

Cybersecurity Incident Report

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

The attack most likely the cause of the incident is Denial of service attack and to be precise a SYN Flood attack

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

The IP address 203.0.113.0 is overloading our network with a SYN Flood attack since they're sending multiple SYN packets all at once. This uses up the company's resources to acknowledge these packets according to the TCP protocol and any new visits to the site are timed out. Thus it becomes a denial of service.