Subject: URGENT: Web Server Downtime Caused by SYN Flood Attack

Date/Time: April 14, 2025 Reported by: MANJEESWAR KV, Security Analyst

Summary: This afternoon, the company's web server experienced a Denial of Service (DoS) attack. The monitoring system triggered an alert indicating server performance issues. When tested manually, the site produced a connection timeout. A traffic analysis confirmed the presence of a SYN flood attack.

Technical Details:

A large number of TCP SYN packets were detected coming from a single, unfamiliar IP address.

The SYN packets were not followed by ACK packets, preventing the TCP handshake from completing.

The web server became flooded with half-open connections, exhausting its ability to respond to legitimate requests.

This attack method is consistent with a TCP SYN flood, a known DoS attack.

Immediate Actions Taken:

Took the server offline to allow resource recovery.

Blocked the attacker's IP address via firewall rules.

Started evaluating additional mitigation steps such as:

Enabling SYN cookies (a defense mechanism against SYN floods)

Implementing rate limiting on connection attempts

Using a Web Application Firewall (WAF) or DDoS mitigation service

Next Steps:

Monitor traffic for signs of spoofed or rotating IP addresses.

Coordinate with hosting provider or cloud service for upstream traffic filtering.

Implement longer-term protections against volumetric DoS attacks.

Review incident response playbook and ensure all teams are briefed.

Recommendation: Consider deploying advanced DoS protection mechanisms like Cloudflare, AWS Shield, or Akamai for continuous protection against similar future attacks.