BloodHound

Information Security Inc.

Contents

- About BloodHound
- Testing Environment
- Installing BloodHound
- Using BloodHound
- References

About BloodHound

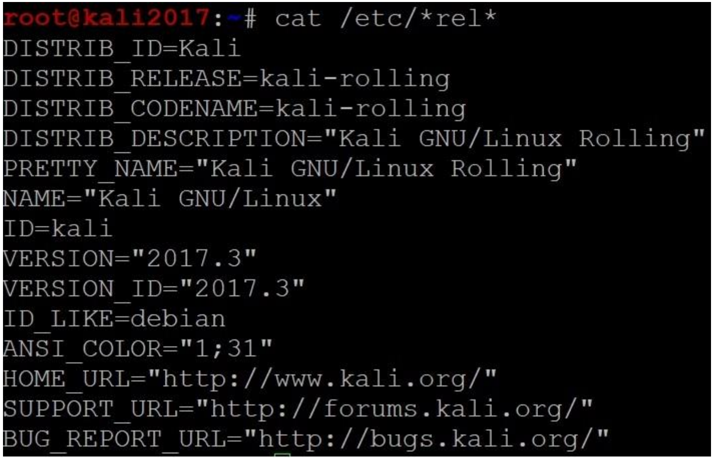
BloodHound is a single page Javascript web application, built on top of Linkurious, compiled with Electron, with a Neo4j database fed by a PowerShell ingestor

About BloodHound

- BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment
- Attackers can use BloodHound to easily identify highly complex attack paths that would otherwise be impossible to quickly identify
- Defenders can use BloodHound to identify and eliminate those same attack path

Testing Environment

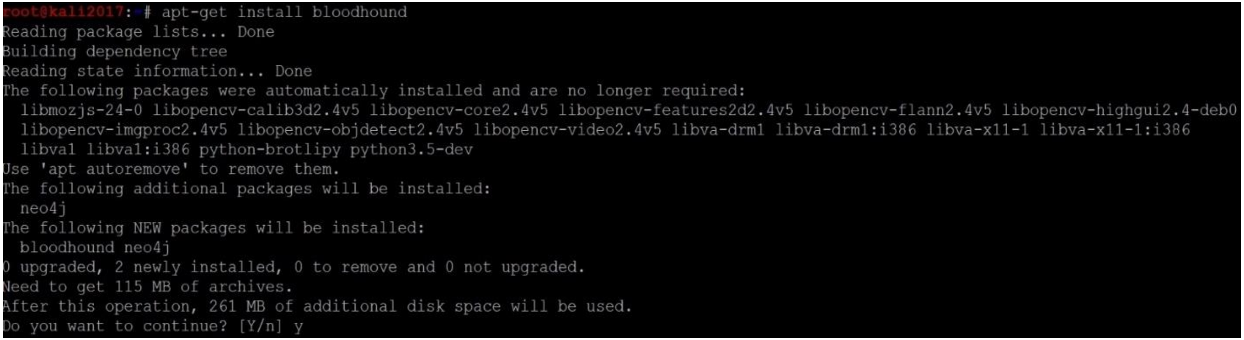
- Kali Linux 2017



```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.3"
VERSION_ID="2017.3"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Installing BloodHound

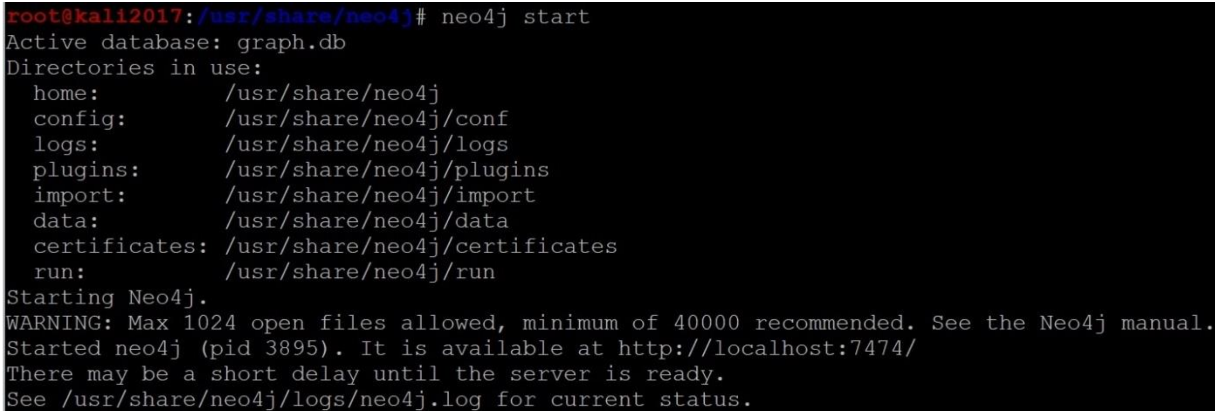
- apt-get install bloodhound



