# TTP Detail – T1134.005

## TTP Information

Name: SID-History Injection

Description: Adversaries may use SID-History Injection to escalate privileges and bypass access controls. The Windows security identifier (SID) is a unique value that identifies a user or group account. SIDs are used by Windows security in both security descriptors and access tokens. (Citation: Microsoft SID) An account can hold additional SIDs in the SID-History Active Directory attribute (Citation: Microsoft SID-History Attribute), allowing inter-operable account migration between domains (e.g., all values in SID-History are included in access tokens).

With Domain Administrator (or equivalent) rights, harvested or well-known SID values (Citation: Microsoft Well Known SIDs Jun 2017) may be inserted into SID-History to enable impersonation of arbitrary users/groups such as Enterprise Administrators. This manipulation may result in elevated access to local resources and/or access to otherwise inaccessible domains via lateral movement techniques such as [Remote Services](https://attack.mitre.org/techniques/T1021), [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002), or [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: privilege-escalation

## Tools

* Empire
* Mimikatz