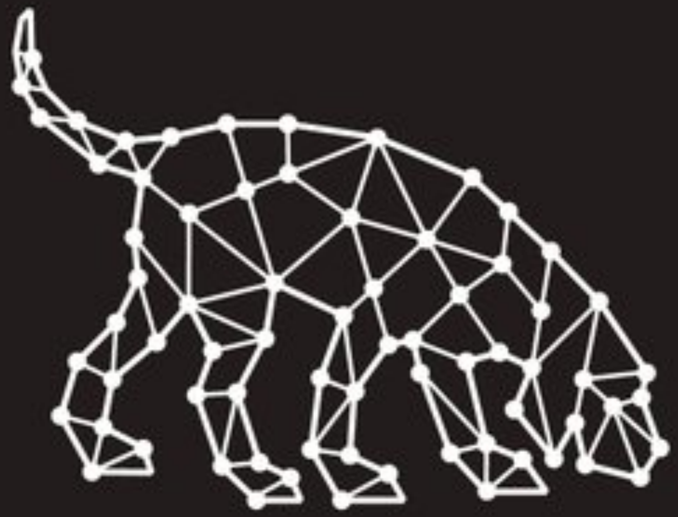
Bloodhound 2.0 Walkthrough

By : Pralhad Chaskar (@c0d3xpl0it)

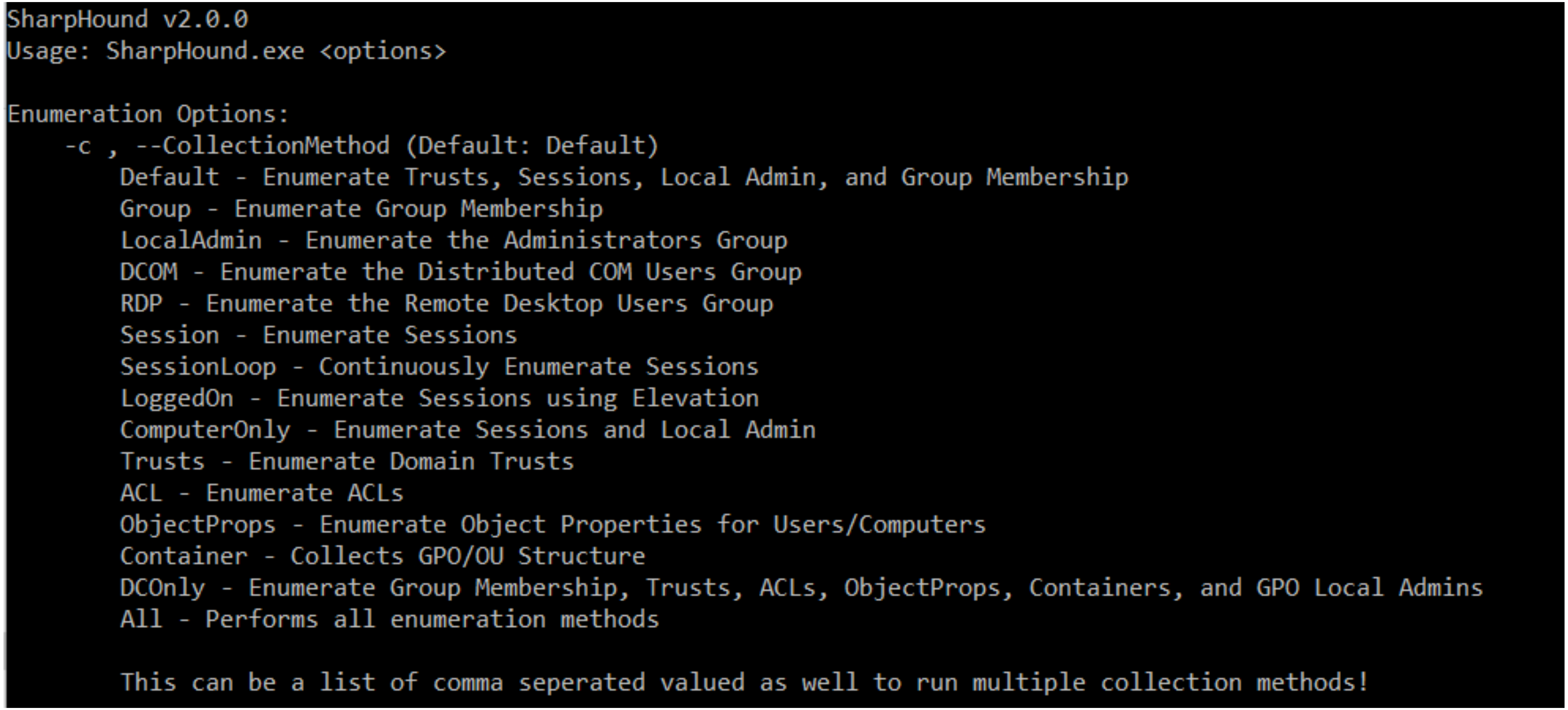


(a:**Attackers**)-[:**Think_in**]->(g:**Graphs**)

