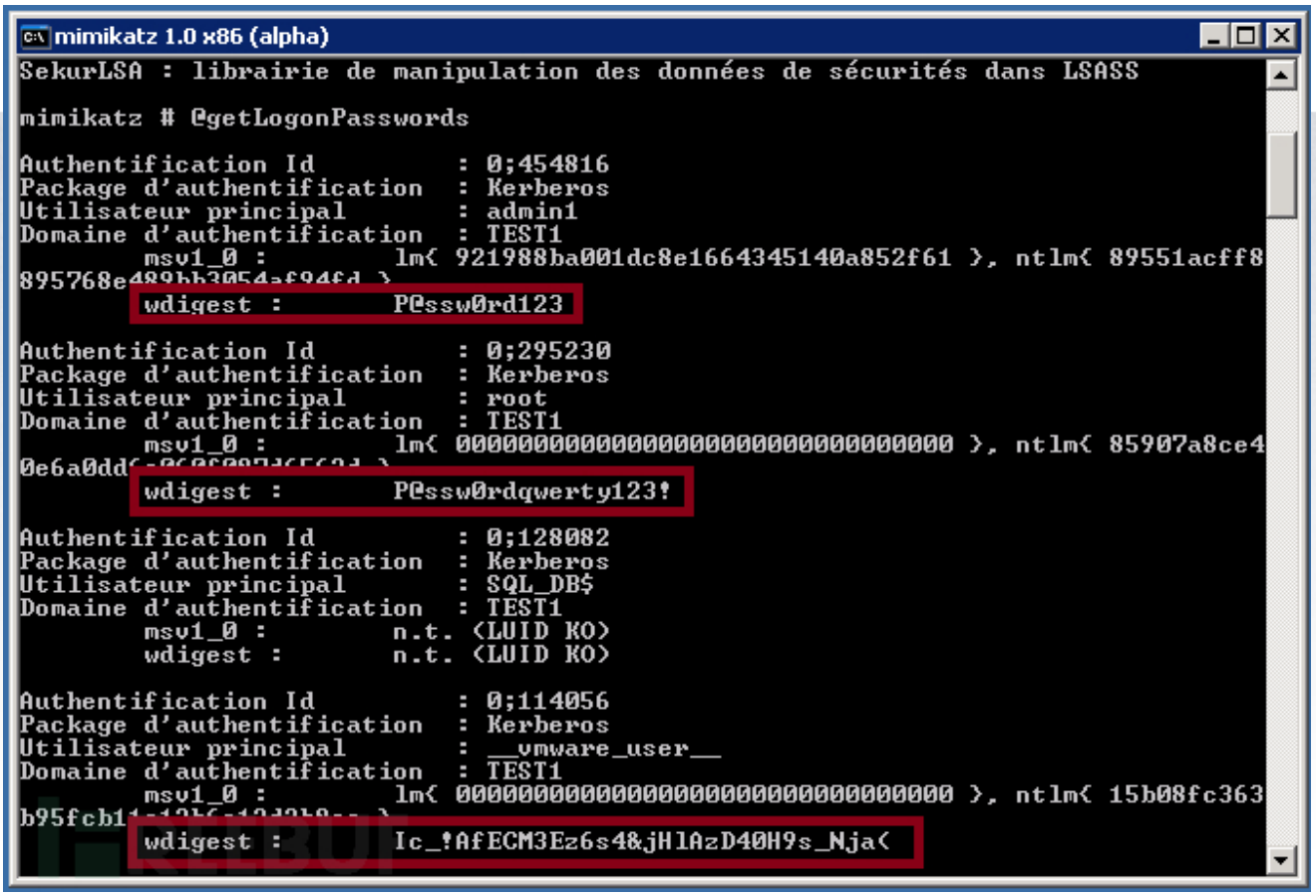


Mimikatz是一款能够从Windows中获取内存，并且获取明文密码和NTLM哈希值的神器，本文将介绍如何防御这款软件获取密码。

Mimikatz介绍

Mimikatz是一款能够从Windows认证(LSASS)的进程中获取内存，并且获取明文密码和NTLM哈希值的工具，攻击者可以借此漫游内网。他们可以通过明文密码或者传递hash值来提权。可能很多人会问“难道微软就没想过怎么防御吗？”

