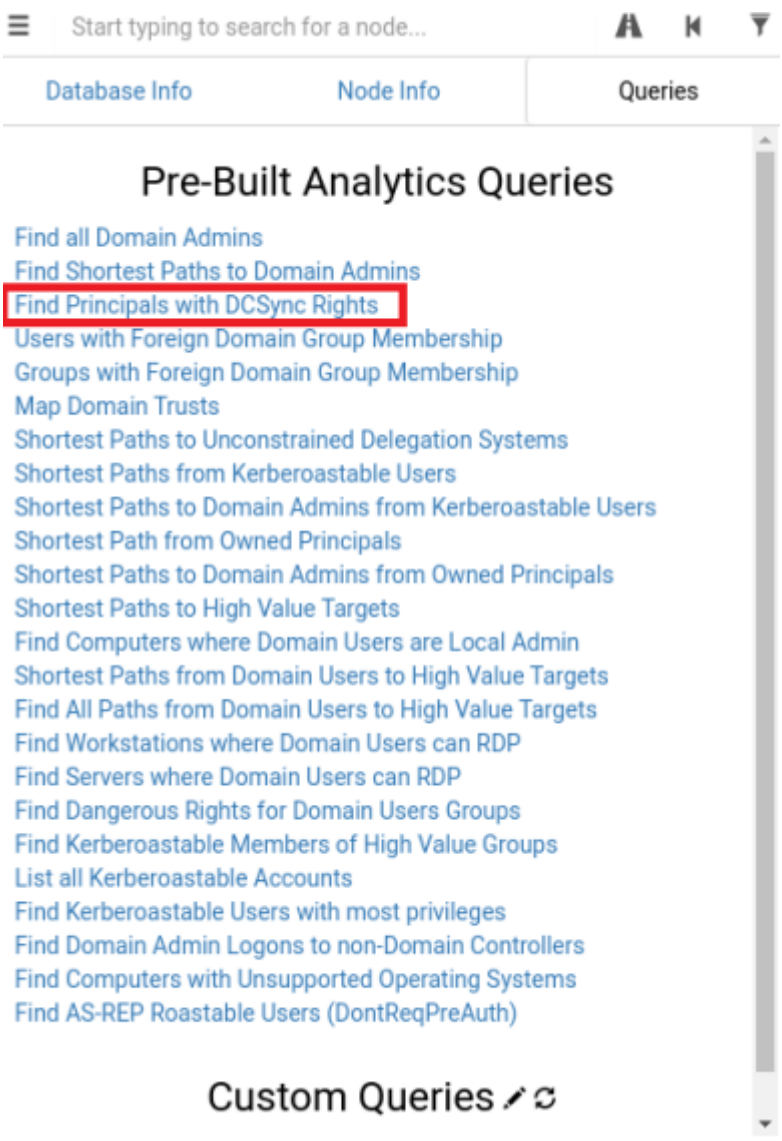
30

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.

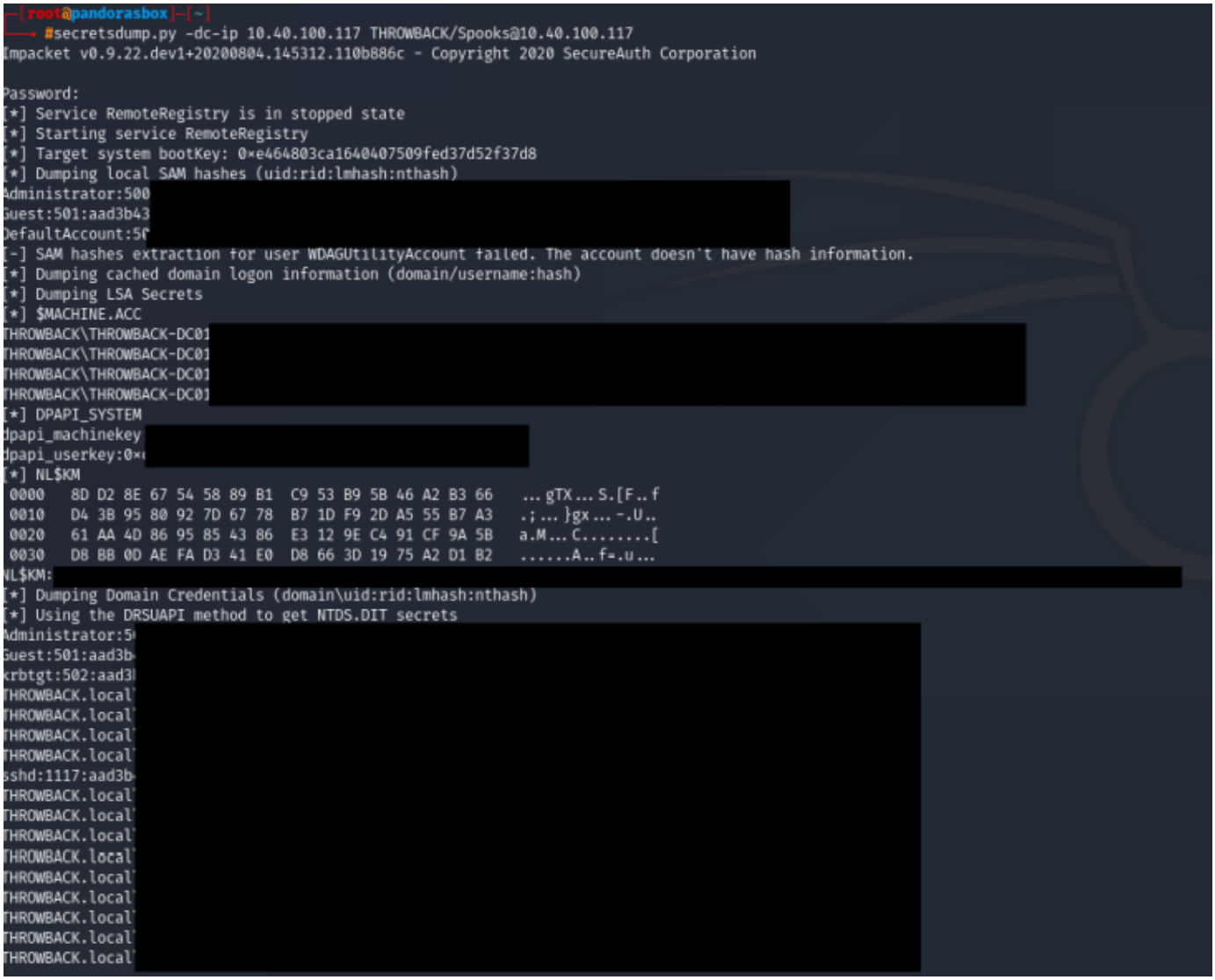


Within Bloodhound queries tab, 'Find Principals with DCSync rights'

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



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