91.3 - Plumbhound - Domain Enumeration

1 - We need to leave Bloodhound running for this. So, do not even bother to close it. If you already did, go back, and get it up and running.

2 - Search for Plumhound. Go to the GitHub repo and get the https address to clone it.

3 - Git and clone the repo. Best to put it under the "/opt" folder. Make new dir, and install the repo in there.

4 - After we downloaded it, we are going to need to install it. To do that we can run "#sudo pip3 install -r requirements.txt" from within the directory which has the downloaded data from the github repo.

Now, we are going to be running the tool.

5 - We can run it by issuing the command "#sudo python3 PlumHound.py --easy -p neo4j1". Remember, we need Bloodhound up and running.

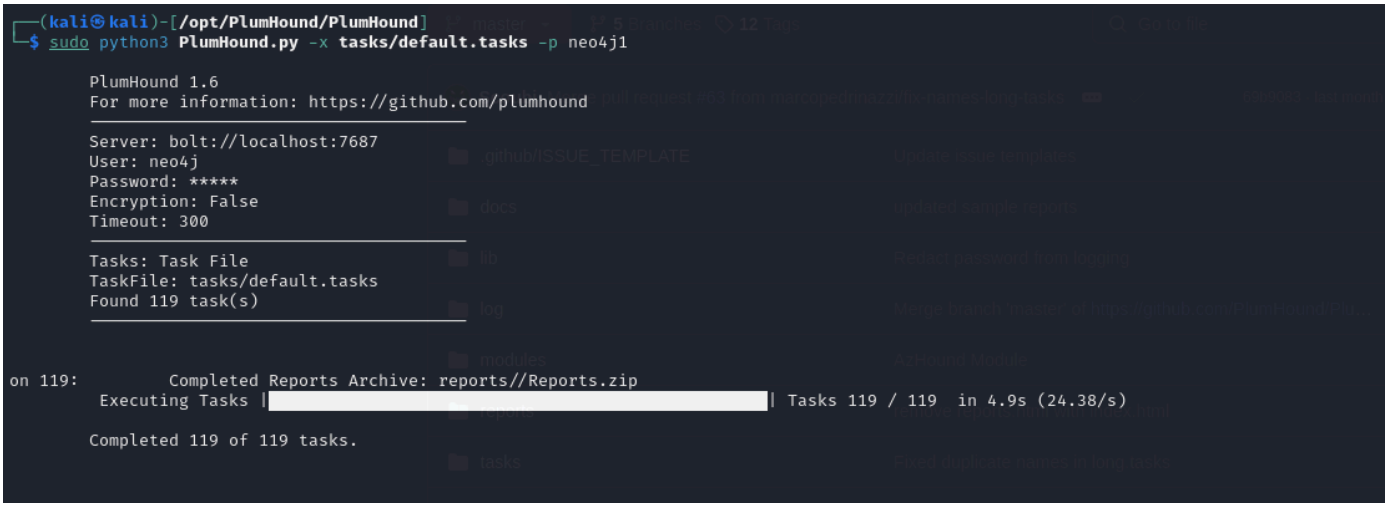
This command will be just a test, that is why we are using --easy. This is just to make sure it is working properly, and we are actually pulling the data from the domain.

```
┌──(kali㉿kali)-[/opt/PlumHound/PlumHound]
└─$ sudo python3 PlumHound.py --easy -p neo4j1

       PlumHound 1.6
       For more information: https://github.com/plumhound
       ------------------------------------------
       Server: bolt://localhost:7687
       User: neo4j
       Password: *****
       Encryption: False
       Timeout: 300
       ------------------------------------------
       Task: Easy
       Query Title: Domain Users
       Query Format: STDOUT
       Query Cypher: MATCH (n:User) RETURN n.name, n.displayname
       ------------------------------------------
INFO   Found 1 task(s)
INFO   ------------------------------------------

on 1: n.name                        n.displayname
     ------------------------------  ------------
     KRBTGT@ONEPIECE.LOCAL
     SQLSERVICE@ONEPIECE.LOCAL      SQL Service
     USOGEKING@ONEPIECE.LOCAL       Usopp Sogeking
     ADMINISTRATOR@ONEPIECE.LOCAL

     GUEST@ONEPIECE.LOCAL
     GDKJEQGFSI@ONEPIECE.LOCAL      gDKjEqGfSI
     ZRORONOA@ONEPIECE.LOCAL        Zoro Roronoa
     LMONKEY@ONEPIECE.LOCAL         Luffy Monkey
     NT AUTHORITY@ONEPIECE.LOCAL

        Executing Tasks |                                        | Tasks 1 / 1  in 0.1s (1047.80/s)

       Completed 1 of 1 tasks.
```

