BloodHound, Software S0521 | MITRE ATT&CK®

Archived: 2026-04-05 13:24:34 UTC

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	BloodHound can identify users with local administrator rights.[2]
		.002	Account Discovery: Domain Account	BloodHound can collect information about domain users, including identification of domain admin accounts.[2]
Enterprise	T1560		Archive Collected Data	BloodHound can compress data collected by its SharpHound ingestor into a ZIP file to be written to disk.[1][4]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	BloodHound can use PowerShell to pull Active Directory information from the target environment.[2]
Enterprise	T1482		Domain Trust Discovery	BloodHound has the ability to map domain trusts and identify misconfigurations for potential abuse.[2]
Enterprise	T1615		Group Policy Discovery	BloodHound has the ability to collect local admin information via GPO.[1]
Enterprise	T1106		Native API	BloodHound can use .NET API calls in the SharpHound ingestor component to pull Active Directory data.[1]

Domain	ID		Name	Use
Enterprise	T1069	.001	Permission Groups Discovery: Local Groups	BloodHound can collect information about local groups and members.[2]
		.002	Permission Groups Discovery: Domain Groups	BloodHound can collect information about domain groups and members.[2]
Enterprise	T1018		Remote System Discovery	BloodHound can enumerate and collect the properties of domain computers, including domain controllers.[2]
Enterprise	T1033		System Owner/User Discovery	BloodHound can collect information on user sessions.[2]

Source: https://attack.mitre.org/software/S0521