Incident Response Playbook: Password Spraying

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 "Password Spraying". 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

Password spraying attempts a small set of common passwords across many accounts to avoid lockouts. Key risks include:

- Credential compromise
- Privilege escalation if weak admin passwords exist
- Silent long-term access if undetected

3 Incident Response Phases

3.1 Phase 1: Preparation

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

- **Roles and Responsibilities:** Define roles (Incident Commander, Lead Analyst, Forensics, IT, Communications) authentication audits are enabled. Deploy specialized detection rules and maintain playbooks for the specific alert type.
- **Hardening:** Implement regular backups and least-privilege access models.

3.2 Phase 2: Identification & Analysis

Goal: Confirm the activity and determine scope and severity.

1. **Initial Triage:** Collect authentication logs and alerts from SIEM and other sources, open an incident ticket, and assemble the response team.
2. **Initial Analysis and IOC Evaluation:** Analyze logs for Indicators of Compromise (IOCs). Common IOCs include:
    - Many accounts with single or few failed attempts.
    - Attempts spread across services (email, VPN, AD) from distributed IPs.
    - Low and slow authentication patterns.
3. **Severity Level Assessment:** 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	Isolated attempts; no successful logins.	A handful of failed attempts across low-privileged accounts.	<4 hrs	<24 hrs
Medium	Multiple users targeted; potential service impact.	Spraying across a department with some account lockouts.	4-12 hrs	1-3 days
High	Successful compromise of several accounts including privileged users.	Multiple service logins observed with suspicious activity.	12-24 hrs	3-7 days
Critical	Domain admin compromise via weak passwords leading to widespread control.	Attack results in AD changes and mass account misuse.	24+ hrs	7-21 days

Table 1: Incident Severity Matrix [: 109]

3.3 Phase 3: Containment

Goal: To limit attacker actions and preserve evidence.

- Apply global lockout policies, enforce password complexity and MFA.
- Identify and block source IP ranges, monitor for distributed patterns.
- Force password resets and session invalidation.

3.4 Phase 4: Eradication

Goal: To remove the attacker's presence and harden systems.

- Gather authentication logs, identify accounts used for lateral movement, revoke credentials and tokens.
- Implement password policy changes and add risk-based MFA rules.

3.5 Phase 5: Recovery

Goal: To safely restore systems and business operations.

- Restore any affected services and validate account integrity.
- Review password policy effectiveness and implement compensating controls.

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 a final incident report and recommended mitigations.
- Implement controls to reduce recurrence.

4 MITRE ATT&CK Framework Mapping

Password Spraying ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1110.003 – Password Spraying.*
  - *T1078 – Valid Accounts.*
- **Tactic: Persistence**
  - *T1136 – Create Account.*
- **Tactic: Defense Evasion**
  - *T1027 – Obfuscated Files or Information.*