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 Denial-of-Service (DoS) attack?

Answer:

Title: NIST-Compliant Incident Response Playbook: Denial-of-Service (DoS) Attack

1. Preparation:

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

- \*\*Security Controls\*\*:

- Deploy a Web Application Firewall (WAF) to filter and block malicious traffic.

- Set rate-limiting policies on servers and APIs to handle traffic spikes.

- Enable DDoS protection services (e.g., Cloudflare, AWS Shield).

- \*\*Incident Response Setup\*\*:

- Establish a DoS response team with clear roles and responsibilities.

- Maintain updated network diagrams and asset inventories.

- \*\*User Awareness\*\*:

- Train staff to recognize symptoms of DoS attacks, such as sudden system unavailability.

2. Detection:

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

- \*\*Identify Threat Indicators\*\*:

- \*\*Network Indicators\*\*:

- Sudden spikes in inbound traffic, particularly from a single source or range.

- Multiple repeated requests to a single endpoint.

- Saturation of network bandwidth or server resources.

- \*\*System Indicators\*\*:

- High CPU or memory utilization on affected systems.

- Increased response times or timeouts for legitimate users.

- \*\*Identify Risk Factors\*\*:

- \*\*Common Risks\*\*:

- Temporary unavailability of critical services or websites.

- Financial loss due to service downtime.

- \*\*Company-Specific Risks\*\*:

- Disruption to customer-facing applications, damaging brand reputation.

- Potential exploitation of service downtime for follow-up attacks.

- \*\*Data Collection\*\*:

- \*\*Log Analysis\*\*:

- Review firewall, router, and server logs for abnormal traffic patterns.

- Identify traffic sources, protocols, and frequency of requests.

- \*\*Traffic Analysis\*\*:

- Use network monitoring tools (e.g., Wireshark, SolarWinds) to analyze packet flow.

- \*\*Categorize\*\*:

- \*\*Attack Vectors\*\*:

- TCP SYN Flood: Exploiting handshake requests to exhaust server resources.

- UDP Flood: Overloading servers with high volumes of UDP packets.

- HTTP GET/POST Flood: Bombarding web applications with HTTP requests.

- \*\*Advanced Attack Indicators\*\*:

- Large-scale Distributed Denial-of-Service (DDoS) involving botnets.

- Use of spoofed IP addresses to evade detection.

- Layer 7 (application layer) attacks designed to bypass traditional defenses.

- \*\*Triage\*\*:

- \*\*Assess Impact\*\*:

- Identify affected systems and services.

- Evaluate downtime duration and business impact.

- \*\*Prioritization\*\*:

- High priority if critical services are down or the attack affects a large user base.

- \*\*False Positive Assessment\*\*:

- Compare traffic patterns to historical data to rule out legitimate traffic spikes.

3. Analyze:

Objective: Verify the attack, identify Indicators of Compromise (IOCs), and share findings.

- \*\*Verify\*\*:

- Confirm the attack by cross-referencing logs, traffic analysis, and user reports.

- \*\*Identify IOCs\*\*:

- Extract attacker IP addresses, payload patterns, and unusual traffic volumes.

- \*\*Extract IOCs\*\*:

- Document the attack characteristics, including protocol type and source details.

- \*\*Submit to Partners\*\*:

- Share IOCs with your ISP and security service providers for mitigation assistance.

- \*\*Scan Enterprise\*\*:

- Investigate whether internal systems contributed to the attack (e.g., compromised devices).

4. Contain/Eradicate:

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

- \*\*Contain the Threat\*\*:

- Implement rate-limiting rules on affected endpoints.

- Block malicious IP addresses or ranges at the firewall level.

- Redirect traffic through a DDoS mitigation service.

- \*\*Eradicate the Root Cause\*\*:

- Patch and harden exposed services to prevent abuse.

- Disable unused network services that could be exploited.

- \*\*Validate\*\*:

- Verify that legitimate traffic can access the service and malicious traffic is blocked.

5. Recover:

Objective: Restore systems to normal operations.

- \*\*Restore Operations\*\*:

- Gradually lift rate limits or restrictions to normalize service delivery.

- Monitor traffic to ensure no resurgence of malicious activity.

- \*\*Post-Incident Recovery\*\*:

- Communicate with affected users, explaining the downtime and corrective measures.

- Perform a comprehensive system health check.

6. Lessons Learned:

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

- \*\*Post-Mortem Analysis\*\*:

- Conduct a detailed review to identify gaps in detection and mitigation.

- Update playbooks and implement additional controls based on attack vectors.

- \*\*Response Testing\*\*:

- Regularly test the response to simulated DoS attacks to improve readiness.