Introducing BloodHound

AUGUST 29, 2016 / 4 COMMENTS

Intro & Background

In February of this year, I posted a proof-of-concept script called "PowerPath" which combined Will Schroeder's PowerView, Justin Warner's concept of derivative local admin, graph theory, and Jim Truher's (@jwtruher) PowerShell implementation of Dijkstra's Algorithm to prove that it is possible to automate Active Directory domain privilege escalation analysis. I had major help from the following people and projects:

- Sam Briesemeister (@systemalias), who introduced me to graph theory and proposed using graphs to automate domain privilege escalation analysis.

- Justin Warner (@sixdub), who helped me understand derivative local admin in a more formal way, and continues to help me mature my red teaming and penetration testing skillset. Justin and Will also initially planted the seed in my brain for this concept of having an "Offensive Dashboard" – a web application to serve as a force multiplier for operators.

- Will Schroeder (@harmj0y), whose PowerView tool has been and continues to be the most comprehensive and advanced offense-focused Active Directory enumeration tool available.

- Lucas Bouillot and Emmanuel Gras, whose Active Directory Control Paths project served as a major inspiration for PowerPath and BloodHound as well.

PowerPath was a really fun proof of concept, and an important stepping stone to something much greater. Our team has long envisioned an "offensive dashboard" that automates much of the tedious work that goes into analyzing Active Directory domain escalation attack paths. We wanted a solution that was operationally focused, easy to use, and had stealthy data collection capabilities.

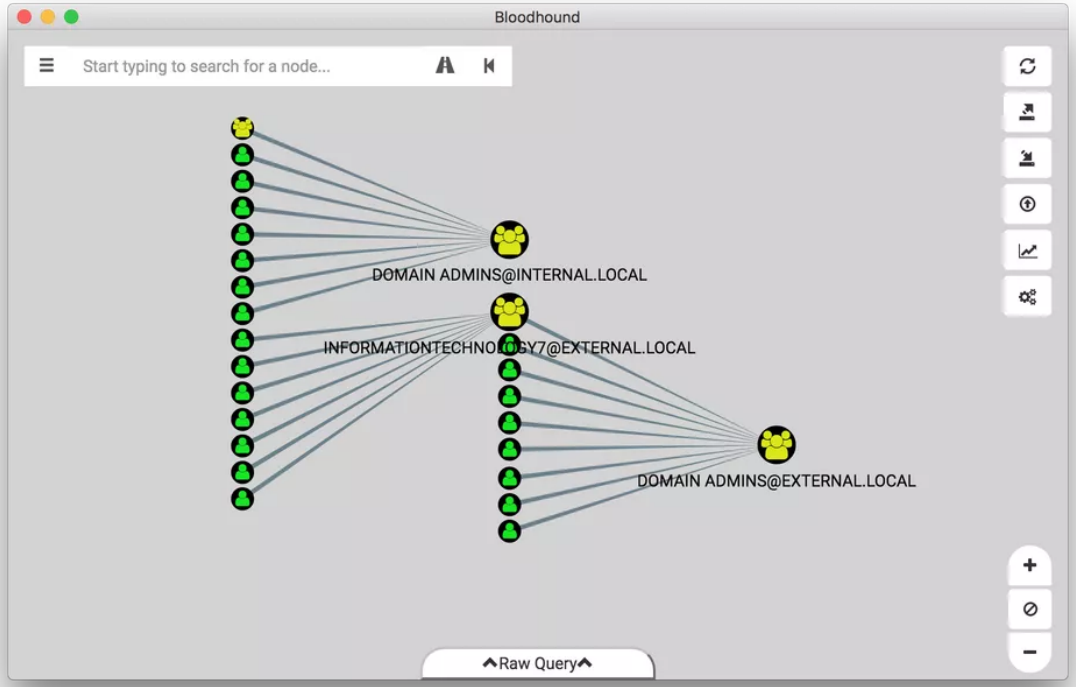
Now, I am extremely proud to introduce BloodHound, which is the end result of months of hard work based on those ideals. BloodHound was released as a free and open source tool at DEF CON 24. BloodHound is co-developed by me, Rohan Vazarkar (@CptJesus) and Will Schroeder (@harmj0y).

What is BloodHound?

BloodHound takes the key concepts behind the original PowerPath proof of concept and puts them into an operational, intuitive, easy-to-use capability for ingesting and analyzing data that can efficiently and precisely show how to escalate rights in an AD domain. BloodHound itself would not have been possible without Rohan and Will:

- Rohan took my rather crude web interface mock-ups and turned them into a real, functional web application. Rohan has also become a cypher expert, developing several general and analytical queries to run with BloodHound. Cypher is the query langauge that drives neo4j interactions.

