

# Behavioral Detection of Permission Groups Discovery, Detection Strategy DET0179

Archived: 2026-04-05 16:58:27 UTC

## AN0507

Detection of adversary enumeration of domain or local group memberships via native tools such as net.exe, PowerShell, or WMI. This activity may precede lateral movement or privilege escalation.

### Log Sources

### Mutable Elements

Field	Description
CommandLineRegex	Regex filters for matching suspicious group enumeration commands (e.g., 'net group', 'Get-ADGroupMember').
TimeWindow	Time threshold for correlating group discovery with subsequent suspicious activity (e.g., lateral movement).
UserContext	Whether the user performing discovery is in a sensitive group or running under unusual context (e.g., non-admin querying Domain Admins).

## AN0508

Detection of group enumeration using commands like 'id', 'groups', or 'getent group', often followed by privilege escalation or SSH lateral movement.

### Log Sources

### Mutable Elements

Field	Description
CommandLine	Variations of enumeration commands tailored to different Linux distros (e.g., 'getent group', 'cut -d' in /etc/group parsing).
TTYSession	TTY context or source terminal (remote shell vs local login) to reduce noise.

## AN0509

Group membership checks via 'dscl', 'dscacheutil', or 'id', typically executed via terminal or automation scripts.

**Log Sources**

**Mutable Elements**

Field	Description
CommandLine	Filters for suspicious execution of 'dscl . -read /Groups', etc.
ParentProcess	Flag group enumeration from automation tools (e.g., LaunchAgents or suspicious apps).

---

Source: <https://attack.mitre.org/detectionstrategies/DET0179>