OS Credential Dumping: Cached Domain Credentials, Sub-technique T1003.005 - Enterprise

Archived: 2026-04-05 13:14:45 UTC

Adversaries may attempt to access cached domain credentials used to allow authentication to occur in the event a domain controller is unavailable.[1]

On Windows Vista and newer, the hash format is DCC2 (Domain Cached Credentials version 2) hash, also known as MS-Cache v2 hash.[2] The number of default cached credentials varies and can be altered per system. This hash does not allow pass-the-hash style attacks, and instead requires Password Cracking to recover the plaintext password.[3]

On Linux systems, Active Directory credentials can be accessed through caches maintained by software like System Security Services Daemon (SSSD) or Quest Authentication Services (formerly VAS). Cached credential hashes are typically located at `/var/lib/sss/db/cache.[domain].ldb` for SSSD or `/var/opt/quest/vas/authcache/vas_auth.vdb` for Quest. Adversaries can use utilities, such as `tdbdump`, on these database files to dump the cached hashes and use Password Cracking to obtain the plaintext password.[4]

With SYSTEM or sudo access, the tools/utilities such as Mimikatz, Reg, and secretsdump.py for Windows or Linikatz for Linux can be used to extract the cached credentials.[4]

Note: Cached credentials for Windows Vista are derived using PBKDF2.[2]

Source: https://attack.mitre.org/techniques/T1003/005