Attacking Active Directory: Post-Compromise Enumeration

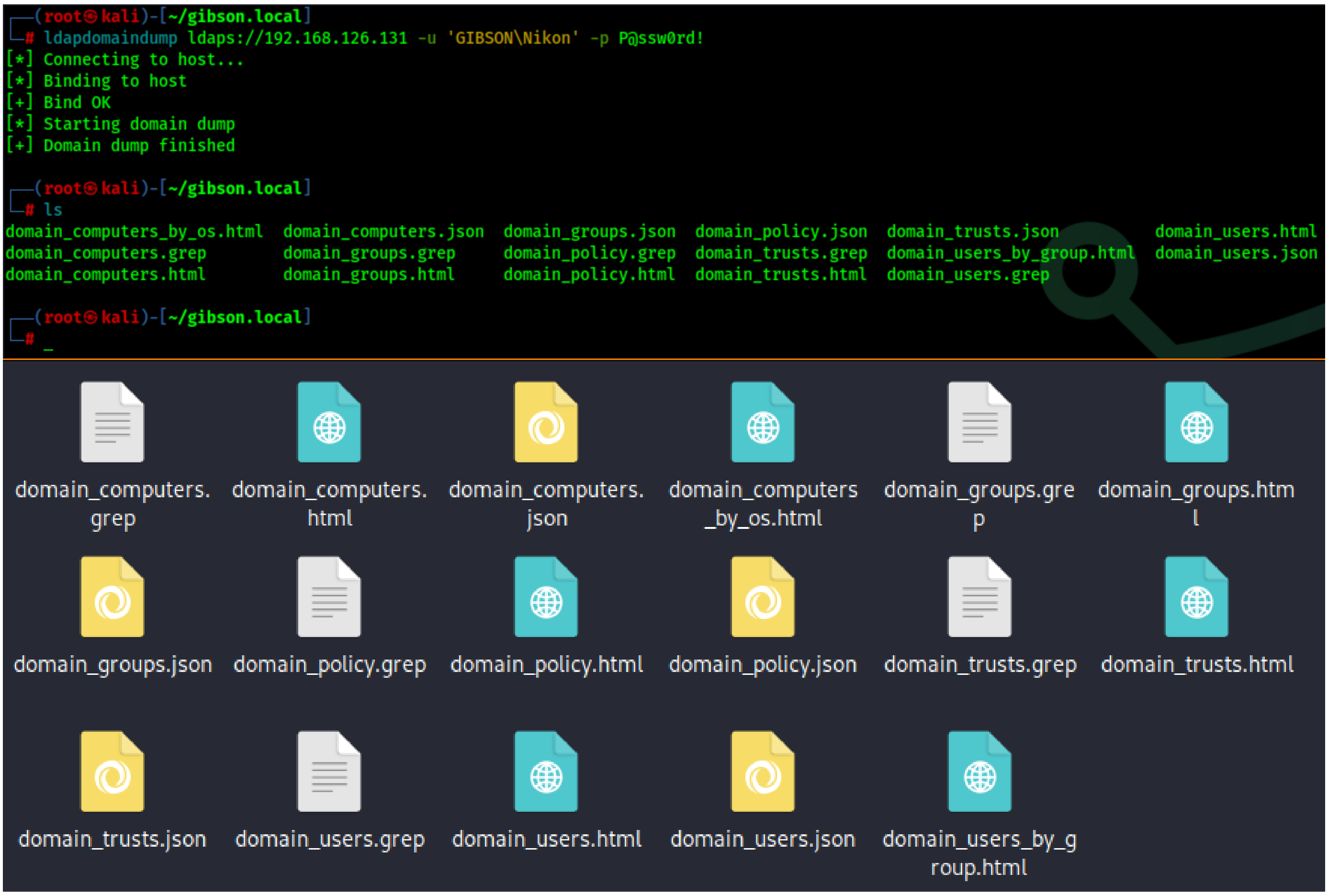
Introduction

- Enumeration using
- Bloodhound
- Plumhound
- ldapdomaindump
- PingCastle
  etc.

Domain Enumeration with ldapdomaindump

Same thing used NTLMRelayX

```
ldapdomaindump ldaps://IP -u 'domain\user' -p password
```

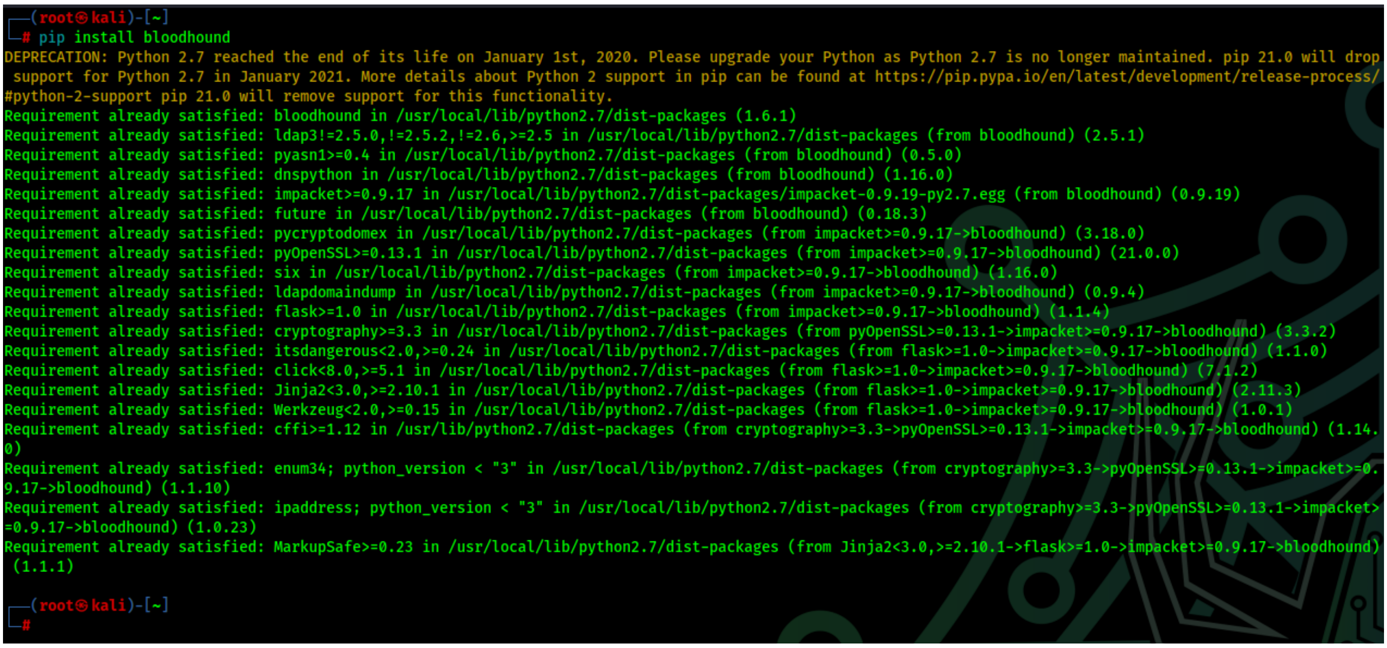


```
┌──(root㉿kali)-[~/gibson.local]
└─# ldapdomaindump ldaps://192.168.126.131 -u 'GIBSON\Nikon' -p P@ssw0rd!
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished

┌──(root㉿kali)-[~/gibson.local]
└─# ls
domain_computers_by_os.html  domain_computers.json  domain_groups.json  domain_policy.json  domain_trusts.json          domain_users.html
domain_computers.grep        domain_groups.grep     domain_policy.grep  domain_trusts.grep  domain_users_by_group.html  domain_users.json
domain_computers.html        domain_groups.html     domain_policy.html  domain_trusts.html  domain_users.grep

┌──(root㉿kali)-[~/gibson.local]
└─# _
```