What is Bloodhound

- Active Directory privileges, rights and trust relationships mapping tool
- Makes finding attack paths super easy
- Uses a Neo4j Graph Database
- Data collection using C# binary called SharpHound
- Bloodhound UI is built with Linkurious, compiled into an Electron app
- Free and open source software

Sharphound Collection Methods

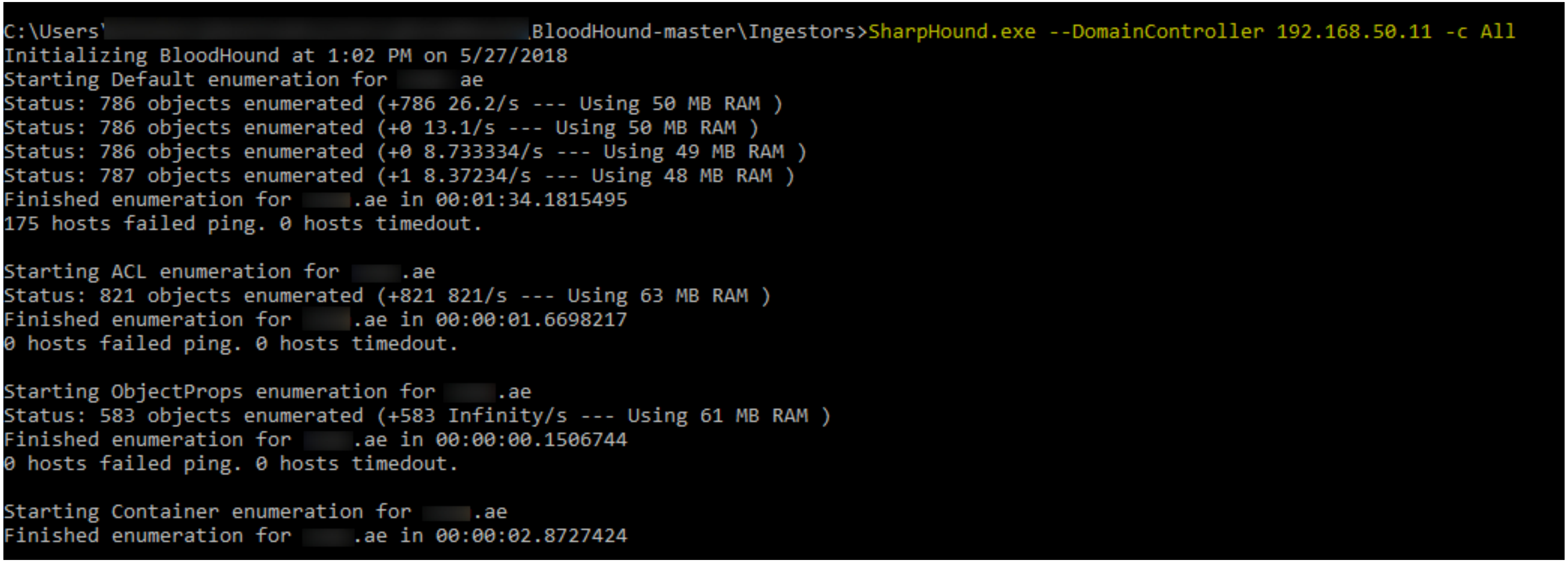


```
SharpHound v2.0.0
Usage: SharpHound.exe <options>

Enumeration Options:
    -c , --CollectionMethod (Default: Default)
        Default - Enumerate Trusts, Sessions, Local Admin, and Group Membership
        Group - Enumerate Group Membership
        LocalAdmin - Enumerate the Administrators Group
        DCOM - Enumerate the Distributed COM Users Group
        RDP - Enumerate the Remote Desktop Users Group
        Session - Enumerate Sessions
        SessionLoop - Continuously Enumerate Sessions
        LoggedOn - Enumerate Sessions using Elevation
        ComputerOnly - Enumerate Sessions and Local Admin
        Trusts - Enumerate Domain Trusts
        ACL - Enumerate ACLs
        ObjectProps - Enumerate Object Properties for Users/Computers
        Container - Collects GPO/OU Structure
        DCOnly - Enumerate Group Membership, Trusts, ACLs, ObjectProps, Containers, and GPO Local Admins
        All - Performs all enumeration methods

        This can be a list of comma seperated valued as well to run multiple collection methods!
```

