

Leveraging graphs to understand our **AD security**

Guillaume Ross

Schedule

9 to 10:15

Setup and Intro to
Graph Security

10:15 to 10:45
Break!

10:45 to 12:00

Let's find what's wrong
in our domains!

Part 1

#psumac2023-graph

We will use this if copy-pasta is needed, support requests etc.

It will be archived at the end of the week.

Why graph?

Guillaume

Myles

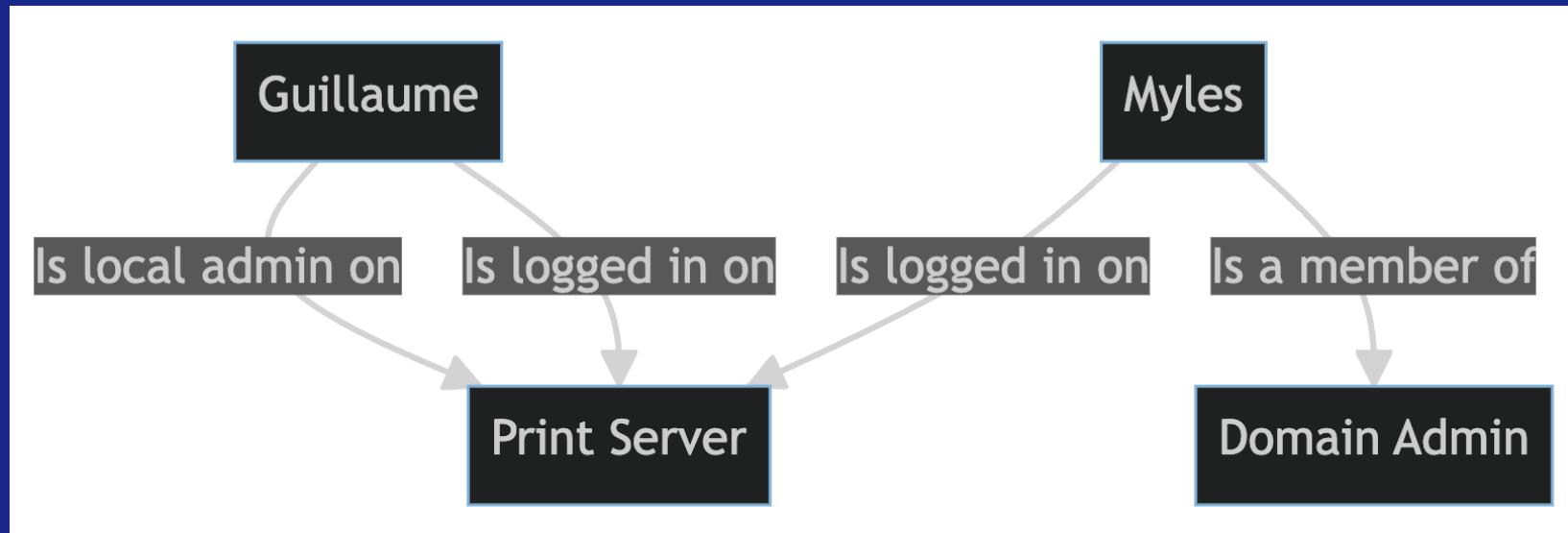
Print Server

Domain Admin

Objects exist in AD, but they're related to each other. A list is useful...

But a graph is way more useful.

Nested groups multiply benefits 10x too!



Typical BloodHound Setup

1. Neo4j Community v4
2. BloodHound
3. SharpHound

This is the graph database "back end" that BloodHound uses.



Installing on Mac

The official instructions will require that some form of Java is installed... so maybe we should just use Docker.

1. Install/Start Docker
2. `docker pull neo4j`
3. `docker run -p 7474:7474 -p 7687:7687 neo4j`
4. Browse to `http://localhost:7474/browser/`
5. Default username/pwd: `neo4j` - I'm changing mine to `psumac23`
6.  up react on my Slack post "Done installing?"

Installing on Windows

You brought a Windows machine to this conference??

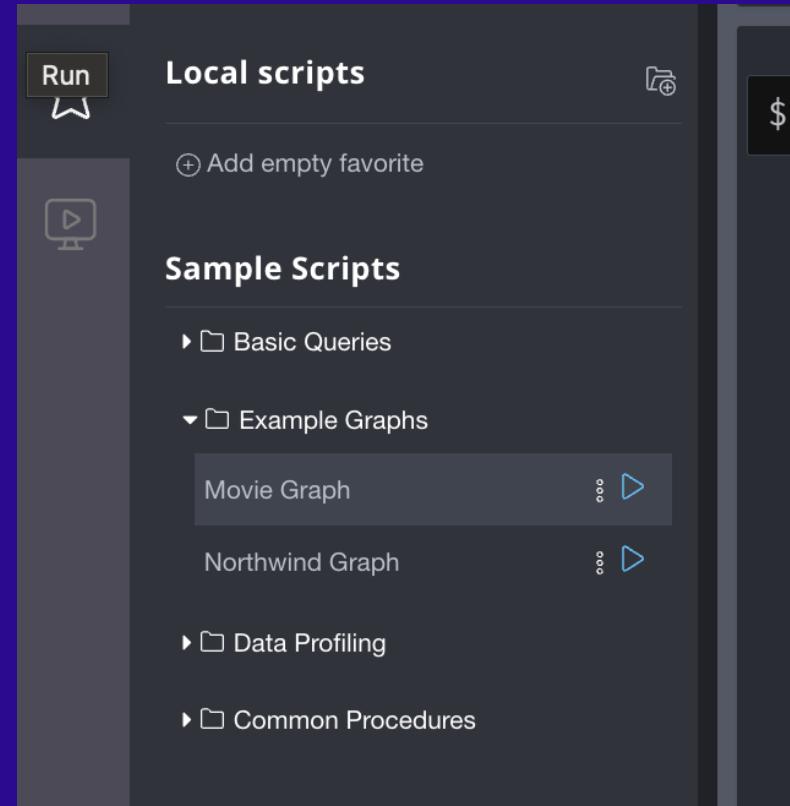
Instructions should actually be the same 😂