Domain Enumeration with Bloodhound

Update Bloodhound

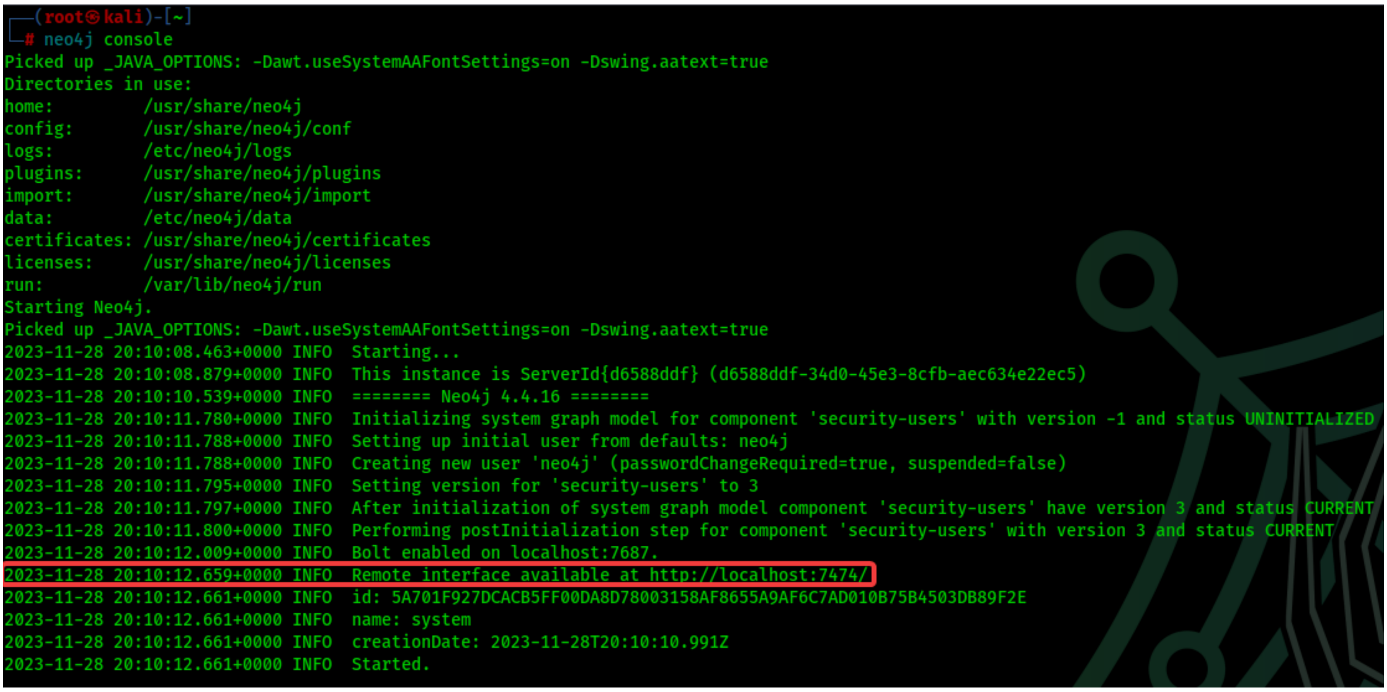
```
pip install bloodhound
```



```
┌──(root㉿kali)-[~]
└─# pip install bloodhound
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop
 support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/
#python-2-support pip 21.0 will remove support for this functionality.
Requirement already satisfied: bloodhound in /usr/local/lib/python2.7/dist-packages (1.6.1)
Requirement already satisfied: ldap3!=2.5.0,!=2.5.2,!=2.6,>=2.5 in /usr/local/lib/python2.7/dist-packages (from bloodhound) (2.5.1)
Requirement already satisfied: pyasn1>=0.4 in /usr/local/lib/python2.7/dist-packages (from bloodhound) (0.5.0)
Requirement already satisfied: dnspython in /usr/local/lib/python2.7/dist-packages (from bloodhound) (1.16.0)
Requirement already satisfied: impacket>=0.9.17 in /usr/local/lib/python2.7/dist-packages/impacket-0.9.19-py2.7.egg (from bloodhound) (0.9.19)
Requirement already satisfied: future in /usr/local/lib/python2.7/dist-packages (from bloodhound) (0.18.3)
Requirement already satisfied: pycryptodomex in /usr/local/lib/python2.7/dist-packages (from impacket>=0.9.17->bloodhound) (3.18.0)
Requirement already satisfied: pyOpenSSL>=0.13.1 in /usr/local/lib/python2.7/dist-packages (from impacket>=0.9.17->bloodhound) (21.0.0)
Requirement already satisfied: six in /usr/local/lib/python2.7/dist-packages (from impacket>=0.9.17->bloodhound) (1.16.0)
Requirement already satisfied: ldapdomaindump in /usr/local/lib/python2.7/dist-packages (from impacket>=0.9.17->bloodhound) (0.9.4)
Requirement already satisfied: flask>=1.0 in /usr/local/lib/python2.7/dist-packages (from impacket>=0.9.17->bloodhound) (1.1.4)
Requirement already satisfied: cryptography>=3.3 in /usr/local/lib/python2.7/dist-packages (from pyOpenSSL>=0.13.1->impacket>=0.9.17->bloodhound) (3.3.2)
Requirement already satisfied: itsdangerous<2.0,>=0.24 in /usr/local/lib/python2.7/dist-packages (from flask>=1.0->impacket>=0.9.17->bloodhound) (1.1.0)
Requirement already satisfied: click<8.0,>=5.1 in /usr/local/lib/python2.7/dist-packages (from flask>=1.0->impacket>=0.9.17->bloodhound) (7.1.2)
Requirement already satisfied: Jinja2<3.0,>=2.10.1 in /usr/local/lib/python2.7/dist-packages (from flask>=1.0->impacket>=0.9.17->bloodhound) (2.11.3)
Requirement already satisfied: Werkzeug<2.0,>=0.15 in /usr/local/lib/python2.7/dist-packages (from flask>=1.0->impacket>=0.9.17->bloodhound) (1.0.1)
Requirement already satisfied: cffi>=1.12 in /usr/lib/python2.7/dist-packages (from cryptography>=3.3->pyOpenSSL>=0.13.1->impacket>=0.9.17->bloodhound) (1.14.
0)
Requirement already satisfied: enum34; python_version < "3" in /usr/local/lib/python2.7/dist-packages (from cryptography>=3.3->pyOpenSSL>=0.13.1->impacket>=0.
9.17->bloodhound) (1.1.10)
Requirement already satisfied: ipaddress; python_version < "3" in /usr/local/lib/python2.7/dist-packages (from cryptography>=3.3->pyOpenSSL>=0.13.1->impacket>
=0.9.17->bloodhound) (1.0.23)
Requirement already satisfied: MarkupSafe>=0.23 in /usr/local/lib/python2.7/dist-packages (from Jinja2<3.0,>=2.10.1->flask>=1.0->impacket>=0.9.17->bloodhound)
 (1.1.1)

┌──(root㉿kali)-[~]
└─#
```

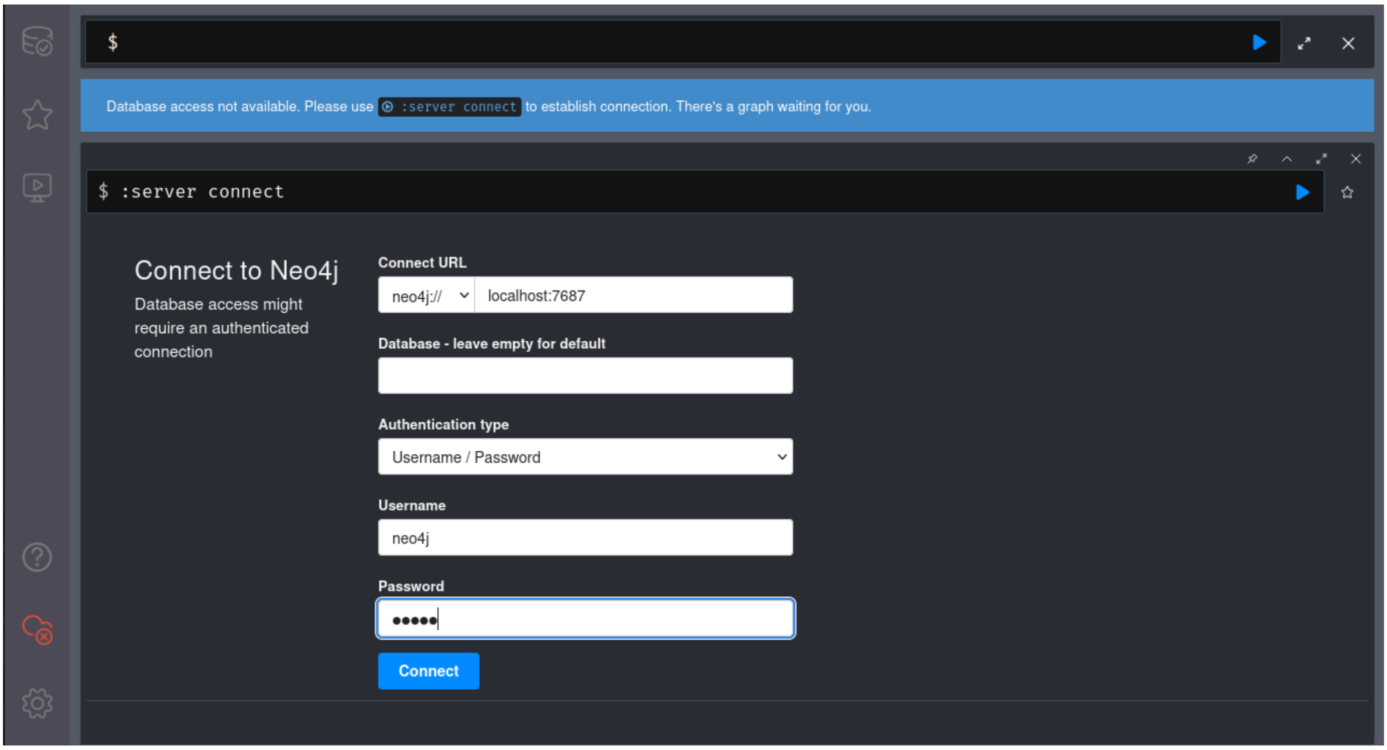
Start Neo4j

```
neo4j console
```



```
┌──(root㉿kali)-[~]
└─# neo4j console
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Directories in use:
home:         /usr/share/neo4j
config:       /usr/share/neo4j/conf
logs:         /etc/neo4j/logs
plugins:      /usr/share/neo4j/plugins
import:       /usr/share/neo4j/import
data:         /etc/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses:     /usr/share/neo4j/licenses
run:          /var/lib/neo4j/run
Starting Neo4j.
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
2023-11-28 20:10:08.463+0000 INFO  Starting...
2023-11-28 20:10:08.879+0000 INFO  This instance is ServerId{d6588ddf} (d6588ddf-34d0-45e3-8cfb-aec634e22ec5)
2023-11-28 20:10:10.539+0000 INFO  ======== Neo4j 4.4.16 ========
2023-11-28 20:10:11.780+0000 INFO  Initializing system graph model for component 'security-users' with version -1 and status UNINITIALIZED
2023-11-28 20:10:11.788+0000 INFO  Setting up initial user from defaults: neo4j
2023-11-28 20:10:11.788+0000 INFO  Creating new user 'neo4j' (passwordChangeRequired=true, suspended=false)
2023-11-28 20:10:11.795+0000 INFO  Setting version for 'security-users' to 3
2023-11-28 20:10:11.797+0000 INFO  After initialization of system graph model component 'security-users' have version 3 and status CURRENT
2023-11-28 20:10:11.800+0000 INFO  Performing postInitialization step for component 'security-users' with version 3 and status CURRENT
2023-11-28 20:10:12.009+0000 INFO  Bolt enabled on localhost:7687.
2023-11-28 20:10:12.659+0000 INFO  Remote interface available at http://localhost:7474/
2023-11-28 20:10:12.661+0000 INFO  id: 5A701F927DCACB5FF00DA8D78003158AF8655A9AF6C7AD010B75B4503DB89F2E
2023-11-28 20:10:12.661+0000 INFO  name: system
2023-11-28 20:10:12.661+0000 INFO  creationDate: 2023-11-28T20:10:10.991Z
2023-11-28 20:10:12.661+0000 INFO  Started.
```

The Remote Interface link, can open the Neo4j Browser. First user/pass is `neo4j:neo4j`



```
$
```

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 might require an authenticated connection

