What is overpass-the-hash?

Overpass-the-hash, also called pass-the-key, converts a stolen NT hash (or AES key) into a legitimate Kerberos Ticket Granting Ticket. Instead of replaying the hash over NTLM, the attacker uses it as the account's Kerberos long-term key to request a TGT, then authenticates over Kerberos to any service. This blends into normal Kerberos traffic and reaches services that reject NTLM. Defend by protecting credential material (LSASS, Credential Guard), preferring AES, and detecting anomalous ticket requests.

HOW IT WORKS

01 How the attack works

After dumping a hash (for example from LSASS), the attacker requests a TGT with the hash as the key using `Rubeus asktgt /user:<user> /rc4:<nthash> /ptt`, or `mimikatz sekurlsa::pth /user:<user> /ntlm:<hash>`. The returned TGT is injected into the session, and the attacker then requests service tickets and moves laterally over Kerberos. Using the account's AES key instead of the RC4 hash makes it blend in even more. Shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Kerberos authentication overview

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/overpass-the-hash

Open online