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

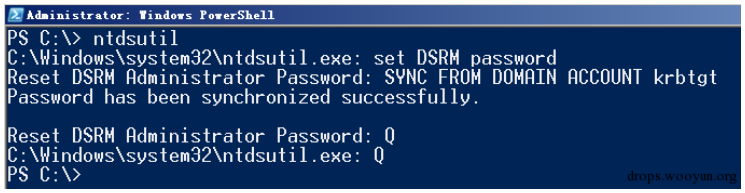
0x00 前言

本文将会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

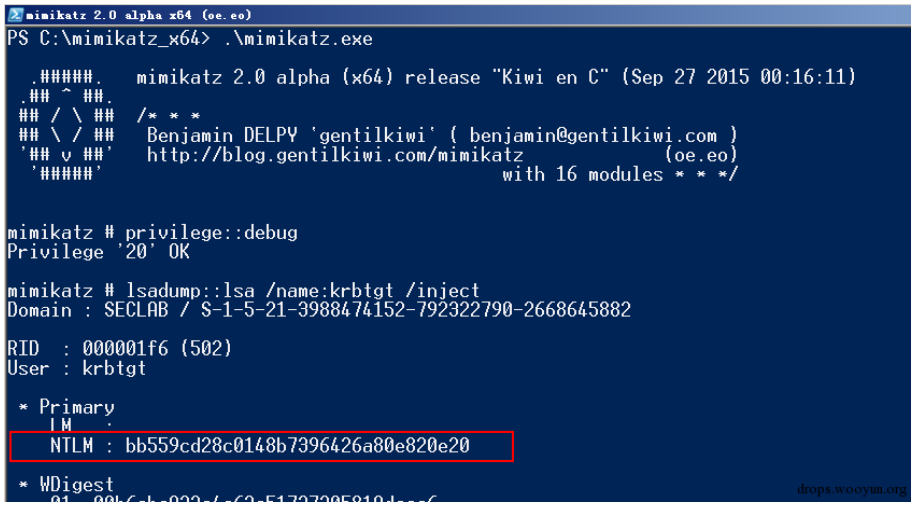
0x01 DSRM密码同步

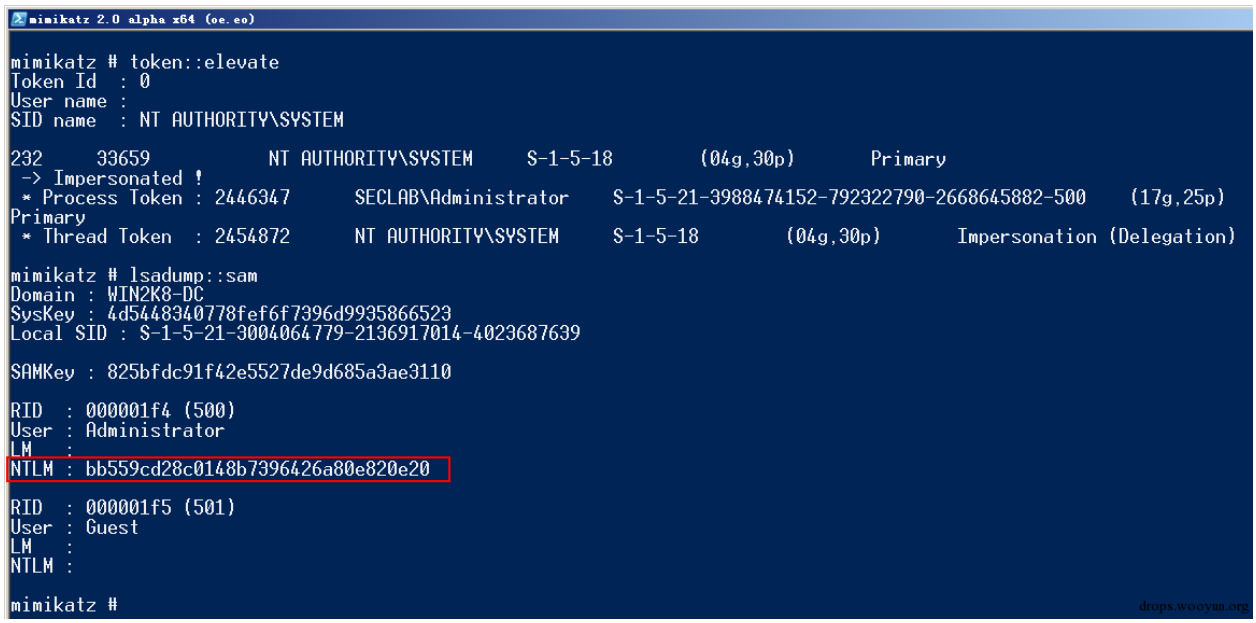
这里使用系统安装域时内置的用于Kerberos验证的普通域账户krbtgt。



