

Cybersecurity Incident Report

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

The attack that caused the network interruption was a DoS made with a SYN flood

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

The ip 203.0.113.0 starts a TCP connection with us, but after the SYN, SYN/ACK and ACK he starts a SYN flood attack, after some SYN requests another user starts to get the RST, ACK indicating that the connection has been affected.

The logs indicate that the web server has become overwhelmed and is unable to process the visitors' SYN requests. The server is unable to open a new connection to new visitors who receive a connection timeout message.