LAPS: What is LAPS - Secframe

secframe.com/docs/ramp/phase1/laps/what_is_laps

LAPS: What is LAPS

What is LAPS? Local Admin Password Solution

Laps is Microsoft's deployment to remedy the issue of password reuse on local administrator accounts. The base for LAPs is based from a github repo Admpwd.

What happens when computers have he same local password

Attackers love easy paths through a network or domain. Attackers don't use unique attacks. they repeat the eay they come into a network. They repeat the way they move through a network.

Creating unique and complex local passwords for computers, and rotating those password hinders an attached movement

A Typical 24 hour attack

1. Beachhead (Phishing Attack, etc.)
2. Lateral Movement
    1. Steal Credentials
    2. Compromise more hosts & credentials
3. Privilege Escalation
    1. Get Domain Admin credentials
4. Execute Attacker Mission
    1. Steal data, destroy systems, etc.
    2. Persist Presence

> source: Critical Hygiene for Preventing Major Breaches

Item #2 is what LAPS targets to remediate. The compromising of an entire computer system because of common passwords.

LAPS Free or Open Source Tools

Tool Name	Download URL	Secframe Quick Deploy Guide
Microsoft LAPS	Microsoft LAPS	Install and Configure LAPS
AdmPwd	AdmPwd project	Not yet Written
AdmPwd.E	AdmPwd.E	Not yet Written