# Incident Response Playbook: Suspicious Network Scanning / Reconnaissance

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 "Suspicious Network Scanning / Reconnaissance". 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

Network scanning and reconnaissance identify live hosts, open ports, and services to map targets for later attacks. Key risks include:

- Discovery of vulnerable hosts
- Information leakage about network topology
- Recon may be precursor to targeted attacks

# 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 network scanning 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:
    - High rate of port scans from single or distributed IPs
    - Unusual DNS queries for internal resources
    - ARP/NetBIOS sweeps on internal subnets

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** | Single benign vulnerability scan by IT. | Scheduled vulnerability scan authorized by team. | <1 hr | <24 hrs |
| **Medium** | Unauthorized scans on multiple subnets. | Unscheduled scanning activity from unknown source. | 1-4 hrs | 1-3 days |
| **High** | Targeted scanning followed by exploitation attempts. | Scanning followed by login attempts or exploit traffic. | 4-12 hrs | 3-7 days |
| **Critical** | Coordinated reconnaissance preceding major breach. | Extensive mapping used to orchestrate multi-stage attacks. | 12+ hrs | 7-21 days |

Table 1: Incident Severity Matrix

### 3.3 Phase 3: Containment

*Goal: To limit attacker actions and preserve evidence.*

- Identify source(s) of scans and block at perimeter.
- Notify network teams and isolate scanning origin.
- Review internal scan schedules to rule out false positives.

### 3.4 Phase 4: Eradication

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

- Collect pcap and logs, update network ACLs, hunt for follow-up activity.
- Harden exposed services, apply patches.

### 3.5 Phase 5: Recovery

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

- Validate no further scanning and ensure patched hosts are monitored.
- Update perimeter defenses and blacklists.

### 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

**Suspicious Network Scanning ATT&CK Mapping**

- **Tactic: Reconnaissance**
  - *T1595 – Active Scanning*
  - *T1592 – Gather Victim Network Information*
- **Tactic: Initial Access**
  - *T1190 – Exploit Public-Facing Application*