Incident Response Playbook: Privilege Escalation Detection

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 structured incident response plan for detecting and responding to privilege escalation events—specifically local administrator account creation and SUID/permission changes on Unix-like systems. The objective is to detect unauthorized privilege gains early, remove illegitimate privileges, and restore secure access controls.

1.2 Scope

This playbook applies to endpoints, servers (Windows, Linux, macOS), identity services, and administrative processes. It covers detection, analysis, containment, eradication, recovery, and post-incident activities related to privilege escalation.

2 Overview of Privilege Escalation

Privilege escalation refers to techniques attackers use to obtain higher privileges than originally granted. Examples include creating local administrator accounts on Windows or changing SUID/permission bits on Unix-like systems. Unauthorized privilege escalation enables lateral movement, persistent access, and access to sensitive data or critical functions.

3 Incident Response Phases

This playbook follows the NIST Incident Response lifecycle framework.

3.1 Phase 1: Preparation

Goal: To ensure the team is ready to detect and respond to privilege escalation events.

- **Roles and Responsibilities:** Define roles (Incident Commander, Lead Analyst, Forensic Analyst, Identity/Admin Lead, Communications Lead).
- **Tools & Resources:** Ensure availability of EDR, SIEM, host-based auditing (Windows Event Logs, Linux auditd), privileged access monitoring, and forensic tools.
- **Training:** Run tabletop exercises focused on privilege escalation scenarios and admin misuse.
- **Hardening Controls:** Enforce least privilege, restrict local admin creation, use centralized account management (e.g., LAPS, PAM), enforce sudo policies, monitor SUID changes.
- **Contact Lists:** Maintain contacts for AD admins, system owners, executive management, and external IR partners.
- **Threat Intelligence:** Monitor for TTPs that leverage privilege escalation techniques and known post-exploitation frameworks.

3.2 Phase 2: Identification & Analysis

Goal: To confirm privilege escalation activity and determine its scope and severity.

1. **Initial Triage:** Collect alerts, endpoint telemetry, system audit logs, 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:
   - **Windows:** New local admin user creation events (Event ID 4720/4732/4670 changes), unexpected group membership changes, creation of scheduled tasks with elevated privileges.
   - **Linux/macOS:** SUID/permission bit changes (e.g., chmod +s), creation of new users in /etc/passwd or unexpected sudoers modifications, artifacts of privilege escalation tools.
   - **Endpoint:** Unexpected processes running as SYSTEM/root, presence of known escalation tools (e.g., Mimikatz, pkexec exploit), suspicious service installations.
3. **Severity Level Assessment:** Classify the incident to ensure appropriate allocation of resources. Severity is determined based on the operational impact, the sensitivity of the affected systems, and the scope of unauthorized privilege.

Level	Description	Example	MTTD	MTTR
Low	Single unauthorized privilege change on a non-critical workstation with no further activity.	A developer test VM shows a new local admin created during a maintenance task and verified by the owner.	6-12 hours	24-48 hours
Medium	Unauthorized admin or SUID change on a production server with limited misuse.	An application server had a new sudoers entry added and a single administrative command executed unexpectedly.	12-24 hours	2-4 days
High	Multiple hosts with unauthorized admin creation or SUID modifications and evidence of misuse.	Several Linux servers show SUID changes to binaries and new admin accounts used to access restricted data.	24-48 hours	4-7 days
Critical	Widespread privilege escalation leading to domain/admin compromise or persistent root-level access.	Attackers create local admin accounts across domain-joined systems and modify sudoers/suid widely, enabling domain privilege escalation.	48 hours	7-14 days

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious privilege escalation indicators with other telemetry and threat intelligence.
   - **If True Positive (TP):** The activity is confirmed as unauthorized privilege escalation. **Action:** Immediately proceed to the **Containment** phase, escalate to the Incident Commander, and activate the privilege escalation 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 privilege escalation incident and escalate to leadership, legal, and relevant IT teams.

3.3 Phase 3: Containment

Goal: To prevent the misuse of escalated privileges and limit attacker control.

- **Short-Term Containment (Immediate Actions):**
  - Isolate affected hosts from the network.
  - Disable or remove unauthorized local admin accounts and revoke associated sessions.
  - Restore original SUID/permission bits from known-good baselines or backups.
- **Evidence Preservation:** Acquire security and audit logs and memory captures **before** remediation.
- **Long-Term Containment Strategy:** Block attacker C2 and restrict lateral authentication channels.

3.4 Phase 4: Eradication

Goal: To remove attacker artifacts and close escalation pathways.

- **Root Cause Analysis:** Identify the vulnerability or misconfiguration that allowed escalation.
- **Malware Removal:** Remove tools and backdoors used for escalation.
- **Persistence Removal:** Reimage compromised systems where root/SYSTEM integrity is in doubt. Reset credentials for affected accounts.
- **Security Hardening:** Apply patches and harden privileged access configurations (disable unnecessary SUIDs, tighten sudoers, use PAM controls).

3.5 Phase 5: Recovery

Goal: To safely restore systems and normal operations.

- **System Restoration:** Restore systems from clean images or backups and verify the integrity of system binaries and permissions.
- **Enhanced Monitoring:** Reintroduce systems to production with increased monitoring on privileged account activity.
- **Validation:** Review and tighten privileged access policies and audit schedules.
- **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 post-mortem with identity, security, and operations teams.
- **Final Incident Report:** Produce a detailed incident report including timeline, root cause, and remediation.
- **Action Plan:** Implement improved detection for admin creation and SUID changes, enforce change management for privilege changes, and adopt stronger PAM solutions.

4 MITRE ATT&CK Framework Mapping

Privilege Escalation Detection ATT&CK Mapping

- **Tactic: Privilege Escalation**
  - *T1068 – Exploitation for Privilege Escalation*
  - *T1548 – Abuse Elevation Control Mechanism*
  - *T1134 – Access Token Manipulation*
- **Tactic: Persistence**
  - *T1136 – Create Account*
  - *T1543 – Create or Modify System Process*
  - *T1547 – Boot or Logon Autostart Execution*
- **Tactic: Defense Evasion**
  - *T1562 – Impair Defenses*
  - *T1070 – Indicator Removal on Host*
- **Tactic: Credential Access**
  - *T1003 – OS Credential Dumping*
  - *T1555 – Credentials from Password Stores*
- **Tactic: Discovery**
  - *T1087 – Account Discovery*
  - *T1018 – Remote System Discovery*
- **Tactic: Lateral Movement**
  - *T1021 – Remote Services*
  - *T1570 – Lateral Tool Transfer*