Incident Response Playbook: Network Scanning & Denial-of-Service Attacks

Team AnubisX

Version 1.0
October 2025

Document Control

Attribute	Value
Version	1.0
Status	Draft / Operational
Owner	AnubisX Security Team
Review Cycle	Quarterly or after major incident
Approver	SOC Manager / Head of IR

Contents

1 Introduction

1.1 Purpose

This playbook covers operational detection, triage, containment, mitigation, and recovery steps for incidents involving **Network Scanning / Reconnaissance** and **Denial-of-Service (DoS/DDoS)** attacks. It is intended for SOC analysts, network operations, incident responders, and leadership. The goal is to rapidly detect reconnaissance activity and mitigate volumetric or application-layer floods to preserve availability and reduce attack surface.

1.2 Scope

Applies to perimeter and internal network monitoring (firewalls, routers, load balancers), IDS/IPS, NetFlow/IPFIX, cloud/CDN DDoS mitigation services, application load balancers, WAFs, DNS infrastructure, and relevant telemetry collectors (SIEM, NMS).

2 Overview of the Category

2.1 Definition

Network Scanning / Reconnaissance — active probing of network hosts and services (port scans, banner grabs, vulnerability probes) used to discover targets and potential attack vectors. **Denial-of-Service (DoS/DDoS)** — attempts to render a service unavailable through volumetric traffic, resource exhaustion, protocol misuse, or application-layer floods.

2.2 Common Attack Chain

1. **Reconnaissance:** Internet/target discovery using automated scanners (Masscan, Nmap) and web application scanners.
2. **Weaponization:** Identify vulnerable services and craft floods (SYN/UDP floods, HTTP GET/POST floods).
3. **Attack:** Launch volumetric or application-level waves, often from botnets / reflection/amplification techniques.
4. **Sustain / Pivot:** Maintain pressure while exploiting discovered weaknesses or forcing operational mistakes.
5. **Impact:** Service degradation, outages, increased costs (autoscaling), or distraction for concurrent intrusions.

2.3 Primary Risks & Business Impact

- Service unavailability affecting customers and revenue.
- Operational costs due to emergency mitigation (scrubbing, cloud egress).
- Masked intrusions where DDoS serves as a diversion.
- Exposure of internal services discovered during scans leading to successful exploitation later.

3 Severity Level Assessment & MTTD / MTTR

Level	Description / Criteria	Example	MTTD	MTTR
Critical	Widespread, sustained DDoS causing production outage, or coordinated scanning followed by exploitation across many services.	Multi-hour HTTP flood impacting customer portal and API endpoints.	$\leq$ 15 min	Contain within 4 hrs; recovery 24–72 hrs.
High	Volumetric attack impacting some customers or high-rate scanning targeting critical infrastructure.	SYN floods generating degraded service responses; mass port scanning against DMZ.	$\leq$ 1 hr	6–24 hrs.
Medium	Repeated reconnaissance or intermittent low-rate floods causing intermittent performance issues.	Repeated Masscan scans from multiple IP ranges.	$\leq$ 2 hrs	12–48 hrs.
Low	Single-source scan or blocked probe with no successful exploitation or service impact.	One-off Nmap scan blocked by firewall.	$\leq$ 4 hrs	Monitor / minor remediation within 24–72 hrs.

Table 1: Severity Matrix - Network Scanning & Denial-of-Service

4 Tools & Preparation (Recommended)

- **Network Sensors:** Zeek (Bro), Suricata, IDS/IPS with tuned signatures.
- **Flow Telemetry:** NetFlow, sFlow, IPFIX collectors and analytics (Elasticsearch/Logstash/Kibana).
- **DDoS Mitigation:** CDN and scrubbing providers (Cloudflare, Akamai, AWS Shield Advanced), ISP DDoS contacts and BGP flow control.
- **Perimeter Controls:** NGFWs, rate-limiting, ACLs, and blackhole routing procedures.
- **Application Protections:** WAF, rate-limiting, connection throttling and CAPTCHA / challenge-response for HTTP floods.
- **Playbook Resources:** ISP abuse contact templates, scrubbing service onboarding, runbooks for blackholing/BGP announcements.

5 Incident Response Phases

5.1 Identification & Triage

Signals/Detections:

- Sudden spike in bytes/sec or flows in NetFlow/IPFIX; high SYN rates; abnormally high connection attempts per second.
- IDS/Suricata alerts for scanning tools (Nmap fingerprints, Masscan patterns) or high-rate HTTP request patterns.
- Cloud/CDN alerting (increased requests, abnormal geographic distribution) and backend autoscaling events.

