black hat®
ASIA 2017

DELEGATE TO THE TOP

Abusing Kerberos for Arbitrary Impersonations and RCE

Matan Hart
@machosec
me@matanhart.com

black hat ASIA 2017

DELEGATE TO THE TOP

Abusing Kerberos for Arbitrary Impersonations and RCE

Matan Hart
@machosec
me@matanhart.com

“You can delegate authority, but you cannot delegate responsibility.”

Byron Dorgan

THE FACT

Delegation is risky

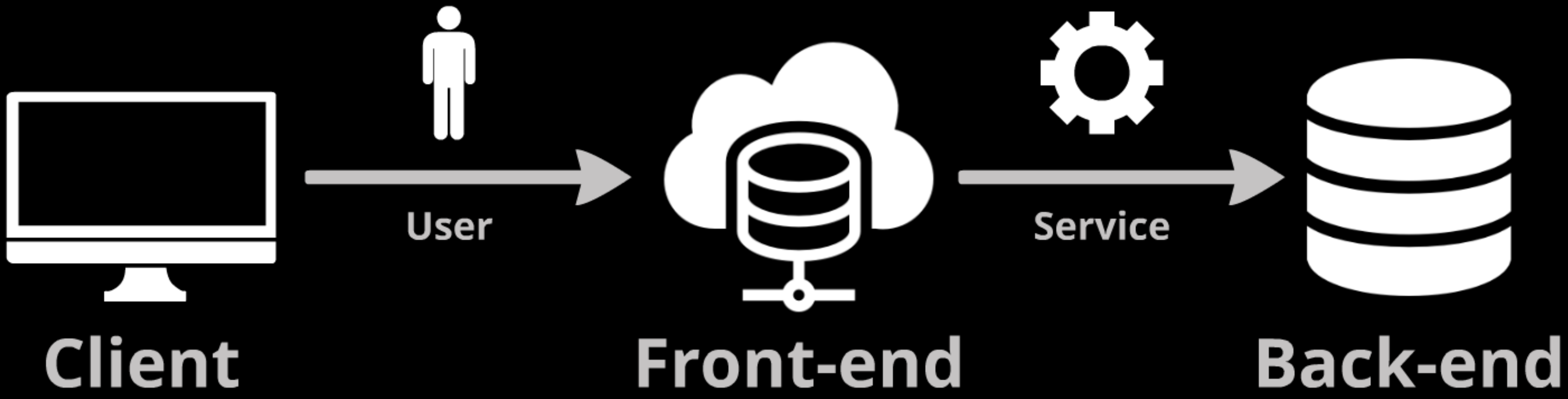
WHO AM I

- Security Researcher @ CyberArk
- IAF and IDF veteran
- Focus on Kerberos and Active Directory
- <3 PowerShell
- <333 Mr. Robot

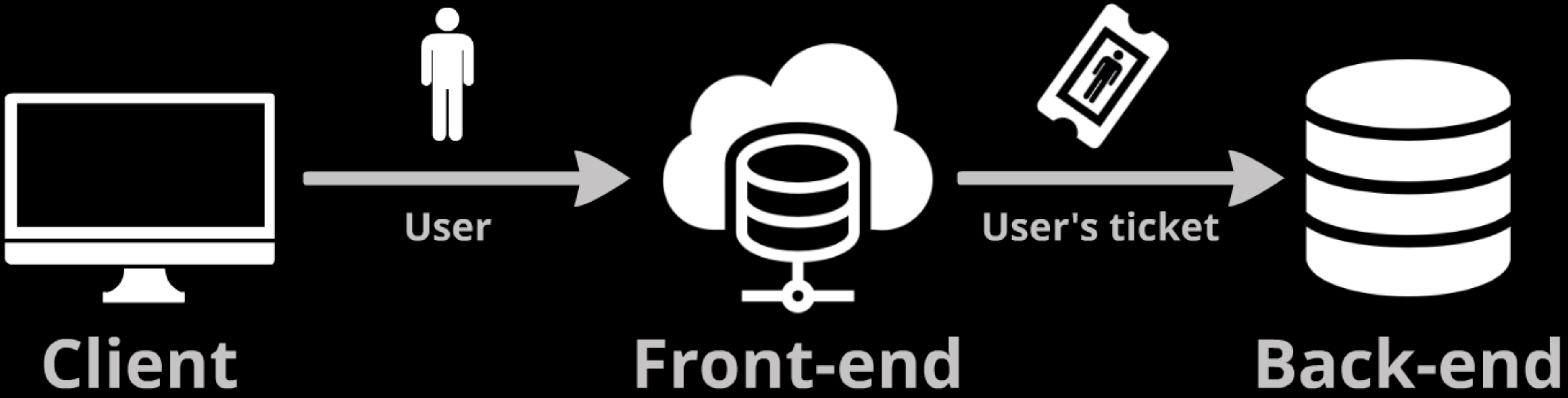
AGENDA

- Kerberos Delegation, flavors and limitations
- Service Principal Names
- Attack Surface
- Tool and Demo
- Detection and Mitigation

