Title: Denial of Service Playbook

* 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:

1. Preparation:

Objective: Prepare to respond to a cyber incident in a timely and effective manner, and inform employees of their role in remediating a DoS incident.

- \*\*Prepare to Respond\*\*:

- Review and exercise cyber incident response procedures, including technical and business roles and responsibilities.

- Review recent cyber incidents and their outputs.

- Review threat intelligence for threats to the organisation, brands, and the sector.

- Ensure access to necessary documentation (e.g., CIRP, Network Architecture Diagrams, Data Flow Diagrams).

- Identify and obtain services of a third-party Cyber Forensic provider.

- Define Threat and Risk Indicators and alerting patterns in the SIEM solution.

- \*\*Inform Employees\*\*:

- Conduct regular awareness campaigns highlighting risks like phishing, ransomware, and DoS attacks.

- Mandate regular security training for employees managing personal, confidential, or high-risk data.

- Exercise tactical, operational, and strategic scenarios using tools like NCSC Exercise in a Box Toolkit.

2. Detection and Analysis:

Objective: Detect and report a DoS attack, complete initial investigation, and involve appropriate teams.

- \*\*Detect and Report\*\*:

- Confirm the system is under attack by comparing against baseline operational loads.

- Analyse traffic for common patterns (e.g., IP addresses, ports, protocols, user agents, payloads).

- Report the incident via the Service Desk and classify it according to CIRP guidelines.

- Share intelligence value with other organisations via CiSP.

- \*\*Initial Investigation\*\*:

- Mobilise the Core IT CIRT to investigate the cyber incident.

- Collate data (e.g., affected systems, impact, attack patterns, bandwidth usage, communication from attackers).

- Validate incident categorisation and assess priority using CIRP severity matrix.

- \*\*Incident Reporting\*\*:

- Report the cyber incident as per CIRP, considering requirements for regulators or competent authorities (e.g., ICO, NCSC, SC3).

3. Containment:

Objective: Mitigate the effects of the DoS attack on the targeted environment.

- \*\*Containment Actions\*\*:

- Regain service by requesting the ISP to drop traffic targeting affected services.

- Implement the Business Continuity Plan, aware of potential follow-on attacks.

- Filter traffic at the border and place IP restrictions on sensitive services.

- Segregate internal email and web traffic from product services to reduce impact.

- Contact the ISP for filtering options based on the contractual agreement.

- \*\*Inform Stakeholders\*\*:

- Update stakeholders on containment progress as per CIRP guidelines.

4. Eradication:

Objective: Remove the threat and prevent future incidents.

- \*\*Eradication Measures\*\*:

- Patch systems to protect against exploited vulnerabilities.

- Implement network segmentation.

- Remove vulnerable systems/services.

- Blacklist attack source IPs and whitelist allowed source IPs.

5. Recovery:

Objective: Restore systems to normal operations.

- \*\*Assess End of DoS Condition\*\*:

- Ensure impacted services are reachable again and infrastructure performance matches baseline levels.

- \*\*Rollback Mitigation Measures\*\*:

- Switch traffic back to the original network and restart stopped services in coordination with network teams.

6. Lessons Learned:

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

- \*\*Incident Report\*\*:

- Draft a report detailing cause, impact, and actions taken to mitigate the incident.

- Include recommendations to prevent similar incidents in the future.

- \*\*Lessons Identified\*\*:

- Feedback lessons into preparation activities and share with stakeholders.

- Conduct root cause analysis to remediate vulnerabilities.

- \*\*Human Resources\*\*:

- Review staff welfare (e.g., working hours, overtime, expenses).

- \*\*Communications\*\*:

- Publish internal communications to educate employees on security awareness.

- Publish external communications to inform customers, engage the market, and mitigate reputational risks.

Appendix A: DoS Attack Types

- \*\*HTTP Flood\*\*: Resource exhaustion attack sending large volumes of legitimate requests to overwhelm a server.

- \*\*ICMP (Ping) Flood\*\*: Volumetric attack sending excessive ICMP Ping packets to exhaust bandwidth.

- \*\*NTP Amplification\*\*: Volumetric attack manipulating NTP servers to amplify traffic to the target.

- \*\*Ping of Death (POD)\*\*: Volumetric attack sending oversized packets to crash the target system.

- \*\*Slowloris\*\*: Resource exhaustion attack stalling connections to exhaust server memory.

- \*\*SNMP Flood\*\*: Similar to NTP flood but with lower packet rate.

- \*\*SYN Flood\*\*: Resource exhaustion attack exploiting TCP protocol weaknesses.

- \*\*UDP Flood\*\*: Volumetric attack sending excessive session-less packets to exhaust bandwidth.

- \*\*Zero-Day Attacks\*\*: Brand new attacks targeting previously secure systems.