Connect URL: neo4j:// localhost:7687

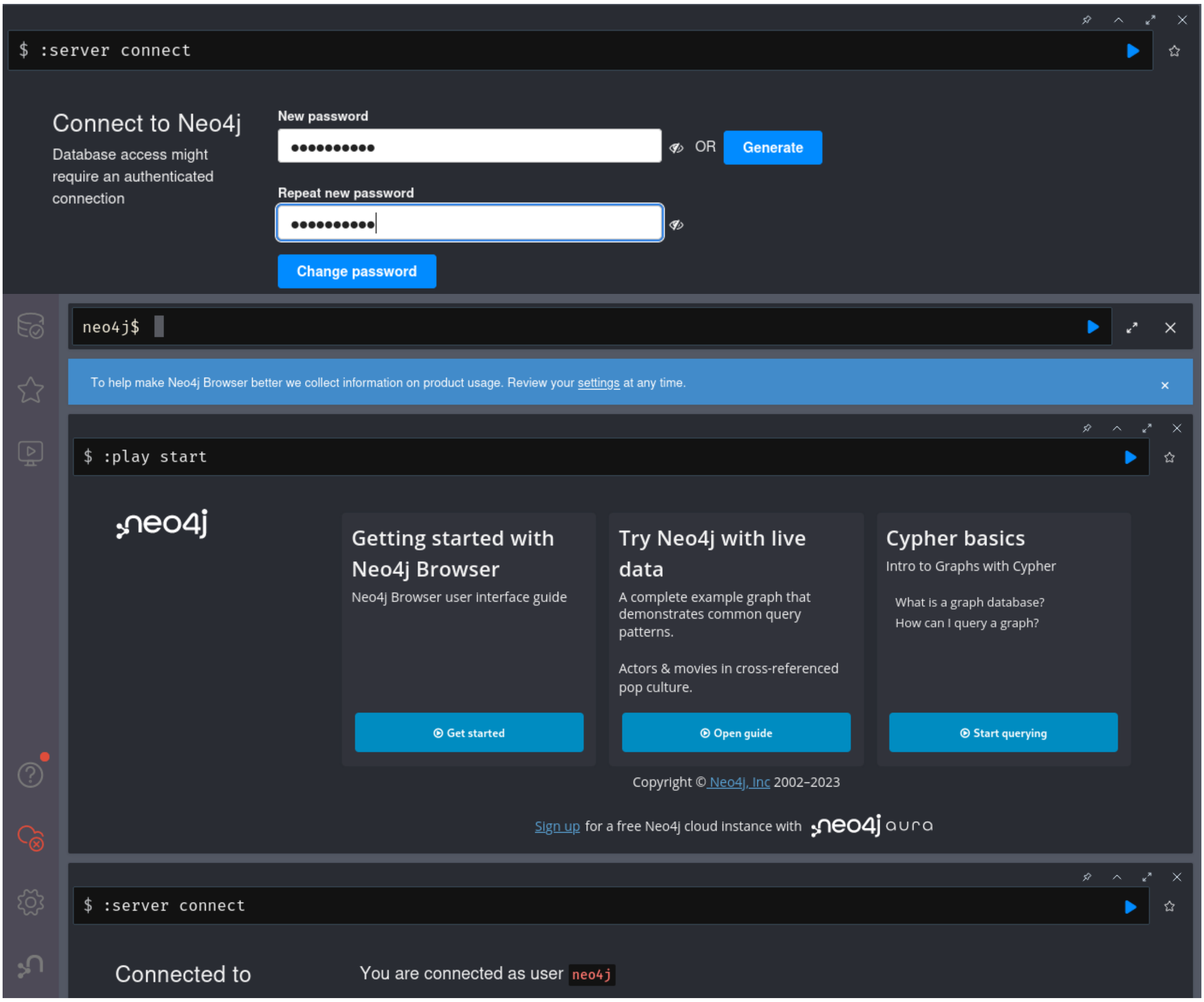
Database - leave empty for default:

Authentication type: Username / Password

Username: neo4j

Password: •••••

Change your password to what you prefer



```
$ :server connect
```

Connect to Neo4j

Database access might require an authenticated connection

New password: ••••••••••

Repeat new password: ••••••••••

```
neo4j$
```

To help make Neo4j Browser better we collect information on product usage. Review your settings at any time.

```
$ :play start
```

Getting started with Neo4j Browser

Neo4j Browser user interface guide

Try Neo4j with live data

A complete example graph that demonstrates common query patterns.

Actors & movies in cross-referenced pop culture.

Cypher basics

Intro to Graphs with Cypher

What is a graph database?
How can I query a graph?

