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 web server is having to keep up with the abnormal number of SYN requests coming in at a rapid pace.

The logs show that:

- 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: The only items logged at that point are from the attack. As there is only one IP address attacking the web server, we 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. SYN Packet: Synchronization Packet from Client system, that contains the message it wants to establish a connection with the Server.
2. SYN/ACK Packet: Synchronization / Acknowledgement Packet from the Server, which states that it accepts the connection request from the Client, in response to the request packet.

3. ACK Packet: Acknowledgement Packet from the Client machine that it has understood that server is connected, after this packet it would start sending the necessary work stuff to the server.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: the web server stops responding.

Explain what the logs indicate and how that affects the server: 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. The attacker is sending several SYN requests every second. The rows highlighted and labeled yellow are failed communications between legitimate employee website visitors and the web server.