What is BloodHound?

BloodHound is an open-source tool that maps Active Directory attack paths. Its collector (SharpHound) gathers users, groups, sessions, and permissions, and BloodHound stores them as a graph to compute the shortest path to Domain Admin through abusable rights like GenericAll, WriteDACL, and group membership. Because the same map helps attackers and defenders, running BloodHound against your own directory is one of the highest-value Active Directory exercises.

HOW IT WORKS

01 How it is used and payload

Attackers run BloodHound after a foothold to plan the fastest route up; defenders run it to find the same routes first.

- Collect the data: `SharpHound.exe -c All` or `bloodhound-python -d corp.local -u user -p pass -c All`
- Load the output into BloodHound and run the built-in "Shortest Path to Domain Admins" query.
- Each highlighted edge (GenericWrite, WriteDACL, AddMember, ForceChangePassword) is a step to investigate.

Collection is non-destructive reconnaissance, but the output is a literal map of how to take over the domain, so treat it as sensitive.

> DEFENDER FIRST
>
> *Run BloodHound as a recurring audit. Cutting one over-broad edge can erase a whole class of attack paths to Tier 0, which beats hardening machines one by one.*

HOW TO DEFEND

- Run it against your own directory and review the shortest paths to Domain Admins and other Tier 0 assets.
- Cut needless edges: remove WriteDACL/GenericAll on sensitive objects, empty over-privileged groups, and prune stale delegations.
- Re-run after major changes to catch new short paths.
- Protect the collected data, since it is a complete attack map.
- Monitor for mass LDAP collection, a sign someone else is running it.

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/what-is-bloodhound

Open online