Cybersecurity Incident Report

Prepared By: Dhyanam
Role: Cyber Security Student (Training)
Year: 2025

Scenario Summary: A travel agency’s web server became unresponsive after employees reported connection timeout errors while accessing the company’s sales webpage. Packet capture analysis revealed an unusually high volume of TCP SYN requests originating from an unfamiliar IP address. The excessive SYN traffic overwhelmed the server’s ability to complete TCP handshakes, indicating a likely SYN flood attack designed to exhaust server resources and disrupt normal operations. The server was temporarily taken offline to recover, and the malicious IP was blocked at the firewall. Further action is required to prevent repeated attacks, as the attacker can easily spoof additional IP addresses to bypass simple blocking measures.

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: The website is showing a connection timeout error when tried to access on the browser which can be due to a DoS attack which could be carried out on the web server. The logs show that there is a legitimate user who successfully established TCP connection with the web server and also accessed the sales website successfully but then suddenly there is one malicious IP address 203.0.113.0 which starts flooding the web server with SYN flag requests on port 443 by which the web server gets overwhelmed.

This event could be a SYN flood attack which is a type of Dos (Denial Of Service) attack where the attacker disrupts the normal business operations by overloading the organization’s network with unwanted network traffic.

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. The three steps of the handshake:

1. SYN: The client sends a SYN flag to request a connection.
2. SYN-ACK: The server replies with a SYN-ACK packet to acknowledge and synchronize.
3. ACK: The client responds with an ACK packet to confirm, establishing the connection.

So when the attacker sends the server with a large number of SYN requests the server gets overwhelmed and does not know what to do with this sudden flood of SYN packets so starts using the RST flag which the emergency brakes of TCP connection use when the communication must stop immediately rather than ending politely.