What is an LDAP relay attack?

An LDAP relay attack is an NTLM relay aimed at a domain controller's LDAP (or LDAPS) service. The attacker coerces or captures a victim's NTLM authentication and forwards it to LDAP; if LDAP signing and channel binding are not enforced, the relayed session performs privileged writes as the victim, for example granting resource-based constrained delegation or adding shadow credentials to take over a target account. Defend by enforcing LDAP signing and channel binding, disabling NTLM, and reducing coercion surfaces.

HOW IT WORKS

01 How the attack works

The attacker starts a relay to LDAP with `ntlmrelayx.py -t ldap://<dc> --delegate-access` (or `--add-computer` / shadow-credential options), then coerces a target machine to authenticate (via PetitPotam, the printer bug, or poisoning). The relayed session writes msDS-AllowedToActOnBehalfOfOtherIdentity (RBCD) or msDS-KeyCredentialLink (shadow credentials) on a target, after which the attacker impersonates it. Shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: How to enable LDAP signing

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/ldap-relay

Open online