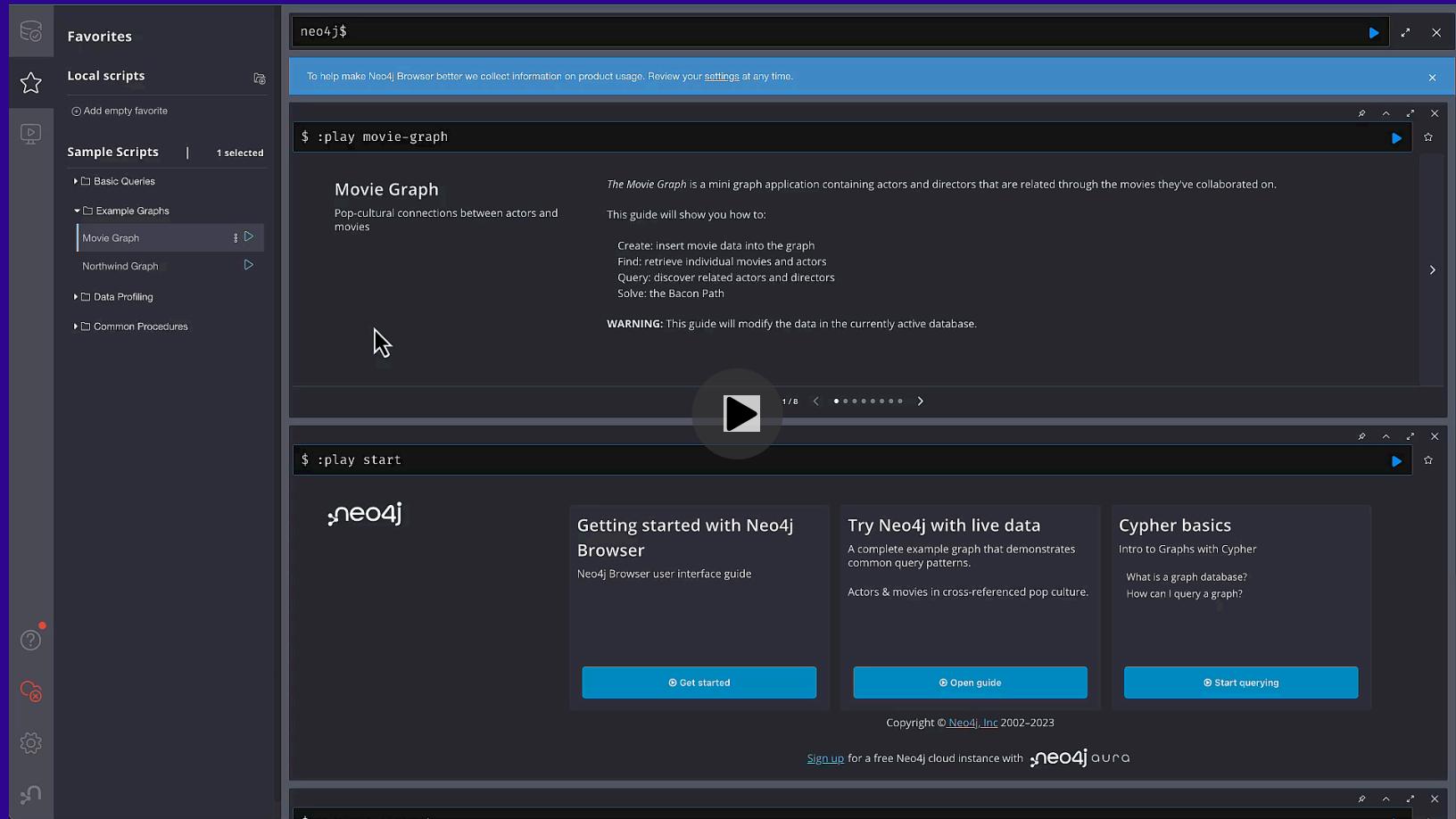
BUT I DID NOT TEST! GOOD LUCK!

1. Install/Start Docker
2. `docker pull neo4j`
3. `docker run -p 7474:7474 -p 7687:7687 neo4j`
4. Browse to `http://localhost:7474/browser/`
5. Default username/pwd: `neo4j` – I'm changing mine to `psumac23`
6.  up react on my Slack post "Done installing?"

Movie Graph

To try neo4j -
let's make it
generate its
"movie"
database.







Your slide does not contain any visual elements. You can display text by adding a tabulator ➔ in front of a paragraph. We discourage using a lot of text that is read from the slide. Use simple headlines, images or videos instead.

You can turn off this message in
Preferences → **Presentation** .

Bacon Path

```
MATCH p=shortestPath ( bacon:Person {name:"Kevin Bacon" } ) - [ * ] - (meg:Person {name:"Meg Ryan" } ) RETURN p
```

**What does the
Bacon Path make
you think of in
Active Directory
terms?**

Someone who can introduce Toms

```
MATCH  (tom:Person {name:'Tom Hanks'}) -  
[ :ACTED_IN] ->(m)<- [ :ACTED_IN] -  
(coActors), (coActors)-[ :ACTED_IN]->  
(m2)<- [ :ACTED_IN] - (cruise:Person  
{name:'Tom Cruise'}) ) RETURN tom, m,  
coActors, m2, cruise
```

**This is why we
need graphs to
understand
AD:
COMPLEXITY!**

1. Download BloodHound from
`https://github.com/BloodHoundAD/BloodHound/releases`
– X64 version is more reliable and works fine in Rosetta. You might need to `wget` as Chrome considers `sharphound` to be malware and will block the zip. (Warning: Your EDR/AV might also trigger)
2. Unzip it (This is when a lot of EDRs will trigger. If only `sharphound` gets deleted, no worries, you won't need it today).
3. Right click to run it and bypass GateKeeper
4. Log in with previously configured credentials
5. Don't forget to  message asking if you installed BloodHound properly. Or other reaction if you're having issues.

