ON TOUR | NEW YORK

PASS

Kerberos
A dive into delegation & SQL Server

Danny de Haan

He/Him

Solutions Engineer

Redgate Software

Danny de Haan

He/Him

Solutions Engineer
Redgate Software

I've been working in IT for about 20 years in various roles. With over 15 years of experience with SQL Server, I've always placed a strong emphasis on Security, Risk Management, and Compliance for the SQL Server Data Platform. Ensuring industry best practices and regulatory requirements are followed from an infrastructural point of view.

thatinfradba@pm.me

/in/dannydh

Session Breakdown

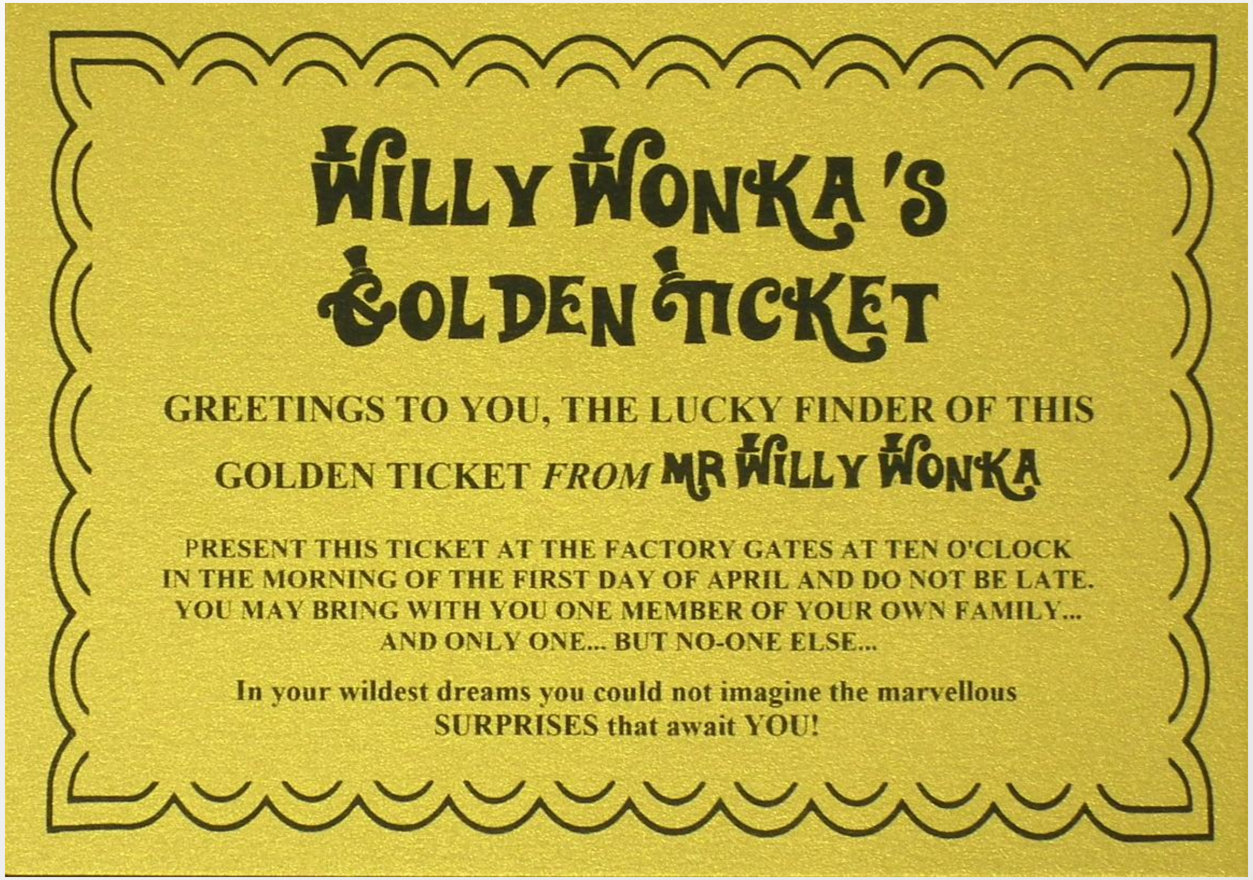
- Kerberos Process in AD
- Service Principal Names
- Database Engine
- Delegation
- Reporting Services
- Troubleshooting Tips
- Attack Scenario’s

ON TOUR | NEW YORK

PASS

Kerberos in AD

Something with tickets?



