Incident Response Playbook: Lateral Movement & Privilege Escalation

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 provides a repeatable, operational response for incidents involving **Lateral Movement** and **Privilege Escalation**. It guides SOC analysts, incident responders, IT ops, identity teams and leadership through detection, containment, forensic triage, eradication and recovery for techniques such as Pass-the-Hash, Pass-the-Ticket, token theft, SUID misconfigurations, local admin creation, and other escalation vectors.

1.2 Scope

Applies to Windows and Linux hosts, Active Directory (on-prem / Azure AD hybrid), domain controllers, jump hosts/bastions, privileged access workstations, identity providers, and cloud control planes. Covers both human-driven and automated lateral movement and escalation techniques.

2 Overview of the Category

2.1 Definition

Lateral Movement — techniques attackers use to move from an initially compromised system to other systems across the environment. **Privilege Escalation** — techniques by which attackers gain higher privileges (local admin, root, domain admin, cloud owner) to increase control and persistence.

2.2 Common Attack Chain

1. **Initial foothold:** compromised endpoint or account.
2. **Credential harvesting:** LSASS memory access, keyloggers, Mimikatz, cached creds.
3. **Credential reuse / Pass-the-Hash / Pass-the-Ticket:** reusing NTLM hashes or forged Kerberos tickets to authenticate to additional hosts.
4. **Remote execution:** WMI, PsExec, RDP, SSH, WinRM, remote scheduled tasks.
5. **Privilege escalation:** exploiting SUID binaries, misconfigurations, kernel exploits, or abusing delegated rights.
6. **Persistence and consolidation:** creating new privileged accounts, modifying ACLs, creating service accounts with broad rights.

2.3 Primary Risks & Business Impact

- Compromise of critical infrastructure (domain controllers, AD replication).
- Rapid spread of ransomware or data theft across estate.
- Long-term undetected presence with escalated privileges.
- Large remediation cost (rebuilds, credential rotations, regulatory exposure).

3 Severity Level Assessment & MTTD / MTTR

Level	Description / Criteria	Example	MTTD	MTTR
Critical	Active domain compromise or confirmed Golden Ticket/Golden Ticket forgery, mass credential theft and creation of persistent admin accounts.	Domain controller authentication using forged ticket; multiple new domain admins.	$\leq$ 15 min	Contain within 4 hrs; recovery 24-72 hrs.
High	Confirmed Pass-the-Hash / lateral movement to many servers with evidence of credential dumping or ticket reuse.	NTLM hash reuse to access file servers and jump hosts.	$\leq$ 1 hr	6-24 hrs.
Medium	Isolated privilege escalation event (local admin created, SUID changed) or single host lateral move without domain-level impact.	SUID bit added to custom binary on several servers.	$\leq$ 2 hrs	12-48 hrs.
Low	Reconnaissance and single failed attempts to escalate privileges or lateral movement blocked by controls.	Single blocked Pass-the-Hash attempt caught by EDR.	$\leq$ 4 hrs	Monitor / minor remediation within 24-72 hrs.

Table 1: Severity Matrix - Lateral Movement & Privilege Escalation

4 Tools & Preparation (Recommended)

- **Endpoint / Forensics:** EDR with process-tree, memory acquisition (WinPMEM), Sysmon with recommended config (network, image loads, process create, pipe events).
- **Directory / Identity Telemetry:** Advanced logging for AD (audit logs, DCSync monitoring), Kerberos auditing, Windows Security events (4624, 4688, 4672, 4769), and Azure AD sign-in logs.
- **Network Telemetry:** NetFlow/IPFIX, DNS logs, SMB audit logging, and PCAP capture at key points (jump-hosts, DCs).
- **Hunting Tools:** BloodHound/SharpHound outputs for attack paths, Velociraptor, osquery, and YARA/Sigma rules for known tools.
- **Controls:** LSA Protection, Credential Guard, restrict NTLM, enforce SMB signing, implement JEA/JIT for admin tasks, and use Privileged Access Workstations (PAWs).
- **Playbook Resources:** IR runbooks for LSASS memory capture, AD emergency account reset checklist, vendor contacts for forensic analysis.

5 Incident Response Phases

5.1 Identification & Triage

Signals/Detections:

- EDR: process injection alerts, suspicious parent-child chains (explorer→rundll32→CreateRemoteThread).
- Sysmon: EventIDs for network connections from service accounts, ImageLoaded from unusual paths.
- Kerberos logs: suspicious TGT requests, unusual S4U2Self or ticket-granting behaviors.
- AD logs: attempts to enumerate domain objects, unexpected DCSync activity.

Quick actions:

- Validate alerts, determine impacted hosts and accounts, and classify severity via the severity matrix.
- Capture volatile evidence (memory images of suspect processes/LSASS) and preserve event logs.
- If domain-level activity suspected, notify AD/identity owners and escalate to IR leadership immediately.

