Incident Analysis

Log Analysis

Upon examining the Wireshark logs, we identified a significant traffic anomaly originating from IP address 203.0.113.0. Initially, this IP attempted to establish a connection with our server by sending a SYN packet, to which our server responded with a SYN-ACK packet. However, instead of completing the TCP handshake, the IP address in question proceeded to flood our server with an excessive number of SYN packets. This behavior is indicative of a potential SYN flood attack, aimed at overwhelming our server's resources and disrupting its normal functioning.

Consequences of a SYN Flood Attack

1. Legitimate TCP connection requests are denied due to resource unavailability.
2. The web server becomes overwhelmed, unable to process incoming SYN requests.
3. New visitors experience connection timeouts, as the server cannot establish new connections.

Recommended Actions

1. Implement SYN flood mitigation measures (e.g., SYN cookies, rate limiting).
2. Block malicious IP addresses.
3. Monitor server resources and adjust capacity as needed.