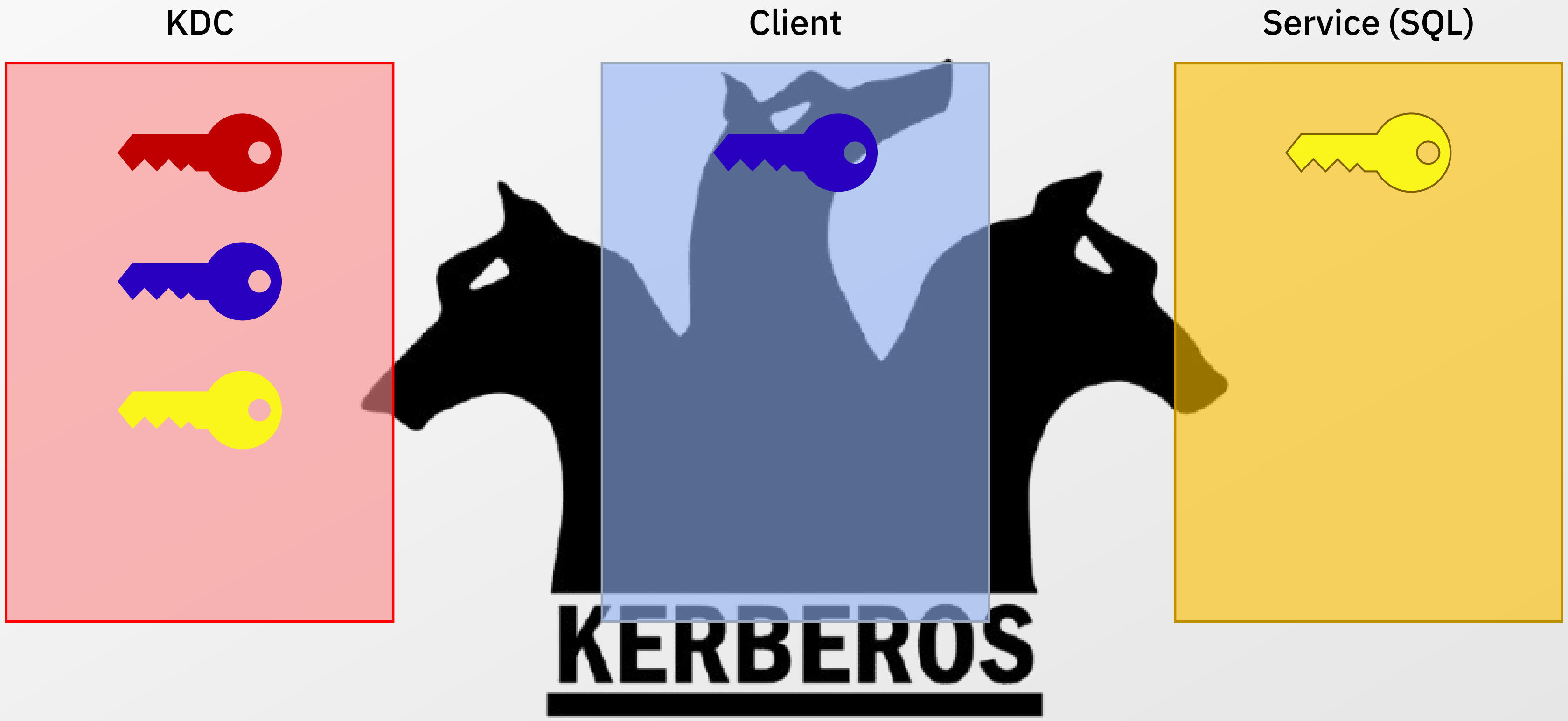
WILLY WONKA'S
GOLDEN TICKET

GREETINGS TO YOU, THE LUCKY FINDER OF THIS GOLDEN TICKET *FROM* MR WILLY WONKA

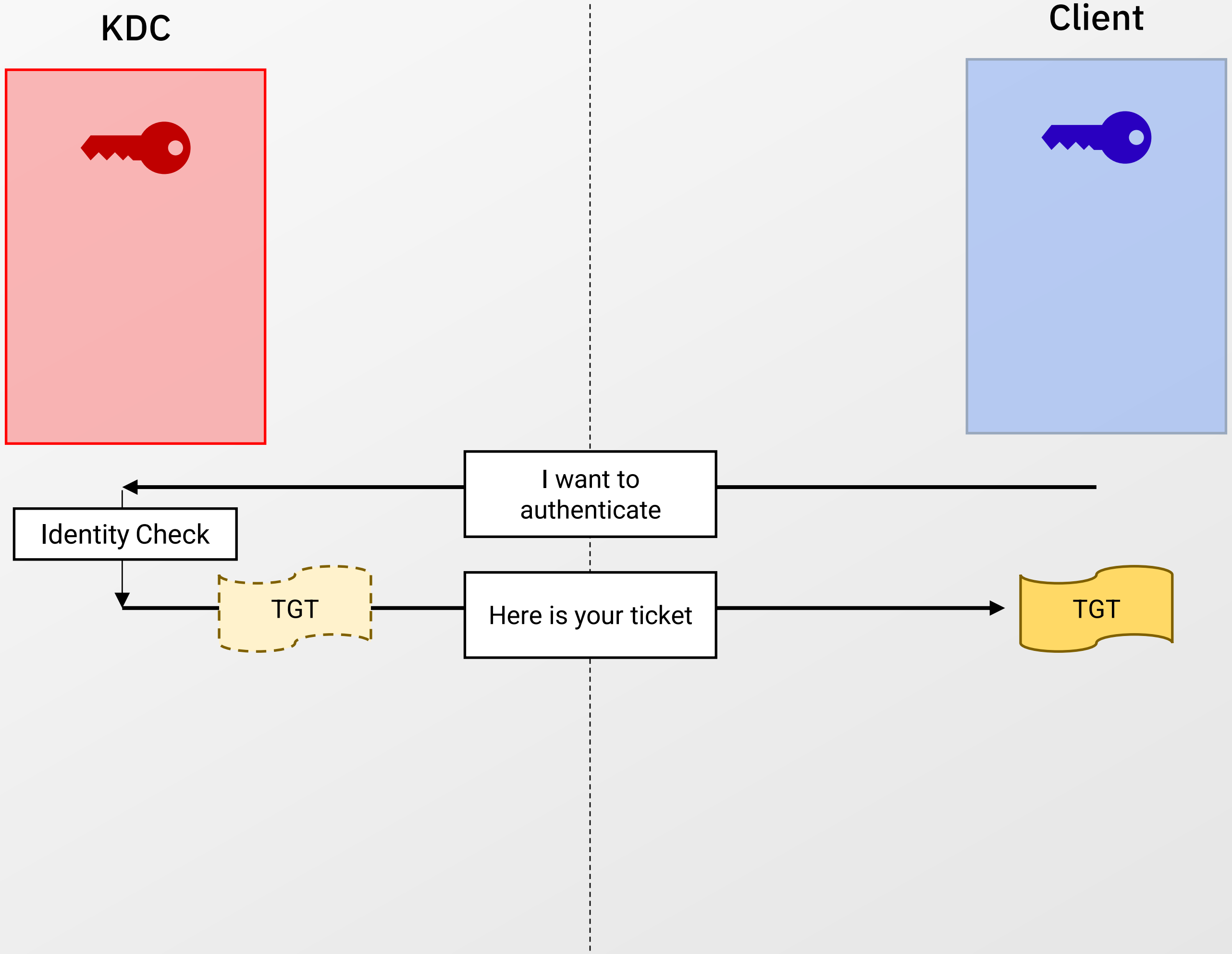
PRESENT THIS TICKET AT THE FACTORY GATES AT TEN O'CLOCK IN THE MORNING OF THE FIRST DAY OF APRIL AND DO NOT BE LATE. YOU MAY BRING WITH YOU ONE MEMBER OF YOUR OWN FAMILY... AND ONLY ONE... BUT NO-ONE ELSE...

In your wildest dreams you could not imagine the marvellous SURPRISES that await YOU!

