# TTP Detail – T1087.004

## TTP Information

Name: Cloud Account

Description: Adversaries may attempt to get a listing of cloud accounts. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application.

With authenticated access there are several tools that can be used to find accounts. The <code>Get-MsolRoleMember</code> PowerShell cmdlet can be used to obtain account names given a role or permissions group in Office 365.(Citation: Microsoft msolrolemember)(Citation: GitHub Raindance) The Azure CLI (AZ CLI) also provides an interface to obtain user accounts with authenticated access to a domain. The command <code>az ad user list</code> will list all users within a domain.(Citation: Microsoft AZ CLI)(Citation: Black Hills Red Teaming MS AD Azure, 2018)

The AWS command <code>aws iam list-users</code> may be used to obtain a list of users in the current account while <code>aws iam list-roles</code> can obtain IAM roles that have a specified path prefix.(Citation: AWS List Roles)(Citation: AWS List Users) In GCP, <code>gcloud iam service-accounts list</code> and <code>gcloud projects get-iam-policy</code> may be used to obtain a listing of service accounts and users in a project.(Citation: Google Cloud - IAM Servie Accounts List API)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: discovery

## Tools

* AADInternals
* Pacu
* ROADTools

## APTs (Intrusion Sets)

* APT29