Copyright © Neo4j, Inc 2002–2023

Sign up for a free Neo4j cloud instance with neo4j aura

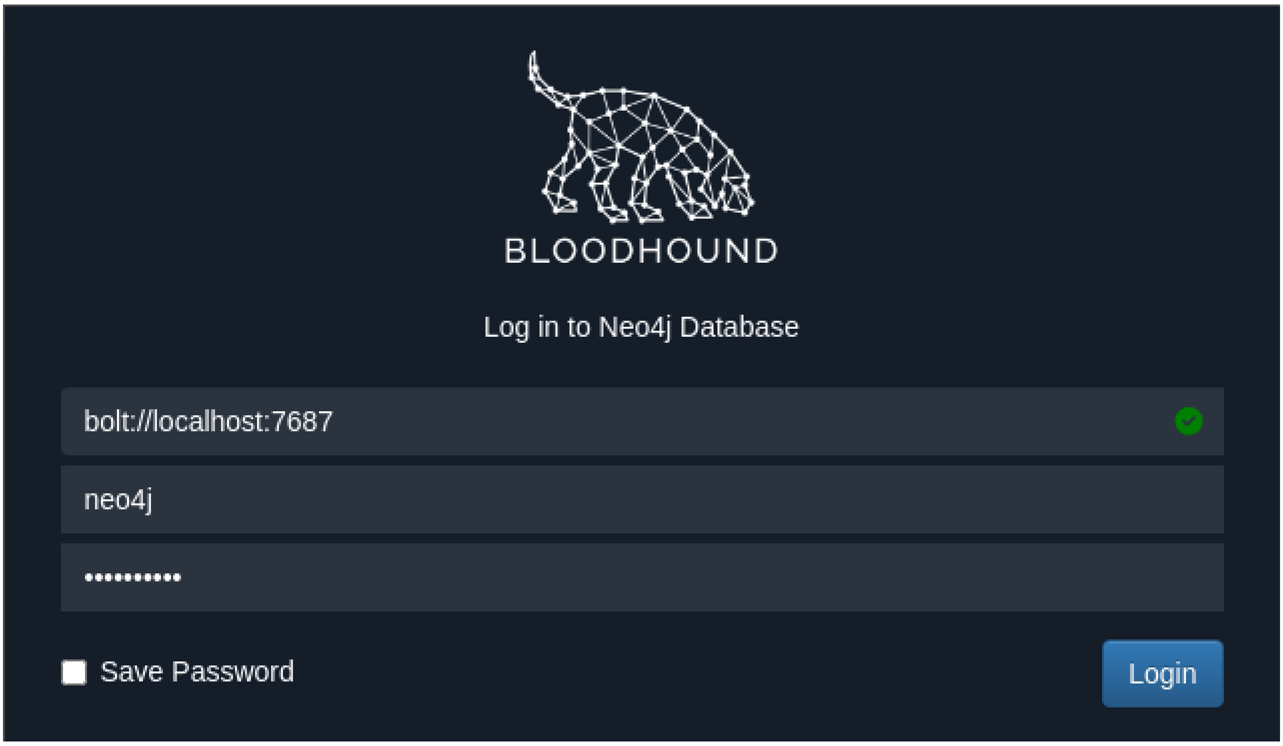
```
$ :server connect
```

Connected to

You are connected as user `neo4j`

Now run Bloodhound

```
bloodhound
```



Log in to Neo4j Database

bolt://localhost:7687

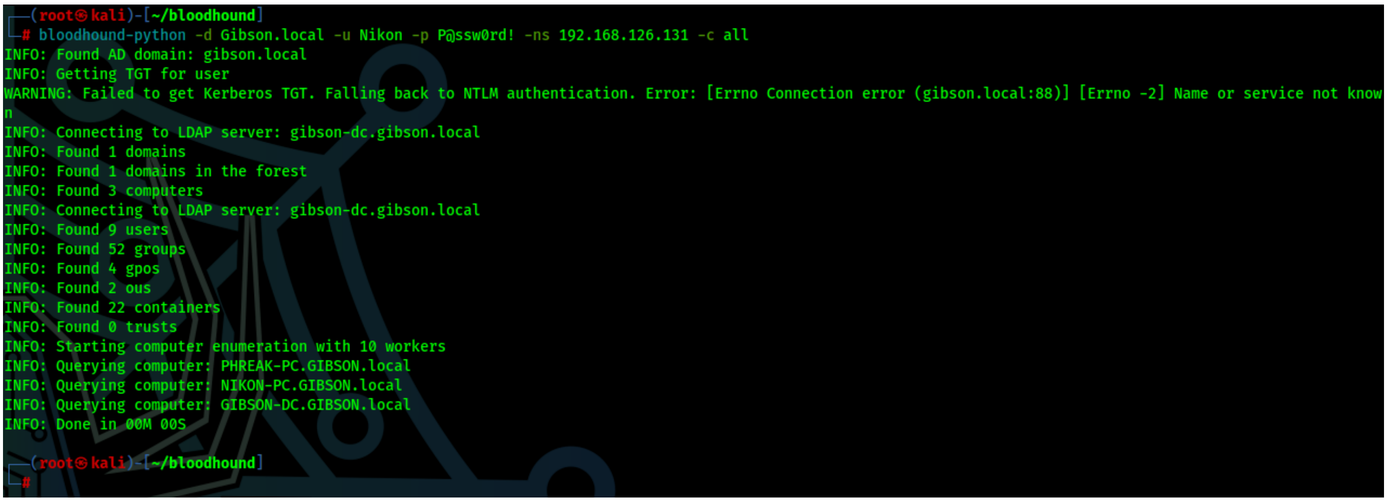
neo4j

••••••••••

Start Data Collection

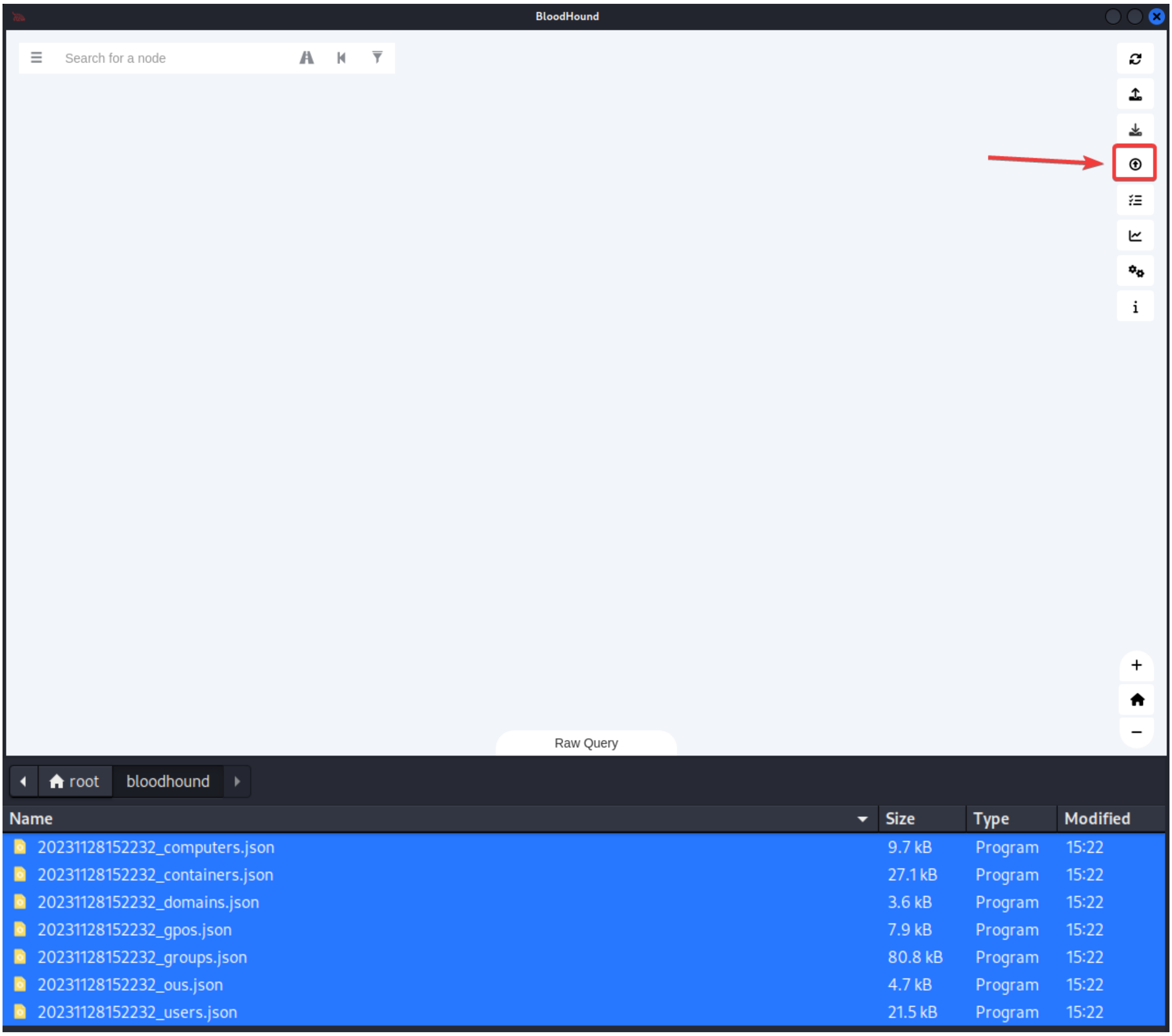
Make a Directory for the data, and start the collection

```
bloodhound-python -d domain -u user -p password -ns ip -c all
```

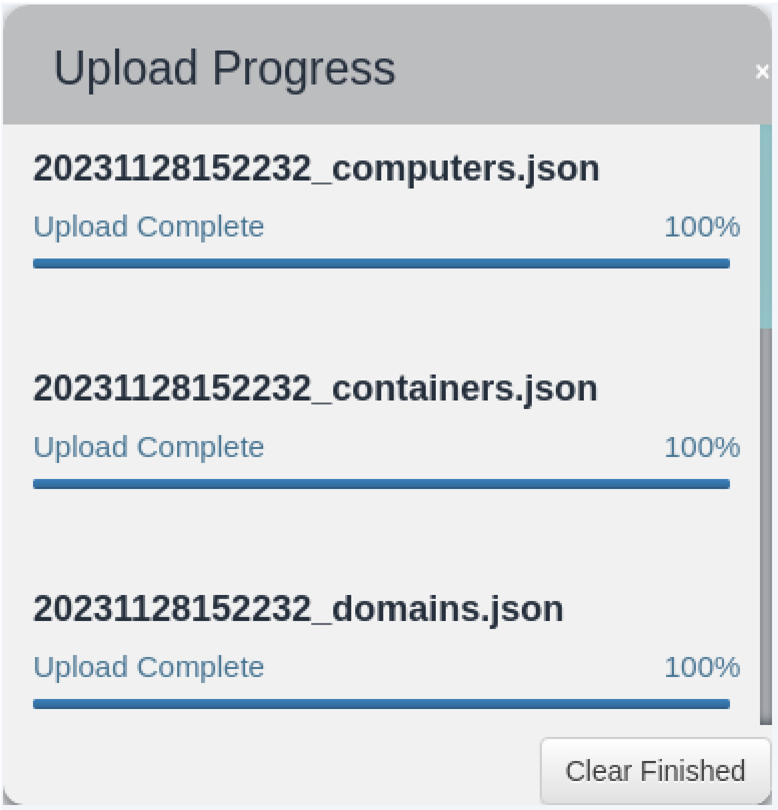


```
┌──(root㉿kali)-[~/bloodhound]
└─# bloodhound-python -d Gibson.local -u Nikon -p P@ssw0rd! -ns 192.168.126.131 -c all
INFO: Found AD domain: gibson.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (gibson.local:88)] [Errno -2] Name or service not know
n
INFO: Connecting to LDAP server: gibson-dc.gibson.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 3 computers
INFO: Connecting to LDAP server: gibson-dc.gibson.local
INFO: Found 9 users
INFO: Found 52 groups
INFO: Found 4 gpos
INFO: Found 2 ous
INFO: Found 22 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: PHREAK-PC.GIBSON.local
INFO: Querying computer: NIKON-PC.GIBSON.local
INFO: Querying computer: GIBSON-DC.GIBSON.local
INFO: Done in 00M 00S

┌──(root㉿kali)-[~/bloodhound]
└─#
```

Import the data



Name	Size	Type	Modified
20231128152232_computers.json	9.7 kB	Program	15:22
20231128152232_containers.json	27.1 kB	Program	15:22
20231128152232_domains.json	3.6 kB	Program	15:22
20231128152232_gpos.json	7.9 kB	Program	15:22
20231128152232_groups.json	80.8 kB	Program	15:22
20231128152232_ous.json	4.7 kB	Program	15:22
20231128152232_users.json	21.5 kB	Program	15:22