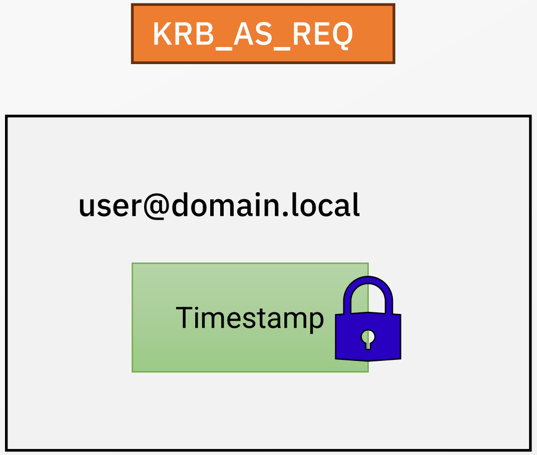
Kerberos Process



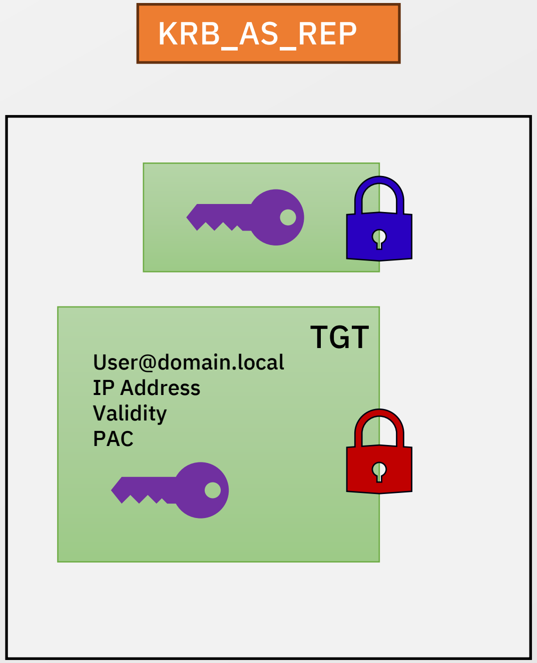
Authentication Service



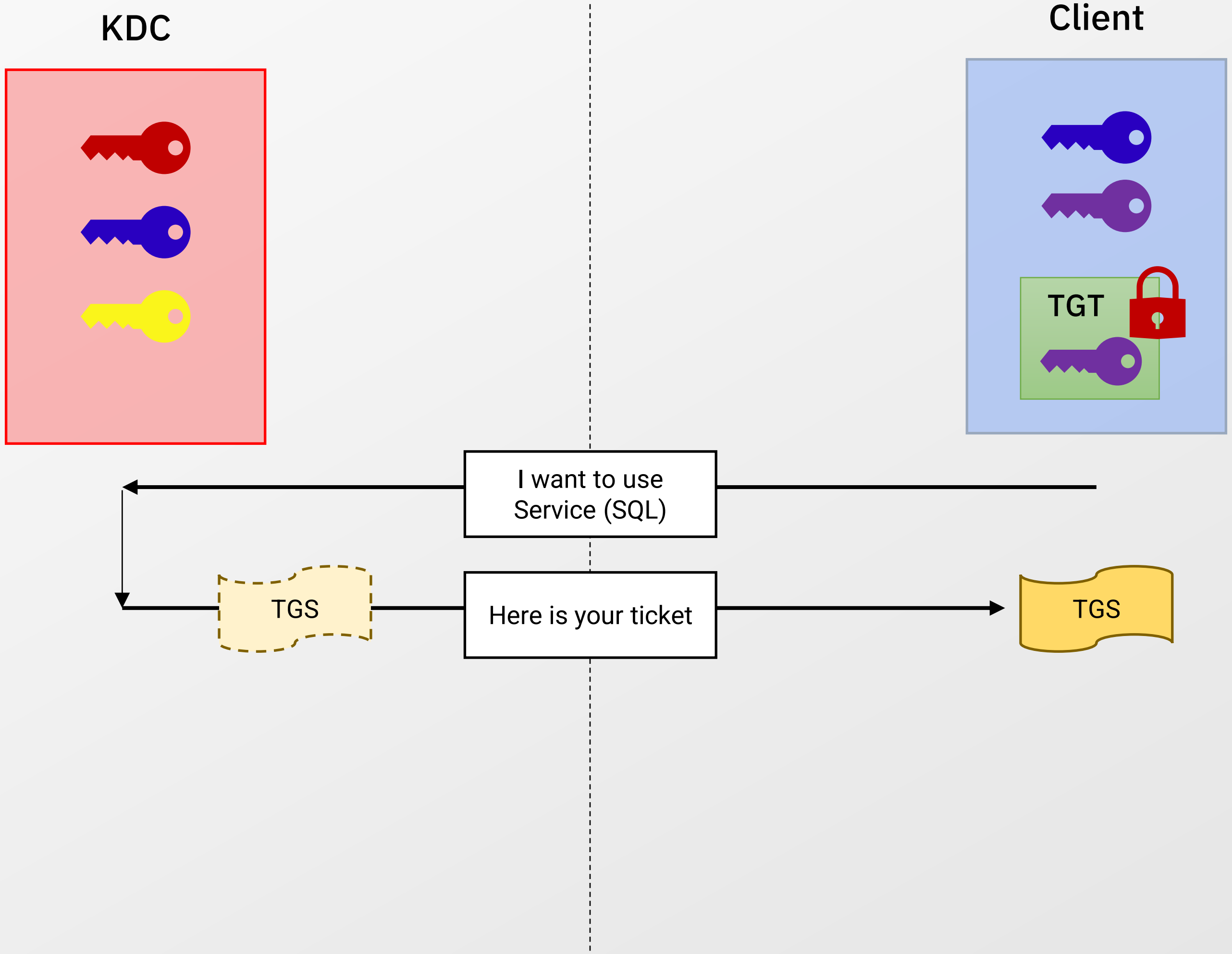
Authentication Service (KDC)



User	Hash
Anna	<Anna’s hash>
Chris	<Chris’ hash>
…	…
User	<User’s hash>
…	…



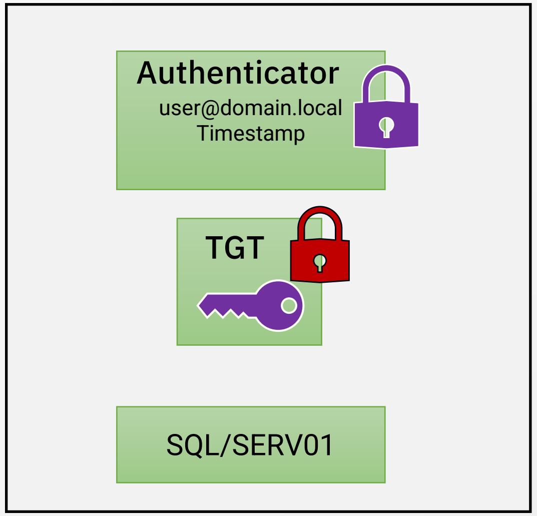
Ticket-Granting Service



Ticket-Granting Service (tickets)

