# TTP Detail – T1069.001

## TTP Information

Name: Local Groups

Description: Adversaries may attempt to find local system groups and permission settings. The knowledge of local system permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as the users found within the local administrators group.

Commands such as <code>net localgroup</code> of the [Net](https://attack.mitre.org/software/S0039) utility, <code>dscl . -list /Groups</code> on macOS, and <code>groups</code> on Linux can list local groups.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Caterpillar WebShell
* Cobalt Strike
* Emissary
* Epic
* Exbyte
* Flagpro
* FlawedAmmyy
* Gomir
* Helminth
* JPIN
* Kazuar
* Kwampirs
* LunarWeb
* OSInfo
* POWRUNER
* QakBot
* Sys10

## Tools

* BloodHound
* Net
* PoshC2
* SILENTTRINITY

## APTs (Intrusion Sets)

* Chimera
* HEXANE
* OilRig
* Tonto Team
* Turla
* Volt Typhoon
* admin@338