Setup BloodHound tool on Windows and enumerate Active Directory Objects

gaya3-r.medium.com/setup-bloodhound-tool-on-windows-and-enumerate-active-directory-objects-117a8d6c9f4c

gayatri r February 17, 2021

gayatri r

BloodHound is an application used to visualize active directory environments. The front-end is built on electron and the back-end is a Neo4j database, the data leveraged is pulled from a series of data collectors also referred to as ingestors which come in PowerShell and C# flavours.

> It identifies different attack paths in Active Directory , maps access control lists (ACLs), users, groups, trust relationships and unique AD objects.

Setup

•BloodHound is supported by Linux, Windows, and MacOS. Bloodhound is built on neo4j and depends on it. Neo4j is a graph database management system, which uses NoSQL as a graph database.

•Download the Windows binary from Bloodhound GitHub Page

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

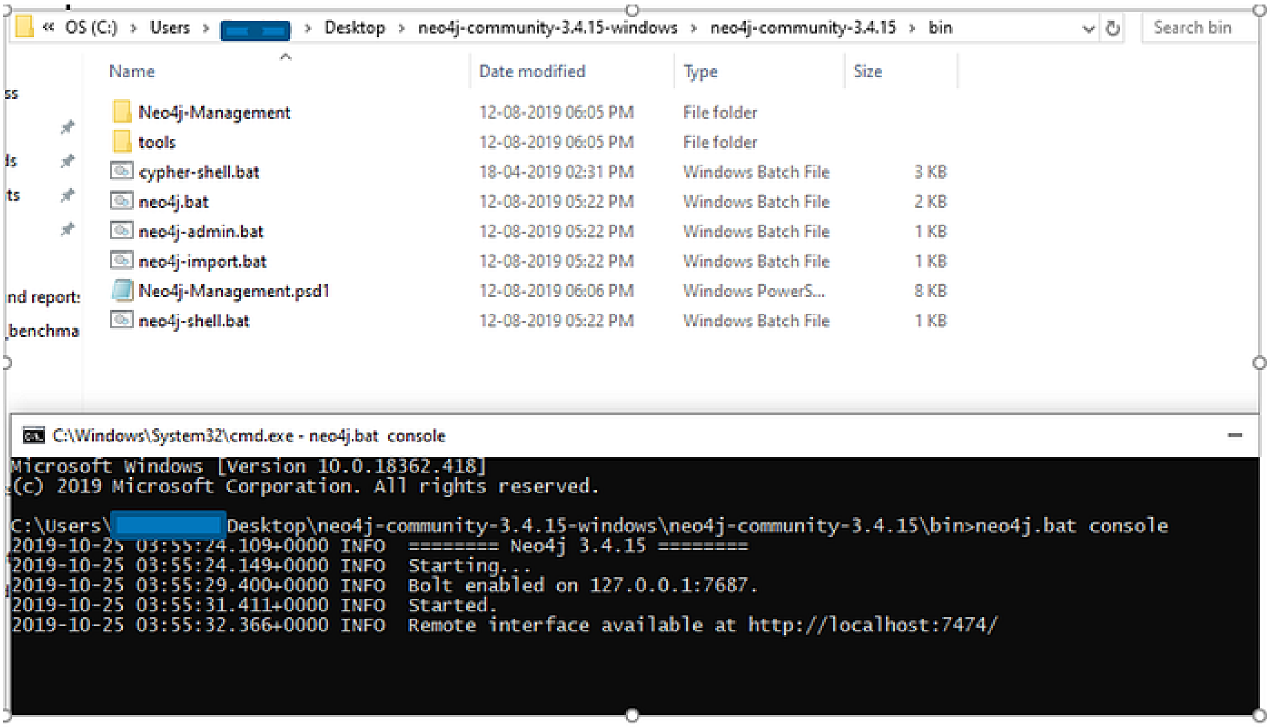
•Download Neo4J community Server

Thanks for Downloading Neo4j - Neo4j Graph Database Platform

The installer includes the Java version needed for running Neo4j. Open the dmg file you just downloaded. Drag the…

neo4j.com

> Open Neo4j Folder and run the Neo4j database for the use of Bloodhound



« OS (C:) › Users › [redacted] › Desktop › neo4j-community-3.4.15-windows › neo4j-community-3.4.15 › bin