THE "DOUBLE-HOP" PROBLEM



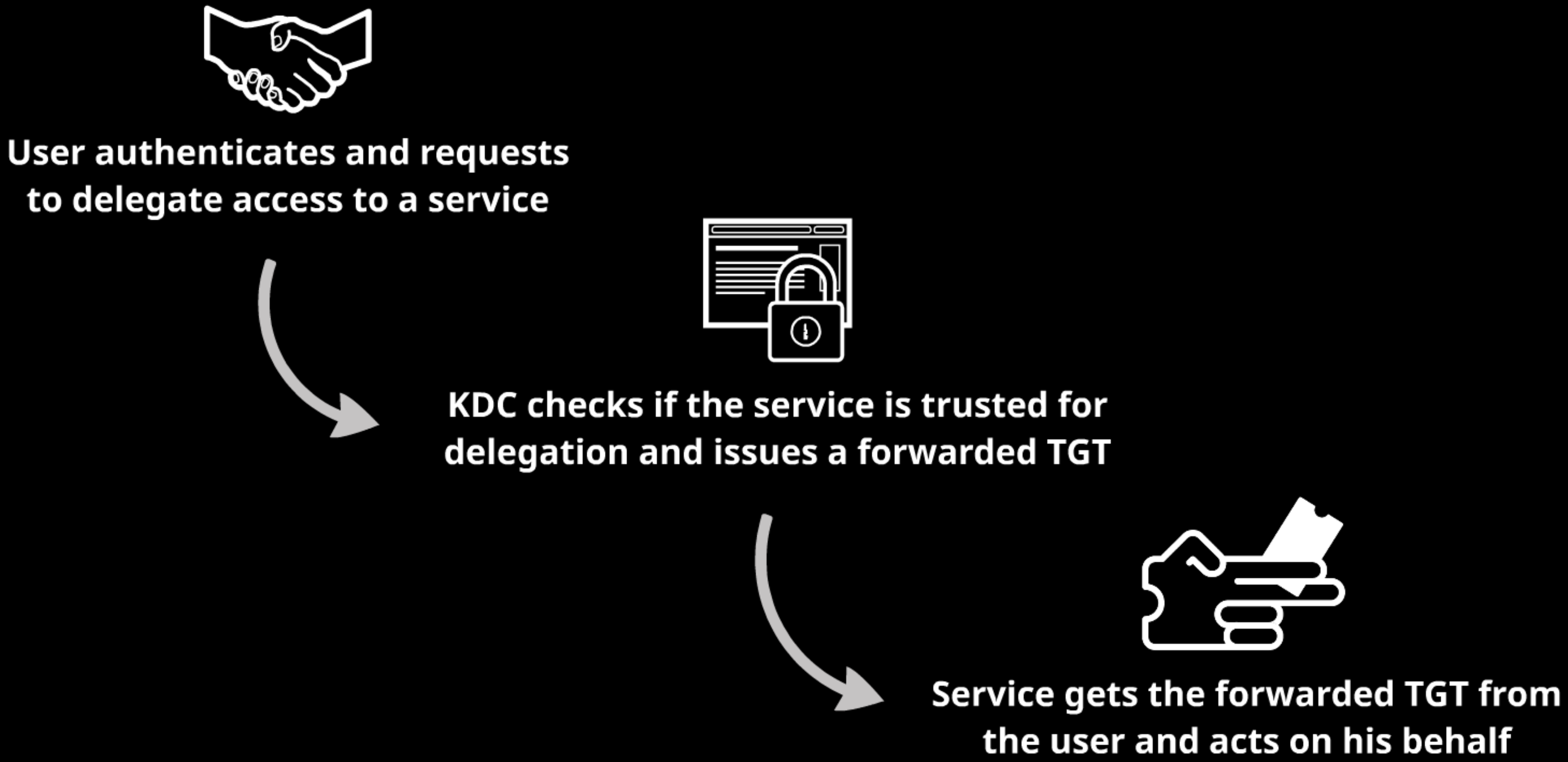
KERBEROS DELEGATION



UNCONSTRAINED DELEGATION

Full delegation by TGT forwarding

Windows 2000

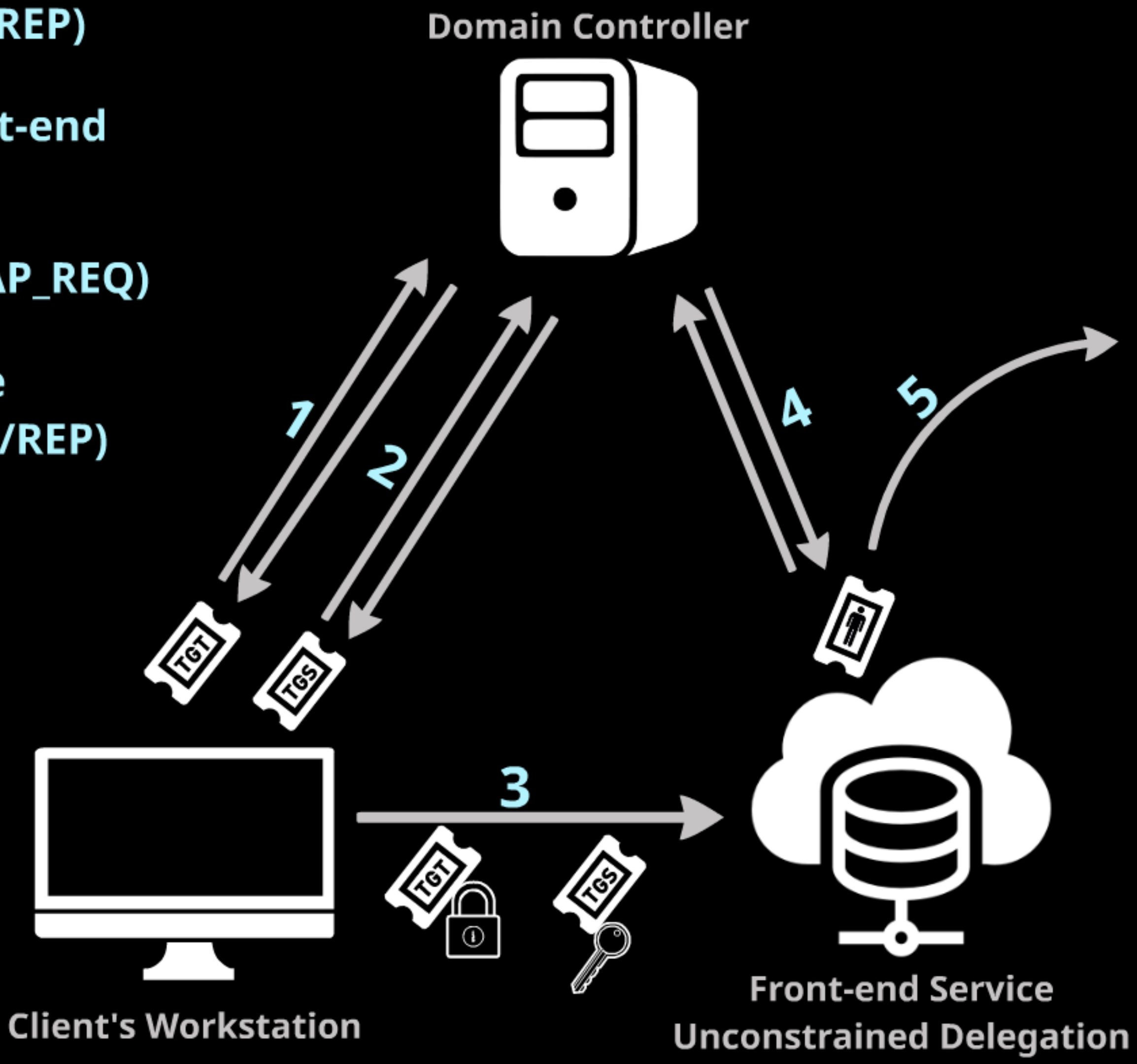


User authenticates and requests to delegate access to a service

KDC checks if the service is trusted for delegation and issues a forwarded TGT

Service gets the forwarded TGT from the user and acts on his behalf

1. User obtains a forwarded TGT (TGS_REQ/REP)
2. User obtains a service ticket for the front-end service (TGS_REQ/REP)
3. User makes a request to the front-end (AP_REQ)
4. Front-end obtains a service ticket for the back-end on behalf of the user (TGS_REQ/REP)
5. Front-end makes a request to back-end, acting as the user (AP_REQ)