5.2 Containment (Immediate / Short-term)

- Isolate affected hosts at network layer (EDR quarantine) and block lateral protocols (SMB, WinRM) between segments if safe.
- Revoke Kerberos tickets and force ticket renewal where possible; disable suspicious service accounts and sessions.
- Enforce account lockout for suspected compromised accounts and temporarily disable privileged accounts until validated.

5.3 Investigation & Forensic Triage

- Collect Sysmon logs, Windows Security logs, LSASS memory dump (preserve chain-of-custody), relevant registry hives, scheduled tasks, and service definitions.
- Retrieve NetFlow/PCAP for lateral movement windows; analyze SMB/LDAP/Kerberos traffic patterns.
- Use BloodHound/SharpHound to map relationships and identify likely attack paths and abused privileges.

5.4 Eradication

- Remove attacker-created accounts, scheduled tasks, services, and persistence mechanisms after evidence collection and documentation.
- Rotate credentials and keys for affected accounts; enforce Kerberos ticket invalidation where possible.
- Reimage hosts when integrity cannot be guaranteed or where kernel/LSASS tampering is suspected.
- Apply configuration changes: disable NTLM, enable SMB signing, and apply principle-of-least-privilege to service accounts.

5.5 Recovery

- Bring systems back in staged fashion; validate with forensic scans and enhanced monitoring.
- Re-enable admin accounts only after controlled validation and rotate privileged credentials.
- Run post-recovery hunts for re-use of harvested credentials and monitor DC/identity logs closely for 30–90 days.

5.6 Post-Incident Activities

- Full incident report, timeline, root cause analysis and IOCs for sharing with threat intel and partners.
- Update detection content (EDR rules, Sigma, YARA), hardening guidance and AD security baselines.
- Run tabletop exercises simulating Pass-the-Hash/Golden Ticket scenarios and update playbooks accordingly.

6 MITRE ATT&CK Framework Mapping

Lateral Movement & Privilege Escalation - ATT&CK Mapping

- **Credential Access & Reuse:** T1003 (OS Credential Dumping), T1550 (Use of Valid Accounts), T1078 (Valid Accounts)
- **Lateral Movement:** T1021 (Remote Services), T1570 (Lateral Tool Transfer), T1563 (Remote Services)
- **Privilege Escalation:** T1068 (Exploitation for Privilege Escalation), T1548 (Abuse Elevation Control Mechanism)
- **Defense Evasion:** T1134 (Access Token Manipulation), T1055 (Process Injection)

7 Key Telemetry & Logs to Collect

- Sysmon process create/network connect/image load events; Windows Security events (4624, 4672, 4688, 4769, 4776) and Kerberos events (4768/4770/4769).
- LSASS memory images and EDR process memory dumps.
- AD replication and DCSync-related events; Group Policy modification logs.
- NetFlow and PCAPs for lateral movement windows; SMB/LDAP traffic logs.
- Jump-host / bastion session logs and bastion recordings.

8 Subcategory Scenarios (Realistic)

Note: The scenarios below are written as operational SOC/IR narratives — each covers detection, investigation, containment, eradication, recovery and lessons learned.

Scenario A: Suspicious Lateral Movement (Pass-the-Hash / Pass-the-Ticket)

Summary: A workstation is compromised via a phishing-delivered loader which dumps credentials from LSASS. The attacker reuses NTLM hashes with Pass-the-Hash to authenticate to file servers and then obtains a service account's Kerberos ticket to access a jump host. From the jump host the attacker attempts to enumerate AD and create a new service account.

Detection:

- EDR: process tree showing suspicious LSASS access and Mimikatz-like tooling signature.
- Sysmon: multiple source hosts authenticating to file servers using the same administrative SID from different endpoints.
- AD/Kerberos: anomalous ticket requests and signs of ticket reuse; odd timestampts for ticket age.

Investigation & Actions:

1. **Triage & classification:** Classified as *Critical* because of evidence of credential dumping and lateral use of high-privilege credentials.
2. **Immediate containment:** Quarantine the initial workstation and isolate the jump host; block the compromised service account and remove current sessions and Kerberos tickets if possible.
3. **Forensic collection:** Capture LSASS memory image from affected hosts (preserve chain-of-custody), collect Sysmon logs, and snapshot jump host activity logs and NetFlow for lateral window.
4. **Hunt:** Search estate for identical hashes, token reuse patterns, and unusual use of service accounts; enumerate scheduled tasks and services created in the timeframe.
5. **Block & Mitigate:** Block lateral protocols from the compromised network segment, rotate service account credentials, and enforce temporary deny of PsExec/remote admin tools.

