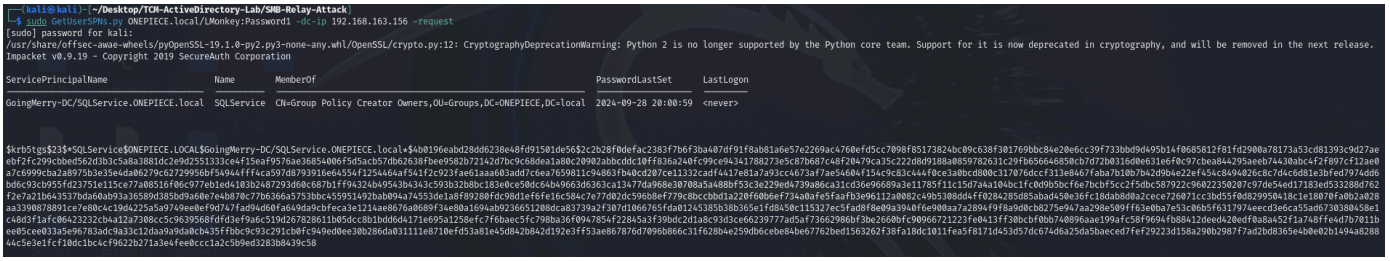
06 - Kerberoasting - Lab

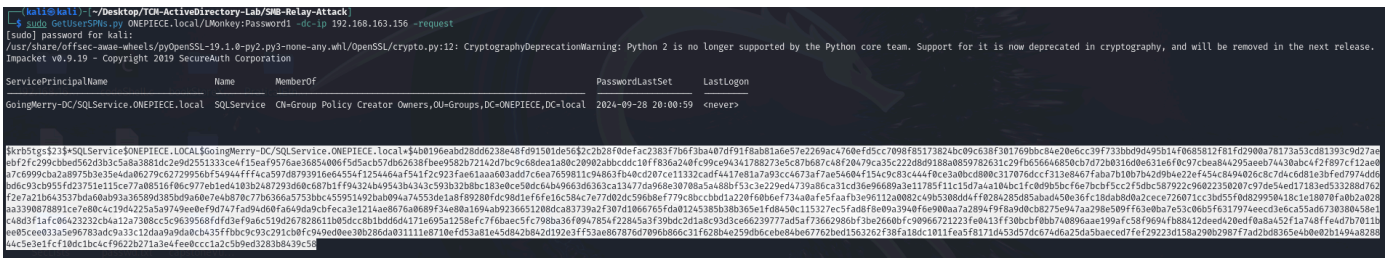
This will only require the DC machine to be on.

We just need to issue:

"#sudo GetUserSPNs.py ONEPIECE.local/LMonkey:Password1 -dc-ip 192.168.163.156 -request"



We are going to grab this long ass hash. And, I mean everything. Then, crack it.



Put in a txt file, then we can crack it.

To crack this one it is going to be code 13100 on hashcat. We need to learn how to properly look these up.

Password: MYpassword123# .

Now, we should be able to use this Domain Admin account, and own the domain. But we are not doing that yet.