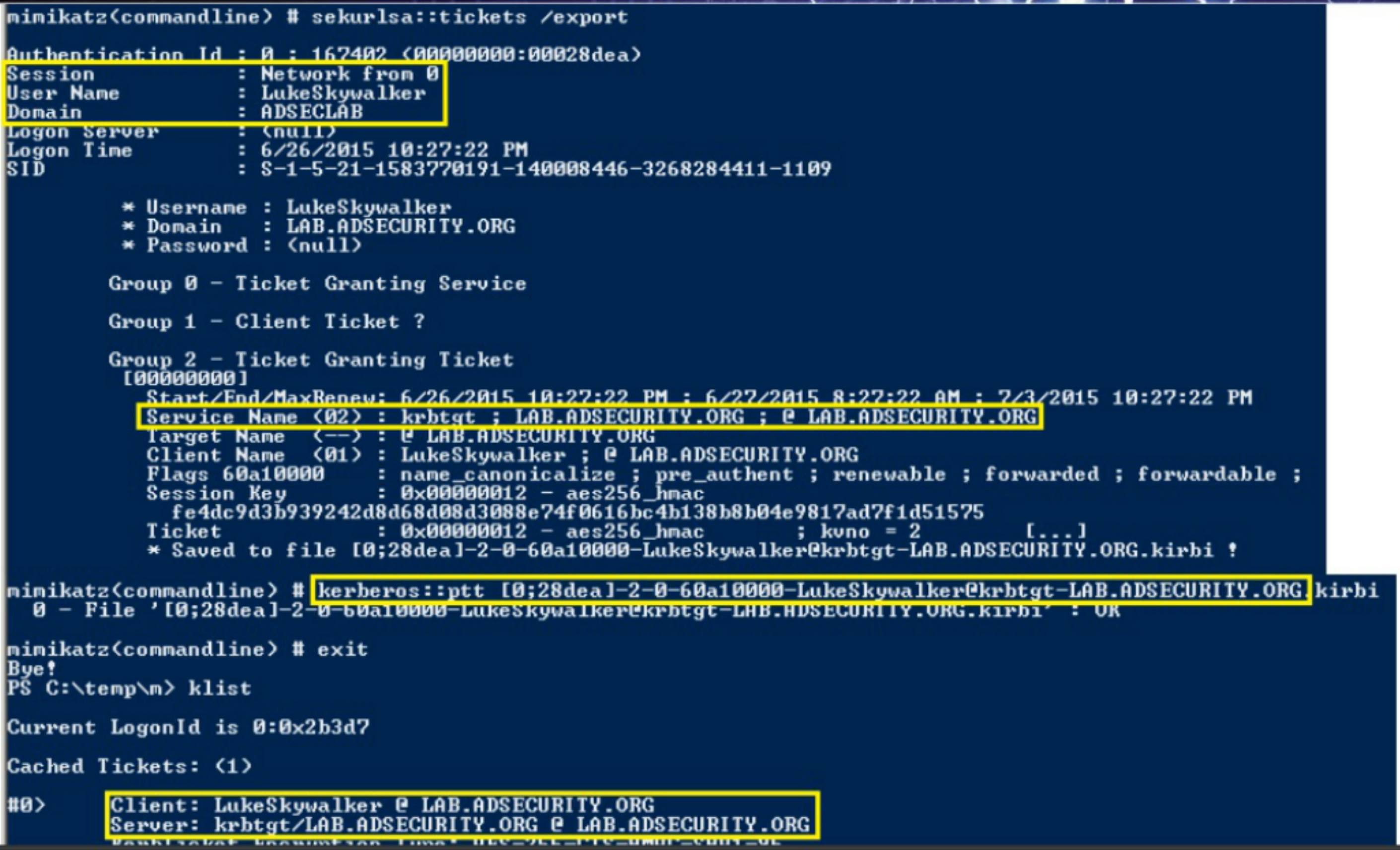
LIMITATIONS

Unlimited access

Services are exposed to broader impersonation risks

Kerberos only

No support for other authentication protocols black hat USA 2015



```
mimikatz(commandline) # sekurlsa::tickets /export

Authentication Id : 0 ; 167402 (00000000:00028dea)
Session           : Network from 0
User Name         : LukeSkywalker
Domain            : ADSECLAB
Logon Server      : (null)
Logon Time        : 6/26/2015 10:27:22 PM
SID               : S-1-5-21-1583770191-140008446-3268284411-1109

         * Username : LukeSkywalker
         * Domain   : LAB.ADSECURITY.ORG
         * Password : (null)

        Group 0 - Ticket Granting Service

        Group 1 - Client Ticket ?

        Group 2 - Ticket Granting Ticket
         [00000000]
           Start/End/MaxRenew: 6/26/2015 10:27:22 PM ; 6/27/2015 8:27:22 AM ; 7/3/2015 10:27:22 PM
           Service Name (02) : krbtgt ; LAB.ADSECURITY.ORG ; @ LAB.ADSECURITY.ORG
           Target Name  (--) : @ LAB.ADSECURITY.ORG
           Client Name  (01) : LukeSkywalker ; @ LAB.ADSECURITY.ORG
           Flags 60a10000    : name_canonicalize ; pre_authent ; renewable ; forwarded ; forwardable ;
           Session Key       : 0x00000012 - aes256_hmac
             fe4dc9d3b939242d8d68d08d3088e74f0616bc4b138b8b04e9817ad7f1d51575
           Ticket            : 0x00000012 - aes256_hmac       ; kvno = 2        [...]
           * Saved to file [0;28dea]-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.kirbi !

mimikatz(commandline) # kerberos::ptt [0;28dea]-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.kirbi
  0 - File '[0;28dea]-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.kirbi' : OK

mimikatz(commandline) # exit
Bye!
PS C:\temp\m> klist

Current LogonId is 0:0x2b3d7

Cached Tickets: (1)

#0>     Client: LukeSkywalker @ LAB.ADSECURITY.ORG
        Server: krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
```

"Nobody is going to delegate a lot of power to a secretary that they can't control."

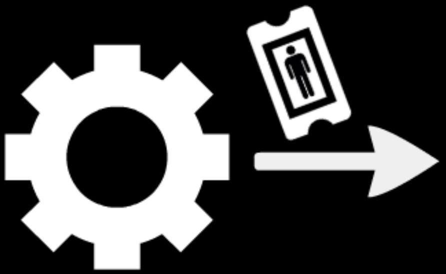
Michael Bloomberg

CONSTRAINED DELEGATION

Service-for-User delegation

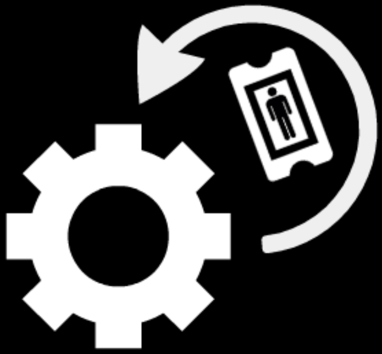
Windows 2003

S4U EXTENSIONS



S4U2Proxy

Allows a service to obtain a service ticket on behalf of a user to a different service



S4U2Self

Allows a service to obtain a service ticket to itself in the name of a different user

Restricts the services that can be accessed by impersonation

TGTs are not forwarded to the front-end

Support protocol transitioning

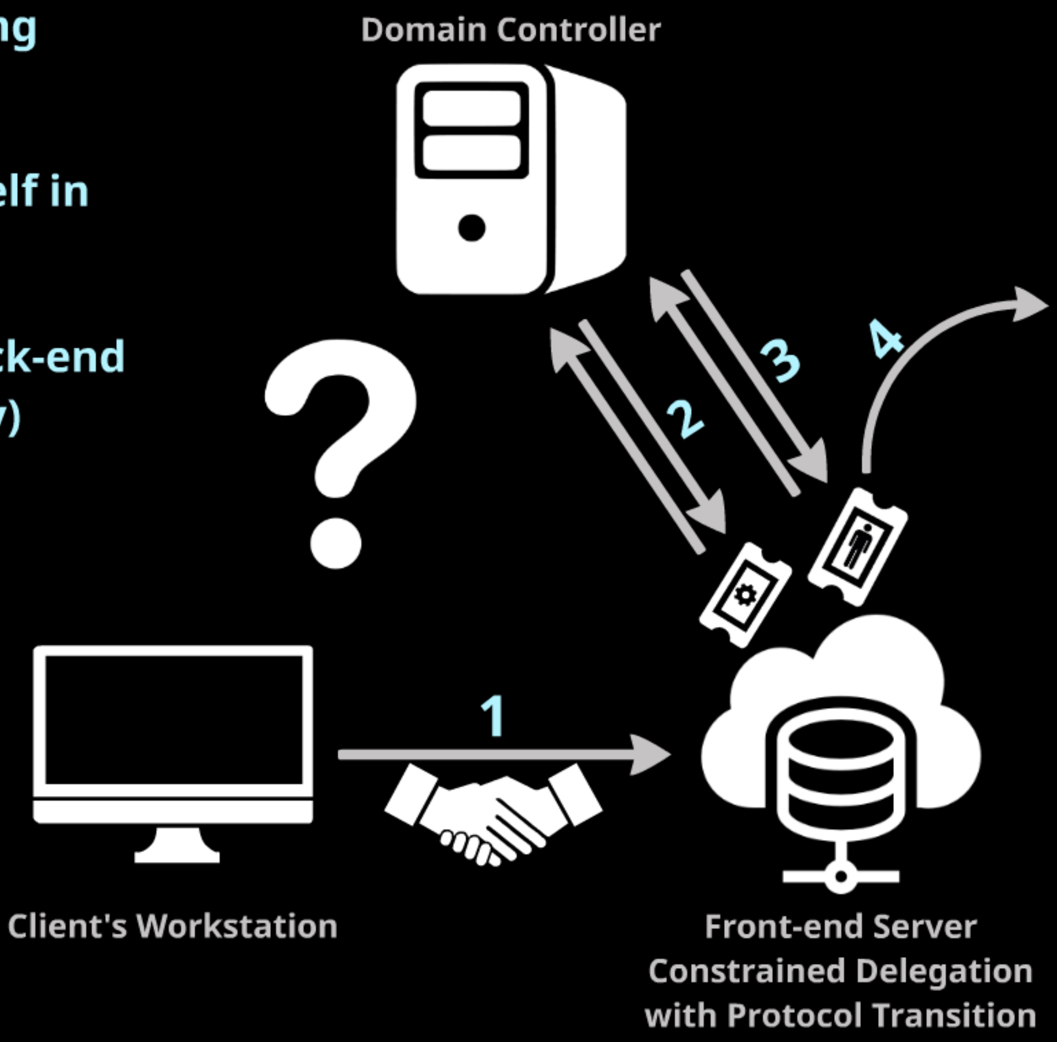
Limited to a single domain

1. User authenticates to the front-end using non-Kerberos authentication

2. Front-end obtains a service ticket to itself in the named user (S4U2Self)

3. Front-end obtains a service ticket to back-end on behalf of the named user (S4U2Proxy)

4. Front-end makes a request to back-end, acting as the user (AP_REQ)



"S4U allows a service to obtain a Kerberos service ticket for a user that has not authenticated to the KDC"

"S4U2Self allows you to obtain a Windows token for the client by supplying a UPN without a password."

[MS-SFU] - Kerberos Protocol Extensions: Service for User and Constrained Delegation Protocol
https://msdn.microsoft.com/en-us/library/cc246071.aspx

How To: Use Protocol Transition and Constrained Delegation in ASP.NET 2.0
https://msdn.microsoft.com/en-us/library/ff649317.aspx

Which means it's not going to be changed soon..