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。

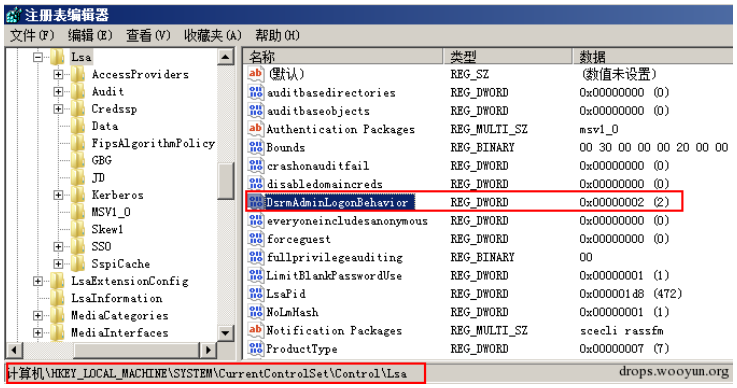




0x02 修改注册表允许DSRM账户远程访问

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。

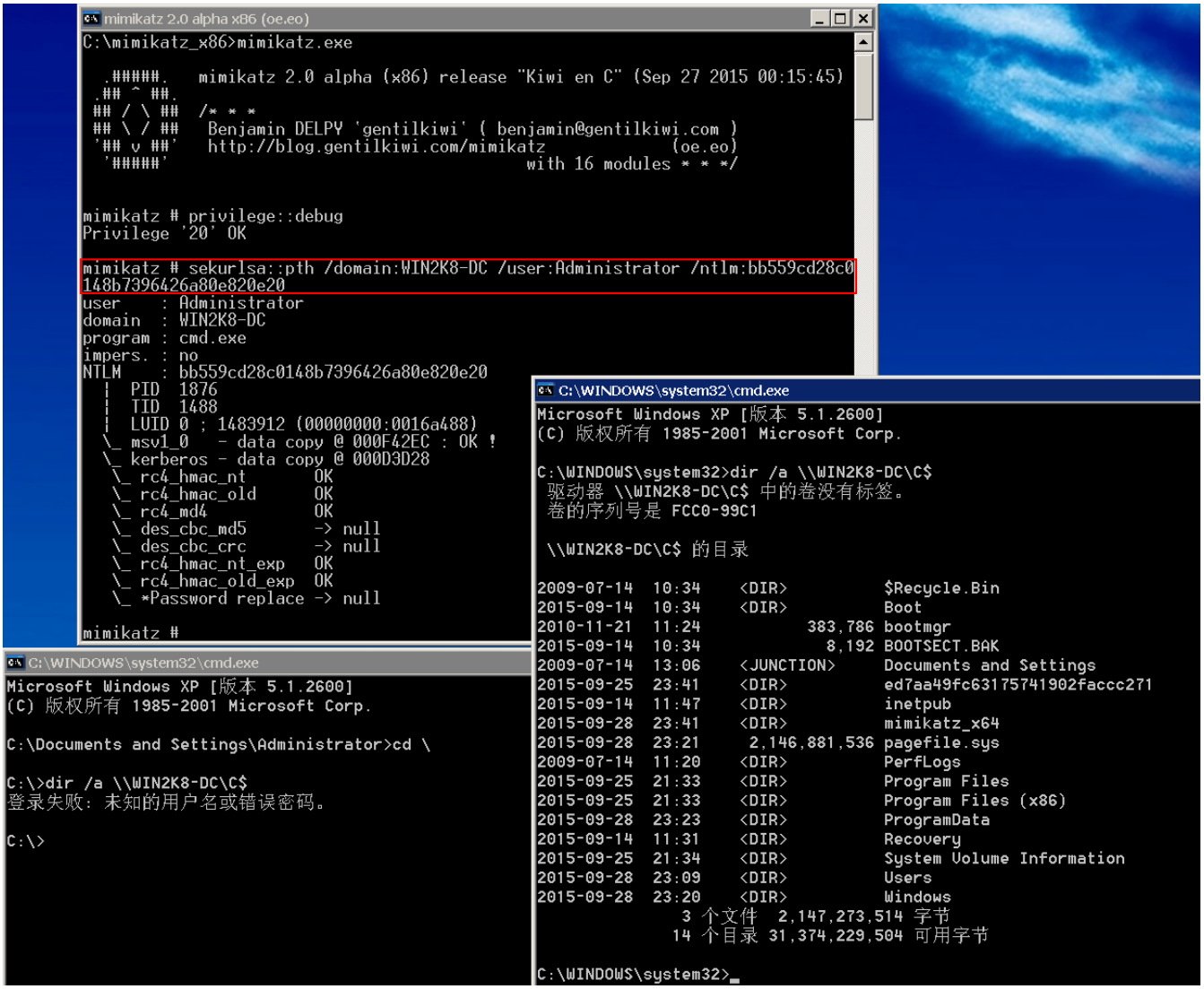


0x03 使用HASH远程登录域控

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，在下一次进行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。