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 DoS attack, in which the attacker sends a continuous stream of SYN packets to the server, exhausting its available connection resources.

The logs show that: IP 203.0.113.0 repeatedly sends SYN packets without completing the handshake, overwhelming the server.

This event could be: 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. visitor sends an SYN packet to initiate the connection

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

3. visitor sends back and ACK to complete the handshake, establishing a TCP connection

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends a large number of SYN packets at once, the server's connection table becomes full, preventing legitimate visitors from completing the handshake

Explain what the logs indicate and how that affects the server: Initially, normal employees complete the handshake and request pages successfully (highlighted in green). The attacker (IP 203.0.113.0, red) continuously sends SYN packets without completing the handshake. The server eventually cannot respond to legitimate traffic, resulting in errors RST-ACK packets to visitors and HTTP 504 Gateway Time-out. The web server becomes unavailable to legitimate users, while still logging only the attacker's requests.