30M Break

Part 2

SharpHound: Warnings

SharpHound can be noisy and generate quite a bit of load. If you run it "by default", you will likely trigger at least some EDRs, IPS, etc. Don't go and run this against domains you don't own, please, and if you do, read the full instructions!

Using SharpHound

We won't in this lab but you will need it in real life.

```
sharphound -d  
psumac.local
```

Collect sessions?

```
sharphound --  
CollectionMethods Session
```

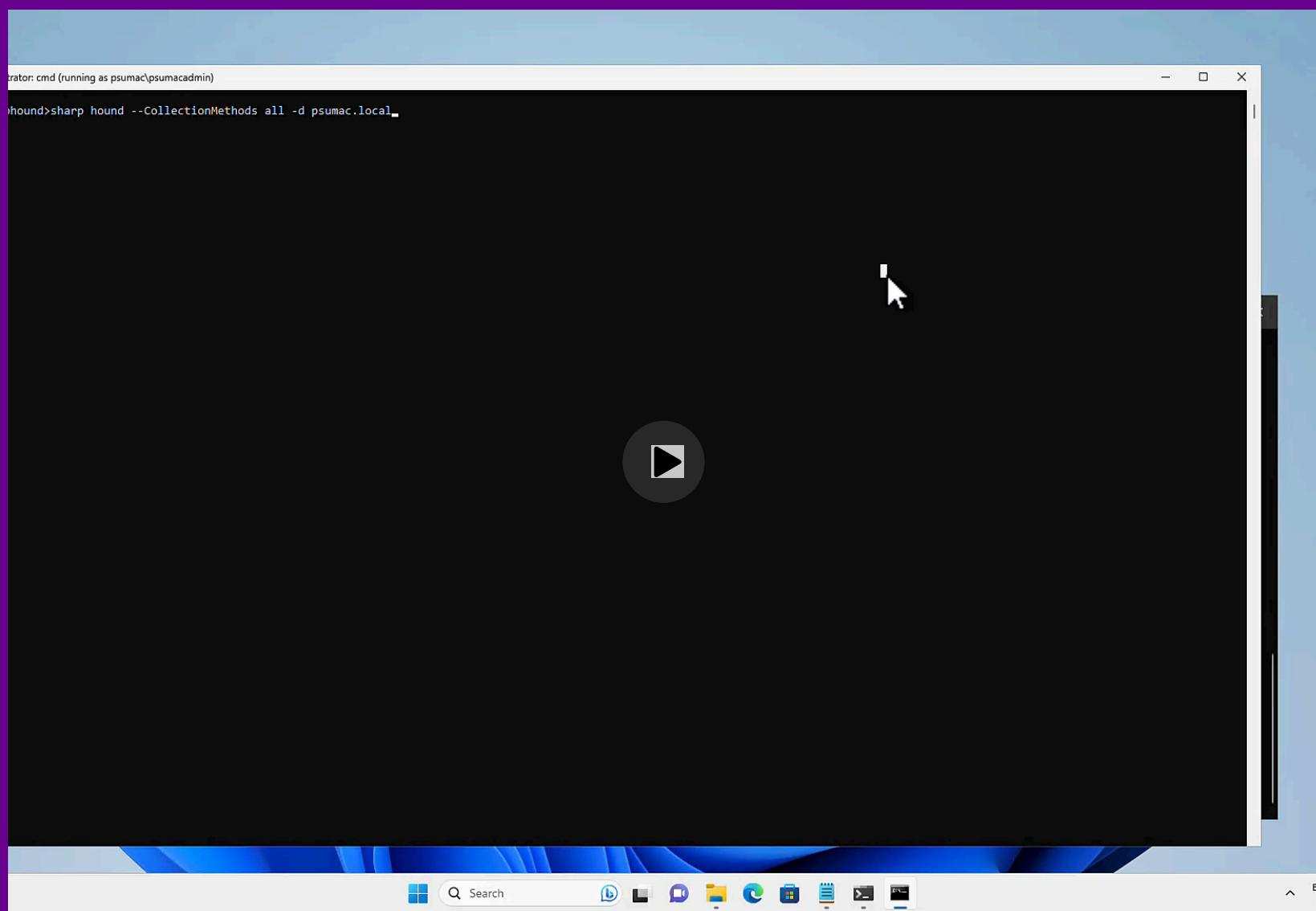
Stealth?
sharphound --
CollectionMethods Session
--Stealth

ALL! (NOISY!)
sharphound
--CollectionMethods all

Other Options

1. Target only specific DCs (useful to not load important DCs)
2. Various throttling options (useful to prevent detection but also to reduce performance impact on huge domains)
3. EncryptZip (useful so if someone finds your zip laying around, they can't open it easily).
4. Much more!

