# TTP Detail – T1087.002

## TTP Information

Name: Domain Account

Description: Adversaries may attempt to get a listing of domain accounts. This information can help adversaries determine which domain accounts exist to aid in follow-on behavior such as targeting specific accounts which possess particular privileges.

Commands such as <code>net user /domain</code> and <code>net group /domain</code> of the [Net](https://attack.mitre.org/software/S0039) utility, <code>dscacheutil -q group</code> on macOS, and <code>ldapsearch</code> on Linux can list domain users and groups. [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets including <code>Get-ADUser</code> and <code>Get-ADGroupMember</code> may enumerate members of Active Directory groups.(Citation: CrowdStrike StellarParticle January 2022)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Bankshot
* Bazar
* BlackCat
* BoomBox
* Cobalt Strike
* DUSTTRAP
* IceApple
* IcedID
* Latrodectus
* MgBot
* OSInfo
* POWRUNER
* SoreFang
* Stuxnet
* Sykipot
* Valak

## Tools

* AdFind
* BloodHound
* Brute Ratel C4
* CrackMapExec
* Empire
* Net
* PoshC2
* SILENTTRINITY
* dsquery

## APTs (Intrusion Sets)

* APT41
* BRONZE BUTLER
* BlackByte
* Chimera
* Dragonfly
* FIN13
* FIN6
* Fox Kitten
* INC Ransom
* Ke3chang
* LAPSUS$
* Lotus Blossom
* MuddyWater
* OilRig
* Poseidon Group
* RedCurl
* Sandworm Team
* Scattered Spider
* Storm-1811
* ToddyCat
* Turla
* Volt Typhoon
* Wizard Spider
* menuPass