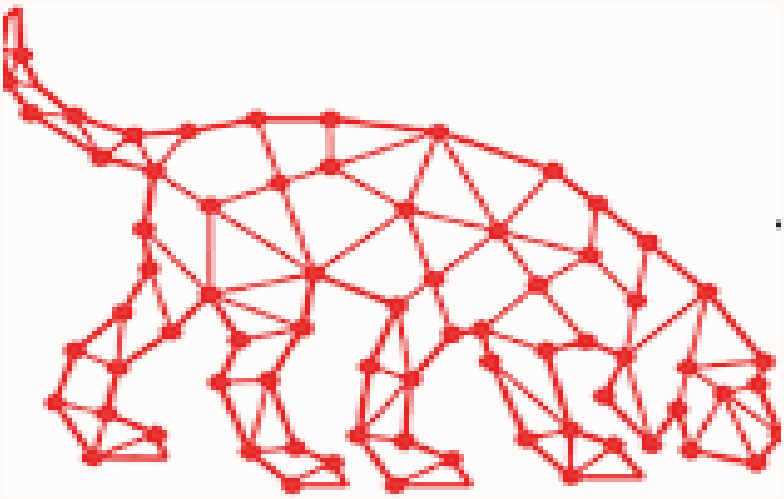
Cyber Public School

BloodHound

Link

Bloodhound



The hidden and generally unforeseen relationships in an Active Directory or Azure system are uncovered by BloodHound using graph theory. Attackers can use BloodHound to rapidly and efficiently locate intricate attacking trajectories that would otherwise be unfeasible. It can be used by defenders to locate and stop the same attack routes. BloodHound makes it simple for both blue and red teams to understand more about the interconnections of privilege in an Active Directory or Azure environment. It is a tool for visualising Active Directory environments, the data used is obtained from several data collectors, also known as ingestors, that are available in PowerShell and C# flavours. The front end is built on electron and the back end is a Neo4j database.

SharpHound

Written in C#, Sharphound plays the role of data collector for BloodHound. It gathers information from domain controllers and domain-joined Windows systems using native Windows API functions and LDAP namespace functions.

Link

Installation: *apt-get install bloodhound*

Use the following command to launch Neo4j after installation is finished. *sudo neo4j console*