Running from Domain Joined machine



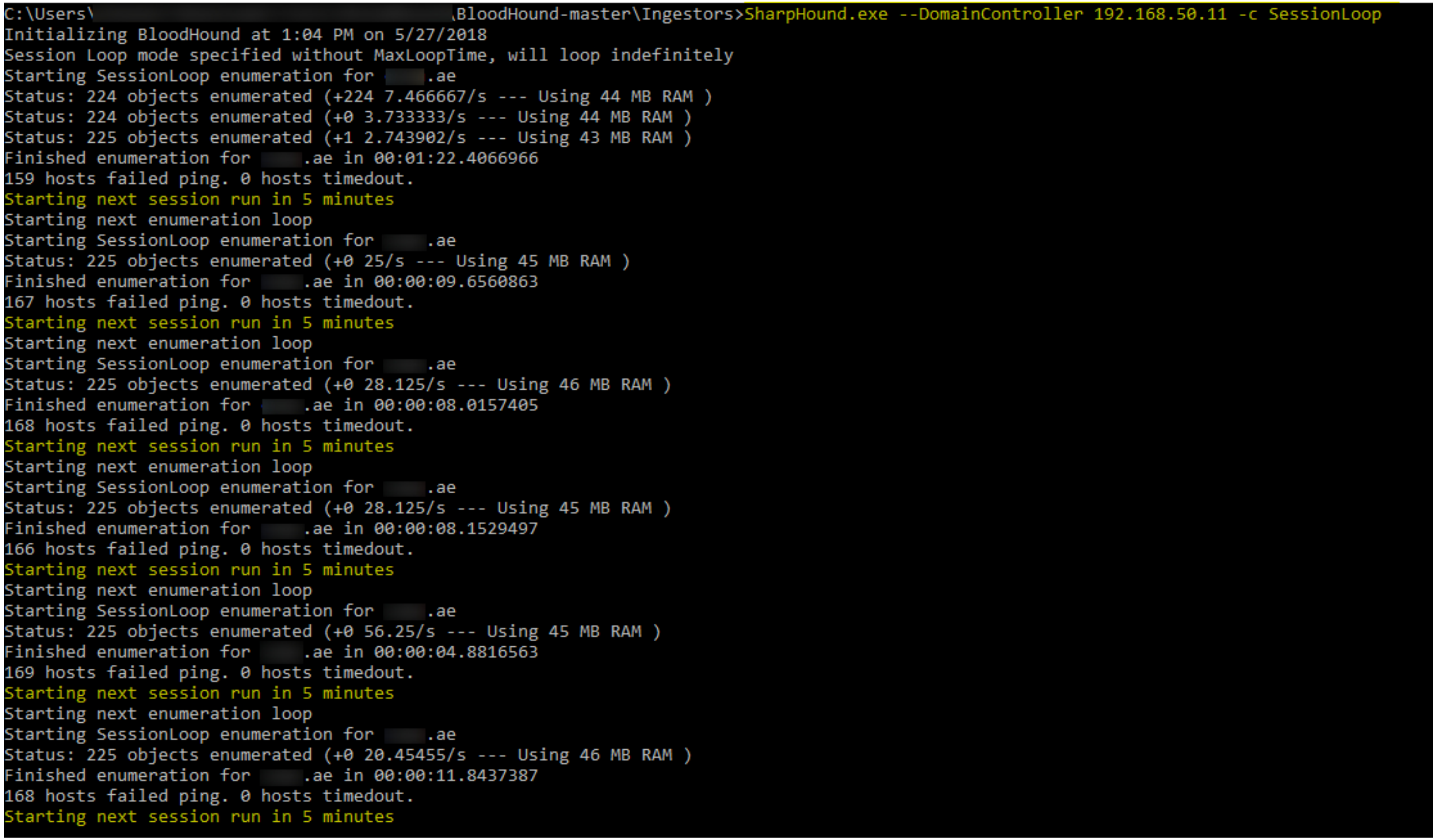
```
C:\Users\[redacted]BloodHound-master\Ingestors>SharpHound.exe --DomainController 192.168.50.11 -c All
Initializing BloodHound at 1:02 PM on 5/27/2018
Starting Default enumeration for [redacted]ae
Status: 786 objects enumerated (+786 26.2/s --- Using 50 MB RAM )
Status: 786 objects enumerated (+0 13.1/s --- Using 50 MB RAM )
Status: 786 objects enumerated (+0 8.733334/s --- Using 49 MB RAM )
Status: 787 objects enumerated (+1 8.37234/s --- Using 48 MB RAM )
Finished enumeration for [redacted].ae in 00:01:34.1815495
175 hosts failed ping. 0 hosts timedout.

Starting ACL enumeration for [redacted].ae
Status: 821 objects enumerated (+821 821/s --- Using 63 MB RAM )
Finished enumeration for [redacted].ae in 00:00:01.6698217
0 hosts failed ping. 0 hosts timedout.

Starting ObjectProps enumeration for [redacted].ae
Status: 583 objects enumerated (+583 Infinity/s --- Using 61 MB RAM )
Finished enumeration for [redacted].ae in 00:00:00.1506744
0 hosts failed ping. 0 hosts timedout.

Starting Container enumeration for [redacted].ae
Finished enumeration for [redacted].ae in 00:00:02.8727424
```

