What is credential access?

Credential access is the attacker phase of stealing account credentials, passwords, password hashes, Kerberos tickets, and API keys, to authenticate as legitimate users and spread through an environment. Credentials are harvested from memory (LSASS), registry hives (SAM, LSA secrets), disk (config files, /etc/shadow), the network (LLMNR poisoning), and applications (browsers, Credential Manager). It is the engine behind lateral movement, because a reused credential turns one host into many.

HOW IT WORKS

01 Where credentials hide

Credentials live in many places, each with its own page:

- Memory: the LSASS process caches signed-in users' secrets.
- Registry hives: the SAM (local hashes), LSA secrets, and cached domain credentials.
- Application stores: DPAPI, Credential Manager, and browsers.
- Disk: /etc/shadow and unsecured credentials in files.
- The network: LLMNR poisoning captures hashes on the wire.

02 What attackers do with credentials

Harvested credentials feed straight into lateral movement. Cleartext passwords are reused directly; hashes are either cracked with Hashcat or John, or used as-is via Pass-the-Hash; tickets are replayed with Pass-the-Ticket.

The loop, dump on host A, reuse on host B, dump host B, is what carries an attacker to a Domain Controller.

> CREDENTIALS ARE THE CURRENCY
>
> *Almost every serious intrusion runs on stolen credentials, not exploits. Harvest, reuse, repeat is how one foothold becomes domain-wide control.*

SOURCES

[1] MITRE ATT&CK: Credential Access (TA0006)

[2] MITRE ATT&CK: OS Credential Dumping (T1003)

[3] NIST SP 800-63B Digital Identity Guidelines

Find the exposed credentials before an attacker does.

securelayer7.net/learn/credential-access/what-is-credential-access

Open online