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: A SYN flood attack that is caused by mass SYN requests which then subsequently overwhelm the web server and prevent visitors from securing a connection with the site.

The logs show that: A large number of SYN requests were sent from a single IP without completing the standard three-way handshake. Some errors in the log include:

- HTTP/1.1 504 Gateway Time-out: generated because the webpage took too long to load
- [RST, ACK] packet: generated because the requesting visitor did not receive the packet from the webpage (reset, acknowledge)

This event could be: A DoS attack on the webserver where the attacker aims to bring down the site.

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]: Synchronize, the initial request received from the site visitor to establish a connection

2. [SYN, ACK]: Synchronize-acknowledge, the server responds to the visitor request by acknowledging the request and prepping to establish a connection

3. [ACK]: Acknowledge, visitors machine acknowledging permission to connect

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When an attacker sends a large number of SYN packets at once without the handshake, the server holds initial SYN requests and allocates resources for them waiting for the ACK requests. However, ACK requests never arrive and the server is left holding uncompleted connections eventually leading to resource exhaustion.

Explain what the logs indicate and how that affects the server: The logs indicate an abnormal amount of SYN requests from a single IP location without the ACK request going through. The server is then left in a continuous state of waiting for complete connections

from initial requests, resulting in timeouts and backlogs that overwhelm the server resources.