在Google上搜索“mimikatz的防御”，你会发现搜索结果很有限。我找到的最好的一篇文章就是这篇。里面提到了很多好的建议，诸如使用最近版本的活动目录中的“受保护的用户”用户组(SID:S-1-5-21–525)，或者是限制使用管理员，或者通过注册表设置不在内存中储存密码。你可以限制以系统身份运行的服务数量，或者移除调试权限，防止攻击者使用mimikatz。这篇文章和其他的那些文章都要让你安装Windows8或者8.1或者10版本。那那么多运行Windows7/2008 R2的电脑怎么办呢？对于这些版本的Windows，你一样有防御手段。

防御措施

第一步：Active Directory 2012 R2功能级别

首先你可以升级你的域或林的功能级别到2012 R2。这个级别添加了个“受保护的用户”用户组。如果你看过TechNet上对它的介绍，你可能会感觉这个用户组会防止mimikatz获取密码。实际情况是怎样的呢？

```
Session           : Interactive from 2
User Name         : Administrator
Domain            : TESTDOMAIN
Logon Server      : WIN-12UU57SPIN9
Logon Time        : 1/31/2016 12:51:07 PM
SID               : S-1-5-21-1100472043-2579244664-3974358937-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : TESTDOMAIN
         * NTLM     : 1543a4536a25d208e652dba231e73cdd
         * SHA1     : 9621d46214582077d5b31ed76fe8f59d899b4ccf
         [00010000] CredentialKeys
         * NTLM     : 1543a4536a25d208e652dba231e73cdd
         * SHA1     : 9621d46214582077d5b31ed76fe8f59d899b4ccf
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : TESTDOMAIN
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : TESTDOMAIN.LOCAL
         * Password : (null)
        ssp :   KO
        credman :
```

注意：对于非保护用户，mimikatz是可以获取到NTLM哈希的。

```
Authentication Id : 0 ; 144339 (00000000:000233d3)
Session           : Interactive from 1
User Name         : Administrator
Domain            : TESTDOMAIN
Logon Server      : WIN-12UU57SPIN9
Logon Time        : 1/31/2016 10:54:46 AM
SID               : S-1-5-21-1100472043-2579244664-3974358937-500
        msv :
         [00010000] CredentialKeys
         * RootKey  : 3d209d9c7e8dd2a68c9bb01c44fa47866cef6bc2d34694c9448588d630
929004
         * DPAPI    : 514e5c8e20264c64b7de758dd8541717
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : TESTDOMAIN
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : TESTDOMAIN.LOCAL
         * Password : (null)
        ssp :   KO
        credman :
```