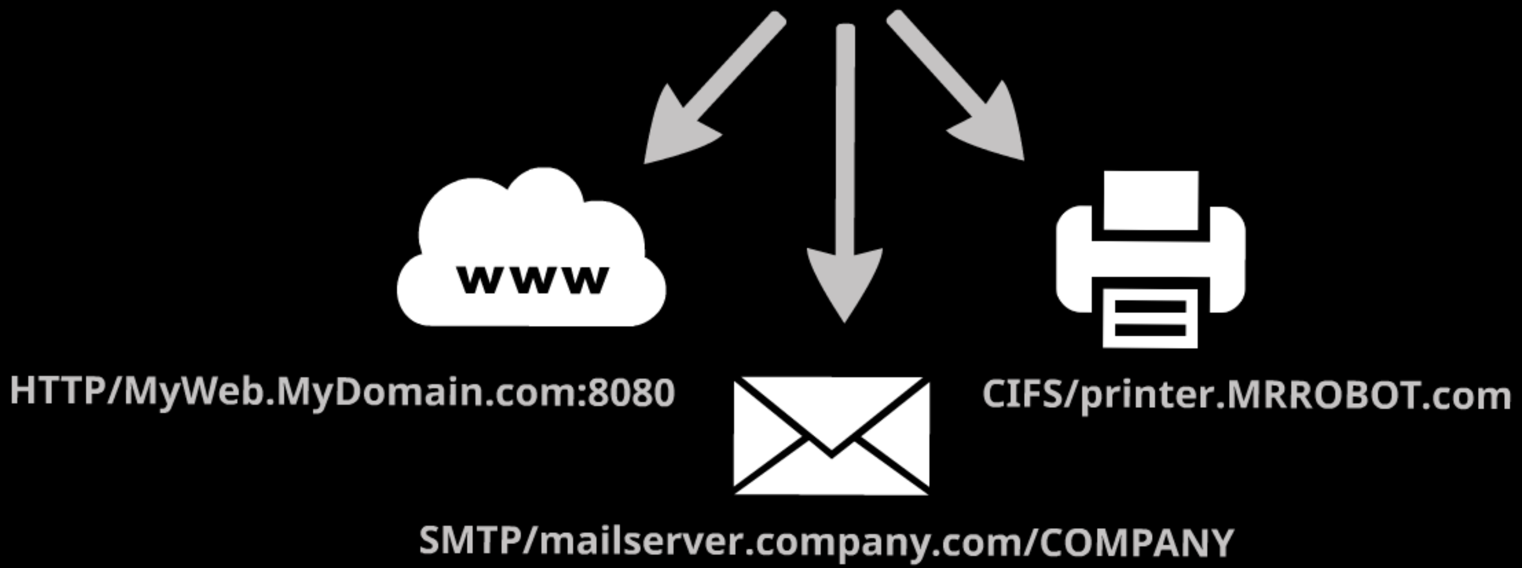
“The S4U2proxy combined with S4U2self allows a service to impersonate any user principal while accessing a second service. This gives any service allowed by the S4U2proxy a degree of power similar to that of the KDC itself. ”

Security Considerations for Implementers
https://msdn.microsoft.com/en-us/library/cc246112.aspx

SERVICE PRINCIPAL NAME

uniquely identifies an instance of a service

<service type>/<host name>:<port number>/<distinguished name>



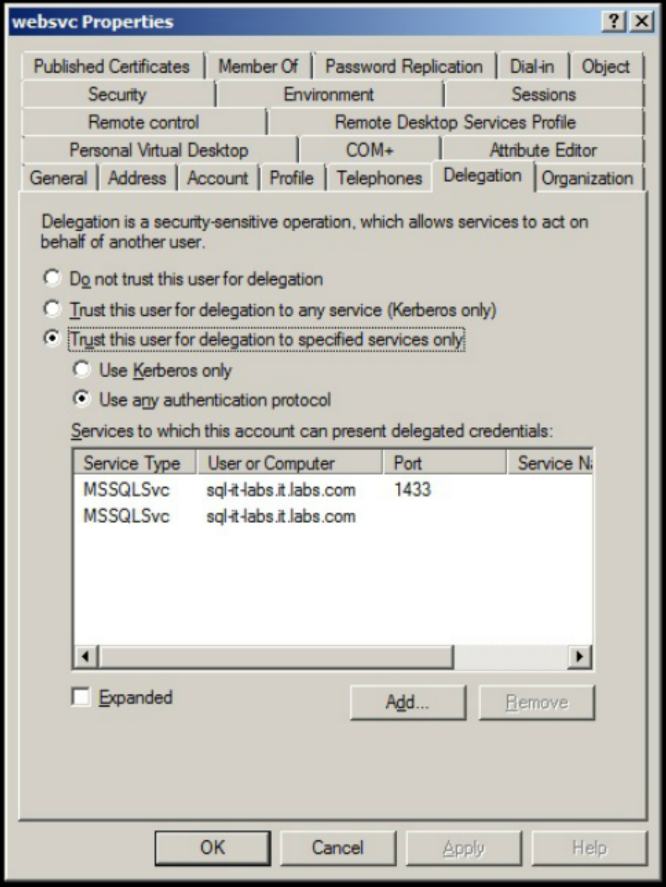
HTTP/MyWeb.MyDomain.com:8080

SMTP/mailserver.company.com/COMPANY

CIFS/printer.MRROBOT.com

DELEGATION ACCOUNTS

- A computer or a user account
- Must be registered with an SPN
- Configured by Domain Administrators
- S4U2Self requires to act as part of the operating system (SeTcbPrivilege)



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

○ Do not trust this user for delegation

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

● Trust this user for delegation to specified services only

○ Use Kerberos only

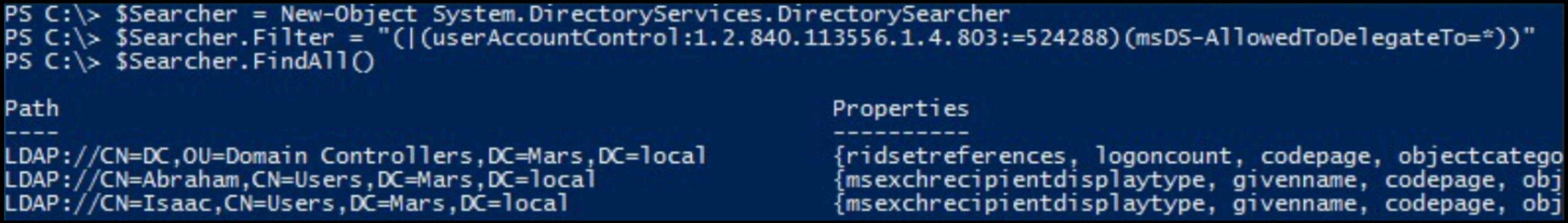
● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
MSSQLSvc	sql-it-labs.it.labs.com	1433	
MSSQLSvc	sql-it-labs.it.labs.com		

□ Expanded

Unconstrained Delegation	Constrained Delegation	Protocol Transition
TRUSTED_FOR_DELEGATION **(0x80000)**	**MsDS-AllowedToDelegateTo** **(List of SPNs)**	**Trusted_To_Authenticate_For_Delegation (0x100000)** **&** **MsDS-AllowedToDelegateTo** **(List of SPNs)**

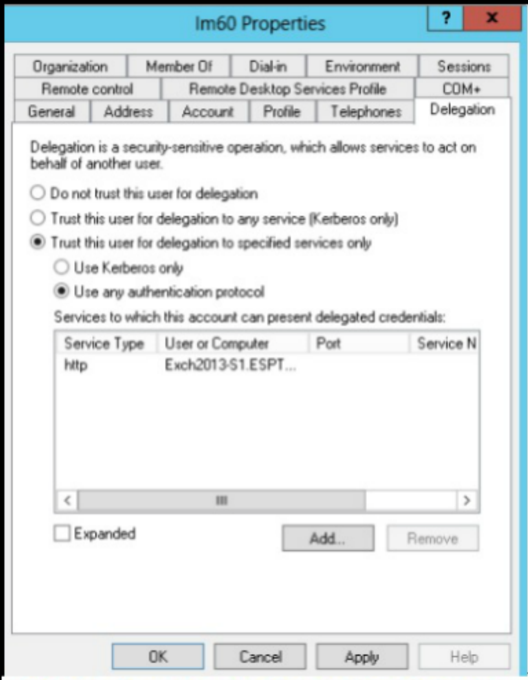


```
PS C:\> $Searcher = New-Object System.DirectoryServices.DirectorySearcher
PS C:\> $Searcher.Filter = "(|(userAccountControl:1.2.840.113556.1.4.803:=524288)(msDS-AllowedToDelegateTo=*))"
PS C:\> $Searcher.FindAll()

Path                                                     Properties
----                                                     ----------
LDAP://CN=DC,OU=Domain Controllers,DC=Mars,DC=local      {ridsetreferences, logoncount, codepage, objectcatego
LDAP://CN=Abraham,CN=Users,DC=Mars,DC=local              {msexchrecipientdisplaytype, givenname, codepage, obj
LDAP://CN=Isaac,CN=Users,DC=Mars,DC=local                {msexchrecipientdisplaytype, givenname, codepage, obj
```

EXPLOITABILITY

Delegation accounts are:

- easily discovered
- exposed by the host service
- often unmanaged
- vulnerable to Kerberoasting
- always logged-on