KRB_TGS_REQ

KRB_TGS_REP



Authenticator

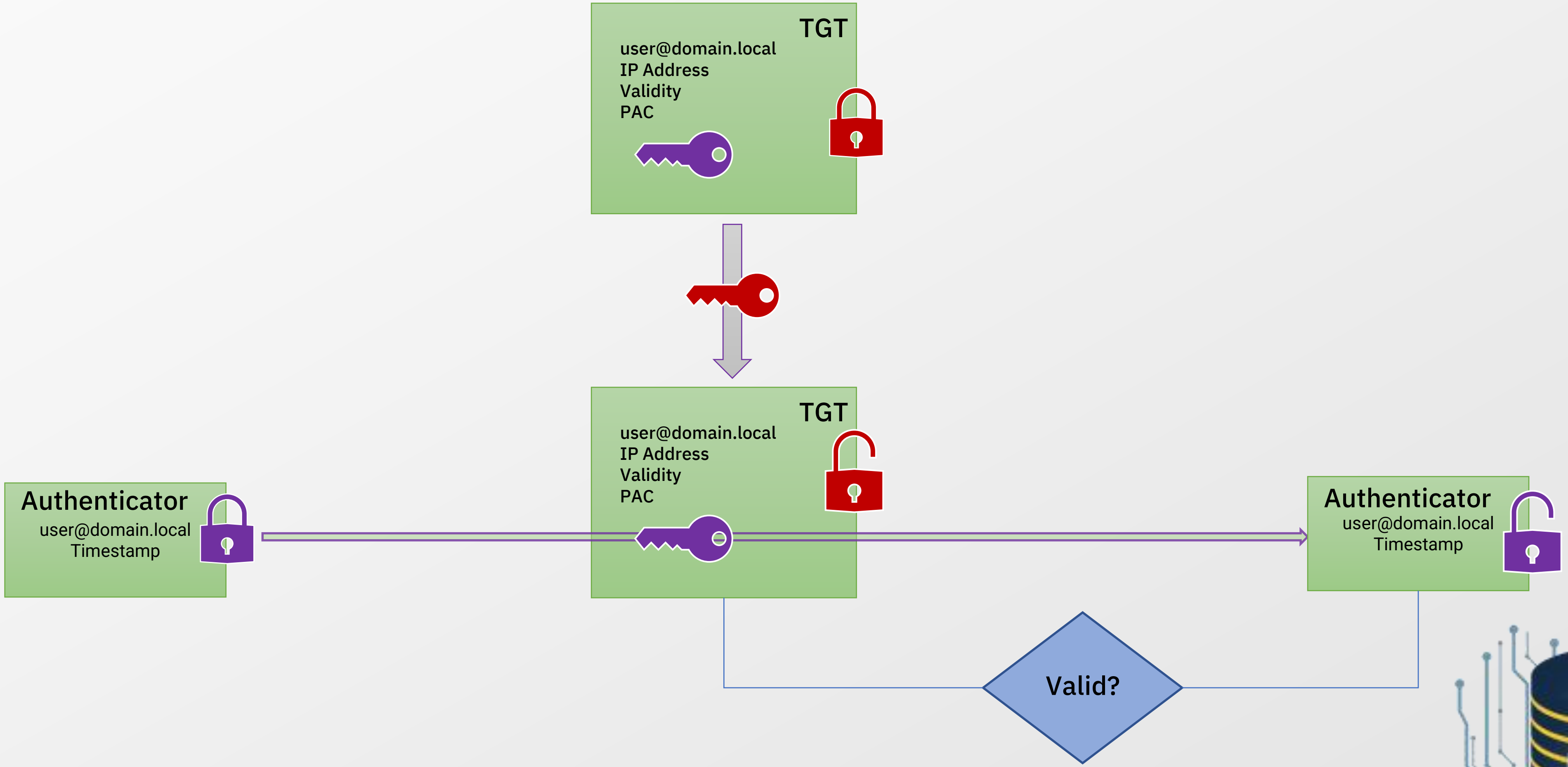
user@domain.local

Timestamp

TGT

SQL/SERV01

Ticket-Granting Service (KDC)


TGT

user@domain.local
IP Address
Validity
PAC

TGT

user@domain.local
IP Address
Validity
PAC

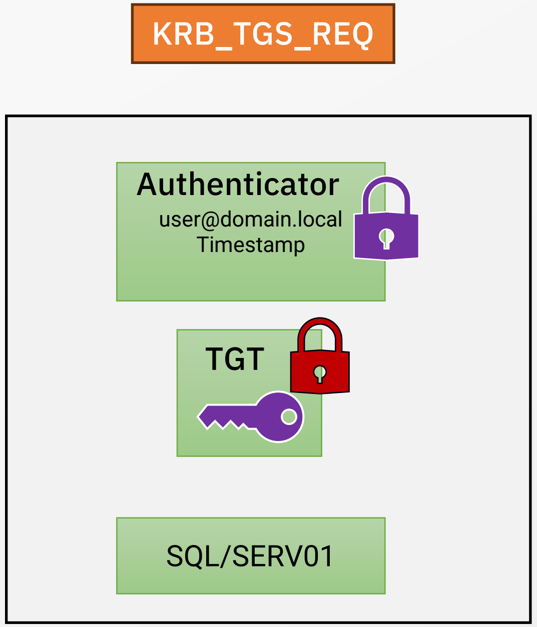
Authenticator

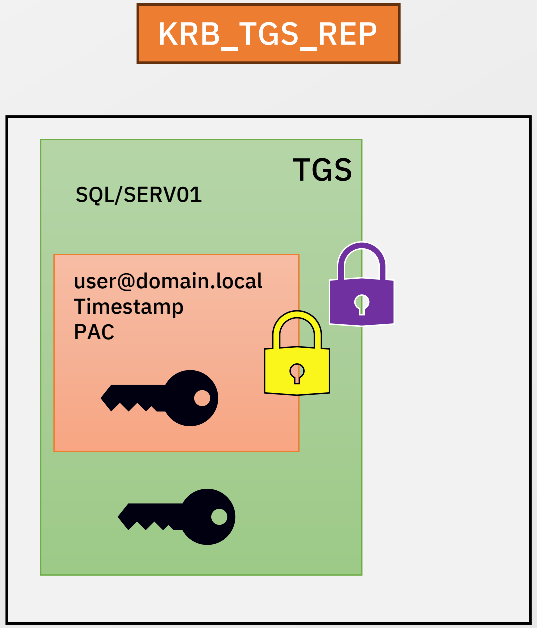
user@domain.local
Timestamp

Authenticator

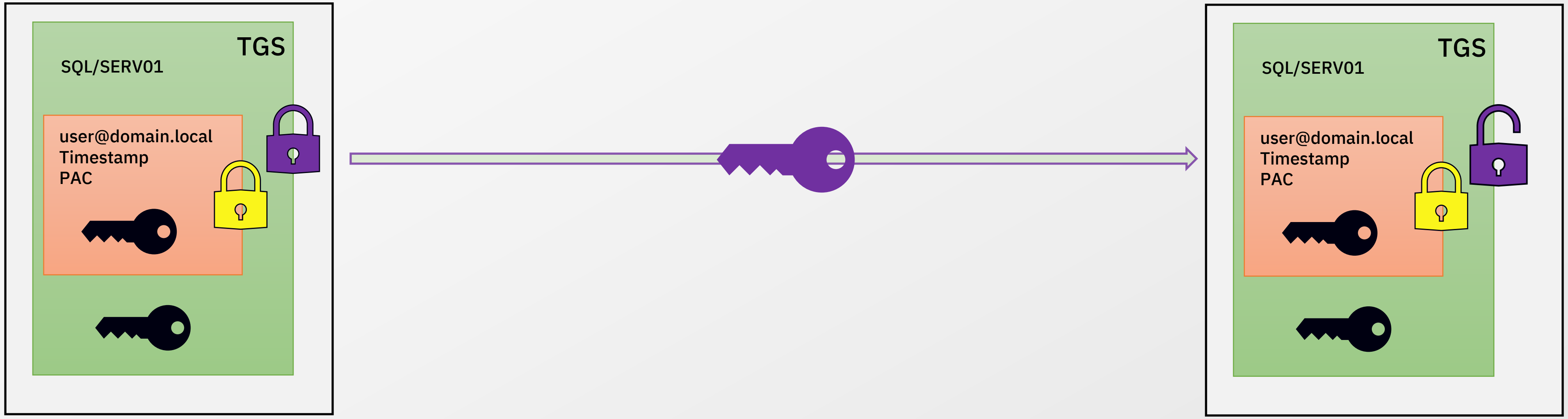
user@domain.local
Timestamp

Ticket-Granting Service (tickets)

