

# Detection of System Service Discovery Commands Across OS Platforms, Detection Strategy DET0483

Archived: 2026-04-05 17:01:00 UTC

## AN1325

Enumeration of services via native CLI tools (e.g., `sc query`, `tasklist /svc`, `net start`) or API calls via PowerShell and WMI.

### Log Sources

### Mutable Elements

Field	Description
ProcessName	Can be tuned to specific binaries used for service enumeration (e.g., <code>`sc.exe`</code> , <code>`tasklist.exe`</code> ).
CommandLineMatch	Filters for variations like <code>`sc query`</code> , <code>`net start`</code> , <code>`Get-Service`</code> .
ParentProcess	Used to suppress known admin scripts or automation jobs.

## AN1326

Execution of service management commands like `systemctl list-units`, `service --status-all`, or direct reading of `/etc/init.d`.

### Log Sources

### Mutable Elements

Field	Description
CommandPattern	Includes service enumeration commands like <code>`systemctl`</code> , <code>`service`</code> , or custom scripts.
ExecutionUser	Tunable by user context (e.g., <code>root</code> vs. <code>standard user</code> ).
TimeWindow	Used for correlation with privilege escalation or lateral movement.

## AN1327

Discovery via `launchctl` commands, or process enumeration using `ps aux | grep com.apple` to identify daemons and services.

## Log Sources

## Mutable Elements

Field	Description
CommandLineContent	Tune to recognize `launchctl list`, `launchctl print`, or service grep strings.
ProcessParent	Filter known benign automation or MDM agent invocations.

---

Source: <https://attack.mitre.org/detectionstrategies/DET0483#AN1326>