCP connection is successful. ACK stands for “Acknowledge” Explain what happens when a malicious actor sends a large number of SYN packets all at once: there will be a lot of traffic on the web server which will not make the webpage available to be accessed by the employee visitors. Explain what the logs indicate and how that affects the server: The logs indicate that there’s a SYN flood attack on the web server and it will affect the server cause employee visitors won’t be able to access the web page, which might cause lost of customers.