BloodHound Cheat Sheet

redfoxsec.com/blog/bloodhound-cheat-sheet

Kunal Kumar July 17, 2023

- July 17, 2023
- Active Directory
- Kunal Kumar

BloodHound is a powerful security tool that uses graph theory to reveal the relationships between users, groups, and computers in a domain. In this comprehensive guide, we'll take a deep dive into BloodHound and its companion tool SharpHound, providing you with the knowledge and skills needed to navigate and utilize these tools to their fullest potential.

Introduction to BloodHound

BloodHound is an open-source tool that allows you to map out the relationships between users, groups, and computers in a domain. It uses graph theory to analyze the data it collects and visually represents the relationships between different entities. BloodHound can be used to identify potential attack paths, misconfigured permissions, and other security weaknesses in your Active Directory environment.

To start with BloodHound, you must install it on your system and connect it to your Active Directory domain. Once connected, you can use BloodHound to perform a variety of tasks, including:

- Identifying high-value targets
- Mapping out attack paths
- Analyzing permissions and access controls
- Finding misconfigured settings
- Identifying potential security weaknesses

SharpHound Enumeration Options

SharpHound is a companion tool to BloodHound to gather data from Active Directory. It provides various enumeration options that allow you to collect information about users, groups, and computers in a domain. These options include:

- CollectionMethod: This option determines which data is collected. The default option collects group membership, domain trust, local admin, and session information. Other options include group membership only, local admin only, RDP users, and more.
- Domainname: This option specifies the domain to enumerate.
- Stealth: This option lowers the amount of noise the tool generates and runs it single-threaded.
- ExcludeDomainControllers: This option excludes domain controllers from the enumeration process.
- ComputerFile: This option specifies a list of computer names or IPs to enumerate.
- LDAPFilter: This option filters on specific AD attributes.

SharpHound Connection & Performance Options

To use SharpHound effectively, you need to specify connection and performance options. These options include:

- DomainController: This option specifies which domain controller to use.
- Stealth: This option lowers the amount of noise the tool generates and runs it single-threaded.
- Throttle: This option specifies the delay between requests in milliseconds. The default value is 0.
- Jitter: This option adds jitter to the throttle value in percent.

SharpHound Output Options

SharpHound provides several options for outputting the data it collects. These options include:

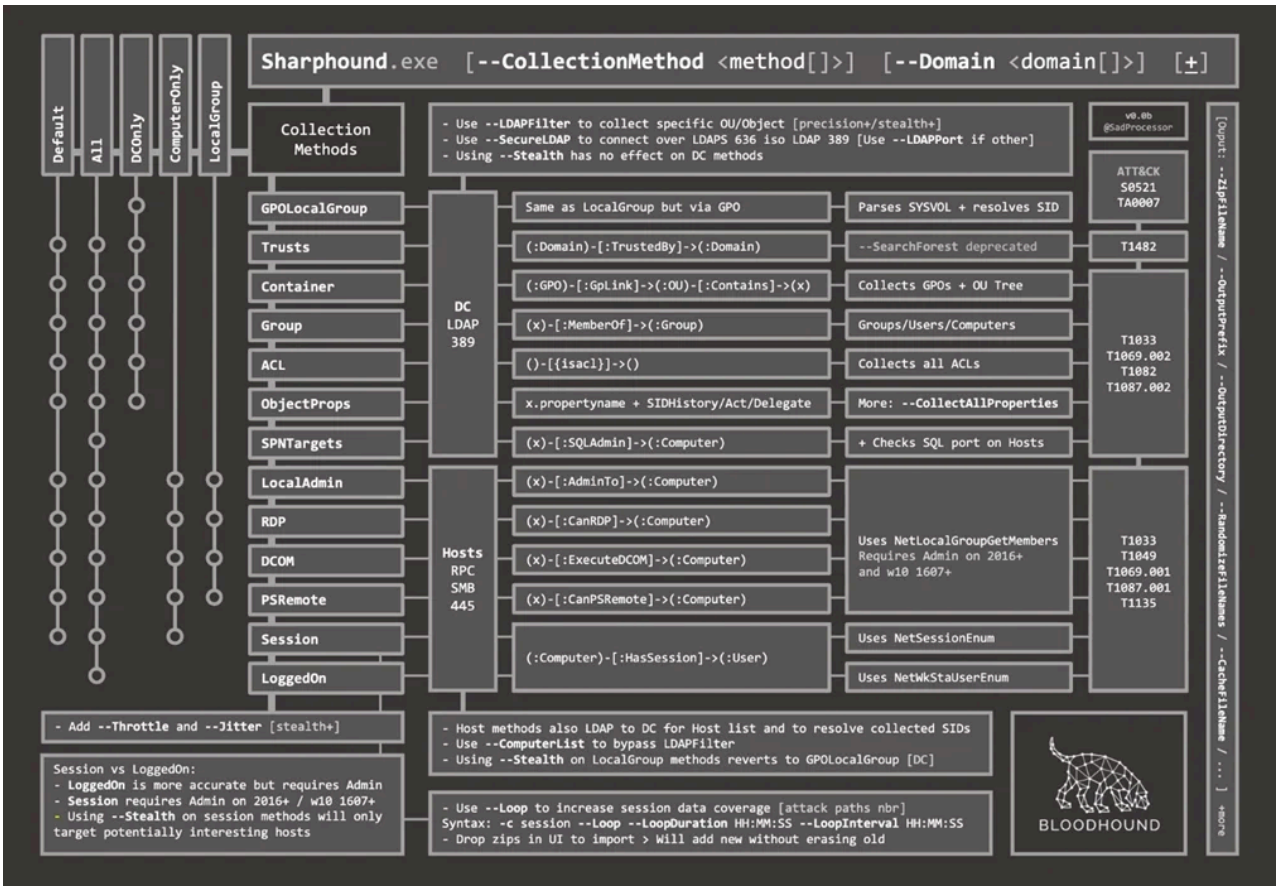
- OutputDirectory: This option specifies the directory to store the JSON output files. The default value is “.”.