Upload Progress

20231128152232_computers.json

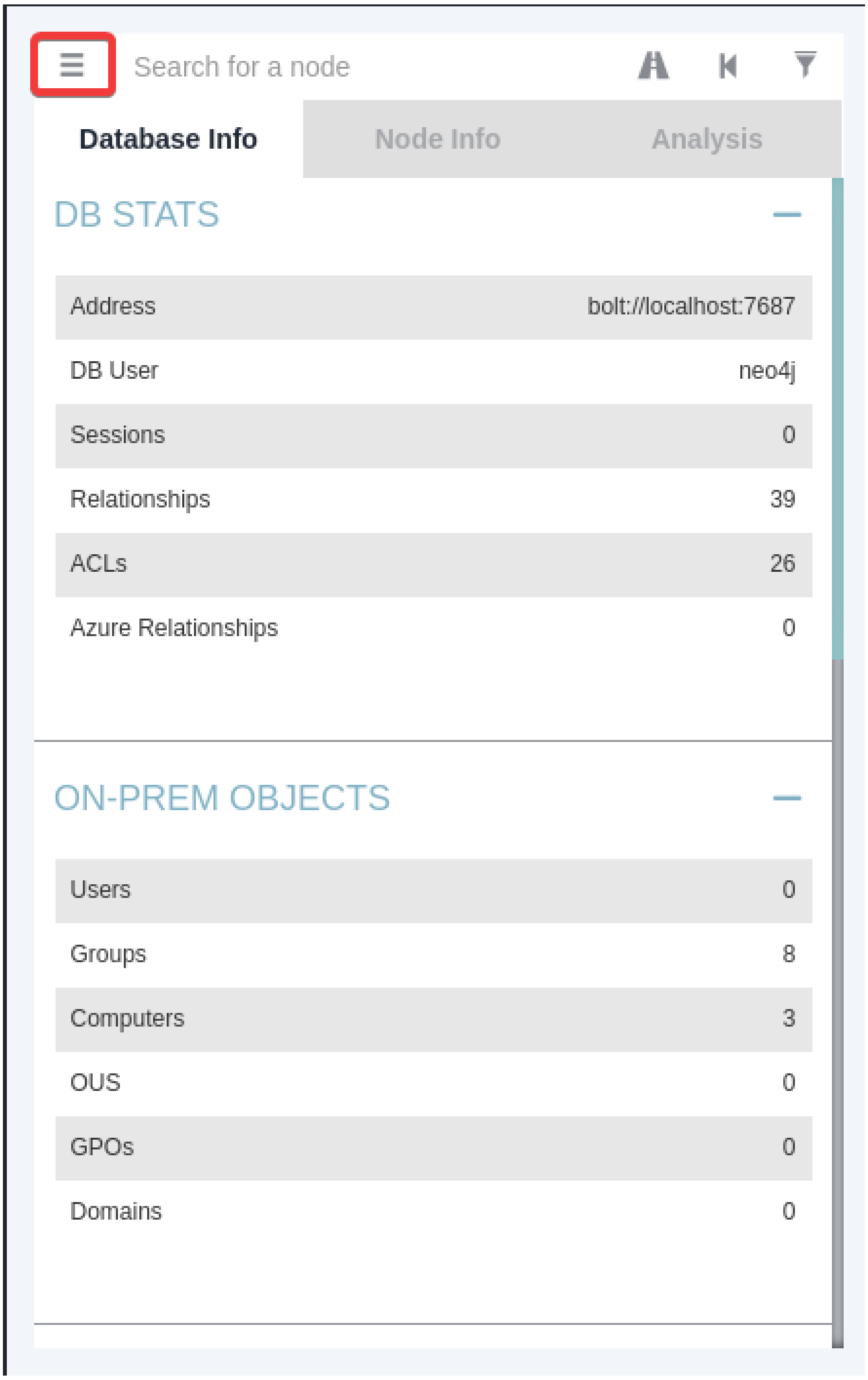
Upload Complete 100%

20231128152232_containers.json

Upload Complete 100%

20231128152232_domains.json

Upload Complete 100%



DB STATS

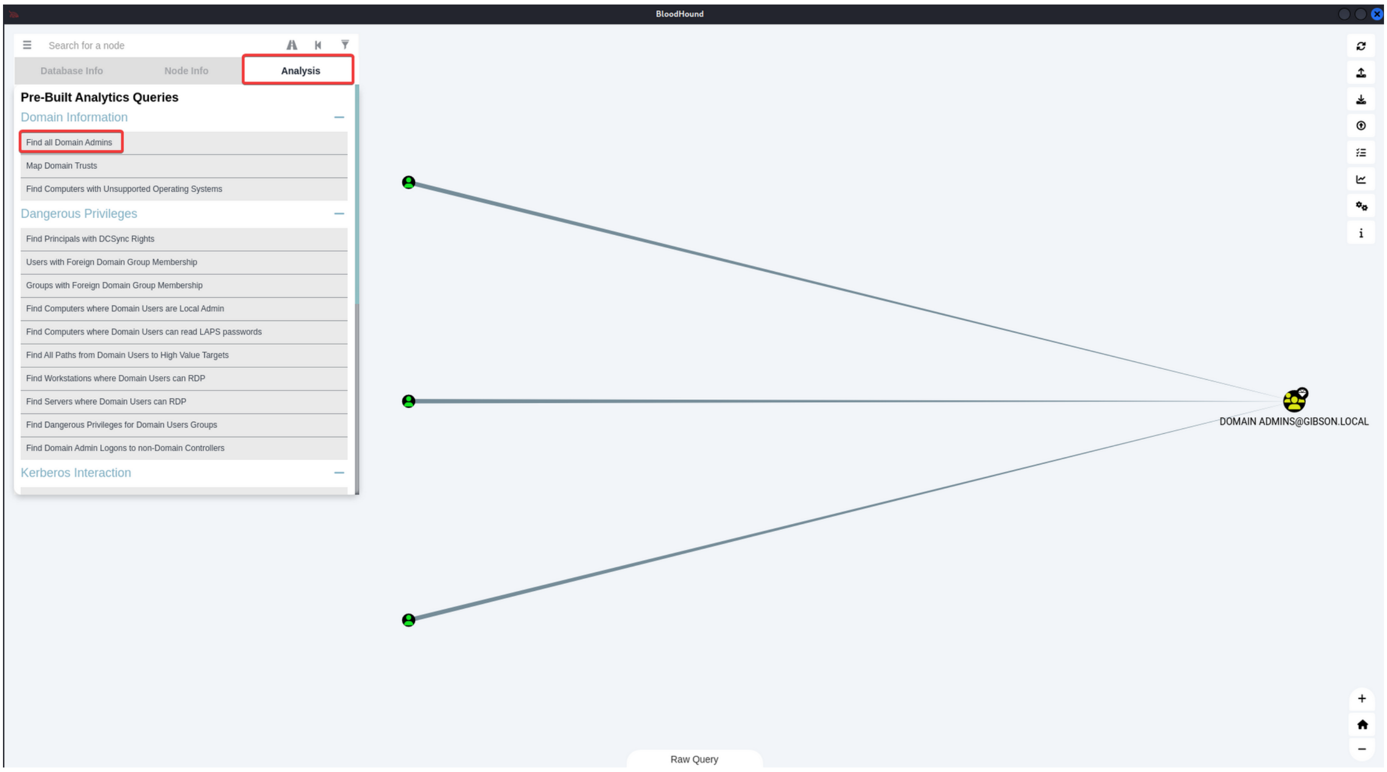
Address	bolt://localhost:7687
DB User	neo4j
Sessions	0
Relationships	39
ACLs	26
Azure Relationships	0

ON-PREM OBJECTS

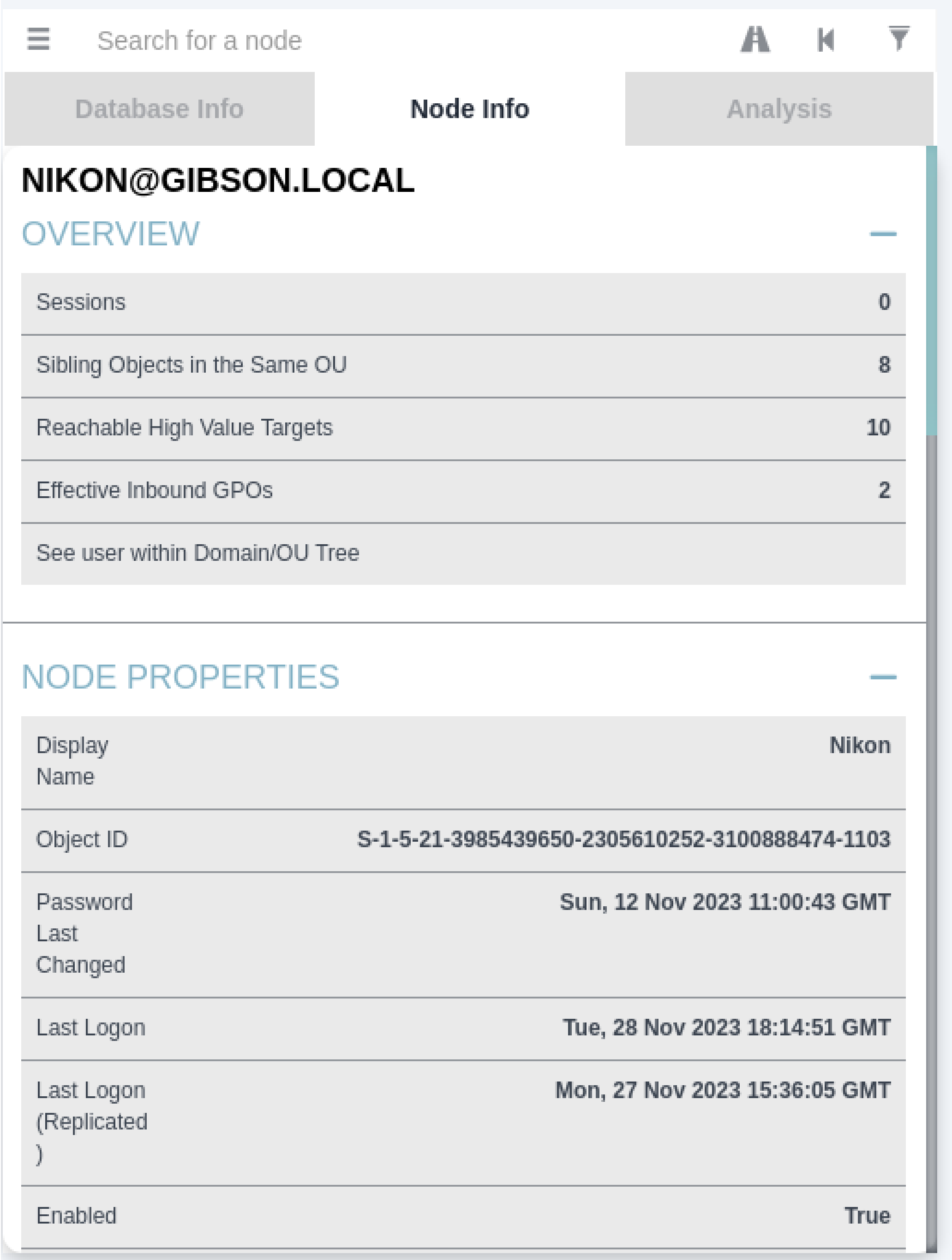
Users	0
Groups	8
Computers	3
OUS	0
GPOs	0
Domains	0

Analysis

There's a lot of Analysis tools, selecting users/machines/etc will open additional info



BloodHound
Search for a node
Database Info
Node Info
Analysis
Pre-Built Analytics Queries
Domain Information
Find all Domain Admins
Map Domain Trusts
Find Computers with Unsupported Operating Systems
Dangerous Privileges
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Find Computers where Domain Users are Local Admin
Find Computers where Domain Users can read LAPS passwords
Find All Paths from Domain Users to High Value Targets
Find Workstations where Domain Users can RDP
Find Servers where Domain Users can RDP
Find Dangerous Privileges for Domain Users Groups
Find Domain Admin Logons to non-Domain Controllers
Kerberos Interaction
DOMAIN ADMINS@GIBSON.LOCAL
Raw Query



