What is a DACL backdoor?

A DACL backdoor is persistence created by editing the discretionary access control list (DACL) on Active Directory objects to grant an attacker hidden rights, for example DCSync on the domain, GenericAll on a privileged group, or password-reset on an admin account. The rights survive password resets and blend into normal object permissions, so they are easy to miss. Defend by auditing ACLs on tier-0 objects with BloodHound and monitoring for DACL changes.

HOW IT WORKS

01 How the attack works

With enough rights the attacker adds an ACE granting themselves control, for example DCSync on the domain via `Add-DomainObjectAcl -TargetIdentity 'DC=corp,DC=local' -Rights DCSync`, or GenericAll on a privileged group, or password-reset on an admin. From then on they can dump hashes or seize the account at will. Impacket's `dacledit` does the same over the network. Payloads are shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: How access tokens and ACLs work

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/dacl-backdoor

Open online