# 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 denial‐of‐service (DoS) attack in the form of a SYN flood. The logs show that while normal employee traffic (from IPs in the 198.51.100.0/24 range) successfully completes the TCP three‐way handshake and accesses the sales.html page, the attacker's IP (203.0.113.0) continuously sends an abnormally high number of SYN packets. This barrage of connection requests overwhelms the web server’s available resources, eventually preventing it from processing legitimate requests. Since all malicious traffic originates from a single IP address, this event is classified as a direct DoS attack rather than a distributed denial‐of‐service (DDoS) attack. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| When a website visitor attempts to establish a connection with the web server, the following three-way handshake normally occurs using the TCP protocol:   1. **SYN:** The visitor’s client sends a SYN packet to the server to request a connection. 2. **SYN, ACK:** The server responds with a SYN, ACK packet, indicating its readiness to establish the connection and reserving resources. 3. **ACK:** The client sends an ACK packet to complete the handshake, resulting in a fully established connection.   In a SYN flood attack, a malicious actor sends a large number of SYN packets without following up with the final ACK. This results in numerous half-open connections that consume the server’s connection table and other system resources. As the logs indicate, the attacker's repeated SYN packets (evidenced by the constant, unacknowledged SYN requests from 203.0.113.0) interfere with normal operations. Consequently, when legitimate employees try to connect, their connection attempts time out or are reset (as seen with the HTTP 504 Gateway Timeout errors and [RST, ACK] responses). This resource exhaustion prevents the server from properly establishing or maintaining valid connections, ultimately causing the website to malfunction and significantly degrading network performance. |