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 TCP SYN flood attack, which is a type of Denial-of-Service (DoS) attack that overwhelms a server by sending an excessive number of SYN requests.

The logs show that:

A single unfamiliar IP address, 203.0.113.0, repeatedly sends thousands of SYN packets to the web server at 192.0.2.1 with no attempt to complete the TCP handshake. These packets appear continuously and rapidly across the log (for example, entries 52, 57, 59, and then every few milliseconds through entries 119–152)

Wireshark TCP_HTTP log - TCP log

Meanwhile, legitimate employee traffic (198.51.100.x) begins failing with reset packets and gateway timeout errors.

This event could be:

A direct DoS SYN flood attack from a single attacking source, since all malicious traffic originates from the same IP and overwhelms the server's ability to respond to legitimate requests, as explained in the course reading's description of SYN flood behavior

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 – The client sends a SYN packet to request a connection.

2. SYN-ACK – The server responds with SYN-ACK, reserving resources for the connection.

3. ACK – The client replies with ACK, completing the handshake and opening the session.
   (Example of normal traffic: log entries 47–51 showing a complete handshake followed by an HTTP GET request

Explain what happens when a malicious actor sends a large number of SYN packets all at once:

When an attacker sends a massive number of SYN packets without completing the handshake, the server allocates connection resources for each “half-open” connection and quickly becomes overloaded. Since the attacker never replies with the final ACK, the server’s connection table fills up, preventing it from accepting new connections. This leads to slow responses, dropped connections, and eventually full service outages.

Explain what the logs indicate and how that affects the server:

The logs show the attacking IP repeatedly flooding the server with SYN packets at extremely high frequency (for example, entries 52–54, 57, 59, and then a continuous stream from entries 119–152) while legitimate employee requests begin failing with 504 Gateway Timeout errors and RST, ACK resets (e.g., entries 73, 77, 80, 121)

Wireshark TCP_HTTP log - TCP log

According to the reading, this pattern matches a SYN flood in which the web server becomes overwhelmed and unable to respond to legitimate traffic. As the attack intensifies, the server stops responding entirely after log entry 125, where only attacker traffic remains and the web server no longer processes any employee requests

How to read a Wireshark TCP_HTT…

As a result, the server becomes unreachable, causing employees to receive timeout errors and blocking all access to the company’s website.