Importing demo data



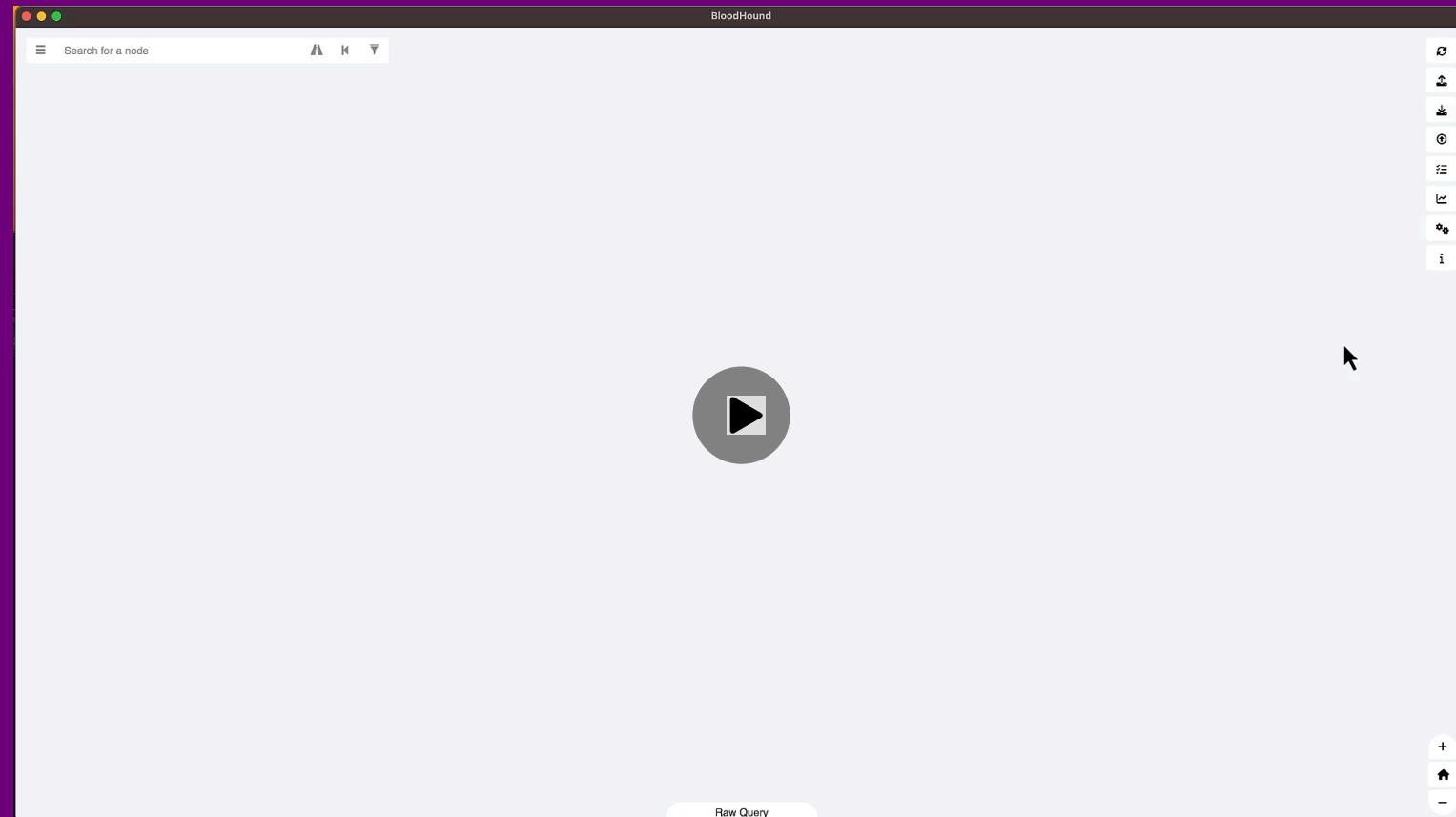
<https://evil.plumbing>

First link top left.. or QR code
on next slide



Why did I make a QR code for this?

