Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

This afternoon, I received an alert indicating that the website was experiencing performance issues. When I attempted to access the website, I received a connection timed out error.

I investigated the issue further and found that the website was receiving an abnormally large number of TCP SYN requests from an unfamiliar IP address. These requests were not completing the three-way handshake, which is a normal part of the TCP protocol. This indicates that the requests were likely part of a SYN flood attack.

Section 2: Explain how the attack is causing the website to malfunction

When a website visitor tries to connect to a web server, they send a SYN packet to the server. The server responds with a SYN-ACK packet, reserving resources for the connection. The visitor then sends an ACK packet to acknowledge the connection.

In a SYN flood attack, a malicious actor sends a large number of SYN packets to the server. The server reserves resources for each of these connections, even though they are not legitimate. This eventually overwhelms the server's resources, and it is unable to process any more SYN packets.

As a result, legitimate visitors are unable to connect to the server. They receive a connection timeout message, indicating that the server is unavailable.