而当用户被添加到保护用户组的时候，NTLM哈希和明文密码都看不到了。

很显然，这招很管用，那Windows 7或者2008 R2上的保护用户组又是怎样的呢？

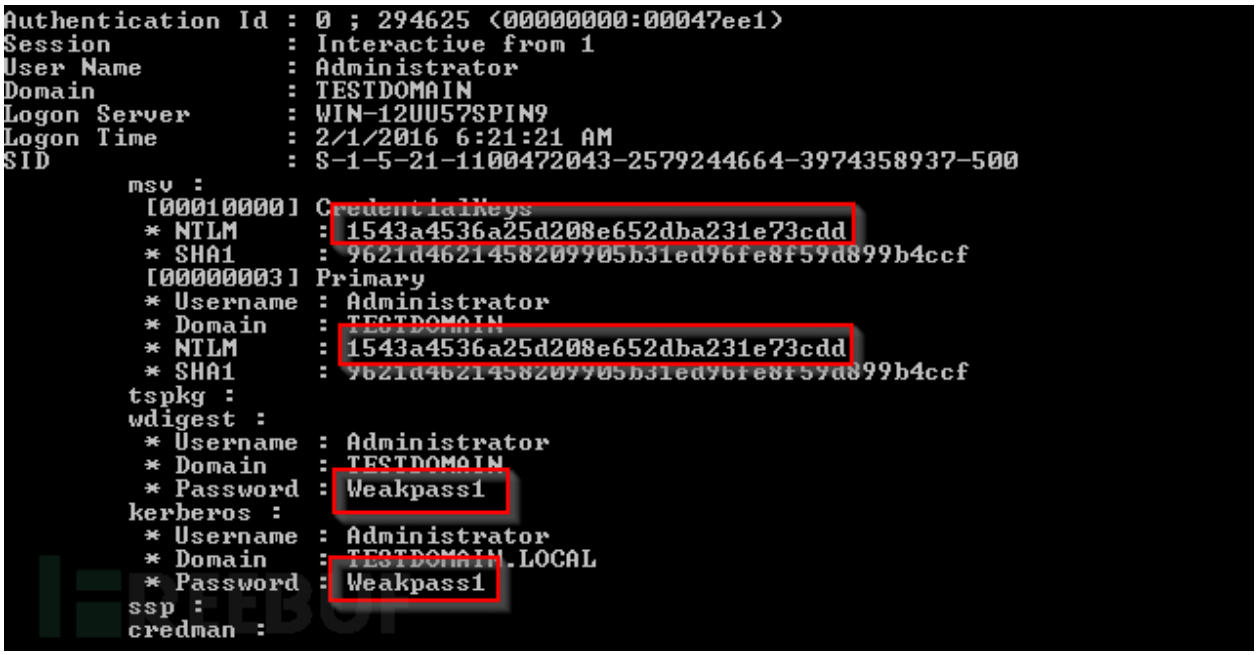
```
Authentication Id : 0 ; 93291 (00000000:00016c6b)
Session           : Interactive from 1
User Name         : administrator
Domain            : TESTDOMAIN
Logon Server      : WIN-12UU57SPIN9
Logon Time        : 1/31/2016 11:08:02 AM
SID               : S-1-5-21-1100472043-2579244664-3974358937-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : TESTDOMAIN
         * LM       : 19a78e2624d768e48ee2eb564b068947
         * NTLM     : 1543a4536a25d208e652dba231e73cdd
         * SHA1     : 9621d46214582077d5b31ed76fe8f59d899b4ccf
        tspkg :
         * Username : Administrator
         * Domain   : TESTDOMAIN
         * Password : Weakpass1
        wdigest :
         * Username : Administrator
         * Domain   : TESTDOMAIN
         * Password : Weakpass1
        kerberos :
         * Username : administrator
         * Domain   : TESTDOMAIN.LOCAL
         * Password : Weakpass1
        ssp :
        credman :
```

