NTLM relay and Pass-the-Hash.

NTLM is the legacy Windows authentication protocol, and it has two abuse classes. In Pass-the-Hash, an attacker who has stolen a user's NTLM hash authenticates as that user without ever knowing or cracking the plaintext, because NTLM treats the hash as the secret. In NTLM relay, the attacker sits in the middle, captures a victim machine's authentication, and forwards it to another server to act as that victim, often without touching a password at all. Both are why Microsoft is steadily disabling NTLM and why SMB signing and removing NTLM are core AD hardening steps.

HOW IT WORKS

01 How it drives lateral movement

Pass-the-Hash is the engine of lateral movement. The pattern is:

1. Compromise one machine and dump the hashes of everyone logged in to it. 2. Reuse a hash to authenticate to the next machine where that account has access. 3. Dump that machine's memory for fresh, more privileged hashes. 4. Repeat until a Domain Admin's hash appears.

The problem is amplified by password reuse: a single local administrator password shared across hundreds of machines means one stolen hash unlocks all of them.

02 NTLM relay, in one idea

NTLM relay does not even require stealing a stored hash. The attacker tricks or waits for a victim machine to authenticate to a server the attacker controls, then forwards that authentication, live, to a different target server.

The target sees a valid NTLM authentication and grants access as the victim. Tools like ntlmrelayx automate it. Relay is especially dangerous against services that do not enforce signing, and it has powered serious chains when combined with coercion tricks that force a Domain Controller to authenticate to the attacker.

HOW TO DEFEND

- Enable SMB signing and channel binding so relayed authentication is rejected.
- Disable NTLM where you can and move to Kerberos, then audit for remaining NTLM use.
- Use the Protected Users group and Credential Guard so privileged hashes are not left in memory to steal.
- Use LAPS to give every machine a unique local administrator password, killing hash reuse across the estate.
- Limit where Domain Admins log in. A privileged hash that never lands on an ordinary workstation cannot be dumped from one.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Kerberos Authentication Overview

[3] NIST SP 800-115 Technical Guide to Security Testing

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/ntlm-relay-pass-the-hash

Open online