What is Pass-the-Hash?

Pass-the-Hash (PtH) is an attack where an attacker authenticates as a user using their NTLM password hash directly, without knowing or cracking the plaintext. NTLM treats the hash as the secret, so a hash stolen from LSASS memory or NTDS.dit is enough to log in. It is the engine of lateral movement across a Windows network, and it is amplified by reused local-administrator passwords. The strongest single defence is LAPS.

HOW IT WORKS

01 Lateral movement and payload

Pass-the-Hash drives the climb to Domain Admin:

1. Compromise a machine and dump hashes: `sekurlsa::logonpasswords` (Mimikatz). 2. Reuse a hash to authenticate to the next machine: `wmiexec.py -hashes :<nt-hash> corp.local/admin@host` or `psexec.py -hashes ...` (Impacket). 3. Dump that machine for fresher, more privileged hashes; repeat until a Domain Admin hash appears.

Reused local-admin passwords let one stolen hash unlock hundreds of machines. Documented techniques shown for defenders.

> THE AMPLIFIER
>
> *A single shared local-administrator password across many machines means one harvested hash unlocks them all. Unique per-machine passwords (LAPS) break that chain.*

HOW TO DEFEND

- Deploy LAPS so every machine has a unique, rotating local-admin password.
- Enable Credential Guard and add privileged accounts to Protected Users so reusable hashes are not left in memory.
- Keep Domain Admins off ordinary workstations, the most common source of harvestable hashes.
- Prefer Kerberos and disable NTLM where possible, then audit remaining NTLM use.
- Detect lateral authentication patterns and LSASS access.

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/what-is-pass-the-hash

Open online