More Sessions for more paths



```
C:\Users\[redacted]\BloodHound-master\Ingestors>SharpHound.exe --DomainController 192.168.50.11 -c SessionLoop
Initializing BloodHound at 1:04 PM on 5/27/2018
Session Loop mode specified without MaxLoopTime, will loop indefinitely
Starting SessionLoop enumeration for [redacted].ae
Status: 224 objects enumerated (+224 7.466667/s --- Using 44 MB RAM )
Status: 224 objects enumerated (+0 3.733333/s --- Using 44 MB RAM )
Status: 225 objects enumerated (+1 2.743902/s --- Using 43 MB RAM )
Finished enumeration for [redacted].ae in 00:01:22.4066966
159 hosts failed ping. 0 hosts timedout.
Starting next session run in 5 minutes
Starting next enumeration loop
Starting SessionLoop enumeration for [redacted].ae
Status: 225 objects enumerated (+0 25/s --- Using 45 MB RAM )
Finished enumeration for [redacted].ae in 00:00:09.6560863
167 hosts failed ping. 0 hosts timedout.
Starting next session run in 5 minutes
Starting next enumeration loop
Starting SessionLoop enumeration for [redacted].ae
Status: 225 objects enumerated (+0 28.125/s --- Using 46 MB RAM )
Finished enumeration for [redacted].ae in 00:00:08.0157405
168 hosts failed ping. 0 hosts timedout.
Starting next session run in 5 minutes
Starting next enumeration loop
Starting SessionLoop enumeration for [redacted].ae
Status: 225 objects enumerated (+0 28.125/s --- Using 45 MB RAM )
Finished enumeration for [redacted].ae in 00:00:08.1529497
166 hosts failed ping. 0 hosts timedout.
Starting next session run in 5 minutes
Starting next enumeration loop
Starting SessionLoop enumeration for [redacted].ae
Status: 225 objects enumerated (+0 56.25/s --- Using 45 MB RAM )
Finished enumeration for [redacted].ae in 00:00:04.8816563
169 hosts failed ping. 0 hosts timedout.
Starting next session run in 5 minutes
Starting next enumeration loop
Starting SessionLoop enumeration for [redacted].ae
Status: 225 objects enumerated (+0 20.45455/s --- Using 46 MB RAM )
Finished enumeration for [redacted].ae in 00:00:11.8437387
168 hosts failed ping. 0 hosts timedout.
Starting next session run in 5 minutes
```