- DNS logs showing reflective/amplification attempts or spikes in DNS query volume.

Quick actions:

- Confirm the detection and classify severity using the Severity Matrix.
- Identify affected IPs/subnets, target service endpoints, and attack vectors (SYN/UDP/HTTP).
- Notify network operations, activate DDoS runbook and escalate to leadership if service impact is likely.

5.2 Containment (Immediate / Short-term)

- Engage scrubbing/CDN provider or ISP to filter traffic (BGP diversion to scrubbing center) for volumetric attacks.
- Apply targeted firewall/edge ACLs to block offending source IPs or ASNs (use with caution to avoid blocking legitimate traffic).
- Enable rate-limiting, connection timeouts, and WAF rules to mitigate application-layer floods.
- Implement geo-blocking or traffic throttling for non-essential regions if attack sources are concentrated.

5.3 Investigation & Forensic Triage

- Collect NetFlow/IPFIX summaries, PCAPs at egress/ingress chokepoints, IDS logs and relevant system metrics (CPU, memory).
- Analyze packet characteristics (SYN flags, TTL, source port distributions), user-agent strings, and unique signatures (Nmap flags, HTTP header anomalies).
- Correlate attack timestamps with other alerts to detect if DDoS is a diversion for intrusions.

5.4 Eradication / Mitigation

- Remove or block malicious sources where feasible, work with ISPs to sinkhole or nullroute persistent volumetric sources.
- Harden services: disable unnecessary open ports, implement connection limits, and patch any exposed vulnerabilities discovered during scans.
- Harden application logic to reduce resource consumption per request (caching, timeouts, queuing).

5.5 Recovery

- Gradually reintroduce normal routing after scrubbing and verify service stability and client connectivity.
- Review scaling costs from attack and reconcile with cloud provider / scrubbing service.
- Restore normal monitoring thresholds and remove emergency ACLs after careful validation.

5.6 Post-Incident Activities

- Produce a post-incident report: timeline, affected services, mitigation steps and costs.
- Tune IDS/flow thresholds, deploy additional protections (global rate-limits, WAF rules), and update the DDoS runbook.
- Engage in threat-sharing (ISAC/peers) and update contracts/SLAs with ISPs and scrubbing providers.

6 MITRE ATT&CK Framework Mapping

Network Scanning & DDoS - ATT&CK Mapping

- **Reconnaissance / Scanning:** T1595 (Active Scanning), T1046 (Network Service Scanning)
- **Denial-of-Service:** T1498 (Network Denial of Service), T1499 (Endpoint Denial of Service)
- **Command and Control / Impact Linkage:** T1071 (Application Layer Protocol) — when floods disguise C2 traffic.

7 Key Telemetry & Logs to Collect

- NetFlow/IPFIX / sFlow: bytes/packets per flow, top talkers, unique source ASNs.
- Firewall and edge router logs (connection attempts, drops, blackholed routes).
- IDS/Suricata/Zeek logs and PCAPs captured during attack windows.
- Load balancer and application server metrics (concurrent connections, request latency, error rates).
- DNS query/response logs and CDN/Cloud provider DDoS telemetry (requests per second, origin geo-distribution).

8 Subcategory Scenarios (Realistic)

Note: The scenarios below are operational SOC/IR narratives — each includes detection, investigative steps, containment actions, eradication, recovery and lessons learned.

Scenario A: Suspicious Network Scanning / Reconnaissance

Summary: External IP ranges are observed scanning the DMZ range and performing banner grabs against HTTP, SSH and SMB ports. The scanning cadence matches Masscan signatures and is originating from multiple cloud provider ASNs.

Detection:

- NetFlow: high connection attempt rate from a small set of source ASNs targeting many destination ports.
- IDS/Zeek: signatures indicating SYN scans and HTTP banner enumeration.

- Firewall: many short-lived TCP sessions with SYN packets and immediate RSTs.

Investigation & Actions:

1. **Triage & classification:** Classified as *Medium/High* depending on scope and target criticality.
2. **Immediate containment:** Apply temporary ACLs to block offending IP ranges at the edge; enable additional logging on targeted hosts.
3. **Forensic collection:** Capture PCAPs for the offending windows, export IDS/Zeek logs and NetFlow slices for analysis.
4. **Hunt:** Scan internal inventory for exposed services discovered by the attacker and check for follow-on exploit attempts.
5. **External coordination:** Send abuse reports to cloud providers (include PCAP snippets and timestamps) to request takedown or suspension of offending tenant activity.