- BloodHound relies heavily upon Will's tool, PowerView, for data collection. Additionally, Will built upon PowerView and made several custom changes and added several functions to feed the BloodHound database with the information it needs.

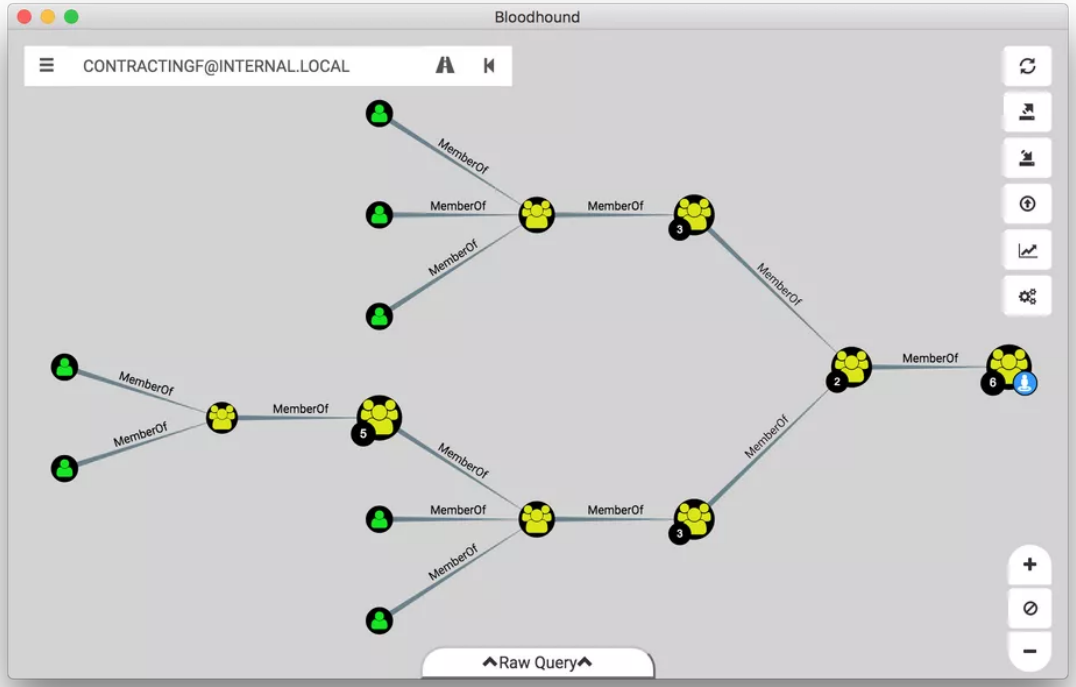


The BloodHound interface, showing effective members of the “Domain Admins” groups in two domains.

Why Should My Team Use BloodHound?

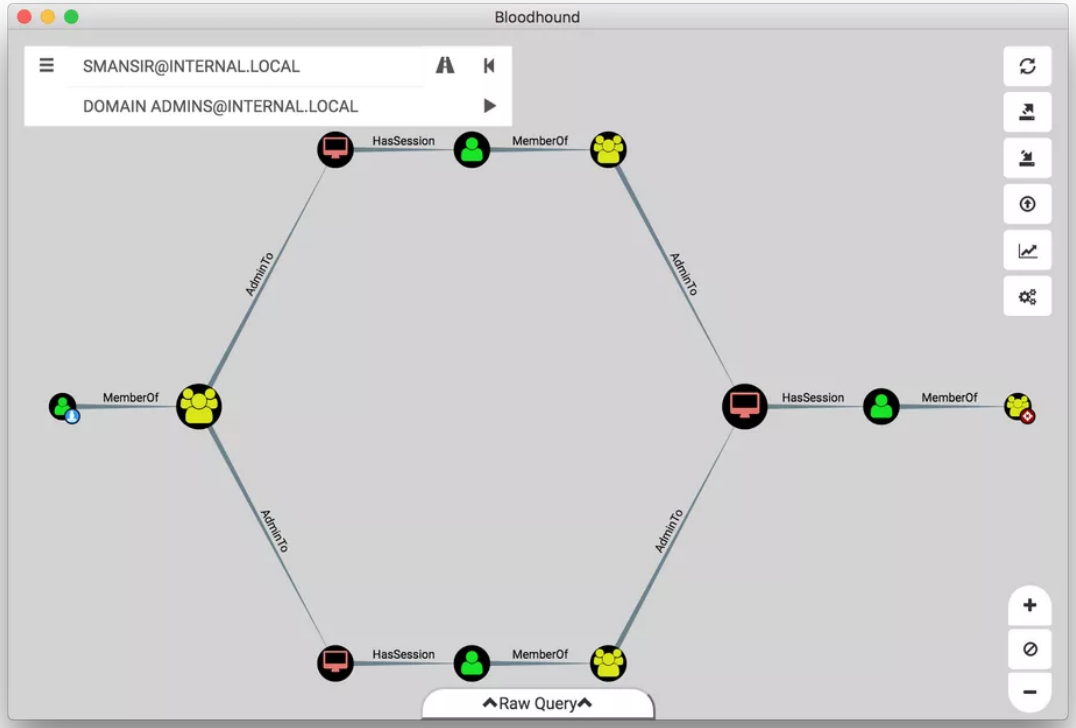
BloodHound a public and freely available tool that uses graph theory to automate much of the rigamarole and tedium behind understanding relationships in an Active Directory environment. Your team can use BloodHound to quickly gain deep insights into AD, knowing precisely which computers any user has admin rights to, which

