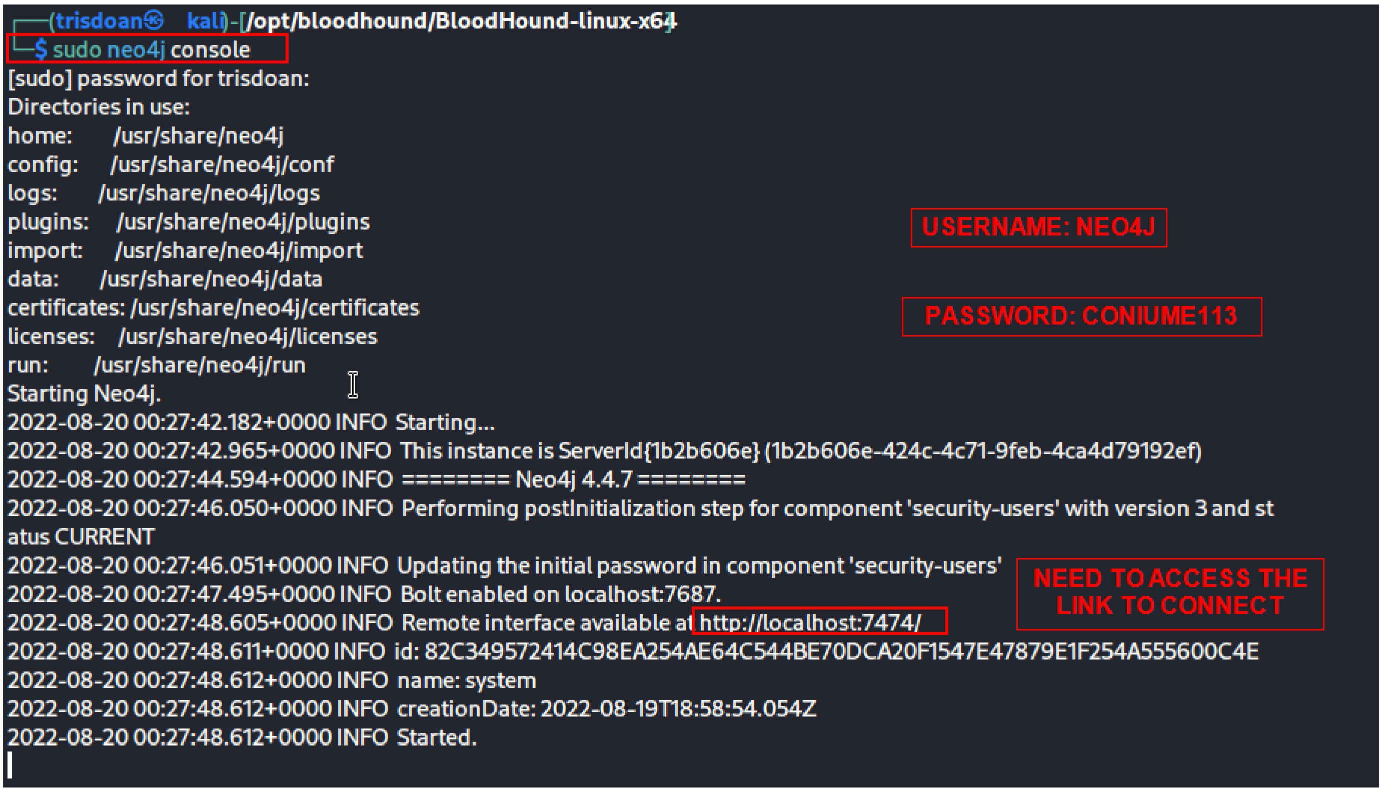
BLOODHOUND

**ALLOW US TO VISUALIZE IN A GRAPH FORM WHAT IS GOING ON IN THE DOMAIN IN THE NETWORK AND WHERE WE CAN FIND SENSITIVE USERS THAT MIGHT BE LOGIN, OR WHERE WE CAN FIND THE SHORTEST PATH TO DOMAIN ADMIN. **

1.

SET UP NEO4J



```
┌──(trisdoan㉿ kali)-[/opt/bloodhound/BloodHound-linux-x64]
└─$ sudo neo4j console
[sudo] password for trisdoan:
Directories in use:
home:       /usr/share/neo4j
config:     /usr/share/neo4j/conf
logs:       /usr/share/neo4j/logs
plugins:    /usr/share/neo4j/plugins
import:     /usr/share/neo4j/import
data:       /usr/share/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses:   /usr/share/neo4j/licenses
run:        /usr/share/neo4j/run
Starting Neo4j.
2022-08-20 00:27:42.182+0000 INFO  Starting...
2022-08-20 00:27:42.965+0000 INFO  This instance is ServerId{1b2b606e} (1b2b606e-424c-4c71-9feb-4ca4d79192ef)
2022-08-20 00:27:44.594+0000 INFO  ======== Neo4j 4.4.7 ========
2022-08-20 00:27:46.050+0000 INFO  Performing postInitialization step for component 'security-users' with version 3 and st
atus CURRENT
2022-08-20 00:27:46.051+0000 INFO  Updating the initial password in component 'security-users'
2022-08-20 00:27:47.495+0000 INFO  Bolt enabled on localhost:7687.
2022-08-20 00:27:48.605+0000 INFO  Remote interface available at http://localhost:7474/
2022-08-20 00:27:48.611+0000 INFO  id: 82C349572414C98EA254AE64C544BE70DCA20F1547E47879E1F254A555600C4E
2022-08-20 00:27:48.612+0000 INFO  name: system
2022-08-20 00:27:48.612+0000 INFO  creationDate: 2022-08-19T18:58:54.054Z
2022-08-20 00:27:48.612+0000 INFO  Started.
```

