What is Mimikatz?

Mimikatz is an open-source Windows post-exploitation tool, written by Benjamin Delpy, that extracts credentials from a compromised machine: NTLM hashes and plaintext passwords from LSASS memory, Kerberos tickets, and domain hashes via DCSync. It also forges Kerberos tickets (Golden and Silver). It needs local administrator rights to read LSASS, and it is the reference implementation for most Active Directory credential attacks. Defenders use the same tool to test exposure.

HOW IT WORKS

01 What it does and payload

The common Mimikatz commands map directly to AD attacks:

- Harvest credentials from memory: `sekurlsa::logonpasswords`
- Steal the KRBTGT hash via replication: `lsadump::dcsync /user:krbtgt`
- Forge a Golden Ticket: `kerberos::golden /user:Administrator /sid:<SID> /krbtgt:<hash> /ptt`

Reading LSASS requires local administrator or SYSTEM rights, which is why the first foothold and any local escalation matter. Shown here for defensive context.

> IT IS A SYMPTOM FINDER
>
> *If Mimikatz can harvest a Domain Admin credential from a workstation, the real problem is that the credential was there to harvest. Fix credential exposure, not just the tool.*

HOW TO DEFEND

- Enable Credential Guard to isolate LSASS secrets from tools like Mimikatz.
- Use the Protected Users group and LSASS protection (RunAsPPL).
- Keep Domain Admins off ordinary machines so their credentials are never cached where Mimikatz runs.
- Deploy LAPS so a harvested local-admin hash does not unlock other machines.
- Detect processes opening a handle to `lsass.exe` and abnormal Kerberos ticket activity.

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-mimikatz

Open online