# ACL and delegation abuse.

Active Directory lets administrators delegate fine-grained rights: who can reset whose password, edit which group, or modify which object's permissions. Attackers abuse these ACLs (access control lists) by chaining rights like GenericAll, WriteDACL, and ForceChangePassword into a route to privilege. Kerberos delegation, a feature that lets a service act on a user's behalf, has its own abuses (unconstrained, constrained, and resource-based delegation) that can let an attacker impersonate anyone, including a Domain Admin. None of it is a vulnerability in the classic sense. It is configuration, which is why it hides in plain sight.

## HOW IT WORKS

### 01 A worked example: targeted Kerberoasting

Suppose your compromised user has GenericWrite over a service account. On its own that looks minor. But you can:

1. Write a fake SPN onto that account using your GenericWrite. 2. Now that it has an SPN, Kerberoast it: request its ticket and crack the password offline. 3. If the cracked account is privileged, you have escalated.

This is how a single, boring-looking permission becomes a full escalation. The lesson: in AD, the danger is in how rights combine, not in any one right alone.

### 02 Kerberos delegation abuse

Delegation lets a service act on behalf of a user, for example a web app reaching a database as the logged-in user. Three flavours, three abuses:

- Unconstrained delegation: a server with this can capture the TGT of any user who connects, then impersonate them anywhere. If you can coerce a Domain Admin or a Domain Controller to connect, you win.
- Constrained delegation: limited to specific services, but S4U tricks can still let an attacker who controls the account impersonate other users to those services.

## HOW TO DEFEND

- Audit ACLs regularly with BloodHound and remove rights that no longer serve a purpose, especially WriteDACL and GenericAll on sensitive objects.
- Avoid unconstrained delegation entirely on anything but Domain Controllers, and mark privileged accounts as "sensitive and cannot be delegated."
- Protect the RBCD attribute. Restrict who can write `msDS-AllowedToActOnBehalfOfOtherIdentity` and watch for changes to it.
- Tier administration so that control of a low-value object never chains up to a Tier 0 asset.

## SOURCES

[1] Microsoft: Best Practices for Securing Active Directory

[2] MITRE ATT&CK Enterprise Matrix

[3] Microsoft: Active Directory Certificate Services

- Resource-based constrained delegation (RBCD): configured on the target object via the `msDS-AllowedToActOnBehalfOfOtherIdentity` attribute. If an attacker can write that attribute (often via GenericWrite or WriteDACL), they can grant a controlled machine the right to impersonate any user to the target, including a Domain Admin.

**Test your Active Directory before an attacker does.**

securelayer7.net/learn/active-directory/acl-and-delegation-abuse

Open online