

# Behavioral Detection of Local Group Enumeration Across OS Platforms, Detection Strategy DET0114

Archived: 2026-04-05 16:05:38 UTC

## AN0317

Detects attempts to enumerate local groups via Net.exe, PowerShell, or native API calls that precede lateral movement or privilege abuse.

### Log Sources

### Mutable Elements

Field	Description
TimeWindow	Time window between group enumeration and lateral movement or privilege escalation activity.
UserContext	Whether the process was executed by a privileged or low-privilege account.

## AN0318

Detects enumeration of local groups using common binaries (groups, getent, cat /etc/group) or scripting with suspicious lineage.

### Log Sources

### Mutable Elements

Field	Description
ProcessName	Detection tuning for binaries like `groups`, `getent`, `awk`, or `cut` that may be used in pipelines.
ParentProcess	Used to determine whether enumeration was triggered by a script or terminal.

## AN0319

Detects use of dscl or id/group commands to enumerate local system groups, often by post-exploitation tools or persistence checks.

### Log Sources

### Mutable Elements

Field	Description
CommandLineContains	Match on specific dscl paths like '/Groups' or known enumeration options.
InteractiveSession	Used to scope out enumeration from user terminals versus background utilities.

---

Source: <https://attack.mitre.org/detectionstrategies/DET0114#AN0319>