- OutputPrefix: This option specifies the prefix for the JSON output files.
- PrettyJson: This option adds indentation to the JSON for readability but increases the file size.
- NoZip: This option disables the compression of JSON files.
- ZipFileName: This option specifies the filename for the zip file.
- EncryptZip: This option adds a password to the zip file, which is randomly generated.

SharpHound Loop Options

SharpHound also provides options for looping through the enumeration process. These options include:

- Loop: This option enables looping.
- LoopDuration: This option specifies the duration of the loop.
- LoopInterval: This option specifies the wait time between loops.



Handy DB Queries

Once you've collected data using SharpHound, you can utilize BloodHound to visualize the relationships between different entities. BloodHound uses a query language called Cypher to query the graph database. Here are some handy DB queries that you can use to analyze the data:

Count the LAPS status of all computers

MATCH (c:Computer) RETURN c.haslaps, COUNT(*)

Get a list of all OS versions with a count

MATCH (c:Computer) RETURN DISTINCT c.operatingsystem, COUNT(c.operatingsystem)

Get a list of all OS versions containing ‘Server’

MATCH (c:Computer) WHERE c.operatingsystem CONTAINS ‘Server’ RETURN DISTINCT c.operatingsystem

Get all Windows 2008 computers and sort by last logon timestamp descending and human-readable

MATCH (c:Computer) WHERE c.operatingsystem CONTAINS ‘2008’ RETURN c.name, c.operatingsystem, datetime({ epochSeconds: toInteger(c.lastlogontimestamp) }) AS rdate ORDER BY rdate DESC

Get all Domain Admins

MATCH (g:Group) WHERE g.name =~ “(?i).*DOMAIN ADMINS.*” WITH g MATCH (g)<-[r:MemberOf*1..]-(a) RETURN a.name

Get active sessions of Domain Admins

MATCH (u:User)-[:MemberOf*1..]->(g:Group) WHERE g.objectid ENDS WITH ‘-512’ MATCH p = (c:Computer)-[:HasSession]->(u) RETURN c.name, u.name

