AD enumeration and BloodHound.

Enumeration is the reconnaissance phase of an Active Directory attack: reading the directory to list users, groups, computers, sessions, and permissions, most of which any authenticated user can query over LDAP. BloodHound ingests that data and renders it as a graph, then finds the shortest path from an account you control to Domain Admin by following abusable rights like GenericAll, WriteDACL, and group membership. Because the same query that helps an attacker helps a defender, mapping your own graph is one of the highest-value AD security exercises.

HOW IT WORKS

01 What BloodHound does with it

BloodHound takes the collected data and stores it as a graph: nodes are users, groups, and computers; edges are relationships like "is a member of," "can reset the password of," or "has a session on."

The power is the query "shortest path to Domain Admins." Instead of a human eyeballing thousands of permissions, BloodHound highlights the exact chain: *your user* can write to *this group*, which can reset *this admin account*, which is a member of *Domain Admins*. What looked like noise becomes a three-hop route to total control.

02 The abusable rights to recognise

A handful of permission edges turn up again and again as the rungs of the ladder:

- GenericAll / GenericWrite: full or broad control over an object, often enough to reset its password or grab its credentials.
- WriteDACL: the right to rewrite an object's permissions, so you grant yourself whatever access you need.
- AddMember: the right to add accounts to a group, including privileged groups.
- ForceChangePassword: reset another user's password without knowing the old one.

Individually these are normal delegated-admin features. Strung together by BloodHound, they are an attack path.

SOURCES

[1] Microsoft: Best Practices for Securing Active Directory

[2] MITRE ATT&CK Enterprise Matrix

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

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/active-directory-enumeration-bloodhound

Open online