Group Metadata, Data Component DC0105

Archived: 2026-04-05 17:12:23 UTC

Group metadata includes attributes like name, permissions, purpose, and associated user accounts or roles, which adversaries may exploit for privilege escalation. Examples:

- Active Directory: `Get-ADGroup -Identity "Domain Admins" -Properties Members, Description`
- Azure AD: `Get-AzureADGroup -ObjectId <GroupId>`
- Google Workspace: `GET https://admin.googleapis.com/admin/directory/v1/groups/<groupKey>`
- AWS IAM: `aws iam list-group-policies --group-name <group_name>`
- Office 365: `GET https://graph.microsoft.com/v1.0/groups/<id>`

Data Collection Measures:

- Cloud Logging:
  - AWS CloudTrail for IAM group-related activities.
  - Azure AD Sign-In/Audit logs for metadata changes.
  - Google Admin Activity logs for API calls.
- Directory Logging: Log metadata access (e.g., Windows Event ID 4662).
- API Monitoring: Log API calls to modify group metadata (e.g., Microsoft Graph API).
- SIEM Integration: Centralize group metadata logs for analysis.
