# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| Based on the provided packet capture data, it appears that there is a significant amount of SYN flood traffic directed towards the destination server (192.0.2.1) on port 443. This pattern is evident from the repeated "SYN" packets from various source IP addresses to the destination IP address. This type of network behavior is indicative of a Distributed Denial of Service (DDoS) attack, specifically a SYN flood attack.  In a SYN flood attack, the attacker sends a large number of SYN packets to a target server without completing the full TCP handshake process. This floods the server's resources, causing it to become overwhelmed and unable to respond to legitimate connection requests. The goal of such an attack is to consume the server's resources, rendering it unavailable to legitimate users.  In the provided packet capture, you can see numerous "SYN" packets being sent from multiple source IP addresses to the same destination IP address and port. Additionally, there are no corresponding "ACK" responses, indicating that the full TCP handshake is not being completed, which is characteristic of a SYN flood attack. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| In a normal scenario, when a client (user's device) wants to establish a connection to a server, it goes through a three-way handshake process:  SYN (Synchronize) - The client sends a SYN packet to the server to initiate a connection request.  SYN-ACK (Synchronize-Acknowledge) - The server responds with a SYN-ACK packet, acknowledging the request and indicating its willingness to establish a connection.  ACK (Acknowledge) - Finally, the client sends an ACK packet back to the server, and the connection is established. After this, data transfer can occur.  In a SYN flood attack, the attacker sends a large volume of SYN packets to the target server, but they do not send the final ACK packets to complete the handshake. This causes the server to keep waiting for the ACK that never arrives, as the requests are often coming from fake or non-responsive source IP addresses.  As a result, the server's resources, such as available ports and memory, become tied up with these half-open connections. It has a limited backlog of half-open connections it can maintain, and when this limit is reached, the server cannot accept legitimate connection requests from actual users. This leads to a situation where legitimate users trying to access the website can't establish connections, resulting in a denial of service.  In addition to consuming server resources, the attack can also lead to network congestion, as all the SYN packets flood the network, causing a slowdown in overall network performance.  So, in summary, the SYN flood attack causes the website to malfunction by overwhelming the server's resources with half-open connections, making it unable to respond to legitimate connection requests and effectively denying access to legitimate users. |