# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| One potential explanation for the website's connection timeout error message is:  A **SYN flood denial-of-service (DoS)** attack overwhelming the web server’s TCP resources on **port 443 (HTTPS)**, causing slow responses and timeouts for legitimate users.  The logs show that:   * A single external IP **203.0.113.0** sends **repeated TCP [SYN]** packets to the web server **192.0.2.1:443** at a rapid pace (marked **red** in the log). Meanwhile, normal employee traffic (198.51.100.x) initially succeeds but then begins to fail. * Legitimate sessions start returning **HTTP/1.1 504 Gateway Time-out** and **[RST, ACK]** errors as the server struggles to complete handshakes. * From log item **125** onward, the server stops responding to employees; entries are **only from the attacker**, confirming resource exhaustion.   This event could be:  A **direct DoS SYN flood** (single attacking IP) that simulates connection starts without completing them, consuming server resources and degrading availability. | |
|

| **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:   1. The client sends **[SYN]** to start a session. 2. The server replies **[SYN, ACK]** to acknowledge and reserve resources. 3. The client sends **[ACK]**, and application data (e.g., **HTTP GET**) follows on success.   Explain what happens when a malicious actor sends a large number of SYN packets all at once:  The server allocates half-open connection resources for each **[SYN]** but never gets the final **[ACK]**. In a **SYN flood**, this backlog fills up, preventing new legitimate handshakes from completing; users experience slow loading and **timeouts**.  Explain what the logs indicate and how that affects the server:   * Early “green” entries show normal handshakes and **HTTP 200 OK** responses; then **red** entries from **203.0.113.0** spike with continuous **[SYN]** packets; **yellow** entries appear as the server sends **[RST, ACK]** and gateways return **504** errors to employees. Finally, after item **125**, only attack traffic remains, demonstrating that the server’s TCP resources are saturated, so **legitimate users cannot establish or maintain connections**.  How to read a Wireshark TCP\_HTT…   **Name of the network intrusion attack:**  **SYN flood (DoS)** targeting TCP/443 of the web server.  **How it negatively impacts network performance:**  Exhausts the web server’s connection backlog, **degrades availability**, and causes **connection resets** and **gateway timeouts** for legitimate users attempting to reach the site. |