# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| The network traffic capture showed a large volume of **TCP SYN packets** coming from an unfamiliar IP address.  These SYN packets were **not followed by proper ACKs**, resulting in many **half-open connections**.  The server could not handle this volume of incomplete handshakes, leading to **resource exhaustion** and **timeout errors**.  This indicates a **TCP SYN flood**, which is a **type of Denial-of-Service (DoS) attack**. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| * The issue was first identified when the **monitoring system alerted you** to abnormal behavior on the web server. * Employees confirmed they were unable to load the webpage due to **connection timeouts**. * You used a **packet sniffer** to identify a flood of **TCP SYN requests from a suspicious IP**. * The server was being overwhelmed, and unable to respond to real traffic. * **You blocked the IP address and took the server offline temporarily** to recover. * However, IP blocking is a temporary fix — attackers can easily **spoof different IPs**. * The suspected root cause is a **SYN flood attack** intended to **exhaust server resources** and cause a **Denial of Service**. * To prevent future attacks, implement:    + **SYN cookies**   + **Firewall rate-limiting**   + **DDoS mitigation tools**   + **IDS/IPS monitoring** |