What are shadow credentials?

A Shadow Credentials attack abuses the msDS-KeyCredentialLink attribute, which stores public keys for certificate-based (PKINIT) authentication. An attacker who can write that attribute on a target account adds their own key, authenticates as the account via Kerberos PKINIT, and recovers its NT hash, a stealthy account takeover that needs no password reset. It requires the domain to support Key Trust (PKINIT, typically via AD CS). Defend by auditing write access to msDS-KeyCredentialLink and monitoring changes to it.

HOW IT WORKS

01 How the attack works

With write access to a target's msDS-KeyCredentialLink (often via GenericWrite or a delegation), the attacker adds a key with `Whisker add /target:victim$`, then requests a TGT via PKINIT with `Rubeus asktgt /certificate:... /getcredentials`, which returns the account's NT hash. From there they impersonate the account. It relies on the domain supporting PKINIT (Key Trust via AD CS). Payloads are shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Key Trust authentication (Windows Hello for Business)

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/shadow-credentials

Open online