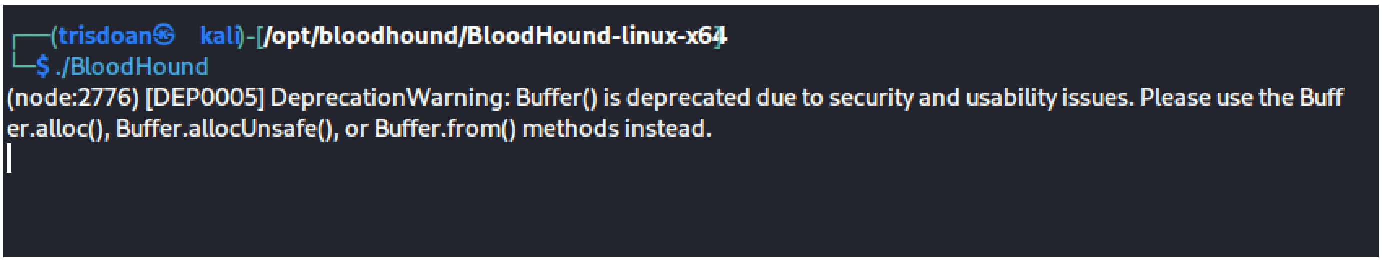
USERNAME: NEO4J

PASSWORD: CONIUME113

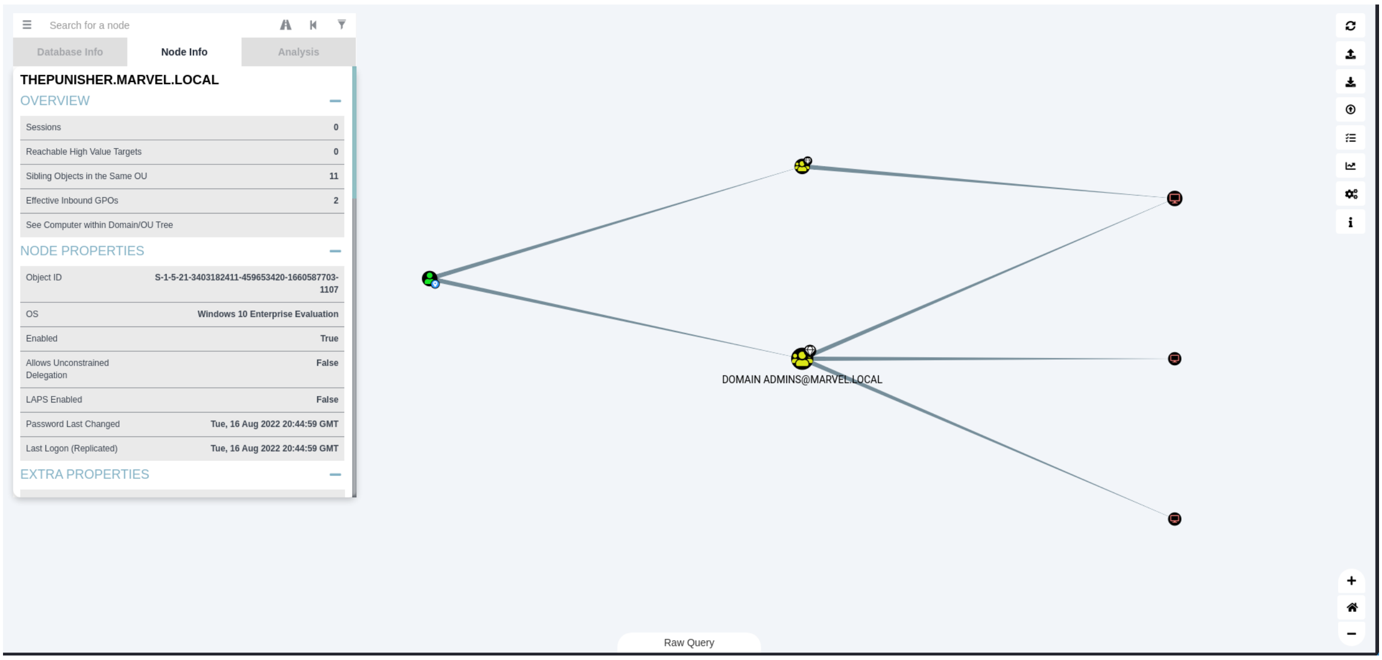
NEED TO ACCESS THE LINK TO CONNECT

2.

RUN NEW TAB AND RUN BLOODHOUND IN /OPT FOLDER



```
┌──(trisdoan㉿ kali)-[/opt/bloodhound/BloodHound-linux-x64]
└─$ ./BloodHound
(node:2776) [DEP0005] DeprecationWarning: Buffer() is deprecated due to security and usability issues. Please use the Buff
er.alloc(), Buffer.allocUnsafe(), or Buffer.from() methods instead.
```



THEPUNISHER.MARVEL.LOCAL

OVERVIEW

Sessions	0
Reachable High Value Targets	0
Sibling Objects in the Same OU	11
Effective Inbound GPOs	2
See Computer within Domain/OU Tree	

NODE PROPERTIES

Object ID	S-1-5-21-3403182411-459653420-1660587703-1107
OS	Windows 10 Enterprise Evaluation
Enabled	True
Allows Unconstrained Delegation	False
LAPS Enabled	False
Password Last Changed	Tue, 16 Aug 2022 20:44:59 GMT
Last Logon (Replicated)	Tue, 16 Aug 2022 20:44:59 GMT

EXTRA PROPERTIES