New feature in 2.0

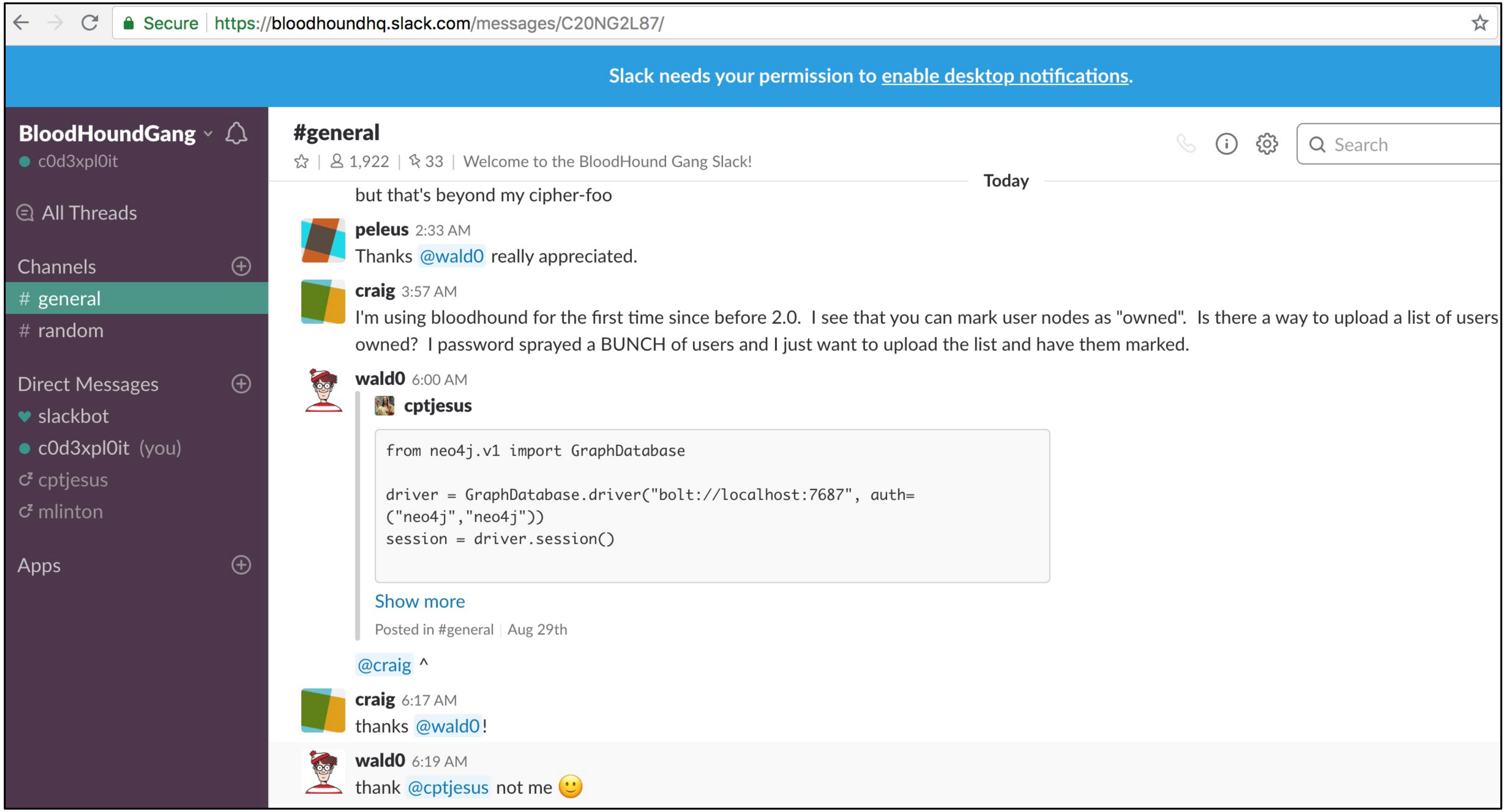
- CanRDP, ExecuteDCOM, ReadLAPSPassword, AllowedToDelegate
- JSON Output (instead of CSV)
- Edge Filtering
- Graph Editing from the UI
- Owned Value Properties
- High Value Properties
- Edge Abuse Help
- Dark Mode

Is it Pentesters Tool or Blue Team Tool ??

Detecting Bloodhound/ Hardening Infra

- Net Cease - Hardening Net Session Enumeration
- SAMRi10 - Hardening SAM Remote Access in Windows 10/Server 2016
- Using Netflow or other tools
- Using DejaVU
- ………or detect the system which makes tons of LDAP queries to DC

Slack channel for queries/new features/etc



Slack needs your permission to enable desktop notifications.

#general

☆ | 1,922 | 33 | Welcome to the BloodHound Gang Slack!

Today

but that's beyond my cipher-foo

peleus 2:33 AM

Thanks @wald0 really appreciated.

craig 3:57 AM

I'm using bloodhound for the first time since before 2.0. I see that you can mark user nodes as "owned". Is there a way to upload a list of users owned? I password sprayed a BUNCH of users and I just want to upload the list and have them marked.

wald0 6:00 AM

cptjesus

```
from neo4j.v1 import GraphDatabase

driver = GraphDatabase.driver("bolt://localhost:7687", auth=
("neo4j","neo4j"))
session = driver.session()
```

Show more

Posted in #general | Aug 29th

@craig ^

craig 6:17 AM

thanks @wald0!

wald0 6:19 AM

thank @cptjesus not me 🙂

References

- https://blog.cptjesus.com/posts/bloodhound20
- Bloodhound: He Attac, but he also Protec (https://www.youtube.com/watch?v=hHfxZug1HHo)
- https://github.com/BloodHoundAD/BloodHound
- https://github.com/SadProcessor/Cheats/blob/master/DogWhispererV2.md
- https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon