Title: NIST Compliant Incident Response Framework Playbook for Application Layer DDoS Attack

* Question: You are a security operations system analyst and helpful cybersecurity assistant that generates detailed incident response playbooks based on NIST guidelines. please generate a playbook for a application-layer DDoS attacks effectively?
* Answer:

1. Preparation:

Objective: Establish contacts, define procedures, and gather information to save time during an incident.

- \*\*Identify Critical Applications\*\*:

- \*\*Documentation\*\*: Create a comprehensive inventory of OT applications such as web interfaces, APIs, SCADA software, HMI, and other monitoring/control systems. Use asset management tools to keep the list updated.

- \*\*Prioritization\*\*: Rank applications based on their criticality using scoring systems that consider dependency, operational impact, and downtime tolerance.

- \*\*Security Assessments\*\*:

- \*\*Regular Assessments\*\*: Schedule and perform vulnerability scans, penetration testing, and code reviews.

- \*\*Third-Party Audits\*\*: Engage external security firms for unbiased audits.

- \*\*Patch Management\*\*: Implement robust patching processes for timely updates.

- \*\*Incident Response Team (IRT)\*\*:

- \*\*Team Formation\*\*: Assemble members from IT, OT, and cybersecurity departments. Include roles such as incident commander, application security experts, and communication leads.

- \*\*Roles and Responsibilities\*\*: Define clear roles and ensure redundancy for critical positions.

- \*\*Training\*\*:

- \*\*Regular Training\*\*: Conduct training sessions with tabletop exercises and simulation drills for application-layer attack scenarios.

- \*\*Awareness Programs\*\*: Educate staff on attack vectors, social engineering tactics, and safe practices.

- \*\*Tools\*\*:

- \*\*Web Application Firewalls (WAF)\*\*: Protect web applications from threats like SQL injection, cross-site scripting (XSS), and HTTP floods.

- \*\*Application Monitoring Tools\*\*: Monitor application performance, user behavior, and transaction anomalies.

- \*\*SIEM Integration\*\*: Centralize application logs in SIEM for real-time analysis and monitoring.

2. Detection and Analysis:

Objective: Detect the incident, determine its scope, and involve appropriate parties.

- \*\*Anomaly Detection\*\*:

- \*\*Behavioral Analytics\*\*: Detect deviations from normal application usage patterns.

- \*\*Threshold Alerts\*\*: Configure alerts for high HTTP requests, failed login attempts, and abnormal API calls.

- \*\*Log Monitoring\*\*:

- \*\*Continuous Monitoring\*\*: Monitor error logs, access logs, and security logs for suspicious activity.

- \*\*Automated Analysis\*\*: Use tools to correlate events and identify threats.

- \*\*Real-Time Alerts\*\*:

- \*\*SIEM Configuration\*\*: Set up alerts for suspicious activity; prioritize alerts based on criticality.

- \*\*Notification Channels\*\*: Use multiple channels (e.g., email, SMS, dashboard alerts) for prompt response.

- \*\*Incident Categorization\*\*:

- \*\*Attack Identification\*\*: Determine the attack type (e.g., HTTP flood, Slowloris, SQL injection) based on symptoms and patterns.

- \*\*Scope Determination\*\*: Assess affected applications, endpoints, and user accounts.

- \*\*Impact Assessment\*\*:

- \*\*Operational Impact\*\*: Evaluate downtime, data integrity issues, and safety risks to OT operations.

- \*\*Resource Utilization\*\*: Assess impact on CPU, memory, and bandwidth.

- \*\*Source Identification\*\*:

- \*\*IP Tracking\*\*: Identify IP addresses involved and analyze geolocation data.

- \*\*User Agent Analysis\*\*: Detect malicious traffic sources.

3. Containment:

Objective: Mitigate the attack’s effects on the targeted environment.

- \*\*Rate Limiting\*\*:

- \*\*Traffic Throttling\*\*: Limit incoming requests to critical applications.

- \*\*Dynamic Controls\*\*: Adjust rate limiting based on traffic patterns and threat levels.

- \*\*Access Control\*\*:

- \*\*Restrict Access\*\*: Temporarily block access to affected applications and endpoints.

- \*\*Multi-Factor Authentication (MFA)\*\*: Enforce MFA for accessing critical systems.

- \*\*WAF Rules\*\*:

- \*\*Custom Rules\*\*: Apply WAF rules tailored to attack patterns.

- \*\*Rule Tuning\*\*: Continuously tune rules to counter evolving threats.

4. Eradication:

Objective: Remove the threat and prevent recurrence.

- \*\*Mitigation Tools\*\*:

- \*\*DDoS Mitigation Services\*\*: Filter and block malicious traffic.

- \*\*Advanced Firewalls\*\*: Employ application-layer filtering.

- \*\*Block IPs/User Agents\*\*:

- \*\*IP Blacklisting\*\*: Block all identified malicious IP addresses.

- \*\*User Agent Blocking\*\*: Restrict suspicious user agents.

- \*\*Patch and Update\*\*:

- \*\*Vulnerability Patching\*\*: Apply patches to close exploited vulnerabilities.

- \*\*Security Updates\*\*: Update underlying systems, libraries, and dependencies.

5. Recovery:

Objective: Restore the system to normal operations.

- \*\*System Checks\*\*:

- \*\*Integrity Verification\*\*: Ensure applications are functional and free of malicious activity.

- \*\*Health Monitoring\*\*: Monitor application performance and security metrics.

- \*\*Traffic Normalization\*\*:

- \*\*Gradual Restoration\*\*: Slowly restore traffic flow, monitoring for residual activity.

- \*\*Baseline Comparison\*\*: Compare traffic patterns with established baselines.

- \*\*Data Integrity\*\*:

- \*\*Data Verification\*\*: Verify that application data and configurations remain intact.

- \*\*Backup Restoration\*\*: Restore corrupted or lost data from secure backups.

6. Lessons Learned:

Objective: Document the incident’s details, discuss lessons learned, and adjust plans and defenses.

- \*\*Documentation\*\*:

- \*\*Incident Report\*\*: Record attack details, detection methods, response actions, timeline, and impact.

- \*\*Lessons Learned\*\*: Note gaps in response and improvement opportunities.

- \*\*Review and Improve\*\*:

- \*\*Post-Incident Review\*\*: Discuss incident response effectiveness with stakeholders.

- \*\*Plan Updates\*\*: Revise IR plans based on findings.

- \*\*Training Update\*\*:

- \*\*Incorporate Learnings\*\*: Update training programs with lessons learned.

- \*\*Ongoing Training\*\*: Schedule regular sessions to maintain readiness.