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 overwhelmed by a large number of half-open TCP connections caused by incomplete connection attempts, which consume system resources and prevent new, legitimate connections from being established.

The logs show that: The network traffic logs display a continuous stream of TCP packets with the `[SYN]` flag sent from the IP address `203.0.113.0` to the server `192.0.2.1` on port `443`. These connection requests are not being completed with an ACK response, indicating a flood of incomplete handshakes. This pattern is consistent with malicious activity aimed at exhausting the server's connection table.

This event could be: A **Denial-of-Service (DoS) attack**, specifically a **TCP SYN Flood**, where an attacker sends a high volume of TCP SYN packets to exhaust server resources, preventing legitimate users from accessing the website.

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 (synchronize) packet to the server to initiate the connection.
2. **SYN-ACK** – The server responds with a SYN-ACK (synchronize-acknowledge) packet to acknowledge the request and synchronize with the client.
3. **ACK** – The client replies with an ACK (acknowledge) packet, completing the handshake and establishing the connection.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor floods the server with a large volume of SYN packets without completing the handshake, the server allocates resources for each of these half-open connections, waiting for the final ACK. Eventually, the server's connection table becomes full, and it cannot handle legitimate requests. This is known as a **TCP SYN Flood attack**, a type of DoS (Denial of Service).

Explain what the logs indicate and how that affects the server: The packet logs show an unusually high number of SYN requests coming from a single IP address (`203.0.113.0`) to the server (`192.0.2.1`) on port `443`. These requests are not followed by ACKs, confirming that the handshake is never completed. As a result, the server is overwhelmed by half-open connections, which leads to slowdowns and prevents legitimate users from accessing the website. This causes timeouts and 504 errors (Gateway Timeout), impacting business operations and customer experience.