


Finding Abusable Active Directory Permissions with BloodHound

 blog.netwrix.com/2022/12/09/bloodhound-active-directory

Joe Dibley

BloodHound is a powerful tool that identifies vulnerabilities in Active Directory (AD). Cybercriminals abuse this tool to visualize chains of abusable Active Directory permissions that can enable them to gain elevated rights, including membership in the powerful Domain Admin group.

This guide is designed to help penetration testers use BloodHound to identify these vulnerabilities first, so enterprises can thwart attacks.

Handpicked related content:

[Active Directory Security Best Practices](#)

What Is BloodHound and How Does It Work?

BloodHound is an Active Directory reconnaissance and attack path management tool that uses graph theory to identify hidden relationships, user permissions, sessions and attack paths in a source Windows domain. Its primary purpose is providing cybersecurity experts with the insight required to defend their IT ecosystem from threat actors.

How does BloodHound work? A single-page JavaScript web app compiled with Electron, it stores Windows AD objects as nodes in a Neo4j database. It has a PowerShell ingestor and supports Azure as of version 4.0.

Collecting Active Directory Permissions

Because BloodHound is a data visualization and analysis tool, you should use it with a data collection tool such as SharpHound or AzureHound. To collect the set of your Active Directory permissions, take the following steps:

1. First, download and install the latest version of AzureHound or SharpHound, and then run it.
2. By default, it will create several JSON files and put them into one zip file. Drag and drop that zip file into BloodHound.
3. Explore the data using BloodHound as described below.

How BloodHound Works with Active Directory Permissions

BloodHound empowers AD penetration testers to map out attack paths — chains of access permissions and other security vulnerabilities that could enable attackers to move laterally and elevate their privileges in the environment. For example, they can use the search bar to find the Domain Users group and see whether the group has local admin rights anywhere and which AD objects it has control over.

The fact is, over the years, many organizations lose control of their Active Directory permissions. As the company grows and changes, the organization forgets to remove rights that users no longer need, creating vulnerabilities that attackers can take advantage of.

Privileges that are commonly abused include:

- **Reset Password** — The right to change the password of a user account without knowing their current password
- **Add Members** — The ability to add users to a particular group
- **Full Control** — The right to do anything you want to a user or group
- **Write Owner / Write DACL** — The right to change permissions and ownership over an object
- **Write** — The ability to write object attributes
- **Extended Rights** — A combination of various rights, including Reset Password (for a full reference from TechNet, [click here](#))

How to Use BloodHound to Collect Active Directory Permissions

The first step in mapping attack paths is collection of permissions. On a computer joined to the domain you want to gather permissions from, run the following PowerShell command:

```
Invoke-Bloodhound -CollectionMethod ACLs
```



This will create a CSV export of all Active Directory permissions, which we will then import into BloodHound.

