# 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:  The server is experiencing a Denial of Service (DoS) attack known as a **SYN flood attack**, where an attacker sends a large number of TCP SYN packets to initiate many half-open connections.  The logs show that:  The IP address 203.0.113.0 sent repeated TCP SYN requests without completing the three-way handshake. Eventually, the server stopped responding to legitimate user requests and produced errors like 504 Gateway Timeout.  This event could be:  A **SYN flood DoS attack**, where a single attacker is attempting to exhaust server resources, causing service outages and blocking employee access to the website. |
|

|  |
| --- |
| **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 a SYN packet to the server to initiate a connection.  2. The server responds with a SYN-ACK to acknowledge the request.  3. The client replies with an ACK to confirm the connection is established.  Explain what happens when a malicious actor sends a large number of SYN packets all at once:  The attacker sends many SYN requests but does not complete the handshake. The server allocates resources for each request, eventually exhausting its capacity and preventing it from processing legitimate traffic.  Explain what the logs indicate and how that affects the server: The logs show many SYN packets from the attacker's IP 203.0.113.0. The server initially responds but becomes overwhelmed. As a result, it cannot finish handshakes with legitimate users and sends timeout errors or resets (RST/ACK), causing website failures. |