# Cybersecurity Incident Report

## Scenario:

**You work as a security analyst for a travel agency that advertises sales and promotions on the company's website. The employees of the company regularly access the company's sales webpage to search for vacation packages their customers might like.**

**One afternoon, you receive an automated alert from your monitoring system indicating a problem with the web server. You attempt to visit the company's website, but you receive a connection timeout error message in your browser.**

**You use a packet sniffer to capture data packets in transit to and from the web server. You notice a large number of TCP SYN requests coming from an unfamiliar IP address. The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests. You suspect the server is under attack by a malicious actor.**

**You take the server offline temporarily so that the machine can recover and return to a normal operating status. You also configure the company's firewall to block the IP address that was sending the abnormal number of SYN requests. You know that your IP blocking solution won't last long, as an attacker can spoof other IP addresses to get around this block. You need to alert your manager about this problem quickly and discuss the next steps to stop this attacker and prevent this problem from happening again. You will need to be prepared to tell your boss about the type of attack you discovered and how it was affecting the web server and employees.**

| Section 1: Identify the type of attack that may have caused this network interruption |
| --- |
| A likely cause of the website's timeout errors is a **SYN Flood attack**, a form of Distributed Denial of Service (DDoS). Packet analysis revealed a significant surge in TCP SYN requests targeting destination IP `192.0.2.1` across multiple ports. This abnormal traffic pattern, likely originating from source IP `203.0.113.0`, is characteristic of a SYN Flood, in which an attacker sends a high volume of TCP connection requests without completing the handshake—ultimately exhausting the server's resources. |

| 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:<br>1. A Request is made to the server<br>2. The server responds with a SYN/ACK<br>3. The requestor responds back with an ACK<br>4. If the connection is successful - TCPhandshake is complete.<br>During a SYN Flood, the attacker sends numerous SYN packets but intentionally omits the final ACK. This leaves the server with a backlog of half-open connections, each of which consumes memory and processing capacity. As the queue fills, the server becomes unable to respond to legitimate connection requests. The logs clearly indicate the early stages of such an attack; if left unaddressed, this behavior could lead to full denial-of-service, rendering the website inaccessible to both internal staff and external users. |