**Playbook 1: 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 DDOS attack?**
* **Answer:**

**Scenario**

An external attacker launches a distributed denial-of-service (DDoS) attack targeting public-facing infrastructure such as websites, APIs, DNS servers or network gateways. The objective is to disrupt service availability, degrade performance or cause reputational and financial damage.

**Incident Classification**

|  |  |
| --- | --- |
| **Category** | **Details** |
| **Incident Type** | Network/Application Layer Availability Attack |
| **Severity** | High (especially for customer-facing or critical systems) |
| **Priority** | Critical if sustained outage or service degradation occurs |
| **Detection Sources** | NOC alerts, SIEM, firewall logs, application monitoring tools, CDN/WAF, ISP notifications |

**Phase 1: Preparation**

* **Implement DDoS protection:** Use cloud-based mitigation services (e.g., Cloudflare, AWS Shield, Akamai).
* **Deploy WAF and rate limiting:** Protect applications and APIs.
* **Ensure scalable infrastructure:** Use autoscaling groups or CDN caching to absorb surges.
* **Establish communication with ISP:** Predefine the escalation process and mitigation support.
* **Conduct DDoS drills:** Simulate DDoS scenarios and validate response procedures.

**Phase 2: Detection and Analysis**

* **Identify traffic surge:** Monitor bandwidth, request rates or connection counts exceeding normal thresholds.
* **Determine attack vector:** Is it volumetric (UDP flood), protocol (SYN flood) or application-layer (HTTP GET flood)?
* **Correlate with logs:** Identify source IPs, user agents, referrers, and payloads.
* **Confirm impact:** Assess performance degradation, service outages, or collateral damage.
* **MITRE ATT&CK mapping:** T1498 (Network Denial of Service), T1499 (Endpoint Denial of Service), T1498.001 (Direct Network Flood).

**Phase 3: Containment**

* **Engage cloud DDoS mitigation service:** Route traffic through the mitigation provider.
* **Block malicious IPs:** Use firewall, WAF, or geo-blocking rules.
* **Implement rate limiting and filters:** Drop traffic based on rate thresholds or specific patterns.
* **Redirect or reroute traffic:** Temporarily divert traffic to an alternate IP or load balancer.

**Phase 4: Eradication**

* **Drop traffic from confirmed malicious sources:** Based on IP reputation or behavioral patterns.
* **Adjust filtering rules:** Fine-tune ACLs, WAF policies, and IDS/IPS signatures.
* **Remove temporary rules post-attack:** Once the attack subsides, restore normal access patterns.
* **Investigate for blended threats:** Confirm no malware or lateral movement occurred during the disruption.

**Phase 5: Recovery**

* **Monitor for residual traffic:** Use NOC dashboards and SIEM to track post-attack anomalies.
* **Confirm service restoration:** Perform user acceptance testing or API health checks.
* **Notify affected customers or partners:** If SLAs or public services were impacted.
* **Resume normal routing:** If temporary redirection or black-holing was used during the attack.

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

* **Conduct incident review:** Document the timeline, impact, attacker strategy, and response actions.
* **Assess mitigation effectiveness:** Determine what worked and what needs to be improved.
* **Update response playbook:** Refine thresholds, alerting rules, and communication steps.
* **Improve vendor coordination:** Review the performance of the ISP and mitigation partners.
* **Report as required:** To regulators, leadership, or clients if the impact was severe or prolonged.