What are cached domain credentials?

Cached domain credentials (also called MSCache or DCC2) are hashes of domain users' passwords that Windows stores locally so a user can log in when no Domain Controller is reachable (laptops, remote sites). They are kept in the SECURITY hive. Unlike NT hashes they cannot be passed, only cracked offline, but a weak password cracks quickly. Dumping them with local admin yields domain passwords for everyone who has logged into that machine, including admins.

HOW IT WORKS

01 The dump and payload

With local admin or SYSTEM, dump the cache and crack it:

- Extract DCC2 hashes: `secretsdump.py -security security.hiv -system system.hiv LOCAL` (shows `$DCC2$` entries).
- These cannot be passed (the format is not usable for Pass-the-Hash), so crack them offline: `hashcat -m 2100 dcc2.txt wordlist`.
- A weak domain password cracks fast, handing the attacker a cleartext domain credential, potentially an admin who logged in once.

Documented techniques shown for defenders.

> CRACK-ONLY, BUT WORTH IT
>
> *DCC2 hashes cannot be passed, only cracked, but a machine that a Domain Admin once logged into may cache *their* credential. One weak password is a domain foothold.*

HOW TO DEFEND

- Reduce the number of cached logons via policy (down to 1 or 0 on sensitive hosts) so fewer credentials sit on each machine.
- Keep privileged accounts off ordinary workstations so their credentials are never cached there (tiered administration).
- Enforce strong domain passwords so DCC2 hashes resist cracking.
- Limit local-admin rights needed to dump the SECURITY hive.
- Detect SECURITY hive access and offline-cracking indicators.

SOURCES

[1] MITRE ATT&CK: OS Credential Dumping (T1003)

[2] Microsoft: Windows credential protection

[3] MITRE ATT&CK: Credential Access (TA0006)

Find the exposed credentials before an attacker does.

securelayer7.net/learn/credential-access/what-are-cached-domain-credentials

Open online