Cybersecurity Incident Report: SYN Flood Attack

1. Incident Overview

- **Incident Type:**
  SYN Flood Denial of Service (DoS) Attack
- **Incident Description:**
  The web server experienced connection timeouts due to being overwhelmed by a large volume of SYN packets from a malicious source. As a result, legitimate traffic could not be processed in a timely manner, leading to HTTP 504 Gateway Timeout errors and disrupted service for legitimate users.

2. Incident Timeline

- **Date and Time of Incident:**
  17/09/2019
- **Incident Duration:**
  The incident was active for several hours before being identified and mitigated.

3. Attack Overview: SYN Flood

A SYN Flood Attack is a type of Denial of Service (DoS) attack where the attacker sends numerous SYN packets to the target server without completing the TCP handshake. This causes the server to allocate resources for each incomplete connection, eventually overwhelming its ability to process legitimate traffic.

Details of the Attack:

- SYN Flood Detected:
  The server logs revealed a high volume of SYN packets originating from a single malicious IP address: 203.0.113.0, targeting port 443 (HTTPS) on the web server.
- Server Response:
  Initially, the server responded to the incoming SYN requests by sending SYN-ACK packets, attempting to establish a legitimate connection. However, the attacker continued to send SYN packets without completing the handshake, overloading the server.
- Impact on Legitimate Traffic:
  The legitimate visitors attempting to access the website during the attack were unable to establish successful connections. This is evident from the logs, which show HTTP 504 Gateway Timeout errors and [RST, ACK] packets—indicating that the server was overwhelmed and unable to complete connections with real users.

4. Technical Breakdown: TCP Handshake and SYN Flood

The attack exploited the TCP handshake process, which typically follows these steps:

1. SYN Request (Synchronize):
   A visitor (client) sends a SYN packet to the server, signaling an intent to establish a connection.
2. SYN-ACK Response (Synchronize-Acknowledge):
   The server replies with a SYN-ACK, confirming its readiness to establish the connection.
3. ACK Confirmation (Acknowledge):
   The client sends an ACK packet, completing the three-way handshake, and a full TCP connection is established.

Attack Scenario:

During a SYN Flood Attack, the malicious actor sends an excessive number of SYN packets to the server but deliberately fails to send the final ACK packet needed to complete the handshake. As a result:

- The server allocates resources for each SYN request and holds them while waiting for the ACK response, which never arrives.
- When the volume of SYN packets exceeds the server's capacity to handle new connections, it becomes saturated, unable to process legitimate traffic, and eventually times out.

5. Log Analysis and Attack Identification

The following indicators were found in the logs:

- SYN Packet Surge:
  A high volume of SYN packets originating from the malicious IP address (203.0.113.0) was detected, flooding port 443 of the web server.
- Gateway Timeout Errors:
  Numerous HTTP 504 Gateway Timeout errors were observed, highlighting the server's failure to respond to legitimate connection attempts due to the overwhelming SYN flood.
- TCP RST (Reset) Packets:
  [RST, ACK] packets were logged, which indicate that the server had to reset connections with users, unable to complete the handshake due to resource exhaustion.

6. Impact Assessment

- Affected Systems:
    - Web Server: The primary target, affected by resource exhaustion due to the SYN flood.
- Impact on Users:
  Legitimate website visitors experienced connection timeouts and were unable to access the site. The server could not handle real traffic while being overwhelmed by malicious SYN requests.
- Downtime:
  The attack caused X hours of downtime for legitimate traffic before it was mitigated.

7. Mitigation Measures

Immediate Actions:

1. Block Malicious IP Address:
   The identified malicious IP 203.0.113.0 was blocked at the firewall to prevent further SYN flood traffic from reaching the server.
2. Connection Rate Limiting:
   Rate-limiting policies were enforced to restrict the number of SYN packets that can be received from a single source in a given time frame, reducing the likelihood of similar attacks overwhelming the server.
3. Enable SYN Cookies:
   SYN cookies were enabled on the server, a technique that helps mitigate SYN flood attacks by ensuring that the server doesn’t allocate resources until the handshake is fully completed.

Future Preventative Measures:

- Traffic Monitoring and Alerts:
  Implement real-time network traffic monitoring with automatic alerting when anomalous traffic patterns, such as a SYN flood, are detected.
- Distributed Denial of Service (DDoS) Protection:
  Deploy a DDoS protection service to detect and mitigate SYN flood attacks before they reach the server infrastructure.
- Harden Server Configurations:
  Apply server hardening techniques, such as limiting the number of concurrent connections and reducing TCP connection timeouts to minimize the impact of resource exhaustion.

8. Lessons Learned

- Proactive Monitoring:
  Continuous monitoring of network traffic could have helped in detecting the SYN flood earlier, preventing prolonged downtime.

- Rate-Limiting Policies:
  The implementation of rate-limiting policies is crucial to prevent future SYN flood attacks from saturating the server's resources.

9. Action Plan

1. Further Investigation:
   Continue investigating the origins and potential motivations of the attacker to prevent future incidents from the same source.
2. Implement Advanced Security Measures:
   Deploy SYN flood mitigation techniques, such as SYN cookies, DDoS protection, and rate limiting, as a standard defense against this type of attack.
3. Ongoing Monitoring and Response**:**
   Establish an ongoing incident response and monitoring strategy, including continuous traffic analysis and the use of advanced firewalls or IDS/IPS (Intrusion Detection and Prevention Systems).