**内网渗透用frp实现反向代理**

frp客户端上传到dmz区用拥有内外网的主机

frp服务端上传到公网vps主机

攻击机通过vps主机实现的代理服务器访问到内网主机

这种操作就相当于反向代理中的“服务器通过代理服务器访问客户端主机”

所以是反向代理

环境搭建

vps-frp服务端：

主机名Win10(lizhikai001)

IP 192.168.52.130

Web服务器-frp客户端：

主机名 win10(lizhikai002)

互联网IP 192.168.52.132

内网IP 192.168.200.129

Phpstudy开启web服务

防火墙关闭

内网主机：

主机名 win10(lizhikai003)

内网IP 192.168.200.130

phpstudy开启web服务

防火墙关闭

高级防火墙出入站规则禁止宿主机的ip连接虚拟机lizhikai003

说明：经过环境搭建之后，实现宿主机无法访问内网主机的web服务

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

工具准备

frp

下载地址：<https://github.com/fatedier/frp/releases/tag/v0.37.1>

frp配置

服务端配置



运行以下命令：

.\frps.exe -c .\frpc.ini

文本

描述已自动生成

客户端配置

[common]

server\_addr = 192.168.52.130

server\_port = 7000

[socks5]

type = tcp

remote\_port = 6666

plugin = socks5

use\_encryption = true

use\_compression = true

图形用户界面

中度可信度描述已自动生成

运行下面的命令

.\frpc.exe -c .\frpc.ini

图片包含 文本

描述已自动生成

宿主机（攻击机）配置

在浏览器中使用插件，并且按照该图中的进行配置，ip为vps的公网ip，端口为客户端上配置的socks5中的端口。

图形用户界面, 应用程序

描述已自动生成

代理结果

文本

描述已自动生成

代理成功