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

○ Do not trust this user for delegation

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

● Trust this user for delegation to specified services only

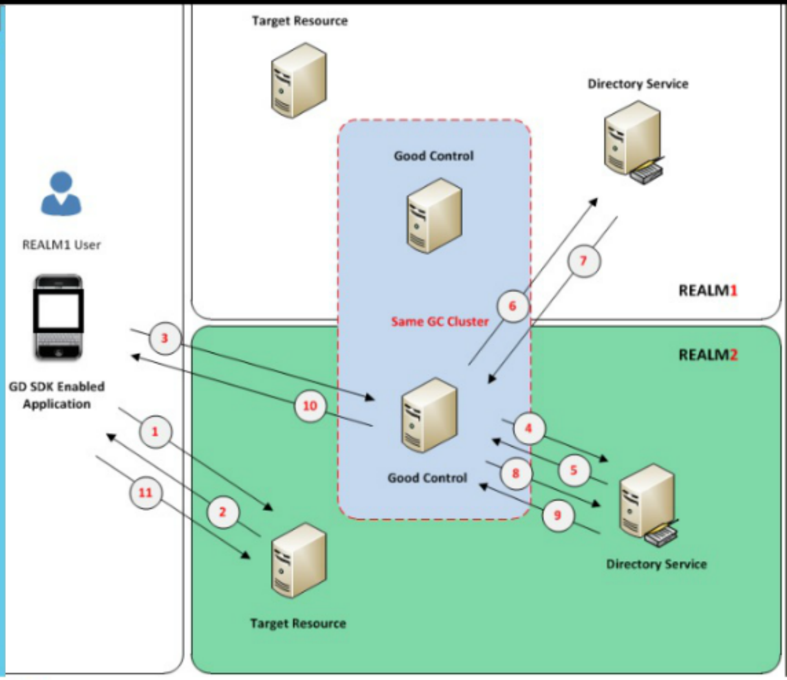
○ Use Kerberos only

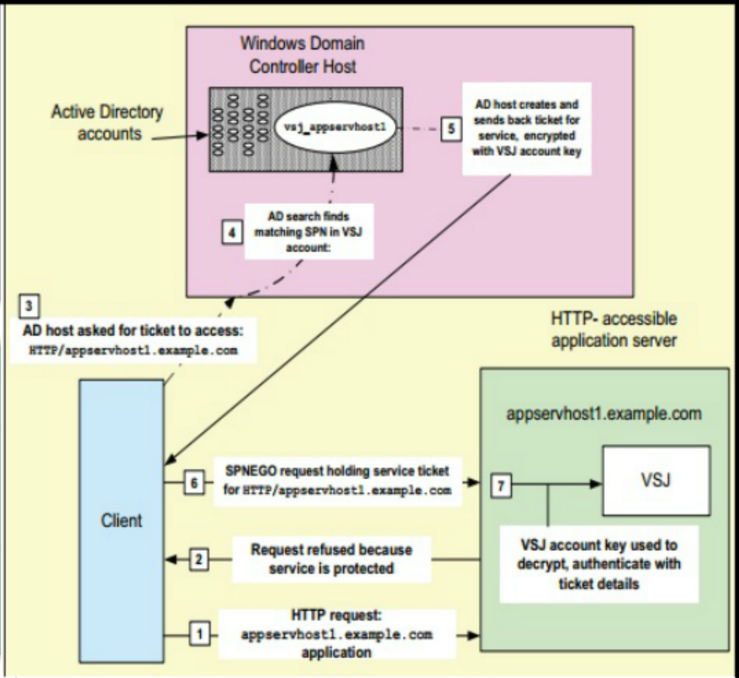
● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
http	Exch2013-S1.ESPT...		

☐ Expanded

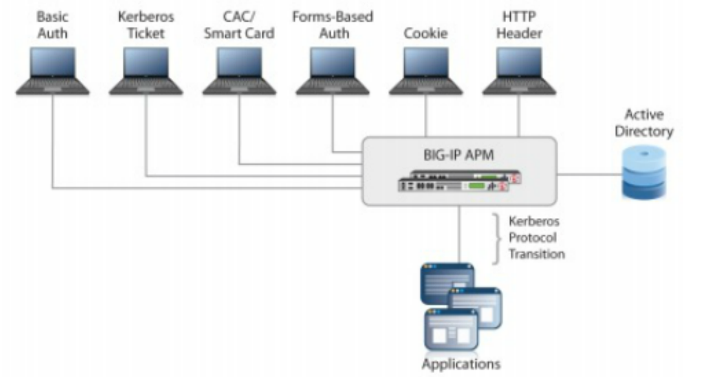



Windows Domain Controller Host
Active Directory accounts
vsj_appservhost1
5
AD host creates and sends back ticket for service, encrypted with VSJ account key
4
AD search finds matching SPN in VSJ account:
3
AD host asked for ticket to access: HTTP/appservhost1.example.com
HTTP- accessible application server
appservhost1.example.com
Client
6
SPNEGO request holding service ticket for HTTP/appservhost1.example.com
7
VSJ
2
Request refused because service is protected
VSJ account key used to decrypt, authenticate with ticket details
1
HTTP request: appservhost1.example.com application

Configuring Trust for the Active Directory user

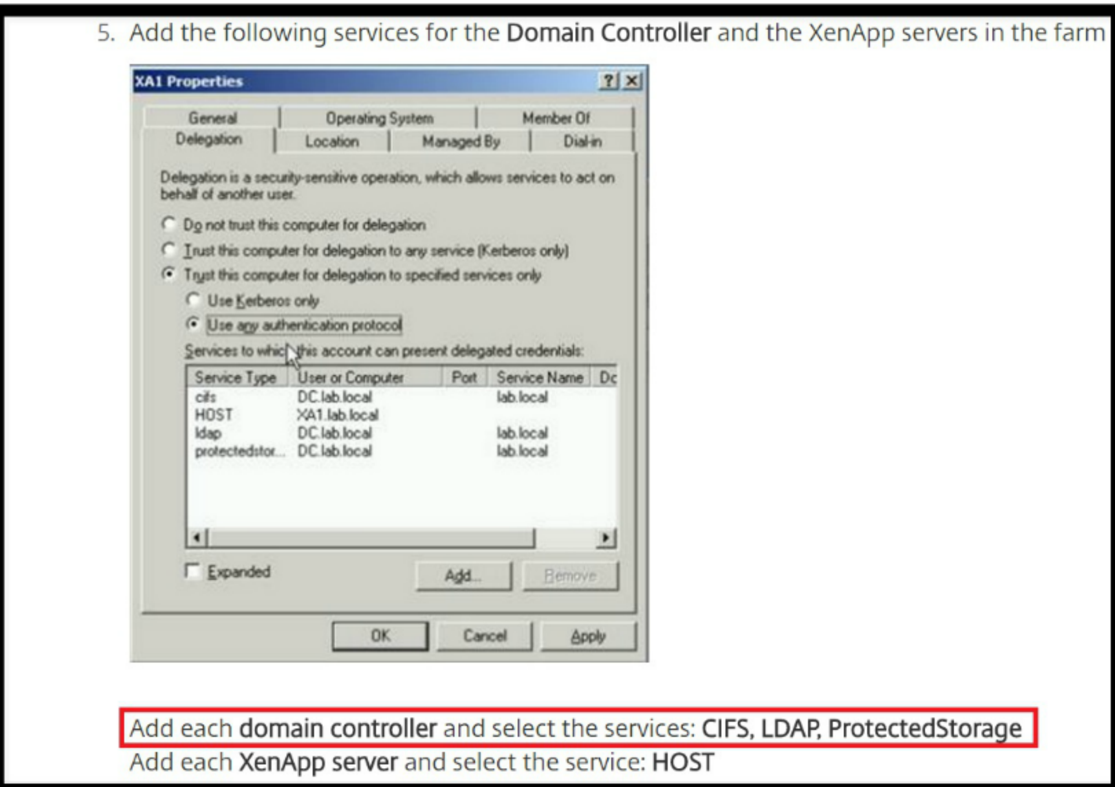
In this section, you configure the trust for specfic services for the user you created.

1. From the Windows Domain controller, from the Administrative Tools menu, open **Active Directory Users and Computers**.
2. Right-click the user account you created.
3. Click the Delegation tab.
4. Click **Trust this user for delegation to specified services only**. This enables Kerberos constrained delegation.
5. Under Trust this user for delegation to specified services only, click **Use any authentication protocol**. This enables Kerberos protocol transition on the server-side.
6. In the Services to which this account can present delegated credentials area, click the **Add** button to add services to the list.



