# Incident Response Playbook: DDoS Attack (Layer 3/4 or HTTP Flood)

Team AnubisX

Version 1.0
September 23, 2025

**Document Control**

| Attribute | Value |
|---|---|
| **Version** | 1.0 |
| **Status** | Draft |
| **Owner** | AnubisX Security Team |
| **Review Cycle** | Every Quarter |

# Contents

# 1 Introduction

## 1.1 Purpose

This playbook defines incident response procedures for handling "DDoS Attack (Layer 3/4 or HTTP Flood)". It provides roles, responsibilities, detection indicators, containment steps, and recovery guidance to minimize impact and restore services.

## 1.2 Scope

This playbook applies to systems, network components, cloud services, and personnel. It is intended for use by incident responders, SOC analysts, IT operations, legal, and leadership.

# 2 Overview of the Attack

Distributed Denial of Service (DDoS) overwhelms network or application resources, causing service outages. Key risks include:

- Service unavailability, revenue loss
- Diversion of security resources
- Collateral damage to infrastructure

# 3 Incident Response Phases

This playbook follows the NIST Incident Response lifecycle framework.

## 3.1 Phase 1: Preparation

*Goal: To ensure the team is equipped and ready to respond to a DDoS incident before it occurs.*

- **Roles and Responsibilities:** Define roles: Incident Commander, Lead Analyst, Forensics, IT, Communications.
- **Logging Auditing:** Ensure logging and centralized authentication audits are enabled.
- **Tools Resources:** Deploy specialized detection rules and maintain playbooks for the specific alert type.
- **Training:** Regular backups and least-privilege access models.

## 3.2 Phase 2: Identification & Analysis

*Goal: Confirm the activity and determine scope and severity.*

1. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:
    - Spike in inbound traffic, unusual SYN/UDP floods
    - High rate of HTTP requests with low session depth
    - Traffic from botnets or spoofed sources

2. **Severity Level Assessment:** Classify the incident to ensure appropriate allocation of resources. Severity is based on: Operational Impact, Criticality of affected systems/data, Scope of attack, and Detection/Recovery timelines (MTTD/MTTR).

| Level | Description | Example | MTTD | MTTR |
|---|---|---|---|---|
| **Low** | Short-lived flood with minimal impact. | Brief spike handled by auto-scaling or scrubbing. | <1 hr | <24 hrs |
| **Medium** | Sustained traffic causing partial degradation. | Service slowed and some requests dropped. | 1-6 hrs | 1-3 days |
| **High** | Extended attack affecting multiple services. | Major service degradation with customer impact. | 6-24 hrs | 3-7 days |
| **Critical** | Complete service outage across critical systems. | Prolonged DDoS affecting core business functions. | 24+ hrs | 7-21 days |

Table 1: Incident Severity Matrix

### 3.3 Phase 3: Containment

*Goal: Limit attacker actions and preserve evidence.*

- Engage DDoS mitigation service or CDN scrubbing.
- Apply ACLs and blackhole malicious prefixes.
- Scale resources where possible and enable rate-limiting.

### 3.4 Phase 4: Eradication

*Goal: To remove malicious components and prevent reinfection.*

- Block malicious vectors, analyze attack patterns, coordinate with ISP and mitigation partners.

### 3.5 Phase 5: Recovery

*Goal: To safely restore systems and business operations.*

- Restore normal traffic routing, validate current filtering rules, and review SLA impacts.

### 3.6 Phase 6: Post-Incident Activities (Lessons Learned)

*Goal: To strengthen resilience and prevent recurrence.*

- Conduct a blameless post-mortem and update playbooks.
- Produce final incident report and recommended mitigations.
- Implement controls to reduce recurrence.

# 4 MITRE ATT&CK Framework Mapping

**DDoS Attack ATT&CK Mapping**

- **Tactic: Impact**
  - *T1499 – Endpoint Denial of Service*
- **Tactic: Command and Control**
  - *T1071 – Application Layer Protocol*