Cybersecurity Incident Report

Incident Title: SYN Flood Denial-of-Service Attack
Incident Date/Time: Morning 9AM
Reported By: Security Analyst
Affected System: Corporate Web Server – IP 192.0.2.1
Severity Level: High – Complete service outage of sales page

Executive Summary

At approximately 9am, the corporate website's sales page became unreachable. Network monitoring alerts indicated abnormal inbound traffic. Packet analysis revealed a high volume of TCP SYN packets from IP **203.0.113.0**, overwhelming the server's connection queue. This behavior matches a **SYN Flood Denial-of-Service (DoS)** attack. The server's resources were consumed by half-open TCP connections, preventing legitimate traffic from being processed.

Incident Timeline

Time (LogEntry)	Event	Details
47–51	Normal operation	Complete 3-way handshake and HTTP 200 OK responses observed.
52–61	Attack initiation	Repeated TCP SYN requests from IP 203.0.113.0 to port 443 without completing handshakes.
77	Service degradation	HTTP 504 Gateway Timeout errors to legitimate clients.
125+	Full outage	Log entries dominated by SYN packets from attacker; legitimate traffic unable to connect.

Technical Analysis

Attack Type: TCP SYN Flood (DoS)

- **Mechanism:** The attacker sends excessive SYN packets to initiate TCP connections but never completes the handshake.
- **Impact:** Server allocates resources for each half-open connection until its backlog is exhausted, causing denial of service for legitimate users.

- **DoS vs. DDoS:** This event originated from a **single IP source**, fitting the DoS category. DDoS attacks use multiple distributed sources.

Indicators in Logs:

- Abnormally high SYN rate to TCP port 443.
- Incomplete TCP handshakes.
- HTTP timeout errors and TCP resets sent to real clients.

Business Impact

- **Availability:** Complete outage of the sales page.
- **Operations:** Employees could not access travel package information for clients.
- **Revenue Risk:** Loss of potential sales during downtime.
- **Reputation:** Negative customer perception due to service disruption.

Actions Taken

1. Temporarily removed the web server from service to allow recovery.
2. Configured firewall to block traffic from IP **203.0.113.0**.
3. Monitored recovery and restored service after traffic volume decreased.
4. Documented attack indicators for future threat intelligence.

Root Cause

The outage was caused by a **TCP SYN Flood DoS attack** targeting the HTTPS service (TCP/443) of the corporate web server.
The attacker exploited TCP connection handling to fill the server's backlog with incomplete connections, denying service to legitimate clients.

Recommendations

Immediate Mitigation:

- Enable **SYN cookies** to prevent backlog exhaustion.
- Reduce TCP half-open timeout settings.
- Apply rate limiting per source IP at firewall or load balancer.

- Coordinate with ISP for upstream filtering.

Long-Term Measures:

- Deploy a **Web Application Firewall (WAF)** or **CDN** for traffic absorption and filtering.
- Implement SYN proxy or TCP handshake verification.
- Subscribe to DDoS protection services.
- Maintain and test a DoS/DDoS incident response plan.
- Conduct regular stress testing of infrastructure.

Next Steps

1. Implement recommended mitigation controls within 24 hours.
2. Engage ISP to discuss permanent DoS/DDoS mitigation.
3. Schedule post-incident review with IT and security teams.
4. Update security documentation and response procedures.

Appendix A – Evidence Summary

Example of normal traffic:

47 198.51.100.23 → 192.0.2.1 TCP [SYN]

48 192.0.2.1 → 198.51.100.23 TCP [SYN, ACK]

49 198.51.100.23 → 192.0.2.1 TCP [ACK]

50 HTTP GET /sales.html

51 HTTP 200 OK

Example of attack traffic:

52 203.0.113.0 → 192.0.2.1 TCP [SYN]

57 203.0.113.0 → 192.0.2.1 TCP [SYN]

59 203.0.113.0 → 192.0.2.1 TCP [SYN]

… Repeated continuously without handshake completion …