Incident Response – SYN Flood Mitigation Actions

1. SYN Cookies Enabled on the Web Server

- The SYN cookie feature was enabled to mitigate the impact of SYN flood traffic and prevent resource exhaustion on the web server.
- This allowed the server to continue processing legitimate connection requests despite the attack.

2. Firewall IP Filtering

- All IP addresses identified in the IDS, kernel logs, and packet capture as sources of the SYN flood were blocked at the firewall:
  - 203.0.113.45
  - 198.51.100.200
  - 198.51.100.71
- Blocking these IPS via the firewall prevented further attack traffic from reaching the web server. Unlike Apache-level IP blocking, which filters traffic at the application level but still consumes server resources, firewall-level filtering stops malicious traffic before it reaches the server.

3. Temporary Rate SYN rate Limiting

- Temporary rate limiting was configured to restrict the number of new connections per IP per second.
- This measure helps protect the web server against potential SYN flood traffic from new or previously undetected malicious IPs.
- The rate limiting is temporary, allowing the server to maintain normal operations while ongoing monitoring is conducted.

Post-Mitigation Status:
Following the immediate implementation of these three-mitigation measure by the cybersecurity team, the web server resumed normal functionality and has remained stable with no further signs of SYN flood activity.

Future Improvements:
Performing regular stress and penetration testing is recommended to simulate SYN flood scenarios and evaluate the network’s resilience under high traffic conditions. These controlled simulations will help assess the effectiveness of current mitigation measures, identify potential bottlenecks, and ensure the web server and firewall configurations remain optimized to withstand future attacks.