Credential access, in plain terms.

Credential access is the engine of lateral movement: harvest a password, hash, or ticket on one host, reuse it on the next. This section breaks the Windows credential stores (SAM, DPAPI, LSA secrets, cached domain credentials, Credential Manager), the Linux and network angles (/etc/shadow, LLMNR poisoning), and cracking (Hashcat, John) into plain-language explainers, each ending with how a penetration test finds the exposure in your environment.

HOW IT WORKS

01 Key terms explained

Plain-language definitions of the credential stores and techniques behind credential theft. Each page covers what it is, the attack, the payload, and how to defend.

Windows credential stores

- What is the SAM database?
- What is DPAPI?
- What are LSA secrets?
- What are cached domain credentials?
- What is Windows Credential Manager?
- What is a Volume Shadow Copy attack?
- What is an NT hash?
- What is browser credential theft?

Linux, network and cracking

- What is /etc/shadow?
- What is LLMNR poisoning?
- What is Hashcat?
- What is John the Ripper?
- What are unsecured credentials?

Related (Active Directory)

- What is LSASS?
- What is Mimikatz?
- Pass-the-Hash
- DCSync, Golden and Silver tickets

02 How to read this section

SOURCES

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

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

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

The pages follow how an attacker collects credentials and reuses them.

- Foundations first: credential access and credential dumping.
- Windows credential stores: where Windows keeps secrets (SAM, DPAPI, LSA secrets, cached domain credentials, Credential Manager) and how each is extracted, plus the NT hash format and shadow-copy theft.
- Linux, network and cracking: /etc/shadow, capturing hashes on the wire with LLMNR poisoning, and cracking them with Hashcat and John.
- Related: the Active Directory credential pages (LSASS, Mimikatz, Pass-the-Hash, DCSync) that pair with this section.

Each explainer ends with how a penetration test confirms the exposure in your own environment.

Find the exposed credentials before an attacker does.

securelayer7.net/learn/credential-access

Open online