Incident Report: SYN Flood Attack 2024-05-13 #2

Globe Sistemas - Av. Libertador Jardin America

| **Part 1: Identify the type of attack that may have caused this network outage** |
| --- |
| One possible explanation for the website down connection timeout error message is a DoS attack. The logs show that the web server stops responding after being overloaded with SYN packet requests. This event could be a type of DoS attack called a SYN flood. |

| **Part 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. The handshake consists of three steps:   1. A SYN packet is sent from the source to the destination, requesting to connect. 2. The destination responds to the source with a SYN-ACK packet to accept the connection request. The destination will reserve resources for the source to connect. 3. A final ACK packet is sent from the source to the destination acknowledging permission to connect.   In the case of a SYN flood attack, a malicious actor will send a large number of SYN packets at once, overwhelming the server's available resources to reserve for the connection. When this happens, there are no server resources left for legitimate TCP connection requests.  The logs indicate that the web server has been overwhelmed and is unable to process SYN requests from visitors. The server is unable to open a new connection for new visitors receiving a connection timeout message. |