users effectively have admin rights to any computer, and effective group membership information.



BloodHound showing all the effective (or unrolled) members of a group.

The most exciting feature of BloodHound is its ability to identify attack paths. This concept, which Justin outlines very well in his blog post here, is incredibly powerful and reliable for elevating rights in an AD domain. By automating the analysis required to exploit this concept, BloodHound will serve your team, your client, and your employer well by bringing significant efficiency gains to your engagements.



BloodHound finds the shortest attack path for the user on the left to the Domain Admins group on the right.

How Do I Get Started with BloodHound?

We are using a GitHub wiki for the official documentation for BloodHound. At the wiki you can find the Getting Started page which has everything you need to get up and running quickly.

Where Can I Find More Info?

This blog post will serve as a jumping off point for future reading as resources specific to BloodHound emerge.

Official documentation and content from the creators:

- Get started with BloodHound at the official Github repo: https://github.com/adaptivethreat/Bloodhound.
- Find specific information on installation, data ingestion, CSV formatting, and other useful tips at the BloodHound wiki: https://github.com/adaptivethreat/Bloodhound/wiki
- The BloodHound deck used during DEF CON 24, BSidesLV 2016, and Black Hat Arsenal 2016: http://www.slideshare.net/AndyRobbins3/six-degrees-of-domain-admin-bloodhound-at-def-con-24
- The official BloodHound Gang Slack: https://bloodhoundgang.herokuapp.com/
- The recording of our BSidesLV 2016 talk: https://www.youtube.com/watch?v=lxd2rerVsLo

Other resources:

- Daily Security Byte's video on BloodHound: https://www.youtube.com/watch?v=pKbN9_6zhKo&feature=youtu.be

- Additional in-depth instructions for installing in Linux: https://www.shellandco.net/understand-privilege-relationships-active-directory-environment/

Share this:

Related

Automated Derivative Administrator Search
February 15, 2016
In "Active Directory"

BloodHound 1.3 - The ACL Attack Path Update
May 15, 2017
In "ACL"

A Red Teamer's Guide to GPOs and OUs
April 2, 2018
In "ACL"

Older Post

Next Post

4 thoughts on "Introducing BloodHound"

Active Directory Risk Auditing with BloodHound | the Defense Dude
September 28, 2016

Reply

1. […] highest privileged accounts. For more info about the history of BloodHound check out Andy's Intro to BloodHound. Andy is a friend, and my networks are better off having been put to the test by his great […]

Red + Blue = Purple – Black Hills Information Security
October 26, 2016
Reply

2. […] Bloodhound – https://www.youtube.com/watch?v=MYxk73DsGQI Bloodhound – https://wald0.com/?p=68 Mimikatz – http://www.blackhillsinfosec.com/?p=4667 LAPS – […]

Active Directory Access Control List – Attacks and Defense – Enterprise Mobility and Security Blog
September 18, 2017
Reply

3. […] Introducing BloodHound […]

Test your network by Bloodhound – Explaining Security
February 12, 2018

Reply

4. […] is a tool to analyze and understand Active Directory Trust Relationships. For an offensive practitioner, this tool can highlight the hops you might take to reach a goal […]

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.