Enumeration of User or Account Information Across Platforms, Detection Strategy DET0587

Archived: 2026-04-02 10:41:49 UTC

AN1612

Detection of suspicious enumeration of local or domain accounts via command-line tools, WMI, or scripts.

Log Sources

Mutable Elements

Field	Description
CommandLinePattern	Match variations in enumeration commands like 'net user', 'Get-ADUser', 'dsquery'.
TimeWindow	Short burst of account enumeration commands may indicate automation.
UserContext	Restrict to non-admin accounts or unexpected users executing enumeration commands.

AN1613

Enumeration of users and groups through suspicious shell commands or unauthorized access to /etc/passwd or /etc/shadow.

Log Sources

Mutable Elements

Field	Description
AccessedFile	Tune based on file paths such as '/etc/passwd', '/etc/group', '/etc/shadow'.
ParentProcessName	Filter known admin processes to reduce false positives.

AN1614

Detection of user account enumeration through tools like dscl, dscacheutil, or loginshell enumeration via command-line.

Log Sources

Mutable Elements

Field	Description
CommandLine	Tune for dscl -list, dscacheutil -q user, id -un, etc.
ExecutionContext	Alert if enumeration is performed in non-console session or by unusual users.

AN1615

Detection of API calls listing users, IAM roles, or groups in cloud environments.

Log Sources

Mutable Elements

Field	Description
API_Method	Tune based on which IAM APIs are used and their frequency.
CallerType	Differentiate user-initiated from automated/scripted enumeration.

AN1616

Enumeration of user or role objects via IdP API endpoints or LDAP queries.

Log Sources

Mutable Elements

Field	Description
QueryType	Detect user vs role enumeration. Tune based on query scope.
AppContext	Correlate enumeration with unexpected app registrations or identities.

AN1617

Account enumeration via esxcli, vim-cmd, or API calls to vSphere.

Log Sources

Mutable Elements

Field	Description
CommandPattern	Tune based on known enumeration commands: 'vim-cmd vimsvc/auth/userlist'.
PrivilegedSession	Elevated enumeration from vpxuser or root may indicate threat activity.

AN1618

Account enumeration via bulk access to user directory features or hidden APIs.

Log Sources

Mutable Elements

Field	Description
EndpointURL	Tune based on enumeration from directory endpoints such as /users, /groups.
UserAgent	Detect scripted enumeration via curl/wget or unknown tools.

AN1619

Account discovery via VBA macros, COM objects, or embedded scripting.

Log Sources

Mutable Elements

Field	Description
MacroName	Alert on auto-running macros accessing directory or user info.
ExecutionScope	Focus on macros invoking LDAP, ADODB, or WMI queries.
