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

Archived: 2026-04-05 17:06:28 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., `sc.exe`, `tasklist.exe`).
CommandLineMatch	Filters for variations like `sc query`, `net start`, `Get-Service`.
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 `systemctl`, `service`, or custom scripts.
ExecutionUser	Tunable by user context (e.g., root vs. standard user).
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#AN1327