Containment & Eradication:

- Remove malware/loaders from compromised endpoints after capturing evidence; reimage hosts where persistence may exist.
- Reset and rotate all credentials for accounts observed in the dump and remove or disable attacker-created accounts.
- Deploy EDR rules to detect immediate re-use patterns (identical hashes used from multiple hosts).

Recovery:

- Restore hosts from known-good images with updated agents and hardened configurations.
- Reintroduce service accounts after rotating credentials and limiting their scope/privileges.
- Monitor AD and Kerberos logs with elevated retention and detection for 30–90 days.

Outcome & Lessons:

- Root cause: insufficient protection of LSASS and overly-permissive service account privileges.
- Mitigations: deploy Credential Guard, restrict NTLM, enforce LSA protection, and minimize service account privileges and scope.
- Added proactive hunts for token/hash reuse across the estate.

Scenario B: Privilege Escalation Detection (Local Admin Creation / SUID changes)

Summary: On a set of Linux servers, ‘sudo‘ configuration changes and SUID bit modifications are detected by configuration management alerts. An attacker exploited a misconfigured deployment script to place a SUID-enabled binary that provides a root shell when invoked.

Detection:

- Configuration management / CMDB: unexpected changes to file mode / SUID bits on multiple servers.
- Auditd / syslog: suspicious ‘chmod‘ and ‘chown‘ operations and creation of new binaries in ‘/usr/local/bin‘.
- EDR/Host: suspicious process executing with elevated privileges spawned from a non-standard path.

Investigation & Actions:

1. **Triage & classification:** Classified as *High* due to persistence via SUID and root escalation potential.
2. **Immediate containment:** Isolate affected servers and freeze any deployment jobs; remove the SUID bit from suspicious binaries (after capturing binary for analysis).
3. **Forensic collection:** Preserve the SUID binary and related logs, collect process trees and auditd events for the timeline, and check for presence of crontab entries or backdoor user accounts.
4. **Hunt:** Search other servers for similar SUID changes or uploaded binaries and investigate automation pipelines for misconfiguration or secret exposure.

Containment & Eradication:

- Remove malicious SUID binaries, revoke any unauthorized sudoers modifications, and revert to known-good configurations from CMDB.
- Rebuild/reimage hosts where root-level persistence is suspected; rotate privileged SSH keys.
- Patch the deployment pipeline and enforce code signing and least-privilege in automation accounts.

Recovery:

- Validate system integrity, restore from trusted images, and reconfigure monitoring and alerting for SUID changes.
- Conduct a permissions audit and harden ‘sudo‘ policies and file integrity monitoring.

Outcome & Lessons:

- Root cause: insecure deployment process and insufficient file integrity monitoring.
- Mitigations: enforce CI/CD scanning, code-signing for deployment artifacts, and restrict automation accounts to minimal privileges.
- Add automated alerts for file-mode changes and immediate blocking of changed binaries pending review.

9 Appendices

9.1 Appendix A — Useful SIEM / Investigation Queries

Splunk: find suspicious LSASS access / credential dumping traces

```
index=edr process_name="mimikatz.exe" OR (CommandLine="*sekurlsa*" OR CommandLine="*
    lsass*")
| table _time host user process_name CommandLine
```

Kusto / Sentinel: detect multiple hosts using same NTLM hash (example heuristic)

```
SecurityEvent
| where EventID == 4624
| summarize hosts = dcount(Computer) by TargetAccount, LogonType,
    AuthenticationPackage
| where hosts > 1 and AuthenticationPackage == "NTLM"
```

Linux: find recent SUID file creations

```
find / -perm -4000 -type f -mtime -7 -exec ls -l {} \;
```

9.2 Appendix B — Forensic Artifact Locations

- Windows: LSASS memory (dump with WinPMEM), Sysmon logs (ProcessCreate 1, ImageLoaded 7), Security logs (4624, 4688, 4672, 4769), Scheduled Tasks folder, Services registry keys.
- Linux: /var/log/auth.log, auditd logs (/var/log/audit/audit.log), /etc/sudoers and /etc/sudoers.d, files with SUID bit, bash history, cron jobs.
- AD/Identity: Domain Controller Security logs, DCSync detection events, Kerberos KDC logs, AD replication metadata.
- Network: SMB logs, NetFlow/IPFIX, jump-host session logs, PCAPs capturing lateral activity.

9.3 Appendix C — Incident Report Template (Summary)

- Incident ID / Detection timestamp / Playbook invoked (Lateral Movement & Privilege Escalation).
- Affected hosts, accounts, services; scope of lateral movement and escalation.
- Evidence preserved (memory images, PCAPs, Sysmon/AD logs) and IOCs (hashes, accounts, tickets, IPs).
- Actions taken (containment, eradication, recovery) with timestamps and owners.
- Root cause analysis, remediation actions, and long-term hardening items.
- Notifications performed (internal/external), legal/regulatory obligations, and lessons learned.