Find all Kerberoastable users

MATCH (u:User) WHERE u.hasspn=true RETURN u.name

Find all AS-REP-roastable users

MATCH (u:User {dontreqpreauth: true}) RETURN u.name

Get the local admins to all computers

MATCH p=(u:User)-[r:AdminTo]->(c:Computer) RETURN u.name, c.name ORDER BY u.name

Find all Kerberoastable users with the path to DA

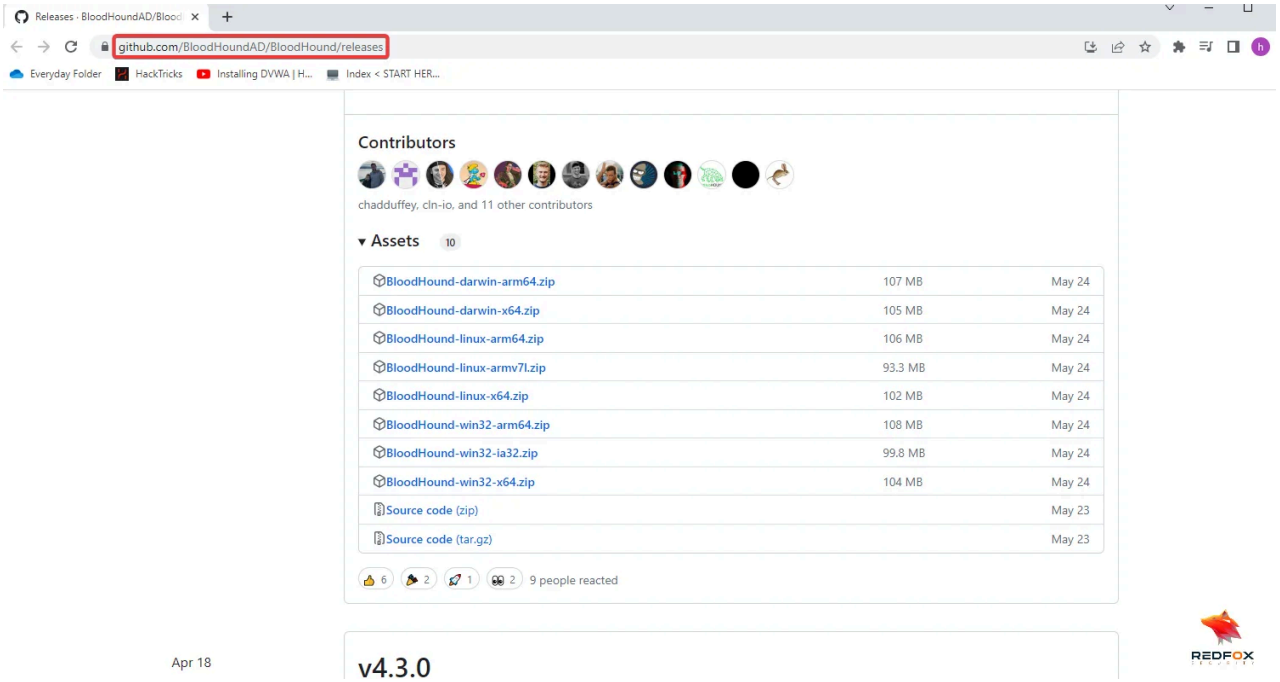
MATCH (u:User {hasspn:true}) MATCH (g:Group) WHERE g.name CONTAINS ‘DOMAIN ADMINS’ MATCH p = shortestPath((u)-[*1..]->(g)) RETURN p

Find all computers domain users can RDP to

MATCH p=(g:Group)-[:CanRDP]->(c:Computer) WHERE g.objectid ENDS WITH ‘-513’ RETURN p