How to Set Up Kerberos Constrained Delegation to use Single Sign-On (Password Manager) and Smartcard Authentication from Clients Not Joined to the Domain

Article | Authentication | 6 found this helpful | Created: 26 Mar 2014 | Modified: 15 Apr 2016



5. Add the following services for the **Domain Controller** and the XenApp servers in the farm

XA1 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:

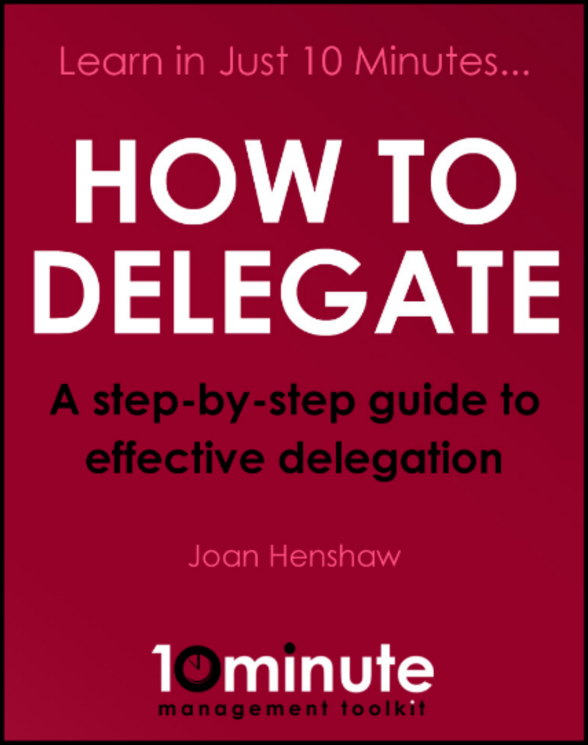
Service Type	User or Computer	Port	Service Name	Dc
cifs	DC.lab.local		lab.local	
HOST	XA1.lab.local			
ldap	DC.lab.local		lab.local	
protectedstor...	DC.lab.local		lab.local	

□ Expanded

Add each **domain controller** and select the services: **CIFS, LDAP, ProtectedStorage**

Add each **XenApp server** and select the service: **HOST**

ATTACK SURFACE



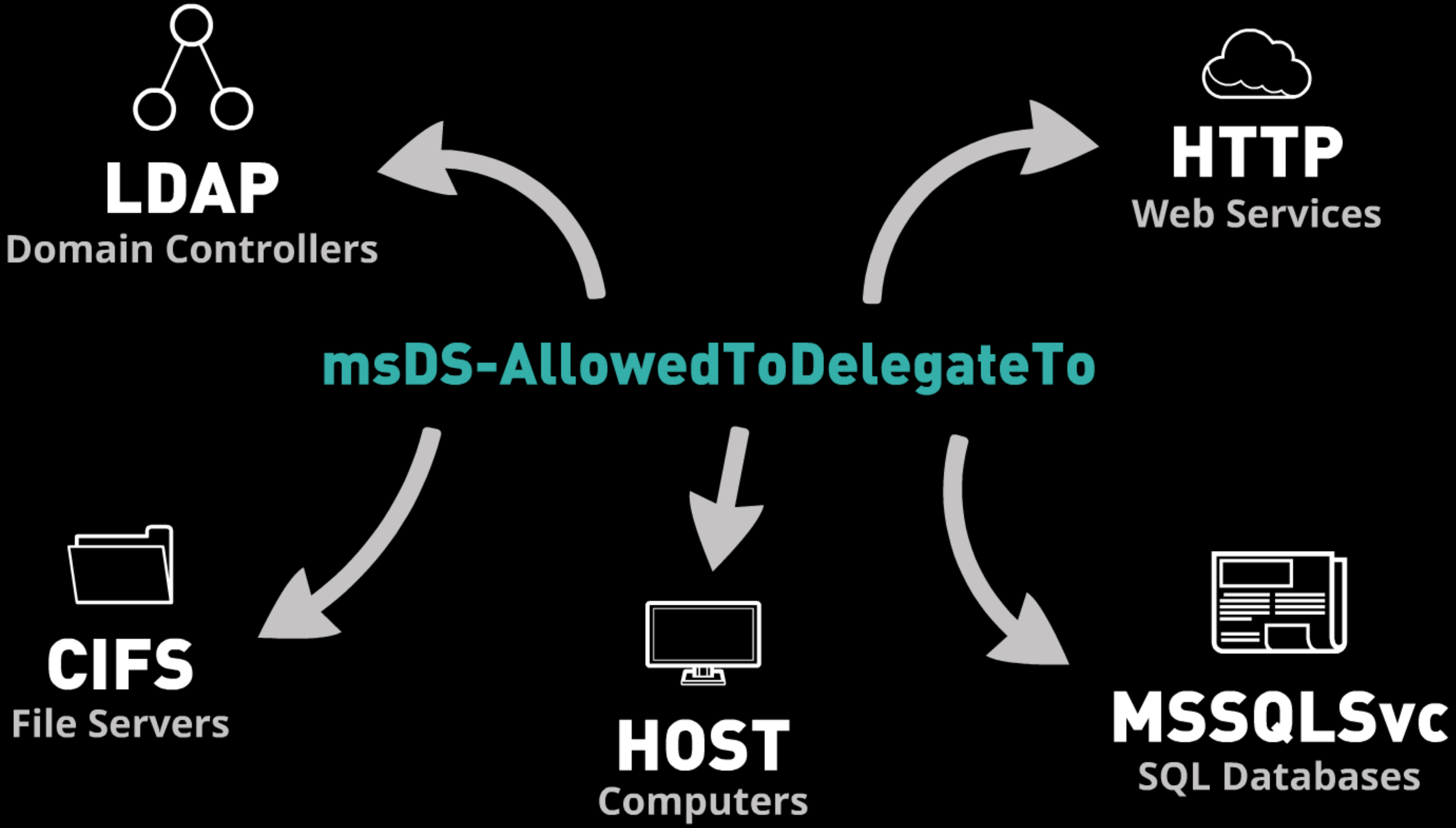
Learn in Just 10 Minutes...

HOW TO DELEGATE

A step-by-step guide to effective delegation

Joan Henshaw

10minute
management toolkit



msDS-AllowedToDelegateTo

LDAP
Domain Controllers

HTTP
Web Services

CIFS
File Servers

HOST
Computers

MSSQLSvc
SQL Databases

ATTACK VECTORS
ATTACK VECTORS EVERYWHERE
LIGHTYEAR
SPACE RANGER
imgflip.com

Credential Theft

DCSync

Remote Execution

xp_cmdshell, Invoke-Command, HOST

Privilege Escalation

Arbitrary impersonations

Data Exfiltration

Applications, file shares and databases

THE FLOW

Hunt accounts trusted for delegation

Impersonate another user

Abuse the allowed services

MYSTIQUE

PowerShell tool to play with S4U

- Find accounts trusted for delegation
- Read delegation flags and attributes
- Impersonate arbitrary users

