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:Validating this, we can see from the text that after a large number of SYN packet requests to the server, the maximum number of responses was exceeded, causing the server to crash. This led to the server no longer accepting requests, resulting in a connection timeout error in your browser.

The logs show that: A large number of TCP SYN requests from an unknown IP address.

This event could be:SYN 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. TCP packet is sent from the user to the host

2. TCP packet is received by the host and sent to the user, SYN/ACK packet to start the connection

3. ACK packet is sent to the server, granting it a secure port for the connection

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When the hacker sends a large number of SYN packets, the server becomes slow, but when it reaches the maximum, the server stops accepting packet requests and stops.

Explain what the logs indicate and how that affects the server:

Christian Danglades