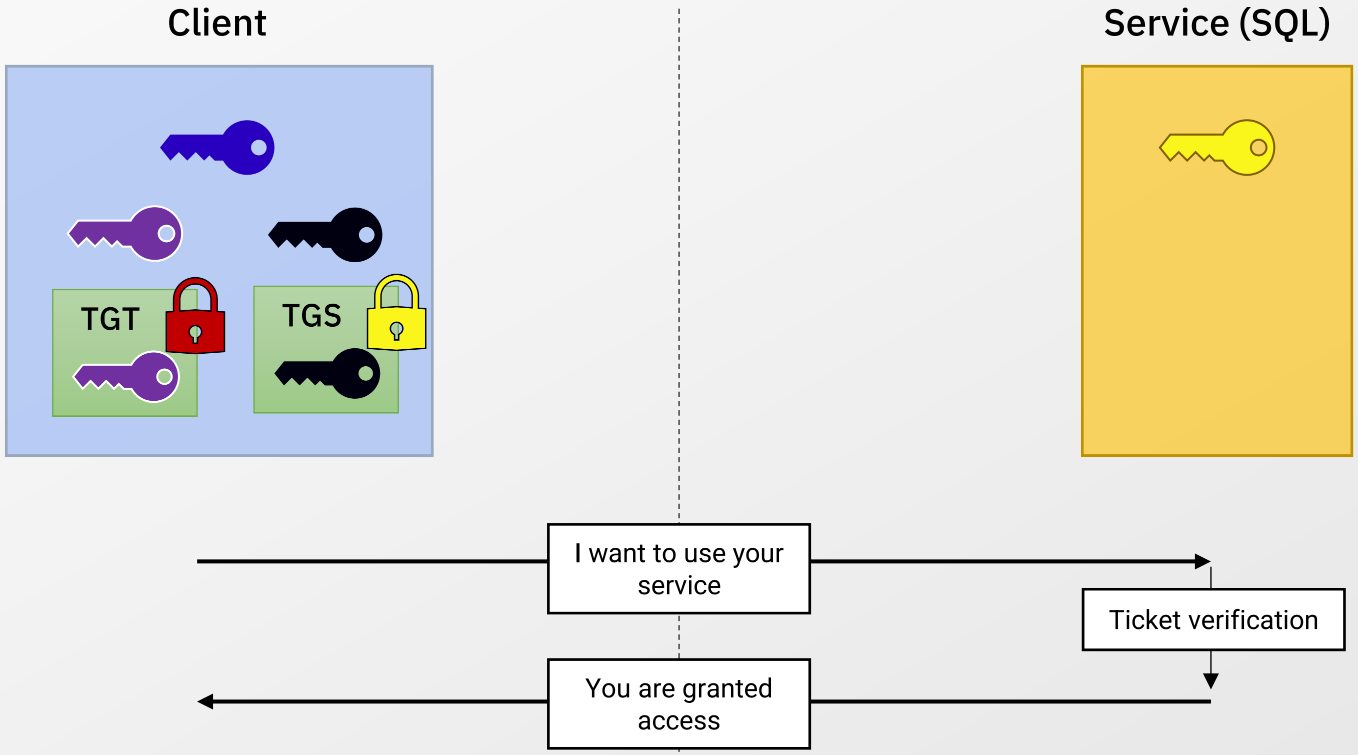




Ticket-Granting Service (Client)

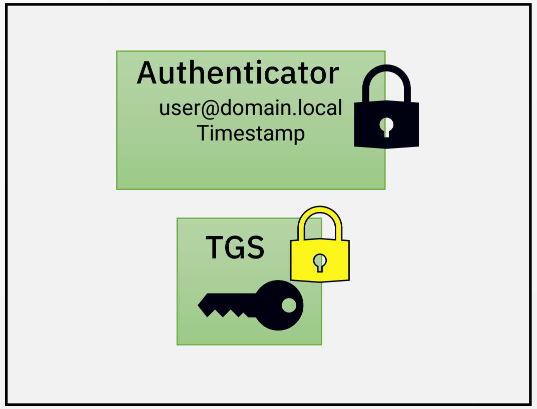


Application Request



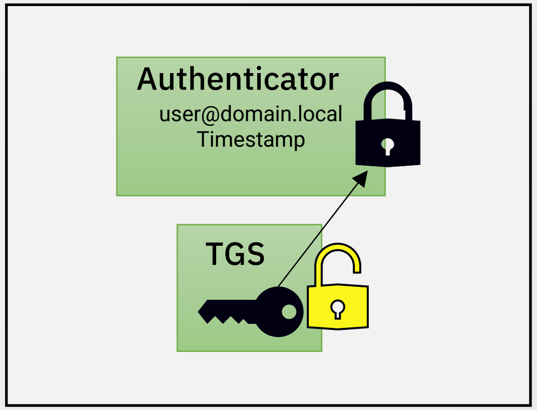
Application Request (Service)

KRB_AP_REQ



Authenticator
user@domain.local
Timestamp

TGS



Authenticator
user@domain.local
Timestamp

TGS

KRB_AP_REP

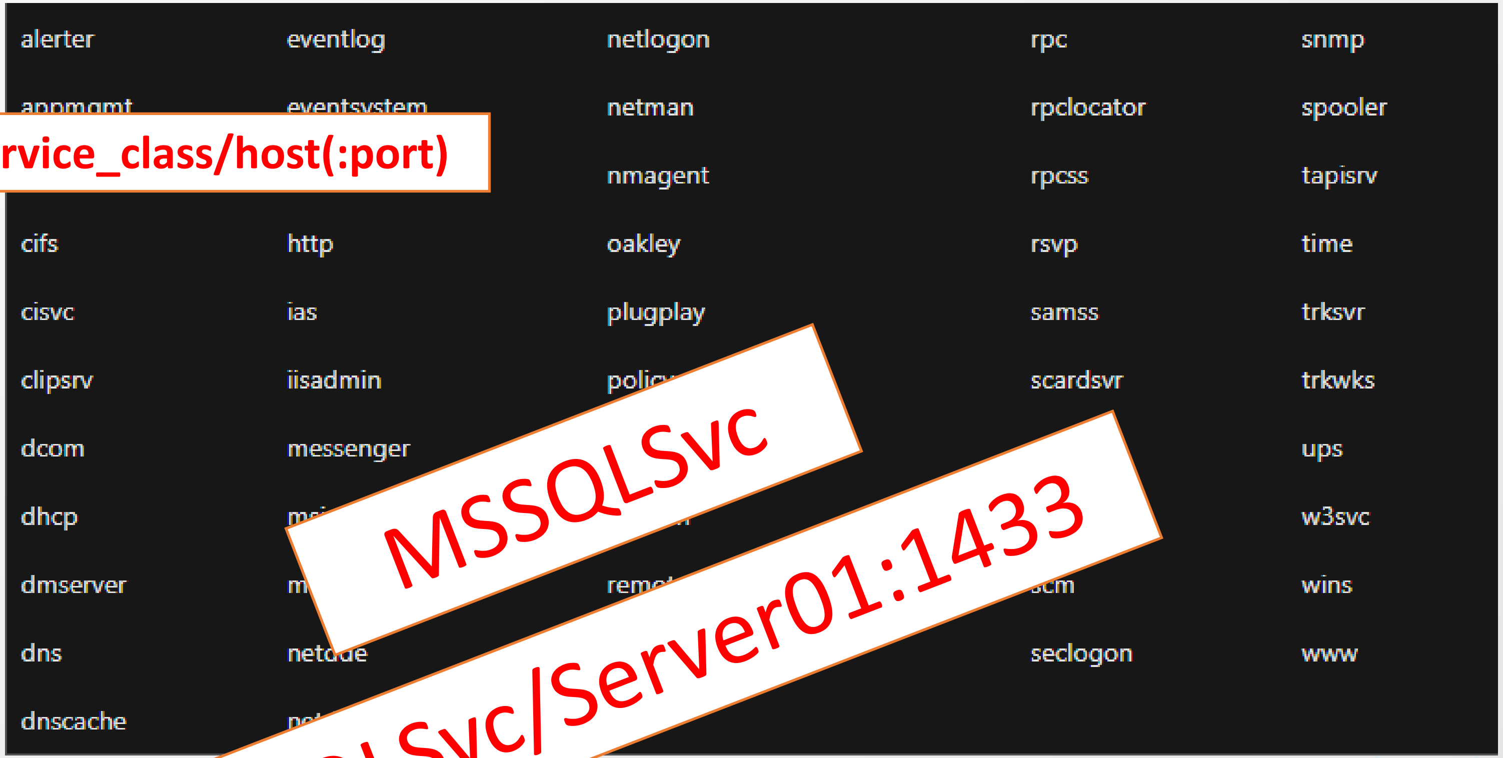
ON TOUR | NEW YORK

PASS

Service Principal Names

Service Principal Names

- What is a Service?
- SPN Definition
- Service Class
- SQL Server



alerter
appmgmt
cifs
cisvc
clipsrv
dcom
dhcp
dmserver
dns
dnscache

eventlog
eventsystem
http
ias
iisadmin
messenger
ms
m
netdde
ne

netlogon
netman
nmagent
oakley
plugplay
polic
remo

rpc
rpclocator
rpcss
rsvp
samss
scardsvr
scm
seclogon

snmp
spooler
tapisrv
time
trksvr
trkwks
ups
w3svc
wins
www

service_class/host(:port)