可以看到，即使加入了保护用户组，密码和哈希还是可见的。

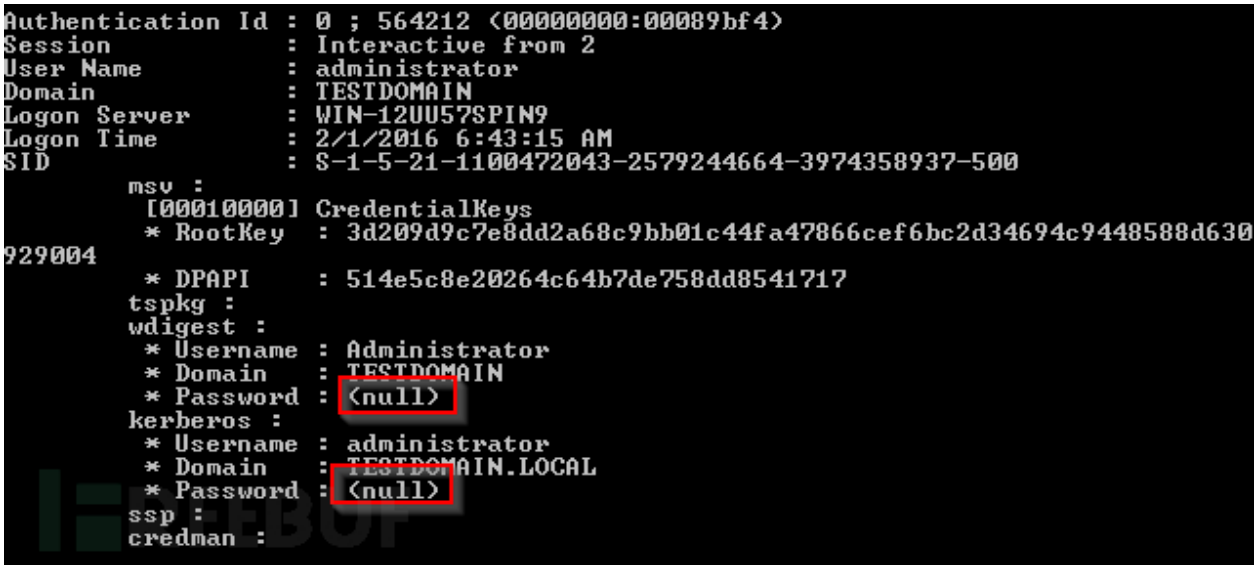
不过这台机器没有打过补丁。实际上如果电脑不知道保护用户组意味着什么，那这个用户组也就失去了意义。幸运的是，微软已经把这个Windows8.1 和2012R2有的功能移植到旧版本的Windows上了。

第二步：安装KB2871997

如果你一直安装Windows更新的话，KB2871997应该已经装好了。这个更新会把保护用户组的功能移植到旧版的Windows中。一旦安装了这个更新，Windows2008 R2就也能防御mimikatz了。



安装KB2871997更新后没有把用户放入保护用户组就是这样的效果



而一旦加入了保护用户组，效果就跟2012 R2上的一样了

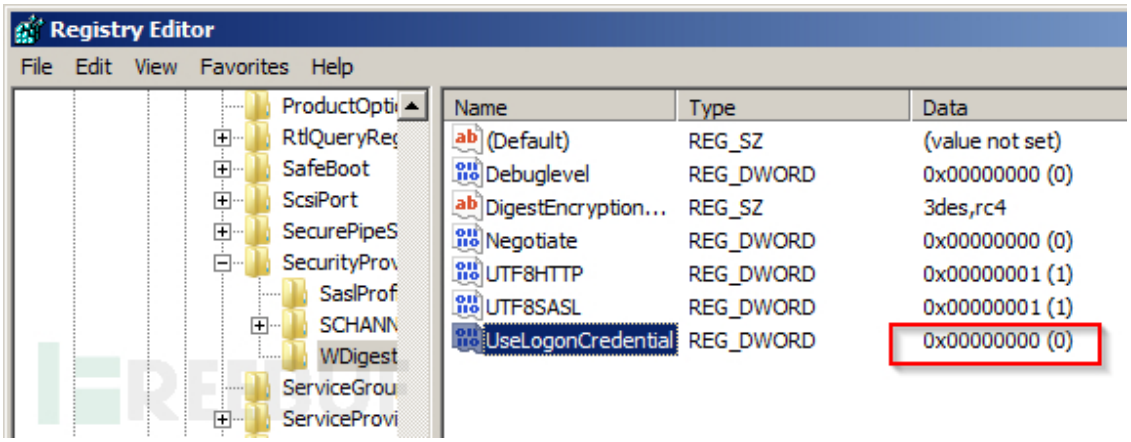
第三步：去除内存中的存储空间

这一步是可选的，因为你可能想把所有的账号放到保护用户组里面，但是实际上不行。微软反对把计算机账号和服务账号放到保护用户组里面。所以这一步是针对那些不在保护用户组里面的用户的。