```
root@kali2017:~# apt-get install bloodhound
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libmozjs-24-0 libopencv-calib3d2.4v5 libopencv-core2.4v5 libopencv-features2d2.4v5 libopencv-flann2.4v5 libopencv-highgui2.4-deb0
  libopencv-imgproc2.4v5 libopencv-objdetect2.4v5 libopencv-video2.4v5 libva-drm1 libva-drm1:i386 libva-x11-1 libva-x11-1:i386
  libva1 libva1:i386 python-brotlipy python3.5-dev
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  neo4j
The following NEW packages will be installed:
  bloodhound neo4j
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 115 MB of archives.
After this operation, 261 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Installing BloodHound

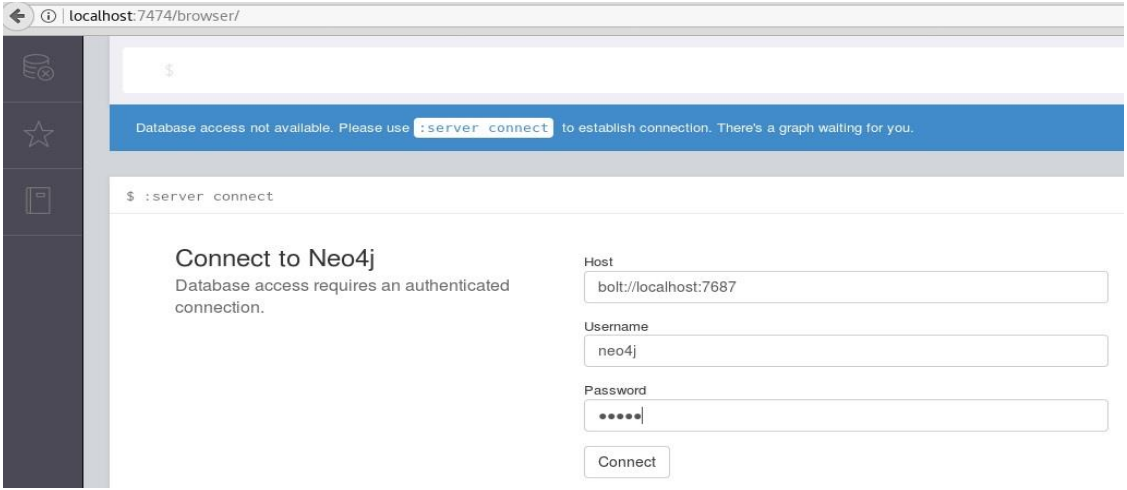
- Starting neo4j



```
root@kali2017:/usr/share/neo4j# neo4j start
Active database: graph.db
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
  run:          /usr/share/neo4j/run
Starting Neo4j.
WARNING: Max 1024 open files allowed, minimum of 40000 recommended. See the Neo4j manual.
Started neo4j (pid 3895). It is available at http://localhost:7474/
There may be a short delay until the server is ready.
See /usr/share/neo4j/logs/neo4j.log for current status.
```

Installing BloodHound

- Open browser to http://localhost:7474 neo4j web interface and set initial admin password



Database access not available. Please use `:server connect` to establish connection. There's a graph waiting for you.

```
$ :server connect
```

Connect to Neo4j

Database access requires an authenticated connection.