MSSQLSvc

MSSQLSvc/Server01:1433

Commands

- SETSPN
  - setspn -l (list)
  - setspn -s (create)
  - setspn -d (remove)

ON TOUR | NEW YORK

PASS

Database Engine

Database Engine

Setup:

- Domain Controller (purpledc)
- SQL Server Host (sql22-01)
- Workstation (ws11)

DEMO

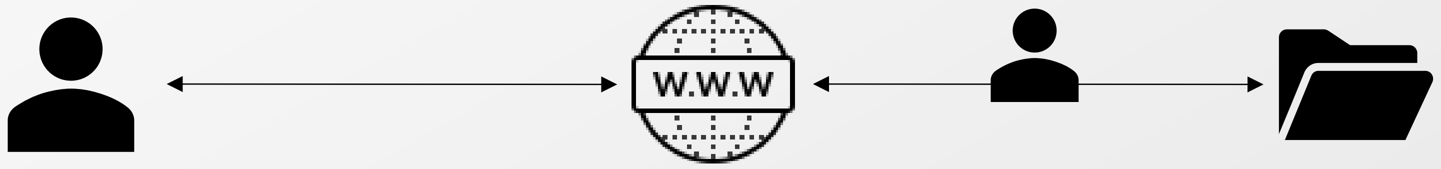
ON TOUR | NEW YORK

PASS

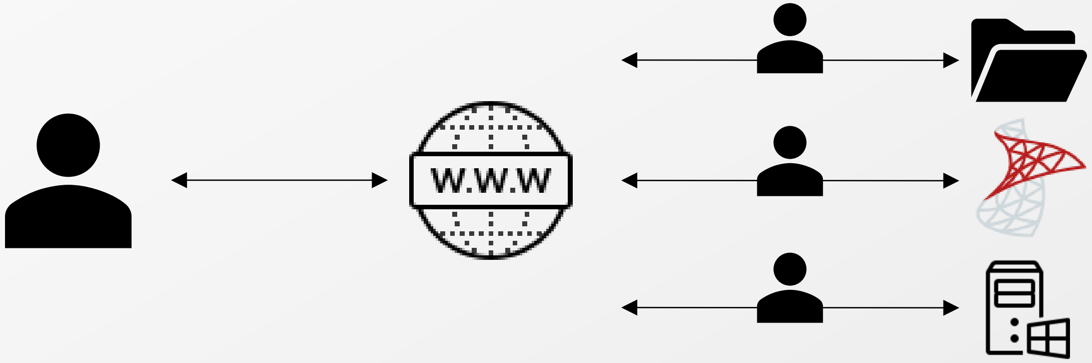
Delegation

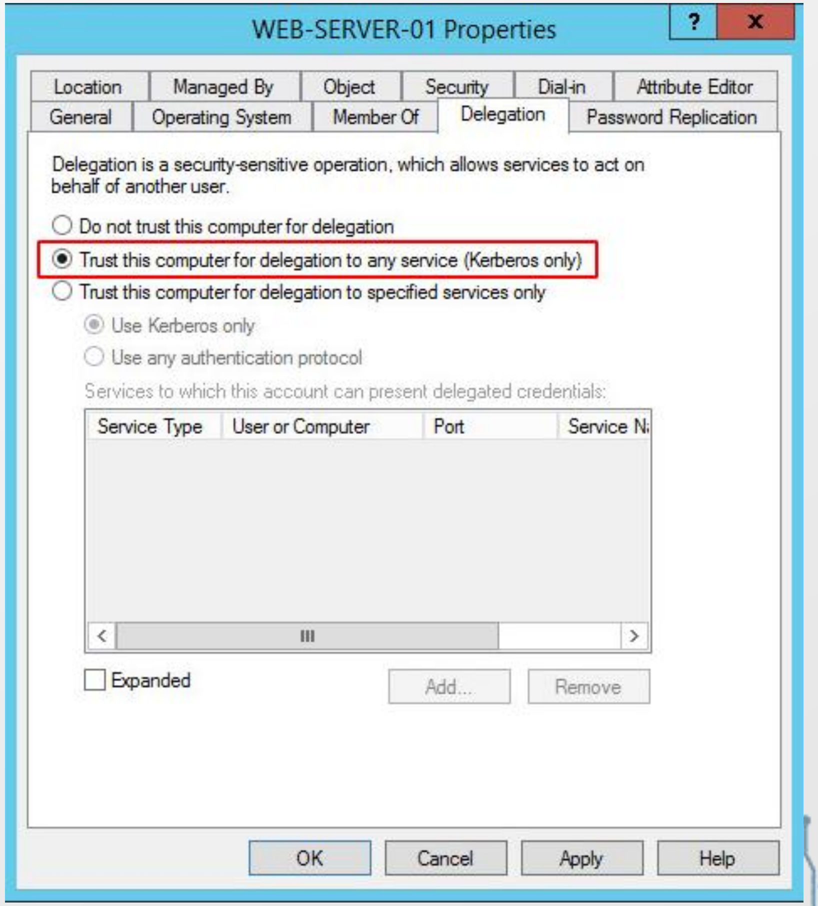
Delegation

- What is delegation?



Unconstrained Delegation




WEB-SERVER-01 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

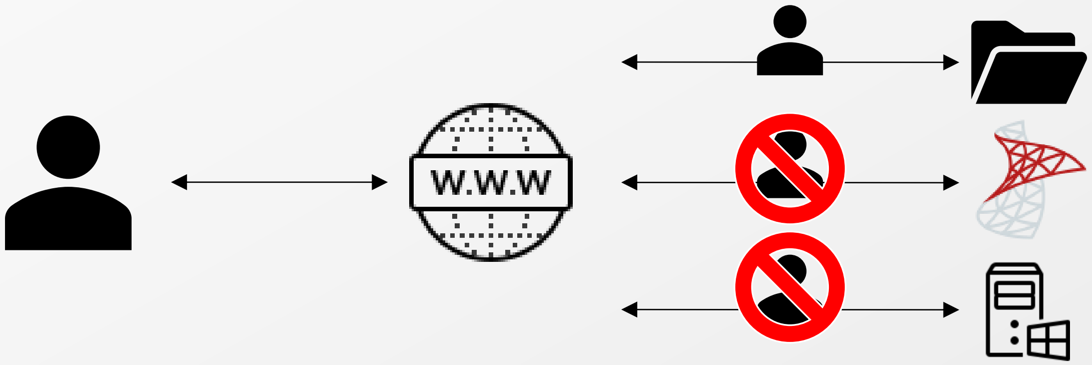
Services to which this account can present delegated credentials:

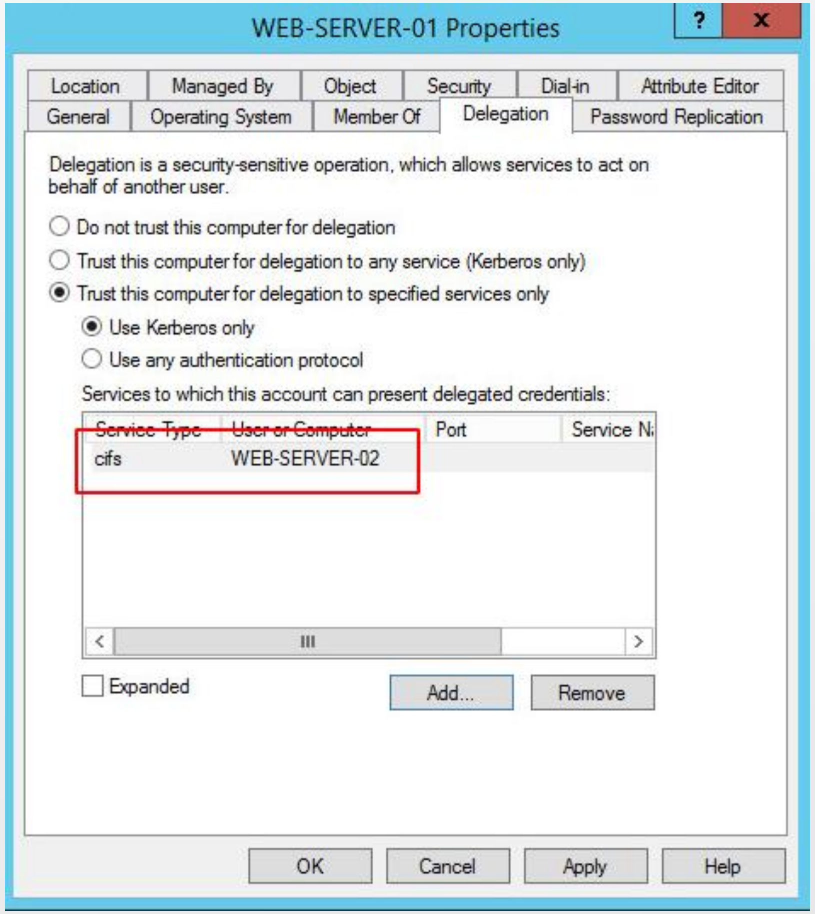
Service Type	User or Computer	Port	Service N

□ Expanded

Constrained Delegation

Constrained Delegation:
CIFS/WEB-SERVER-02





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:
cifs	WEB-SERVER-02		

□ Expanded

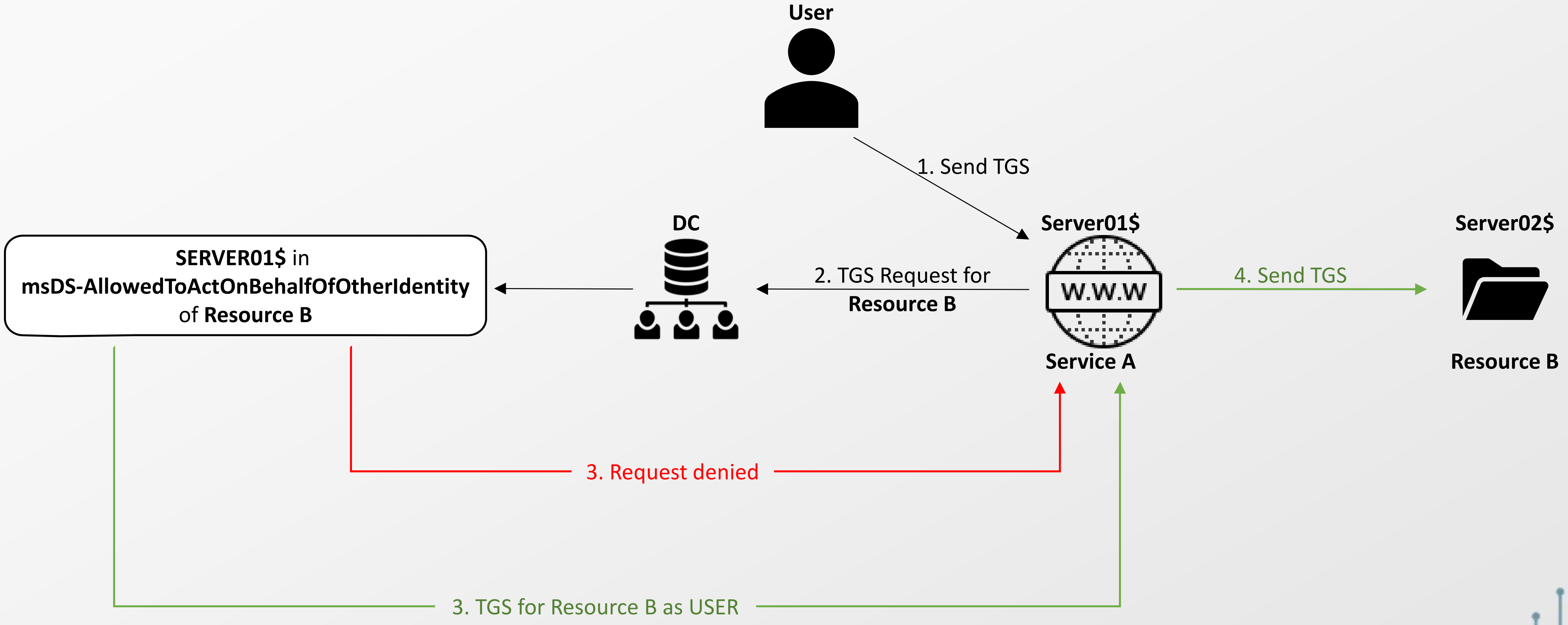
Resource Based Constrained Delegation

- Responsibility lies with the Back-end Service
- Inter-Domain delegation
- Can be configured using PowerShell or Extended Attributes

New-ADComputer	Set-ADComputer
New-ADServiceAccount	Set-ADServiceAccount
New-ADUser	Set-ADUser

PrincipalsAllowedToDelegateToAccount

Resource Based Constrained Delegation



Delegation Summary

- **Unconstrained delegation**: In this case, the client sends a copy of his TGT to a service, and that service uses it to impersonate the client to any other service. *Only an administrator can set this option on an account.*
- **Constrained delegation**: A list of resources is set on the service that wishes to delegate authentication. If protocol transition is allowed, then the service can pretend to be anyone when accessing resources in its list. *In any case, only an administrator can set this option.*
- **Resource-based Constraint Delegation**: The final resource has a list of trusted accounts. All accounts in this list can delegate authentication when accessing the resource. *Resources can modify this list as they wish, they don't need an administrator to update it.*

ON TOUR | NEW YORK

PASS

Reporting Services

Reporting Services

- WinRM uses HTTP Service Class on machine name
- SPN on different A-record for Reporting Services
- Constrained Delegation to HTTP SPN
- Constrained Delegation to SPN of Data Source (MSSQLSvc)

Reporting Services Demo

Setup:

- Domain Controller (purpledc)
- SQL Server Host (sql22-01)
- Reporting Services (ssrs01 on sql22-01)
- SQL Server Host (sql22-02)
- Workstation (WS11)

