What is the SAM database?

The SAM (Security Account Manager) is the Windows registry hive that stores the password hashes of local accounts on a machine (`HKLM\SAM`). The hashes are NT hashes, encrypted with a key (the boot key) held in the SYSTEM hive, so an attacker needs both. With local admin or SYSTEM they save the hives or read them from memory, extract the local hashes, and crack or pass them. Reused local-admin passwords make a single SAM dump a path across many machines.

HOW IT WORKS

01 The dump and payload

With local admin or SYSTEM, the attacker grabs both hives and extracts the hashes:

- Save the hives: `reg save HKLM\SAM sam.hiv` and `reg save HKLM\SYSTEM system.hiv`
- Extract local NT hashes offline: `secretsdump.py -sam sam.hiv -system system.hiv LOCAL`
- Or live, in memory, with a credential tool that reads the SAM directly.

The result is every local account's NT hash, ready to crack or use via Pass-the-Hash. Documented techniques shown for defenders.

> SAM + SYSTEM TOGETHER
>
> *The SAM hashes are useless without the boot key in the SYSTEM hive. Attackers always take both. A reused local-admin hash from one SAM then unlocks every machine that shares it.*

HOW TO DEFEND

- Use [LAPS](/learn/active-directory/what-is-laps) so every machine has a unique local-admin password and one SAM dump unlocks only that host.
- Limit local-administrator rights, the prerequisite for dumping the SAM.
- Enable [Credential Guard](/learn/active-directory/what-is-credential-gu and restrict debug/SYSTEM access.
- Detect `reg save` of SAM/SYSTEM and suspicious access to the hives.
- Disable NTLM where possible so a passed local hash is less useful.

SOURCES

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

[2] Microsoft: Windows credential security

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

Find the exposed credentials before an attacker does.

`securelayer7.net/learn/credential-access/what-is-the-sam-database`

Open online