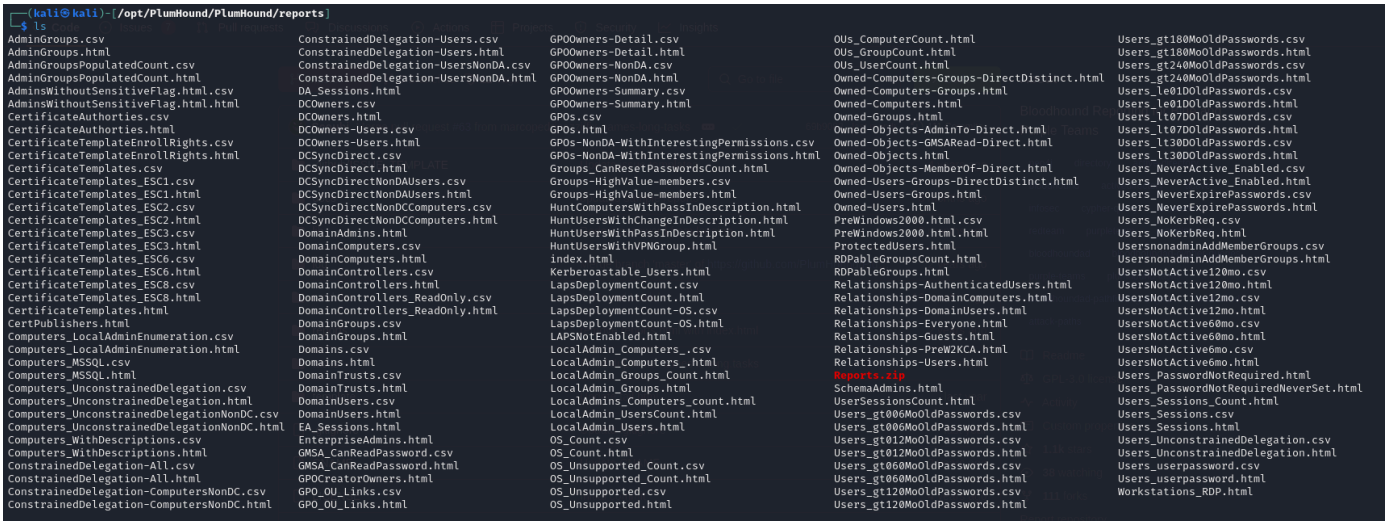
We can see it is working properly.

6 - We are going to run "#sudo python3 PlumHound.py -x tasks/default.tasks -p neo4j1"

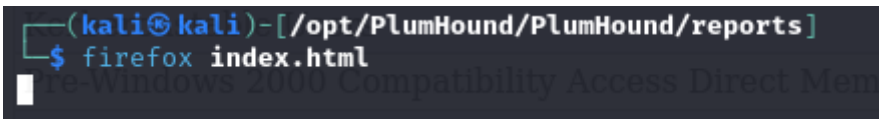
We can also check the other modules, and features scans we can use in PlumHound.

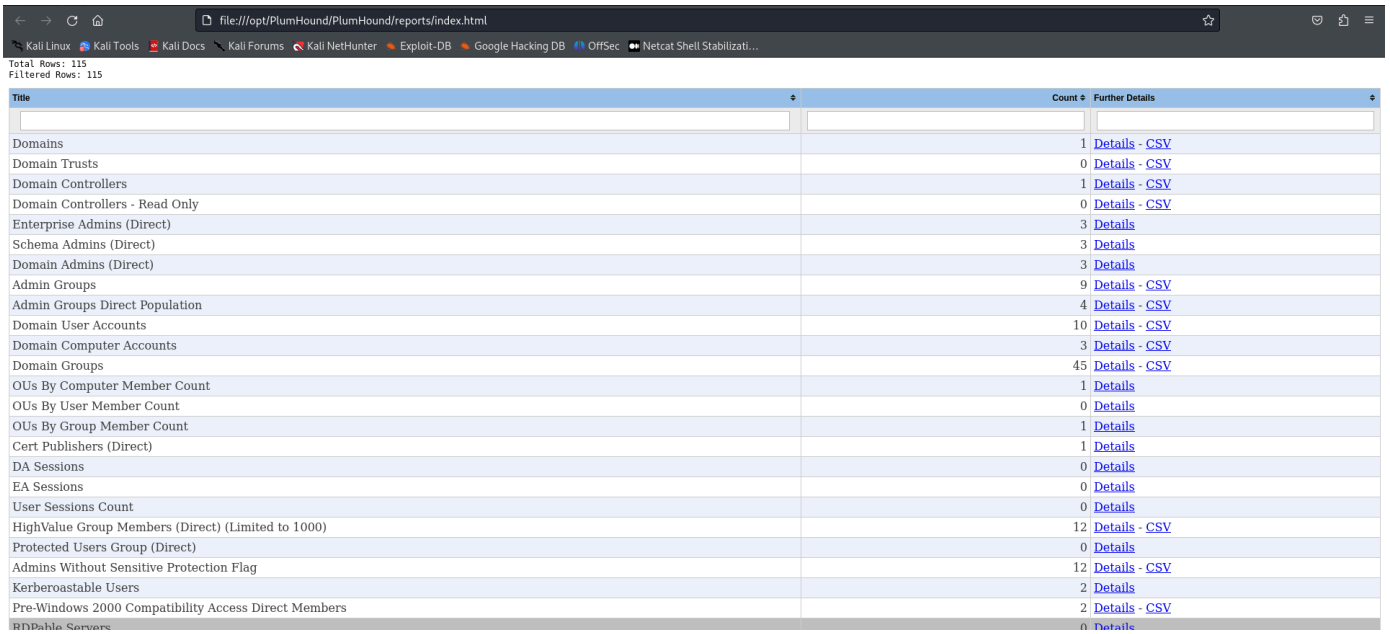


This will create a folder with all the reports called "reports", and a zip file as well.



Our best friend here is going to be the "index.html" file, where we can see all the other reports, and access it through a web browser.





We can access a lot of data here.