DEMO

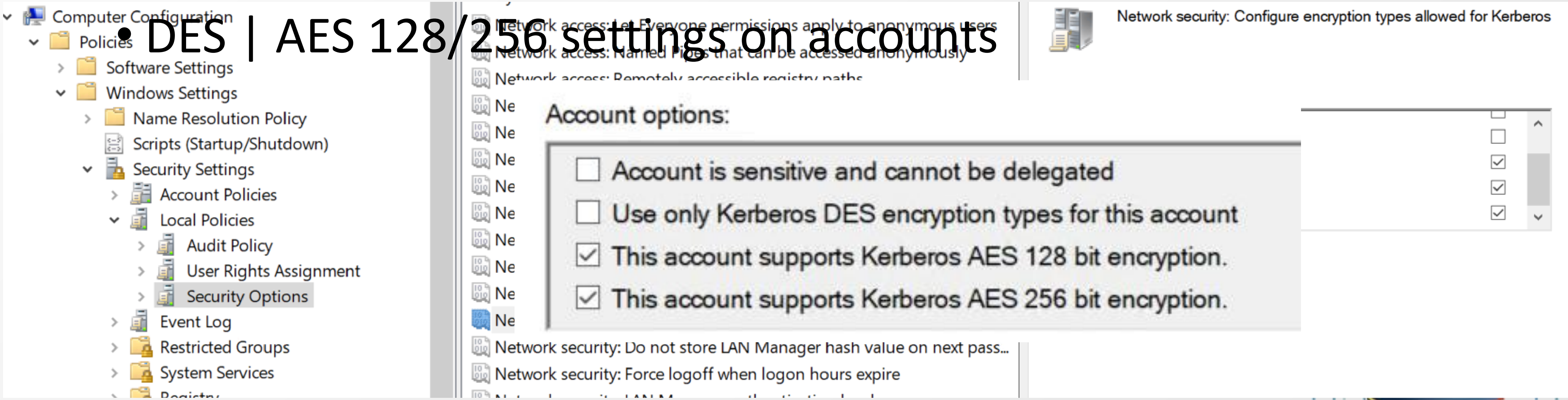
ON TOUR | NEW YORK

PASS

Troubleshooting Tips

Ciphers

- Network Security Settings (Network security: Configure encryption types allowed for Kerberos)
- DES | AES 128/256 settings on accounts



Network access: Let Everyone permissions apply to anonymous users

Network access: Named Pipes that can be accessed anonymously

Network access: Remotely accessible registry paths

Ne

Ne

Ne

Ne

Ne

Ne

Ne

Ne

Ne

Network security: Do not store LAN Manager hash value on next pass...

Network security: Force logoff when logon hours expire

Network security: Configure encryption types allowed for Kerberos

□
□
☑
☑
☑

Account options:

- □ Account is sensitive and cannot be delegated
- □ Use only Kerberos DES encryption types for this account
- ☑ This account supports Kerberos AES 128 bit encryption.
- ☑ This account supports Kerberos AES 256 bit encryption.

Troubleshooting Tips

- Verify SPN’s
- Verify delegation settings
- Microsoft Kerberos Configuration Manager / SQLCHECK
- Ensure the account can be delegated

https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/connect/resolve-connectivity-errors-checklist

ON TOUR | NEW YORK

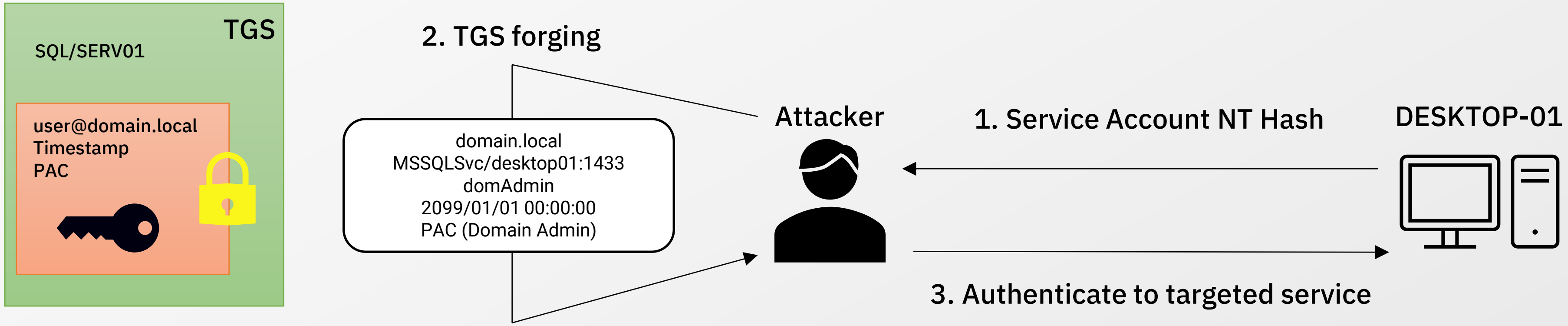
PASS

Attack Scenario’s

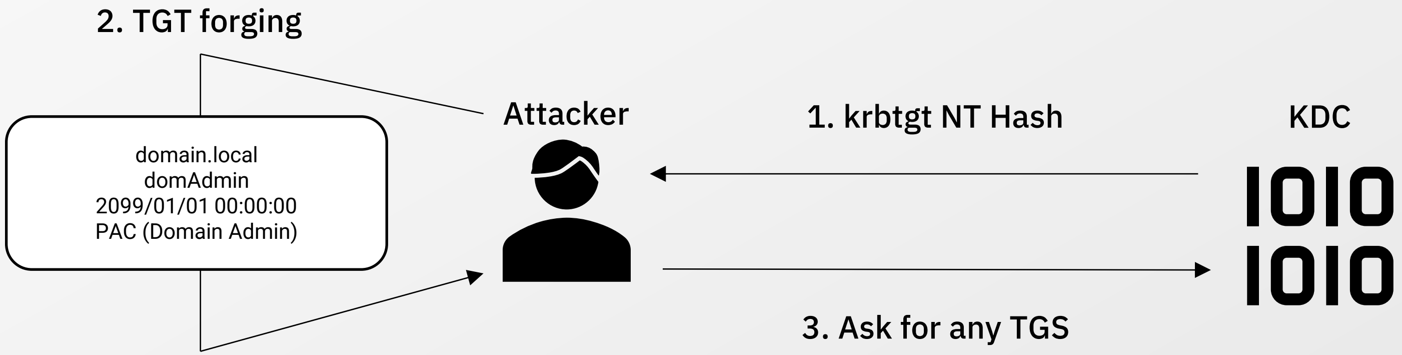
Attack Scenario’s

- Pass the Hash
- Pass the Ticket
- Kerberoasting
- Silver / Golden Tickets

Silver Ticket



Golden Ticket



2. TGT forging

domain.local
domAdmin
2099/01/01 00:00:00
PAC (Domain Admin)

Attacker

1. krbtgt NT Hash

KDC

3. Ask for any TGS

How to protect?

- Encryption ciphers (only AES128/128/future ciphers)
- Honey pots (weak account security)
- Credential Guard

Lessons Learned

- Kerberos phases
- Service Principal Names
- Delegation
- How to set up SQL Server & Reporting Services
- Troubleshooting tips
- Attack scenario’s

Your feedback is important to us

Evaluate this session at:

passdatacommunitysummit.com/evaluation-nyc

Thank you

Enjoy the rest of the event!

Danny de Haan

thatinfradba@pm.me

in /in/dannydh