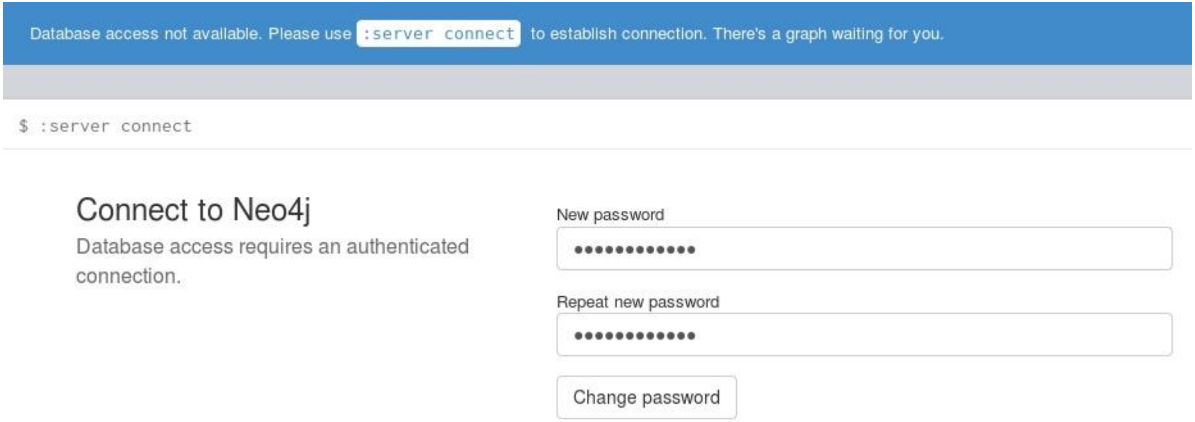
Host: bolt://localhost:7687

Username: neo4j

Password: •••••

Installing BloodHound

- Open browser to http://localhost:7474 neo4j web interface and set initial admin password



Database access not available. Please use `:server connect` to establish connection. There's a graph waiting for you.

```
$ :server connect
```

Connect to Neo4j

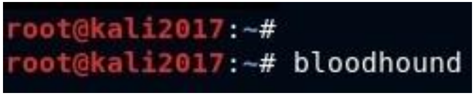
Database access requires an authenticated connection.

New password: ••••••••••••

Repeat new password: ••••••••••••

Using BloodHound

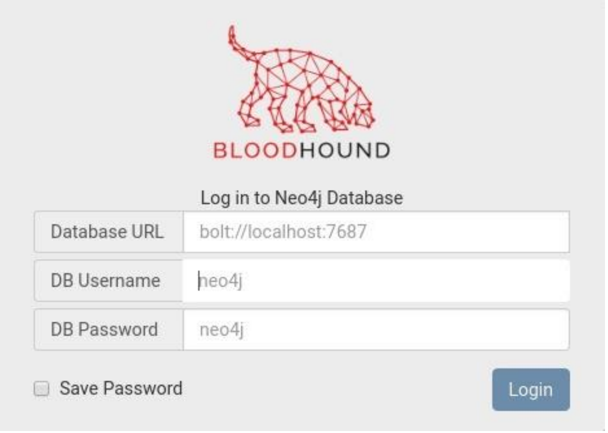
- Running BloodHound



```
root@kali2017:~#
root@kali2017:~# bloodhound
```

