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: SYN flood attack.The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests. This could be the doing of a threat actor intending to turn down the company's web server causing significant loss. The logs show that: A large number of SYN requests were sent to the server by a specific IP address. The two types of errors in the logs include: ● 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 would be sent to the requesting visitor if the [SYN, ACK] packet is not received by the web server. RST stands for reset, acknowledge. The visitor will 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. This event could be: A 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. A [SYN] request is sent by the client to the server requesting permission to synchronize and form a secure connection. 2. The server sends back a [SYN, ACK] packet to the client acknowledging the synchronization request and giving the green light to form a connection to initiate secure data transfer. 3.The client responds with [ACK] packet acknowledging the server's acknowledgement. This completes the establishment of secure connection between the client and server. Data can now be streamed securely through this network.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When the number of SYN requests is greater than the number of resources available with the server, the server gets overwhelmed by the number of requests and crashes. This is a network level denial of service (DoS) attack, called a SYN flood attack, that targets network bandwidth to slow traffic. A SYN flood attack simulates a TCP connection and floods the server with SYN packets.

Explain what the logs indicate and how that affects the server:
The logs indicate Initially, the attacker's SYN request is answered normally by the web server. However, the attacker keeps sending more SYN requests. Eventually, 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.This is proven in the logs by the failed communications between legitimate employee website visitors and the web server.
From log item number 125 on, the web server stops responding. The only items logged at that point are from the attack. As there is only one IP address attacking the web server, it can be assumed that this is a direct DoS SYN flood attack.