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 server is unable to treat all the syn packets sent to it .

The logs show that: Multiple syn requests sent to the a server from a single IP address

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.The client initiates the connection by sending a SYN packet to the server. This packet includes a randomly generated sequence number, used to track the data flow.

2. The server responds with a SYN-ACK packet. This packet acknowledges the client's SYN by including the client's sequence number incremented by one, and also includes a randomly generated sequence number for the server's own data flow.

3.The client sends an ACK packet to the server, acknowledging the server's SYN-ACK. This packet includes the server's sequence number incremented by one.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: A SYN flood attack simulates a TCP connection and floods the server with SYN packets rendering unable to respond to the requests if the number of SYN requests is greater than the server resources available to handle the requests .

Explain what the logs indicate and how that affects the server:
the web server stops responding to legitimate employee visitor traffic. The visitors receive more error messages indicating that they cannot establish or maintain a connection to 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. Here is tow error messages observed in the logs :An HTTP/1.1 504 Gateway Time-out (text/html) error 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 .