# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| The logs show a large number of TCP SYN requests originating from an unfamiliar IP address, overwhelming the web server. This event could be a Denial of Service (DoS) attack.A DoS attack is a cyberattack intended to disrupt a service or resource by overwhelming it with traffic. In this case, the attacker is flooding the web server with SYN packets, preventing it from establishing legitimate connections and processing requests.  This specific type of DoS attack is often referred to as a SYN flood attack. | |
|

| **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:  Three-Way Handshake:   1. SYN: The client sends a SYN packet to the server, requesting a connection. 2. SYN-ACK: The server receives the SYN packet and responds with a SYN-ACK packet, acknowledging the request and initiating the connection. 3. ACK: The client receives the SYN-ACK packet and sends an ACK packet back to the server, confirming the connection.   Malicious Actor Sending a Large Number of SYN Packets:  When a malicious actor sends a large number of SYN packets all at once, it overwhelms the server's resources. The server is forced to allocate resources for each incoming SYN packet, expecting a subsequent ACK packet to complete the connection. However, the attacker doesn't send the ACK packets, leaving the server with a large number of half-open connections.  Log Indications and Server Impact:  The logs indicate a large number of TCP SYN requests coming from an unfamiliar IP address. This suggests that the server is being flooded with connection requests.  The impact on the server is significant:   * Resource Exhaustion: As the server allocates resources for each half-open connection, it eventually runs out of available resources, such as memory and CPU cycles. * Service Disruption: The server becomes unable to handle legitimate connection requests from other clients, leading to service outages and performance degradation. * Security Risk: The attacker could potentially exploit vulnerabilities in the server's software or configuration to gain unauthorized access. |