

# Unix-like File Permission Manipulation Behavioral Chain

## Detection Strategy, Detection Strategy DET0351

Archived: 2026-04-05 14:46:28 UTC

### AN0998

Linux permission escalation behavioral chain: (1) Process creation of permission modification utilities (chmod, chown, chgrp, setfacl) with suspicious parameters indicating privilege escalation intent, (2) System call analysis revealing direct file metadata manipulation (chmod, fchmod, chown, fchown syscalls), (3) Extended attribute and ACL modifications targeting critical system paths, (4) Temporal correlation with subsequent file access or process execution from modified locations, (5) Anomalous permission patterns deviating from system baselines

### Log Sources

| Data Component  | Name             | Channel  |
|---|------------------|--|
| <a href="#">File Metadata</a><br>( <a href="#">DC0059</a> )     | auditd:SYSCALL   | syscall in (chmod, fchmod, fchmodat, chown, fchown, fchownat, lchown, setxattr, lsetxattr, fsetxattr, removexattr, lremovexattr, fremovexattr) |
| <a href="#">Command Execution</a><br>( <a href="#">DC0064</a> ) | auditd:PROCTITLE | proctitle contains chmod, chown, chgrp, setfacl, or attr with suspicious parameters (777, 755, +x, -R)   |
| <a href="#">Process Creation</a><br>( <a href="#">DC0032</a> )  | linux:osquery    | process execution events for permission modification utilities with command-line analysis  |

### Mutable Elements

| Field                      | Description   |
|----------------------------|---|
| SuspiciousPermissionValues | Octal permission values indicating potential malicious intent - customize based on organizational security policy (default: 777, 755, 4755, 2755, 1755 for sticky/setuid/setgid)  |
| CriticalSystemPaths        | Linux filesystem paths requiring enhanced permission change monitoring - adapt to environment-specific critical directories (/etc, /usr/bin, /usr/sbin, /var, /opt, /root, /boot) |

| Field                          | Description   |
|--------------------------------|---|
| AuthorizedSystemAdministrators | User accounts and service accounts authorized for system-level permission modifications - maintain current list of legitimate administrators                |
| TemporalCorrelationWindow      | Time window for correlating permission changes with subsequent file access or process execution - adjust based on system performance (default: 300 seconds) |
| RecursiveOperationThreshold    | Maximum depth or file count for recursive permission operations before triggering anomaly detection (-R flag monitoring)                                    |
| ACLComplexityBaseline          | Baseline complexity metrics for setfacl operations to detect anomalous extended ACL configurations  |
| FileAccessFrequencyBaseline    | Statistical baseline for normal file access patterns post-permission modification to detect privilege abuse   |

**AN0999**

macOS permission and attribute manipulation behavioral chain: (1) Process execution of permission utilities (chmod, chown, chgrp) or macOS-specific tools (chflags) with suspicious parameters, (2) System Integrity Protection (SIP) bypass attempts through permission modifications, (3) File flags manipulation (uchg, schg, hidden) for evasion or persistence, (4) Extended attribute (xattr) modifications affecting security metadata, (5) Unified log correlation with file system events and subsequent access patterns, (6) Gatekeeper and code signing bypass through permission/attribute manipulation

**Log Sources**

| Data Component                             | Name               | Channel  |
|--|--------------------|--|
| <a href="#">Process Creation (DC0032)</a>  | macos:unifiedlog   | process execution events for chmod, chown, chflags with parameter analysis and target path examination   |
| <a href="#">File Modification (DC0061)</a> | fs:fsevents        | file system events indicating permission, ownership, or extended attribute changes on critical paths. File system modification events with kFSEventStreamEventFlagItemChangeOwner, kFSEventStreamEventFlagItemXattrMod flags |
| <a href="#">File Metadata (DC0059)</a>     | OpenBSM:AuditTrail | BSM audit events for file permission, ownership, and attribute modifications with user context   |

### Mutable Elements

| Field                       | Description   |
|-----------------------------|---|
| SIPProtectedPaths           | macOS system paths protected by SIP that should never have permission modifications - maintain current list based on macOS version (/System, /usr, /bin, /sbin) |
| SuspiciousFileFlags         | chflags parameter combinations indicating potential evasive behavior - customize based on security requirements (uchg, schg, hidden, archived)                  |
| CriticalExtendedAttributes  | Extended attributes requiring monitoring for unauthorized removal or modification (com.apple.quarantine, com.apple.metadata, com.apple.FinderInfo)              |
| GatekeeperBypassIndicators  | Patterns in permission/attribute changes that may indicate Gatekeeper bypass attempts   |
| ApplicationBundleMonitoring | Scope of .app directory monitoring for internal permission modifications indicating bundle tampering  |
| UnifiedLogRetentionPeriod   | Log retention period for correlating permission changes with subsequent access patterns - balance storage with detection capability                             |
| FSEventsFilteringThreshold  | File system event filtering threshold to manage high-volume environments while maintaining detection coverage   |

---

Source: <https://attack.mitre.org/detectionstrategies/DET0351#AN0998>