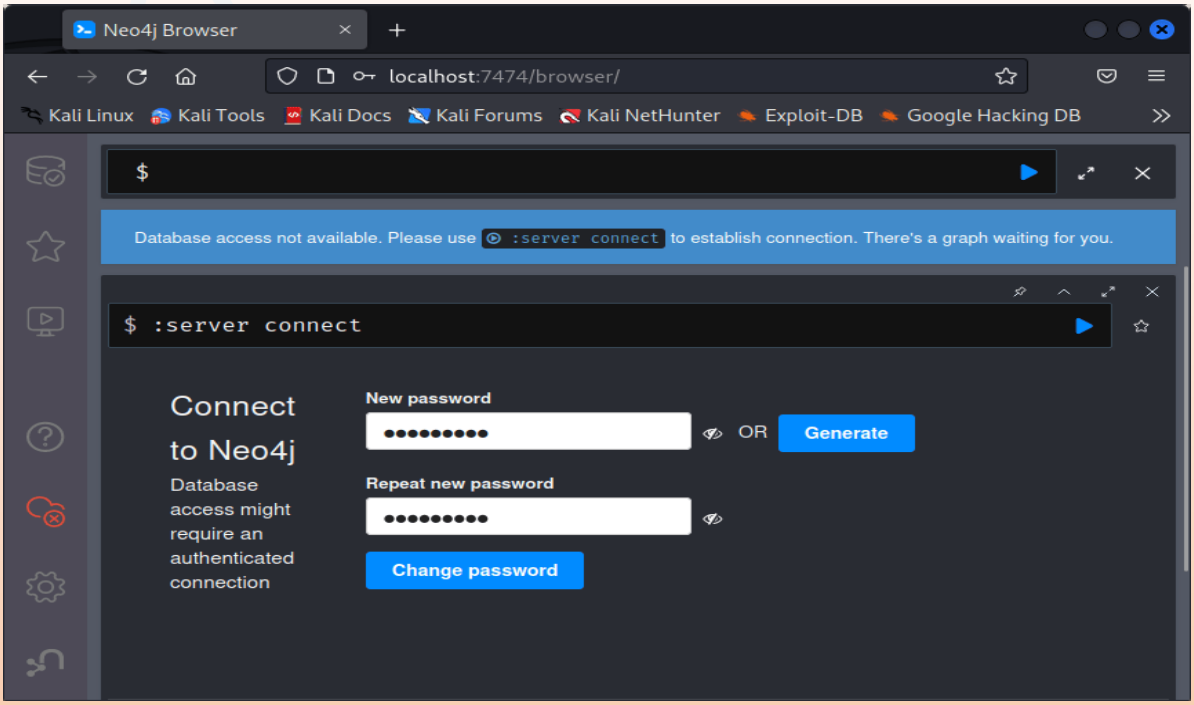
Default

Credentials

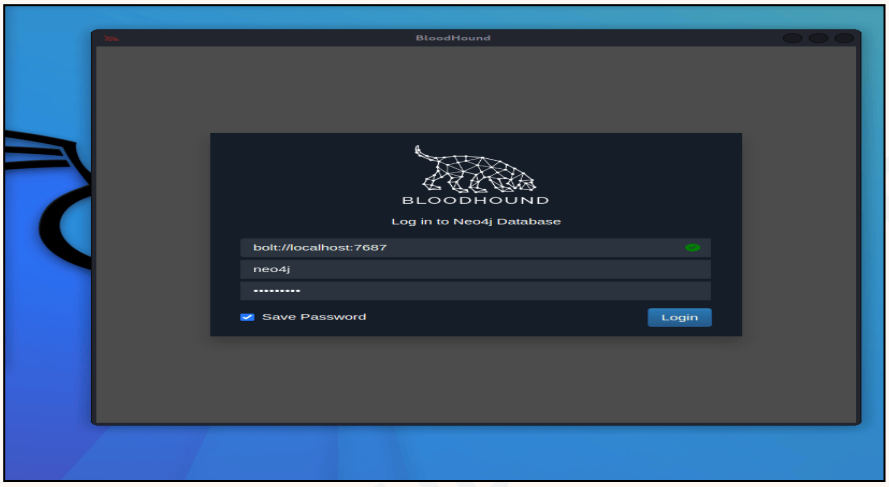
username: neo4j

password: neo4j

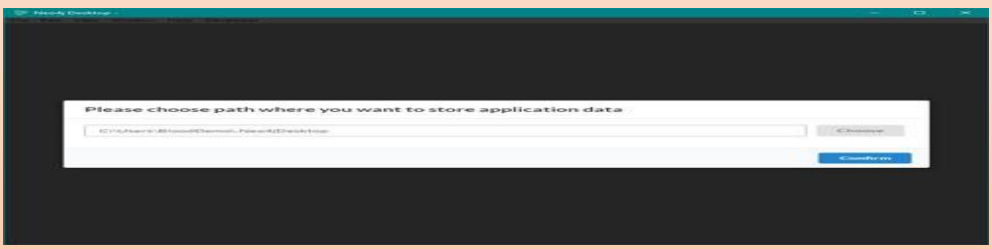
After signing in, one will be prompted to reset the default password with a new one. To subsequently log in to the Bloodhound interface, one needs this password.



After successfully changing the password, one can now run Bloodhound usingthe updated login information.



Installing the tool and downloading the Neo4j database is the preliminary stage in initiating a BloodHound analysis. After downloading the newest BloodHound version, turn the downloaded file into a folder. Get your ingestor at this point. Install "SharpHound.exe" by visiting the ingestor folder in the BloodHound GitHub page and for this one also turns the downloaded files into a folder. Eventually, a database is all you require. You can select to install Neo4j desktop for multiple users or only for you. It will appear as an app data folder when you download it. The Neo4j desktop GUI ought to function at this point. Choose the location for data storage, then click the confirm button.



Follow the steps below to complete the procedure:

- Choose **projects** from the menu, then give the default project the title
  BloodHound.

- Choose **add a graph** after clicking **create a local graph**.

- Put **BloodHound** in the graph's name, then create a password.Your installation is now finished!

Data Collection

It's time to use the SharpHound.exe file that we downloaded to a folder to gather the data that BloodHound requires. Although we will be using SharpHound.exe, if you'd prefer to utilise the PowerShell version, feel free to read up on it on the **BloodHound wiki.**

Launch PowerShell as an ordinary user. Make a directory for the information that SharpHound generates and designate it as the current directory.

```
mkdir “name of the directory”:-Force | cd
```

