What is NTDS.dit?

NTDS.dit is the main Active Directory database file, stored on every Domain Controller (usually at `C:\Windows\NTDS\ntds.dit`). It holds every directory object and, critically, the password hash of every user and computer account in the domain. An attacker who copies it, together with the SYSTEM registry hive needed to decrypt it, walks away with the credentials of the entire organisation, including Domain Admins and KRBTGT. Stealing NTDS.dit is one of the clearest "game over" events in Active Directory, which is why it sits at the very top of the assets that must be protected.

HOW IT WORKS

01 The attack: dumping every hash

Once an attacker reaches a Domain Controller or Domain Admin rights, extracting NTDS.dit gives them every credential in one move. Unlike harvesting hashes machine by machine, this is the whole domain at once: every user, every service account, the Domain Admins, and KRBTGT (whose hash then enables Golden Tickets).

With every hash in hand, the attacker can Pass-the-Hash as anyone, crack passwords offline at leisure, and maintain access long after the incident appears closed. There is no partial recovery: a stolen NTDS.dit means every password in the domain should be considered compromised.

02 How the attack runs

Attackers either pull the hashes remotely via replication or copy the file from the DC. The documented methods include:

- Remote, over DCSync replication: `secretsdump.py -just-dc corp.local/admin@dc-ip`
- From a shadow copy of the volume, then offline: `secretsdump.py -ntds ntds.dit -system SYSTEM LOCAL` (Impacket)
- Native extraction on the DC with `ntdsutil` "ifm" snapshots

Each ends the same way: a complete list of domain password hashes. These are well-known techniques included for defenders to recognise.

HOW TO DEFEND

- Harden and isolate Domain Controllers. Only Tier 0 admins should ever touch them, and never from an ordinary workstation.
- Keep Domain Admin credentials off lower-tier machines so an attacker cannot pivot up to a DC in the first place.
- Monitor for DCSync replication from non-DC sources and for volume shadow-copy activity on Domain Controllers.
- Restrict backup access, since DC backups contain NTDS.dit and are a softer target than the live DC.
- Alert on `ntdsutil` and secretsdump-style activity on Domain Controllers.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Kerberos Authentication Overview

[3] NIST SP 800-115 Technical Guide to Security Testing

NO PARTIAL BREACH

If NTDS.dit leaves your Domain Controller, treat every account as compromised, including KRBTGT. Recovery means a domain-wide password reset and the KRBTGT double-reset, not cleaning up a single account.

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/what-is-ntds-dit

Open online