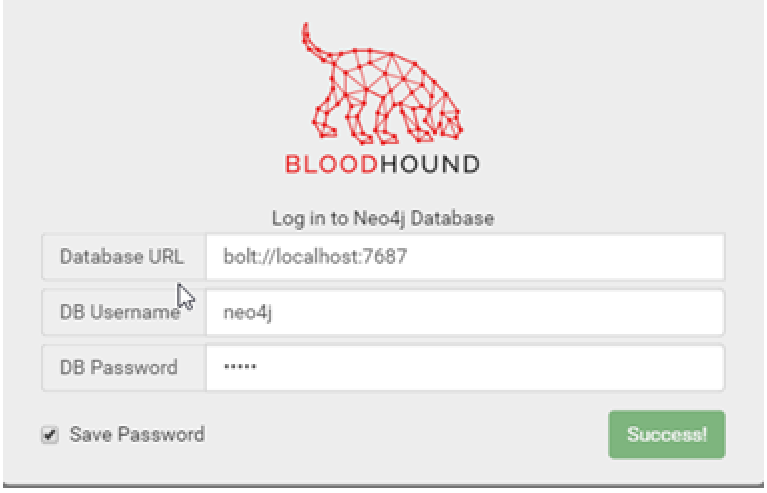
Name	Date modified	Type	Size
Neo4j-Management	12-08-2019 06:05 PM	File folder	
tools	12-08-2019 06:05 PM	File folder	
cypher-shell.bat	18-04-2019 02:31 PM	Windows Batch File	3 KB
neo4j.bat	12-08-2019 05:22 PM	Windows Batch File	2 KB
neo4j-admin.bat	12-08-2019 05:22 PM	Windows Batch File	1 KB
neo4j-import.bat	12-08-2019 05:22 PM	Windows Batch File	1 KB
Neo4j-Management.psd1	12-08-2019 06:06 PM	Windows PowerS...	8 KB
neo4j-shell.bat	12-08-2019 05:22 PM	Windows Batch File	1 KB

C:\Windows\System32\cmd.exe - neo4j.bat console

```
Microsoft Windows [Version 10.0.18362.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\[redacted]Desktop\neo4j-community-3.4.15-windows\neo4j-community-3.4.15\bin>neo4j.bat console
2019-10-25 03:55:24.109+0000 INFO  ======== Neo4j 3.4.15 ========
2019-10-25 03:55:24.149+0000 INFO  Starting...
2019-10-25 03:55:29.400+0000 INFO  Bolt enabled on 127.0.0.1:7687.
2019-10-25 03:55:31.411+0000 INFO  Started.
2019-10-25 03:55:32.366+0000 INFO  Remote interface available at http://localhost:7474/
```

- Run the bloodhound and connect to the neo4j database by giving username neo4j and password as neo4j



BLOODHOUND

Log in to Neo4j Database

Database URL: bolt://localhost:7687

DB Username: neo4j

DB Password: •••••

☑ Save Password

Usage

•Inorder to collect the data of Active Directory, should use Ingestiors like Sharphound and Powershell Script that is given in Bloodhound

https://github.com/BloodHoundAD/BloodHound/tree/master/Ingestors

•if you are running on non-AD member first you need to run it as AD member by issuing command

runas /netonly /user:ad.redacted.com\<username> “cmd.exe -nop -executionPolicy bypass”

•Connect to Pulsesecure(VPN) where you connect to your Active Directory to enumerate AD objects

SharpHound.exe Invoke-BloodHound — CollectionMethod All

•The default if this parameter is not supplied is Default:

Default — This performs a collection of the local admins on machines, group memberships, domain trusts, and sessions.