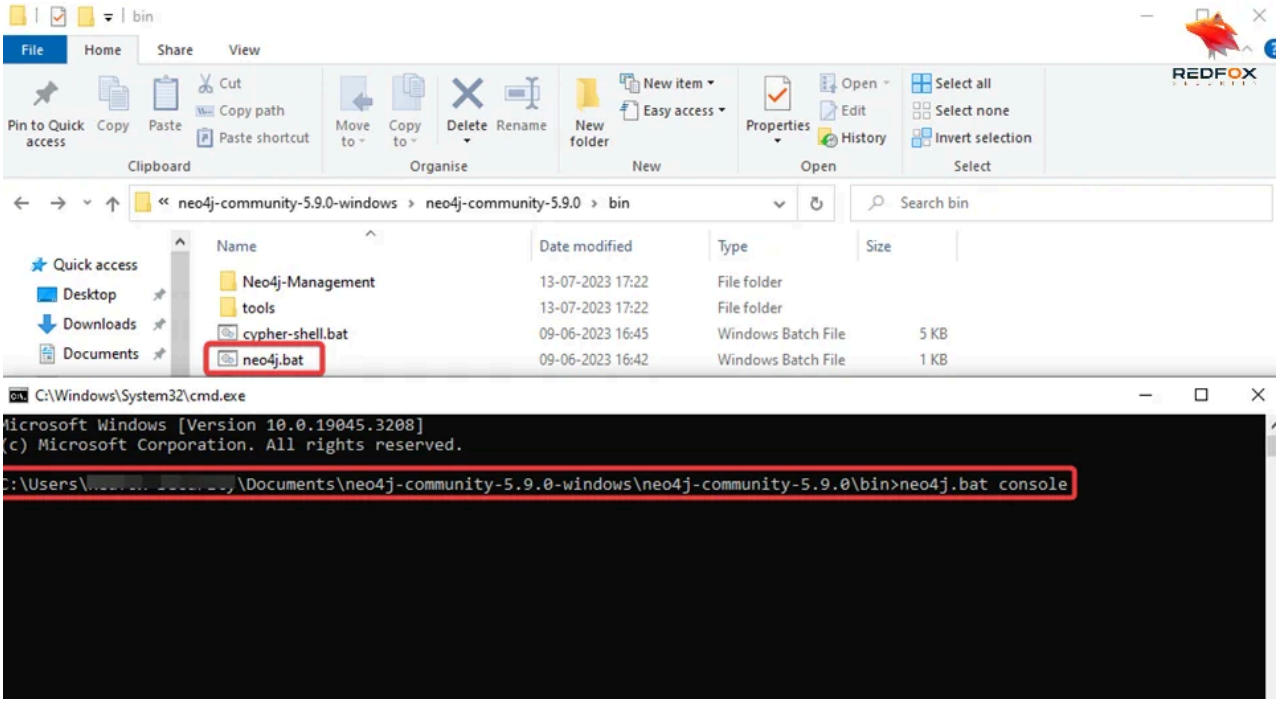
BloodHound Installation and Usage

To use BloodHound, you first need to install it on your system. BloodHound is available for download from the official BloodHound Github repository. Depending on your preference, you can choose to download the C#, ps1, or Python version of the tool.