Importing

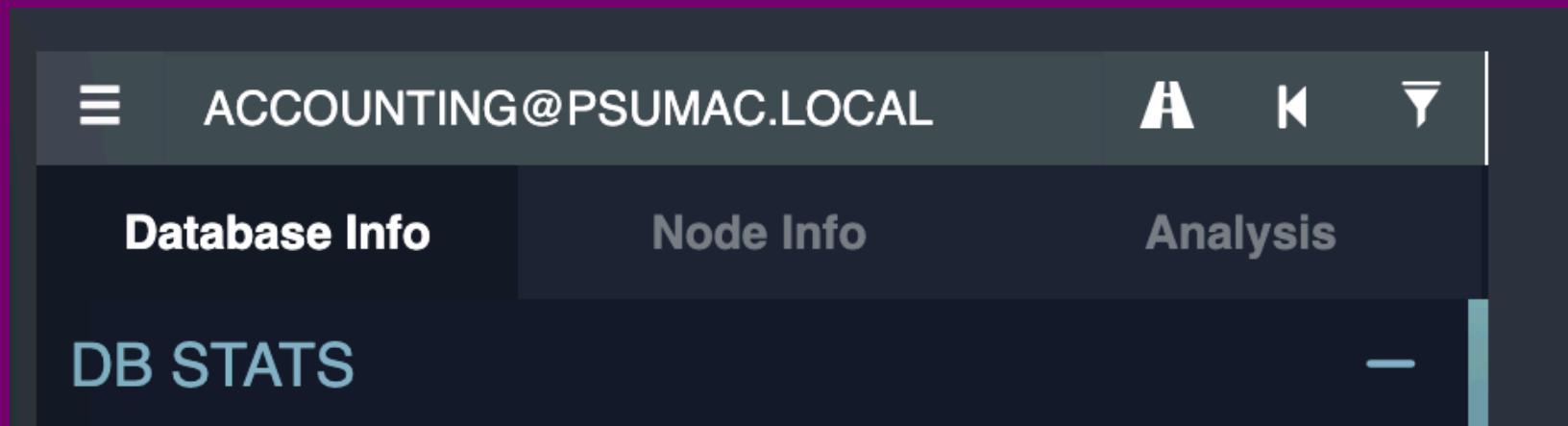


Navigating BloodHound

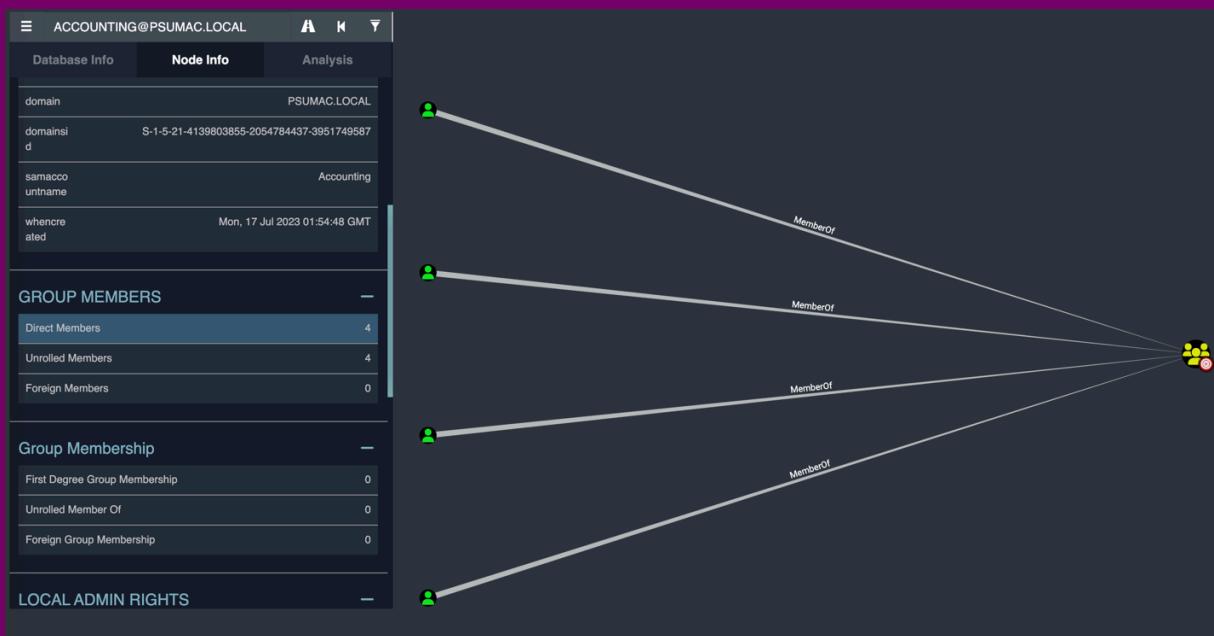
Draw domain trusts



Searching for something



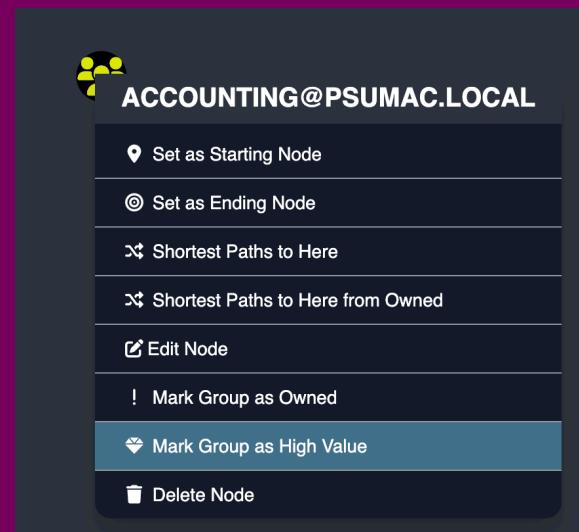
Viewing details



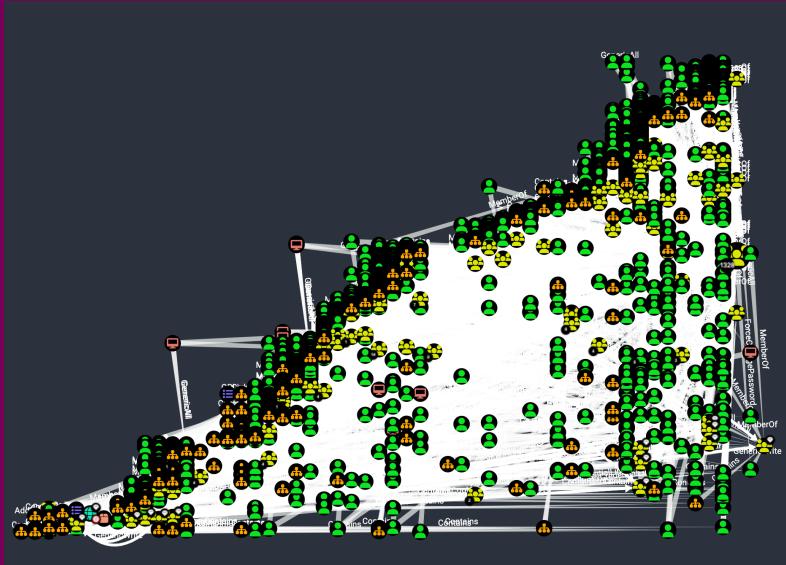
Digging into a user

Let's set some targets!

