Cybersecurity Incident Report: Analyze network Attacks

Cybersecurity Incident Report

Incident Summary:

On review of the network traffic logs, the company's web server (IP: 192.0.2.1) experienced service disruption caused by a SYN flood attack. This led to frequent timeout errors and connection resets for employees accessing the website, particularly the sales page. Logs show excessive TCP SYN packets sent from the IP address 203.0.113.0 to the server's port 443, which is used for secure HTTP (HTTPS) traffic. The server began responding slower over time and eventually stopped responding to legitimate traffic entirely.

Incident Analysis:

Network traffic captured using Wireshark revealed:

- Normal traffic initially occurred between employee devices (198.51.100.x) and the web server. These connections followed the standard TCP three-way handshake and HTTP communication flow.
- At timestamp 3.390692, traffic from a suspicious IP address (203.0.113.0) began, sending repeated SYN packets to the web server.
- Although the server responded with SYN-ACK messages, the attacker continually sent new SYNs, overwhelming server resources.
- From log entry 125 onward, no successful legitimate connections were made to the server. The only ongoing traffic was repeated SYN packets from the attacker.
- ICMP echo responses and HTTP 504 Gateway Timeout errors were observed, confirming that the web server failed to handle legitimate requests in a timely manner.
- RST, ACK (Reset Acknowledge) responses were sent to employee IPs, indicating that the server could not maintain or establish connections.

Detection and Response:

- The incident was detected through a combination of automated monitoring alerts and employee reports of website inaccessibility.
- The IT team analyzed the traffic logs and identified the single source IP (203.0.113.0) responsible for the high-volume SYN traffic.
- The server was temporarily taken offline to stabilize performance.
- A firewall rule was implemented to block traffic from the attacking IP address.

Key Findings:

- Attack Type: SYN flood attack (DoS — Denial of Service)
- Source IP: 203.0.113.0 (single source, not distributed)
- Targeted Port: TCP port 443 (HTTPS)
- Symptoms: Connection timeouts, 504 errors, TCP resets
- Impact: Website downtime, blocked employee access, degraded server performance

Conclusion and Recommendations:

The attack was a direct Denial of Service (DoS) SYN flood that exploited the TCP handshake mechanism to exhaust the server’s connection table. To mitigate future risks:

- Implement SYN cookies or rate limiting on TCP connections.
- Use Intrusion Detection/Prevention Systems (IDS/IPS) to detect abnormal traffic patterns early.
- Consider cloud-based DDoS protection services to absorb malicious traffic.
- Monitor logs continuously for repeated patterns from unknown IPs.