Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

Based on the packet capture logs from Wireshark, we observed a **large number of TCP SYN packets** originating from a single IP address (`203.0.113.0`). These repeated SYN packets flood the server, exploiting the **TCP three-way handshake**, which requires the server to maintain connection state for each incoming SYN.

This indicates a SYN Flood attack, which is a type of **Denial of Service (DoS) attack**. Since most packets are coming from a single IP, this appears to be a **DoS rather than a DDoS**, which would involve multiple source IPs.

Section 2: Explain how the attack is causing the website to malfunction

Normal TCP handshake:

- Client sends **SYN** to initiate a connection.
- Server replies with **SYN-ACK**.
- Client completes handshake with **ACK**, and the connection is established.

During the attack:

- The attacker sends **a large number of SYN packets simultaneously**.
- The server allocates resources for each incomplete connection and quickly becomes **overloaded**.
- Legitimate users cannot establish connections, resulting in timeouts and website unavailability.

Log evidence:

- Logs show an **abnormally high number of TCP connection attempts** from `203.0.113.0` in a very short period.
- All packets are SYN requests, consistent with a SYN flood.
- The server cannot respond to legitimate traffic, confirming a **DoS attack**.