

# Local Account Enumeration Across Host Platforms, Detection Strategy DET0303

Archived: 2026-04-05 13:15:36 UTC

## AN0846

Adversary enumeration of local user accounts using Net.exe, WMI, or PowerShell.

### Log Sources

### Mutable Elements

Field	Description
CommandLinePattern	Detects variations of 'net user', 'net localgroup', 'Get-LocalUser'.
UserContext	Restrict monitoring to low-privileged or unexpected users executing enumeration.
TimeWindow	Tune for bursts of enumeration commands in short succession.

## AN0847

Enumeration of local users or groups via file access (/etc/passwd) or commands like id, groups.

### Log Sources

### Mutable Elements

Field	Description
AccessedFile	Monitors sensitive file access such as '/etc/passwd', '/etc/group'.
ExecutionScope	Restrict detection to user-initiated sessions or specific parent processes.

## AN0848

Enumeration of macOS local users using dscl, id, dscacheutil, or /etc/passwd access.

### Log Sources

### Mutable Elements

Field	Description
CommandLine	Monitor dscl . list /Users, dscacheutil -q user, id -un.
InteractiveSession	Focus on enumeration from non-console users or untrusted apps.

## AN0849

Enumeration of local ESXi accounts using esxcli or vSphere API from unauthorized sessions.

### Log Sources

### Mutable Elements

Field	Description
CommandPattern	Look for 'esxcli system account list' and API calls from unusual sources.
SessionType	Restrict detection to interactive sessions vs. maintenance/automation jobs.

---

Source: <https://attack.mitre.org/detectionstrategies/DET0303>