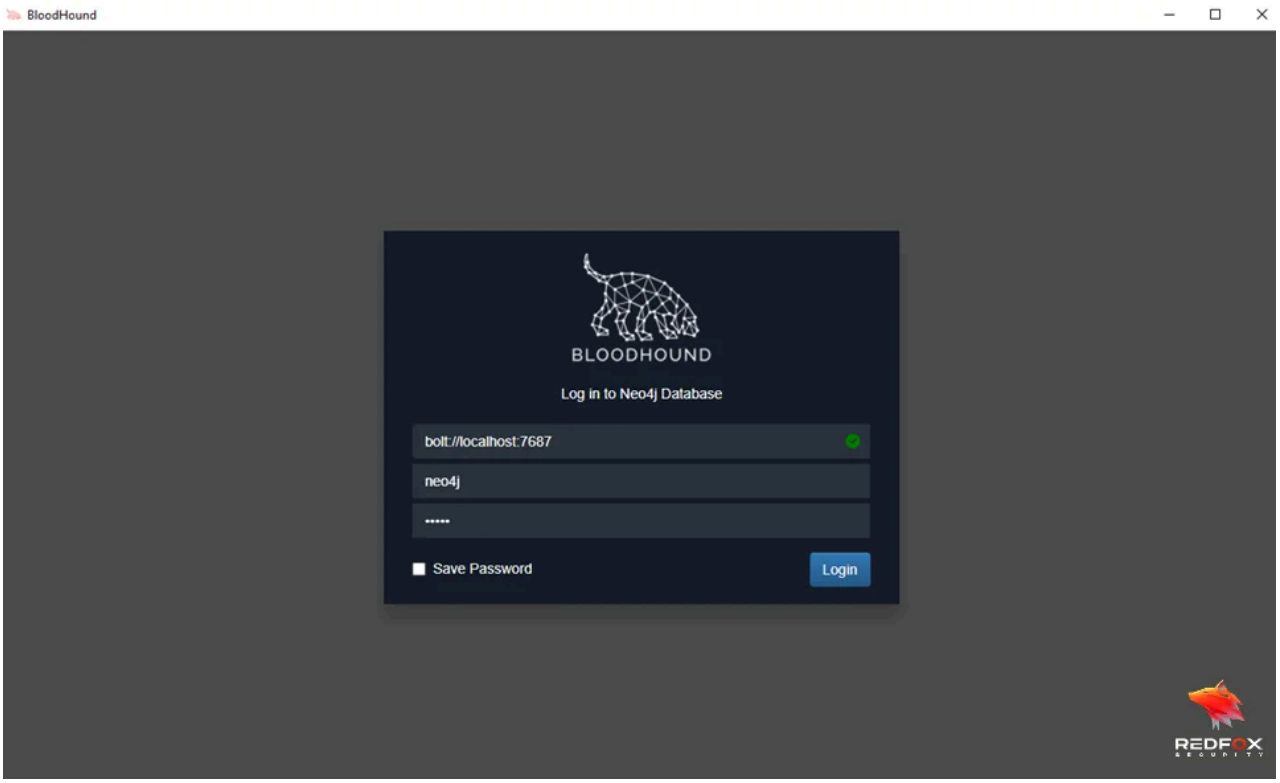


https://github.com/BloodHoundAD/BloodHound/releases

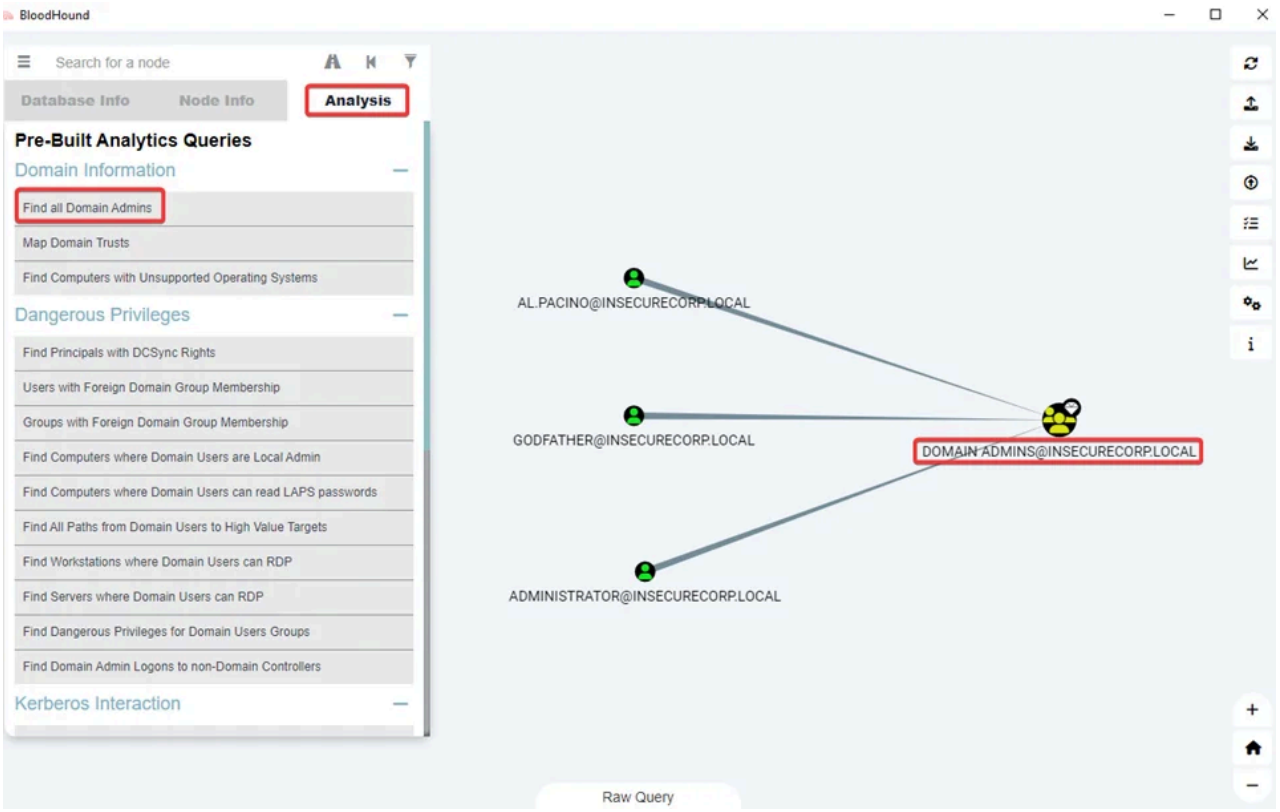
Once you've downloaded BloodHound, you need to start Neo4j, the graph database that BloodHound uses to store data. You can do this by navigating to the BloodHound folder and running the command "Neo4j.bat console". This will start Neo4j in console mode.

