# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| After thoroughly checking through all the logs the most likely cause for the website’s connection timeout is a SYN Flood attack, which Is a form of DoS(Denial of Service) attack.  This is based on the observation that:   1. The suspicious IP address 203.0.113.0 has sent multiple TCP SYN packets to the webserver 192.0.2.1 without completing the TCP three-way-handshake (SYN – SYN, ACK- ACK). 2. These incomplete handshakes are an indication of an attempt to exhaust the server resources and deny service to legitimate users which is the main motive of the SYN Flood DoS attack. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| Normally, users connect to a web server via a TCP 3-way handshake:   1. SYN: Client -> Server. The client requests the server. 2. SYN-ACK: Server -> Client. The server acknowledges the clients synchronization request and responds. 3. ACK: Server -> Client. Server completes the connection and webpage is loaded.   When a SYN Flood attack occurs, the attacker sends numerous SYN packets without completing the handshake. This causes the server to allocate resources for each half-open connection and wait for ACKs that never arrive. Eventually, the server reaches its limit of pending connections and stops accepting legitimate ones.  Log Evidence: Repeated SYN packets from 203.0.113.0 to 192.0.2.1.443.  Connections from normal clients like 192.0.2.1.443 succeed initially but later entries show RST, ACK responses and Connection Reset, indicating resources exhaustion leading to server not responding. |

|  |
| --- |
| **Section 3: Recommend a response plan for your team and company** |
| To address this attack and prevent recurrence, we recommend the following action plan:  **Immediate Response**   * Inform the network or security team about the unusual traffic from the IP address 203.0.113.0 and have them investigate further. * Temporarily block the IP address if confirmed to be the source of malicious traffic. * Restart the affected server or services to clear any stuck or half-open connections.   **Future Prevention**   * Deploy a DDoS protection service. * Install and configure Intrusion Detection and Prevention Systems (IDPS) to detect unusual TCP SYN behaviour. * Conduct regular network audits and penetration testing. * Add Rate-limit SYN packets to Future Prevention as a technical mitigation. |

|  |
| --- |
| **Section 4: Describe how to communicate the issue to customers** |
| We’re currently experiencing technical difficulties that may affect website access. Our team is actively working to resolve the issue. We appreciate your patience and will provide updates as soon as possible. |