https://github.com/machosec/Mystique

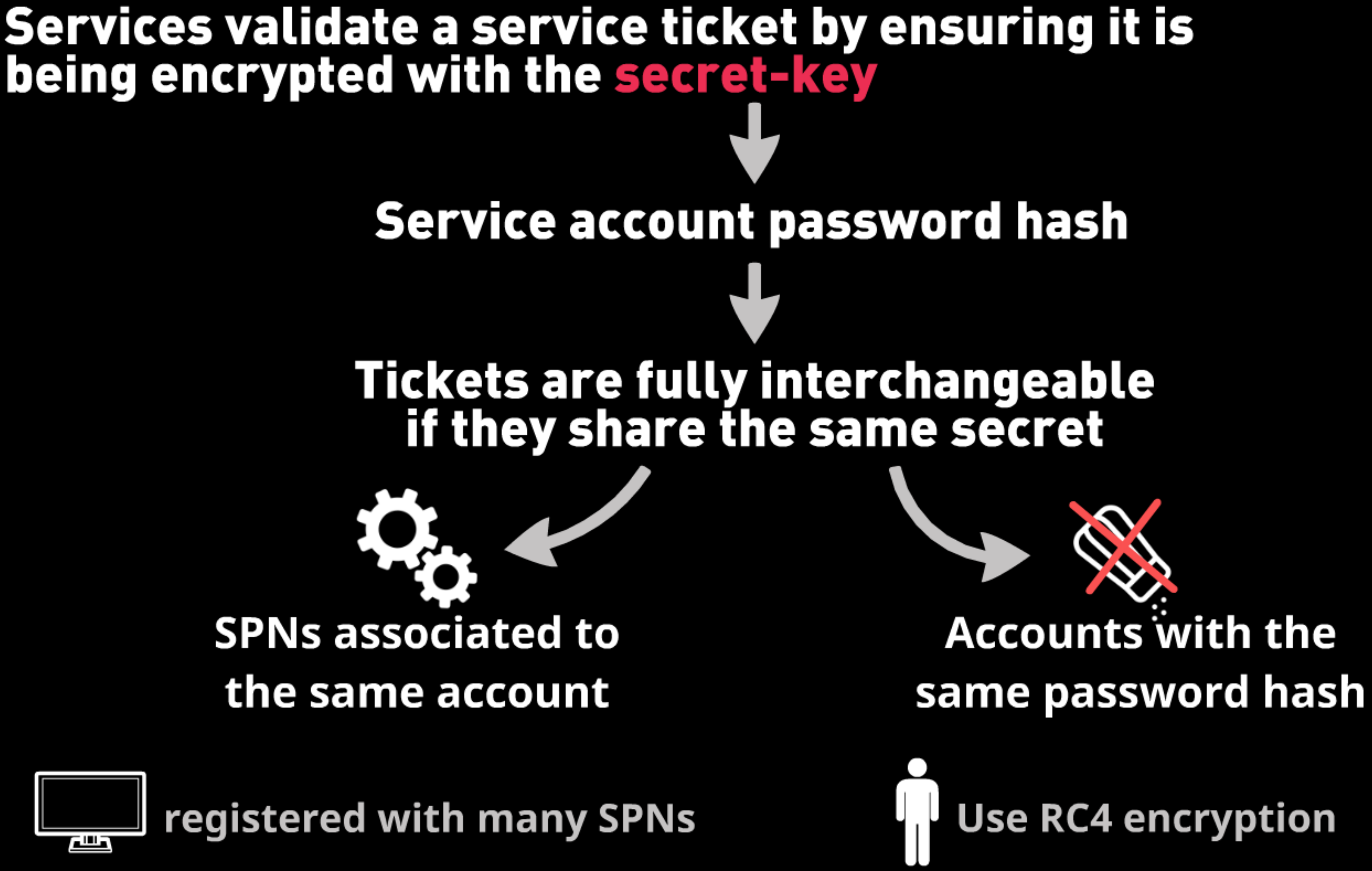
DELEGATE
ALL THE THINGS
imgflip.com

“If I have seen further, it is by standing on the shoulders of giants."

Isaac Newton

THE TWIST

SPNs are not validated!



Services validate a service ticket by ensuring it is being encrypted with the secret-key

Service account password hash

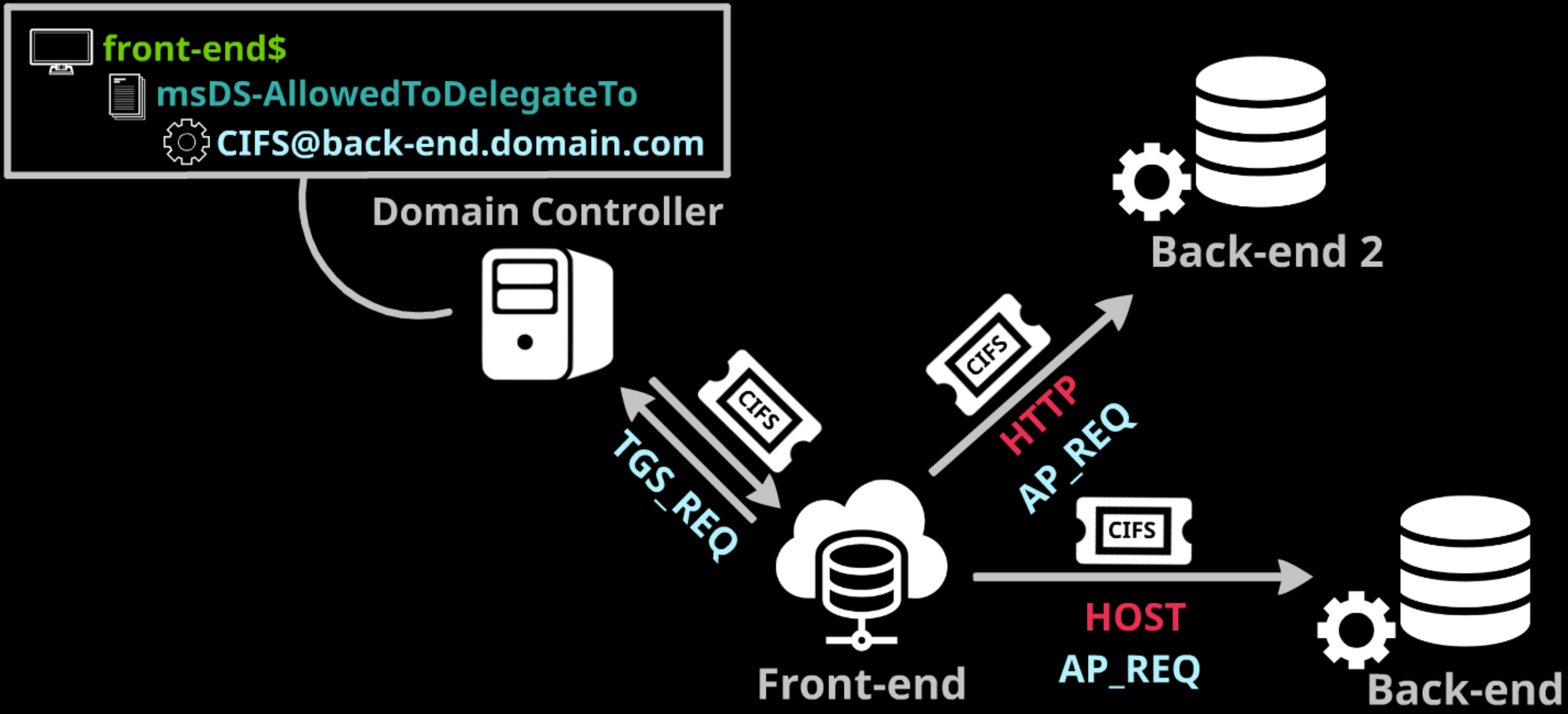
Tickets are fully interchangeable if they share the same secret

SPNs associated to the same account

Accounts with the same password hash

registered with many SPNs

Use RC4 encryption


front-end$
msDS-AllowedToDelegateTo
CIFS@back-end.domain.com
Domain Controller
TGS_REQ
CIFS
Front-end
CIFS
HTTP
AP_REQ
Back-end 2
CIFS
HOST
AP_REQ
Back-end

RESOURCE-BASED CONSTRAINED DELEGATION

Introducing msDS-AllowedToActOnBehalfOfOtherIdentity

- Limit access per account rather than SPN
- Returns some control to the back-end administrator
- Support Delegation across domains and forests
- Requires Server 2012 on front-end and DCs

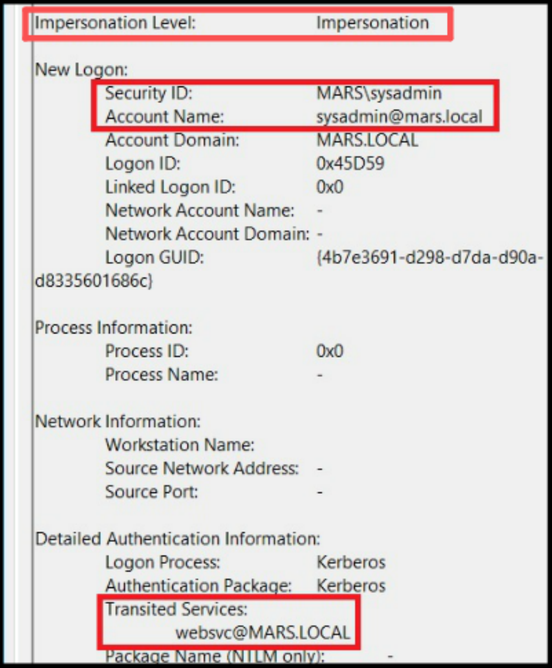
NOT SURE IF GOOD THING
OR VERY BAD THING
imgflip.com

