Cybersecurity Incident Report

Incident Report for: Travel Agency Website Server Attack

Section 1: Summary of the Problem Found in the Network Traffic Log

The network protocol analyzer logs indicate a large number of TCP SYN requests coming from an unknown IP address. This surge in SYN requests has overwhelmed the web server, causing it to lose its capacity to respond to legitimate traffic and resulting in connection timeouts for users attempting to access the website. This behavior is indicative of a SYN Flood attack, a type of Denial of Service (DoS) attack designed to exhaust the resources of the server by flooding it with half-open connections.

Section 2: Analysis of the Data and One Solution to Implement

Incident Occurrence:

- **Date and Time:** 05/08/2024 16:05
- **Reported by:** Automated system monitoring alerts

Incident Description: Earlier this afternoon, the system monitoring tools alerted us to a problem with the web server. Upon investigation, it was discovered that the server was receiving an abnormally high volume of TCP SYN requests from an unknown IP address. This flood of requests led to the server becoming overwhelmed and unable to respond to legitimate traffic, resulting in connection timeout errors for users.

Analysis of Network Logs:

- The logs show a significant number of TCP SYN packets sent to the server.
- The source IP was consistently sending SYN packets, indicating an attempt to open numerous connections without completing the three-way handshake.
- This pattern is typical of a SYN Flood attack, where the attacker aims to exhaust server resources by creating numerous half-open connections.

Root Cause: The attack is a SYN Flood, a type of Denial of Service (DoS) attack aimed at depleting server resources by overwhelming it with SYN requests.

Proposed Solution:

1. **Immediate Response:**
    - **Disconnect the Server:** Temporarily take the server offline to allow it to recover.
    - **Block the Attacking IP:** Configure the firewall to block the IP address sending the SYN requests.
2. **Long-term Mitigation:**
    - **Implement SYN Cookies:** Use SYN cookies to handle SYN Flood attacks more efficiently without using excessive server resources.
    - **Rate Limiting:** Configure rate limiting on the firewall to restrict the number of SYN requests from a single IP address.
    - **Network Intrusion Detection Systems (NIDS):** Deploy NIDS to monitor and detect unusual traffic patterns in real-time.
    - **Load Balancing:** Use load balancers to distribute traffic and prevent any single server from becoming overwhelmed.

Next Steps:

- Communicate with the IT team to ensure the implementation of SYN cookies and rate limiting.
- Monitor the network traffic closely to identify any further attempts of attack.
- Keep the server administrators and the security team informed about the incident and the mitigation measures being taken.

Conclusion: The SYN Flood attack led to the web server being overwhelmed, resulting in connection timeouts for users. By implementing SYN cookies, rate limiting, and other security measures, we can prevent similar attacks in the future and ensure the stability and availability of the web server.

Reported by: Ezequiel Arce
Cybersecurity Analyst