**Incident Response Playbook: Denial of Service (DoS) 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 DoS attack.?
* Answer:

**Scenario**

This playbook is initiated when a Denial of Service (DoS) attack intentionally paralyzes a computer network by flooding it with data. The goal is to make a machine or network resource unavailable to its intended users by disrupting its services temporarily or indefinitely.

**## Incident Classification**

|  |  |
| --- | --- |
| **Category** | **Details** |
| **Incident Type** | Denial of Service (DoS) |
| **Severity** | High (due to potential to be a significant business disruptor) |
| **Priority** | High (due to the need to limit impact on brand, value, and service delivery) |
| **Detection Sources** | Network diagnostic tools (e.g., Netflow), Service Desk reports, System baselining tools |

**Phase 1: Preparation**

* Review and exercise cyber incident response procedures, including technical and business roles and responsibilities.
* Review recent cyber incidents and their outputs to inform current readiness.
* Review threat intelligence for threats to the organization, brands, and sector, as well as new risks and vulnerabilities.
* Ensure appropriate out-of-hours access to all necessary documentation, such as the Cyber Incident Response Plan (CIRP), network architecture diagrams, and data flow diagrams.
* Define Threat and Risk Indicators and alerting patterns within the organization’s SIEM solution.
* Conduct regular awareness campaigns for employees regarding cyber security risks, including DoS attacks and how to report them.
* Conduct exercises based on this scenario at Tactical, Operational, and Strategic levels.

**Phase 2: Detection and Analysis**

* Confirm the system is genuinely under attack rather than just experiencing a heavy load by comparing current conditions against pre-established operational baselines.
* Analyze incoming packets with network specialists to identify common patterns, such as common sending IP addresses, ports, protocols, user agents, or payloads.
* Report the incident via the Service Desk according to the process defined in the Cyber Incident Response Plan (CIRP).
* Mobilize the Core IT Cyber Incident Response Team (CIRT) to begin the initial investigation.
* Collate initial incident data, including which systems are targeted, the impact on them, whether the attack is spreading, and if any communication has been received from an attacker.
* Research threat intelligence sources and consider submission to the Cyber Security Information Sharing Partnership (CiSP) for further intelligence.

**Phase 3: Containment**

* Consider immediate steps to regain some level of service, such as requesting the Internet Service Provider (ISP) to drop all traffic targeting the affected service.
* In extreme cases, consider blocking all traffic from the ISP to maintain internal services, while being aware of the implications (e.g., loss of email and internet access).
* Consider implementing the Business Continuity Plan, but be aware that the attack may follow to a new location if a different data center is used.
* Filter traffic at the border once analysis is complete, which may be effective against resource exhaustion attacks like Slowloris.
* Place IP restrictions on sensitive services to reduce the impact of heightened traffic.
* Contact the ISP to discuss what filtering options they can provide, as defined in the contractual relationship.

**Phase 4: Eradication**

* Apply patches to systems to protect against any vulnerabilities exploited in the attack.
* Implement network segmentation to isolate affected areas.
* Remove any systems or services that are deemed vulnerable.
* Blacklist the source IPs of the attack.
* Maintain a whitelist of source IPs and services that are allowed into the network.

**Phase 5: Recovery**

* The primary objective of the remediation phase is to recover affected systems and services back to a Business As Usual (BAU) state.

**Phase 6: Post-Incident Activity (Lessons Learned)**

* Draft a comprehensive post-incident report detailing the cause, impact, and actions taken to mitigate the incident.
* Complete a formal lessons-identified process to provide feedback for future preparation activities.
* Conduct a root cause analysis to identify and remediate underlying vulnerabilities.
* Publish internal communications to inform and educate employees on DoS attacks and security awareness.
* Publish external communications, if appropriate and in line with the communications strategy, to provide advice to customers or inform the press.