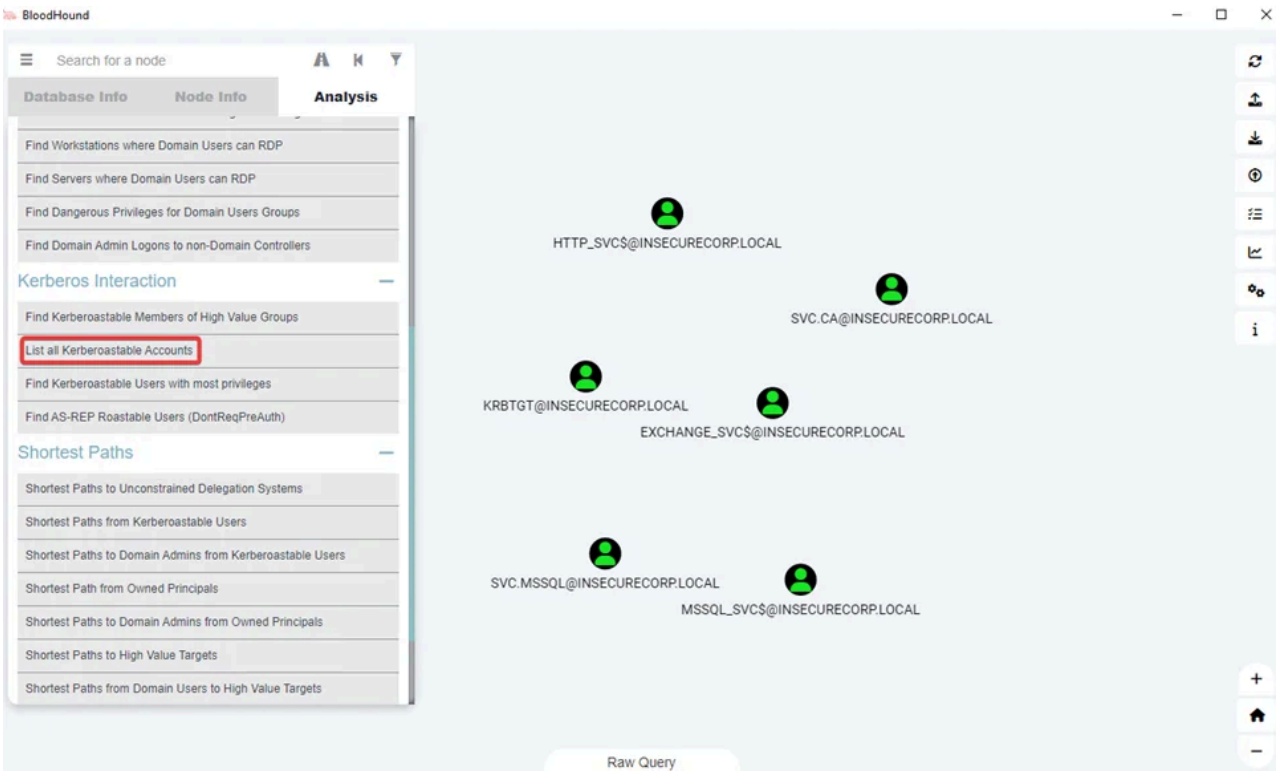


Next, you'll need to run the BloodHound application and connect it to the database. Drag and drop the SharpHound zip file onto the BloodHound interface to do this. This will begin the data import process. Once the data has been imported, you can use the BloodHound interface to visualize the relationships between different entities in your domain.

