Incident Response Playbook: Suspicious Lateral Movement

Team AnubisX

Version 1.0
September 17, 2025

Document Control

Attribute	Value
Version	1.0
Status	Final
Owner	AnubisX Security Team
Review Cycle	Every Quarter

Contents

1 Introduction

1.1 Purpose

The purpose of this playbook is to provide a clear incident response plan for detecting and responding to suspicious lateral movement using techniques such as Pass-the-Hash (PtH) and Pass-the-Ticket (PtT), with the objective of minimizing unauthorized access, preventing privilege escalation, and restoring secure operations.

1.2 Scope

This playbook applies to all systems, endpoints, credentials, identity services (e.g., Active Directory), and staff involved in authentication and access management. It covers all stages of incident response, from preparation to post-incident lessons learned.

2 Overview of Suspicious Lateral Movement

Suspicious lateral movement refers to techniques attackers use to move across a network using stolen credentials or authentication artifacts. Pass-the-Hash (PtH) involves reusing hashed credentials to authenticate without cracking passwords. Pass-the-Ticket (PtT) involves stealing Kerberos tickets to gain access. These techniques allow attackers to access additional systems, escalate privileges, and maintain persistence.

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 detect and respond to lateral movement incidents before they occur.

- **Roles and Responsibilities:** Define roles (Incident Commander, Lead Analyst, Forensic Analyst, Identity/AD Lead, Network Security Lead).
- **Tools & Resources:** Ensure availability of EDR, SIEM, Kerberos/AD monitoring tools, authentication logs, and forensic tools for memory and ticket analysis.
- **Training:** Run tabletop exercises focusing on PtH/PtT scenarios and credential theft detection.
- **Hardening Controls:** Enforce least privilege, restrict lateral authentication (RDP, SMB), implement credential hygiene (no local admin reuse), enable LAPS where applicable.
- **Contact Lists:** Maintain contacts for identity providers, AD admins, executive management, legal, and external IR partners.
- **Threat Intelligence:** Monitor for credential theft campaigns and indicators related to PtH/PtT techniques.

3.2 Phase 2: Identification & Analysis

Goal: To confirm lateral movement activity (PtH/PtT) and determine its scope and severity.

1. **Initial Triage:** Collect authentication logs, Kerberos/LSASS telemetry, EDR alerts, and open an incident ticket. Activate secure communications.

2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:

   - **Authentication:** Unusual NTLM authentication patterns, authentication from unusual hosts, reuse of local account hashes, mismatched logon GUIDs.
   - **Endpoint:** Signs of credential dumping (LSASS memory access), presence of Mimikatz-related activity, unusual service creations.
   - **Network:** Multiple authentications from a single host to many destinations, unexpected RDP/SMB sessions.

3. **Severity Level Assessment:** Classify the incident to ensure appropriate allocation of resources. Severity is determined based on the operational impact, the privilege level of accounts used, and the scope of lateral spread.

Level	Description	Example	MTTD	MTTR
Low	Single instance of suspicious authentication with no lateral success.	An endpoint shows an anomalous NTLM request from a local admin account but failed authentication on target systems.	6-12 hours	24-48 hours
Medium	Confirmed credential theft on a few accounts with limited movement.	LSASS memory access detected on a workstation and stolen hash used to access a secondary non-critical server.	12-24 hours	2-4 days
High	Widespread lateral movement using stolen hashes/tickets with privilege escalation.	Attackers use stolen Kerberos tickets to access domain-joined servers and create new service accounts.	24-48 hours	4-7 days
Critical	Active attacker control with broad lateral movement and domain compromise.	PtH/PtT techniques observed against domain controllers, AD modifications detected, and persistence established.	48 hours	7-14 days

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious activity with other data points and threat intelligence.

   - **If True Positive (TP):** The activity is confirmed as lateral movement. **Action:** Immediately proceed to the **Containment** phase, escalate to the Incident Commander, and activate the PtH/PtT playbook.
   - **If False Positive (FP):** The activity is confirmed benign. **Action:** Document findings, close the alert, and recommend tuning detection rules.

5. **Incident Declaration:** If confirmed, formally declare a lateral movement incident and escalate to leadership, legal, and relevant IT teams.

3.3 Phase 3: Containment

Goal: To limit the attacker's ability to move across the network.

- **Short-Term Containment (Immediate Actions):**
  - Isolate affected hosts and endpoints from the network.
  - Revoke or rotate compromised user and service account credentials.
  - Block lateral authentication channels (restrict SMB/RDP where possible).
- **Evidence Preservation:** Acquire memory dumps, authentication logs, and Kerberos ticket caches **before** remediation.
- **Long-Term Containment Strategy:** Segment networks to inhibit movement from lower-trust to higher-trust zones.

3.4 Phase 4: Eradication

Goal: To remove attacker artifacts and close access vectors.

- **Root Cause Analysis:** Identify the initial point of compromise and credential theft.
- **Malware Removal:** Remove tools used for credential dumping and persistence from all affected systems.
- **Persistence Removal:** Reimage compromised systems; reset passwords and keys; remove unauthorized accounts and service principals.
- **Security Hardening:** Patch vulnerabilities and harden identity infrastructure (e.g., Kerberos settings, disable NTLM).

3.5 Phase 5: Recovery

Goal: To safely restore systems and business operations.

- **System Restoration:** Restore systems and validate their integrity before returning them to production.
- **Enhanced Monitoring:** Reinstate hardened authentication policies and increase monitoring for recurrence.
- **Validation:** Gradually re-enable restricted services while closely monitoring for anomalous behavior.
- **Business Continuity:** Coordinate with business units to resume normal operations securely.

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

Goal: To strengthen resilience and prevent recurrence.

- **Post-Incident Meeting:** Conduct a blameless post-mortem with identity, AD, security, and operations teams.
- **Final Incident Report:** Prepare a detailed report covering timeline, root cause, impact, and remediation actions.
- **Action Plan:** Implement improved credential management (MFA everywhere, eliminate local admin reuse, enable LAPS, enforce Kerberos ticket lifetimes).

4 MITRE ATT&CK Framework Mapping

Suspicious Lateral Movement ATT&CK Mapping

- **Tactic: Credential Access**
  - *T1003 – OS Credential Dumping*
  - *T1550.002 – Use Alternate Authentication Material: Pass the Hash*
  - *T1550.003 – Use Alternate Authentication Material: Pass the Ticket*
- **Tactic: Persistence**
  - *T1136 – Create Account*
  - *T1053 – Scheduled Task/Job*
- **Tactic: Privilege Escalation**
  - *T1068 – Exploitation for Privilege Escalation*
  - *T1078 – Valid Accounts*
- **Tactic: Defense Evasion**
  - *T1562 – Impair Defenses*
  - *T1098 – Account Manipulation*
- **Tactic: Discovery**
  - *T1087 – Account Discovery*
  - *T1046 – Network Service Scanning*
- **Tactic: Lateral Movement**
  - *T1021 – Remote Services*
  - *T1570 – Lateral Tool Transfer*
- **Tactic: Impact**
  - *T1486 – Data Encrypted for Impact*
  - *T1531 – Account Access Removal*