In the step of enumerating active directory after getting some valid creds our best and most powerfull tool for enumerating the AD environment is **BloodHound,** so now as we have a valid creds we will use it to get more information about our environment.

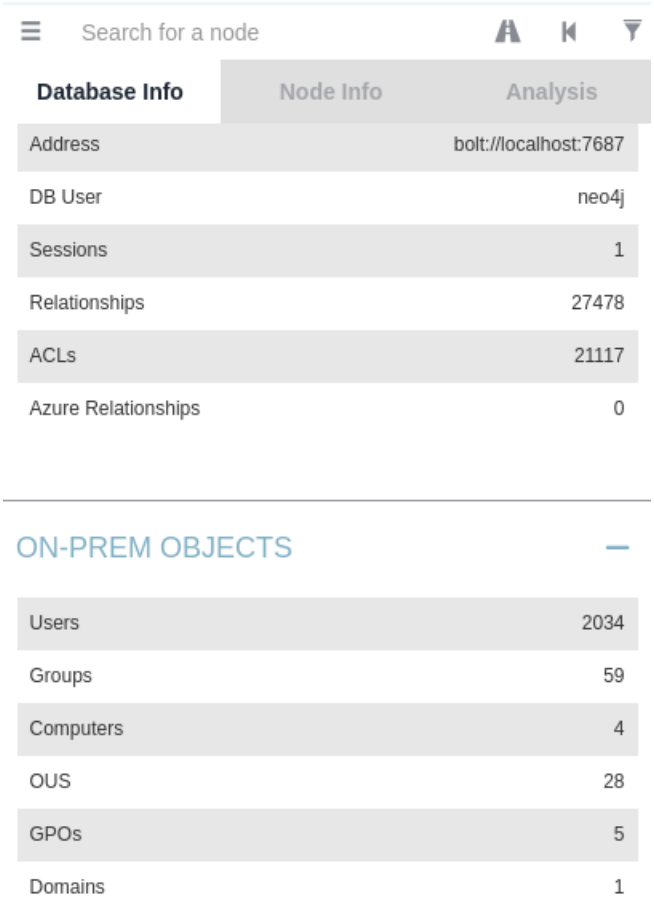
At first in order to use BloodHound and visualize information on it, we must use Sharphound.

Sharphound is the enumeration tool of Bloodhound. It is used to enumerate the AD information that can then be visually displayed in Bloodhound.

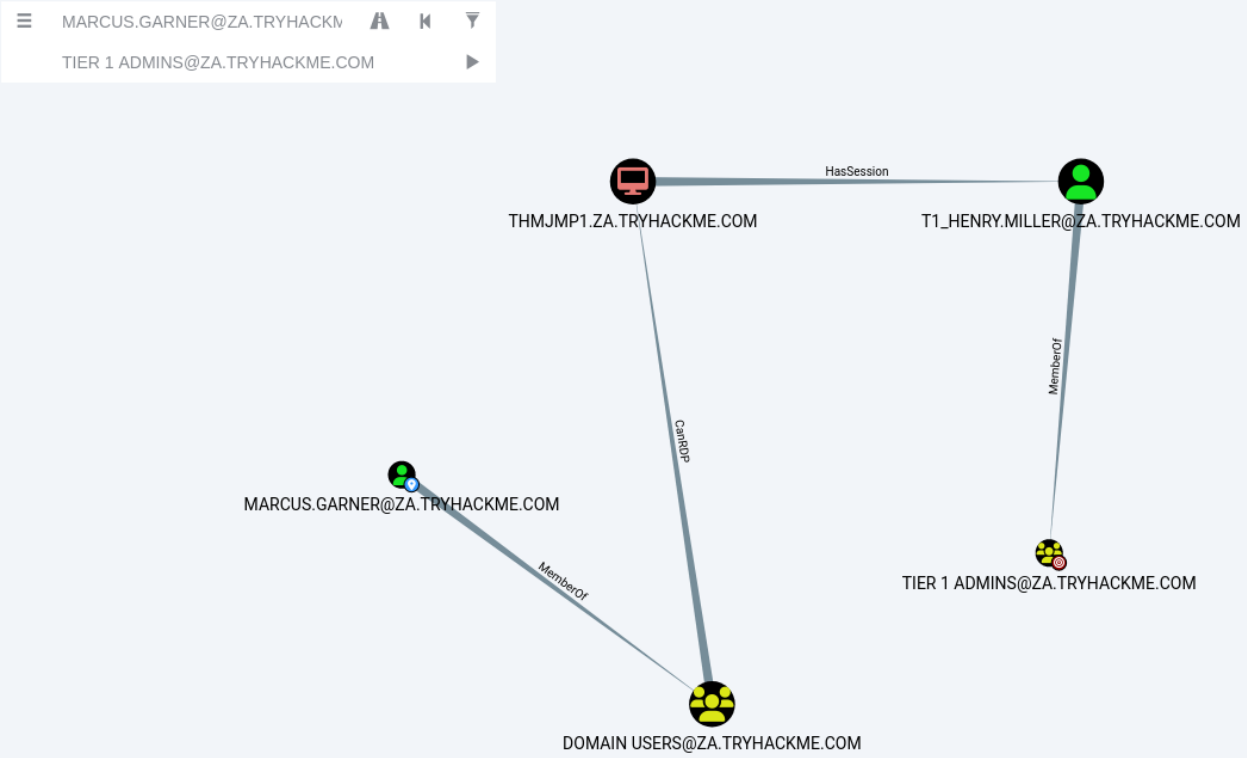
We will use this command in order to collect all the files we need to use BloodHound.

SharpHound.exe --CollectionMethods All --Domain za.tryhackme.com --ExcludeDCs

After uploading the data to bloodhound at the top left under the search bar we can see usefull and general information about our environment



As we are currently having creds of a user called **marcus.garner** we will check for attack pathes to the admins groups in order to escalate our privileges and we will find that there is an available attack path to the **Tier 1 Admins group**



BloodHound also gives us suggestions about what we can do in order to follow this attack path and get to the account we want and this is what we will do:

1. Use our AD credentials to RDP into **THMJMP1**.
2. Look for a privilege escalation vector on the host that would provide us with Administrative access.
3. Using Administrative access, we can use credential harvesting techniques and tools such as Mimikatz.
4. Since the T1 Admin has an active session on **THMJMP1**, our credential harvesting would provide us with the NTLM hash of the associated account.

We can do the same thing for every user we exposed its creds every time we may find another interesting attack paths to discover because of the powerful tool bloodhound.