# Cybersecurity Incident Report Submitted by Junior SOC Analyst : M.Murtaza

|  |
| --- |
| **The type of attack that may have caused this**  **network interruption** |
| One potential explanation for the website's connection timeout error message is: The website is experiencing a SYN flood attack, where a malicious actor sends a high volume of TCP SYN packets from a single IP address (203.0.113.10), overwhelming the server’s connection table. This causes the server to be unable to process legitimate connection requests, resulting in timeout errors for users.  The logs show that: The server logs indicate a large number of half-open TCP connections due to an influx of SYN packets without corresponding ACK responses. The TCP backlog queue is overflowing, and the server is experiencing high CPU and memory usage, leading to increased latency and dropped connections.  This event could be: A targeted Denial of Service (DoS) attack aimed at disrupting the availability of the website. The use of a single, non-spoofed IP suggests it may be an intentional act by a malicious actor to exhaust server resources, potentially for competitive sabotage, extortion, or testing vulnerabilities. |
|

|  |
| --- |
| **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. The three way handshake Is explained below:  1. **SYN**: The client sends a SYN (synchronize) packet to the server, requesting a connection and specifying an initial sequence number.  2. **SYN-ACK**: The server responds with a SYN-ACK (synchronize-acknowledgment) packet, acknowledging the client’s SYN, providing its own sequence number, and allocating resources for the connection.  3. **ACK**: The client sends an ACK (acknowledgment) packet to confirm receipt of the SYN-ACK, completing the handshake and establishing the connection.  ATTACK EXPLAINATION  When A malicious actor sends numerous SYN packets, initiating TCP handshakes. The server responds with SYN-ACKs and allocates resources, but the attacker doesn’t send ACKs, leaving half-open connections. This fills the server’s backlog queue, exhausting resources and blocking legitimate connections, causing website timeouts.      What Logs are showing  The logs show a high volume of SYN packets from a single IP (203.0.113.10) with no corresponding ACK responses, resulting in a backlog queue overflow and numerous half-open connections. The server’s CPU and memory usage are near capacity (e.g., 95%), indicating resource exhaustion. This affects the server by:   * **Blocking Legitimate Connections**: The filled backlog queue prevents the server from accepting new connection requests from legitimate users. * **Increased Latency**: Resource exhaustion slows down the server’s ability to process existing connections, causing delays. * **Service Disruption**: The server becomes unresponsive, leading to connection timeouts and website unavailability for users. |