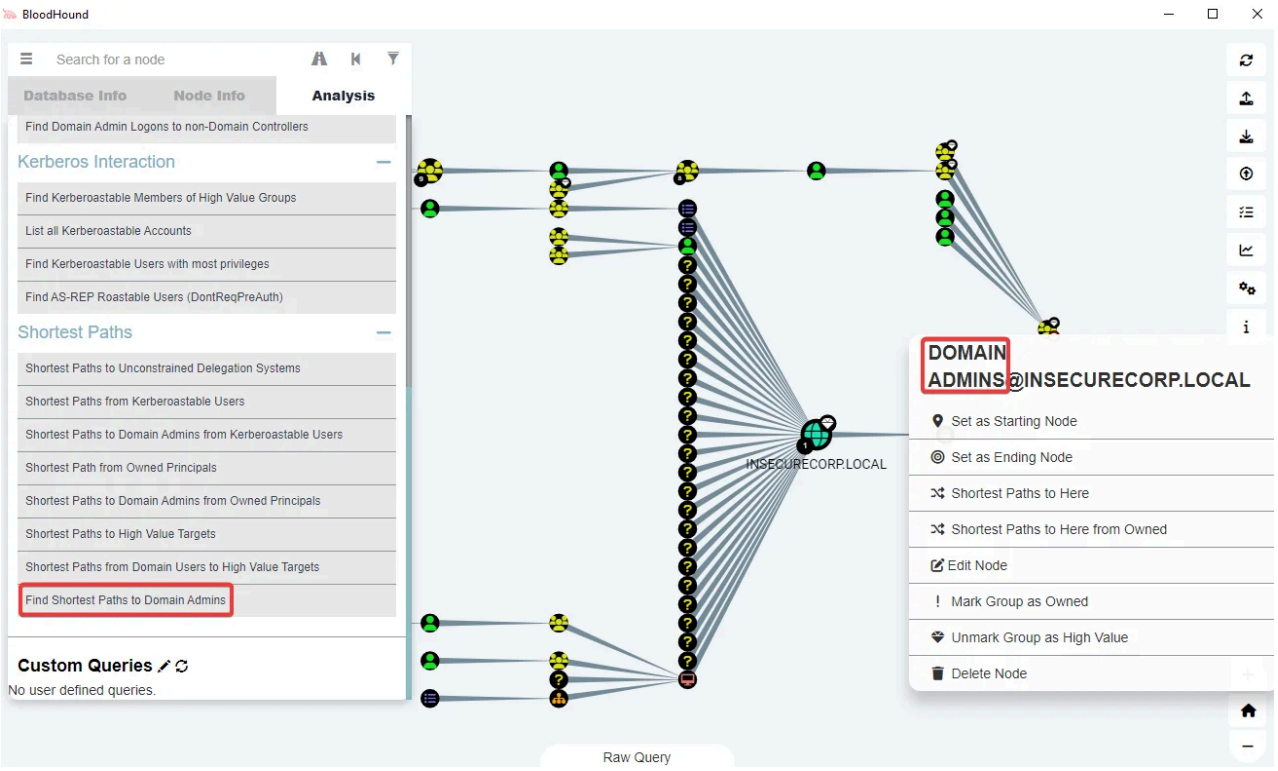


The BloodHound interface has various features that allow you to analyze the data it collects. The "Analysis" section contains pre-built queries that you can use to explore the data. The "Pathfinding" feature allows you to find potential attack paths between entities. You can click on a node to view details about that entity, and the "Unrolled" items will show parent items.