DEFENSE

DETECTION

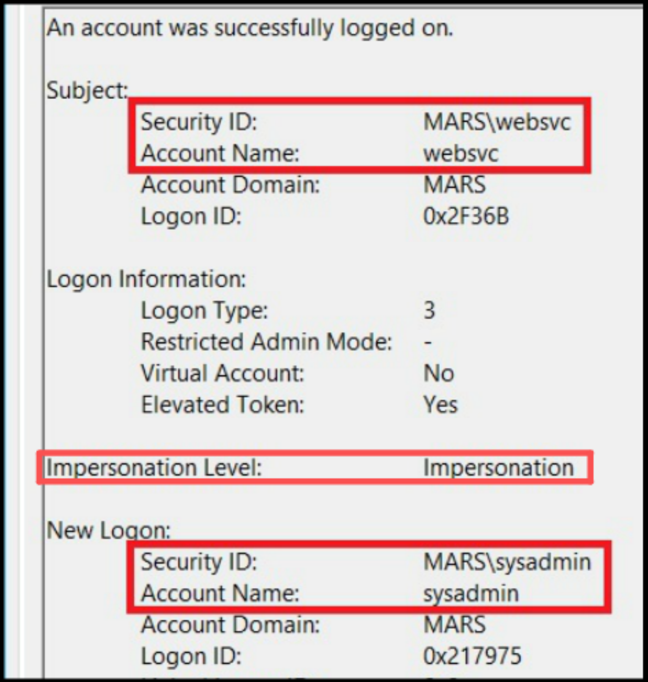
Event log 4624 on Windows 8/2012+

Front-end



```
Impersonation Level:            Impersonation

New Logon:
        Security ID:            MARS\sysadmin
        Account Name:           sysadmin@mars.local
        Account Domain:         MARS.LOCAL
        Logon ID:               0x45D59
        Linked Logon ID:        0x0
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {4b7e3691-d298-d7da-d90a-
d8335601686c}

Process Information:
        Process ID:             0x0
        Process Name:           -

Network Information:
        Workstation Name:
        Source Network Address: -
        Source Port:            -

Detailed Authentication Information:
        Logon Process:          Kerberos
        Authentication Package: Kerberos
        Transited Services:
                websvc@MARS.LOCAL
        Package Name (NTLM only):       -
```

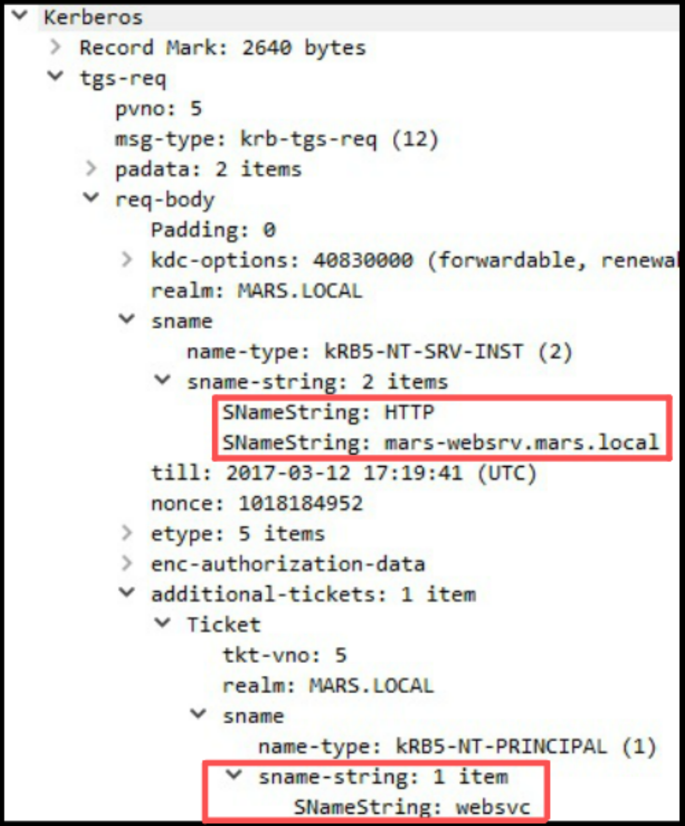
Back-end



```
An account was successfully logged on.

Subject:
        Security ID:            MARS\websvc
        Account Name:           websvc
        Account Domain:         MARS
        Logon ID:               0x2F36B

Logon Information:
        Logon Type:             3
        Restricted Admin Mode:  -
        Virtual Account:        No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            MARS\sysadmin
        Account Name:           sysadmin
        Account Domain:         MARS
        Logon ID:               0x217975
```

S4U2Proxy network traffic correlation

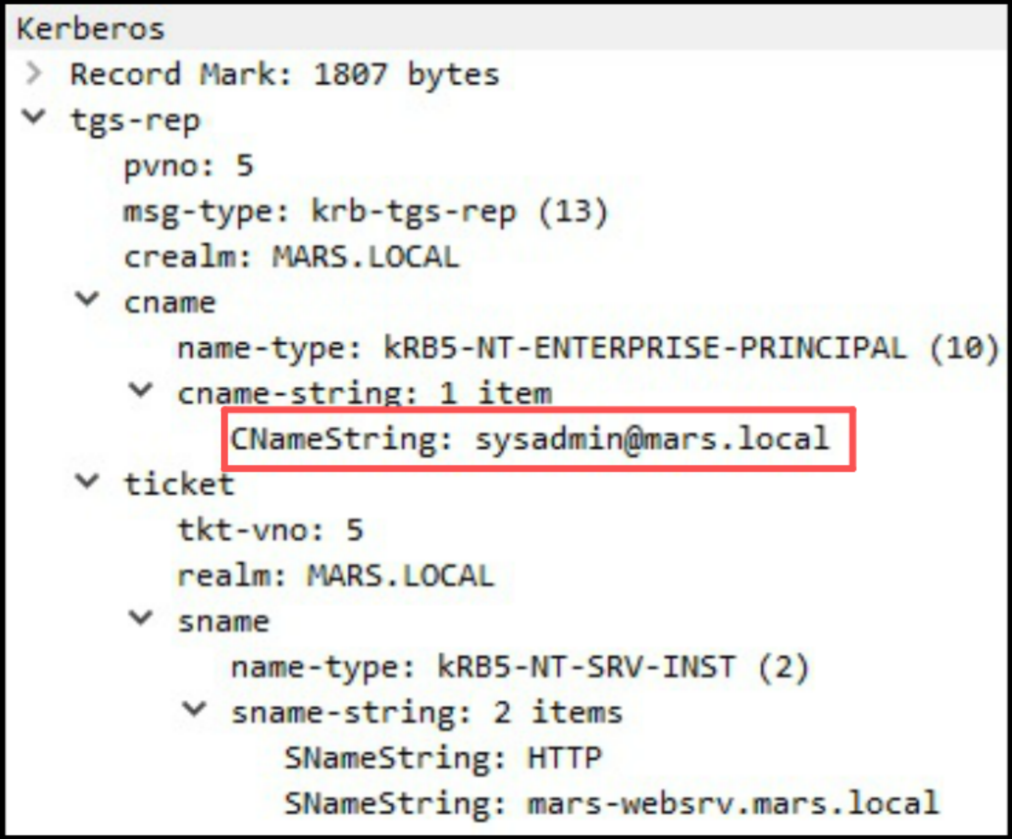
TGS_REQ



```
Kerberos
  Record Mark: 2640 bytes
  tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    padata: 2 items
    req-body
      Padding: 0
      kdc-options: 40830000 (forwardable, renewa
      realm: MARS.LOCAL
      sname
        name-type: kRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: HTTP
          SNameString: mars-websrv.mars.local
      till: 2017-03-12 17:19:41 (UTC)
      nonce: 1018184952
      etype: 5 items
      enc-authorization-data
      additional-tickets: 1 item
        Ticket
          tkt-vno: 5
          realm: MARS.LOCAL
          sname
            name-type: kRB5-NT-PRINCIPAL (1)
            sname-string: 1 item
              SNameString: websvc
```

+

TGS_REP



```
Kerberos
  Record Mark: 1807 bytes
  tgs-rep
    pvno: 5
    msg-type: krb-tgs-rep (13)
    crealm: MARS.LOCAL
    cname
      name-type: kRB5-NT-ENTERPRISE-PRINCIPAL (10)
      cname-string: 1 item
        CNameString: sysadmin@mars.local
    ticket
      tkt-vno: 5
      realm: MARS.LOCAL
      sname
        name-type: kRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: HTTP
          SNameString: mars-websrv.mars.local
```

MITIGATION

- Configure sevices with a dedicated service account
  - 👎 Avoid dual-use or using computer accounts
  - 👍 Ensure password rotation and complexity

- Set unique SPNs to be allowed for delegation
  - 👎 Do not delegate to built-in SPNs
  - 👍 Specify specific port numbers

Other options to consider..

- Set privileged accounts as "account is sensitive and cannot be delegated"
- Restrict access per account instead of SPNs (Server 2012)
- Enforce forest boundary in unconstrained delegation (2012R2)

SOUND BYTES

Kerberos delegation can be easily abused for privilege escalation and remote execution

Services and service accounts can introduce more risk than you think

Hardening delegation rights is tough - but possible

QUESTIONS?

THANKS!

- CyberArk
- MSRC
- Benjamin Delpy (@gentilkiwi)
- Alberto Solino (@agsolino)
- To all of you for taking delegation seriously

Let's talk!

@machosec

me@matanhart.com

black hat ASIA 2017

DELEGATE TO THE TOP

Abusing Kerberos for Arbitrary Impersonations and RCE

Matan Hart
@machosec
me@matanhart.com