# Cybersecurity Incident Report

**Date of Report:** July 28, 2025

**Subject:** Analysis of Network Interruption and Website Unavailability

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| An analysis of the provided network traffic logs reveals that the organization's web server was the target of a Denial of Service (DoS) attack. Specifically, a TCP SYN Flood attack was initiated from the IP address 203.0.113.0. This attack overwhelmed the server's resources, causing the website to become slow and inaccessible to legitimate users, resulting in connection timeout errors. This report details the nature of the attack, its effects, and potential mitigation strategies. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| **Description of the Attack**  The attack was a classic **TCP SYN Flood**. Here are its main characteristics as seen in the logs:   * **High Volume of SYN Packets:** The attacker's machine (203.0.113.0) sent a continuous stream of SYN packets to the organization's web server (192.0.2.1). This is the first step in establishing a normal TCP connection. * **Incomplete Handshakes:** The attacker never sent the final ACK packet to complete the connection. This left the server waiting with many "half-open" connections. * **Resource Exhaustion:** Each half-open connection consumes server memory and processing power. By creating thousands of them, the attack depleted the server's resources, preventing it from functioning correctly.   **Effect on the Organization's Network**  The primary effect was on the web server, which hosts the organization's website. By overwhelming the server, the attack made the website and any associated online services completely unavailable to the outside world. Legitimate traffic, like the user at 198.51.100.23 trying to access sales.html, was blocked because the server was too busy handling the flood of fake requests.  **Potential Consequences of the Attack**  This type of service interruption can have significant negative consequences for an organization, including:   * **Financial Loss:** If the website is used for sales or customer transactions, any downtime directly results in lost revenue. * **Reputational Damage:** An unavailable website can frustrate customers and partners, damaging the organization's reputation for reliability and security. * **Operational Disruption:** Employees, partners, or customers who rely on the website for information or services are unable to perform their tasks. * **Loss of Customer Trust:** Users may lose confidence in the organization's ability to protect its digital assets and may take their business elsewhere. |