Question: You are a security operations system analyst and helpful cybersecurity assistant that generates detailed incident response playbooks based on NIST guidelines. Generate a playbook for a Web Application Dos/DDoS Attack.

Answer:

Title: Web Application Dos Attack Response Playbook

1. Preparation:

- \*\*Educate Team\*\*: Train your security and operations teams on recognizing Dos/DDoS attack scenarios, including protocol exploitation and resource exhaustion.

- \*\*Implement Best Practices\*\*: Follow AWS Best Practices for DDoS Resiliency to strengthen application defenses.

- \*\*Monitor Resources\*\*: Configure monitoring tools, such as AWS CloudWatch, to detect abnormal traffic patterns or performance degradation.

- \*\*Incident Response Process\*\*: Establish clear incident response processes and test them regularly via Game Days or simulations.

2. Detection and Analysis:

- \*\*Identify Symptoms\*\*: Look for signs such as degraded service, application unavailability, or increased error rates (e.g., 4xx and 5xx error codes).

- \*\*Analyze Alerts\*\*: Review alerts from monitoring tools like CloudWatch metrics for Amazon EC2, CloudFront, and AWS WAF.

- \*\*Review Logs\*\*: Dive into logs to identify attack signatures, such as unusual IPs, unexpected HTTP verbs, or elevated traffic volumes.

- \*\*Verify Impact\*\*: Confirm the affected application and resources using AWS CMDB or tagged identifiers.

- \*\*Assess Metrics\*\*: Compare current metrics against baseline performance to quantify the scope and severity of the attack.

3. Containment:

- \*\*Scale Resources\*\*: Use AWS Auto Scaling to add capacity and handle traffic spikes.

- \*\*Deploy CloudFront\*\*: Protect the application by setting up a CloudFront distribution as a shielding layer.

- \*\*Restrict Access\*\*: Update DNS records and configure security groups to limit public access.

- \*\*Apply AWS WAF Rules\*\*: Block malicious traffic with AWS Managed Rules or custom Web ACL configurations tailored to attack patterns.

4. Eradication:

- \*\*Review Web ACLs\*\*: Ensure CloudFront and Load Balancers are protected by Web ACLs.

- \*\*Deploy Rules\*\*: Use AWS WAF Managed Rules or work with developers to create custom rules for blocking attack vectors.

- \*\*Validate Protections\*\*: Confirm that the mitigations in place are effectively stopping the attack.

5. Recovery:

- \*\*Compare Metrics\*\*: Analyze pre- and post-mitigation logs to determine the impact of actions taken.

- \*\*Monitor Post-Attack\*\*: Continue observing the application for potential changes in attack methods or behaviors.

- \*\*Restore Services\*\*: Ensure the application is fully operational and accessible to legitimate users.

6. Lessons Learned:

- \*\*Collaborate with Stakeholders\*\*: Conduct a post-incident review with key personnel to assess response effectiveness.

- \*\*Document Findings\*\*: Record lessons learned, including attack vectors, mitigations, and misconfigurations.

- \*\*Update Processes\*\*: Revise the incident response playbook and risk documentation based on new insights.

- \*\*Improve Defenses\*\*: Implement changes in application and infrastructure configurations to address vulnerabilities revealed during the incident.