CYPHERDOG CHEATSHEET

April 15, 2019 Hausec Infosec Leave a comment

Bloodhound is a phenominal tool that should be in every pentester's toolkit, as it literally graphs an attack plan, but that also means that it's just as useful to the blue team. When I do pentests or risk assessments and show the client Bloodhound, they're both

1. Amazed
2. Confused on how to use it

The tool in itself isn't confusing, it's just there's *so much data* and *so much* you can do, that it becomes overwhelming quickly, especially from a blue team perspective where there's all these paths leading to a domain controller. Often times, I just wanted to list only the machines that allowed Unconstrained Delegation, or just the output of the node details for all domain admins to see when their passwords were changed last. Generating these metrics was a pain, because you'd have to click on a node, screenshot, paste into report, then click on the next node and so

on. Luckily, @SadProcessor read my mind and probably other people's as well, and developed CypherDog. Instantly, this made generating statistics so much easier. You want the node details of every DA? Easy. You want to list every computer that allows Unconstrained Delegation? Done. This is all done via Powershell and it's extremely simple to use. I encourage you to watch SadProcessor's talk at Troopers on using CypherDog as it's a phenomenal talk.

With that being said, I figured I'd publish some of my favorite commands for CypherDog. This is more geared towards the blue team, but obviously that means the red team could use it too.

First, setting up CypherDog is easy. Once you have Bloodhound worked and have active data in it, download the repository for CypherDog here, then import the .ps1 file.

```
Import-Module .\CypherDog2.1.ps1
```

Stop the neo4j service

```
net stop neo4j
```

Open the neo4j config file in your neo4j directory /conf/neo4j.conf and uncomment the line that says

```
dbms.security.auth_enabled=false
```

So that it can use the DB without authentication locally.

Then start neo4j

```
net start neo4j
```

And you can now see the commands you can use with CypherDog via the command

```
BloodHound
```

Here's a few of my most used commands.

Purpose	Command
List all members of the Domain Admins group	List Member 'DOMAIN ADMINS@DOMAIN.LOCAL' | ft name,description,pwdlastset,lastlogon,serviceprincipalnames,homedirectory
List all computers that allow Unconstrained Delegation, list only the name and Object ID	Node Computer | where unconstraineddelegation -eq $true | select name,objectsid
Find all groups with 'admin' in it	NodeSearch Group admin | ft name,description
Path find from user to Domain Admins group	Path User Group BOB@DOMAIN.LOCAL 'DOMAIN

	ADMINS@DOMAIN.LOCAL’
Path find from user to computer	Path User Computer BOB@DOMAIN.LOCAL ‘EXCHANGE@DOMAIN.LOCAL’
See what groups an object is part of	Edge User USER@DOMAIN.LOCAL MemberOf Group
See what computers a user can RDP to	Edge User BOB@DOMAIN.LOCAL CanRDP Computer
See what users can RDP into a computer	EdgeR User CanRDP Computer DC01.DOMAIN.LOCAL
See what users have GenericWrite on a computer	EdgeR User GenericWrite Computer DC01.DOMAIN.LOCAL
See what users have GenericWrite into a group	EdgeR User GenericWrite Group ‘DOMAIN ADMINS@DOMAIN.LOCAL’
View all objects with SPNs	Node User | where hasspn -eq $true | ft name,serviceprincipalnames
View all high value groups and their descriptions	HighValue Group | ft name, description
View all GPOs and their path	Node GPO | ft name,gpcpath
See all OUs that allow inheritance	Node OU | where blocksinheritance -eq $false | ft name
View all user’s email addresses	Node User | ft displayname, name, email

View all 2003 machines. Replace 2003 with xp, 7, 10, 2012, etc. for that OS.	Node Computer | where operatingsystem -match 2003 | ft name,operatingsystem
View all GPOs for a domain. Press enter when PS asks for a 'key'.	NodeSearch GPO | where name -match DOMAIN | ft name,description
View if a computer with a specific OS has logged on recently (Use first four digits from toady's Unix Epoch time: http://epochconverter.com)	Node Computer | where operatingsystem -match 2008 | where lastlogontimestamp -match 1566

This list is of course not comprehensive and will be updated regularly, but these are just some of the ones I use the most. I'm open to any suggestions, feel free to message me on Twitter @haus3c

Credits:

CypherD0g – @SadProcessor

BloodHound – @SpecterOps, @CptJesus, @Wald0, & @harj0y

Be the first to like this.

« Penetration Testing Active Directory, Part II

Offensive Lateral Movement »

LEAVE A REPLY

Enter your comment here...