Group — Collects the group memberships only

LocalGroup — Collects just the local admins

GPOLocalGroup — Performs local admin collection using Group Policy Objects

ComputerOnly — Performs local admin collection and session collection

Session — Collects the user sessions on machines on the domain

LoggedOn — Performs privileged session collection (this requires local admin rights on target systems

Usage

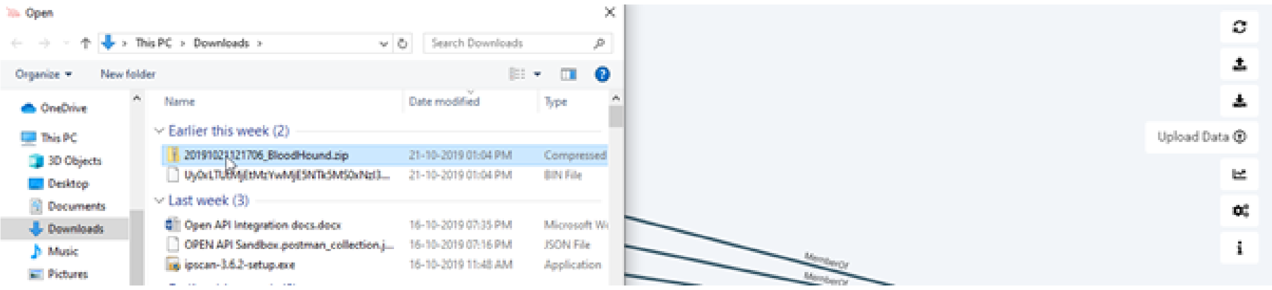
Trusts — Enumerates the domain trusts for the specified target domain

ACL — Collects the access control lists from the domain

Container — Performs collection of Containers

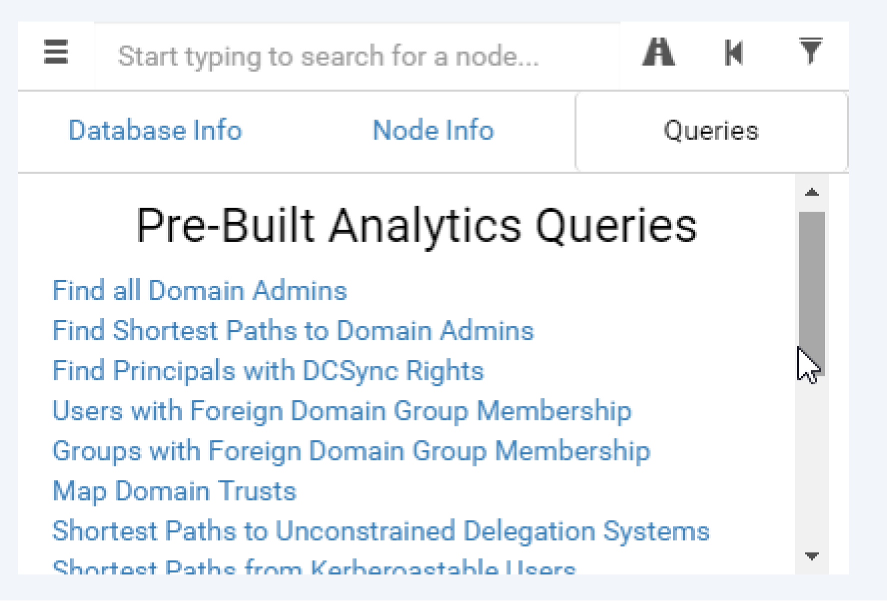
All — Performs all Collection Methods listed above.

Once the command successfully executed it gives you a zip folder , Import the zip in the Bloodhound



Name	Date modified	Type
Earlier this week (2)		
20191021121706_BloodHound.zip	21-10-2019 01:04 PM	Compressed
UyOxLTUtMjEtMzYwMjE5NTk5MS0xNzI3...	21-10-2019 01:04 PM	BIN File
Last week (3)		
Open API Integration docs.docx	16-10-2019 07:35 PM	Microsoft W
OPEN API Sandbox.postman_collection.j...	16-10-2019 07:16 PM	JSON File
ipscan-3.6.2-setup.exe	16-10-2019 11:48 AM	Application

Bloodhound has some default Queries which gives you understanding objects of Domain



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

Custom Queries Usage

•Custome Queries can also use to query the database

https://hausec.com/2019/09/09/bloodhound-cypher-cheatsheet/

> The command is intended for the graph/GUI or console. For the console, it means they cannot be executed via Bloodhound GUI and must be done via the neo4j console.

References

•https://www.pentestpartners.com/security-blog/bloodhound-walkthrough-a-tool-for-many-tradecrafts/

•https://ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-with-bloodhound-on-kali-linux

•https://github.com/chryzsh/awesome-bloodhound