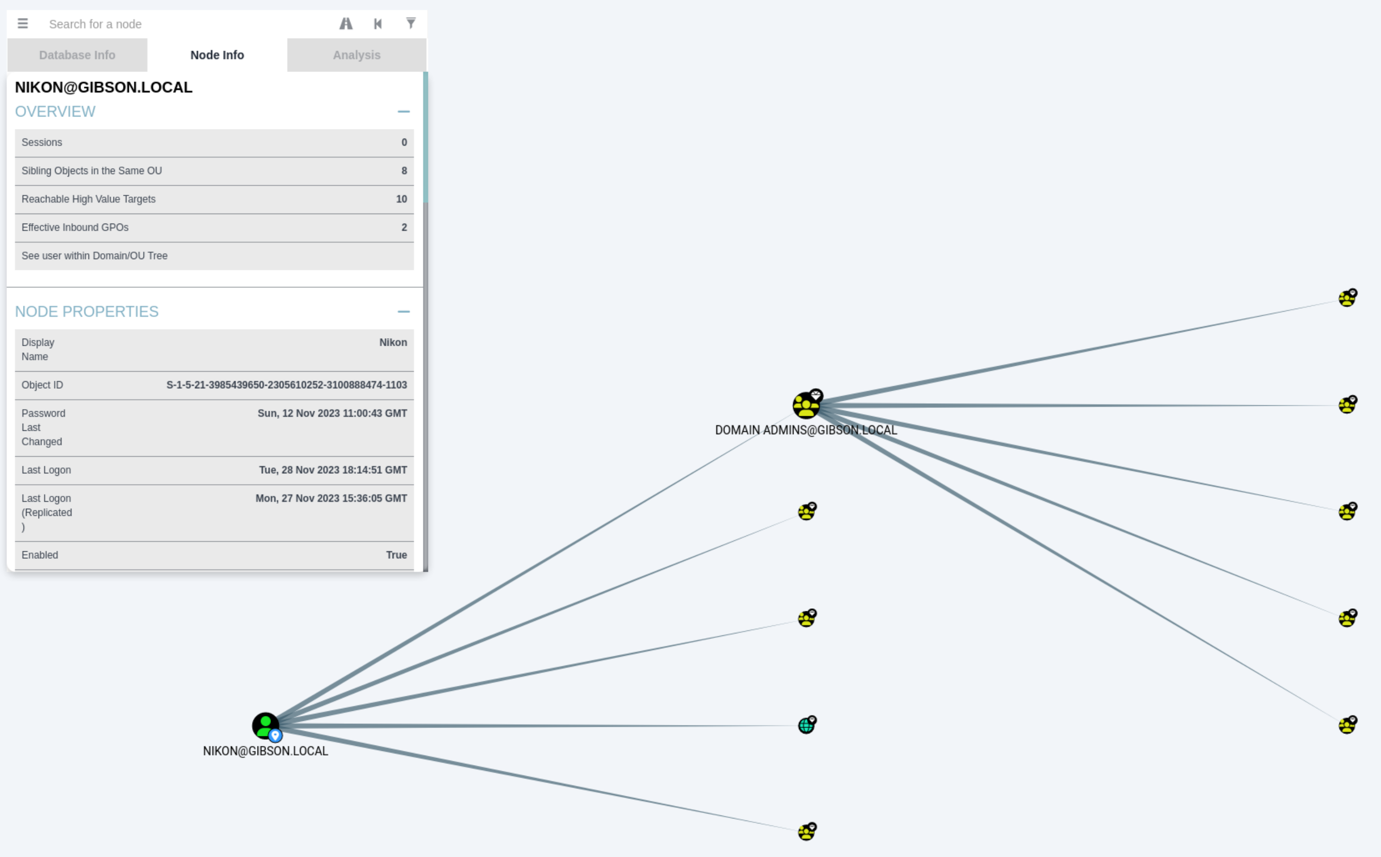
NIKON@GIBSON.LOCAL

OVERVIEW

Sessions	**0**
Sibling Objects in the Same OU	**8**
Reachable High Value Targets	**10**
Effective Inbound GPOs	**2**
See user within Domain/OU Tree	

NODE PROPERTIES

Display Name	**Nikon**
Object ID	**S-1-5-21-3985439650-2305610252-3100888474-1103**
Password Last Changed	**Sun, 12 Nov 2023 11:00:43 GMT**
Last Logon	**Tue, 28 Nov 2023 18:14:51 GMT**
Last Logon (Replicated)	**Mon, 27 Nov 2023 15:36:05 GMT**
Enabled	**True**



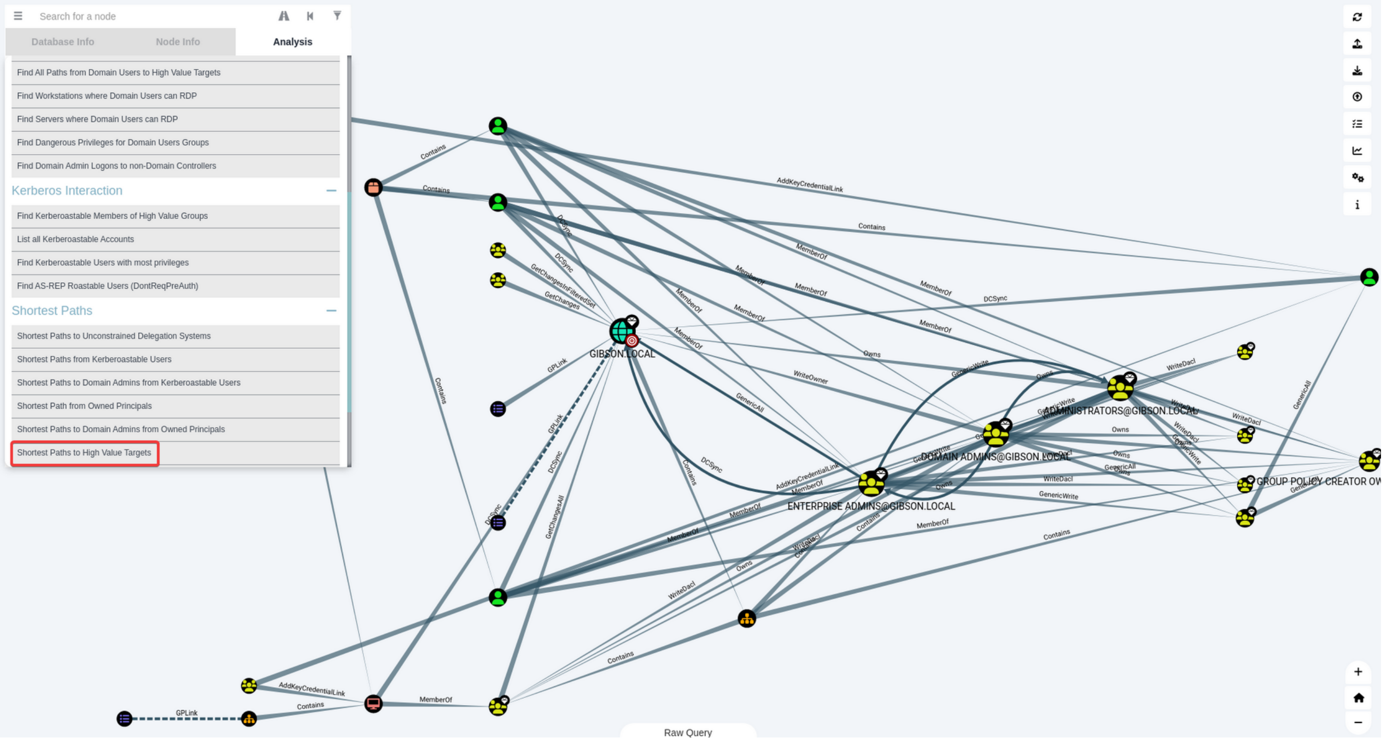
NIKON@GIBSON.LOCAL

OVERVIEW

Sessions	0
Sibling Objects in the Same OU	8
Reachable High Value Targets	10
Effective Inbound GPOs	2
See user within Domain/OU Tree	

NODE PROPERTIES

Display Name	Nikon
Object ID	S-1-5-21-3985439650-2305610252-3100888474-1103
Password Last Changed	Sun, 12 Nov 2023 11:00:43 GMT
Last Logon	Tue, 28 Nov 2023 18:14:51 GMT
Last Logon (Replicated)	Mon, 27 Nov 2023 15:36:05 GMT
Enabled	True



Find All Paths from Domain Users to High Value Targets
Find Workstations where Domain Users can RDP
Find Servers where Domain Users can RDP
Find Dangerous Privileges for Domain Users Groups
Find Domain Admin Logons to non-Domain Controllers

Kerberos Interaction

Find Kerberoastable Members of High Value Groups
List all Kerberoastable Accounts
Find Kerberoastable Users with most privileges
Find AS-REP Roastable Users (DontReqPreAuth)

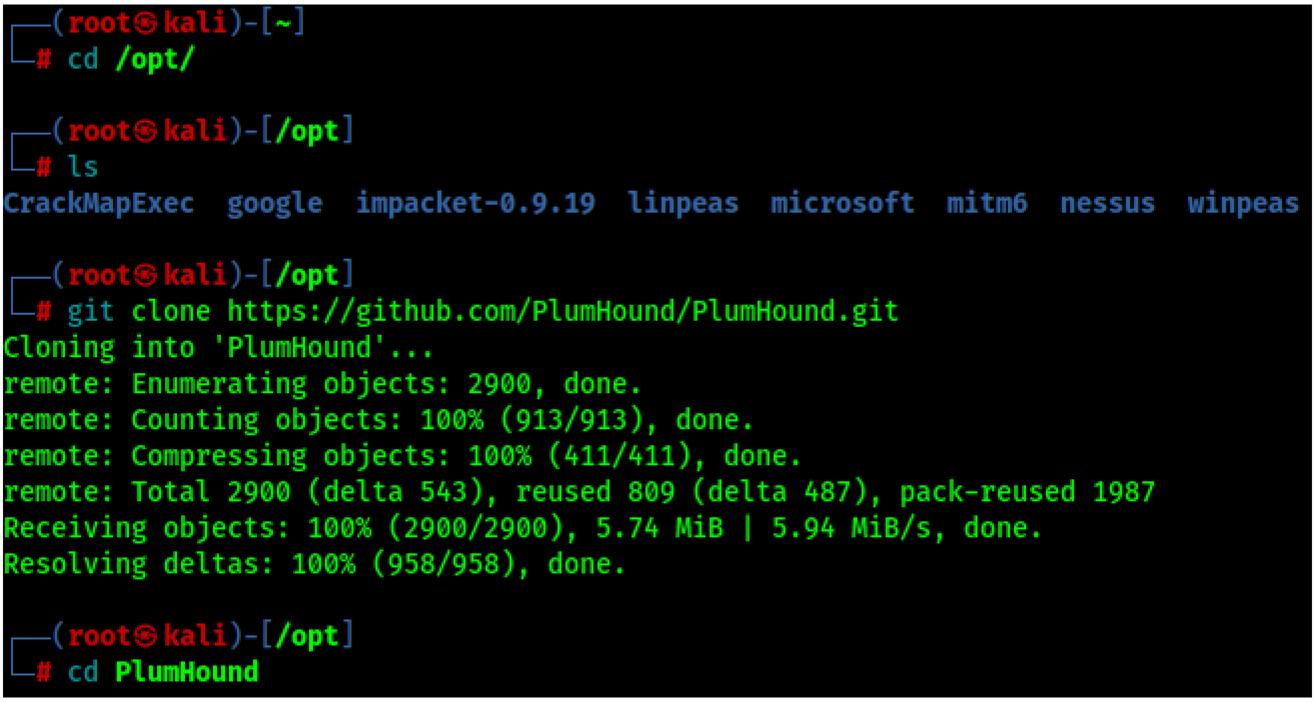
Shortest Paths

Shortest Paths to Unconstrained Delegation Systems
Shortest Paths from Kerberoastable Users
Shortest Paths to Domain Admins from Kerberoastable Users
Shortest Path from Owned Principals
Shortest Paths to Domain Admins from Owned Principals
Shortest Paths to High Value Targets