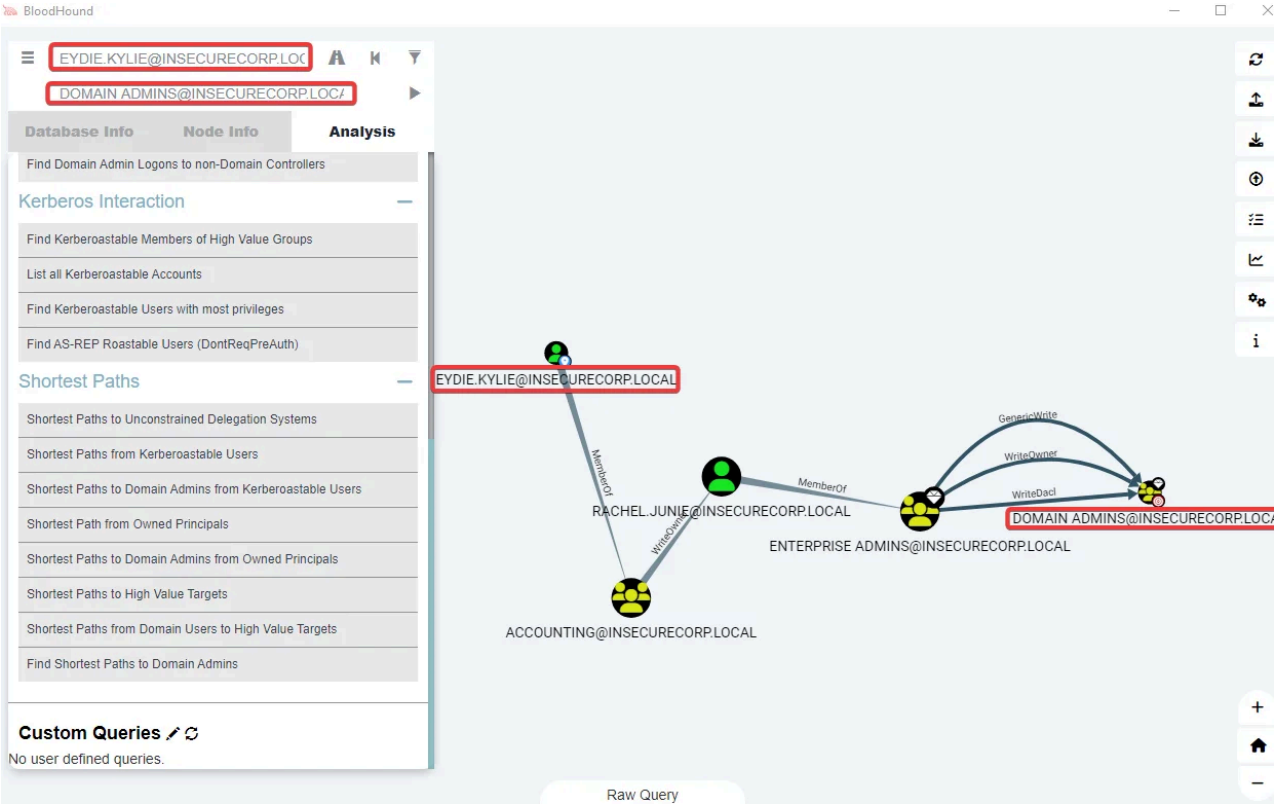




Also, it is really useful in finding all the shortest paths to Domain Admins.



The “Pathfinding” feature allows you to find potential attack paths between entities as shown below.



You can click on a node to view details about that entity, and the “Unrolled” items will show parent items.

TL;DR

BloodHound and SharpHound are powerful tools to help you identify potential security weaknesses in your Active Directory environment. By utilizing the query language Cypher and the visualization capabilities of BloodHound, you can gain valuable insights into the relationships between different entities in your domain. With the knowledge and skills gained from this comprehensive guide, you'll be well on your way to becoming a skilled, innovative, and reliable security expert who values efficiency and creativity, able to cater to various security needs with practical solutions.

Redfox Security is a diverse network of expert security consultants with a global mindset and a collaborative culture. If you are looking to improve your organization's security posture, **contact us** today to discuss your security testing needs. Our team of security professionals can help you **identify vulnerabilities and weaknesses in your systems, and provide recommendations to remediate them.**

"Join us on our journey of growth and development by signing up for our comprehensive **courses**."

PreviousResource-Based Constrained Delegation (RBCD) Attack
NextExploiting MS SQL Servers

Recent Blog

September 09, 2025
Is APK Decompilation Legal? What You Need To Know
September 06, 2025
When Hackers Hit the Road: The Jaguar Land Rover Cyberattack

September 05, 2025
This Is the Hacker’s Swiss Army Knife. Have You Heard About It?