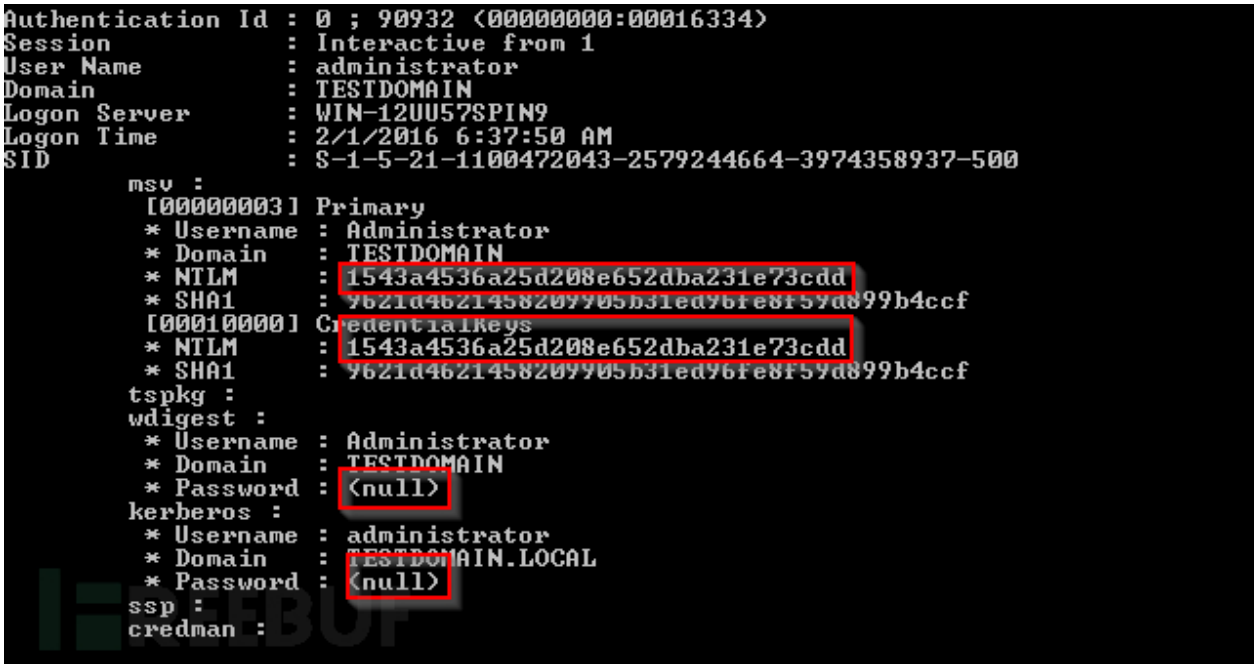
在Windows 2012 R2上，无论用户有没有被添加到保护用户组，mimikatz都没有获取到过密码，而Windows2008中，如果不添加到保护用户组，mimikatz还是能够获取密码的。

密码的存储是由一个注册表设置决定的。就像保护用户组的功能一样，在新版本的Windows(8.1+ & 2012R2+)中，密码默认不会储存在内存中。这一特性也在KB2871997更新中被移植到了老版本中。但是由于兼容原因，在安装更新后，老版本人就会默认在内存中存储密码。你只要把注册表中的“UseLogonCr

edential”项设置成0就好了。




```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest
```



这位用户没有被添加到保护用户组，但是注册表的值改过了，因此，Mimikatz无法获取到明文密码。

结论

总结一下，把Active Directory功能级别升级到2012 R2，及时进行Windows更新，把重要账号加入保护用户组，设置注册表值。另外，不要授予账号过多的管理权限。希望这篇文章能够帮助大家防御Mimikatz。

*** 参考来源：Jim Shaver** >