What is a shadow copy attack?

A Volume Shadow Copy attack abuses Windows VSS, the snapshot feature behind backups, to copy files that are locked while Windows runs, most importantly NTDS.dit (the Active Directory database) and the SAM/SYSTEM hives. With admin rights an attacker creates a shadow copy and reads those files from the snapshot, then extracts every domain hash offline. It is a classic way to dump a Domain Controller's entire credential store without touching the live, locked files.

HOW IT WORKS

01 The attack and payload

On a Domain Controller (or any host), with admin rights:

- Create a shadow copy: `vssadmin create shadow /for=C:`
- Copy the locked files from the snapshot: `NTDS.dit` and `SYSTEM` (and `SAM`).
- Extract every domain account's NT hash offline: `secretsdump.py -ntds ntds.dit -system system.hiv LOCAL`.

The result is the entire domain's password hashes, including krbtgt. Built-in tools like `ntdsutil` and `diskshadow` do the same. Documented techniques shown for defenders.

> COPY WHAT IS LOCKED
>
> *VSS lets an attacker copy NTDS.dit and the hives even though Windows locks them. On a DC that is the whole domain's credentials in one move, using only built-in tools.*

HOW TO DEFEND

- Tightly restrict Domain Controller access: only Domain Admins should log in, and that group should be tiny.
- Monitor for `vssadmin`, `ntdsutil`, and `diskshadow` use and shadow-copy creation on DCs.
- Detect NTDS.dit and hive reads and copies off the DC.
- Limit local admin broadly so the technique is unavailable on member hosts.
- Rotate [krbtgt](/learn/active-directory/what-is-krbtgt) if a DC dump is suspected.

SOURCES

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

[2] Microsoft: Volume Shadow Copy Service

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

Find the exposed credentials before an attacker does.

securelayer7.net/learn/credential-access/what-is-a-volume-shadow-copy-attack

Open online