Title: Incident Response Playbook for Volumetric 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 volumetric DDoS attacks effectively?
* Answer:

1. Preparation:

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

- \*\*Internet Service Provider Support\*\*:

- Contact your ISP to understand the DDoS mitigation services it offers.

- Subscribe to redundant Internet connections and/or Anti-DDoS services providers.

- Establish contacts with your ISP and law enforcement entities.

- Ensure availability of an out-of-band communication channel.

- Confirm 24/7 phone support availability from your ISP and DDoS mitigation service.

- \*\*Inventory\*\*:

- Create a whitelist of IP addresses and protocols to prioritize traffic during an attack.

- Document IT infrastructure details (business owners, IP addresses, circuit IDs, routing settings).

- Prepare network topology diagrams and asset inventories.

- \*\*Network Infrastructure\*\*:

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

- Deploy DDoS protection services capable of handling high traffic volumes.

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

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

- Baseline current infrastructure performance metrics for faster attack identification.

- Purchase specialized DDoS mitigation products or services for Internet-dependent businesses.

- Confirm DNS TTL settings; lower TTLs if necessary to facilitate DNS redirection during attacks.

- Set up backups for critical services to switch during disruptions.

- \*\*Internal Contacts\*\*:

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

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

- Involve BCP/DR planning teams in DDoS incident planning.

2. Detection and Analysis:

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

- \*\*Communication\*\*:

- Prepare internal and external communication templates for DDoS incidents.

- Identify appropriate channels for communication.

- \*\*Analyze the Attack\*\*:

- Recognize DDoS as potential smokescreens for more advanced attacks.

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

- Map the logical flow of the DDoS attack to affected infrastructure components.

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

- Analyze traffic logs for patterns differentiating benign and malicious traffic:

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

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

- Create NIDS signatures for precise differentiation.

- \*\*Involve Internal and External Actors\*\*:

- Engage internal teams for visibility into the attack.

- Request ISP support for controlling specific traffic (network blocks, source IPs, protocols).

- Notify legal and executive teams.

- \*\*Check the Background\*\*:

- Investigate extortion demands or social media claims linked to the attack.

- Identify possible motivations (e.g., competitors, hacktivists, former employees).

3. Containment:

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

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

- Throttle or block incoming DDoS traffic using routers, firewalls, load balancers, or specialized devices.

- Terminate unwanted connections or processes on servers and routers.

- Switch traffic to alternate sites/networks; blackhole traffic targeting original IPs.

- Route traffic through scrubbing services or products.

- Configure egress filters to block unnecessary packets.

- For extortion attempts, buy time with fraudsters while escalating to management.

- \*\*ISP or Anti-DDoS Service Actions\*\*:

- Work closely with ISP or Anti-DDoS providers to implement efficient mitigation actions.

4. Eradication:

Objective: Remove the threat and prevent recurrence.

- \*\*Remediation Measures\*\*:

- Enforce DDoS remediation measures with ISP or Anti-DDoS providers:

- Filtering, traffic scrubbing, sinkhole/clean-pipe solutions.

- IP balancing/splitting/switching, blackhole routing.

- Submit incident reports to regulators if necessary and involve law enforcement upon executive/ legal team direction.

5. Recovery:

Objective: Restore the system to normal operations.

- \*\*Assess the End of the DDoS Condition\*\*:

- Verify services are reachable and infrastructure performance matches baseline metrics.

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

- Resume traffic routing to original networks.

- Restart stopped services in coordination with network teams to avoid side effects.

6. Lessons Learned:

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

- \*\*Report\*\*:

- Draft a comprehensive incident report covering detection, response actions, timelines, successes/failures, and impact.

- \*\*Lessons Learned\*\*:

- Define actions to improve DDoS management processes.

- Build relationships inside and outside the organization for future incidents.

- Regularly review and update DDoS response plans based on incident analysis.