Domain Enumeration with Plumhound

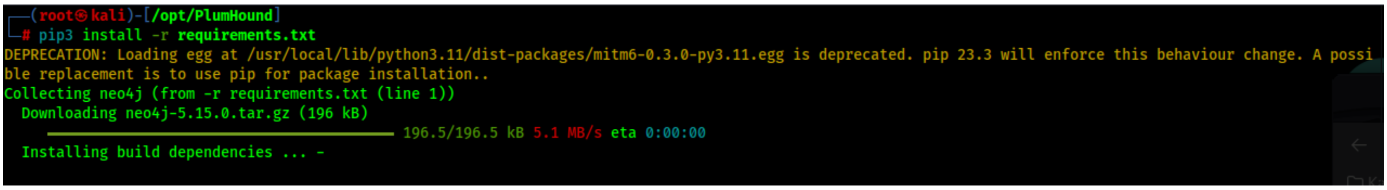
Plumhound - Bloodhound for Blue and Purple Teams

Obtain



```
┌──(root㉿kali)-[~]
└─# cd /opt/

┌──(root㉿kali)-[/opt]
└─# ls
CrackMapExec  google  impacket-0.9.19  linpeas  microsoft  mitm6  nessus  winpeas

┌──(root㉿kali)-[/opt]
└─# git clone https://github.com/PlumHound/PlumHound.git
Cloning into 'PlumHound'...
remote: Enumerating objects: 2900, done.
remote: Counting objects: 100% (913/913), done.
remote: Compressing objects: 100% (411/411), done.
remote: Total 2900 (delta 543), reused 809 (delta 487), pack-reused 1987
Receiving objects: 100% (2900/2900), 5.74 MiB | 5.94 MiB/s, done.
Resolving deltas: 100% (958/958), done.

┌──(root㉿kali)-[/opt]
└─# cd PlumHound
```

Install



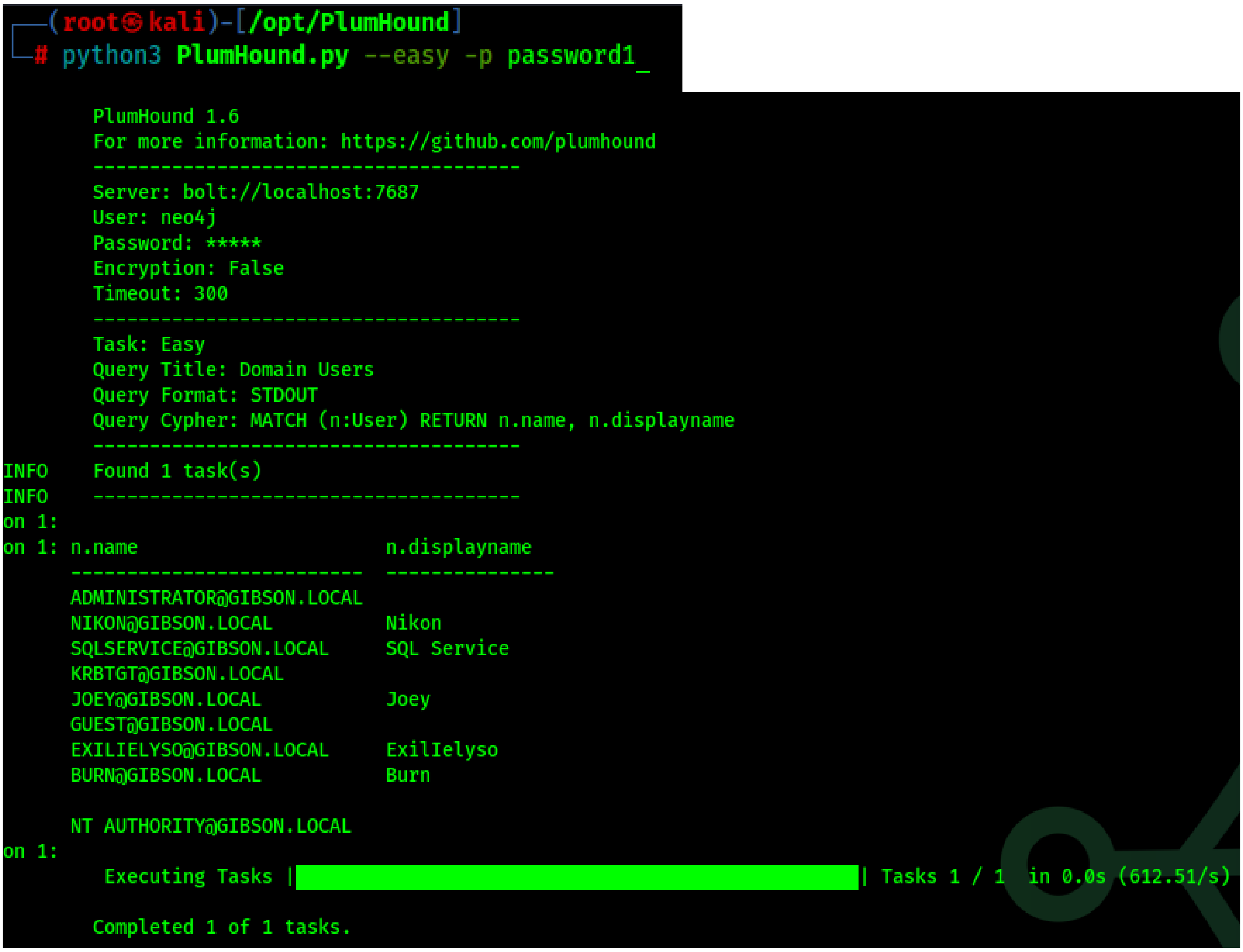
```
┌──(root㉿kali)-[/opt/PlumHound]
└─# pip3 install -r requirements.txt
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/mitm6-0.3.0-py3.11.egg is deprecated. pip 23.3 will enforce this behaviour change. A possi
ble replacement is to use pip for package installation..
Collecting neo4j (from -r requirements.txt (line 1))
  Downloading neo4j-5.15.0.tar.gz (196 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 196.5/196.5 kB 5.1 MB/s eta 0:00:00
  Installing build dependencies ... -
```

Using

Have Bloodhound Up and Running

Test to make sure Plumhound works

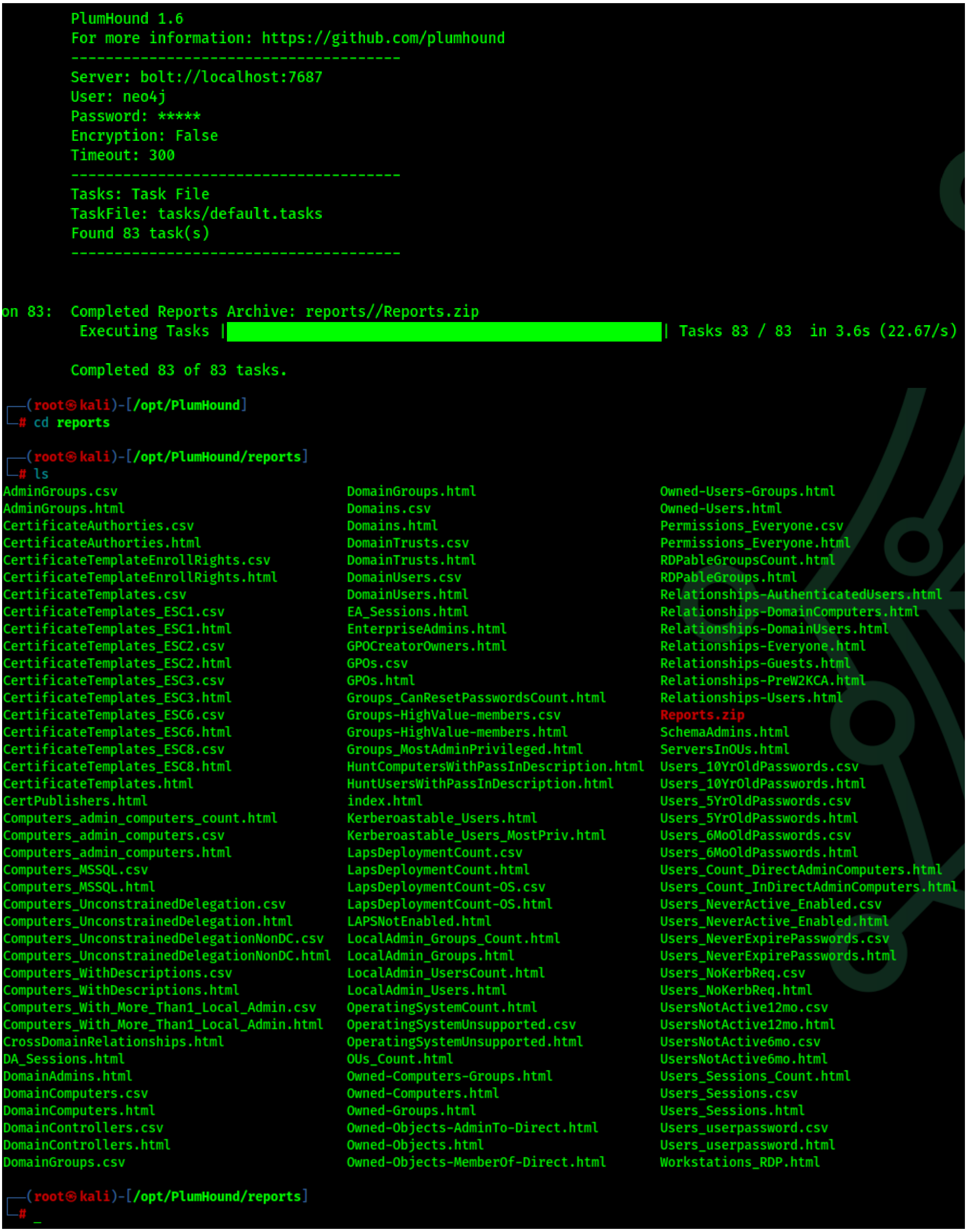
```
python3 PlumHound.py --easy -p password
```



```
┌──(root㉿kali)-[/opt/PlumHound]
└─# python3 PlumHound.py --easy -p password1_

        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:
on 1: n.name                     n.displayname
      --------------------------  ---------------
      ADMINISTRATOR@GIBSON.LOCAL
      NIKON@GIBSON.LOCAL          Nikon
      SQLSERVICE@GIBSON.LOCAL     SQL Service
      KRBTGT@GIBSON.LOCAL
      JOEY@GIBSON.LOCAL           Joey
      GUEST@GIBSON.LOCAL
      EXILIELYSO@GIBSON.LOCAL     ExilIelyso
      BURN@GIBSON.LOCAL           Burn

      NT AUTHORITY@GIBSON.LOCAL
on 1:
         Executing Tasks |██████████████████████████████████████████████████| Tasks 1 / 1  in 0.0s (612.51/s)

        Completed 1 of 1 tasks.
```

