91.2 - Bloodhound - Domain Enumeration

1 - install latest version of bloodhound (#sudo pip install bloodhound)

This will install the latest and greatest. And, if there is not already, it is going to install the ingestors.

2 - Now, we are going to run "#sudo neo4j console". This is required for us to be able to run bloodhound. We are going to be hosting the program on the local host, and a link should show up in the output of the command with the link to the just started service. We can open it and interact with the program through a web browser. The right term is remote interface. So, we have a remote interface that gets spin up for us, so we can use the features of the program. We can right rick and select "open link".

3 - We are going to need to sign in, and set new password for account. The default credentials are user: neo4j , and password: neo4j . Change password to : neo4j1 . We need to have this running in order to run bloodhound. So, keep it running, and move along.

4 - Run "# sudo bloodhound". If you have any data, clear that out.

5 - Lets make a directory. "cd" into it.

6 - Run "#sudo bloodhound-python -d ONEPIECE.local -u LMonkey -p Password1 -ns 192.168.163.156 -c all"

This is the command that generates the dump.

-ns for Name Server, which in our case is going to be the Domain Controller IP Address.

-c is what are we collecting. in this case "all".

```
┌──(kali㉿kali)-[~/Desktop/TCM-ActiveDirectory-Lab/DomainController-Enumaration/bloodhound]
└─$ sudo /usr/bin/bloodhound-python -d ONEPIECE.local -u LMonkey -p Password1 -ns 192.168.163.156 -c all
INFO: Found AD domain: onepiece.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (goingmerry-dc.onepiece.local:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: goingmerry-dc.onepiece.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 3 computers
INFO: Connecting to LDAP server: goingmerry-dc.onepiece.local
INFO: Found 9 users
INFO: Found 52 groups
INFO: Found 3 gpos
INFO: Found 2 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: THEROBOT.ONEPIECE.local
INFO: Querying computer: THENAVIGATOR.ONEPIECE.local
INFO: Querying computer: GoingMerry-DC.ONEPIECE.local
INFO: Done in 00M 01S
```

Tadah!

We are going to import all the data into bloodhound.

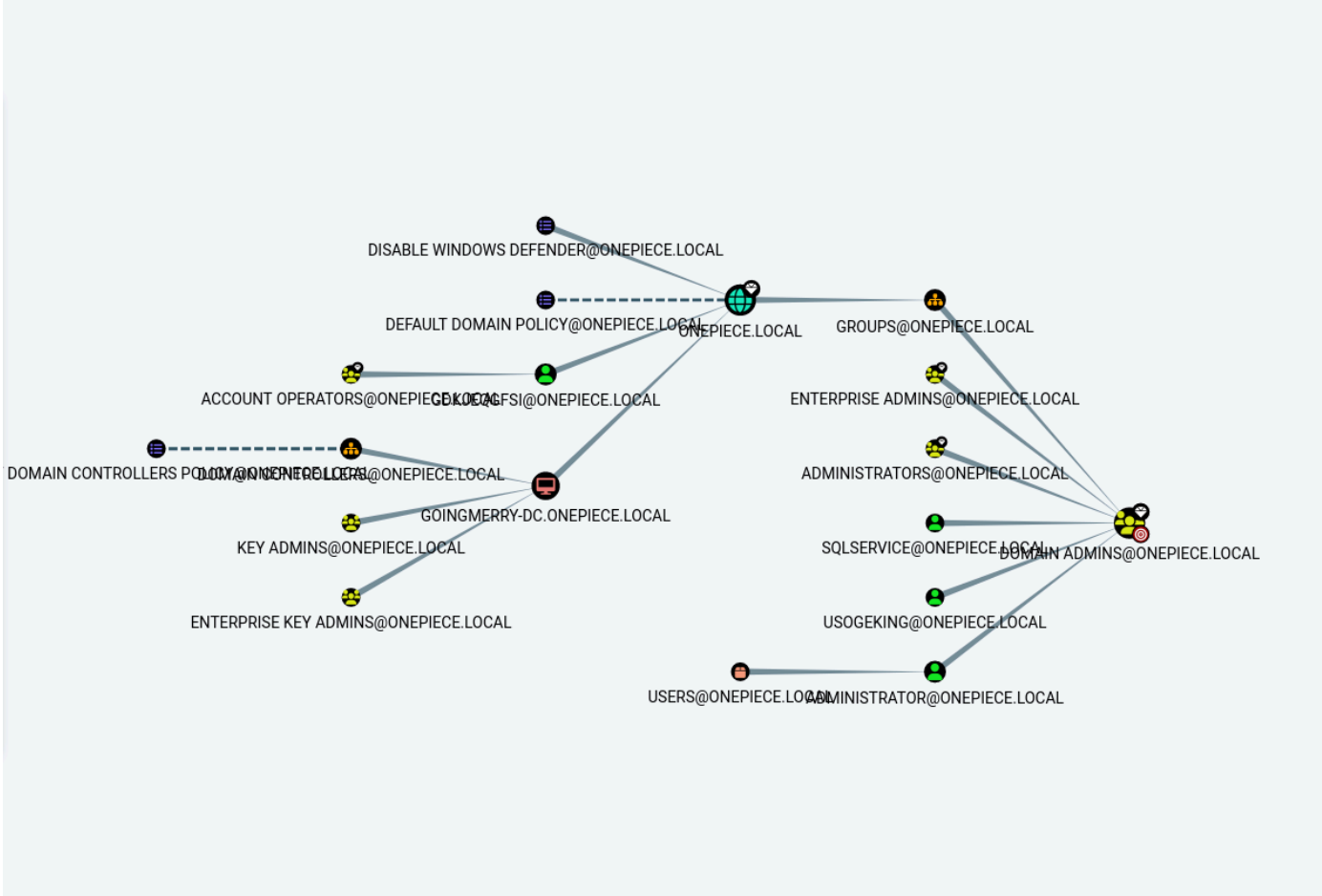
We want to go to bloodhound remote interface > upload data > select all that you want, we can select all of them > open.

The nice thing about Bloodhound is that it generates graphics and it shows the data in a easy to ready format, which allows for a quicker and better understanding of what we are dealing with.

Explore as much as you can.

"Shortest Paths" section under the Analysis tab seems to be really interesting.

"Kerberos Interaction" under the Analysis tab is also very valuable information.



Shortest Path to Domain Admin accounts.