

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 flood of too many SYN packets.

The logs show that: there has been an overflow of SYN packets.

This event could be: a SYN flood attack.

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 device sends a SYN request to the server for a TCP connection to be established.
2. The server responds with a SYN/ACK packet, acknowledging the request.
3. The device sends an ACK packet, yes, the device sends an ACK packet and a TCP connection is established.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: the network server crashes.

Explain what the logs indicate and how that affects the server: They indicate a flood of too many SYN packets and that crashes the server.