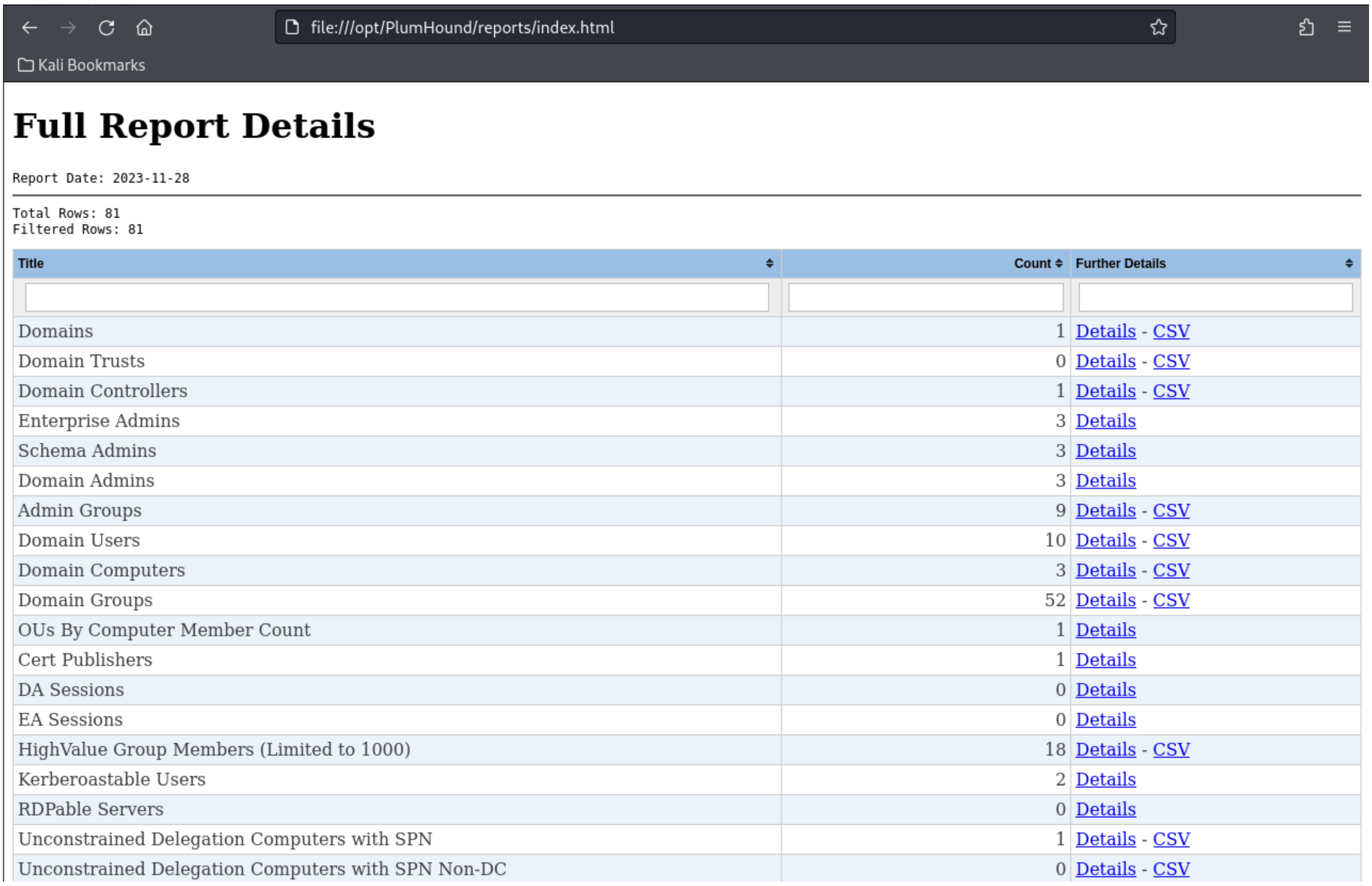
Running it with defaults

```
python3 PlumHound.py -x tasks/default.tasks -p password1
```



```
        PlumHound 1.6
        For more information: https://github.com/plumhound
        --------------------------------------
        Server: bolt://localhost:7687
        User: neo4j
        Password: *****
        Encryption: False
        Timeout: 300
        --------------------------------------
        Tasks: Task File
        TaskFile: tasks/default.tasks
        Found 83 task(s)
        --------------------------------------


on 83:  Completed Reports Archive: reports//Reports.zip
         Executing Tasks |█████████████████████████████████████████████████████████| Tasks 83 / 83  in 3.6s (22.67/s)

        Completed 83 of 83 tasks.

┌──(root㉿kali)-[/opt/PlumHound]
└─# cd reports

┌──(root㉿kali)-[/opt/PlumHound/reports]
└─# ls
AdminGroups.csv                              DomainGroups.html                        Owned-Users-Groups.html
AdminGroups.html                             Domains.csv                              Owned-Users.html
CertificateAuthorties.csv                    Domains.html                             Permissions_Everyone.csv
CertificateAuthorties.html                   DomainTrusts.csv                         Permissions_Everyone.html
CertificateTemplateEnrollRights.csv          DomainTrusts.html                        RDPableGroupsCount.html
CertificateTemplateEnrollRights.html         DomainUsers.csv                          RDPableGroups.html
CertificateTemplates.csv                     DomainUsers.html                         Relationships-AuthenticatedUsers.html
CertificateTemplates_ESC1.csv                EA_Sessions.html                         Relationships-DomainComputers.html
CertificateTemplates_ESC1.html               EnterpriseAdmins.html                    Relationships-DomainUsers.html
CertificateTemplates_ESC2.csv                GPOCreatorOwners.html                    Relationships-Everyone.html
CertificateTemplates_ESC2.html               GPOs.csv                                 Relationships-Guests.html
CertificateTemplates_ESC3.csv                GPOs.html                                Relationships-PreW2KCA.html
CertificateTemplates_ESC3.html               Groups_CanResetPasswordsCount.html       Relationships-Users.html
CertificateTemplates_ESC6.csv                Groups-HighValue-members.csv             Reports.zip
CertificateTemplates_ESC6.html               Groups-HighValue-members.html            SchemaAdmins.html
CertificateTemplates_ESC8.csv                Groups_MostAdminPrivileged.html          ServersInOUs.html
CertificateTemplates_ESC8.html               HuntComputersWithPassInDescription.html  Users_10YrOldPasswords.csv
CertificateTemplates.html                    HuntUsersWithPassInDescription.html      Users_10YrOldPasswords.html
CertPublishers.html                          index.html                               Users_5YrOldPasswords.csv
Computers_admin_computers_count.html         Kerberoastable_Users.html                Users_5YrOldPasswords.html
Computers_admin_computers.csv                Kerberoastable_Users_MostPriv.html       Users_6MoOldPasswords.csv
Computers_admin_computers.html               LapsDeploymentCount.csv                  Users_6MoOldPasswords.html
Computers_MSSQL.csv                          LapsDeploymentCount.html                 Users_Count_DirectAdminComputers.html
Computers_MSSQL.html                         LapsDeploymentCount-OS.csv               Users_Count_InDirectAdminComputers.html
Computers_UnconstrainedDelegation.csv        LapsDeploymentCount-OS.html              Users_NeverActive_Enabled.csv
Computers_UnconstrainedDelegation.html       LAPSNotEnabled.html                      Users_NeverActive_Enabled.html
Computers_UnconstrainedDelegationNonDC.csv   LocalAdmin_Groups_Count.html             Users_NeverExpirePasswords.csv
Computers_UnconstrainedDelegationNonDC.html  LocalAdmin_Groups.html                   Users_NeverExpirePasswords.html
Computers_WithDescriptions.csv               LocalAdmin_UsersCount.html               Users_NoKerbReq.csv
Computers_WithDescriptions.html              LocalAdmin_Users.html                    Users_NoKerbReq.html
Computers_With_More_Than1_Local_Admin.csv    OperatingSystemCount.html                UsersNotActive12mo.csv
Computers_With_More_Than1_Local_Admin.html   OperatingSystemUnsupported.csv           UsersNotActive12mo.html
CrossDomainRelationships.html                OperatingSystemUnsupported.html          UsersNotActive6mo.csv
DA_Sessions.html                             OUs_Count.html                           UsersNotActive6mo.html
DomainAdmins.html                            Owned-Computers-Groups.html              Users_Sessions_Count.html
DomainComputers.csv                          Owned-Computers.html                     Users_Sessions.csv
DomainComputers.html                         Owned-Groups.html                        Users_Sessions.html
DomainControllers.csv                        Owned-Objects-AdminTo-Direct.html        Users_userpassword.csv
DomainControllers.html                       Owned-Objects.html                       Users_userpassword.html
DomainGroups.csv                             Owned-Objects-MemberOf-Direct.html       Workstations_RDP.html

┌──(root㉿kali)-[/opt/PlumHound/reports]
└─# _
```

Open the index.html file to see everything



Full Report Details

```
Report Date: 2023-11-28

Total Rows: 81
Filtered Rows: 81
```

Title	Count	Further Details
Domains	1	Details - CSV
Domain Trusts	0	Details - CSV
Domain Controllers	1	Details - CSV
Enterprise Admins	3	Details
Schema Admins	3	Details
Domain Admins	3	Details
Admin Groups	9	Details - CSV
Domain Users	10	Details - CSV
Domain Computers	3	Details - CSV
Domain Groups	52	Details - CSV
OUs By Computer Member Count	1	Details
Cert Publishers	1	Details
DA Sessions	0	Details
EA Sessions	0	Details
HighValue Group Members (Limited to 1000)	18	Details - CSV
Kerberoastable Users	2	Details
RDPable Servers	0	Details
Unconstrained Delegation Computers with SPN	1	Details - CSV
Unconstrained Delegation Computers with SPN Non-DC	0	Details - CSV

Domain Enumeration with PingCastle

PingCastle - Is Free but has better options when paid. Just followed video for this.