accounting@
hr@
engineering@
legal@



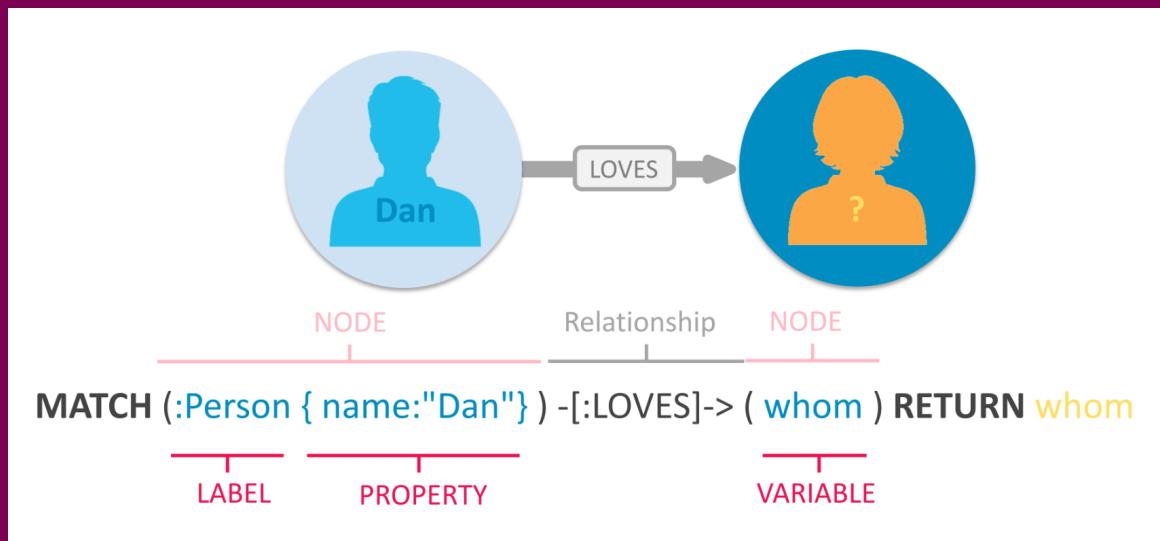
Path to high value targets



Too many
options.. we'll
come back later.

Cipher/Custom queries

```
MATCH p=(m:Group)-[r:AdminTo]->(n:Computer)  
RETURN p
```



Find users created in last 30 days

```
MATCH (u:User) where  
u.enabled=TRUE and u.whencreated  
> (datetime().epochseconds - (30  
* 86400)) RETURN u
```

ord|GenericAll|GenericWrite|Owns|WriteDacl|WriteOwner|CanRDP|ExecuteDCOM|AllowedToDelegate|ReadLAPSPassword|Contains|GpLink|AddAllowedTo|

Kerberoasting

Kerberoasting is a post-exploitation attack technique that attempts to obtain a password hash of an Active Directory account that has a Service Principal Name ("SPN"). In such an attack, an authenticated domain user requests a Kerberos ticket for an SPN.

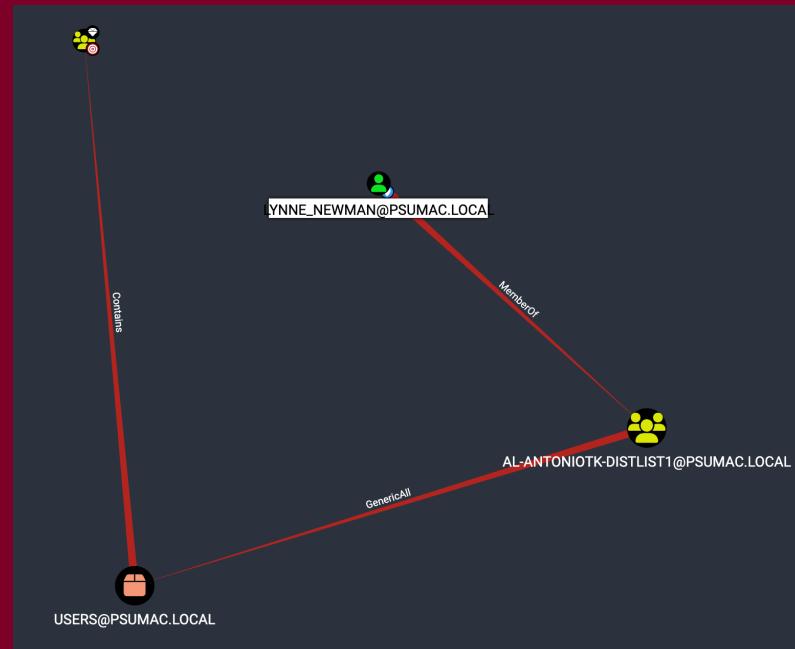
TL;DR -> You get a SPN – encrypted with the password of the service account, allowing you to brute-force the password. Service accounts with weak passwords are especially at risk.

**Which
Kerberoastable
account is the
most interesting?**

5m

My answer

Other answers can
be good too, so
much of the domain
is MESSY and
RANDOMLY GENERATED:
Lynne Newman ... or
PRINT_AUTOMATOR.