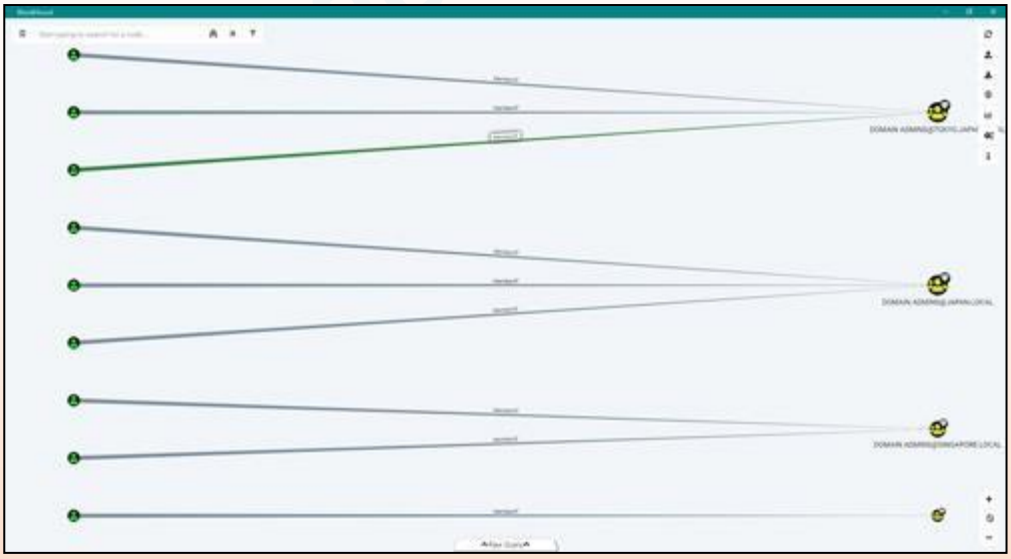
It is now time to begin gathering data. Enter “***Name of the directory”.exe -c all*** to begin gathering information. You can see that SharpHound has created a file with the name yyyyMMddhhmmss BloodHound.zip after the collection is complete. We will upload the Neo4j database for BloodHound there.

After the data collection procedure is finished. It's time to upload that into BloodHound and begin creating some queries.

Uploading Data and Finding Shortest Path

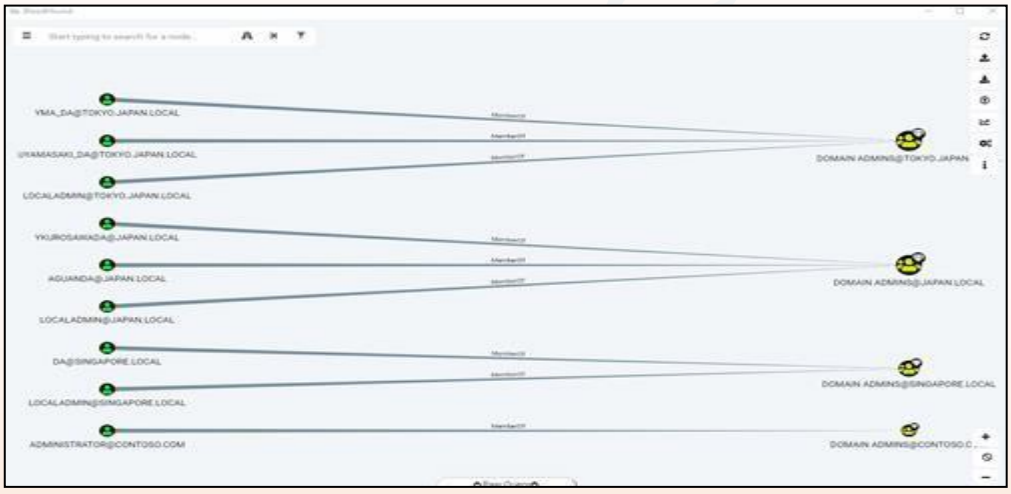
The Neo4j database is empty in the beginning, so it returns, "No data returned from query." Upload the .zip file that SharpHound generated by pressing Upload and selecting the file.

BloodHound will import the JSON files contained in the .zip into Neo4j. You will now be presented with a screen that looks something like this, a default view showing all domain admins:



Depending on how many domains you have or have had scanned by SharpHound, there may be a different number of domain admin groups.

Let us now do a built-in query to determine the shortest route to domain admin. By selecting the icon to the left of the search box, choosing Queries, and then selecting Find Shortest Paths to Domain Admin, we can accomplish this.



Conclusion

It is advisable to choose a BloodHound evaluation when you intend to investigate trustworthy connections in Active Directory environments. It enables you to restrict the path and prevents attackers from acquiring domain admin permissions by bringing you insights into intricate attack paths on a network.

References

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

https://tryhackme.com/room/postexploit

For enumeration details

https://bloodhound.readthedocs.io/en/latest/data-collection/sharphound-all-flags.html

Link

@CYBERPUBLICSCHOOL

CYBERPUBLICSCHOOL
JOIN AND FOLLOW US EVERYWHERE

CYBER PUBLIC SCHOOL

- JR. Penetration Tester
- Offensive Security (OSCP)
- Red Teaming
- Cloud Penetration Testing
- CEH (V12)

Phone no.: +91 9631750498 India
+61 424866396 Australia

OUR SUCCESSFUL OSCP STUDENT.

- WEBSITE

https://cyberpublicschool.com/

@CYBERPUBLICSCHOOL SHARE- IF YOU LIKE

Link