Containment & Eradication:

- Close unnecessary ports/services identified by reconnaissance, apply service-specific access controls (restrict SSH to bastion IPs).
- Deploy tarpit/honeypot services for additional intelligence and to slow attackers.
- Harden public-facing services (patch, update banners to hide versions) and apply network segmentation.

Recovery:

- Reassess exposure and re-open ports only when necessary with strict ACLs and monitoring.
- Run authenticated vulnerability scans to ensure no exploitation occurred.
- Continue monitoring for repeated scan campaigns and feed IOC lists to perimeter devices.

Outcome & Lessons:

- Root cause: internet-exposed services and lax access controls. Mitigations: minimize exposed attack surface, enforce bastion patterns and improve scanning/hardening cadence.

Scenario B: DDoS Attack (Layer 3/4 and HTTP Flood)

Summary: A high-volume multi-vector attack combines UDP amplification and HTTP GET floods, saturating bandwidth to the public web tier and causing autoscaling costs and degraded response times for customers.

Detection:

- CDN/Cloud provider alert: sudden spike in requests per second and increased origin error rate.
- NetFlow: dramatic increase in inbound UDP/ICMP traffic and abnormal distribution of source IPs across many ASNs.
- Load balancer: high drop rates, increased timeouts, and connection queue exhaustion.

Investigation & Actions:

1. **Triage & classification:** Classified as *Critical* due to customer-facing outage risk.
2. **Immediate containment:** Engage CDN/scrubbing provider (activate Always-On or on-demand scrubbing), apply BGP diversion to scrubbing center if needed, and enable CDN WAF/Rate-limits.
3. **Communications:** Notify incident command, downstream customers (if SLAs affected), and legal/regulatory as appropriate.
4. **Forensic collection:** Preserve NetFlow samples, CDN logs, and any PCAPs available during the attack for post-mortem analysis.

Containment & Eradication:

- Apply geo-fencing or progressive challenge mechanisms (CAPTCHA, JS challenges) for HTTP floods while scrubbing handles volumetric load.
- Work with ISP to implement source-based filtering and request upstream rate-limiting.
- Block confirmed malicious ASN ranges and update edge rules to drop malformed packets (e.g., reflection/amplification signatures).

Recovery:

- Gradually remove emergency mitigations while monitoring for resurgence; re-evaluate autoscaling triggers to control cost.
- Restore normal routing once scrubbing is confirmed to be complete and traffic is clean.
- Conduct a post-incident review of mitigation timeline, costs, and detection gaps.

Outcome & Lessons:

- Invest in pre-established scrubbing contracts and playbook run-throughs; implement more aggressive edge filtering and application-level throttling to reduce impact and cost.

9 Appendices

9.1 Appendix A — Useful SIEM / Investigation Queries

Splunk: detect sudden spike in inbound traffic (example)

```
index=network sourcetype=netflow
| timechart span=1m sum(bytes) as total_bytes by dest_ip
| where total_bytes > threshold_value
```

Zeek: find SYN flood patterns (example)

```
# Use conn.log and look for high syn/retrans counts per dst
cat conn.log | zeek-cut id.orig_h id.resp_h proto conn_state
```

Kusto / Sentinel: identify high request rates to LB / AppGW

```
AppGatewayFirewallLog
| where TimeGenerated > ago(1h)
| summarize requests = count() by client_IP_s, bin(TimeGenerated, 1m)
| where requests > 100
```

9.2 Appendix B — Forensic Artifact Locations

- Network: NetFlow/IPFIX archives, router/firewall logs, edge ACL change logs.
- IDS: Suricata/Zeek logs, PCAPs captured at ingress/egress chokepoints.
- Cloud/CDN: Cloud provider DDoS telemetry, load balancer logs, edge WAF logs.
- Hosts: system metrics (CPU, netstat), web server logs, and application-level metrics during attack window.

9.3 Appendix C — Incident Report Template (Summary)

- Incident ID / Detection timestamp / Playbook invoked.
- Affected services / IPs / ASNs, attack vector (SYN/UDP/HTTP), and impact (latency, errors, outages).
- Evidence preserved (NetFlow slices, PCAPs, CDN logs) and IOCs (source IPs, ASNs, malicious signatures).
- Actions taken with timestamps and owners (engaged CDN/scrub, BGP diversion, edge blocks).
- Post-incident recommendations (scrubbing contracts, IDS tuning, improved telemetry retention).