**Can you
explain why?**

**Why might
they actually
not be
interesting at
all?**

**Who would be
users that are
similarly
interesting?**

**Why do you
want to have
multiple targets
for
Kerberoasting?**

**Assume we
owned
Lynne_Newman**

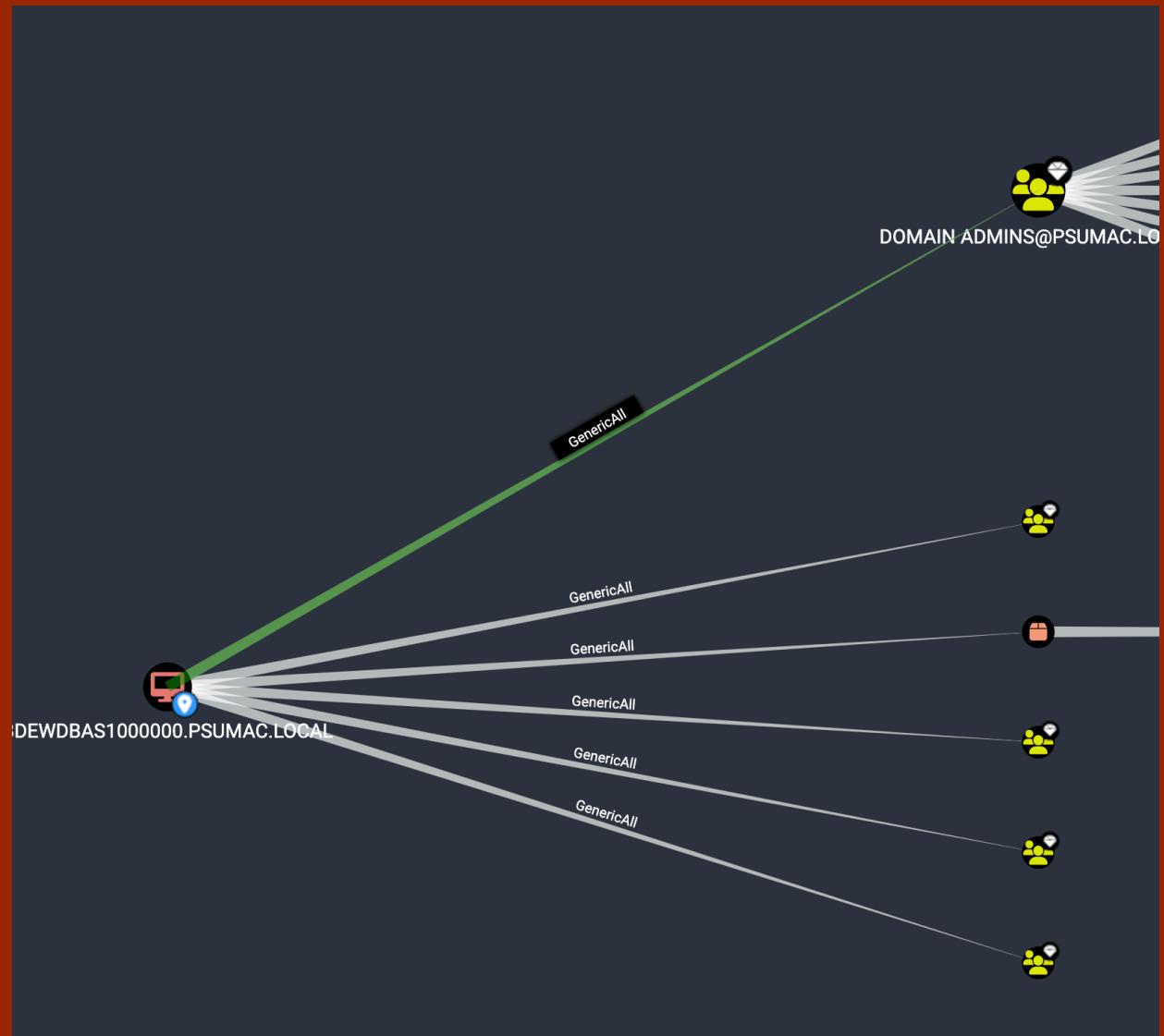
Let's mark her as owned

Lynne_Newman to high value targets

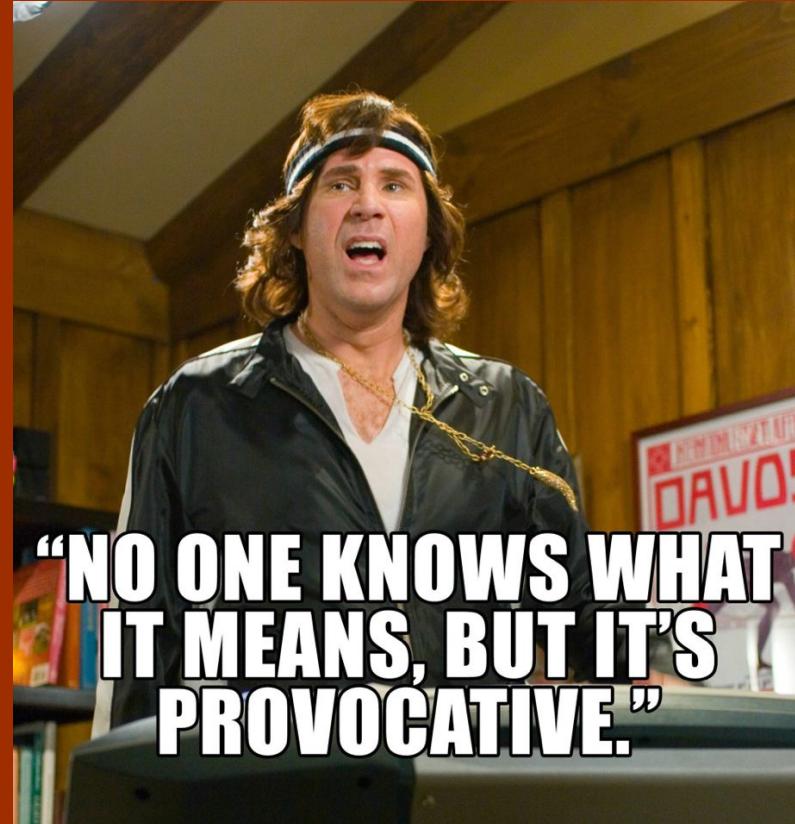
List her reachable high value targets
Is there something that could be
filtered out?

Can you tell me about two paths to
domain admin she has?

**Why is this
system
interesting?
BDEWDBAS100000**



What does GenericAll even MEAN?



