# TTP Detail – T1087.001

## TTP Information

Name: Local Account

Description: Adversaries may attempt to get a listing of local system accounts. This information can help adversaries determine which local accounts exist on a system to aid in follow-on behavior.

Commands such as <code>net user</code> and <code>net localgroup</code> of the [Net](https://attack.mitre.org/software/S0039) utility and <code>id</code> and <code>groups</code> on macOS and Linux can list local users and groups.(Citation: Mandiant APT1)(Citation: id man page)(Citation: groups man page) On Linux, local users can also be enumerated through the use of the <code>/etc/passwd</code> file. On macOS, the <code>dscl . list /Users</code> command can be used to enumerate local accounts. On ESXi servers, the `esxcli system account list` command can list local user accounts.(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Agent Tesla
* Bankshot
* Bazar
* BitPaymer
* Comnie
* DUSTTRAP
* Duqu
* Elise
* Epic
* GeminiDuke
* HyperStack
* InvisiMole
* Kazuar
* Kwampirs
* MURKYTOP
* MgBot
* Milan
* Mis-Type
* OSInfo
* P.A.S. Webshell
* POWERSTATS
* PUNCHBUGGY
* Pikabot
* Pony
* RATANKBA
* Raccoon Stealer
* Remsec
* S-Type
* SHOTPUT
* SMOKEDHAM
* SoreFang
* Stuxnet
* TrickBot
* USBferry
* Valak

## Tools

* BloodHound
* Empire
* Net
* PoshC2
* PowerSploit
* Pupy

## APTs (Intrusion Sets)

* APT1
* APT3
* APT32
* APT41
* APT42
* Chimera
* Fox Kitten
* Ke3chang
* Lotus Blossom
* Moses Staff
* OilRig
* Poseidon Group
* RedCurl
* Threat Group-3390
* Turla
* Volt Typhoon
* admin@338