What are LSA secrets?

LSA secrets are a protected area of the Windows registry (`HKLM\SECURITY\Policy\Secrets`) where the Local Security Authority stores sensitive credentials: service account passwords, auto-logon passwords, machine account secrets, and cached data. Many of these decrypt back to cleartext, not just hashes, so dumping LSA secrets with local admin/SYSTEM can hand an attacker working passwords for services and scheduled tasks, sometimes high-privilege ones. It is a core target of credential dumping.

HOW IT WORKS

01 The dump and payload

With local admin or SYSTEM, the attacker dumps LSA secrets:

- Save the hives and extract them: `secretsdump.py -security security.hiv -system system.hiv LOCAL`
- Or read them live with a credential tool (`-lsadump::secrets`).

Out come service-account and auto-logon passwords in cleartext. A service running as a domain account is especially valuable, that cleartext password is immediately reusable across the domain. Documented techniques shown for defenders.

> OFTEN CLEARTEXT
>
> *Unlike SAM hashes, many LSA secrets decrypt to cleartext passwords, including service accounts that may be domain-privileged. That makes LSA secrets one of the highest-value dumps on a host.*

HOW TO DEFEND

- Use [gMSAs](/learn/active-directory/what-is-a-gmsa) for services so passwords are machine-managed and not reusable cleartext.
- Avoid auto-logon and never store privileged credentials in service/scheduled-task configs.
- Limit local-admin rights and enable Credential Guard.
- Run services with least privilege, never with Domain Admin.
- Detect access to the SECURITY hive and LSA secret dumps.

SOURCES

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

[2] Microsoft: Windows Server security

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

Find the exposed credentials before an attacker does.

`securelayer7.net/learn/credential-access/what-are-lsa-secrets`

Open online