Title: DDOS attack Incident Response 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 DDOS attack?
* Answer:

1. Preparation:

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

1.1 Internet Service Provider Support:

- Contact your ISP to understand the DDoS mitigation services it offers (free and paid) and what process you should follow.

- Subscribe to a redundant Internet connection if possible, and to an Anti-DDoS services provider.

- Establish contacts with your ISP and law enforcement entities. Ensure the availability of out-of-band communication channels.

- Ensure your ISP and DDoS mitigation service have 24/7 phone support.

1.2 Inventory:

- Create a whitelist of IP addresses and protocols to prioritize traffic during an attack (include critical customers and key partners).

- Document IT infrastructure details, including business owners, IP addresses, circuit IDs, routing settings, network topology, and asset inventory.

1.3 Network Infrastructure:

- Design a robust network infrastructure without Single Points of Failure or bottlenecks.

- Deploy a Web Application Firewall to protect against application-layer DDoS.

- Distribute DNS servers and critical services across different Autonomous Systems (AS).

- Harden the configuration of network, OS, and application components targeted by DDoS.

- Baseline infrastructure performance to identify attacks faster and more accurately.

- Confirm DNS time-to-live (TTL) settings for systems that might be attacked; lower TTLs if necessary (600 is a good value).

- Depending on service criticality, set up backups that can be switched on during issues.

1.4 Internal Contacts:

- Establish contacts for IDS, firewall, systems, and network teams.

- Collaborate with business lines to understand implications of likely DDoS attack scenarios.

- Involve the BCP/DR planning team on DDoS incidents.

2. Detection and Analysis:

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

2.1 Communication:

- Prepare internal and external communication templates for DDoS incidents.

- Identify channels for posting communication.

- Emphasize preparation as the key element for successful DDoS incident response.

2.2 Analyze the Attack:

- Consider the possibility of a DDoS attack being a smokescreen for a more sophisticated attack.

- Review anti-DDoS service analysis and scrubbing center reports.

- Analyze the logical flow of the DDoS attack and impacted infrastructure components.

- Determine if your organization is the target or a collateral victim.

- Review logs from servers, routers, firewalls, applications, and affected infrastructure.

- Differentiate DDoS traffic from benign traffic using:

- Source IP addresses, AS, destination ports, URLs, protocols flags.

- Use network analysis tools for traffic review (e.g., Tcpdump, Tshark, Snort, Netflow).

- If possible, create NIDS signatures to differentiate malicious traffic.

2.3 Involve Internal and External Actors:

- Contact internal teams to gather visibility into the attack.

- Contact your ISP for help, specifying traffic control needs (network blocks, source IP addresses, protocols).

- Notify executive and legal teams.

2.4 Check Background:

- Investigate extortion demands as precursors to the attack (e.g., emails targeting Whois records of websites).

- Look for claims of responsibility on social media.

- Search for motivations behind the attack (competitors, hacktivists, former employees).

3. Containment:

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

3.1 Containment Actions:

- Temporarily disable problematic application features.

- Block DDoS traffic as close to the network’s “cloud” as possible using routers, firewalls, load balancers, or specialized devices.

- Terminate unwanted connections or processes on servers and routers.

- Switch to alternate sites or networks using DNS or other mechanisms; blackhole traffic targeting original IPs.

- Set up alternate communication channels for users/customers.

- Route traffic through scrubbing services/products.

- Configure egress filters to block unnecessary response traffic.

- During extortion attempts, buy time by explaining the need for management approval.

3.2 ISP or Anti-DDoS Service Actions:

- Work closely with ISP or anti-DDoS providers to manage bottlenecks efficiently.

4. Eradication:

Objective: Remove the threat and prevent future incidents.

4.1 Remediation Measures:

- Contact ISP and/or anti-DDoS provider to enforce measures such as:

- Filtering, traffic-scrubbing, sinkhole/clean-pipe, IP public balancing/splitting/switching, blackhole routing.

- If the attack had a major impact, report the incident to regulators.

5. Recovery:

Objective: Restore the system to normal operations.

5.1 Assess the End of the DDoS Condition:

- Ensure impacted services are reachable again.

- Verify infrastructure performance matches baseline levels.

5.2 Rollback Mitigation Measures:

- Switch traffic back to the original network and restart stopped services.

- Coordinate recovery-related actions with network teams to avoid unexpected side effects.

6. Lessons Learned:

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

6.1 Report:

- Write an incident report covering:

- Initial detection, timelines, actions, what went right/wrong, impact, indicators of compromise.

6.2 Lessons Learned:

- Define actions to improve DDoS management processes based on this experience.

- Consider relationships inside and outside the organization that could help with future incidents.