What is an NT hash?

An NT hash (often called the NTLM hash) is the value Windows derives from a user's password and stores instead of the password itself, MD4 of the UTF-16 password, with no salt. Windows uses it directly to authenticate over NTLM, which is why a stolen NT hash can be reused without cracking via Pass-the-Hash. Because it is unsalted, identical passwords produce identical hashes, and weak ones crack fast. It is the core credential in Windows attacks.

HOW IT WORKS

01 Why it matters and payload

The NT hash is special because of how it is used:

- Pass-the-Hash: authenticate to other systems with the hash, no cracking needed (`secretsdump-/psexec.py -hashes`). See Pass-the-Hash.
- Cracking: because it is unsalted MD4, weak passwords fall fast: `hashcat -m 1000 hashes.txt wordlist`.
- Comparison: identical NT hashes reveal users sharing a password (for example a common local-admin password across machines).

Documented for defensive context.

> USABLE WITHOUT CRACKING
>
> *The NT hash's danger is that Windows accepts it directly for NTLM auth, so an attacker often does not need the password at all. Unsalted MD4 also means weak passwords crack in seconds.*

HOW TO DEFEND

- Reduce or disable NTLM in favor of Kerberos so passing the hash stops working.
- Use [LAPS](/learn/active-directory/what-is-laps) so no two machines share a local NT hash.
- Enforce long, unique passwords so any cracking is infeasible.
- Enable [Credential Guard](/learn/active-directory/what-is-credential-gu to keep hashes out of reach in memory.
- Limit local admin so hashes are hard to dump in the first place.

SOURCES

[1] Microsoft: NTLM overview

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

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

Find the exposed credentials before an attacker does.

`securelayer7.net/learn/credential-access/what-is-an-nt-hash`

Open online