What is credential dumping?

Credential dumping is extracting stored account credentials from a system, typically password hashes from the Windows SAM and the LSASS process, the NTDS.dit database on a Domain Controller, or `/etc/shadow` on Linux. The dumped hashes are then cracked or passed to authenticate elsewhere. It usually requires local admin or SYSTEM, and tools like Mimikatz and secretsdump automate it. It maps to MITRE T1003.

HOW IT WORKS

01 How it is done

Dumping generally needs local admin or SYSTEM on the target. Common routes:

- LSASS memory: Mimikatz `sekurlsa::logonpasswords` or a process dump parsed offline.
- SAM + SYSTEM hives: save the registry hives and extract local hashes (`secretsdump.py`).
- NTDS.dit: pull it from a DC (often via a Volume Shadow Copy) or with DCSync.
- /etc/shadow: read it as root and crack with John.

02 What happens to the dump

Dumped credentials are turned into access two ways:

- Crack the hash offline with Hashcat or John to recover the cleartext password.
- Use the hash directly with Pass-the-Hash, no cracking needed for NTLM authentication.

Either way the attacker now authenticates as that account and continues across the network.

> NEEDS ADMIN, RETURNS HASHES
>
> *Credential dumping almost always needs local admin or SYSTEM, and what it returns is hashes, cracked offline or passed directly. Limiting local admin limits dumping.*

SOURCES

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

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

[3] NIST SP 800-63B Digital Identity Guidelines

Find the exposed credentials before an attacker does.

`securelayer7.net/learn/credential-access/what-is-credential-dumping`

Open online