Using BloodHound

- Running BloodHound -> the login screen



BLOODHOUND

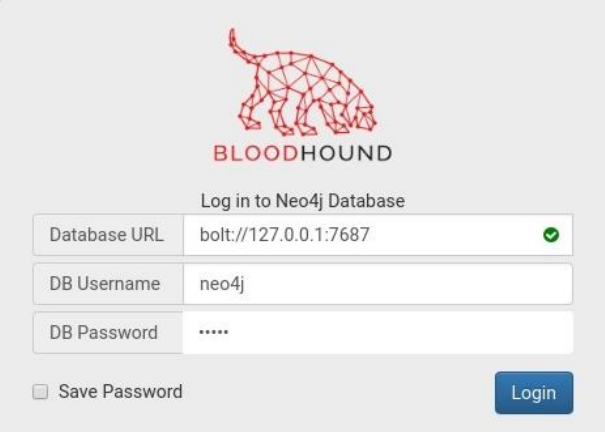
Log in to Neo4j Database

Database URL	bolt://localhost:7687
DB Username	neo4j
DB Password	neo4j

☐ Save Password

Using BloodHound

- Running BloodHound -> logging default username neo4j, default password neo4j



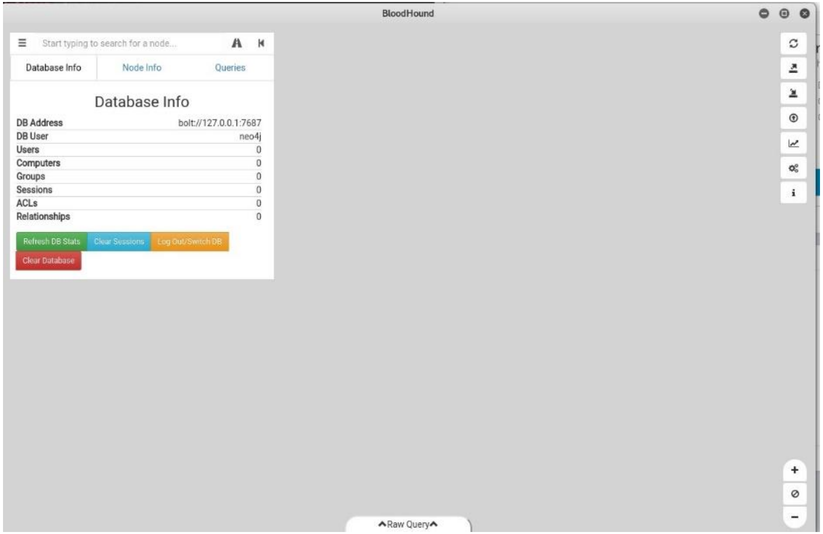
Log in to Neo4j Database

Database URL	bolt://127.0.0.1:7687
DB Username	neo4j
DB Password	•••••

□ Save Password

Using BloodHound

- After login -> Can see Bloodhound tool minus any data. You can now import your data and get analyzing.

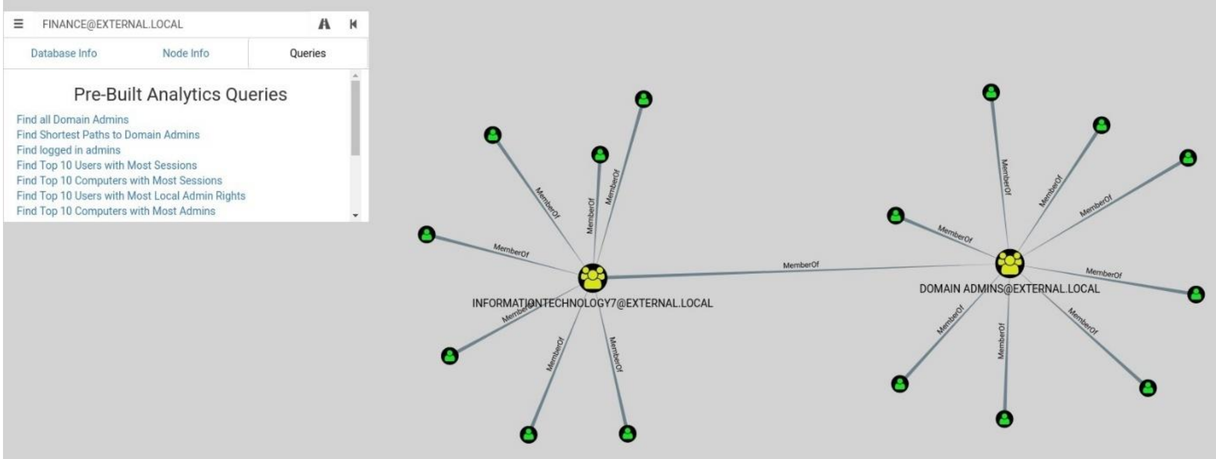


Database Info

DB Address	bolt://127.0.0.1:7687
DB User	neo4j
Users	0
Computers	0
Groups	0
Sessions	0
ACLs	0
Relationships	0

Using BloodHound

- Pre-built Analytics Query


FINANCE@EXTERNAL.LOCAL
Database Info
Node Info
Queries

Pre-Built Analytics Queries

Find all Domain Admins
Find Shortest Paths to Domain Admins
Find logged in admins
Find Top 10 Users with Most Sessions
Find Top 10 Computers with Most Sessions
Find Top 10 Users with Most Local Admin Rights
Find Top 10 Computers with Most Admins

INFORMATIONTECHNOLOGY7@EXTERNAL.LOCAL
DOMAIN ADMINS@EXTERNAL.LOCAL
MemberOf

References

- Kitploit
http://www.kitploit.com/2017/09/bloodhound-six-degrees-of-domain-admin.html

- Kali Linux 2017
http://www.kitploit.com/2017/09/kali-linux-20172-release-best.html

- Bloodhound quick guide
https://stealingthe.network/quick-guide-to-installing-bloodhound-in-kali-rolling/

- Interface intro
https://github.com/BloodHoundAD/BloodHound/wiki/Interface-Intro

- Users intro
https://github.com/BloodHoundAD/BloodHound/wiki/Users

- Data ingestion
https://github.com/BloodHoundAD/BloodHound/wiki/Data-Collection-Intro