Behavioral Detection of User Discovery via Local and Remote Enumeration, Detection Strategy DET0093

Archived: 2026-04-05 14:44:32 UTC

AN0254

Adversary launches built-in system tools (e.g., whoami, query user, net user) or scripts that enumerate user account information via local execution or remote API queries (e.g., WMI, PowerShell).

Log Sources

Mutable Elements

Field	Description
ParentProcessContext	Identify if enumeration originates from non-interactive shell or system service
TimeWindow	Tune temporal grouping of enumeration + lateral movement attempts
UserContext	Flag unexpected users issuing enumeration commands (e.g., service accounts)

AN0255

Adversary runs commands like `whoami`, `id`, `w`, or `cat /etc/passwd` from non-interactive or scripting contexts to enumerate system user details.

Log Sources

Mutable Elements

Field	Description
CommandLineRegex	Tune detection based on argument presence (e.g., `cat /etc/passwd` vs. `cat` alone)
ShellContext	Identify if command issued via cron, systemd, or reverse shell
AccessFrequency	Define how often user/account commands are expected on endpoint

AN0256

Adversary uses `dscl`, `who`, or environment variables like `$USER` to identify accounts or sessions via Terminal or malicious LaunchAgents.

Log Sources

Mutable Elements

Field	Description
LaunchAgentPersistence	Correlate dscl usage with known persistence vectors
CommandExecutionPath	Distinguish between user-initiated terminal vs. script execution
UsernameEnumerationPattern	Regex-based pattern tuning for `dscl . -list /Users` + grep filters

AN0257

Adversary executes CLI commands like `show users`, `show ssh`, or attempts to dump AAA user lists from routers or switches.

Log Sources

Mutable Elements

Field	Description
CLICommandBaseline	Expected command set per device role/user role combination
DeviceRoleSensitivity	Correlate access with core vs. edge vs. management plane sensitivity
CommandFrequencyThreshold	Detect burst usage of `show` or `debug` commands by non-admin users

---