Mark it as high value

BDEWDBAS1000000

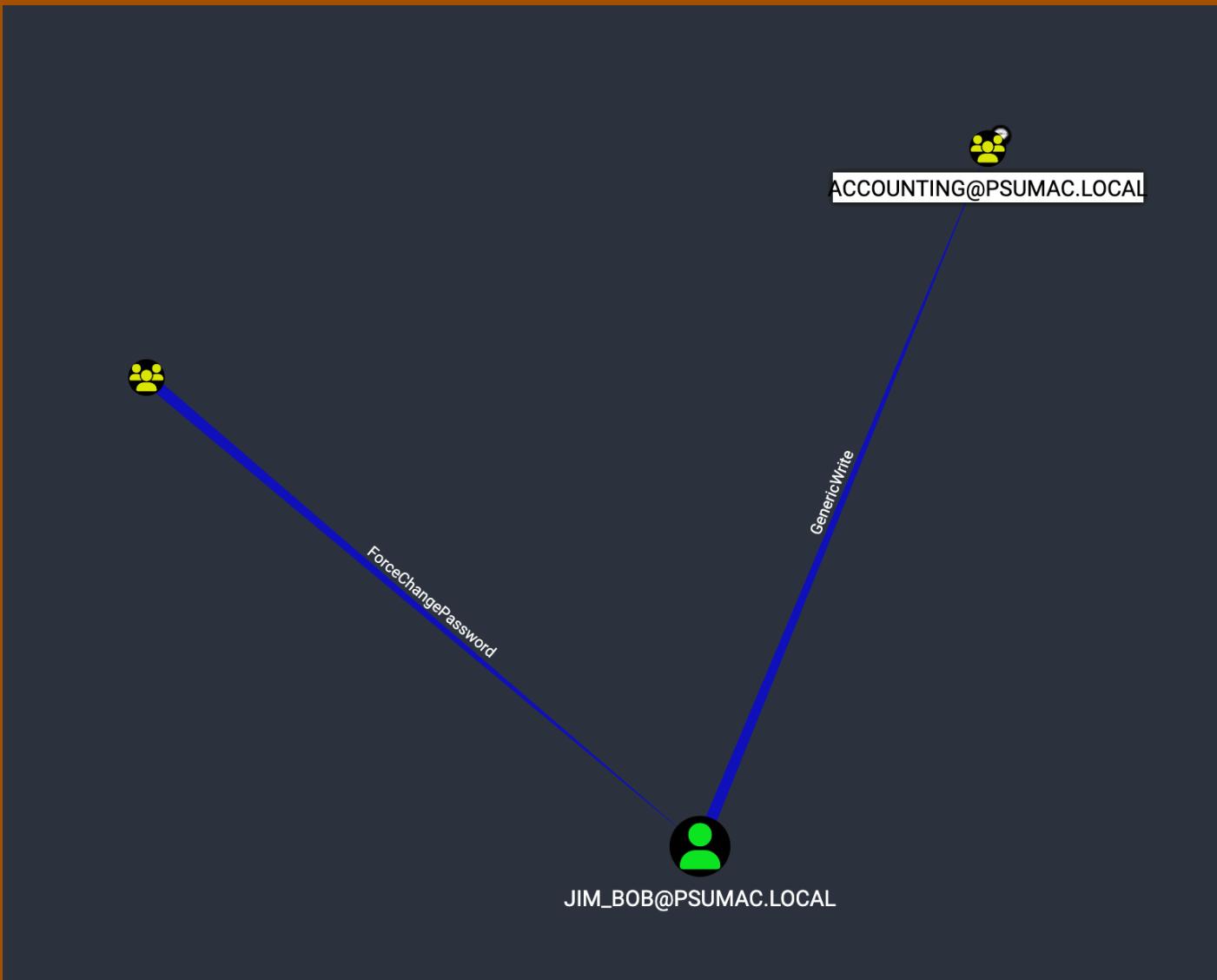
**Let's add
some other
owned
accounts**

**What are some
fun paths we
now have from
owned assets?**

**I don't have a
single solution,
let's just talk
about fun
paths!**

Domain users to high value targets

Sometimes domain users have surprising permissions. At least one is at play... where?



This means anyone can own JIM_BOB and then add users to accounting. Let's mark JIM_BOB as owned!

BloodHound and AD Security Links

1. <https://github.com/ZphrFish/Bloodhound-CustomQueries>
2. AdSecurity.org

Remember

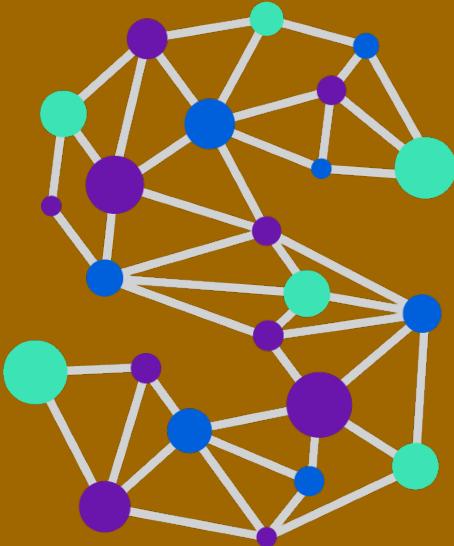
BloodHound also works for
Azure thingies!

Addicted to graphs yet?

<https://github.com/JupiterOne/starbase>

TONS of integrations! AD, MDMs, EDRs, GitHub, much more!

DEF CON workshop in a few weeks!



STARBASE

Thank you all!

Thanks for your time this early into the conference week!

Stay tuned for **Manage macOS Risk with Adv. Auditing Capabilities**

FEEDBACK

<https://bit.ly/psumac2023-104A>

