What is LAPS?

LAPS (Local Administrator Password Solution) is a Microsoft feature that gives every machine a unique, random local-administrator password that rotates automatically, stored in Active Directory and readable only by authorised admins. It directly breaks Pass-the-Hash lateral movement, because a local-admin hash stolen from one machine no longer unlocks any other. It is one of the highest-impact Active Directory hardening steps, with one rule: tightly control who can read the stored passwords.

HOW IT WORKS

01 Why it matters and the one caveat

LAPS removes the password reuse that makes Pass-the-Hash so powerful:

- A local-admin hash dumped from one machine no longer works on the next, because every machine's password is different.
- That alone can break a lateral-movement chain at its most common rung.

The caveat is read access: whoever can read the LAPS password attribute can get local admin on those machines. If those read rights are over-granted, an attacker who reaches such an account collects local-admin passwords directly:

- `pyLAPS.py --action get -u user -p pass -d corp.local` or BloodHound's ReadLAPSPassword edge

So LAPS shifts the risk to a small, auditable "who can read it" question.

> THE REUSE KILLER
>
> *LAPS is the single most effective stop for Pass-the-Hash lateral movement. Deploy it broadly, then make sure only the right admins hold ReadLAPSPassword.*

02 How to use LAPS well

- Deploy LAPS everywhere, so every machine has a unique, rotating local-admin password.
- Restrict who can read the LAPS attribute to the minimal admin set, and audit it with BloodHound (ReadLAPSPassword).
- Prefer Windows LAPS (built in, supports encryption and Entra ID).

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Best Practices for Securing Active Directory

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

- Pair with Credential Guard and Protected Users so harvested credentials are scarce in the first place.
- Monitor for bulk reads of LAPS passwords.

Test your Active Directory before an attacker does.
securelayer7.net/learn/active-directory/what-is-laps

Open online