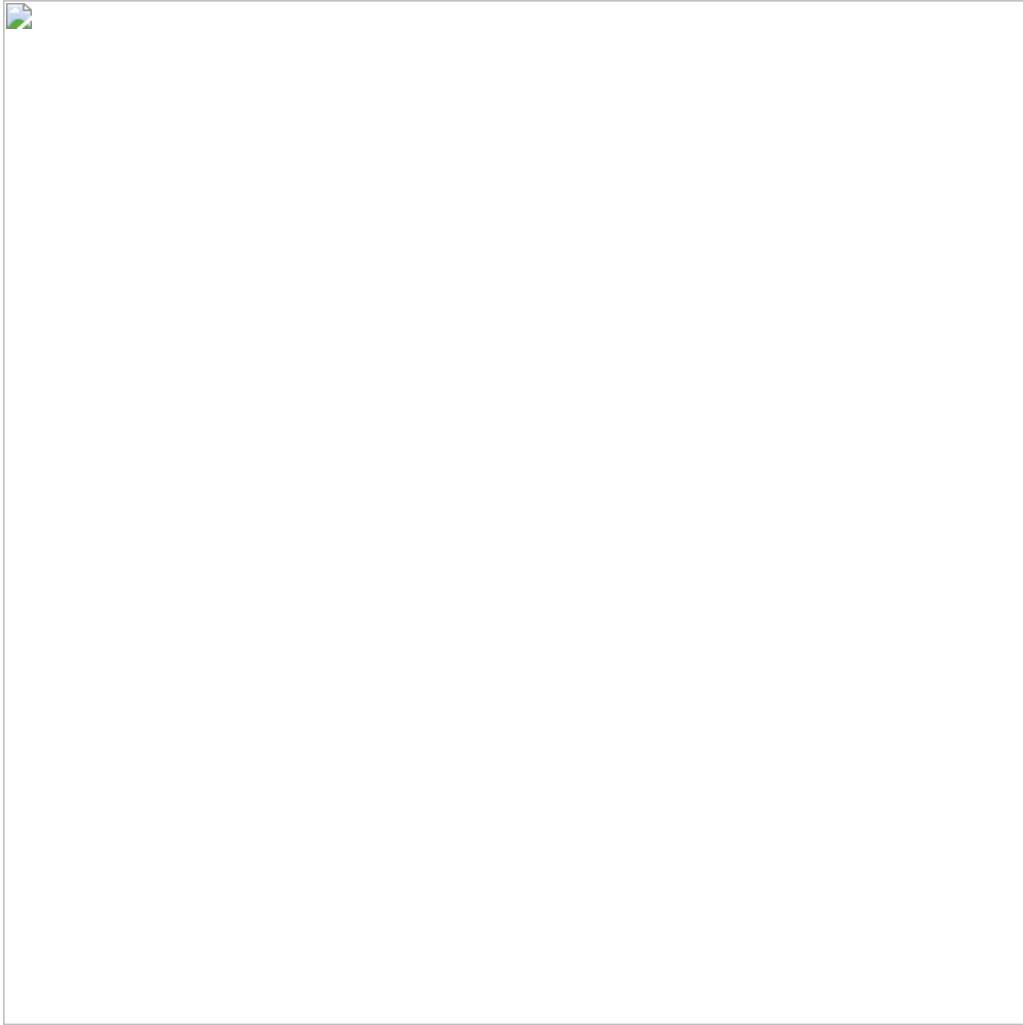
Example Attack Paths

Let's review several examples of attack paths.

Attack Path 1: Reset Password

The first BloodHound attack path we'll explore is the ability to reset user passwords.

The ability to reset a password will show up in BloodHound as an attack path labeled "ForceChangePassword":



By tying together multiple password resets, it may be possible to go from an unprivileged account to a Domain Admin, as illustrated below:



Note that if a user is actively using their account, they will notice if their password is reset. Accordingly, an attacker might check the last logon time for the account to see whether they can perform a password reset without being exposed.

Attack Path 2: Group Membership

Another attack path abuses the ability to write members to groups. By adding users to groups, an attacker can slowly elevate their access until they can add themselves to a group that has access to the sensitive data they are targeting. This approach is very useful to adversaries because they rarely need membership in a highly privileged group like Domain Admins to access the data they want, and adding a user to less-privileged groups rarely raises alarms.

In BloodHound, the ability to change a group will show up in an attack path with the label “AddMember”, as shown below:



By tying together a number of group membership changes, an attacker can slowly increase their rights until they reach their target. The example illustrates how an unprivileged user can become a Domain Admin through group membership changes:



Attack Path 3: Change Permissions

Changing permissions to an object lets you do basically anything you want. For example, you can give yourself the rights to change a group's membership, reset a password or extract valuable information from extended attributes. This is especially dangerous when using Local Administrator Password Solution (LAPS).

In BloodHound, the ability to change permissions to an object will be labeled "WriteDacl":



By tying together multiple permission changes, an attacker can move laterally and gain elevated rights, as shown below:



Attack Path 4: Combination Attacks

Most attack paths involve multiple types of permission. The example below illustrates three attack paths from the unprivileged user account “Michael” to a Domain Admin account:



How Netwrix Can Help You Protect Against Active Directory Permission Attacks

To improve your security, start by reviewing the permissions discussed above, since they are among the most commonly exploited rights.

BloodHound is a great way to visualize potential issues in your Windows [AD domain](#). However, it requires a lot of manual work. Accordingly, your cybersecurity team may be unable to use BloodHound to protect your assets and systems, especially when they are already preoccupied with projects and tech requests.

One of the best ways to decrease your Windows Active Directory domain attack surface is to use Netwrix's end-to-end [Active Directory security solution](#). Powerful, comprehensive, and user-friendly, our software helps you secure your Active Directory, prioritize your risk mitigation efforts, and strengthen your security posture. Specifically, our tool empowers you to:

- Identify, evaluate, and prioritize risks in your [AD security](#) posture
- Protect against identity theft
- Keep tabs on privilege changes
- Promptly detect and respond threats, including advanced threats like [Golden Ticket attacks](#) and [Kerberoasting](#)

- Minimize business disruptions with lightning-speed AD recovery

Joe Dibley

Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.

